NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

JOINT TASK FORCE OLYMPICS: MONITORING POTENTIAL TERRORISTS' BEHAVIOR VIA DECEPTIVE COMPUTER MEANS

by

Christopher Cheung
and
Daniel J. Zodda

June 2002

Thesis Advisor:	Steven J. Iatrou
Second Reader:	Hy Rothstein

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Joint Task Force Olympics: Monitoring Potential Terrorists' Behavior Via Deceptive Computer Means			**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher Cheung and Daniel J. Zodda			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Authorized for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The purpose of this thesis is to deploy tactical deception via a public website. The perception is to have the website be a supportive tool for the Joint Task Force Olympics. In actuality, it will be used to collect various data from those who attempt to access the site. The goal is not to implement a secure, impenetrable computer site or to capture hackers. On the contrary, the preference is to entice individuals or groups to enter the site and study its contents in the hope that we may discover why and from where they have accessed this site, and what files or directories allured them. The objective is to implement a successful deception by following the guidelines of the JP 3-58, *Joint Doctrine for Military Deception,* which contributes to the successful achievement of military objectives. The deception is focused on people researching information on the Internet for potential terrorist use. Although there are many threats to national security, terrorism is currently the most deadly of threats using one of the most trusted monitors: the Internet. There exists a relationship between the Internet and terrorism, and this thesis intends to exploit it with deception.

14. SUBJECT TERMS Information Operations, Web Deception, Deception, Terrorism, Internet, Honeypots, Homeland Security, Homeland Defense			**15. NUMBER OF PAGES** 99
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

JOINT TASK FORCE OLYMPICS: MONITORING POTENTIAL TERRORISTS' BEHAVIOR VIA DECEPTIVE COMPUTER MEANS

Christopher Cheung
Ensign, United States Naval Reserve
B.S., United States Naval Academy, 2001

Daniel J. Zodda
Ensign, United States Naval Reserve
B.S., Florida State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL

June 2002

Authors: Christopher Cheung

Daniel Zodda

Approved by: Steven J. Iatrou
Thesis Advisor

Hy Rothstein
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to employ tactical deception via a public website. The perception is to have the website be a supportive tool for the Joint Task Force Olympics. In actuality, it will be used to collect various data from those who attempt to access the site. The goal is not to implement a secure, impenetrable computer site or to capture hackers. On the contrary, the preference is to entice individuals or groups to enter the site and study its contents in the hope that their origins, habits, and characteristics may be studied, and what files or directories on the website lured them. The objective is to implement a successful deception by following the guidelines of the JP 3-58, *Joint Doctrine for Military Deception,* which contributes to the successful achievement of military objectives. The deception is focused on people researching information on the Internet for potential terrorist use. Although there are many threats to national security, terrorism is currently the most deadly of threats, using one of the most trusted monitors: the Internet. There exists a relationship between the Internet and terrorism, and this thesis intends to exploit it with deception.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors want to thank LCDR Steven J. Iatrou, USN and Professor Hy Rothstein for their guidance and patience during the work in performing this investigation. In addition, we would like to thank Capt. Jesus Torres, USMC, and the rest of the members of the RIDLR staff for their technical assistance in setting up and maintaining the website. Finally, another "thank you" to ENS Will Rimmer, USN for setting up the server and volunteering to help us out.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Winter Olympic Games were held in Salt Lake City, Utah from 8-24 February 2002. This city of 181,743 gathered about 3,500 athletes and officials; 174,000 spectators; and over 13,000 media persons during the seventeen days of competition. The Olympics consisted of 140 ticketed events; 70 medal events and over 70 non-competition venues, which added 38,000 vendors and volunteers to the already substantial number of new arrivals to Salt Lake City. It was a priority to provide safety and security for the competitors, visitors, local residents and businesses. In the aftermath of the terrorist attacks on the World Trade Center and the Pentagon, the Olympics offered a grand stage for terrorists to make a destructive and deadly statement, with plenty of television coverage, numerous spectators, and involvement of over 80 nations. As a result, unprecedented security measures were developed and carried out in Salt Lake City.

The Winter Olympics presented a lucrative setting for criminals and terrorists. Likewise, the Winter Olympics presented a near-perfect laboratory for experiments in deception. The intent of this thesis was to determine trends that may be associated with terrorist activity by employing selected deception techniques on the Internet. This study was done in conjunction with the Joint Task Force Olympics (JTFO), under the authority of United States Joint Forces Command (USJFCOM). The JTFO was the organization responsible for security at the Olympics. The focus of this research was to determine which information (directories, files, documents) and links would entice individuals with terrorist profiles to seek access to a website. From this information, the following questions could be answered: What were their habits? Where were they located? How long were they in the site?

The methodology within this research included a review of the existing means of deception, particularly those associated with computers. The next step was to use selected deception tools on a website with a seemingly non-military orientation. The intent was not to implement a secure, impenetrable computer site or to capture hackers. On the contrary, the intent was to have hackers enter the site and study them without their

knowledge. There was an extensive examination of what phrases, key words, files, and other items may have triggered the interest of any individual to enter and search the website, located at **www.jtfo.org**. The operational plan involved obtaining information from the JTFO in order to carry out the deception and portray a realistic website. The hits on the website were recorded and entered into a database with assessments being supported by graphs and charts. The hope was to record, study and analyze patterns and behaviors in hopes of understanding the mentality of those interested in violating computer security and determine of whether those people were threats. The information collected focused on the existing profiles of terrorists and other transnational criminals. The data collected would hopefully be sufficient to execute deception operations in support of military or law enforcement activities against terrorists and other criminals.

II. BACKGROUND

During the fourth century B.C. Sun Tzu noted, "all warfare is based on deception."[1] In Tzu's opinion, the objective of deception in war is to throw the enemy into a state of confusion. This confusion provides an advantage that can be influential in the success of military operations, allowing those adept at deception to shape the battlefield before actually engaging in combat. Military deception is defined as:

> …those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission. (Joint Pub 3-58, 1996, 5)

Basically, deception is used to create a false reality in the minds of the enemy decision-makers. Creating this false reality, however, is a difficult task.

Joint Pub 3-58, "Joint Doctrine for Military Deception," provides some guidelines that, if followed, will help in creating this false reality. To create the false version of the operational situation JP 3-58 recommends the following:

1. All deception efforts should be **focused** on the single decision maker with the authority to effect the action required to meet your own objective.

2. All actions within a deception plan work toward a single **objective -** an action or inaction that must be carried out by the enemy to support your own cause. The objective of deception in general is to cause an enemy to take or not to take specific actions.

3. In deception, a single element must have **centralized control**. This is essential in order to avoid confusion and ensure that the various elements involved in the deception are portraying the same story and are not in conflict with other operational objectives. Centralized control of the deception plan and execution must be in place in order to achieve the high level of synergy between the deception plan and the actual operation plan.

---

1 Sun Wu Tzu, The Art of War. Translated by Samuel B. Griffith, the Oxford University Press, London, 1963, p. 66.

4. Airtight **security** must exist around the deception plan before the enemy realizes that they are being misled. Successful deception requires strict security, as information about the intent to deceive and the execution of that intent needs to be denied to the enemy.

5. Clever **timeliness** of each element of the deception plan must exist to allow the enemy time to observe intended indicators, process and correlate the information, and take appropriate action in support of your objective.

6. This entire deception plan must be **integrated** with the overall operation plan, both to increase its credibility to the target and help to accomplish military goals.

When focusing their deceptive tools, planners must target the enemy's decision maker. In a deception scheme, the objective is to cause the enemy decision-makers to perform or not perform a specific action. Well-planned schemes develop specific objectives. Determining exactly what actions are desired of the enemy will lead to a more defined and focused objective. Centralized control is essential to control and direct the deception, as well as ensuring leak-proof operational security. Deception alone does not defeat the enemy; it is used to enhance the effectiveness of other military operations. As Donald C. Daniel declares

> …there are three goals in any deception. The immediate aim is to condition a target's beliefs; the intermediate aim is to influence the target's actions; and the ultimate aim is for the deceiver to benefit from the target's actions. (1982, p. 5)

The proper implementation and adoption of these principles will provide the advantage needed to establish a false reality.

A. DECEPTION

There are two types of deceptions as pointed out by Donald C. Daniel, A-type and M-type. The A-type is characterized as an *ambiguous* deception scheme. The intent of this deception is to confuse the enemy to the point where the enemy is uncertain of what is real and what is not. A-type deception is designed to create and maintain a high level of uncertainty around the enemy, which will protect the secrecy of the real operation. An A-type deception forces the enemy to defend against several scenarios, thereby weakening the strength of each of those defenses. It forces the enemy to stretch its

resources thin in attempt to prepare for all possibilities. Examples of ambiguous deception schemes occurred during World War II in Operation Bodyguard and Operation Barclay. Bodyguard is an example of an overall A-type deception scheme that consisted of several individual M-type deception operations. Bodyguard supported the Allied invasion of Normandy. One of the Allies' primary goals was to prevent Germany from moving its forces from other European fronts into position to further strengthen the defenses along the English Channel coast. Bodyguard created ambiguity (A-type deception) with regards to the exact location of an Allied invasion. As a result insufficient German troops were moved to the Normandy beaches, enabling the Allies' landing. Operation Barclay was the deception plan for the Allied invasion of Sicily in 1943. Similar to the objectives of Bodyguard, Barclay's main goal was to create ambiguity of the timing and location of the invasion. (Daniel, 1982, p. 6) Both of these schemes succeeded in creating the false realities needed to maintain ambiguity in the mind of the enemy commanders.

The second type of deception, M-type, is characterized as *misleading*, which tries to reduce ambiguity around enemy decision-makers; the aim is to make them certain but wrong. The technique is effective in making the enemy think the deceiver is doing one thing, when in actuality the deceiver has chosen another course of action. In other words, the intent is to make the alternative scenario seem more appealing to the enemy than the actual one. The enemy should feel almost certain that the scenario created by the scheme is reality. The advantage of using such a deception lies in decreasing risk and surprising the enemy, which was obvious in Operations Barbarossa and Fortitude South. Plan Barbarossa was a German campaign to deceive Russian dictator Joseph Stalin, in order to achieve surprise during Germany's attack on Russia on 22 June 1941 (Daniel, 1982, p. 6). Operation Fortitude South was a subcomponent of the Allies' Operation Bodyguard. Fortitude South aimed to mislead the Germans by making them think the Normandy landings were simply a prelude to a larger invasion at Pas de Calais.[2] These M-type deception schemes were used to surprise the enemy when their accompanying actual operations took place. The two types of deception share the same objective of influencing enemy decisions, but follow different paths to achieve it. Both are

2 Operations Barbarossa Fortitude South is further described in Part B of this chapter.

advantageous when executed properly, and both provide the opportunity to gain the upper hand on the physical and virtual battlefields.

B. THE DECEPTION PROCESS

Now that elements and techniques have been examined, the theory and principles behind the deception process will be addressed in order to provide a complete analysis of deceptive measures. According to Donald C. Daniels and Katherine L. Herbig, deception consists of a loop with two distinct players, the deceiver and the intended target. The intended target of the deception process is the enemy decision maker, however, the target can rarely be reached without going through some form of information processing system: the intelligence agency. Within the intelligence agency there are channel monitors, gatekeepers, and decision maker. The channel monitor picks up signals from the deceiver. These individuals will collect information and have the data analyzed. From there the gatekeepers, whose role includes screening information and analysis, determine what information to send the decision maker. The decision-makers will take this information and direct the action of their assigned forces. The deceiver must convince all three levels (monitor, gatekeeper, and decision maker) of the validity of the false information to achieve success; a tall order, indeed. (Daniel, 1982, pp. 8-10)

In order to create an effective military deception plan, there needs to be believability in the deception that is presented. The scheme needs to be plausible, as Daniel states, meaning

> …the deceiver's scenario must not only be one that could conceivably happen, but also one that seems ominous enough, and likely enough, to provoke the target to forestall it. (1982, p. 18)

If the deception plan is so far-fetched or seemingly impossible to conduct, then it is likely that the target will reject it and the plan will fail. The lies within the plan are only as strong and credible as what the deceiver can do. As a result, the deceiver will sometimes need to actually carry out some of the "deception" given to the enemy, to lend credibility to the rest of the plan.

To add to the believability of the deception, reliable sources (i.e., sources which the target deem reliable) are needed for confirmation. In order to accept something for the truth, there needs to be evidence to support the claim. The information becomes more

credible with more reliable resources to confirm it. It then becomes in the best interest of the deceiver to manipulate more channels, in order for the deception to gain more credibility. Reassurance and acceptance of the deception becomes a product of credible confirmation. During World War II, the Allies enhanced the credibility of information within Operation Bodyguard by channeling much of it through German secret agents, to reach Hitler (Breuer, 1993, pp. 99-108). Hitler trusted most of the information passed by these secret agents, although the Allies were actually controlling the agents. Confirmation of the deception may also be achieved by surrounding the lie with some true facts, as "the execution of deception requires the protection of its lies by a bodyguard of truth." (Daniel, 1982, p. 20)

Military deception also calls for successful organization and coordination. Failure may result in poor operational security, a concept vital to the success of any deception plan. Daniel stresses the importance of these ideas, stating

> …by definition, secrecy is inherent to deception, and organization and coordination are inherent to the success of any but the most simple endeavors. (1982, p. 16)

Secrecy is needed to maintain an effective deception. Daniel assesses that there are two types of security associated with a deception. The first type consists of the deceivers trying to conceal their true intentions from the intended target. The second type of security aims to hide the actual existence of any deception scheme. However, the probability of total secrecy is difficult to attain and highly unachievable regardless of an ideal organization and coordination. Leaks almost always exist in both types of security levels, normally resulting from errors in organization and coordination. Leaks may not be as disruptive as they are perceived, since they may cause more ambiguity and confusion to the target. The key for success in deception is to reduce the chances of unplanned circumstances. A more accurate gauge in determining the probability of success is, according to Daniel and Herbig, is the plausibility of the plan. (Daniel, 1982, pp. 16-17)

Accurate intelligence is needed for a successful deception. A reliable source of information offers an advantage by providing insight into the intentions and reactions of the intended target. Feedback from the target is needed in order to provide intelligence.

The role of intelligence is to determine if the deception scheme is working. In addition, feedback provides the deceiver with an opportunity to adapt and take advantage of opportunities. The success of the plan relies on the deceiver's ability to adapt. Those that are trying to deceive should take advantage of the opportunities that arise, and adjust to the changing circumstances and unplanned events (Daniel, 1982, p. 20). In order for the plan to remain believable, deception has to change with the facts. The German invasion of Russia during 1941 provides an example in which the Germans adapted well to intelligence. Throughout the war, Germany normally offered an ultimatum before launching an offensive, as evident in their invasions of Czechoslovakia and Poland. However, that changed with the invasion in 1941, when Germany learned that Russia was aware of this normal course of action. As a result, Russia was not offered an ultimatum and the Germans caught Stalin's armies completely by surprise. (Daniel, 1982, p. 20)

C. INFORMAL/INTELLIGENCE CYCLE

1. Judgment and Thinking

In order to understand the nature of deception, deception planners must understand human judgment, perception, and the susceptibilities of the human mind. Human judgment is not perfect; biases exist. There are events that simply cannot be predicted with confidence, or high probability. As a result, human judgment is needed to fill the void of confidence by means of inductive inferences. The most commonly accepted view of human judgment is "seriously biased, and this results from judges' reliance upon inappropriate or irrational procedures to arrive at their judgments." (Beach, 1987, p. 49) These biases have a significant impact on one's judgment and thinking, as both judgment and choice are essential and pervasive activities. Human judgments for the most part are made intuitively and instinctively, without the benefit of reason. Normally, people make judgments based upon the preferences that they express. Or they may make judgments based upon what they expect will happen. In other words, the two types of judgments are those of preference and belief. (Hogarth, 1987, p. 1)

According to Robin Hogarth, the human mind is a "selective, sequential information processing system with limited processing and memory capacity." (1987, p. 10) This creates serious limitations into how effectively an individual can make a judgment. Deception and biases result from the limitations in the mind's processing

capabilities. Human perception of information is selective and not comprehensive. In other words, with so much information available, an individual has to know what information to choose. This results in anticipation and account for "people only see what they want to see." (Hogarth, 1987, p. 4) It is perceived that the human information-processing capability can only be done in a sequential manner because people cannot handle too much information at one time. Observing these sequences of events may lead to biases because of the anticipation of events. These anticipations cloud the accuracy of human judgment. In addition, the accuracy of human judgment depends on the ability of the mind to copy the environment it attempts to predict. Thus, human judgment is a function of both the individual and the task.

2. Biases

Deception plays on the susceptibility of human judgment and is a product of human biases. Deception occurs because people have bias towards certain information and have different inferences. In order for deception to be successful, deception must have a profound effect on the decision maker or the intelligence analyst working for the decision maker. People tend to attach subjective meaning to objective information, and thus various individuals have different interpretations and conceptualizations about the same information. According to Richard Heuer, the effectiveness of deception becomes greater if the deceiver can understand the thought process of the target. Conversely, the intended target can improve the chances of avoiding deception if he or she can learn more about one's own thought capabilities and limitations. (Heuer, 1982, p. 31)

Nevertheless, deception works because of patterns of mistaken perception and judgment. People often make erroneous choices, resulting from the limits of the brain's processing capability. These errors in judgment are called biases and can be both consistent and predictable. Biases are not predictable in the sense that people will make the same mistake under the same circumstances all the time. Instead, the predictability falls into the numerical sense, as most people will be influenced by this tendency a majority of the time (Heuer, 1982, p. 31). There are several types of biases that explain why deception works. However, this perceptual bias is being examined, as it has an affect on people regardless of culture or group affiliations. Perceptual biases link the

individual to what he or she sees in the environment. Regardless of the type, biases of people are contributing factors to how deception works.

Human perception refers to the ability to make assumptions based upon what is seen in the surrounding environment. How information is perceived and how it influences actions is a function of the individuals' past, culture, and education. Perception is a

> …process of inference in which the individual constructs his or her own version of 'reality' on the basis of information provided by the senses. This sensory input is mediated by complex and poorly understood mental process that determine which information we attend to, how we organize it, and the meaning we attribute to it. (Heuer, 1982, p. 33)

An individual sees what he or she expects or wants to see. These expectations create a mind-set that dictates a person to think in a certain way and ask questions that may include what to look for and what is important. These mindsets cannot be avoided. However, the issue is not to ignore these mind-sets but to seek out all information and to compare one's perceptions with reality (Heuer, 1982, p. 36).

Human biases allow deception to work. It is often easier to trick a person than to try to change the target's mind. Because people tend to go with their expectations or to incorporate new information with existing images, it is easier to reinforce the target's existing beliefs. That way the target will ignore all evidences of a deception and remain with his or her perception. Richard Heuer notes that perceptions are quick to form but resistant to change, as individuals will continue to perceive something in the same manner despite the possibility of changes to the perceived item. In other words, established perceptions are tough to modify or eliminate. People would rather make rationalizations about evidence that contradicts their assumptions and perceptions than accept that evidence. So one's perception created by ambiguous or incorrect data may still be wrong despite additional information being made available to offer clarity. (Heuer, 1982, pp. 33-44)

There are implications to what biases can actually mean to a deception. For example, people tend to generate more confidence from a smaller group that is consistent with the information than a larger one with less consistency. What this can actually mean

in a deception is the deceiver has to monitor all the channels or as much as possible in order to reduce any discrepancies that may be available to the target. Another example is using probability to make alternative choices and assessments. As stated earlier, the mind has its limitations, and thus it becomes difficult to come to a distinct conclusion. Bias dealing with probability is influenced by availability, which refers to the ease of recalling or imaging the instances of whatever is being estimated. Knowing these biases is beneficial in either planning a deception or avoiding one. (Heuer, 62)

D. SUMMARY

Deception is a proven military device. Proper application of the guidelines put forth in JP 3-58 in keeping with an understanding of human judgment and perception can contribute greatly to the successful achievement of military objectives. Historically, deception has been used to increase the advantage on the battlefield, although its potential extends beyond the traditional fronts. The possibility of expanding deceptive tools to the realm of the Internet and computer security may be beneficial to warfighting in the 21st century.

Military objectives exist to support the national security strategy. Although there are many threats to national security, terrorism is currently the most deadly. Its deadly potential is enhanced by its use of a widely used and trusted medium in America: the Internet. A new style of deception described in this study will show the significance of the relations between terrorism and the Internet, while exploring the opportunities to exploit this relationship. The deception scheme detailed in the following chapters will seek to explore a new brand of "Internet terrorists" and how the Internet may be used to aid in prevention of future terrorist attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THREATS TO NATIONAL SECURITY

A. TERRORISM

The targets of the deception in this project were those seeking information on the Internet for the support of terrorist acts. Individual acts of terrorism are producing more casualties as improvements in information technology and support from international, radical governments are providing terrorists with an advantage. Terrorism is characterized by its unpredictability and flexibility. According to David Fromkin, terrorism is a tool used to create violence and inspire fear in order to provoke a response. The strategy of terrorism calls for the following: "that it achieves its goal not through its acts but through the response to its acts." (Fromkin, 1978, p. 19) In other words, the consequence from violence caused by terrorists is only the beginning and is really a building block for the real, long-term objective. The success of terrorism depends on how the victims react. If the victims respond in a fashion that the terrorists desire, then terrorism has won. If the victims choose not to respond at all or to respond in a way different from the desire of the terrorists, then the terrorists will have failed in their objectives (Fromkin, 1978, p. 19). Terrorism is a means to an end, and not an end unto itself. Terrorism is an indirect strategy, which intends to start the process of imposing will upon the target and then have someone else come in and complete that imposition. As Fromkin best puts it:

> Terrorism is violence used in order to create fear; but it is aimed at creating fear in order that the fear, in turn, will lead somebody else-not the terrorist-to embark on some quite different program of action that will accomplish whatever it is the terrorist really desires. (1978, p. 19)

The overall aim of terrorist action is to attain a psychological and not a physical result via intimidation with violence. Whether terrorism is successful or not is dependent upon the actions of the target.

1. Trends

Terrorism constantly changes with time. As a result, defending agencies need to truly understand and constantly react to changes in contemporary terrorism in order to protect against it. The focal point of these agencies' concerns is ideally the possible

trends and direction of future terrorism. Analysis of these trends may provide a better understanding of terrorists' intent and potential plans. Brian Michael Jenkins predicts several trends for terrorism in the future. The first trend involves more developed terrorist groups providing military and economic assistance and guidance to less developed groups. The support from the better terrorist groups ensures that the lesser groups have the resources to do a job they normally cannot do. In this trend, even local citizens can be used to carry out an attack with the support of more organized terrorist actors. Jenkins' second trend focuses on greater destruction because of increased vulnerabilities. With technological advances weaponry has become more devastating, since they can be smaller, portable, cheaper, accurate, and easy to operate. (Jenkins, 1978, pp. 242-244)

Another visible trend shows that openly state-sponsored terrorism is diminishing. National governments are unwilling to become directly involved in terrorism. There are seven governments designated by the U.S. State Department as sponsors of terrorism: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. In the past couple of years, only Iran is known to have direct involvement in terrorist attacks. Meanwhile, the other nations can support terrorism by providing resources, logistical support, sanctuary, and diplomatic facilities. Afghanistan was known to be a training area and a base of operations for terrorist activities. Sanctions imposed by the United States on these state sponsors is a huge factor in this decline. The United States has imposed sanctions on those seven designated governments, while the United Nations has imposed sanctions against Iraq, Libya, and Sudan for their continued support of terrorism. While state sponsored terrorism is declining, smaller militant organizations are gaining influence. These organizations include Aum Shrinrikyo of Japan, which executed a Sarin gas attack on the Tokyo subway, and Osama Bin Laden's al-Qaeda, responsible for the embassy bombings in Kenya and Tanzania, the bombing of the USS Cole in Yemen, and the September 11 attacks on the World Trade Center and Pentagon.

Terrorism intends to ultimately avoid using an informational technology approach, such as attacking telecommunications, data processing systems, or anything that would bring about disruption rather than destruction. The reasons are the technical requirements and the lack of drama. Terrorism looks for a visual display in order to draw

publicity to their actions. There are terrorist groups that do not claim responsibility for their actions, for fear of retaliation. As stated earlier, state-sponsored terrorism is on the decline, and nation-states such as the United States are actively fighting terrorism. States sponsoring terrorism fear U.S.-imposed sanctions, while terrorists may fear being caught and prosecuted. Regardless of whether or not a terrorist group claims responsibility for their actions, their acts still draw attention. The overall goal is to obtain a psychological effect by spreading fear and instilling a sense of intimidation upon society. Visible destruction helps to achieve that affect. The characteristics of terrorist attacks will continue to focus on destruction and not disruption. (Jenkins, 1987, p. 156)

Brian Jenkins noted years ago that terrorists are unlikely to cause mass destruction, as "terrorists want a lot of people watching and a lot of people listening, not a lot of people dead." (Jenkins, 1978, p. 236) Terrorism is not aimed to simply kill large numbers of people, but instead to gain political advantages from attacks and to draw attention from a large audience without discouraging their support. Random violence may be perceived as immoral. Nation-states are unlikely candidates to use weapons of mass destruction[3] (WMD) because of fear of severe retaliation. Some terrorist groups are afraid that the use of WMD would incite repulsion from the public and weaken their cause. However, times have changed and the trend is toward attacks that inflict greater number of casualties, whether WMD is used or not. The threat of WMD has gained attention as a result of several events: the Aum Shinrikyo's Sarin gas attack and Bin Laden's publicly declaring his search for WMD. At the same time, there have been notable events that caused huge numbers of casualties and damage, *without* using weapons categorized as WMD: the Oklahoma City and World Trade Center bombings, the 1998 bombings of the U.S. embassies in Kenya and Tanzania, and the events on September 11. According to David Tucker there are a number of reasons for this trend of attacks with high casualties: the spread of lethal technologies, the constant need for terrorists to attract new attention, the lack of restraint on new terrorists, who are not concerned with the repercussions, and the erosion of the worldwide taboo against the use of WMD (Tucker, 2001, p. 3).

3 Weapons of mass destruction include nuclear, chemical, biological, and radiological (NBCR) weapons that are intended to annihilate the target or kill large amounts of people.

2. Response to Trends

In order to defend against terrorism, accurate foreknowledge is needed to prepare a plan and deter the terrorists' actions and capabilities. Intelligence agencies have the objective of making predictions and looking out for possible threats. Proper assessment of the threat is needed for those in authority to foil the actions of terrorists. In other words, information is collected and evaluated, and warnings of potential terrorism are distributed to the applicable authorities in a timely fashion. From there the authorities would decide on countermeasures to defend against or preempt acts from terrorists. Relevant information includes possible trends and characteristics. Information is needed to know about the intimate knowledge of the terrorist organization, their personalities, and their inner workings. Possessing and understanding this information and obtaining early warning from intelligence can play an important role in combating terrorism.

3. Terrorist Profile

The terrorist profile has changed with the collapse of communism in the former Soviet Union and other East European countries. Because of the communist collapse in several countries terrorism inspired by ideology is on the decline despite the continued efforts of Marxist and Maoist groups in India, Nepal, the Philippines, Japan, and a few Latin American countries. The major ideological terrorist groups of West Europe have ceased to exist, which include the Baader-Meinhof and the Red Army faction of the former West Germany, the Red Brigade of Italy, the Action Directe of France, and the Revolutionary Communist Cells of Belgium. The same is also occurring in West Asia. Replacing the ideological based terrorist groups, are those based on religion and ethnicity. Their actions are based upon anger, as the minority religious and ethnic communities feel that the majority communities mistreat them. In addition, these minority groups view their actions as a sign of separation from the majority. Their anger also originates from threats to their culture through external influences. Examples of these feelings of anger include the injustice towards the Palestinians, Soviet occupation of Afghanistan in the 1980s, and Western troops in Saudi Arabia during and after the Gulf War in 1991. Both incidents in Afghanistan and the Gulf are viewed as foreign interference whose aim is to protect the political and economic interests of the foreign powers. (Raman, 1999, pp. 1-9)

Another trend occurred in the 1980s and the 1990s in which terrorism occurred within the same religion (Islam) in Pakistan and Afghanistan. For example, the Sunni majority would use terrorism against the Shi'ite minority, and the Shi'ite would respond in the same fashion. The majority faction would use terrorism to force the minority faction to accept their interpretation of the religion's teachings and practices. In the 1990s, rich individuals such as Osama Bin Laden and private organizations have sponsored terrorist groups to achieve their own objectives. In addition, nation states have used these organizations to conduct terrorism in other states without getting directly involved. Still there are irrational groups or individuals that use terrorism to display their resentment toward society or the government. An example would be the Oklahoma City bombing, in which two U.S. citizens bombed a federal building in Oklahoma City in April of 1995 (Raman, 1999, pp. 1-9).

The terrorist groups of today have had better communications and weapons as a result of contributions from rich members throughout the world and from their drug trade. According to David Tucker, terrorism has assumed a new form based on a network structure supported by information technology, or IT (Tucker, 2001. p. 1). Although information technology has created many opportunities and advantages, it has also created vulnerabilities. Terrorists can use the advantages of IT to serve their purposes. The information revolution has lowered the cost of communication, which means terrorists can operate outside a controlling hierarchical structure. They are able to operate as separate entities connected together by higher communications and a common objective. Modern forms of communications such as cellular and satellite phones, fax machines, cyber cafes, and commercialization of cryptography products have given terrorists improved operational flexibility. Terrorists are able to draw on greater resources, such as money, knowledge, political and individual support, with communication being cheaper and easier to use. They can connect with ethnic or religious groups or political sympathizers around the world and spread their message in order to get support for their struggles (Tucker, 2001, p. 3). In addition, amateur terrorists and ad hoc terrorist groups can easily communicate and work together with improvements in information technology. Improved communication can be attributed to

the success of the Internet, as people in various corners of the globe can potentially be linked together via the World Wide Web.

The terrorists groups most likely to attempt weapons of mass destruction (WMD) attacks are fanatical religious groups, small terrorist cells, and groups wanting revenge. It was identified that these groups possessed certain characteristics: charismatic leadership, no external constituency, apocalyptic vision, splinter group, paranoia, and preemptive aggression.[4] The two common characteristics that appeared in all of terrorist groups were a lack of an outside constituency and a sense of paranoia.[5] With the collapse of the Soviet Union, various ex-Soviet scientists were left jobless and security at WMD establishments has diminished. With this combination, the likelihood of terrorists obtaining WMD is increased. Bin Laden has stated in an interview in *Time* magazine that he is searching for a WMD, while the Aum Shinrikiyo of Japan has already used Sarin gas in highly populated areas of Tokyo. These examples show that there is a distinct possibility of terrorists using WMD to intimidate states, governments, and societies. The threat of WMD terrorism exists if a terrorist group can realistically attain a WMD and are willing to use it to achieve their objective. Only a limited number of groups and individuals have had the motivation to use WMD and fewer have the ability to obtain them. Only the Aum Shinrikyo to this point has had both the intent and the capability to carry out a WMD attack. However, the desire to use WMD does not equate to capability, as the Aum Shinrikyo's displayed poor execution on March 20, 1995. The casualty numbers, 12 dead and 5000 wounded, could have been higher if not for the Aum Shinrikyo's mistakes in preparing the sarin gas that day and the inferior dissemination system used to deploy it. (Raman, 1999, pp. 1-9)

Peter Flemming contends that terrorism is categorized into four classes: nationalist, religious, political, and single issue. They all have distinct group characteristics and it can be hypothesized as to how they act in a cyber environment. Examples of the nationalist terrorist groups are the Provisional Wing of the Irish Republican Army (PIRA) and the Liberation Tigers of Tamil Eelam (LTTE). They have

4 For more information see Steve Bowman and Helit Barel, "Weapons of Mass Destruction – the Terrorist Threat" December 1999 http://news.findlaw.com/cnn/docs/crs/wpnsmssdst120899.pdf.

5 Ibid.

an ethnic identity, are large in numbers, mature in age, have a political standing and representation, and have well defined political constituency, adversaries, and theater of operations. It is hypothesized that the nationalist terrorist group will adopt cyber technology to gain financial revenues from abroad, spread terrorist propaganda, and broaden and diversify their political campaigns (Flemming, 2000, pp. 1-6).

Religious terrorist groups include the Armed Islamic Group (GIA) and the Egyptian Islamic Jihad. Their size usually varies in number, and they are generally immature. Their religious identity is influenced by a fundamentalist standpoint. They have minimal representation in politics and have loosely defined political constituency, specific adversaries and variable theater of operations. It is hypothesized that the religious terrorist group will adopt cyberterrorism to coordinate small cells into large terrorist campaigns and to look for ways to inflict heavy damage and casualties (Flemming, 2000, pp. 1-6).

Political terrorist groups include the Sword and the Arm of the Lord (CSA) and the Tupac Amaru Revolutionary Movement (MRTA). They are usually small in size and immature in development. Ideologically they are either to the far left or right and have little political representation. Furthermore, they are well defined but are a disinterested political constituency. They have limited theater of operations and have a specific adversary. These groups would use cyberterrorism to emphasize their strength and hide their weaknesses. Basically, they will use cyberterrorism for threats, propaganda, recruiting, communication, and attempting to gain greater acknowledgment (Flemming, 2000, pp. 1-6).

Examples of the single-issue terrorist groups include the Animal Liberation Front (ALF) and Earth Liberation Front. They are relatively small in numbers and their goal is to address a political grievance. They are a narrowly defined constituency, have well-defined adversaries, and have limited theater of operations. They would use cyber technology for propaganda, threats, and communication (Flemming, 2000, pp. 1-6). The technology and methods used by all of these terrorist groups will be discussed in the upcoming section.

B. THE INTERNET

1. Growth of the Internet

The rapid growth of the Internet since its inception is most prevalent in the United States, one of the most informationally rich environments. The numbers of both users and sites on the web have increased exponentially. A report released by the US Department of Commerce declares the rate of new Internet users in America at two million per month. As of September 2001, 55% of all Americans are regular Internet users (at least once per month), while regular Internet users in Europe average 31% according to a European Union figure. Overall, over 300 million people worldwide have Web access (Evans, 2001, p. 3). These numbers are on the rise, as they have been throughout the 1990s. In a report by the United States Internet Council (USIC), they project that by 2005 the total number of users worldwide will have reached one billion (Evans, p. 3). The increasing number means more sources of information and opportunities for use of A-type or M-type deception will become available.

2. Hacker Profiles

The intended targets of this research were those that used the Internet as a tool to research and plan acts of potential violence and terrorism. There are several types of hackers[6] that can or did hack into the JTFO website, but the main focus was the people looking for information that could be used by terrorists. With the growth of the Internet, hackers are becoming a larger threat with their ability to use the information revolution to support and conduct their malicious intent. Their presence was uncovered in this project. The objective of this project was to act as a law enforcement tool that could be used to research the actions of Internet terrorists and provide assistance in prosecuting these people. With this research, the behavior of terrorists within computer networks can begin to be understood more clearly. This project featured the Winter Olympics, which introduced a high potential for criminal and terrorist activities. Marc Rogers and Jerrold M. Post, two experts in the field of cyber forensics and psychology, have noted some common behavioral trends for hackers committing crimes.[7] Marc Rogers emphasizes

6 The types of hackers include: old school hackers, cyberpunks or script kiddies, professional criminal or crackers, code and virus writers, and Internet terrorists.

7 Marc Rogers is a behavioral sciences researcher at the University of Manitoba in Winnipeg, Canada, and a former cyber detective and Jerrold M. Post is a psychiatrist at George Washington University in Washington, D.C. Their analysis on the hacker psychology can be founded on http://tlc.discovery.com/convergence/hackers/articles/psych.html.

that hackers downplay or misinterpret the consequences of their actions. They may believe that they are performing a service to society; while others dehumanize and belittle the sites they attack. Jerrold Post points out that hackers lose human contact over the computer and ignore the serious consequences of their actions because hacking is perceived as a game. Post says the same thing about terrorists. In addition, both Post and Rogers agree that hackers may have an inferiority complex. As a result, they gain a sense of power when they shut down a major site or achieve mastery of computer technology. There are various types of hackers, as described below:

- **Internet Terrorists:** These are the hackers of concern in this project. These individuals look for information that may used to support terrorism by hacking into a system. These people use the Internet to collect information about their targets. For example, the conspirators of the September 11 attack used information technology to communicate and find pertinent information to accomplish their objectives. According to the Computer Science Corporation's Bill Tafoya, "These men did their homework. They took flying lessons. They communicated via e-mail at public kiosks, cyber cafes and even public libraries. They went to airports to find weaknesses in security systems, and so forth. They did sophisticated planning and researched vulnerabilities."[8]
- **Old School Hackers**: These hackers view themselves as an elite group of individuals seeking information via computer systems and networks. Hacking to them is seen as a badge of honor. They perceive their actions as acceptable as long as they do not violate the hacker code of ethics, which may include theft, vandalism, or breach of confidentiality. They believe it is their role to seek and point out the breaches or holes in the security systems so people can fix them. These hackers perceive themselves as vigilantes for justice as they seek out flaws in today's software and Internet sites that carelessly expose personal information. They have no malicious intent but ignore privacy and proprietary information because they think the Internet was designed to be an open system.
- **Script Kiddies or Cyber-Punks:** These hackers are mostly young adults, as their age group ranges between 12 and 30 years old, and they possess the intent to vandalize or disrupt systems. They predominately are comprised of white males with a 12th grade education. They are competent with computers and technology, evident by their ability to download readymade scripts and to hack into systems.

8 For more information of Bill Tafoya's article go to http://www.csc.com/features/2002/17.shtml.

- **Professional Criminals or Crackers:** The objective of these people is to break into systems and sell their information. They may be associated with corporate or government espionage or organized crimes.
- **Coders and Virus Writers:** These people possess countless programming background and write code, but they will not use them. Instead, they allow others to bring their code into the Internet.

This project is intended to be used as a tool in order to determine which categories of terrorists have entered the site and, more importantly, make assessments of what type of information potential terrorists are trying to seek on the Internet. This research is an important part of adapting to changes in contemporary terrorism.

This study seeks to identify characteristics and habits of Internet terrorists. As discussed above, these people are terrorists who seek to support their goals through Internet research and possibly Internet disruption. They may be classified as hackers, although their ultimate motives differ from traditional hackers. Traditional hackers tend to focus mainly on the destruction, degradation, or theft of computer resources for the various reasons described above. Internet terrorists have goals that extend beyond computer systems. They may seek information helpful in carrying out physical attacks, or they may look to destroy or degrade their enemy's computer system in support of their ultimate goals. It should be made clear that not all hackers are Internet terrorists, but that all Internet terrorists display some characteristics common to various classes of hackers.

3. Cyberterrorism

Cyberterrorism is characterized as a "convergence of cyberspace and terrorism." (Denning, 1999, p. 241) Cyberterrorism has not actually taken effect in the form of destruction of national infrastructure, but it still has important implications. The real threat of cyberterrorism is that all information is at risk, and that information can be used to support terrorist acts. Terrorists use the Internet and the World Wide Web to conduct the business of terrorism. There is no limit to how terrorists or anyone else use the Internet. Cyberterrorism can be conducted remotely and anonymously, it is inexpensive, and it does not require the handling of explosives or suicide missions. Cyberterrorism offers terrorists independence from state-sponsorship, which means they do not have to rely on the states for funds, training, or sanctuary (Flemming, 2000, pp. 1-6). Cyberterrorism is relatively cheap, especially when considering resources needed for

weapons, international travel, and training facilities. Computer technology can also help facilitate terrorism through information/intelligence gathering, recruitment, communications, and propaganda.

In addition, computer technology also creates vulnerability. People that use and depend on computer technology are susceptible to its weaknesses, and anyone can exploit these vulnerabilities. Terrorists put encrypted messages, including maps of targets, inside Internet chat rooms, bulletin boards, and other Web sites. They can cause considerable damage without attacking physical infrastructures, as computers tie scientific, financial, military, and technological infrastructures together. The damage would not be as devastating as physical destruction, but the impact would come in the form of publicity. Terrorists would receive extensive media attention, as computer attacks normally garner interest from the public. Highly technical individuals proficient in information technology can be hired to help terrorists to disrupt data, communication, and public utilities. (Raman, 1999, pp. 1-9)

C. SUMMARY

The growth of the Internet has increased the effectiveness and speed of communications among terrorist groups. Terrorism now poses the main threat to national security. The devastation of terrorist acts can be aided by the use of the Internet. The focus of this project is to evaluate the relationship between terrorism and the Internet. This relationship has also generated a new type of "Internet terrorist" who seeks information within the millions of websites available through the Internet. With the rise of information technology, the Internet has become a valuable tool for seeking information and communicating. At the same time, information technology has its vulnerabilities, as people have become dependent on it. As a result Internet terrorists, along with other types of hackers, can exploit these vulnerabilities. The deception scheme used in this project aims to examine these Internet terrorists. Their characteristics, habits, and ultimately their weaknesses can be uncovered using a new form of Internet deception.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DECEPTION ON THE WORLD WIDE WEB

A. THE NEED FOR WEB DECEPTION

The Internet has become increasingly popular due to its ease of accessibility and the wealth of information. Although the Internet is widely used by both lawful and criminal organizations, it is largely chaotic. Few laws are in place to prevent theft of information or defacing of websites and databases on the Web. The laws that do exist are extremely difficult to enforce, since people that choose to engage in criminal activity on the Web are usually quite skillful at what they do. Hackers commonly look at what they want, change or take what they need, and cover their own tracks. Chasing these hackers and pinning them to their crimes is sometimes impossible. New methods, including the deception tools used in this study, are needed to protect the information and intellectual property on the Web, while aiding in the prevention of destructive criminal and terrorist acts.

Networked criminal and terrorist organizations is not a new concept; they have been around for many years. But the improved communications and information exchange between members of these groups is the direct result of growth of the Internet. The explosion of the Internet and its contents provides a gold mine of information for all people, but especially those networks that rely on it for their existence. It is a safe assumption that almost all terrorist and organized crime organizations will turn to computer communications at some point during their operations. It is also safe to believe that such organizations are aware of the capabilities of legitimate groups to utilize the Internet for communication and information as well. In other words, the Web is an area that cannot be ignored.

B. THE HONEYPOT CONCEPT

Honeypots are a tool commonly used for research and protection in the field of computer security. According to HoneyNet Project researcher Lance Spitzner, honeypots are defined as "a resource whose value is in being attacked or compromised." (Spitzner, 2002, p. 1) In the context of computer security, this is normally a computer system designed in such a way that illegitimate users can break into it. Honeypots are categorized into two major types, production and research. Research honeypots tend to

be the more common of the two, and are used to "watch" hackers. The research gives the opportunity to monitor techniques, habits, and desires of those that enter the honeypot system. Production honeypots normally serve a specific purpose, usually in pursuing a particular criminal.

A classic example of a production honeypot is presented in Cliff Stoll's *The Cuckoo's Egg*. In it, Stoll describes the methodology he used to track down a particular hacker in his computer system. He constructed a production honeypot on his computer network, in which he placed bogus material designed to attract the hacker. This kept the hacker in the system for long periods of time, while Stoll was able to trace him all the way to Germany. (Stoll, 1989)

The honeypot-style deception of the JTFO project will be most effective when tailored specifically to the habits of the target. The setup of the JTFO deception plan allows for the material to be altered according to the desires of the hackers on the site. For starters, profiles of several types of hackers were collected. These profiles were compared to the styles and habits of intruders, and more deceptive material was added to encourage hackers. Like Stoll's honeypot in *The Cuckoo's Egg*, it is important to keep intruders looking often and for long periods. Then it is possible to closely track, monitor, and determine possible future terrorist activities. In a sense, the JTFO project combines the two main types of honeypots. Beginning as a research tool, the data collected from the website is used to profile the intruders within. After this is completed, the findings can be used as production tools in tracing those intruders.

The style of web deception implemented in this project is slightly different from traditional deception discussed in Chapter II. Honeypot deception differs mainly in its objective. The ultimate goal of a research honeypot is to observe target intruders in order to develop a thorough understanding of their motives, techniques, and characteristics. Traditional deception seeks to influence the target to undertake a particular action in support of an actual operation. This more closely parallels the objective of productive honeypots, where specific goals are determined so that the deceptive aspects of the honeypot support them. The JTFO experiment contained elements of both styles of honeypots, although the research aspects tended to be more successful.

C. SUMMARY

Tactical deception on the web can create valuable opportunities to enhance homeland security. Web deception can help hone Internet terrorist profiles and techniques through research honeypots and can provide valuable "tipper" information to law enforcement and defense agencies through productive honeypots. These research aspects will lead to conclusions about whether tactical web deception can be used for real life operations.

The goals of research honeypot deception differ slightly from productive honeypots and traditional deception. Rather than influence the decisions of the target, research honeypots seek to gain information and apply it to future operations. This is how the JTFO experiment proved to be most effective. Although deception is not a catch all, it may be used effectively when integrated into other operations. The future of Internet deception depends on its effectiveness in test situations, its integration into more conventional operations, and its attractiveness to the opponent. All of these factors will be evaluated in the following chapters.

THIS PAGE LEFT INTENTIONALLY BLANK

V. PROJECT DESIGN AND IMPLEMENTATION

The 2002 Winter Olympics in Salt Lake City created a potentially large target for terrorists or any organization looking to make a highly visible, violent statement to the world. The potential for mass destruction in a relatively small area was high. As a result security and safety were top priorities at Salt Lake City during the Olympics. The Department of Defense was involved, along with the National Guard and the Utah Olympic Public Safety Command (UOPSC).[9] All three agencies were tasked with coming together and ensuring the smoothness of security during the seventeen days of competition.

Along with the high potential for danger, the Olympics provided an ideal time for testing and research in various fields. Some potential testing areas included Joint Force organizations, security agency organizations, and computer networks. The DoD security agency, Joint Task Force Olympics (JTFO), provided a venue for some of this research. An unofficial website representing the JTFO was developed on the domain name www.jtfo.org. The website served as a research honeypot, containing information and files arranged in such a way to encourage unauthorized intrusion and attract information seekers. The website contained both legitimate information as well as material to mislead and confuse intruders.

A. PROJECT OBJECTIVES

The main objective of the JTFO website was to pursue research in web deception. The JTFO experiment provided an evaluation of the usefulness of tactical web deception in support of military or law enforcement operations. The website and data collection tools were designed in a way that each of the six elements of successful deception played a key role.

- The experiment was **focused** on the profiles of various types of known Internet terrorists. When developing a target for the deception scheme, known profiles were considered so that the deception tools could be

9 The DoD agency involved was the Joint Task Force Olympics (JTFO), under the command of United States Joint Forces Command (USJFCOM). The National Guard was under the command of the Utah governor, while UOPSC was a conglomerate of local, state, and federal public safety commands. The three agencies were all under separate commands.

tailored towards the types of intruders that were most attractive to the field of web deception when pursuing terrorists.

- A clear **objective** was developed for this project: to encourage intruders to access the JTFO web server, thus revealing their habits.
- **Centralized control** of the deception operation was distinctly held by a small group so as to minimize errors among the project designers.
- **Operational security** was carefully considered when communicating between members of the project design team. In order to hide the true intentions of www.jtfo.org, e-mails and telephone calls were limited to vague discussions of the project. Any potentially compromising material was communicated either in person or via secure Internet (SIPRNET).
- The plan was **integrated** into a real-life operation: Olympic security. Factual information was included on the website to enhance its credibility and preserve the "bodyguard of lies" created by the deception in order to protect the truth.
- **Timeliness** was the one weakness during the project. The project was developed very quickly in order to be launched before the Olympics began. This was vital to the project's effectiveness, since the deception scheme had to unfold as though it were part of the overall Olympic security plans of the JTFO.

The JTFO experiment also provided a testing ground for improving the methods of web deception. Carefully monitoring and studying the behavior of intruders during the JTFO experiment could possibly help in developing new ideas for future deception plans. Existing techniques could also be improved. The research was intended to answer the following questions:

- What do typical intruders[10] look for on the Internet? Do they search for maps, schedules, specific names, or other keywords?
- Do intruders attempt to access restricted material on the web? Do they simply look at such material, download it, or alter it?
- What material is most attractive to intruders on the web?
- When do intruders do their work? Are there any patterns to their behavior?
- Do intruders mount any attacks on their target's web server? Do they attempt Denial of Service (DoS) or other attacks? Do they attempt to spoof their own identity to confuse their target[11]?

10 For this report, intruders are defined as persons trying to access information for which they have no authority or a need to know.

11 In other words, do intruders conduct a deception plan of their own?

The answers to these questions can provide valuable insight into the profile of Internet terrorists. This, in turn, may allow future web deception plans to maximize their effectiveness by providing more information that may appeal to targeted intruders. The JTFO website was designed to provide the answers.

B. WEB DESIGN AND CONTENT

1. Dual Image

Since the primary function of the JTFO website was deception, its design was carefully constructed to appear as an operational component of the actual JTFO. The intent was for the site to appear as a public-friendly site, while at the same time serving an operational purpose to the JTFO. The site needed to portray military-style characteristics, yet still give the impression that it was independent of the Department of Defense. Components such as protected areas and external links were added to the site to increase its credibility. Most importantly, the website and its web server included several tools, such as a search engine and access logs, to aid in achieving the objectives of the deception experiment.

The domain name, www.jtfo.org, was the first step in creating the illusion of the JTFO website. Several issues were considered when choosing a ".org" name, rather than a ".mil." The site needed to convey an image of an organization that was associated with the military, although one that operated independently from the defense hierarchy. This was done for two reasons. First and foremost, the site was neither designed nor maintained by JTFO or USJFCOM. Secondly, using a ".org" name would create a false sense of security for those who entered the site. The idea of a ".mil" domain name would perhaps intimidate intruders looking to prowl around the website undetected. The main purpose of the website was to induce people to enter and view as much information as possible on the site. Using a ".org" gave the impression that the website enforced a softer security policy, and that activity on the web server was not closely monitored.

In order to accomplish the necessary dual image, the JTFO website was structured into two major parts: the public information area and the restricted area. The public area displayed various factual bits of information about JTFO duties and responsibilities in Salt Lake City. A list of links to other Olympic-related websites connected the JTFO site to others. The public portions were designed to be extremely user-friendly and easily

navigable from page to page. The material on the site was deliberately spread thin so as to encourage users to dig further into the JTFO web, eventually into the restricted areas.

It is important to note that all material within the website was factual, in order to effectively integrate the site into the overall operational plans of the JTFO. The public pages contained actual dates, Internet links, and factual bits of information about the JTFO and the Winter Olympics in general. The restricted areas, described in the next subsection, also contained factual information, although the files were incomplete and disguised as belonging to the JTFO. The validity of the material was necessary in determining how well deception plans work using only true material. This will be further discussed later in this chapter.

2. Restricted Areas

The restricted areas of the JTFO website were clearly separated from the rest of the pages. The separate navigation bars for restricted areas contrasted sharply from the attractive design of public zone navigation bars. The restricted links were clearly marked "JTFO Use Only," helping to further isolate them on the main pages of the website. This isolation was intended to pique the curiosity of site users. Casual web surfers would naturally be attracted to links they cannot access. Intruders would target restricted links; anything that they cannot access must contain material that may benefit their cause.

Access into the restricted areas required user authentication. When users attempted to enter the protected area, they were prompted for a username and password. The list of authorized users was created fictitiously, using combinations of government agencies and personal names. Passwords were created with varying degrees of complexity; some were easy to crack, while others nearly impossible. The usernames and passwords were purposefully designed to create only a weak barrier to the protected area. The usefulness of the restricted area depended on it being seen by unauthorized users. For this reason, "crackable" passwords were chosen to actually permit diligent intruders to enter the restricted area.

The content of the protected area constituted the bulk of the deception in the JTFO experiment. Before the website was designed and implemented, the Salt Lake City-based JTFO provided copies of their entire file database. New dummy files were

created with the exact types, sizes, and names of the real JTFO files. The body of each file contained randomly generated characters, in order to resemble ciphertext, or encryption. In actuality, the files were nothing more than bait to lure potential intruders into the restricted area.

Research opportunities provided by the protected files existed in two forms. Although the files were actually useless, their existence added to the reality of the website. Without these protected files, the website would have seemed to be perhaps just an advertisement for the JTFO. To the outside user, the protected files provided a purpose to the website. To that outside user, the JTFO website appeared to be a means of fast exchange of files between JTFO members. Secondly, the files provided a target for hackers. Since the filenames were real and in plaintext, they were easily readable by anyone with access to the files. The filename provided the bait, while the filling was something for the intruder to download, alter, or even attempt to decipher.[12]

3. Search Engine

The remaining key part of the JTFO website was a user-friendly search engine. The search engine indexed the contents of each page on the JTFO web for easy reference by search users. The search page was intended to act as a portal into the minds of visitors of the site. All inputs to the search form were closely monitored, keystroke-by-keystroke. Most importantly, the filenames of the restricted files were indexed, so that they would appear in a typical search. This allowed the search page to act as a portal into the website for intruders. When keywords were searched that made up parts of filenames, those files came up in the search results. The links provided by the results page, however, did not allow access to the file without authentication. Essentially, the search page served two purposes. One was to track the desires of intruders. The second was to further entice these intruders to explore the website.

4. A Tour of the JTFO Website

When typing in www.jtfo.org or clicking on a link to the website, an intruder unknowingly ventured into a deception plan disguised as a simple website for an Olympic security agency. The first page in the site was a DoD warning, which alerted users that the site was for official uses only. It listed several conditions that users would

12 These attempts would be futile. The files were not actually encrypted; they only appeared to be.

agree to before entering the site. The page existed mainly to add more reality and enhance the credibility of the website, enticing intruders to further explore it.

By agreeing to the stated conditions, users would then see the main page of the JTFO website.[13] A brief description of the JTFO agency made up the text, while navigation bars ran down the left. Clicking on each of the public links (in blue), the user would be directed to the various public information pages within the website. Returning to the main page, the typical user would be drawn to the red links column, designated for "JTFO Use Only." When clicking on one of the red restricted links, an authentication prompt would appear. The user was required to enter a login name and proper password. After three unsuccessful logins, the user was denied access.

Rather than continued attempts at logging in as a JTFO member, the typical user would give up and surf the public pages again. Clicking on the "search" link, the user entered desired keywords, such as "plans." The results page listed several ".doc" files, followed by a few lines of what looked like encrypted text. The user clicked on the ".doc" link, only to be denied access to the file.

According to the plans of the web designers, JTFO website users would encounter such problems when attempting to intrude on the restricted directories. In the above fictitious situation, the user would be extremely curious about the contents of the file. At that point, the user might possibly resort to common "hacking" techniques, such as password sniffing and/or cracking. Hopefully, the user would eventually succeed at gaining access to those files, only to be stumped by the false encryption of the file contents. All of these scenarios will be further examined in the next chapter.

C. PROJECT IMPLEMENTATION

1. Red Hat Linux Operating System

The JTFO project's computer system was running on the Red Hat Linux operating system, with the web server running on Apache. Linux correctly identified all of the computer components and provided a stable platform and an ideal environment to run a web server. The Linux operating system presented various features and functionalities that made it both interesting and appealing, as it continues to grow and develop in today's

13 If users did not agree, they were directed to www.olympics.org, a site maintained by the Salt Lake Olympic Committee (SLOC).

market with the latest technologies. The installation of the operating system for the JTFO website included all of the functions and programs on the Red Hat Linux CD image.

There were many advantages to installing Red Hat Linux as the operating system. Initially, the computer that was used for this project ran Windows NT. The decision to switch to Linux consisted of several factors. The easy implementation of Linux with its step-by-step procedures was an influential factor in accepting this operating system. Linux has become widely used in the industrial world with its growing power and flexibility, as it can be used for networking and software development. The fact that Linux is free makes it a popular system, especially with its source code freely distributed on the global Internet. The open source form allows anyone to take the free source code, and modify or improve it to meet his or her needs. In addition, Linux is the operating system kernel, which comes with development tools that can be downloaded from any FTP server throughout the world or distributed in a medium such as a CD-ROM. These products are free or offered at a very economical price, which makes Linux an excellent, cheaper alternative to other expensive operating systems. With limited funds to start and run the JTFO project, the low cost of Linux ensured budget constraints were met and allowed hard capital to be allocated into other resources. However, there are disadvantages with Linux. Because Linux is well known and popular there are many tools available to hackers who desire to infiltrate Linux systems. The system is widely used, increasing the likelihood that unauthorized people will have the knowledge and capability of hacking into the JTFO computer running on Linux.

The version of Red Hat used in this project was version 7.2, and it can be purchased online at www.redhat.com. This is the latest version of Red Hat, which consists of several new features. It contains a simplified user interface, security and new graphical tools, unified procedures, and improved product support. Red Hat, with its network and technical support services, ensured that the system was up to date and ran securely. Red Hat version 7.2 contained network configuration tools needed to make the Internet connections easier for this project. It also consisted of user management tools that sped up the system administration. The installation ran as smoothly as any Windows installer. The process was straightforward and simple, as the program on the CD took care of installing the operating system and its applications.

2. Apache Web Server

The Apache Web server is, by a huge margin, the most popular Web server on the Internet because of its power, flexibility, and configurablility. Apache hosts more websites than any other web server. It was chosen to power the JTFO website because of its easy implementation and the capabilities that it possessed. The installation of the Apache Web server, like the Red Hat Linux operating system, was very straightforward with simple steps being provided. The JTFO server was configured using all of the default settings except where changes were necessary for naming and network configurations. Apache has the capability to run on sites that get million of hits per day and experience no difficulties with performance. As with Linux, Apache is so widely used that there are a wide range of hackers with experience working with it. This increases the possibilities of people intruding on the JTFO web server, which are needed to guarantee success in this study. The Apache Version 1.3 was used during this project and normally can be downloaded from http://httpd.apache.org/. However, Apache Version 1.3 was included with the installation of Red Hat Linux as the operating system.

An attractive feature to using the Apache Web server was its ability to keep track of log files. It recorded all the requests processed by the server. The format of the access log was highly configurable. It was specified to meet the needs of the project via a format string. The server's activity was recorded onto the log files, which were used for data analysis. The two log formats used in this project were combined and common. The common log format can be read by many log analysis programs and produced by many web servers. An example of this format looks like this:

> 131.120.104.89 - - [08/Feb/2002:10:44:35 -0800] "GET /_themes/corporate-with-flag/flag.jpg HTTP/1.1" 200 5220

The combined log is similar to the common log except for two additional fields. These additional fields tell where the client has been referred from and the identifying information that the client browser reports about itself. An example appears as follows:

> 131.120.104.89 - - [08/Feb/2002:10:44:34 -0800] "GET / HTTP/1.1" 200 2610 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)"

These log formats allow for the interpretation and analysis of the hits the server registered during the Winter Olympic Games.[14]

3. Arrangement of the Web Server

a. Creation of Files and Directories

The JTFO website contained fictitious files and directories that were created to match the actual JTFO directory. This directory contained a complete list of subdirectories and files directly from the JTFO computer in Salt Lake City. These files included executables, documents, power points, spreadsheets, jpegs, bitmaps, and other file types. Each file had a particular size and name and was placed in a certain subdirectory. The intent was to create a facsimile of the JTFO directory with the same files and subdirectories. These files and subdirectories had the same name and size, but contained random ASCII characters. Anyone trying to hack into the JTFO website would believe these files were actually from the Joint Task Force Olympics. This was the primary form of deception in this project, as the hope was to see what files someone hacking into the website would try to access.

A program was created in Microsoft Visual C++ to create these files filled with random characters. The program read from a text document and copied the names of all the files in the document, then duplicated the JTFO files' size and name. In addition, this program looked at the size of each file and filled it with random ASCII and special characters. The size of the file told the program how many ASCII characters to generate. There were two problems in using this computer program. The first was that the "creation date", which included the time, day, month, and year, of the original documents could not be copied and attached to the duplicate documents. Instead, the imitative documents were stamped with the date in which the program created them. This may have detracted from the deception's effectiveness, since most of the files were created on the same day or at least within a couple of days from each other. The second problem was not as glaring but more tedious. There was an inability for this program to create the directories and subdirectories and have all those files placed in the certain subdirectories. Instead, the directories had to be manually created and the files created by the program were manually moved one-by-one into separate directories. This problem

14 Apache HTTP Server Project. http://httpd.apache.org/docs/logs.html.

had no significant effect on the deception, but was extremely time consuming and inefficient.

b. Organization of Files

After the fictitious files were created, they had to be organized in a certain way to promote credibility. The Winter Olympic Games were designated a National Special Security Event under PDD 62. Commander-in-Chief, US Joint Forces Command (CINCUSJFCOM) was designated to provide routine and contingency support to The Games. The JTFO was created by the CINCUSJFCOM Executive Order to provide support to the Utah Olympic Safety Command (UOPSC), FBI, and Secret Service. The US Attorney General approved the routine support, which were divided into five categories: aviation, communication, explosive ordinance disposal, physical security, and temporary facilities. The duplicate files were placed in the restricted area of the JTFO website. The files were divided into different categories, which were: administrative, comptroller, operations, logistics, plans, physical security, temporary facilities, and training.

The five categories of routine support were not used in this project, but instead, the eight different categories previously listed. The "JTFO Use Only" categories that were created on the website and labeled in red color reflected information that would be of noticeable interest to those hacking through the website. The information type included those from the U.S. Joint Staff. The components directly involved in the JTFO were the J1, J2, J3, J4, J6 and J8[15] with each section having a particular function. In addition other information of interest included real-time information, JAG, force protection, Public Affairs, and protocol. The intent was to create categories on the website that would reflect information desired the targeted Internet terrorists. The categories were:

- J1 (Manpower and Personnel) ensures the provisions of adequately trained and skilled people and oversees all military and civilian programs. The information from the J1 section would include joint manning document, names of all the JTFO staff, names of supporting unit personnel and units, security clearance data, and so forth.

15 J*X* refers to a corresponding department in the Joint Staff: J1 (Manpower and Personnel), J2 (Intelligence) J3 (Operations), J4 (Logistics), J6 (Command, Control, Communication, and Computers Systems), and J8 (Force Structure, Resource and Assessment).

- J2 (Intelligence) gathers and analyzes data and provides all-source intelligence to the Joint Chiefs of Staff, Office of the Secretary of Defense, Joint Staff, unified commands, and other national agencies. The J2 section would focus on information pertaining to request for information and threat assessments.
- J3 (Operations) translates the Joint Staff's planning, policies, intelligence, manpower, communications, and logistics into actions. The J3 section would look at aircraft staging areas, date of troop movements, security operation key dates, troop strength per venue, date of troop movements, and aircraft types and number available.
- J4 (Logistics) is responsible for the readiness and capability of U.S. strategic forces. Their information type would include bus route schedules, bus routes for troops, ordering of supplies, food service methods, locations, schedules, and troop travel times from billeting to venues.
- J6 (Command, Control, Communication, and Computers (C^4) Systems) provides advice and recommendations to the Chairman on issues related to C^4 matters. The type of information the J6 provided was IP addresses for JTFO domain, system cell phones, system Email server, system JWICS, system SIPRNET, and radio frequency assignments.
- J8 (Force Structure, Resource and Assessment) is responsible for developing force structure requirements, for conducting studies, analyses, assessments, and for evaluating military forces, plans, programs, and strategies. The J8 section's information included budget, funding plans and status briefing slides, bills, invoices, and budget and finance items.

4. SHADOW

SHADOW (Secondary Heuristic Analysis for Defensive Online Warfare), developed by the U.S. Navy, is a Network Intrusion Detection System (N-IDS) that was used to monitor the logs for the JTFO web server.[16] There are some features of SHADOW that made it attractive for use in this project. It collects information from the network, analyzes information of interest, and reports the conclusion. It takes in packets from the network interface and looks for any hacker trying to break into the system or causing a denial of service attack. As a network intrusion detection system, SHADOW positions itself between the firewall and the Internet and monitors incoming and outgoing packets. It uses traffic analysis to search for a variety of attacks and probes made on the system by looking at the packet headers.

16 For more information look at http://www.inforeading.com/archive/info_articles/Shatto/ids.htm.

SHADOW is comprised of two workstations, which are the sensor station and the analysis station. The sensor station is the machine that sits between the perimeter firewall and the Internet. Its purpose is to capture all the traffic and record it for later analysis. It sniffs all the incoming data by means of tcpdump[17] and logs it to the disk. The analysis station is located on the server side of the perimeter firewall, as its function is to take information captured by the sensor station and check for potentially dangerous traffic. The analysis station connects via a secure shell public key authentication to the sensor and downloads all the information the sensor collected, uses filters to run through the information, and displays the information on a web browser.

In this project SHADOW collected all the hits to the server and created a log for later analysis. Similar to a database, a list of hits that came from all server components, including *JTFO.ftp, JTFO.telnet,* and *JTFO.netBios,* was attained with the specification of the day, month, and year. A record of all the hits was listed and arranged according to time and date. By default SHADOW downloads the traffic information every hour from the sensor station, grouping the logs by hour. Analysis of the information was made possible by looking at the list of all the hits, which came in the form of logs.

5. Access Logs

a. SHADOW Logs

Three main logging mechanisms were used to collect the data used during the JTFO experiment, the SHADOW logs, the Apache logs, and search engine logs. The main logs, which produced the most useful data, were generated by the SHADOW program through the RIDLR[18] analyst computer. These logs kept track of each packet that passed through the connection between the Internet and the JTFO web server. Each entry in the log (described earlier in this chapter), provided the following pieces of information about each packet:

- Date and time of each entry.
- Source IP address of each packet.
- Destination IP address or server of each packet.

17 Tcpdump allows the examination of the header of each packet flowing over an interface or data link.

18 The RIDLR (Reconfigurable Intrusion Detection Laboratory Research) Project at the Naval Postgraduate School is an ongoing research tool used for development of intrusion detection systems. The JTFO computer was a temporary component of this network.

- Appropriate TCP/IP command of each packet.
- Size of each packet.

Information provided by these logs allowed easy monitoring of all activity on the JTFO web server.

b. Apache Logs

Another collection of data was obtained through the web server itself. Apache has the capability to log each hit to the website. Although the logs only indicate hits to the "www" port of the web server[19], they collect valuable information that is not available through the SHADOW logs. In addition to the information supplied by the SHADOW logs, Apache provides the following:

- Individual web pages that each visitor to the site has viewed.
- Operating system that each visitor uses.
- Any input that users type into the authentication form required for entry into the protected area.
- A configuration that converts the source IP address of each visitor into the domain name of that visitor's computer or Internet service provider (ISP).

This information provides more detail than the SHADOW logs, helping to further understand and interpret the behavior of possible intruders when they are on the website. The Apache logs are limited, of course, to only hits on the website portion of the web server.

c. Search Logs

A final source of data surrounding the JTFO web server was included on the search engine page. The search form was inserted into the JTFO website using a freeware version of Perlfect Search 3.30, obtained through the Perlfect website www.perlfect.com/freescripts/search. The script was simple to execute, and only required minor changes to the configuration in order to operate smoothly in the JTFO web server. An important feature of this particular script was its logging capabilities. The script generated simple log entries, which included the date and time of each entry, as well as each keystroke-by-keystroke monitoring of the search form on the website. The logs did not include source IP addresses of the site users, but this was easily

19 Other server ports include those for file transfer protocol (FTP) and telnet functions of the web server. These are all included in the previously described SHADOW logs.

synchronized with information obtained through the other logs. By combining the data collected by the three logs, each visit to the JTFO website was closely documented and monitored.

D. SUMMARY

The elements of deception were carefully worked into the JTFO website. The web pages had to be designed in such a way to promote their credibility so hackers were encouraged to look into it. Many factors were considered in the designing of the JTFO website. The website used a ".org" domain name rather than a ".mil" in hopes of creating a false sense of security for those entering the site. In addition the website had a dual image with both a public and restricted area. The public information contained Internet links, factual information about JTFO and the Winter Olympics, and a search engine. The restricted area was organized into categories of interests to hackers and was filled with fictitious files and directories that were created to match the actual JTFO directory. All of these helped to advance the objective of the website because hackers could easily find or possess the tools needed to bypass Linux and Apache. The setup and design of the website were carefully considered in order to promote a convincing deception and also to analyze the behavior of those entering the system.

The following chapter will describe the various types of attacks that hit the JTFO computer. Each of the logging mechanisms played an important role in the collection of data for this project. They covered separate styles of network attack targeted at the server, and allowed convenient organization of the data as needed. The separate areas of the web server and individual pages also provided numerous targets for intruders, enhancing the effectiveness of the deception scheme. All of these attacks and intrusions will be discussed in Chapter VI.

VI. PROJECT RESULTS

The JTFO project was conceived in the weeks prior to the commencement of the Olympics in February 2002. The original plan was for a mock website to be set up as an aid to security measures in Salt Lake City. As the proposed launching date for the website drew near, the plan gradually evolved until the JTFO website became an independent tool to be used mainly for research, with the possibility of support to actual law enforcement. The website went online on 30 January 2002, although the website and its components were still undergoing continual changes. These changes continued until the start of the Olympics, when the final layout of the website was uploaded to the web server. Refer to Figure 1 on the following page for a visual view of the events during this study.

A. PROJECT PITFALLS

1. Time Period

The JTFO experiment was to provide research and support to law enforcement, but its shortcomings contributed to the low probability of complete success. The time restrictions of the project placed strict limitations on the timeliness and completeness of the deception scheme. Although a time period of several months would have been more useful, project planning and development was compressed into a period of just over four weeks. The JTFO website was available on the public Internet only from the 31st of January to the 3rd of March. With limited time to prepare the deception was quickly implemented, however, this opened the possibility of several mistakes and inconsistencies.

Effective deception achieves its best results when employed for much longer periods of time. Although the aim of the project was not to lure potential terrorists, sufficient amount of time is needed to allow the enemy to observe intended indicators, process and correlate the information, and take appropriate action in support of the deceiver's objective. The project's goal was to deceive those that came across the site. With more time the website would have been online earlier, allowing more time for potential intruders to come across the site. This allows for extensive profiling of intruders, resulting in further refinement of the deception components of the honeypot.

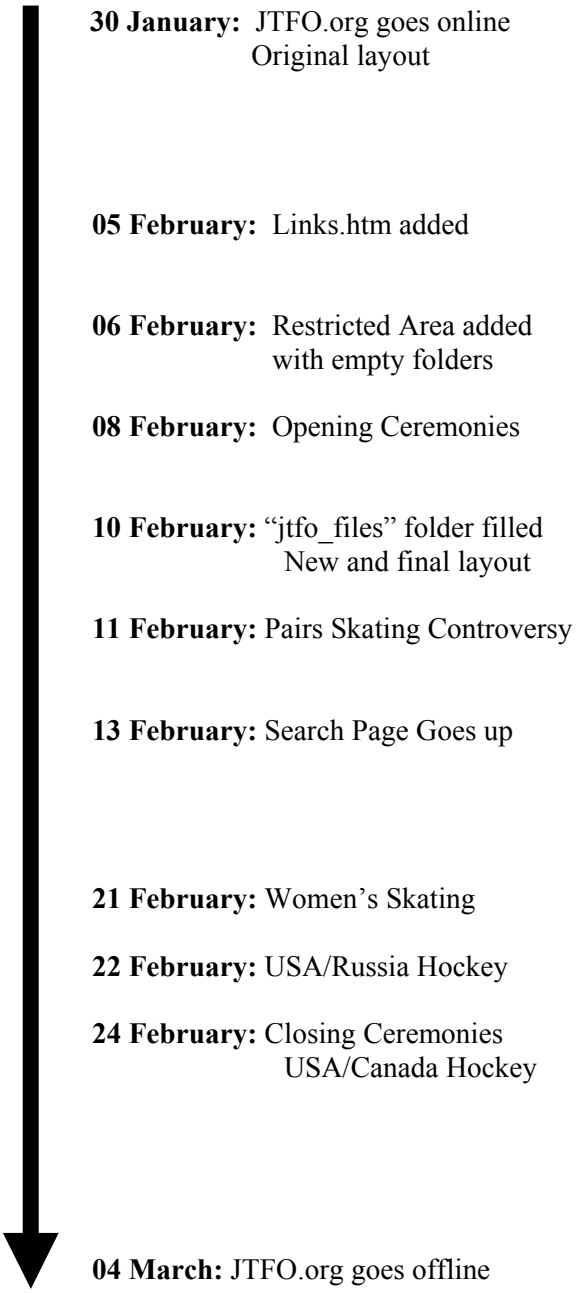

Figure 1. Timeline of Significant Events During the JTFO Experiment.

Ideally, data collected from the JTFO honeypot would have helped produce detailed sketches of the habits of common visitors of the website. The sketches could be compared to known profiles of several types of hackers and Internet terrorists. Although hackers were not the targets studied in this project, knowing their profiles would help to differentiate them from the Internet terrorists. Common styles of the hackers could have been discovered, while continually developing new deception components tailored to those hacker profiles. The time constraints placed on the project reduced the amount of data collected and the numbers of effective changes that could be made to the website. Once profiles were developed using JTFO project data, very little time was left to adjust the web content in order to maximize the effectiveness of the scheme. More material could have been placed on the website as the Olympics carried on. This would have attracted repeat visitors, as well as new ones altogether.

2. Lack of Exposure

Another cause for incompleteness of data collection for this project was a lack of exposure. Part of the project's initial plan was for the website to be an actual component of the JTFO information campaign, while providing research opportunities. As the Olympics drew closer, the role of the website diminished, becoming an independent study with the support of the JTFO in Salt Lake City. With this new role, the website received considerably less publicity than originally planned. Instead of being a link on other high-profile Olympics-related sites, the JTFO website received virtually no exposure on the Web. Applications were filed with major Internet search engines, with one request being processed, but this was only after the Olympics had concluded. On these search engines people with the proper request would have the JTFO website match to their search interests. However, time constraints prevented www.jtfo.org from gaining a place on free search engines like Google, and there were limited funds to advertise on other search engines. With no publicity through the JTFO or any other Olympic agency, the JTFO website was not known to many people outside of the DoD. Relatively few people accessed the website or web server, presumably because they simply did not know about it. However, there were several instances (to be discussed later in this chapter) in which users returned to the site. This generated some quality data with which to carry out the research, although the data was ultimately much less than anticipated.

3. Tracing Users

In order to realistically perform law enforcement functions, a deception scheme such as the JTFO project requires the support of several other groups. A major shortfall in this project was the inability to trace connections to one single user. When a user connected to the JTFO website, Apache accurately logged each connection, recording the source IP address of each user. All connections to the web server were logged through the server's connection to the RIDLR SHADOW program. As often as twice daily, these IP addresses were traced using an Internet tool from a government website, www.nnic.noaa.gov/beta_router.html. Since these connections were already terminated, the trace usually reached a dead end at the address of the user's host domain, computer, or Internet service provider (ISP). Examples of these dead ends were national ISP users such as America Online, local or regional ISPs such as Pacific Bell, and university or commercial computers. The traces could not normally go any further, so the users could not be positively identified. The usefulness of these traces was in characterizing each user according to geographic location, a point that will be further looked at later in this chapter.

The solution to the trace problem lies in tracing the connections while they are still active. This can only be done with the support of other agencies. Perhaps with the help of the FBI or other law enforcement agencies, the identities of unknown computers could have been further researched.

4. Lack of Funding

Rapid development of this project meant that there was no budget allocated for it. . For a project with real world application, no financial support was set aside to facilitate this project. This lack of funds created several disadvantages. The website was to be housed in a simple Apache web server. Required resources for the project, including computer components, software, and Internet domain space, were obtained through loaned material and personal funds. In the end, the server for this project was not up to date with the newest technologies, inhibiting the ability to keep up with the techniques of the intruders that were to be studied.

B. ANALYTICAL FRAME

In this project, the intent was to look at the data attained from the access logs and assess who entered the system. As people entered the system there needed to be a known profile with which to compare them. In other words, a base was needed in order to compare the hackers and the Internet terrorists with known categories in order to determine who actually hacked into the system and what their intent was. Although the targets of this project were Internet terrorists, profiles of different types of hackers were developed in order to differentiate them from Internet terrorists.

1. Blackhat Community

One group of concern was the Blackhat community. These are hackers with malicious intent, whose tools, tactics, and motives were documented in the HoneyNet Project.[20] The HoneyNet Project was a research tool and network specifically designed so hackers would compromise it. The network sat behind a firewall and any system could be attached within it as a honeypot, such as Solaris, Linux, or Windows NT for a more realistic feel as a network environment. The HoneyNet Project consisted of thirty security professionals who were non-profit, and once the honeypot was compromised, they could assess the tools, tactics, and motives of Blackhats.

Within the Blackhat community, a common threat was the script kiddie methodology, in which someone looks for the path of least resistance. Although the motive may be different, the goal of these individuals is the same: finding the easiest way to gain control of as many systems as possible. With this method they focus on a small number of exploits on the system and then search the Internet for the given vulnerability. They randomly search for a specific weakness and then exploit it. The script kiddie methodology could have been used on the JTFO website, as these individuals randomly select targets and eventually probe a system and network. Most of the tools that are used for probing a system are easy to use and widely distributed. With so many people on the Internet using these tools, it becomes only a matter of time for a system or network to be probed. (HoneyNet Project, 2002, pp. 125-126)

20 Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community (New York: Addison-Wesley, 2002).

The Blackhat community is characterized as a robust, strong, complex meritocracy with very stable characteristics. These hackers put strong emphasis on their standing in a status hierarchy within and outside of a local social network. In addition, they use derogatory statements in their conversations for the purpose of challenging the status of others and in social control processes (HoneyNet Project, 2002, p. 263). However, derogatory comments and status conflicts prevent cohesiveness. Their fear of detection and arrest can also reduce the stability of these groups and limit unity.

According to the HoneyNet Project the motives differ for hacking into vulnerable systems. One major motive is the Denial-of-Service (DoS) attacks, in particular distributed denial of service. A single hacker can control hundreds of thousands of compromised systems throughout the world for the coordinated execution of a denial-of-service attack against one or more victims. This makes it difficult to defend against and to identify the source of attack. The attacker randomly finds vulnerable system to compromise and control and the distributed denial of service becomes stronger with more compromised systems. (HoneyNet Project, 2002, p. 132)

A second motive for hacking into a system is to be used as a defensive technique. The reason for hacking into a system by members of the Blackhat community is to hide their source and identity. They do this by compromising systems in a series of hops. The hacker will hop to another system after compromising a system, and will continue this until they achieve their objective. This makes it difficult to trace the hackers back to their source, since language barriers, time zones, and government structures make it impossible to follow the numerous hops of compromised systems. (HoneyNet Project, 2002, p. 133)

Another motive for hacking into a system is hackers want to maintain administrative rights to their Internet relay chat channel, which is used as a primary means of communications among Blackhats. In order to maintain this right, the hacker is required to keep a presence on the channel. They use a tool called a bot to keep their rights at all times, but other hackers can eliminate them. As a result, hackers try to compromise as many systems as possible in order to launch the bots from the compromised systems. With more compromised systems there are more bots, which

means the hacker have more power on the Internet relay chat channels. Furthermore, more compromised systems allow the hackers to launch denial-of-service attacks against other Blackhats in order to take out or remove their bots from the Internet relay chat channels. (HoneyNet Project, 2002, p. 133)

Breaking into a site provides bragging rights for members of the Blackhat community. The sites being broken into do not matter; instead, the sheer number of sites that are compromised is the biggest factor. They often break into the website and modify them to brag. The accounts of the compromised website can be exchanged for things of value, such as credit card numbers. In addition, a compromised site can provide storage and distribution centers, which can be used to distribute tools, documents, and cracked software. (HoneyNet Project, 2002, p. 134)

2. JTFO Hacker Profile

In the JTFO *After Action Report*, threats from the Internet were profiled into two categories, structured and unstructured. The growth of Internet access, combined with the increase of information stored, processed, or transmitted on computer systems, led to increased threats and increased vulnerabilities of information resources. The activity of the hacker can be labeled as suspicious or reconnaissance activity, unauthorized access, denial-of-service, data browsing, data corruption, and malicious code. In a structured attack the hackers are characterized as sophisticated and organized with common goals. They are the most severe threat, as they target specific systems or groups of systems for industrial and military espionage, malicious intentions, financial gains, and, or military operational advantage.

Unstructured attacks have less organization but use the same technique as the structured attacks. The action of a common computer hacker is categorized as an unstructured attack. These hackers randomly pick their targets, probing different domains for the purpose of finding vulnerabilities to exploit in common systems. Some seek success for the purpose of gaining status in the hacker community. Others have malicious intent as they could implant logic bombs and Trojan horses, conduct denial-of-service attacks, or alter data for the purpose of creating hardship to the system users.

C. ANALYSIS OF ATTACKS

The attacks on the JTFO computer targeted two main destinations: the website side of the computer, and the server side of the system.[21] Whenever there was a request for a file on the Apache web server (the website side), a response was generated, creating a record on the log file. The server side generated data through the SHADOW program, as previously discussed. As stated earlier, it is from these log files that data was collected for statistical analysis. The information from the logs will provide a comparison of the hacker against the known profiles stated earlier in this report.

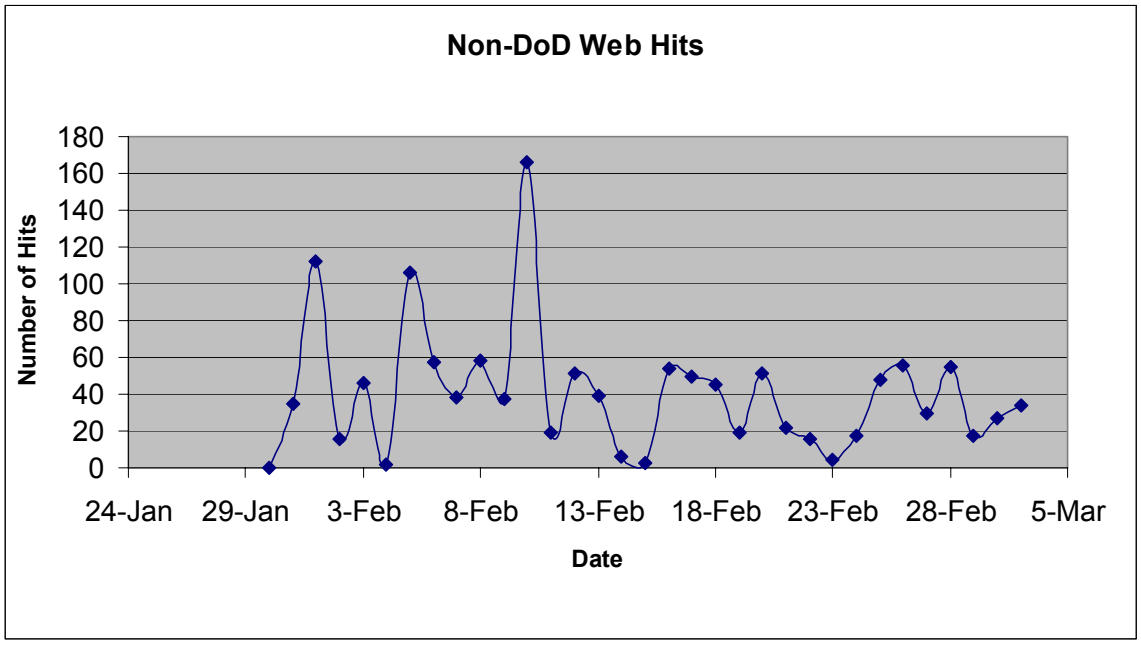

Figure 2. Site Hits per Day on www.jtfo.org.

From the IP address, a basis for identification could be made for each person who entered the website or contacted the server computer. Although absolute identities could not be established with the project's limited capabilities, each intruder could be distinguished from another by relying on IP addresses. As stated before, a public DNS search engine was used to determine whether those entering the site was either affiliated

21 The website side is composed of hits on Port 80, the HTTP port. The server side covered the telnet, FTP, and netBios components of the JTFO computer. These ports are discussed in more detail later in this section.

or not affiliated with the Department of Defense (DoD). During the Winter Olympic Games there was a total of 4709 hits to the JTFO website, 1336 of which were not from the DoD. According to Figure 2 on the previous page, most of those hits came on 10 February. Figure 2 displays a chronology of hits on the JTFO website. The DoD members that accessed the website particularly included the Naval Postgraduate School students and faculty working on this project, the Joint Task Force Command, and the National Guard, which were all military or ".mil" sites. Those not associated with DoD were the main subjects of interest in this project.

One of the initial objectives was to determine who accessed the JTFO website. During this project the server logged approximately 102 different, non-DoD IP addresses, which entered and contributed to the 1336 hits to the website. Figures 3 and 4 on the following pages provide a chart of all the non-DoD IP addresses that accessed the site. Figure 3 contains a list of IP addresses that accessed the JTFO website more than ten times, while Figure 4 displays less significant IP addresses who seldom accessed the website. The reason for the differentiation is those IP addresses that had less than ten hits were considered less of a threat. It is safe to assume those with malicious intent would surf the site and accumulate numerous hits to the website. With that logic the 48 different IP addresses in Figure 3 are considered potential hackers. These IP addresses contributed to the majority of the non-DoD hits to the website; meaning there could be suspicious activity that include looking at .htm or .html pages, downloading JTFO files, or installing viruses into the program. Most of the website side of the analysis in this project is centered on the IP addresses from Figure 3.

A hit to the website did not simply constitute entering and leaving a site. For example, ten hits meant more than a user entering the site and exiting the site at ten different times. Instead, it included the accessing of files, the loading of different images such as .gif and .jpg onto the screen, going to different WebPages within the site, or viruses hacking into the system. Multiple hits can take place in one visit to the JTFO website. To access the site's home page or in this case the index page would have automatically resulted in multiple hits, as the download of each .gif image constituted as a hit. For an IP address to have fewer than ten hits seems unlikely to be a threat, because it provides no evidence of users searching the site for information. Those snooping

around the site would amass many hits. Nevertheless, these IP addresses still remain a potential threat. According to the data, 36 distinct IP addresses had only one hit to the

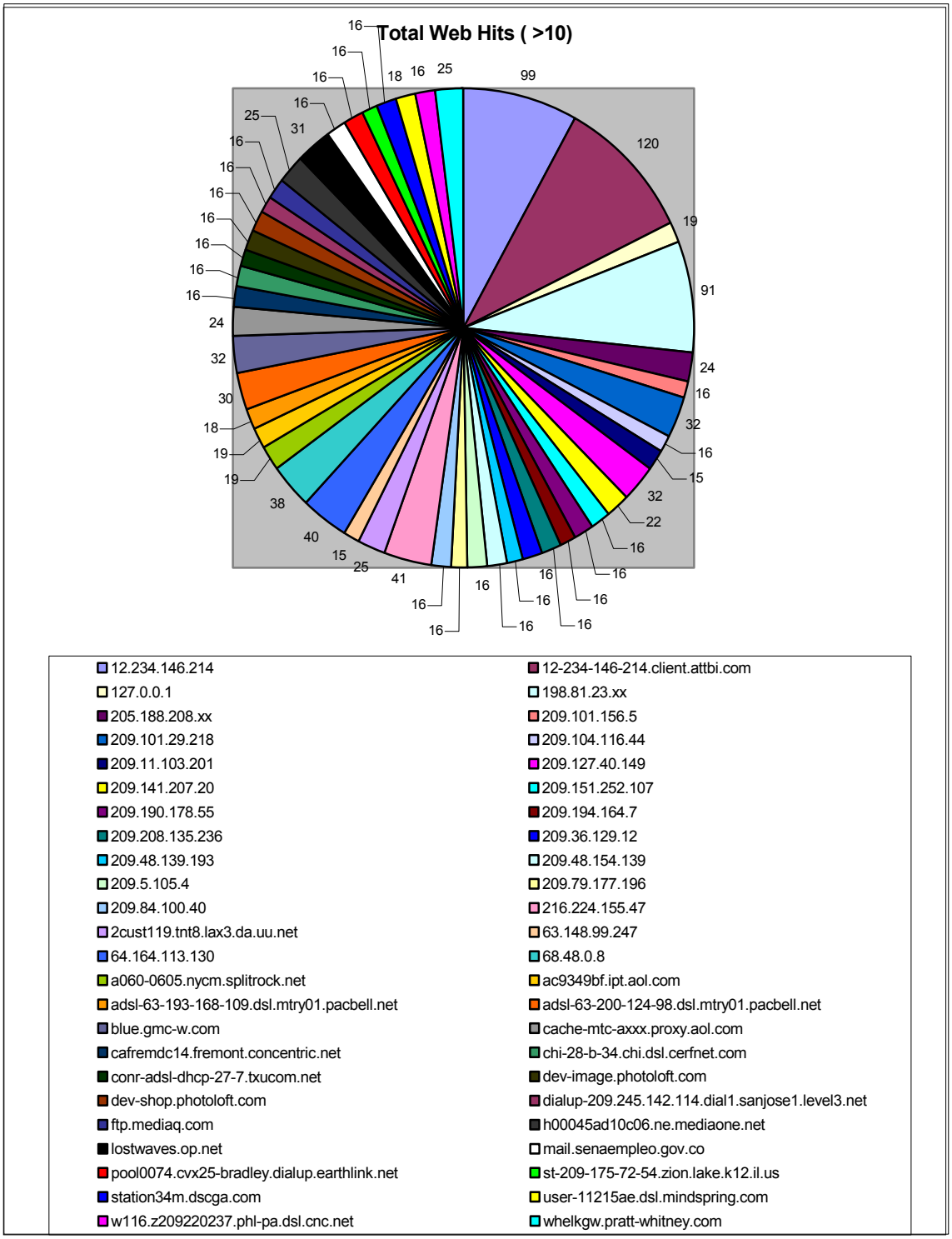

Figure 3. Numbers of Total Web Hits During the Entire Project, Including Only IP Addresses that Appeared More Than 10 Times.

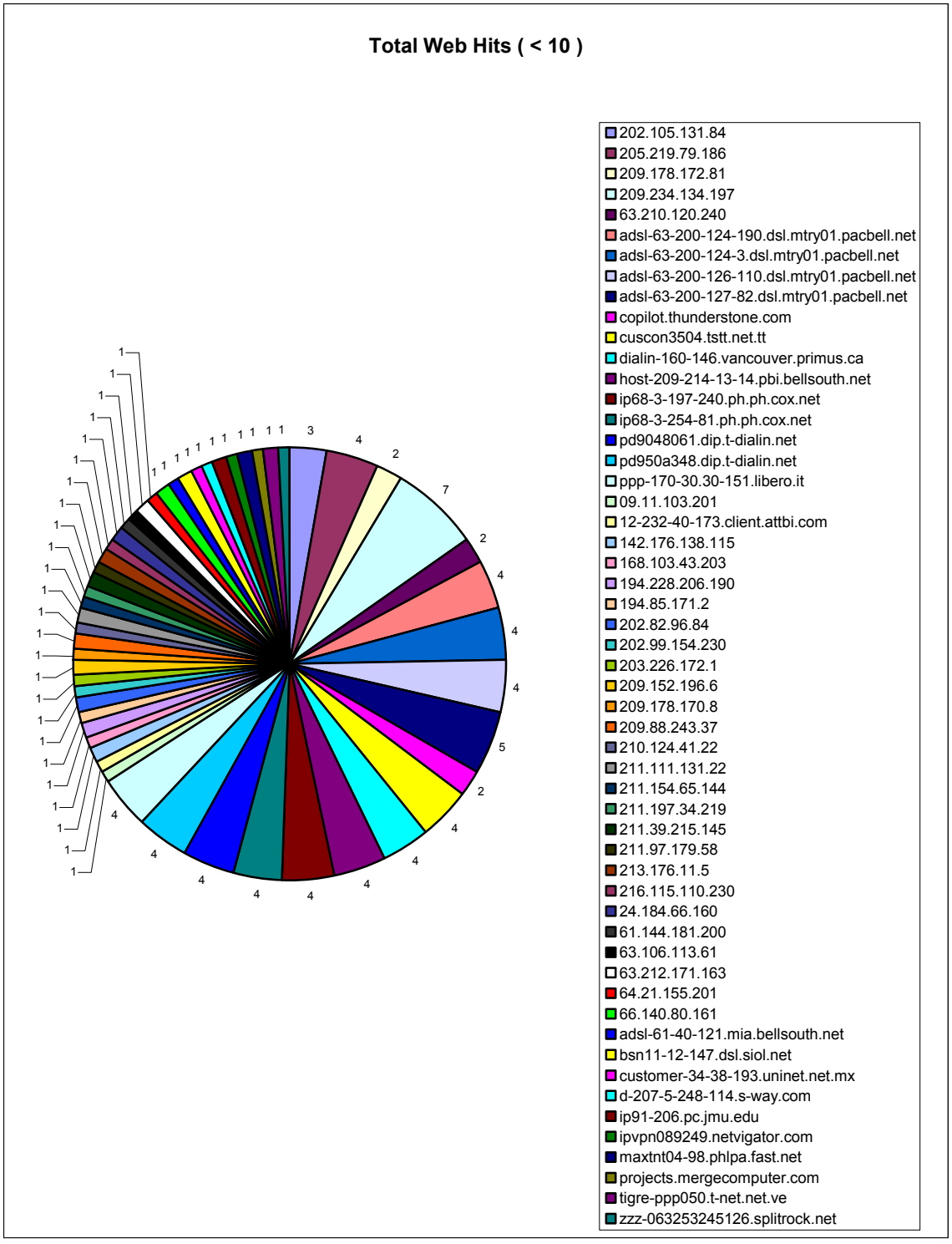

Figure 4. Less Significant Web Hits on the JTFO Server.

site. This could mean those entering the site saw what it was and immediately left for whatever the reason. However, the explanation that needs to be considered is the use of computer worms. In this project two worms, W32/Nimda-A[22] and Code Red[23], were spotted and only one hit from an IP address is needed to implement them.

On the server side, the JTFO system was subject to three large-scale attacks and several minor attacks during the month-long project. From 31 January through 03 March 2002, the SHADOW program logged an average of 5506 entries each day. On three days during the beginnings of the Olympic Games, the server logged extraordinary amounts of activity on its HTTP, FTP, and telnet components. The logs from each of the three main server attack days (09, 10, and 13 February) displayed a blueprint of exactly what the alleged hackers did to disrupt the service of the JTFO computer system. By analyzing these attacks, the tendencies of these attackers can be determined so that proper defenses can be implemented for future website design.

1. Worms

a. Code Red

One type of worm attempting to hack into and infect the machine was the Code Red worm, which is another self-replicating worm that exploits known vulnerabilities in Microsoft IIS servers. This worm exploits buffer overflow vulnerabilities. It affects Microsoft Index Server 2.0 and the Windows 2000 Indexing service on computers running Microsoft Windows NT 4.0 and Windows 2000 with IIS 4.0 and 5.0 Web servers. It goes to a randomly chosen host by spreading through TCP/IP transmissions on port 80. It sends an HTTP GET request to the victim for the purposes of exploiting buffer flow vulnerabilities in the Indexing Service (.ida). The overflow allows the worm to execute code within the IIS server in order to spread itself to other potential victims on randomly chosen IP addresses. A packet flooding, denial-of-service attack will be launched against the victim's host. The infected machines will randomly attack other servers and perform denial-of-service attacks against the White House's official

22For more information on W32/Nimda-A worm refer to http://www.sophos.com/virusinfo/analyses/w32nimdaa.html.

23 For more information on Code Red Worm refer to http://www.cert.org/advisories/CA-2001-19.html.

website, which is the direct target of the worm's attacks. The indirect effect is the large amounts of data hitting the Internet, resulting in degradation in performance.[24]

The footprint of this worm was identified in the web server log files and has the following form:

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%
u0000%u00=a
```

The existence of this string in the log file does not identify compromise to the system, but shows an attempt was made to infect the system. If successful, the worm would deface the web page with the following message:

HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

The worm as a result of its scanning activity can cause performance degradation on the infected systems. The systems and networks that are not compromised and being scanned by infected systems may experience denial-of-service attacks.

There were a total of 24 different attacks to the web server conducted by the Code Red Worm with each attack constituting a hit to the server. The graph in Figure 5 on the following page demonstrates the number of Code Red Worms that attempted to compromise the system during a particular date. In addition, the chart on Figure 6 on the following page provides a list of the IP addresses of the Code Red Worm with the respective time in which it attempted to compromise the system. There were no repeated Code Red attacks from the same IP address. The Code Red Worm attacked the most on the 8th and 10th of February with five hits on each day. The Apache Web server recorded each attack by the Code Red Worm as one entry to the log files. As stated earlier, IP addresses with only one or few hits could pose as a serious threat because only a single entry is needed to send the Code Red Worm.

[24] Lemos, Rob. (2001) Tracking Code Red. http://news.com.com/2009-1001-270471.html (3 June 2002).

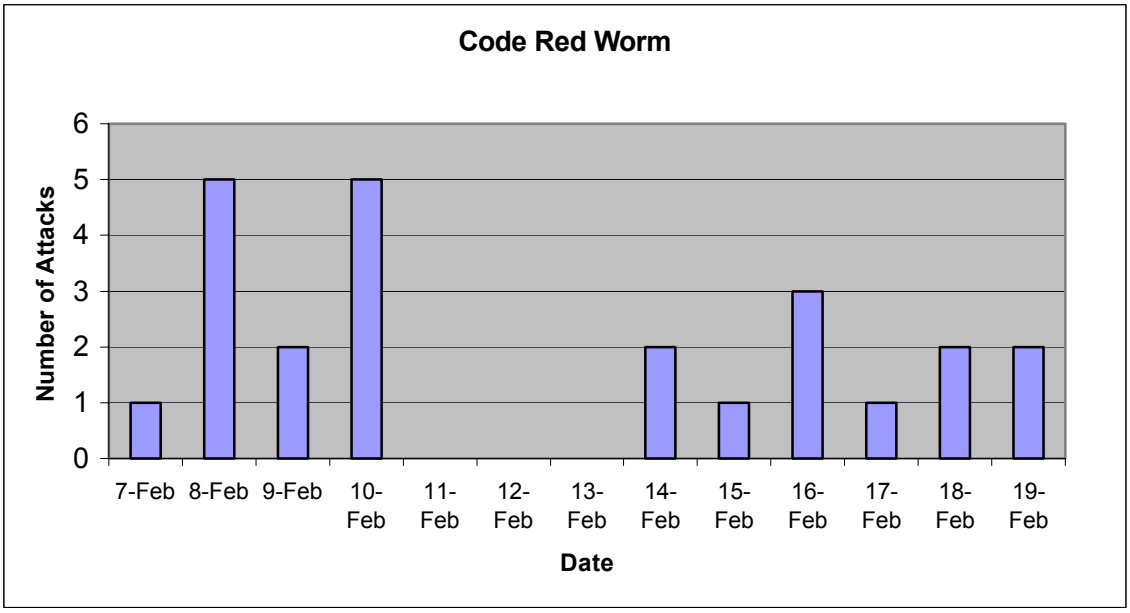

Figure 5. Numbers of Hits by the Code Red Worm Each Day.

IP Address	Date
203.226.172.1	07/Feb/2002:10:05:42
66.140.80.161	08/Feb/2002:01:53:06
168.103.43.203	08/Feb/2002:06:18:27
202.82.96.84	08/Feb/2002:09:54:50
customer-34-38-193.uninet.net.mx	08/Feb/2002:12:21:24
12-232-40-173.client.attbi.com	08/Feb/2002:22:11:05
bsn11-12-147.dsl.siol.net	09/Feb/2002:06:39:21
ip91-206.pc.jmu.edu	09/Feb/2002:09:50:40
d-207-5-248-114.s-way.com	10/Feb/2002:00:16:00
194.85.171.2	10/Feb/2002:02:18:13
adsl-61-40-121.mia.bellsouth.net	10/Feb/2002:11:00:20
zzz-063253245126.splitrock.net	10/Feb/2002:18:07:09
211.111.131.22	10/Feb/2002:23:51:09
ipvpn089249.netvigator.com	14/Feb/2002:02:31:58
202.99.154.230	14/Feb/2002:07:28:35
maxtnt04-98.phlpa.fast.net	15/Feb/2002:14:07:08
projects.mergecomputer.com	16/Feb/2002:05:16:08
211.197.34.219	16/Feb/2002:19:21:28
142.176.138.115	16/Feb/2002:22:09:50
61.144.181.200	17/Feb/2002:14:20:26
63.106.113.61	18/Feb/2002:05:33:29
213.176.11.5	18/Feb/2002:15:08:48
211.39.215.145	19/Feb/2002:01:50:48
tigre-ppp050.t-net.net.ve	19/Feb/2002:03:49:45

Figure 6. Source IP Addresses of Worm Hits During the Project.

b. W32/Nimda-A

On September 18, 2001 a new worm named W32/Nimda-A, also known as Nimda, Minda, Concept Virus, and Code Rainbow, came into existence on a very large scale. This worm spreads itself via website, network shares, and email and targets different machines by using known Microsoft Internet Information Server (IIS) vulnerabilities.[25] Using email this worm goes to people's inboxes as a message with a variable subject line. The affected email has an attachment named "readme.exe." W32/Nimda-A formats the email so that it takes advantages of the patches in older versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer. The virus uses the holes to automatically run the executable file without the user double clicking on the attachment. When the new victim is infected, the worm emails copies of itself to other potential victims and starts looking for vulnerable IIS web servers. After installing itself and infecting the IIS web servers, the worm will modify web documents and certain executable files found on the system, and creates numerous copies of itself under various filenames. If people using Internet Explorer as their browser and are vulnerable to the holes, they will execute the readme.exe attachment as if they opened an infected email message.

The complete signature of the Nimda Worm consists of 16 entries. The format of the worm's attack string used to exploit IIS web servers is as follows:

```
/scripts/root.exe?/c+dir
/MSADC/root.exe?/c+dir
/c/winnt/system32/cmd.exe?/c+dir
/d/winnt/system32/cmd.exe?/c+dir
/scripts/..%255c../winnt/system32/cmd.exe?/c+dir
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../../winnt/system32/c
md.exe?/c+dir
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
/scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
```

25 The Microsoft Internet Information Server (IIS) deploys Internet Explorer and other business applications, host and manage Web sites, and publish and share information securely across a company intranet or the Internet. For more information go to http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/ierk/Ch05_d.asp.

/scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
/scripts/..%252f.. /winnt/system32/cmd.exe?/c+dir

The first four entries consist of attempts to connect to a backdoor left by Code Red II, which is another worm that also hacked into the system. The remaining twelve entries were attempted exploits of IIS vulnerabilities.

When analyzing the log entries to the JTFO website, many of the hits consisted of the Nimda entries, as it attempted to find vulnerabilities in the system. The graph on Figure 7 below exhibits the number of Nimda attacks occurring on a particular date and Figure 8 on the next page shows the number of attacks from a particular IP address. As it can be determined from the graphs, most of the attacks came on the 10th of February. Figure 9 on page 59 provides the number of times each form of the Code Red worm was used. There were a total of 32 Nimda Worms with the complete signature discovered in this project, as they had all sixteen, successive entries. There were other Nimda worms that were incomplete as they did not have the complete signature, but nevertheless, displayed the attempt to hack into the system.

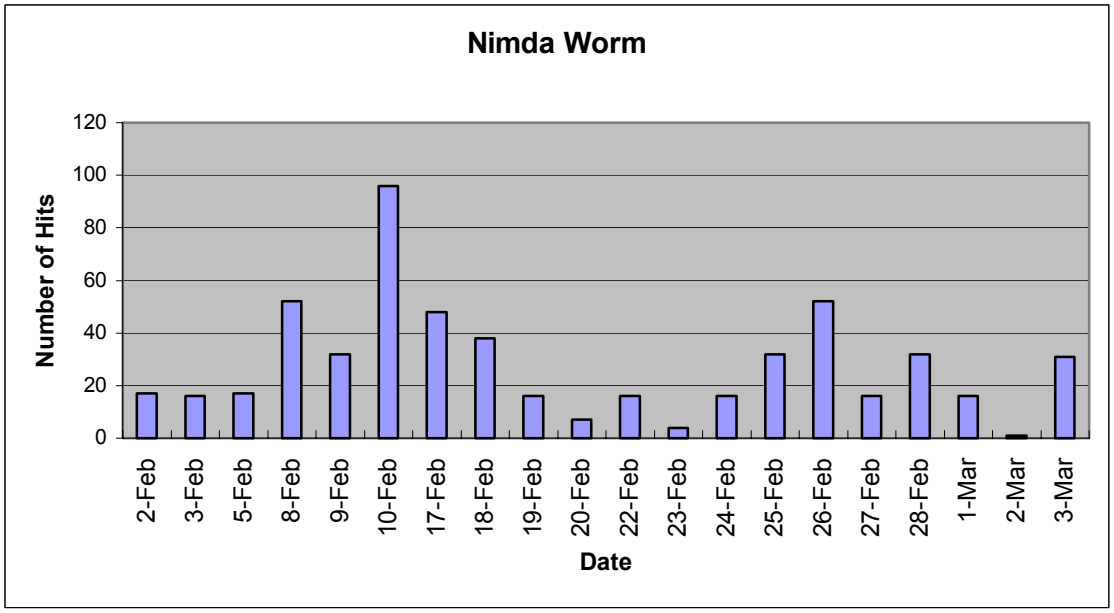

Figure 7. Numbers of Nimda Worm Hits Each Day During the Project.

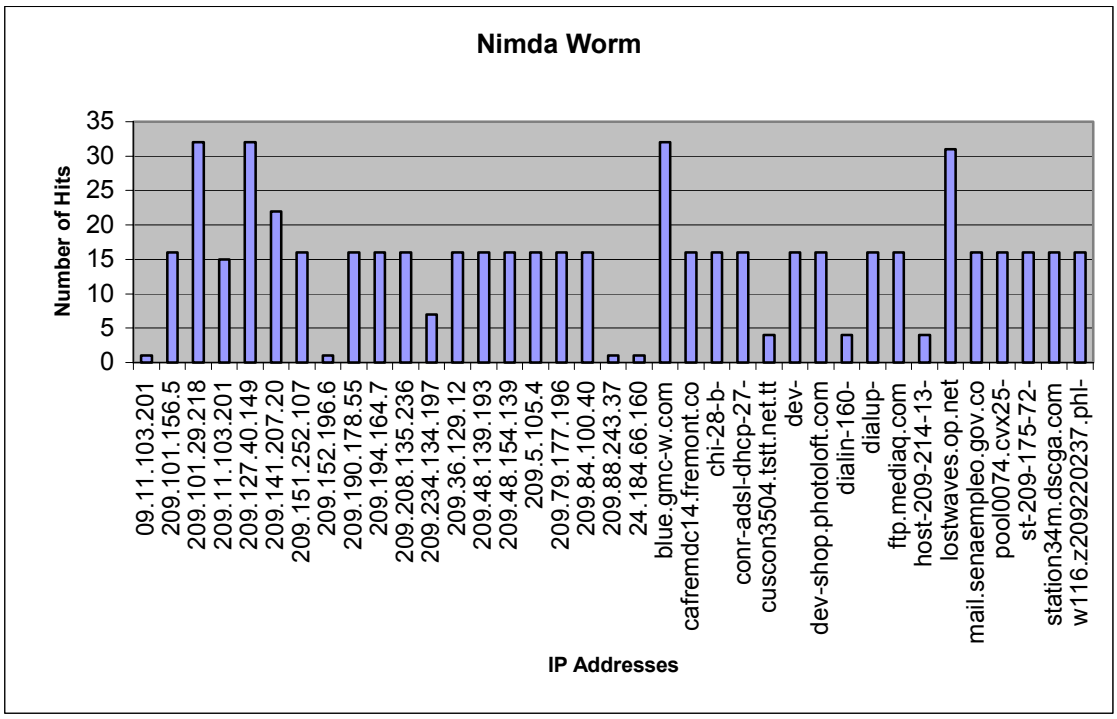

Figure 8. Source IP Addresses of the Nimda Hits, and Their Frequencies.

Possible Nimda Attacks	Attacks
/scripts/root.exe?/c+dir	8
/MSADC/root.exe?/c+dir	7
/c/winnt/system32/cmd.exe?/c+dir	7
/d/winnt/system32/cmd.exe?/c+dir	7
/_mem_bin/..%255c../..%255c../..%255c../winnt/syst	
/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir	2
/_vti_bin/..%255c../..%255c../..%255c../winnt/syst	
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir	2
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c	
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir	1
/scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir	4
/scripts/..%%35c../winnt/system32/cmd.exe?/c+dir	4
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+d	
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir	2
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir	4
/scripts/..%255c../winnt/system32/cmd.exe?/c+dir	4
/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir	3
/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir”	
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir	4
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir	3
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir	4

Figure 9. Nimda Versions Scripts and their Frequency of Use Against the JTFO Server.

2. Other Types of Server Attacks

In general, web servers on the Internet are accessible through several ports. Websites are available through the HTTP (Hypertext Transfer Protocol) port. Other ports include the FTP (File Transfer Protocol) server, which is used to exchange files with other computer systems, and the telnet server, which allows users to remotely log into the computer. It is important to note that the JTFO web server only utilized the HTTP server port. No data or files were placed on the FTP server. Authorized users of the JTFO computer did not access the telnet server, and a very limited number of usernames and passwords existed for remote logins. The analysis of the server side attacks will show activity on these alternate ports, immediately indicating unauthorized use of the system. It was normally quite easy to distinguish unauthorized use, since very few people had legitimate access to the system.

a. Telnet Attacks

The most common attacks on the JTFO web server were targeted at the telnet component, *JTFO.telnet.* The actual motive for targeting the telnet server can vary among different intruders. Some may be trying to remotely log into the system, in an attempt to gain unauthorized access to the entire computer. Telnet intruders may also wish to simply block access to the server by use of a Denial-of-Service (DoS) attack. These attacks aim to inhibit the target server from performing its stated function.

b. FTP Attacks

A significant number of attacks targeted the *JTFO.ftp* server. As with telnet attacks, two main motives exist for targeting the FTP server. One is to use the FTP server for its designed function: to gain access to assorted files placed on the FTP server of the targeted system. Intruders may have been attempting to acquire information through the *JTFO.ftp* server. This would have proved to be impossible, since the FTP component of the JTFO server was not used. The second motive for attacking the FTP server was also a DoS attack. Like the telnet server, the FTP server is subject to such attacks, since intruders may find it helpful to their cause if these servers are unavailable to their authorized users.

c. NetBios Attacks

Several attempts to log into the JTFO server were attempted through the netBios server. These attacks are curiously interesting since this style of attack was doomed to fail against the JTFO server. NetBios attackers were attempting to access the server through Port 137, or the netBios server. This port is used for communication between computers within a Local Area Network (LAN). These attackers tried to enter the JTFO system, only to find that the netBios path was blocked. This was due to the configuration of the RIDLR network to which the JTFO server belonged. The firewall protecting the RIDLR and the rest of the Naval Postgraduate School network prevented all attempts to log in to the netBios server. A specific netBios attacker will be described, and a more extensive analysis of this style will be provided later in this chapter.

D. CHRONOLOGY OF ATTACKS

The notable attacks that targeted the JTFO computer system are described below. In addition to these, numerous day-to-day attacks were logged within the JTFO system. The sources of these attacks normally appeared one time, not to be seen again for the duration of the experiment. As for the main attacks, they are separated into three main categories: worms, unauthorized web hits, and the various server-side attacks. The server-side attacks were made up of the previously discussed targets: the telnet, FTP, and netBios servers. Each of the three categories are included in the following chronological discussion.

1. Worm Attacks 08-10 February 2002

There appeared to be an attack from 08-10 February. The 8th and 10th received the most attacks from both the Code Red and Nimda Worms. There was very little activity from the two worms before the 8th of February. There was a single Nimda Worm attack on the 2nd, 3rd, and 5th of February. In addition, there was one trace of a Code Red worm on the 7th, but the day was filled entirely with one or several individuals going to different .htm pages on the site and the downloading of images that accompany this action. The intensity quickly picked up on the 8th of February, which marked the beginning of the Winter Olympic Games with the introduction of the Opening Ceremonies. The first day of the Olympics would be an ideal time to attack, and as a result, the 8th is an excellent day to examine. That day consisted of 58 entries to the JTFO website from nine distinct IP addresses. However, all the entries were traces of

either the Code Red or Nimda Worm. There was no one entering the website that day to look for information. Instead, it was a total computer attack that consisted of five Code Red Worms, three Nimda Worms with their complete signatures, and one Nimda Worm with only the first four entries, indicating the attempted use of the back door left by the Code Red. The next day, the 9th, was the same but to a lesser extent. Again no files or web pages were looked at, but instead there were other worm attacks: two complete Nimda worms and two Code Red worms. During the two days the Code Red started the attack, which was followed by the Nimda Worm. The intent was for the Nimda to take advantage of the backdoor left by the Code Red Worm. The 10th of February received the most hits to the JTFO website during the length of this project. This day consisted of 11 worm attacks: five Code Red and six Nimda worms with their complete signatures. Two of the Nimda attacks came from the same IP address with a seven-minute interval between them. In addition, there was a Code Red attack that came from the same IP address on the 9th and the 10th. This shows the attacks from the two days were possibly connected. Some individual or group attempted to attack the site on consecutive days. However, there was also a Code Red attack from the same IP address on the 5th and the 10th. This could show the attacks are indiscriminate and unrelated. After the 10th the worm attack came to an end, as there were no worm attacks on during 11-13 February.

2. 09 February 2002

The first major server attack occurred on 09 February. The Apache server logs, which only recorded activity on the HTTP server, indicated an above average number of website hits: 166, compared to an average daily number of 40. The SHADOW logs also indicated vastly more activity than normal, with the number of entries almost six times higher than the average daily figure. A total of 31,569 exchanges took place on this day, with 96% of them resulting from users not affiliated with the DoD. Taking a closer look at the entries, the vast majority of exchanges with the web server came from a small group of four IP addresses. Approximately 35% of these non-DoD hits originated from a telnet server or were directed to the *JTFO.telnet* server, possibly indicating repeated attempts to log into the JTFO system. It is not known for certain whether any of these attempts were successful, although there is no evidence to suggest that this is so. Another equally significant portion of the attack targeted the *JTFO.ftp* server, by repeatedly

attempting to communicate with the server. The remainder of the log entries involved the *JTFO.netbios* server, which normally indicates repeated attempts to gain entry the web server. The number of netBios requests totaled nearly 10,000 for this single day.

The data collected from the logs on 09 February indicate a style of computer network attack known as distributed denial-of-service (DoS) attacks. The objective of this attack is to slow the targeted system to the point where it is inhibited in or prevented from performing its stated functions. DoS attacks repeatedly request the service of the target system, soaking up the target's processing time and its bandwidth. This can be done in a variety of ways, the simplest being with ping requests. In the case of 09 February, the attack only degraded the reaction time of the server. If any web-surfer was attempting to view www.jtfo.org, the download time was likely to have been extremely slow. The ability of the JTFO server to accommodate web requests was not affected on this day.

3. 10 February 2002

a. Website Attack

The 10th of February saw an individual trying to look for information on the website at different times of the day. The IP address almost remained the same with a slight variance in the domain name of the Digital Subscriber Line Internet Service. It appears that the different IP addresses came from the same person or group. The 10th of February had the profile of an Internet terrorist. There appeared to be a single individual that day looking for information on the website. There were six different IP addresses that were not from worms, but individuals entering the site in order to look at it. The domain name came from the same Digital Subscriber Line Internet Service, which suggest a single individual or members from the same group accessed the site. The times in which the individuals entered to look at the site were at the following times: 0010, 0222, 1431, 2101, 2102, and 2135 PST. One of the IP address, which began at 2102, attained a large volume of information with the access of the index, news, and responsibilities .htm pages and in the restricted areas looked at three JTFO categories: administrative, physical security, and training. The individual clicked on the three categories of the restricted section but did not successfully give the correct password or hack into the restricted area. The log entries on the 10th suggest four other IP addresses

did not go past the first page of the site, which has a DoD warning to alert the used that the site is for official use only. The fifth IP address did go past the first page but left after entering the index or home page of the website.

b. Server Attack

The second significant DoS attack on the server also occurred on 10 February. The previous day's activity may be linked to this day's attack because the characteristics of the two are quite similar. However, since the log entries of 10 February originate from a different set of IP addresses, these two days will be treated as separate attacks. SHADOW logged over 44,000 exchanges on 10 February, with 98% resulting from non-DoD users. Spread out over the course of 24 hours, this equates to one exchange every two seconds, with the majority occurring before 0800 PST.

Whoever mounted this attack on 10 February used very similar techniques as those of the day before. The vast majority of hits involved the *JTFO.ftp* server, once again indicating a DoS attack via requests to the FTP server. However, the logs indicated something that did not occur the day before: nearly one-quarter of the log entries showed that the JTFO system was inaccessible at that particular time. This suggests that the DoS attack was successful on this day; it prevented the server from carrying out its normal functions. This also carried over to the website server, as several attempts to access the website via a separate computer all failed.

4. 12 February 2002

On 12 February there were zero attacks from either of the Nimda or Code Red worms. However, there was a single IP address that entered the website that day. That IP address contributed to 25 hits to the website and only appeared on the 12th of February during this project. The individual attempted to enter the restricted areas of the website and looked at the categories of operations, logistics, physical security, training, and administrative. There was no successful entry into the restricted area but clearly there was an attempt to access five categories of the restricted area. The rest of the hits on that day came from the downloading of images that comes with viewing the DoD warning page and JTFO homepage.

5. 13 February 2002

The third and final major DoS attack on the JTFO server took place a few days later, on 13 February. This was the largest attack, with over 55,000 exchanges logged by SHADOW. The percentage of non-DoD exchanges remained true to the other attacks, at 96%, indicating that this was definitely another DoS-type attack on the server. However, this attack displayed slightly different characteristics from the previous two. First of all, it originated from yet another smaller set of IP addresses. Virtually all of the entries associated with this attack came from only three systems. Secondly, each of these three systems performed an equal number of exchanges (or attempted exchanges) with the JTFO server. The *JTFO.ftp* server was once again the main target, although it was notably the only target. No other attempts were made to access other servers, or to send other ping requests to the JTFO server. Throughout the day, there were a significant number of SHADOW entries indicating that the JTFO server was inaccessible, indicating a successful DoS attack.

6. Worm Attacks 17-19 February 2002

The worm attacks of 17-19 February followed a similar pattern to the ones that occurred from the 8th through the 10th. Little activity was experienced prior to the 17th. There was relatively little activity during 14-16 February, with only six Code Red Worms during those three days. The IP addresses that entered the website from 14-16 February were accounted for as Naval Postgraduate School students working on the site from their personal homes. After the 10th there was no Nimda Worms until the 17th. The website encountered large amounts of worm attacks from 17-19 February. During that period only the Code Red and Nimda worms entered the website. The 17th experienced three Nimda with complete signatures and one Code Red. The interesting thing about the 17th was two Nimda Worm attacks came from the same IP address with a seven-minute interval between the two. This pattern was also displayed on 10 February. Furthermore, one of the Nimda Worms had an incomplete signature with only 15 entries but received the 16th entry from a different IP address. The two IP addresses that made the complete Nimda Worm came from the same corporation. The 18th was also unique, as one of the IP addresses with the Nimda Worm would be repeated again on the 25th. The 19th encountered two separate Code Red Worms to start the day with a Nimda worm coming later in the day. After the 19th there was little activity from worms for a couple of days.

7. 20 February 2002

The 20th of February the same pattern as 10 February. Like the 10th, there was an attack in the form of a Nimda Worm with an incomplete signature. More importantly someone tried to access the same type of information from ten days prior. On 10 February someone tried to access three categories within the restricted area: administrative, physical security, and training. On the 20th someone tried to look at the same three categories in the exact order. The user was unsuccessful in entering the restricted area. In addition, on both days the "Responsibilities.htm" page was accessed. The only difference between the two days was the 20th had two distinct IP addresses look at the information.

8. Worm Attacks After 20 February 2002

After 20 February the worm attacks were sporadic. There were no distinct patterns and the last trace of a Code Red Worm was on the 19th. One link between worms showed the 18th and 25th of February logging a Nimda Worm attack from the same IP address. This validates the argument that the attacks from computer worms were random. According to Figure 7, there was a Nimda worm attack on each day between the 22 February and 03 March. The site still received worm attacks after the Olympics were over on the 24th, which reaffirms the site was randomly chosen and attacked. Two of the largest Nimda attacks occurred on 08 and 26 February. On the 26th, there were attacks from five different IP addresses. Two of the Nimda worms had incomplete signatures with one having a single entry while the other had only four entries. This means that the incomplete Nimda worms were looking for a backdoor left by the Code Red Worm.

9. 25 February 2002

The day after the closing ceremonies of the Olympics someone looked at every .htm page (index, feedback, search, news, links, responsibilities) on the website and every category of the restricted area (administrative, comptroller, logistics, plans, physical security, temporary facilities, and training). The individual appeared to be a capable hacker, as he or she entered and looked around the restricted area. Throughout the length of this project, the 25th was the only time someone gained access into the restricted site. However, none of the dummy files were opened. The user was able to bypass the DoD warning page and did not download any of the images that occur when accessing an .htm

page. This suggests the user had some computer knowledge as the Apache server only logged 13 entries to the site, which were the five.htm pages and eight categories in the restricted area. This validates the idea that the user was looking for information.

E. PATTERNS AMONG THE ATTACKS

1. Worms

a. Indiscriminate Use of Worms

All the attacks from the Nimda and Code Red worms marked the profile of a *script kiddie* methodology. These individuals randomly select targets and eventually probe a system and network. As stated earlier, with all the available tools and the countless number of people using the Internet, it becomes only a matter of time before a system or network is probed. The purposes of these worms were to compromise machines so they could attack other machines on the Internet. This would bring damage to system and document files or slow down the network. One of the motives stated earlier of the Blackhat community was the desire to implement a distributed denial of service. The use of computer worms meets this objective, as they allow a single hacker to control thousands of systems with the potential to control more in order to coordinate a distributed denial of service attack. The more compromised systems mean a more powerful attack. Another motive that may suggest the *script kiddie* methodology was the worms were used to hide the hacker's source and identity. Again random systems were compromised in a series of hops, increasing the difficulty to trace a hacker. Consequently, the JTFO website may not have been a specific target but only a random one. Computer worms by nature are self-replicating. The Code Red Worm randomly chooses IP addresses to attack, and the Nimda Worm emails itself to addresses found in infected message boxes in order to spread.

Hence, The JTFO website may have been indiscriminately attacked for the sake of adding systems to the control of Blackhats. There were not many patterns suggesting the worms were directed at the website. The attacks from the Nimda Worm were sporadic and came from distinct IP addresses. Also the last trace of a Nimda Worm was on 19 February. Traces of the Code Red Worms were discovered during the entire period of the project. The evidence to suggest the worms were aimed at the website was weak at best.

b. Discriminate Use of Worms

Another possible explanation with all the hits to the website from 08 – 10 and 17 –20 February is the attempt to compromise the system with the use of two types of worms. The discriminate use of worms can imply either a regular hacker from the Blackhat community or Internet terrorists. A hacker may have planted or directed the worms at the website in hopes of compromising the system and taking control of it. Another possibility is Internet terrorist could have had the computer savvy to discriminately use the worms. This would provide them with the privilege to enter the restricted area and attain its files. On the 8th and 9th the website experienced only attacks from worms. On the 10th they began to look for information and entered the site only briefly to see if the site was compromised. This may explain why four of the six different IP addresses did not go beyond the DoD warning page. This suggests the profile of Internet terrorists with hacking capabilities, as they hacked into the JTFO website in order to attain information to support their actions. On that day they looked at the "Responsibilities" .htm page and three specific categories in the restricted area: personnel, physical security, and training. This information would be helpful in the planning and support of a terrorist plan, as they try to research background information and vulnerabilities. The events from the 17th through the 20th could have been the same thing. There were only worm attacks from 17 – 19 February with no one entering the site to look for information. Finally, on the 20th someone entered the site from two distinct IP addresses in order to look at the same exact information in the same order as on the 10th. That individual allowed ten days to pass in order to look for new or any changes to the existing information for the purpose of developing a plan with the latest resources. That person could have also directed worms at the site in order to gain control of it, which includes access into the restricted files. There were some evidence supporting the concept of discriminately using the worms at the JTFO website. There were several Nimda Worm attacks that come from the same IP address and occurred on different days. On the 10th and 17th there were two Nimda attacks with their complete signature that came from the same IP address. There was a seven-minute interval between the two worms on each of those days.

c. Looking for Information

Another scenario to consider is the attacks from the worms and the accessing of information could be unrelated. The two worms by their very nature are indiscriminate. As stated earlier, the Code Red Worm randomly chooses an IP address to attack and leaves a back door for the Nimda Worm. Worms from other compromised systems randomly selected the JTFO website in order to compromise it. The implementation of these worms meets the *script kiddie* profile of trying to compromise as many systems as possible in order to degrade performance or cause a distributed denial-of-service attacks. Meanwhile, someone not associated with the worms looked for information on the JTFO website, particularly the 10th, 12th, 20th, and 25th of February. It was merely coincidence that someone entered the site to look for information on the same day of a worm attack. Those looking for information on the website and the worm attacks were two completely different entities with each having their own potential profile.

2. Denial-of-Service Attacks

When comparing the three major attacks on the JTFO server, several conclusions can be made concerning their nature and significance to this study. As stated before, the intent of this project, and any honeypot, is for the system to be attacked, penetrated, and compromised in order to get a close look at the intruders. The three days of DoS attacks provided that look. Characteristics of the attacks, as well as the people who masterminded them, are hidden within the data logs.

With limited address tracing capabilities, it is not known for certain if the same person or group launched these attacks. The SHADOW records give several clues that may lead to conclusions about the profiles of these attackers. The first two attacks, 09-10 February, both originated from small, separate groups of IP addresses. Eight unique addresses appeared on 09 February; six appeared on the 10th. Although the two groups had no common addresses, they all originated from the same few locations. The exact addresses were different, but 09 and 10 February both produced attackers from the same regional ISP based in Europe and another ISP located in North Carolina. A small Colorado company computer[26] also appeared on the 9th, while an address from a small

26 The small size of the company is concluded from its Class C IP address. Class C addresses are assigned to networks that can support only 254 computers, while Class A and Class B addresses support significantly more computers.

Colorado-based ISP showed up on the 10th. The style of DoS attacks remained the same during the 9th and 10th. A mixed bag of FTP and netBios server attacks occurred on both days, along with a conspicuous and significant telnet attack taking place on the first day.

The DoS attack on 13 February was characteristically different from the previous two attacks. Most visibly, it did not occur on consecutive days with the others. It exclusively targeted the *JTFO.ftp* server, whereas the other two also aimed for other component servers on the JTFO system. A set of only three separate IP addresses constituted the DoS attack, and the locations of these addresses were quite different from those of the previous days. The addresses originated from[27]:

- A regional ISP based in Colorado, different from both Colorado-based systems that appeared on 10 February.
- Another regional ISP based in Texas.
- A Nevada-based small company's computer system.

In addition, nearly 53,000 recorded data exchanges on the 13th were determined not to be DoD-affiliated. The group of exchanges associated with the DoS attack numbered about 52,500, and these were equally divided among the three IP addresses.

3. Repeat Intruders

There were several instances where suspected DoS attackers of 09-10 and 13 February accessed the JTFO web server on other days. These visits were much shorter, in time and amount of activity, than the major attacks. However, examining these shorter attacks is beneficial when determining the motives and profiles of these intruders. The same intruder who mounted the attack on the *JTFO.telnet* server on 10 February appeared on three previous days: 01, 03, and 06 February. On all three occasions, the intruder followed a similar plan, by targeting the telnet server. On the first of these days, the attack was a brief three minutes long, consisting of 100 attempted exchanges with the telnet server. On 03 February, the attack lasted the same three minutes long, but involved over 300 exchanges. The third day, 06 February, involved something more. The attacker pinged the JTFO server for several minutes before mounting a familiar telnet attack several hours later. This particular telnet attack included over 1000 hits in a period of 20 minutes; much larger than the two earlier days, but not nearly as large as the major attack

27 The names of the computer systems or their respective ISPs will not be disclosed in this work.

of 09 February. Interestingly, the telnet attacker returned again on 20 February to conduct its familiar work. A total of 250 exchanges with the *JTFO.telnet* server took place on this day. Once again, this attack was much smaller than the one on the 9th.

Another attacker of 09-10 February appeared again a few days later on the 14th. This particular intruder targeted the *JTFO.ftp* server, in the same manner as on 09-10 February. The attack on the 14th was in the same style as the larger, previous one. The attacker flooded the *JTFO.ftp* server with entries during an extremely brief period of only a few seconds. The earlier attack was conducted similarly, by employing short bursts of attacks for a few seconds throughout the day. The first attack, however, was coordinated in such a way that the attack was continuous. The IP address representing this attacker was one of many originating from the same European ISP. On the 14th only this one particular IP address appeared; on the 10th, two other IP addresses from the same source were used. Each of these IP addresses shared the work of flooding the JTFO server in a DoS attack.

There was also an IP address appearing on 13 February that returned the next day. Attacking in the same fashion each time, this intruder used periodic short bursts over a long period to hamper the *JTFO.ftp* server. The attack lasted throughout much of the 14th, but the volume was much less than on the previous day, totaling only 130 attempted exchanges (compared with nearly 10,000 from that IP address on the 13th.)

Other IP addresses appeared multiple times throughout the life of the JTFO website. One address originating from a North Carolina-based ISP appeared every day during the first half of the experiment. From 01 through 16 February (except for the 6th), the SHADOW logs indicated this address in a few entries each day, including the three days of DoS attacks. The pattern followed by this intruder was identical each day; the intruder appeared for a few seconds to make contact with the *JTFO.netBios* server, and was limited to three exchanges each day. What follows is a sample of this pattern, taken from the SHADOW logs of 07 February[28]:

> 2/7/2002 4:35:56 AM 208.XXX.XX.XXX.netbios-ns > JTFO.netbios-ns:
> >>> NBT UDP Pkt(137): Query; Req; UNICAST

28 The IP address has been hidden in this sample, although on each day and in each entry it is the same.

2/7/2002 4:35:57 AM 208.XXX.XX.XXX.netbios-ns > JTFO.netbios-ns:
>> NBT UDP Pkt(137): Query; Req; UNICAST

2/7/2002 4:35:59 AM 208.XXX.XX.XXX.netbios-ns > JTFO.netbios-ns:
>>> NBT UDP Pkt(137): Query, Req; UNICAST

The intruder always targeted the netBios server, and also appeared around the same hour each day. Other IP addresses from this particular ISP also appeared on different days, conducting brief attacks on the JTFO server. These were all isolated occurrences, with the only significance being on their source ISP.

F. SUMMARY

The JTFO web server attracted numerous intruders who demonstrated many styles of web server attacks that were useful in this research. A major source of data came from the major Denial-of-Service (DoS) attacks that occurred on 09-10 and 13 February. The data collected from these attacks provided a basis upon which to develop profiles of the responsible attackers. Other sources of data came from day-to-day attacks, some of which were made up of isolated attacks by people who apparently targeted the JTFO server only one time. Another principle data source resulted from hackers who returned once or several times to mount attacks against the JTFO server. It is from these repeat attacks that extensive profiles were generated in order to understand whether the Internet terrorists and various types of hackers were interested in the material on the web server.

This experimental web server attracted many types of hackers. The so-called telnet attacker provides an example of a self-motivated, part-time hacker who may be looking for a joyride through cyberspace or perhaps just a chance to show off for his friends. The European FTP attackers described in Section E appear to be a small group of hackers with a bit more experience. These FTP attackers were likely working as a group, possibly with additional plans of attack through other media, maybe even physical destruction. The final group described in Section E was the attackers who targeted the netBios ports of the JTFO server. Few solid conclusions can be made about any of the individuals or groups, although like all attackers described in this entire chapter, they were likely to be knowledgeable computer users.

The most eye-opening results from the JTFO experiment came from the DoS attacks that took place during mid-February. These attacks showed that there were

groups who specifically targeted the JTFO web server as part of a larger, complex plan of attack. The vast amounts of data on these days provided a look into the minds of these attackers. With certainty, it is concluded that all the people who conducted repeat attacks on the JTFO server had at least a moderate degree of computer knowledge. The style and intensity of the individual DoS attacks suggest that the hackers were experienced in this field; they knew the vulnerabilities and inner workings of a system like the JTFO computer. Their cyberspace habits were on display, which helped to develop extensive characterizations of the hackers in the hope that effective law enforcement actions could follow.

However, the focus of the project was not on the various types of hackers but Internet terrorists. It was acknowledged before the project that computer hackers would enter the system. As a result their profiles were characterized in order to distinguish them from the real threats, Internet terrorists. The attacks to the web server met the profiles of computer hackers, but there were some hits to the JTFO website that suggested Internet terrorists. Events on the 10th, 20th, and 25th met the profile of the Internet terrorist, as someone was trying to access information on the website. The events on those dates also suggested the potential Internet terrorists possessed computer knowledge and used them to access the information.

VII. CONCLUSIONS

A. REVIEW

The Winter Olympics provided a grand stage for criminals and terrorists to make a destructive and deadly statement with its large television coverage, numerous spectators, and involvement of over 80 nations. At the same time it offered an ideal setting to conduct experiments in deception. The purpose of this thesis was to deploy tactical deception via a website on a public domain in order to determine the trends and profiles of those associated with terrorist activity. Joint Publication 3-58, *Joint Doctrine for Military Deception*, provides the guidelines needed to create a successful deception and influence those that entered the site, who could be potential terrorists, with one of the most trusted monitors, the Internet. To follow these principles ensures the website maintains its deception and appear to be an actual site of the JTFO.

The **focus** of the project was aimed at Internet terrorists. The deception was aimed at the decision makers of Internet terrorists, and hopefully they would perform the desired actions (i.e., revealing their patterns, showing what type of information they looked at). During this project, the relationship between terrorism and the Internet was being evaluated along with hackers and their introduction into the system. With the rise of information and computers, the Internet has become a valuable tool, which has its vulnerabilities. Terrorists or anyone else can exploit these vulnerabilities, and this thesis explored this idea through a honeypot. The target can rarely be reached without going through some form of information processing system: the intelligence agency. Within the intelligence agency there are channel monitors, gatekeepers, and decision maker, and the deceiver must convince all three levels of the validity of the false information to achieve success. The Internet terrorists that enter the website are channel monitors conducting research. In this project the focus is to deceive them, and through them the decision maker can be reached.

The **objective** of the deception was to cause those to enter the JTFO website to believe they were in a site that acted as a supporting tool for the Joint Task Force Olympics. Many efforts were made to make the website appear authentic and attractive

to enter, especially the restricted area. The information (directories, files, documents) that enticed the interests of an individual or individuals, who may be potential terrorists, to seek access into the website were administrative, physical security, and training. On the days in which someone attempted or did access the restricted areas these three categories were always accessed. The types of information contained within these topics proved to be most attractive to the Internet terrorists that the project targeted. The goal of the research was to discover which ways they accessed the information so that future deception can guard against the compromise of any sensitive material on the Web.

Centralized control in this project was necessary for keeping accurate synchronization of information with other agencies. The website included information that needed to coincide with any facts displayed on other websites such as the actual JTFO and UOPSC, in order to preserve the bodyguard of lies created by the deception. In this study, those participating in this research were not given step-by-step instructions; they had the flexibility to create and manage the website, as long as the site adhered to the objectives of the research. Because of this, the website had to be periodically checked by the JTFO in order to preserve its accuracy.

The **security** for this project was most vulnerable with communication within the project managers. Communication by e-mail was kept to a minimum in order to prevent compromise of the project's true objectives. All potentially compromising communication was done in person within the small central group that controlled this experiment. Security within the website was not strictly adhered to, since the goal was not to implement a secure site. Instead, the hope was for an individual or a group to enter the site in order to compare them with a list of known profiles. Dummy files and subdirectories were created from the actual JTFO directory to ensure those that entered did not realize they were being misled.

This project was inhibited by a short amount of time. **Time** is needed to make the web design convincing. More time was needed in order to put the website online earlier, giving potential terrorists, who are researching information and acting as the intelligence system, an opportunity to come across the website before the start of the Olympics. Through them the enemy decision maker can be reached, as they could collect, analyze,

and report to the enemy decision maker, who then could react accordingly. After some time the deceiver detects and responds to the actions of the decision maker. The JTFO website was available on the public Internet for only four weeks, leaving the possibility of several mistakes and inconsistencies. This weakness is further discussed under Section C of this chapter.

The deception plan must be fully **integrated** with the operational plan it is supporting. The operational plan was to provide support to the Winter Olympic Games. The website included factual material from the JTFO and its computer system, adding to the site's credibility. Initially, the website was designed to be an actual component of the JTFO information campaign. However, the site never actually fulfilled this role, but instead, was limited to carrying out its research tasks. The role of the website decreased and became an independent study with the support of the JTFO in Salt Lake City, as the Olympics was approaching. This did not affect the deception scheme other than to reduce the publicity generated for the website.

B. EVALUATION

When evaluating the success of this project, measures of effectiveness (MOEs) are needed to gauge it. The MOEs used here for evaluating are:

- **The number of hits on the server and the website.** The JTFO computer received a limited number of hits throughout the duration of the project. However, this alone cannot gauge the effectiveness of the deception plan. The number of hits was a direct result of the lack of publicity that the website received. This will be further discussed in Section C.
- **The numbers of different Internet terrorists, intruders, and other hackers.** Although the true identities of every visitor to the JTFO computer were not established, the site attracted visitors of all kinds. Judging from the patterns displayed in the access logs for the website and the server, several types of hackers, including potential Internet terrorists, visited the site and attacked the system. The types of attacks, frequency of hits, target servers of the hits, and sources of the IP addresses all suggest that different types of visitors showed up on the JTFO computer.
- **How often attackers returned to the JTFO computer for repeat visits.** There were several cases where repeat attackers appeared on the JTFO computer. Most of these repeat attackers targeted the server side of the computer, and were described in detail in the previous chapter.
- **How often each element of the deceptive website was accessed.** This was the one area in which the JTFO project can be deemed unsuccessful.

> Very few cases showed JTFO website visitors scouring through each page on the site. Even fewer visitors attempted to access the restricted areas that made up the main deceptive aspects of the website. This suggests that the JTFO website simply was not convincing enough to attract any persons looking for information.

Despite the limited hits, the JTFO experiment generated a large amount of data that displayed the characteristics and techniques of the hackers and potential Internet terrorists that entered site. This is the ultimate gauge of the success of this project.

This project looked to answer whether or not this style of deception scheme is feasible for future Internet deception operations. The area that the proved most successful in the JTFO project was the server side attacks. Although many factors helped to reduce the amount of exposure, publicity, and material placed on the web server, the system was subject to the actions of a number of intruders and hackers. As stated before, the bulk of the network attacks targeted against the JTFO server came in the form of Denial-of-Service (DoS) attacks. The motive for these attacks is to degrade the services of the JTFO computer, to prevent it from carrying out its purpose. This suggests that the people behind these attacks considered it necessary to disable the JTFO and its computer system. As a result, it is concluded that Internet deception and research honeypots are a very effective means of gaining information on the types of attackers that target Internet computers. The amount of data generated by this project supports this conclusion. The characterizations and profiles developed from this data will be very helpful in inhibiting the actions of Internet terrorists. On the flip side, the failure of the website deception does not necessarily discount it as a viable method of deception. Several factors outside of the deception plan inhibited its effectiveness. Improvements on future plans may prove that other operations of this type may indeed be successful.

C. LESSONS LEARNED

1. Time

The limiting factor throughout the entire project was time. Ideally, a scheme of this type would be developed over the course of several months in order to maximize the benefits of a detailed deception plan. This would allow for more careful initial planning of the contents of the website, and also for refining the contents during the experiment in

order to tailor the deceptive aspects of the website more closely to the target. Several actions could have been conducted differently had the project been set aside more time.

a. Increase Material on the Website

The amount of material on the website should have been increased. The entire site was composed of only eight web pages and a directory containing the dummy files. This was hardly enough to encourage extensive exploration by lawful and unlawful web surfers. More creative public pages would increase the curiosity of site visitors and perhaps encourage them to look further into the JTFO site as well as other Olympic-related sites. Adding more material to the restricted site would be beneficial in the long run as well. Any intruder who viewed the restricted areas repeated times would not have seen any additions or changes to the files. This degrades the credibility of the website being an actual operational tool of the JTFO.

b. Utilize Other Components of the Server

The computer system was virtually void of material other than an HTTP website. Documents and files could have been added to the FTP server in order to research intruder who gain access to it. The *JTFO.telnet* server may also have provided some valuable insight had it been accessible during the experiment. If these servers were made more available to unauthorized users, more data would have been generated to enhance the effectiveness of the research aspect of the scheme.

2. Publicity

In order for a deception to be successful, the target must be exposed to it. The focus of the deception scheme is on this target, and its objective is to influence the actions of that target. Without adequate exposure and publicity, the effectiveness of the scheme is degraded. This site suffered from a lack of adequate exposure. The project carried on without links from other websites to the JTFO site, and without appearing on any major Internet search engines. For future operations, advertisement is needed to gain this necessary exposure. It is recommended to post links on other agencies' websites (i.e. UOPSC, FBI, USJFCOM, other Olympics-related sites). In addition, the JTFO site should be submitted earlier to search engines (i.e., Google, Yahoo!, or AltaVista) so that it will be readily available when the deception scheme is launched. Once again, it comes down to time; a deception scheme needs time to properly unfold.

3. Link With Law Enforcement Agencies

Earlier in this thesis, it was stated that deception is not in itself a complete military operation. It will not solve all computer security problems or defend against all Internet terrorists. Deception must be integrated with other operations. This can effectively be done by communicating and synchronizing plans with the Salt Lake City-based JTFO or other agencies with more exposure than the JTFO experiment.

Although there was no trouble logging user activity and IP addresses, only the location of a particular user's system was identified. A major shortfall in the project was the inability to trace connections to one single user. The solution to the trace problem lies in tracing the connections while they are still active. In the future it is suggested that this project should be coordinated with other law enforcement agencies such as the FBI. The identity of the users could then be determined rather than simply focusing on the behaviors and patterns.

4. Actively Monitor Intruders

Most of the research in this project was conducted after the Olympics had concluded and the website was taken offline. After the website was taken offline, conclusions were drawn from the data logs with patterns being discovered. For future purposes it is beneficial to actively monitor intruders and refine the deception scheme in order to target the intruder more closely. This is essentially a form of feedback from the target. As discussed earlier in Chapter II, feedback is a requirement for success in the deception process. It is the key to developing profiles of the target, which aid in refining the focus element of the deception scheme. When the focus is narrowed through feedback, the deceptive elements of the scheme can be pointed straight at the desired target. In the case of the JTFO experiment, time limited the ability to actively pursue intruders, as most valuable time was spent managing the network aspects of the server instead of the deception target.

D. SUMMARY

The JTFO experiment shows that web deception is an area within Information Operations that cannot be ignored. The goal of the project was to develop a research honeypot web server, while placing enticing material on the website. Intruders were curious to access the JTFO server and show their hands to the deception planners. This

was successful; the JTFO web server drew several intruders. There were cases of DoS attacks, worm attacks, unauthorized website hits, and attempts to remotely log into the system.

With further refinement, the field of web deception will be a valuable tool to future Information Operations. Future possibilities include using productive honeypots to expose false material to the target and protect sensitive material from them as well. By exposing false material (i.e. creating a false reality), future web deception plans may play a role in preventing terrorist attacks and other criminal acts. At the same time, sensitive factual information can be protected from unauthorized use. All of these possibilities can be accomplished using any combination of the deceptive tools discussed in this study.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Beach, Lee Roy. et al. "Assessing Human Judgment: Has It Been Done, Can It Be Done, Should It Be Done?" *Judgmental Forecasting.* Ed. George Wright and Peter Ayton. New York: John Wiley & Sons, 1987.

Bowman, Steve and Barel,Helit. "Weapons of Mass Destruction – the Terrorist Threat" 1999. http://news.findlaw.com/cnn/docs/crs/wpnsmssdst120899.pdf (20 April 2002).

Breuer, William B. *Hoodwinking Hitler: The Normandy Deception.* Westport: Praeger/Greenwood, 1993.

"CERT® Advisory CA-2001-19 'Code Red' Worm Exploiting Buffer Overflow In IIS Indexing Service DLL." 2001. http://www.cert.org/advisories/CA-2001-19.html (18 May 2002).

Daniel, Donald C. and Katherine L, Herbig, ed. *Strategic Military Deception.* New York: Pergamon Press, 1982.

Denning, Dorothy E. *Information Warfare and Security*. Tokyo: Addison-Wesley, Inc., 1999.

Evans, Donald L. "A Nation Online: How Americans are Expanding Their Use of the Internet," United States Department of Commerce, 2001.

Flemming, Peter. "Assessing the Cyberterrorist Threat." *Myths and Realities of Cyberterrorism.* 2000. http://www.ippu.purdue.edu/global_studies/gghr/cyberterror6.cfm (14 April 2002).

Fromkin, David. "The Strategy of Terrorism." *Contemporary Terrorism.* Ed. John D. Elliot & Leslie K. Gibson. Maryland: International Association of Chiefs of Police, 1978.

Heuer, Richards J. "Cognitive Factors in Deception and Counterdeception." *Strategic Military Deception.* Ed. Donald C. Daniel and Herbig L. Katherine. New York: Pergamon Press, 1982.

Hogarth, Robin. *Judgment and Choice.* 2nd ed. New York: John Wiley & Sons, 1987.

Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. Addison-Wesley, Inc., 2002.

Jenkins, Brian. "The Future Course of International Terrorism." *Contemporary Trends in World Terrorism.* Ed. Anat Kurz. New Yorrk: Praeger, 1987.

Jenkins, Brian. "International Terrorism: A Balance Sheet." *Contemporary Terrorism*. Ed. John D. Elliot & Leslie K. Gibson. Maryland: International Association of Chiefs of Police, 1978.

Lloyd, Mark. *The Art of Military Deception*. London: Leo Cooper, 1997.

Quittner, Jeremy. "Hacker Psych 101." 2001. http://tlc.discovery.com/convergence/hackers/articles/psych.html (14 May 2002).

Raman, B. "Terrorism 1999: Changing Profile." 1999. http://www.subcontinent.com/sapra/terrorism/tr_1999_01_001_s.html (12 April 2002).

Smith, Douglas V. *Military Deception and Operational Art.* Rhode Island: U.S. Naval War College, 1993.

Snowden, Ben and Hayes, Laura. "International Terrorism Trends." http://www.infoplease.com/spot/terrorism1.html (10 May 2002).

Spitzner, Lance A. "Honeypots: Definitions and Values of Honeypots," 2002, www.enteract.com/~lspitz/honeypot.html (17 May 2002)

Stoll, Clifford. *The Cuckoo's Egg.* New York: Doubleday, 1989.

"W32/Nimda-A." *Sophos Virus Info.* http://www.sophos.com/virusinfo/analyses/w32nimdaa.html (18 May 2002).

Sun Tzu. *The Art of War.* Trans. Samuel B Griffith. Oxford, U.K: Oxford University Press, 1971.

Tucker, David. "What is New About the New Terrorism and How Dangerous is It?" *Terrorism and Political Violence*. London: Frank Cass, 2001. Vol. 13, No. 3. 1 -14.

United States. "Joint Doctrine for Military Deception." *Joint Pub 3-58*. 31 May 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Department of the Navy
   Office of the Chief of Naval Operations (N6109)
   2000 Navy Pentagon
   Washington DC

4. Fleet Information Warfare Center
   255 Amphibious Drive
   NAB Little Creek
   Norfolk, VA

5. LCDR Steven J. Iatrou
   Naval Postgraduate School
   Code IW/Is
   Monterey, CA

6. Professor Hy Rothstein
   Naval Postgraduate School
   Monterey, CA