APPLYING CYBER THREAT INTELLIGENCE TO INDUSTRIAL CONTROL SYSTEMS

THESIS

Matthew P. Sibiga, Maj, USAF

AFIT-ENG-MS-17-M-069

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-17-M-069

APPLYING CYBER THREAT INTELLIGENCE TO INDUSTRIAL CONTROL SYSTEMS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Matthew P. Sibiga, B.S.A.E.

Maj, USAF

March 2017

AFIT-ENG-MS-17-M-069

APPLYING CYBER THREAT INTELLIGENCE TO INDUSTRIAL CONTROL SYSTEMS

THESIS

Matthew P. Sibiga, B.S.A.E.
Maj, USAF

Committee Membership:

Dr. Robert Mills
Chair

LTC Mason Rice
Member

Mr. Stephen Dunlap
Member

AFIT-ENG-MS-17-M-069

Abstract

A cybersecurity initiative known as cyber threat intelligence (CTI) has recently been developed and deployed. The overall goal of this new technology is to help protect network infrastructures by delivering a capability to identify and appropriately act upon threatening cyber activities in a timely manner. Threat intelligence platforms (TIPs) have also been created to help facilitate CTI effectiveness within organizations. There are many benefits that both can achieve within the information technology (IT) sector. The benefits of CTI can be realized throughout the tactical, operational and strategic levels of an organization's battle-rhythm. A resourceful way to manage and automate intelligence sources, provide situational awareness and integrate with existing network protection tools are a few benefits that TIPs provide. The industrial control system (ICS) sector can also benefit from these technologies, because most ICS networks are connected to IT networks. When using indicators of compromise (IOCs) from known ICS malware attacks and an open source intrusion detection system (IDS), CTI and TIPs can become an effective cybersecurity tool. This research shows how these IT-based technologies may help protect ICS networks. Three known malware attack scenarios are used to showcase its likely deployment. These scenarios are well-documented campaigns that targeted ICS environments and consisted of numerous IT IOCs. Critical asset owners can obtain improved situational awareness on potential attacks and protect their devices with the proper implementation of CTI and TIP technologies. As a result, a capability exists that allows the possible prevention or identification of a future ICS attack.

Table of Contents

Page

List of Figures

List of Tables

APPLYING CYBER THREAT INTELLIGENCE TO INDUSTRIAL CONTROL SYSTEMS

I. Introduction

1.1 Motivation

Threats from improvised explosive devices (IEDs) escalated during the 2003 Iraqi insurgency. As a result, the Department of Defense (DoD) initiated the Joint Improvised Explosive Device Defeat Organization (JIEDDO) with a mission to defeat IEDs as weapons of strategic influence. JIEDDO uses all available sources of information and intelligence for gathering imperative details regarding IEDs. Data that includes how the device is made, how a device operates and where it is located are correlated to provide troops a way to counter these dangers [13]. The Department of Homeland Security (DHS) created an online 24/7 sharing resource called TRIPwire that allows users to gain IED awareness and share lessons learned regarding counter-IED details [30]. These efforts have led to keeping people safer.

Information Technology (IT) professionals are now applying similar information and intelligence gathering techniques to combat malicious actions in cyberspace. The creation of the National Cybersecurity and Communications Integration Center (NCCIC) within DHS in 2009 was the start of this initiative. Sharing cyber related indicators of compromise between federal agencies and the private sector is the main function of this center with the intent to better protect networks and infrastructures [29]. In 2015, the President of the United States created the Cyber Threat Intelligence Integration Center (CTIIC) with the mission of determining connections between or

among malicious cyber incidents. This team will directly support the NCCIC and other federal agencies in enhancing their cyber missions [20].

Industrial control systems (ICS) have seen an increase in attacks over the last several years. DHS reported that there were 295 incidents in 2015, which is slightly up from 2014 with 245 incidents [15]. These systems are gaining in popularity for attacks because they were not built with security in mind. Availability is the most important aspect for ICS devices, which makes implementing security difficult. Additionally, these are mostly legacy systems that were built and installed prior to the Internet revolution with no authentication requirement incorporated. The isolation that these systems once had was considered their security. However, with the evolution of the Internet, ICS's are now increasingly becoming connected to internal and external networks to increase efficiency [31]. There were 98,000 Internet facing ICS devices in 2014 [4], putting these at significant risk for attacks.

Due to the nature of ICS environments and operations, security needs to become a high priority just as it is for IT systems. Both systems have uniquely different purposes, but both absolutely need security to ensure functionality. Devices that sense or trigger physical processes through direct control or monitor processes are considered ICS. These devices are usually event-driven and include real-time software applications with embedded software [4]. Common examples of usage include operation of industrial plant processes and equipment. Industrial sectors that use the systems include oil and gas, water treatment facilities, and power and utilities. The systems that include hardware, software, infrastructure and applications to transform data and information are considered IT. A common example is an organization's use of computers, server and applications to conduct business. Security is vital for both technologies; however, they can have different motives for why and how to be secure. In terms of the CIA triad (confidentiality, integrity and availability), IT is typically

more concerned about security of data, while ICS's are usually more concerned about availability of the system. Electric power stations and grids use ICS devices to regulate and maintain the electrical power throughout nations. These devices need continuous availability and time-critical content to ensure uninterrupted day-to-day functions.

Safety implications can also arise from lack of availability of ICS devices. Within IT systems, lack of availability can be often tolerated without any safety consequences. The applications, operating systems and protocols that run on ICSs tend to be uniquely different than IT systems. Therefore, these devices often create technical knowledge and awareness gaps regarding security for conventional IT personnel [32]. The security needs of ICS devices need just as much attention, or even more, as those of IT.

1.2 Research Hypothesis and Goals

This thesis examines the use of threat intelligence for cyberspace and develops use cases for ICS devices. Three major malware campaign scenarios are provided to show the potential effectiveness.

The overall research problem is to evaluate whether CTI and TIP technologies can benefit security in ICS networks. IT networks can directly benefit from the effective use of CTI and because of ICS's relationship to IT infrastructures, CTI should also benefit these networks. There are two goals that need to be achieved to show applicability of these technologies. The first is the successful integration of CTI and a TIP within an ICS network. The second is the successful employment of CTI and a TIP in providing situational awareness of potential attacks which should lead to better prevention and response to malicious activity in ICS networks.

1.3 Approach

This research strived to model real-world situations and infrastructures. Historic and well-documented malware attacks against ICS environments were analyzed and used to perform experiments. A small network of virtual machines and physical devices were used to mimic ICS infrastructure and conduct the experiments. The experiments analyzed network traffic for specific malicious items. The use of open-source material for cyber threat intelligence data was used due to its readily available nature.

1.4 Research Contributions

This research establishes a framework for using CTI and TIP technologies with ICS networks. At the time of this research, no attempts of using these technologies with ICS environments were found in the research literature. Another contribution is the analysis and inclusion of cyber threat intelligence within the ICS Cyber Kill Chain.

1.5 Thesis Layout

Chapter 2 describes background details on these new technologies and establishes context for this research. Chapter 3 provides details on three case studies and a framework of using CTI and TIP with an ICS network. Chapter 4 presents the result of using the framework based on the three case studies, while Chapter 5 offers conclusions and opportunities for further research. Lastly, Chapter 6 explores initial pilot studies that were conducted to get acquainted to these new technologies.

II. Background and Literature Review

2.1 Introduction

This chapter provides the details on CTI and TIP technologies. First, an in-depth analysis will provide a solid foundation for the knowledge needed to understand how these can benefit ICS environments. Use cases will be provided to establish how the technologies could work in an organization. Lastly, an analysis will be given on how CTI can be incorporated within the ICS Cyber Kill Chain.

2.2 Cyber Threat Intelligence

Historically, it was normal for ICS networks to operate without security concerns due to their closed and proprietary nature [1]. However, with the evolution of the Internet and organizations looking for the most efficient way to do business, ICS and information technology (IT) networks have become interconnected. The challenge with this new environment is that both types of systems have fundamental differences regarding operations and cybersecurity. The core difference is that an ICS network's main security objectives are integrity and availability of the field devices while IT networks are generally concerned about confidentiality of data. There are safety and revenue implications that can arise from the lack of availability to ICS devices. Consequently, ICS and IT technicians often have different perspectives regarding security.

A new and emerging technology known as cyber threat intelligence (CTI) may be able to benefit ICS and traditional IT networks. Research institutes (e.g., Gartner, SANS, Forrester and Carnegie Mellon University) have developed formal definitions of CTI (see [12, 22, 27]). Delivering a capability to identify and appropriately act upon threatening cyber activities in a timely manner is the idea behind CTI. There

are many ways to gather this intelligence. Methods include (but are not limited to) security incident and event management solutions (SIEMs), open source intelligence feeds, commercial feeds, users, and vulnerability and malware databases. From these sources, indicators of compromise (IOCs) can be determined, documented and further analyzed. An IOC is a forensic artifact of an intrusion that can be identified on a host or network. IOCs are tied to observables and related to measurable events [8]. IOCs can be categorized as either network-based or host-based (common examples are shown in Table 1). An indication of attack is the culmination of IOCs.

Table 1. Categories and examples of IOCs.

Network -Based	Email addresses, subject line and attachments. Connections to specific IP addresses or uniform resource locators (URLs). Fully qualified domain names (FQDN) of botnet command and control (C&C) server connections.
Host-Based	Presence of filenames or programs and their associated MD5 or SHA hashes. Creation or manipulation of dynamic link libraries (DLLs), registry keys and mutual exclusions.

The crux of CTI is the contextual information surrounding attacks. This is the comprehension of the past, present and future tactics, techniques and procedures (TTPs) of an extensive range of adversaries. Included in this analysis should be the connection between the technical indicators, adversaries, their incentives and objectives and information about the targeted victim [12]. For an organization to benefit from this intelligence, it needs to be timely, accurate, relevant and actionable. The data needs to address incidents that are happening (or likely to happen) or have actually been observed. These incidents also need to be meaningful to the organization and help achieve security objectives [5]. This should lead to informative and proactive decision making for protecting networks and infrastructures.

CTI requires several essential characteristics in order to be effective. First, it needs to be adversary-based. By knowing details about an adversary, an organization can enhance its protection against their attacks. Secondly, the intelligence needs to be risk focused. Securing an organization's critical assets should be of utmost importance. Next, intelligence collection and processes need to be well-documented and efficiently executed. This will help make organizations think systematically on how to effectively use the collected information. Lastly, intelligence should be customizable for a wide range of consumers. An organization will consume and act on information differently depending on the role within that organization (see Table 2) [6].

Table 2. Levels usage of CTI.

Analyst	Needs just enough context to determine if further investigation is needed.
Incident Response	Needs extensive details to find other related incidents.
Chief Security Officer	Needs evaluation of threat on possible connections to other worldwide events.

A main cornerstone of CTI is that it needs to be sharable so that malicious threats can be thwarted worldwide. The last several years have seen a large number of CTI feeds created and deployed. These feeds are developed and maintained by a number of private companies, various government agencies and non-profit organizations. Most feeds can be categorized into two groups: (i) commercial (fee-based); and (ii) open source. Fee-based feeds contain more of the contextual information that makes for actionable intelligence to an organization, whereas the open source feeds provide basic IOC data with very little context. A few examples of each are shown in Table 3.

Table 3. CTI feeds.

Fee-Based	FireEye, RSA, Symantec, Recorded Future, Secure Works and Verisign.
Open Source	DHS, Hail a Taxii, ThreatCrowd, SANS Internet Storm Center and GitHub repositories.

The benefits of CTI can be realized throughout the tactical, operational and strategic levels of an organization's battle-rhythm. Tactical benefits will be seen instantly with security teams addressing incoming IOC data immediately. As the tactical level starts to connect IOC details, operational benefits will begin to form as the context of an attack becomes apparent. The strategic benefits will be reached by the culmination of the lower levels by providing a broad range of situational awareness that will help current and future security initiatives. Table 4 summarizes the benefits [22, 8, 6].

Table 4. Benefits of CTI.

Tactical	Swiftly deal with threatening indicators. Prioritize vulnerability patches. Connect details associated with attacks quickly and accurately.
Operational	Improve insight into methodologies as attacks can be seen in context. Detect and remedy breaches faster. Prevent future incidents.
Strategic	Obtain organizational-wide situational awareness. Understand the difference between a real threat and hype. Determine IT security expenses based on risks and prospect of adversarial action.

2.3 Threat Intelligence Platforms

A resourceful way to manage and automate intelligence sources, provide situational awareness and integrate with existing network protection tools is to deploy a Threat Intelligence Platform (TIP). As of this writing, there are currently a few TIP vendors (e.g., ThreatQuotient (product: ThreatQ), ThreatConnect (product: ThreatConnect) and Anomali (product: ThreatStream)). By way of comparison, Phantom Cyber [21] claims ThreatQ can support 14 distinct services while ThreatConnect can support 7, and ThreatStream can support 6. With the successful integration of a TIP, an organization will have several key advantages:

- Timely analytics of intelligence from a wide range of sources and the creation of a system of record.
- Threat intelligence visualization that leads to quicker connection and analysis of IOCs.
- Allowing concurrent access for multiple users making existing network tools stronger.

A Security Operations Center (SOC) is where the deployment of a TIP is the most conducive. A SOC generally consists of multiple teams which are responsible for IT control, monitoring and operations within large organizations (e.g., analysts, incident response team and Chief Security Officer). Six key features that TIPs provide for an organization when implemented with existing threat intelligence capabilities are shown in Table 5 [17].

Table 5. Features of TIPs.

Collect	Standardize ingestible threat intelligence for analysts into one platform. Import and parse open source, commercial feeds and ad hoc unstructured formats (e.g., email, webpages and social media).
Act	Activate tasks for teams (e.g., network defensive signature updates and IOC analysis). Create reports to distribute content and alerts to organizational wide users or a specific audience.
Correlate	Provide unique enrichment and pivoting data to determine IOC connections. Produce a convincing landscape of a threat with derivation of authoritative context.
Integrate	Transform higher level data to use with lower level defensive tools and SIEMs. Create and provide signatures and data points for compatible IDS, IPS and firewalls. Create appropriate tickets with an organization's current help desk system.
Categorize	Organize IOCs by threat actor, country or other common characteristics. Gain insight into threat actor TTPs. Mark indicators to offer context and relevance.
Share	Allow collaboration and sharing among internal and external entities. Provide workflow coordination among organizational teams (e.g., SOC operations and help desk). Export data in a sharable format so outside organizations can defend against similar attacks.

2.4 Use Cases for CTI and TIPs

Providers of CTI and TIPs have documented use cases on how these technologies can benefit an organization. The following are generalized scenarios and specific

vignettes to demonstrate efficiency.

2.4.1 Generalized Scenario

The following is a generalized scenario of how CTI and TIP technologies can be used within an organization [28].

2.4.1.1 Collection and Research

The process begins by having the platform ingest open source intelligence and Homeland Secure Network Information along with user feedback and local defensive network data. Some examples include free and paid automatic feeds, whitepapers, government reports, emails, SIEMs logs and databases. Within these sources are potential IOCs and contextual information that might be useful to an organization to detect attacks. A TIP will use an included parser to automatically extract, store, standardize, categorize, display and archive the incoming data from these multiple sources. SOC personnel will monitor this process to ensure proper operations. SOC analysts can perform further research on the data, which may lead to other IOCs that will be manually entered to the TIP.

2.4.1.2 Approval Preparation and Approving Authority Ingestion

As IOCs are incorporated into the TIP, they are automatically classified with a status of "Review" or "Active." At determined intervals, data that is labeled as "Review" is fed into a report for SOC management's analysis of validity. This process is completed with an email to the approving authority with the pertinent information. When an organization has trusted sources (e.g., commercial feeds and internal devices), a TIP can be configured to automatically approve and implement that data. An approval process is needed to attest that an organization is satisfied

with an analyst's recommendations before IOC deployment into their infrastructure.

2.4.1.3 Implementation

Once IOCs are validated for distribution, a TIP can automatically format the data for the appropriate defensive tools active in a network. For the indicators that are denied because of their non-applicability to an infrastructure, a TIP will keep a record to prevent duplications by other team members and provide a threshold of the approving authority's tolerance.

Figure 1 illustrates this generalized process of utilizing CTI and TIP technologies with the open source IDS SNORT. Feeds, users and databases will provide IOCs for investigation that eventually results in CTI. This intelligence will then be imported into a TIP. The TIP will export the necessary data to network defensive tools (i.e., SNORT).

2.4.2 Summarized Vignettes

The following are summarized vignettes at the tactical, operational and strategic levels. These provide insightful examples on how beneficial these technologies have been for organizations.

2.4.2.1 Tactical - Stopping Attacks

Company A had a security team with many tools and processes but no centralized workspace for collaboration or scalability. This resulted in team members having different versions of collected data which led to confusion regarding current threat status. A potential solution was the creation of a shared spreadsheet. However, over the course of time that spreadsheet grew in volume. Queries on data resulted in long wait times. In addition, the security team was without a tool that allowed

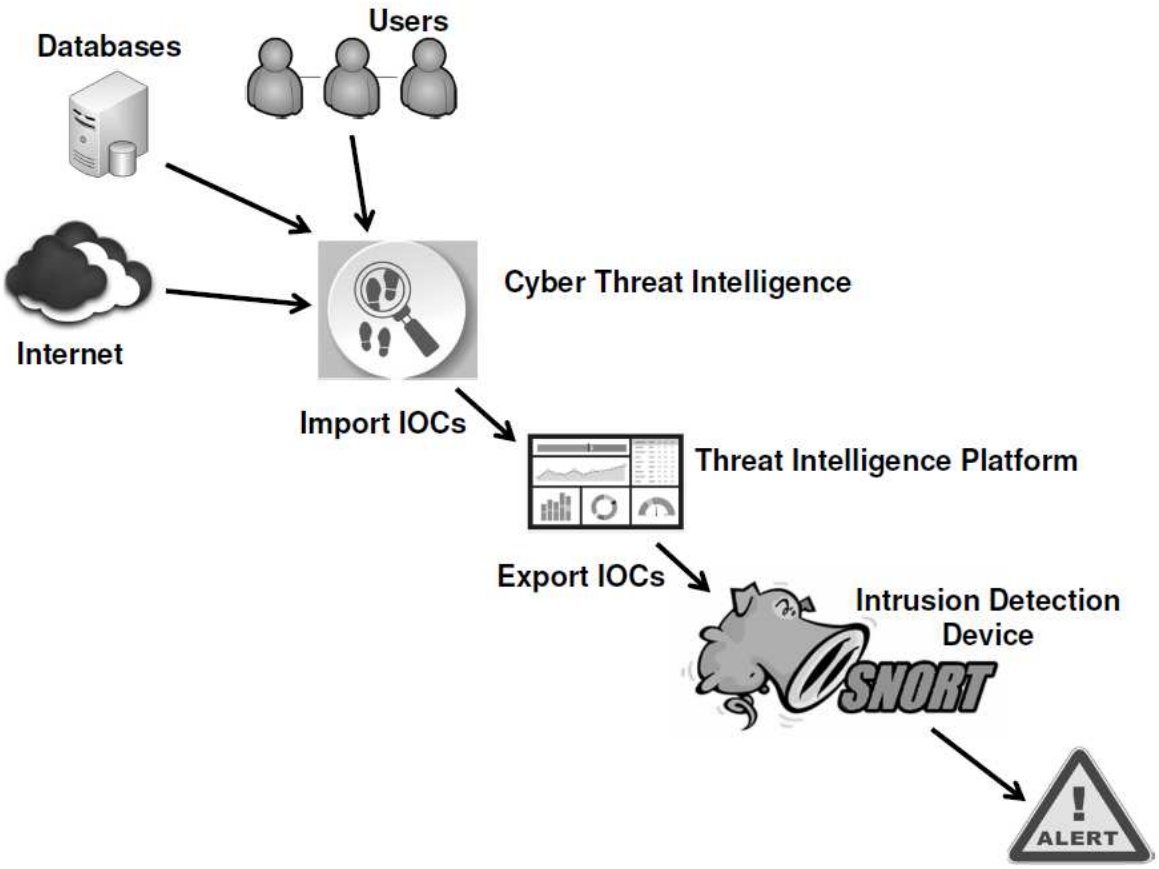


Figure 1. Overview of CTI and TIP process.

in-depth malware analysis. Their network defensive tools were too strict to allow any information to be captured, and no new intelligence was being gathered. The company was eventually attacked by an advanced persistent threat (APT) and was convinced a TIP was needed.

As a result of implementing a TIP, the company saw immediate improvements. Productivity surged for the SOC personnel as the queries on IOCs only took a matter of seconds due to the TIP's ability to simplify searches. Automated data storage allowed for a centralized and continuously updated database which provided efficient situational awareness. Synchronization of the network defensive tools, processes and data provided immediate actions for team members [25].

2.4.2.2 Operational - Predictive Network Defense

While reviewing logs, a SOC team member responsible for monitoring a network intrusion detection device notices a domain connection. A ticket is created and sent to another team to conduct further analysis. This team used the Whois and passive domain name system (pDNS) tools, which are common within a TIP, to recover information on who registered the domain, a history of other associated domain names and additional domains that resolved to the same IP address. Another included TIP tool, ReverseWhois, showed other harmful domains that were linked to the registrant's email address. The relationship of all this data led to a high assurance of attribution from one attacker. The attacker's infrastructure was further unveiled when the discovered indicators were incorporated into the TIP. Uncovered were other malicious indicators which allowed the SOC to predict potentially future domain connections [24].

2.4.2.3 Strategic - Strategic Planning and Security Requirements

Company A used the TIP to assist with strategic planning. Risk assessments are better defined with actual and witnessed threat intelligence. The TIP technology provides a knowledge source for threat data and incident-response efforts. This historical record can be used to support strategic shifts in resources to appropriately address threats. [26].

2.5 ICS Cyber Kill Chain Analysis

Most, if not all, ICS are connected to a traditional IT network in some way (see Figure 2). Stakeholders that effectively implement IT CTI policies and procedures will increase their ability to identify, track, isolate and hopefully prevent attacks targeting ICS infrastructures. The same benefits that CTI provide IT networks can

positively impact connected ICS networks.

At the time of this research, there was not enough data regarding IOCs related to ICS devices. Therefore, investigation was limited to the IT vector.

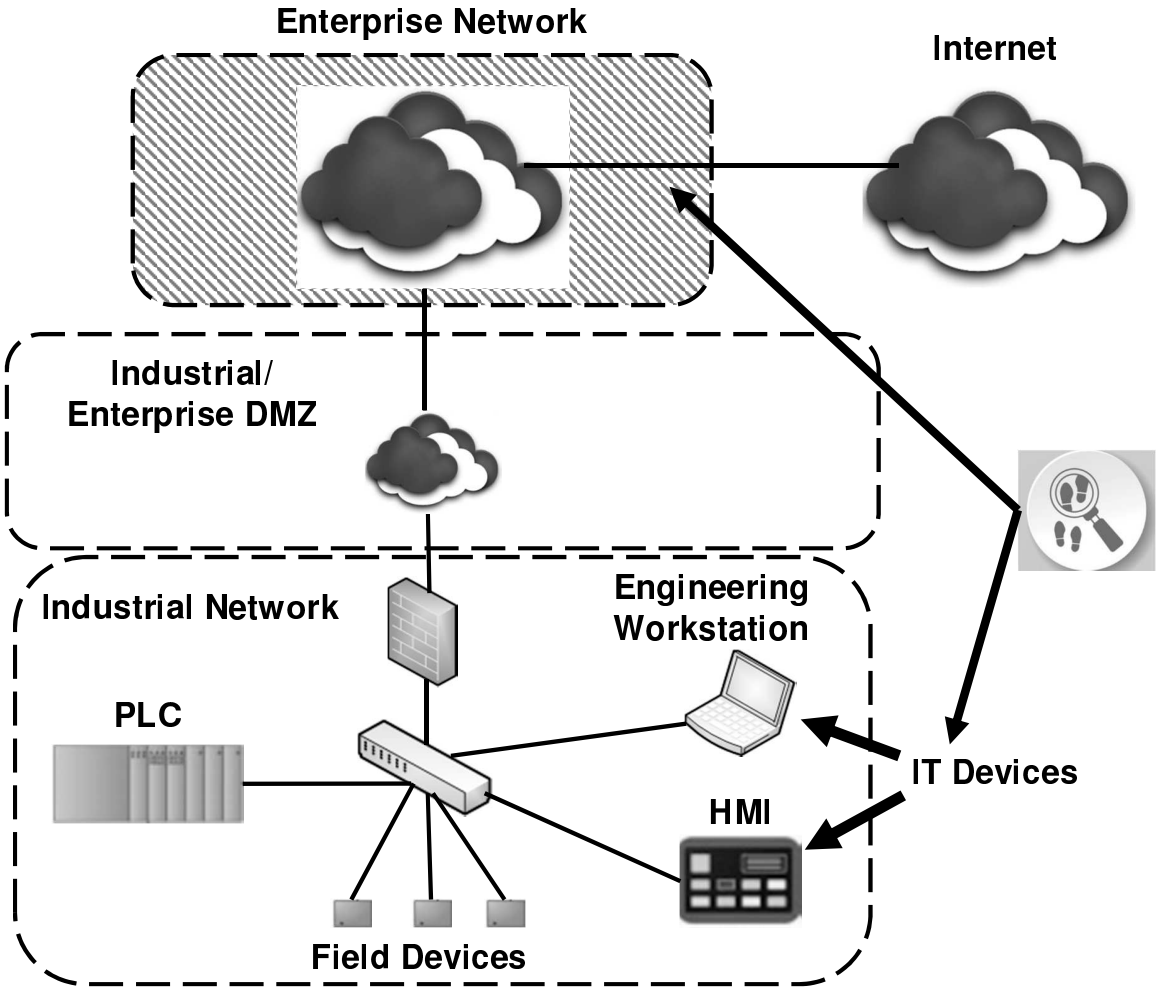


Figure 2. ICS and IT sample network.

A team with the SANS Institute (Assante et al.[2]) developed a cyber-kill chain specificly for ICS environments. There are two stages associated with their version: (i) Intrusion; and (ii) Attack. The Intrusion stage will produce the most prevalent IOCs associated with an attack. Figure 3 illustrates the Intrusion stage and how it can be broken into 3 zones.

1. **Internet**: Threat actors will conduct reconnaissance operations, develop their

weapon and choose a target.

2. **Enterprise Network**: This is where threat actors attempt or successfully gain access to the targeted network. IOCs associated with this area could be the malicious file information (name and hashes) and spear-phishing email details.

3. **Industrial Network**: This is where threat actors are conducting C&C operations, maintaining persistent access and preparing the malicious activity. IOCs associated with this area could be unknown connections to IP addresses and FQDN's, DLL's and any mutual exclusion or registry key creation.

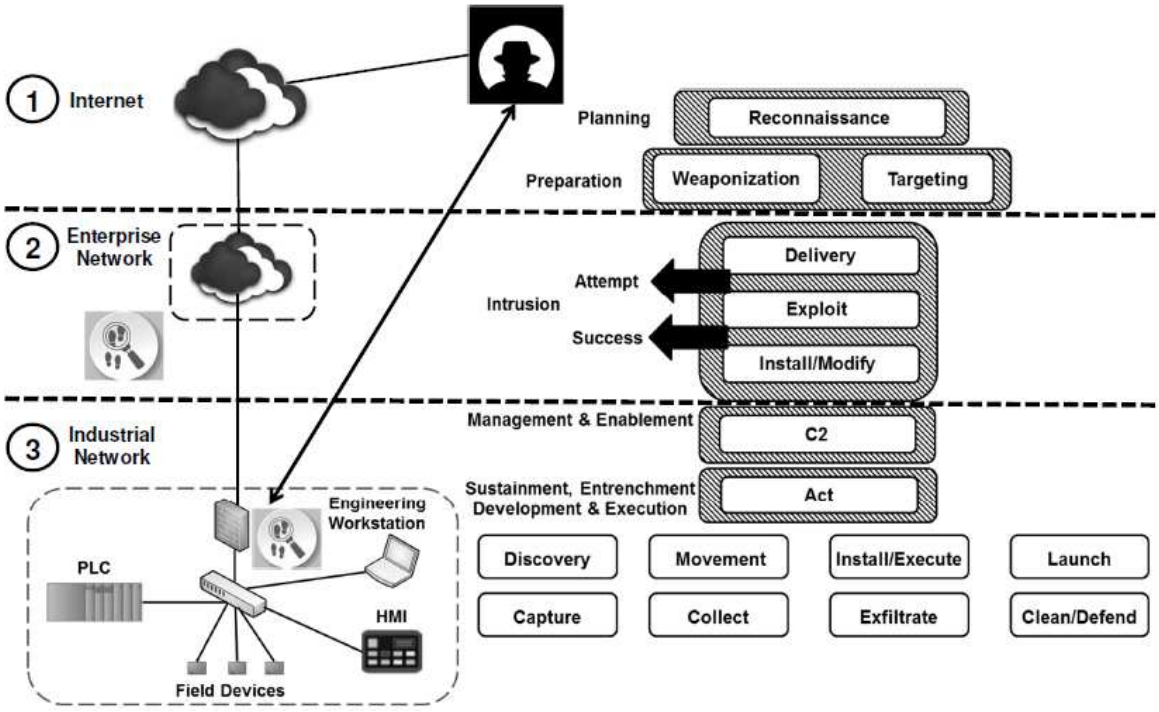


Figure 3. Intrusion Stage of ICS Kill Chain with IOCs.

2.6 Summary

Combining the facts obtained through this background review, three crucial points have been established:

1. ICS networks are commonly connected to IT networks.

2. Purpose of CTI and TIP is to enhance IT cybersecurity.

3. IT IOCs can be observed prior to the Attack Stage within the ICS Kill Chain.

This research will investigate a method for combining these three essential points into one comprehensive process with the purpose of protecting ICS devices.

III. Case Studies and Framework

3.1 Introduction

To accomplish the research objectives, a proof of concept needs to be created. This chapter will explain three historical ICS attack incidents and how each had IT IOCs that CTI will effectively employ. This chapter will also explain the implementation setup and design choices for testing CTI and TIP technologies with ICS networks.

3.2 ICS Attacks with IT IOCs

A campaign known as Dragonfly was launched against a Ukrainian power company that resulted in successful ICS physical impact. The campaign used a variant of the BlackEnergy malware. The malware known as Duqu and Havex were not used for attack purposes but to perform reconnaissance of ICS networks. For each campaign, there are extensive detailed technical reports released by security companies (see [18, 23, 16]). Examination of the reports indicated the attack vectors went through the IT networks. Therefore, all have IOCs related to IT systems. This chapter describes BlackEnergy, Duqu and Havex. Table 6 has a summary of these incidents.

3.2.1 BlackEnergy

In 2015, a Ukrainian power company, Kylvoblenergo, suffered power outages related to a cyber-attack. A use case was generated by the Electricity Information Sharing and Analysis Center (E-ISAC) and SANS Institute regarding this campaign in hopes of educating ICS stake-holders [18]. The attackers used spear-phishing emails to obtain valid credentials to gain initial access to the targeted networks. Included in these emails were Microsoft Office documents that contained the BlackEnergy malware. Enabling the macro functionality of these documents allowed the malware to

Table 6. ICS Malware Attacks.

BlackEnergy	- An ICS attack with physical impact. - Malware was used for reconnaissance and stealing confidential information. **TTPs:** - Spear-phishing to steal VPN credentials and plant malware. - Access ICS devices via VPNs. **IOCs:** - Email addresses and subjects. - C&C outbound connections. - Malicious MS office files.
Duqu	- An ICS attack without physical impact. - Malware was used for reconnaissance and stealing confidential information. **TTPs:** - Send emails with malicious files. - Establish C&C to download other malicious executables. - Remove itself after 30 days. **IOCs:** - Executable filenames along with associated MD5 hashes. - IP addresses that are C&C servers.
Havex	- An ICS attack without physical impact. - Malware was used for reconnaissance and stealing confidential information. **TTPs:** - Spear-phishing with malicious attachments. - Use compromised websites. - Trojanize ICS vendor software via legitimate websites. **IOCs:** - Filenames and MD5 hashes. - Registry entries. - FQDN that are C&C servers.

start C&C communications via outbound connections. With the initial stolen credentials and C&C servers, the attackers were able to obtain network details, pivot throughout the infrastructure and elevate their privileges. Once the attackers had persistent access, they abandoned initial credentials and C&C connections. Virtual

private networks (VPNs) were then used to access the ICS devices that controlled the power breakers. In the end, approximately 27 substations were brought offline by the attackers opening up breakers. IT-related IOCs associated with this case study could be the email subjects, email addresses, Microsoft Office file names and C&C outbound connections.

3.2.2 Duqu

In 2011, Symantec published a report on a threat known as Duqu and confirmed that it is almost equivalent to Stuxnet with the primary difference being the motive [23]. The intent of the malware was to gather intelligence on a target's ICS assets and infrastructure. This data would then lead to a future attack in the same manner as Stuxnet. This malware is primarily a remote access Trojan (RAT) and does not have any ICS related code. It contains three files: (i) a driver; (ii) a main DLL; and (iii) an encrypted configuration file. In a reported case, the malware was delivered by specifically targeted email with a Microsoft Word document that executed a zero-day kernel exploit. The infection process for this malware is complex and extensive. Essentially, an installer injects the main DLL into services.exe and this begins a process of extracting other harmful components, which are injected into other processes allowing security products to be avoided. One of the components is responsible for establishing several C&C server connections outside of the targeted network using HTTP and HTTPs communications. Using these servers, the attackers were able to download executables that enumerated the network, logged keystrokes and gathered system details. This malware spread through a network using network shares and peer-to-peer connections. IT-related IOCs associated with this case study could be the filenames and MD5 hashes of the malicious executables and the IP addresses of the C&C outbound connections.

3.2.3 Havex

The campaign known as Dragonfly was discovered in February 2013 and reportedly had an objective of completing reconnaissance of ICS components within an organization [16]. Multiple types of malware were used to achieve the attacker's goal with the Havex RAT being the most common. The threat actors used three methods of planting malware on targeted machines: (i) spear-phishing emails; (ii) watering hole attacks; and (iii) Trojanized software downloads via ICS supplier websites. All three methods required a user to trigger the malware installation. The emails contained a malicious file for a user to open. The watering hole attacks occurred when users accessed compromised websites and were redirected to other sites containing malicious files. The trojan software used compromised ICS vendor support websites by supplanting legitimate software with malicious software. Once the malware was installed, the first task was to initiate a request to a C&C server via HTTP and once established, multiple modules were embedded in the reply message and then executed on the targeted machine. These modules were executables and DLLs whose main purpose was to maintain persistence on machines by creating an entry in the Windows Registry. Upon start up, malicious programs would run. It was reported that the C&C servers were also able to update the malware on targeted machines because of this persistence. This campaign was able to show that engineering workstations that come back and forth from isolated ICS networks to IT networks are valid entry points. IT-related IOCs from this attack include FQDN, filenames along with their respective hashes and registry entries.

3.3 Framework

The previous case studies have provided foundational details for establishing a potential framework for using CTI and TIP with ICS environments. There are a

few technical and operational requirements needed to build a proof of concept. All requirements need to function together to produce positive results.

3.3.1 Gathering CTI

The public site and secure portal for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has an abundance of data that can be used as CTI for ICS stakeholders. Reputable security firms (e.g., Belden and Symantec) and credible ICS related open source websites (e.g., SCADAhacker.com) provide additional and in some cases, more in-depth CTI associated with ICS environments. Published alerts, advisories, bulletins, reports and white papers are all excellent sources for gathering appropriate data. Open source materials from ICS-CERT, Symantec, SCADAhacker and IOC Bucket were used to gather CTI on the Duqu, BlackEnergy and Havex malware. Deploying a TIP to complement the incoming CTI is vital to adequately managing the data and actions needed to enforce it. A TIP from the company ThreatQuotient called ThreatQ will be used.

3.3.2 Deploying a TIP

ThreatQ was selected as part of a cooperative research and development agreement between ThreatQuotient and the Air Force Institute of Technology. The company provided the necessary hardware and license for research purposes. ThreatQ is a physical machine which can be deployed on-premises. Over 13,000 IOCs were entered into ThreatQ from the sources mentioned earlier A key feature that the ThreatQ device offers is customizable export options for data to practically any network security device. There are some preprogrammed export options that are included with ThreatQ, but the customization options make this product compatible with an organization's infrastructure design.

A key feature that ThreatQ does not have at the moment is the creation of SNORT rules from various data points. The platform relies on users to create customized scripts to pull the necessary data. There are competitive TIP offerings by other major security companies but due to the newness of this technology there are not many. The most competitive offering is from ThreatConnect, which is a considered a cloud offering. Currently, ThreatConnect offers the creation of SNORT rules from crucial input.

Appendix A describes initial pilot studies that were conducted early in the research. The features mentioned above were discovered during those studies along with other important details.

3.3.3 Intrusion Detection System Selection

According to researchers with the SANS Institute [3] and Schweitzer Engineering Laboratories [10], a deployment of an IDS with SNORT functionality will improve security of ICS networks. SNORT's open source nature coupled with its vast IT security industry-wide adaptability make it highly recommendable for IDS purposes. In recent years, ICS rule development within SNORT has led to key enhancements for ICS infrastructures. Renowned security teams (e.g., Talos and Digital Bond) have created specific SNORT rules directly related to vulnerabilities affecting ICS devices and networks.

SNORT was selected as the IDS due to its open-source nature and widely praised applicability. There are many key advantages that SNORT offers and listed below are just a few.

1. Can be installed on various operating systems (e.g., Windows and Ubuntu).

2. Highly involved community of rule writers that include ICS experts.

3. Ability to have rules automatically update when there are new and improved rules.

4. Ease of customization to particular network and infrastructure needs.

SNORT was installed with Ubuntu due to the operating system's ease of customization. Creating and maintaining the scripts needed to create SNORT rules was straightforward. Examples of SNORT rules can be found in Appendix C. Overall, 1,790 rules were created and imported.

BRO is another open-source and highly respected IDS option that was briefly tested during this research. BRO can be downloaded as its own program or included as part of the Security Onion suite. This IDS was not used during this research due to the complicated nature of setup and integration. This program requires significant experience and in-depth training in order to fully utilize its features.

3.3.4 Infrastructure Design

Figure 4 illustrates the infrastructure framework that will be used to show applicability of using CTI with ICS environments. The ThreatQ TIP is deployed in the Industrial/Enterprise Demilitarized Zone. A small network of virtual machines will make up the industrial network. The SNORT IDS is configured on Ubuntu with the industrial network. The configuration process created local rule files that contained prevalent ICS rules from ICS-CERT, Emerging Threats and Digital Bond. Organizations that have a desire for an even wider range of rules can create a free account on SNORT.org and access their comprehensive rule files. This same virtual machine has python scripts that can create additional SNORT rule files from the export functionality from the ThreatQ machine. For example, a script can pull all malicious IP addresses in ThreatQ and create a rule file that contains numerous rules. The same can be done for malicious filenames, MD5 hashes and DNS requests. Two virtual

machines will be used as engineering workstations with one running Ubuntu and the other running Windows 7. An HMI device is also on the network running Windows XP.

A few virtual machines were need to simulate IT devices within the industrial network. A variety of operating systems were chosen to cover possible real-world ICS environments. For example, if Windows XP machines were mentioned frequently during analysis of the malware campaigns, that operating system was created. During this research, Ubuntu, Windows XP and Windows 7 were the most commonly used on IT devices in industrial networks.

3.3.5 Field Devices and Programmable Logic Controllers

These devices were not used within this framework. Currently there is not enough data to associate IOCs to ICS devices and identifying the malicious activity before any ICS devices are accessed is the main objective of this research. Field devices and programmable logic controllers will be controlled by an IT device, which has IOC data.

3.3.6 Validation

Validating that component operations are working as expected is essential to ensuring framework functionality. The following validation was completed:

1. **TIP ingesting CTI**

   A page of the Symantec Duqu technical report was saved locally and imported into ThreatQ. The platform's parsing function correctly organized the IOCs and importation was successfully done.

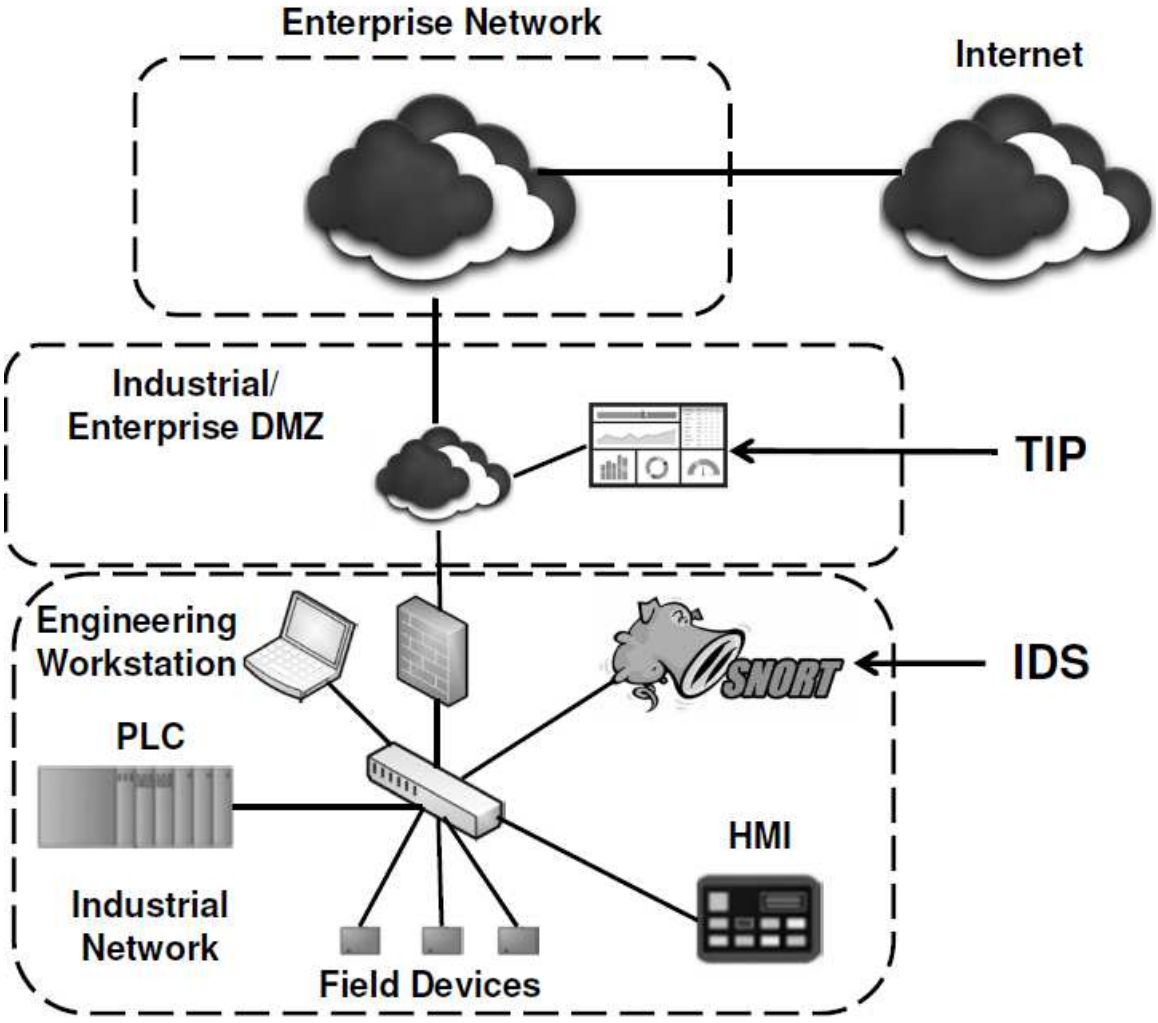


Figure 4. IT and ICS sample network with SNORT and TIP.

2. **IDS Alerting**

SNORT has a built in function that upon initialization, it will check all rules and settings first. If any of those are not configured or set up correctly, SNORT will abort and notify the user of the fatal error. The error would state the line number in the appropriate rule file with a short description on what is wrong. An example would be if a rule was not written in the correct format. After setting up SNORT within the framework and initializing, no errors were reported. Screenshots are provided in Appendix D.

Each virtual machine was configured to have an IP address and connected to the Internet as well as connected with each other. A simple SNORT rule to test any transmission control protocol or user datagram protocol was created. Each virtual machine visited google.com and the SNORT IDS alerted to the connection. Screenshots are provided in Appendix D.

3.4 Summary

This chapter established the framework needed to show a possible proof of concept that utilizes CTI and TIP operations for ICS situations. The three historical ICS malware attack scenarios described will be used to demonstrate applicability within the constructed framework in Chapter 4.

IV. Results and Analysis

4.1 Introduction

This chapter provides analysis of the experiments conducted regarding the three malware attack scenarios from Chapter 4. Presented are the results and technology limitations.

4.2 BlackEnergy

The NCCIC, in cooperation with ICS-CERT, published an incident alert (IR-ALERT-H-16-043-01BP) on 5 April 2016 related to Ukraine's power outage [11]. Figure 5 illustrates the process of obtaining pertinent CTI and using a TIP and SNORT IDS to alert to an IOC.

1. **Collect**: This alert document is pulled from ICS-CERTs secure portal document library. Table 1 within the alert document outlines the IOCs that have been observed regarding this attack. Included are FQDNs, email headers, IP addresses, URLs and filenames.

2. **Import IOCs**: The table, which was six pages, was saved as PDF files allowing for easy importation into ThreatQ. The report document was then imported to ThreatQ.

3. **Correlate and Categorize**: After all the data was successfully imported, it was correlated and categorized as part of the BlackEnergy malware family.

4. **Share**: If an organization intended to share this intelligence with outside entities, a simple export could be prepared for publication.

5. **Act and Integrate**: Scripts were run to enable the Act function of the TIP, which exported and integrated the IOC data into the SNORT IDS.

6. **Alert**: For this scenario, visiting a malicious IP address will be tested. Using the Windows XP machine (HMI device) an Internet Explorer window was opened. Using ThreatQs categorization feature, a known BlackEnergy malicious IP address was found (41.77.136.250). Within the Internet Explorer window, that address was manually entered into the address bar. The IDS successfully alerted that a malicious IP address was being accessed within the network.

7. **Situational Awareness**: As a result, situational awareness was obtained to stop and prevent future attacks.

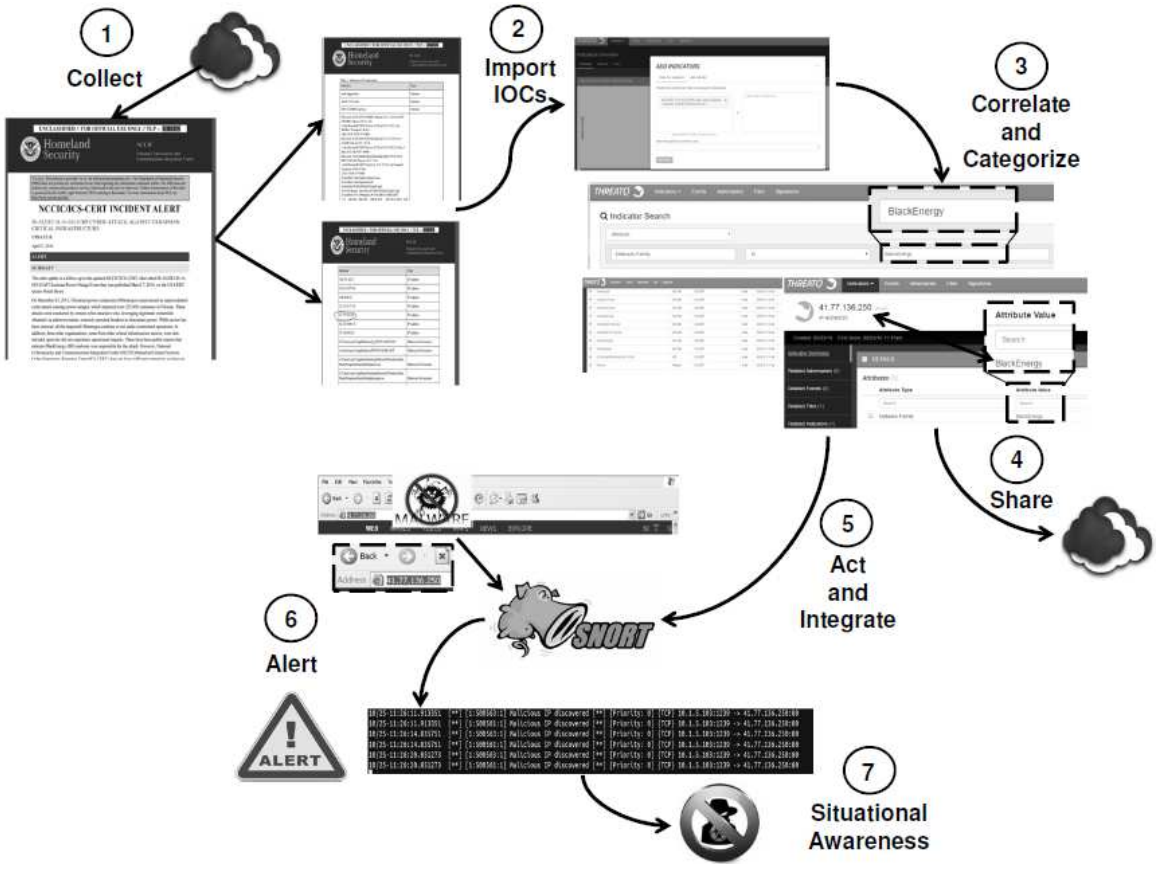


Figure 5. BlackEnergy process.

4.3 Duqu

Symantec's technical analysis report published on 23 November 2011 includes an appendix that has many IOCs associated with the Duqu malware [23]. Screenshots of this process can be found in Appendix A.

1. **Collect**: This report is accessible by a simple search engine query, 'Duqu Symantec Report'. This document included file hashes with the file compilation date and name, IP addresses and a registry entry.

2. **Import IOCs**: The appendix pages of Symantec's report were saved as PDF files and imported to ThreatQ.

3. **Correlate and Categorize**: After all the data was successfully imported, it was classified as being part of the Duqu malware family.

4. **Share**: If an organization intended to share this intelligence with outside entities, a simple export could be prepared for publication.

5. **Act and Integrate**: Scripts were run to enable the Act function of the TIP, which exported and integrated the IOC data into the SNORT IDS.

6. **Alert**: For this scenario, a malicious file movement within the network will be tested. A sample of the cmi4432.pnf (a known malicious file associated with this malware) executable was downloaded from an open source malware site. It was confirmed by using the MD5 hash found in the Symantec report. The file was then placed on the Ubuntu engineering workstation. Using file transfer protocol, the executable was moved to the Windows 7 machine. As expected, SNORT alerted to the violation.

7. **Situational Awareness**: As a result, situational awareness was obtained to stop and prevent future attacks.

4.4 Havex

This malware campaign has been analyzed by multiple IT security companies worldwide. Kaspersky Labs [14], Belden [16] and SANS [19] are just a few examples with each report being easily accessible by a simple search engine query of 'Havex [Company name]'. Most reports provide in depth analytics of the TTPs. Screenshots of this process can be found in Appendix B.

1. **Collect**: ICS-CERT's secure portal has an all-inclusive excel file with multiple sheets of data.

2. **Import IOCs**: After downloading the entire excel file to a local machine, importing to ThreatQ was accomplished. A couple of the detailed Havex reports from the companies mentioned above were also imported for reference.

3. **Correlate and Categorize**: After all the data were successfully imported, it was classified as being part of the Havex malware family.

4. **Share**: If an organization intended to share this intelligence with outside entities, a simple export could be prepared for publication.

5. **Act and Integrate**: Scripts were run to enable the Act function of the TIP, which exported and integrated the IOC data into the SNORT IDS.

6. **Alert**: For this scenario, visiting a malicious C&C FQDN will be tested. According to the excel file, www.swissitaly.com connection is a known IOC. Using the Windows 7 engineering workstation and Google Chrome browser, that domain name was manually entered. As expected, SNORT alerted to the violation.

7. **Situational Awareness**: As a result, situational awareness was obtained to stop and prevent future attacks.

4.5 Results Summary

By using a few simple IT IOC data points, awareness of an potential attack targeting ICS networks can be obtained with the help from CTI and TIP technologies. Properly incorporating them into an organization's security posture should provide an advantage in preventing or identifying malicious activity.

4.6 Technology Limitations

These new cyber intelligence technologies have great potential but there are some limitations as described below

4.6.1 Lack of Standards

Standards for the data structure and sharing this intelligence are still not agreed upon. Directed by the DHS, the MITRE corporation started an initiative that created the Structured Threat Information eXpression (STIX) language and Trusted Automated eXchange of Indicator Information (TAXII) delivery protocol for CTI. However, these two are now in the process of combining into one standard, OASIS, which as no immediate start date as of yet [7]. Commercial feeds operated by vendors use proprietary methods for delivery, leading to more complications for organizations [22].

CTI is not mature enough for most organizations to fully and successfully implement without signification customization. Offerings by vendors are currently vague, which leads to confusion of which intelligence is actionable compared to second-rate information. More time will be needed for the community to determine what in-

telligence is actually useful and provide better tools for effectiveness. IP addresses and MD5 hashes are extremely easy for vendors and government agencies to send to customers. However, that can lead to organizations missing other imperative intelligence. Providers of intelligence are finding it very difficult to supply the TTPs needed for proper defense [9].

4.6.2 Malware Attacks Only

ICS-CERT hosts an advisory website that lists specific known vulnerabilities in ICS systems categorized by vendor. At the time of this writing there are 66 buffer overflow advisories listed. CTI and TIPs will not account for this type of attack because they are not considered IOCs but flaws in software and/or firmware designs. Attackers can use a variety of exploits (e.g., cross site scripting and standard query language injection) to obtain unauthorized access which do not leave an observable or measurable artifact to constitute intelligence.

4.7 Summary

With some basic IOC data from well-documented malware campaigns, the framework proposed in Chapter 3 can provide situational awareness towards potential attacks for ICS asset owners. However, there are limitations that these technologies currently have that may hinder their industry-wide adaptability.

V. Conclusion

This chapter summarizes the overall conclusions of the research based on the results an analysis from Chapter 5 and provides recommendations for possible future work.

5.1 Research Objectives

The creation of CTI and TIP technologies has shown great potential in enhancing IT cybersecurity. With the current disturbing trend of threat actors targeting ICS infrastructures, this research investigated the possibility of using these technologies in protecting these vulnerable networks.

5.2 Research Conclusion

The capabilities of CTI and TIPs show great potential in cybersecurity for ICS and critical infrastructures. These technologies benefit IT and ICS infrastructures because of the connections these environments directly have in this ever-connected world. Similar to the intelligence collection for IEDs, ICS cybersecurity will improve with the evolution of CTI and TIP technologies.

5.3 Research Contributions

A framework for using CTI and TIP technologies within ICS environments has been established with this research. The successful analysis of technical reports on malware attacks provided appropriate threat intelligence. Proper deployment of a TIP within an environment that could ingest intelligence while also exporting data to security devices was accomplished. Implementation of an open-source IDS was completed that allowed for alert capabilities that provided situational awareness of

a potential attack. An integration of CTI, TIP and IDS technologies was built that could provide ICS stakeholders a possible solution for an additional cybersecurity measure.

5.4 Future Work

There are a few areas where future work will further enhance ICS cybersecurity with these technologies.

- **IOCs associated with ICS devices**

  Within the CTI community, there are currently no IOCs specific to ICS infrastructures. If the technology wanted to progress into ICS territory, what would those IOCs be? Since ICS equipment measure physical processes, appropriate IOCs could be abnormal physical instances. For example, an ICS IOC could be the closing of the power breakers in Ukraine, causing power outages. Current CTI and TIP technologies do not have a method to account for these incidents. At this point, the process has obviously been maliciously compromised and manipulated. Future work should investigate into if ICS devices produce IOCs and how, while being easily shareable across the community. There is currently not enough data available to associate IOCs to ICS devices specifically.

- **Creation of MD5 rules with SNORT**

  There is an abundance of CTI related to file hashes, more specifically to MD5. Turning this data into vital SNORT rules would provide another layer of security alerting. Future work should investigate how SNORT can analyze packets for these hashes and the appropriate rule format to create.

Appendix A. Initial Pilot Studies

A.1 Introduction

In order to get familiar and comfortable with CTI and TIP technologies, a couple of pilot studies were conducted early in the research. These studies included an exploration into setting up and using ThreatQ and creating intelligence.

A.2 ThreatQ

Upon obtaining the ThreatQ device, a familiarization period was needed to understand how it operates and its capabilities. This section will describe the process of setting up the ThreatQ device, receiving CTI to the device and reporting of bugs back to ThreatQuotient.

A.2.1 Setting Up

The ThreatQ device is a small, rack-mountable network appliance. Hooking up a keyboard and monitor were initially needed to get the system operational. ThreatQuotient supplied a First Boot guide that consisted of a few commands to download the latest version of the software and to update it. The next step was to create the administrator account and configure the IP address of the device so that network users of an organization could use a web browser to log into it. The setup was complete by successfully logging into the program via the graphical user interface (GUI) with the administrator account.

A.2.2 Receiving CTI

ThreatQ has the ability to receive CTI from multiple feeds, both from open-source and commercial sources. ThreatQ has a feature that allows easy access to feeds with

just the switch of a button. All included feeds are turned off upon installation so that an organization can choose which ones to initiate. Additional feeds are easily enabled within the GUI.

To get an understanding of what vendors offer in regards to CTI, all of the included open-source feeds were turned on. Additionally, a feed was created to collect data from the open-source site of hailataxii.com, which is not included with ThreatQ. Within a few weeks, around 400,000 IOCs were collected from these feeds. Data included IOCs from at least ten malware families.

A.2.3 Reporting of Bugs

During this pilot study, a couple of bugs with ThreatQ were identified. ICS-CERT's secure portal site included a PDF document of SNORT rules regarding possibly ICS vulnerabilities. At the time, ThreatQ had a functionality to import SNORT rules via PDF. However, upon attempting this, a failure occurred and these were not imported. Additionally, a bug with importing IOC data associated with hashes was also identified. When SHA-1 hashes were being imported, they were being categorized as MD5 ones. A note was sent to ThreatQ's support team to notified them of these bugs. All were eventually fixed with proceeding system updates.

A.3 Creating Intelligence

A concern during the background phase of this research was the ability to obtain and generate new CTI, as it is a key component. An initial option was to actually create intelligence and a feed so that data could be sent to the ThreatQ box. Ultimately, ThreatQ's ability to import PDF files was used to collect important CTI related to this research. The section will describe the process of creating intelligence and setting up a server to potentially share that data with others.

A.3.1 Structured Threat Information Expression

STIX was chosen as the primary method for creating intelligence due to its open-source, open-community nature. The MITRE Corporation has extensive resources available to assist the community. STIX is based on the extensible markup language (XML). All required packages were downloaded using an Ubuntu virtual machine. This researcher used the python STIX "Getting Started" resource on the STIX Project website (http://stixproject.github.io/getting-started/) to create a sample intelligence report. This provided a basic knowledge on how IOC can be created from analytics. Due to the extensive nature of XML writing, the option of creating intelligence via STIX was not a priority.

A.3.2 Trusted Automated Exchange of Indicator Information

Once intelligence is created using STIX, a method to send that data is needed and the TAXII protocol is the solution. At the time of this research, a project known as Soltra Edge was the only open-source product that could accomplish this capability. The product can be downloaded as a virtual machine image and then be installed with an appropriate program. A complication became apparent soon after installation as the current version of this program did not support the current version of STIX. Therefore, any created IOC data with STIX would not be able to be sent. Due to this disadvantage, using this product and capability was abandoned.

A.4 Summary

These initial pilot studies and experiences provided an solid foundation for this research. Essential operational knowledge was gained on these technologies that enhanced research methods and objectives. The core of these studies was to obtain the necessary familiarization to these technologies to better solve the research question.

Appendix B. Screenshots of Duqu Experiment

B.1 Duqu

The following screenshots were taken during the Duqu experiment. Here is a brief description of each:

- **Figure 6**

  An appendix of the Symantec Duqu report with all associated IOCs. Circled are two IOC data points that will eventually be tested.

- **Figure 7**

  ThreatQ's record of both IOC data points from Figure 6. This shows that within ThreatQ, Duqu is associated with these IOCs.

- **Figure 8**

  Using the Windows XP virtual machine Internet Explorer to visit the noted malicious IP address. At the same time, SNORT is alerting to the malicious activity.

- **Figure 9**

  ThreatQ's record that the malicious filename is associated with a MD5 hash. Using Open Malware website, downloading a sample of the same filename.

- **Figure 10**

  Putting the malicious file on the Windows 7 virtual machine.

- **Figure 11**

  Performing an FTP between the Windows 7 machine and the Engineering Workstation machine. At the same time, SNORT alerting to the malicious action.

Appendix

File hashes

Table 4

Sample names and hashes

MD5	File compilation date	File name	Comment
0a566b1616c8afeef214372b1a0580c7	7/17/2011 7:12	cmi4432.pnf	Encrypted DLL loaded by cmi4432.sys
0eecd17c6c215b398b7b872b74bf4808	11/3/2010 17:25	jminet7.sys	Originally discovered file
3B51F48378A26F664BF26B32496BD72A		adp55xx.sys	Sys file
3d83b077d32c422d6c7016b5083b9fc2	10/17/2011 20:06	adpu321.sys	Sys file obtained from VirusTotal
4541e850a228eb69fd0f0e924624b245	11/3/2010 17:25	cmi4432.sys	Originally discovered file
4c804ef67168e90da2c3da58b60c3d16	10/18/2011 1:07	N/A	Recon DLL pushed by the C&C
7A331793E65863EFA5B5DA4FD5023695	11/4/2010 16:48	iddr021.pnf	main dll
856a13fcae0407d83499fc9c3dd791ba	10/18/2011 0:26	N/A	"Lifetime" updater pushed by C&C
92aa68425401ffedcfba4235584ad487	8/10/2011 5:37	N/A	Reduced functionality infostealer pushed by C&C
94c4ef91dfcd0c53a96fdc387f9f9c35		netp192.pnf	Config file loaded by netp191.PNF
9749d38ae9b9ddd81b50aad679ee87ec	6/1/2011 3:25	keylogger.exe	Originally discovered infostealer
a0a976215f619a33bf7f52e85539a513	10/17/2011 20:06		igdkmd16b.sys
a1d2a954388775513b3c7d95ab2c9067	11/3/2010 10:25		nfred965.sys
b4ac366e24204d821376653279cbad86	11/4/2010 16:48	netp191.PNF	Encrypted DLL loaded by jminet7.sys
c9a31ea148232b201fe7cb7db5c75f5e	10/17/2011 20:06	nfred965.sys	Sys file obtained from European organization
dccffd4d2fc6a602bea8fdc1fa613dd4		allide1.sys	
e8d6b4dadb96ddb58775e6c85b10b6cc		cmi4464.PNF	Config file loaded by cmi4432.pnf
f60968908f03372d586e71d87fe795cd	11/3/2010 17:25	nred961.sys	Sys file obtained from European organization

Diagnostics

The following traces may indicate an infection of Duqu:

- Unexpected connections to 206.183.111.97 or 77.241.93.160.
- The existence of the following registry entry:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\"CFID"
- Unknown drivers in %System%\Drivers\.
- A services registry subkey with the following attributes:
  - "ImagePath" matching the unknown driver found in %System%\Drivers
  - "Start" = "1"
  - "Type" = "1"
  - "FILTER" has unknown hex data for a value
  - "DisplayName", "Description", and "keyname" all match
- Drivers signed by unknown publishers that expire on August 2, 2012.

Page 21

Figure 6. Duqu screenshot - IOCs associated with Duqu.

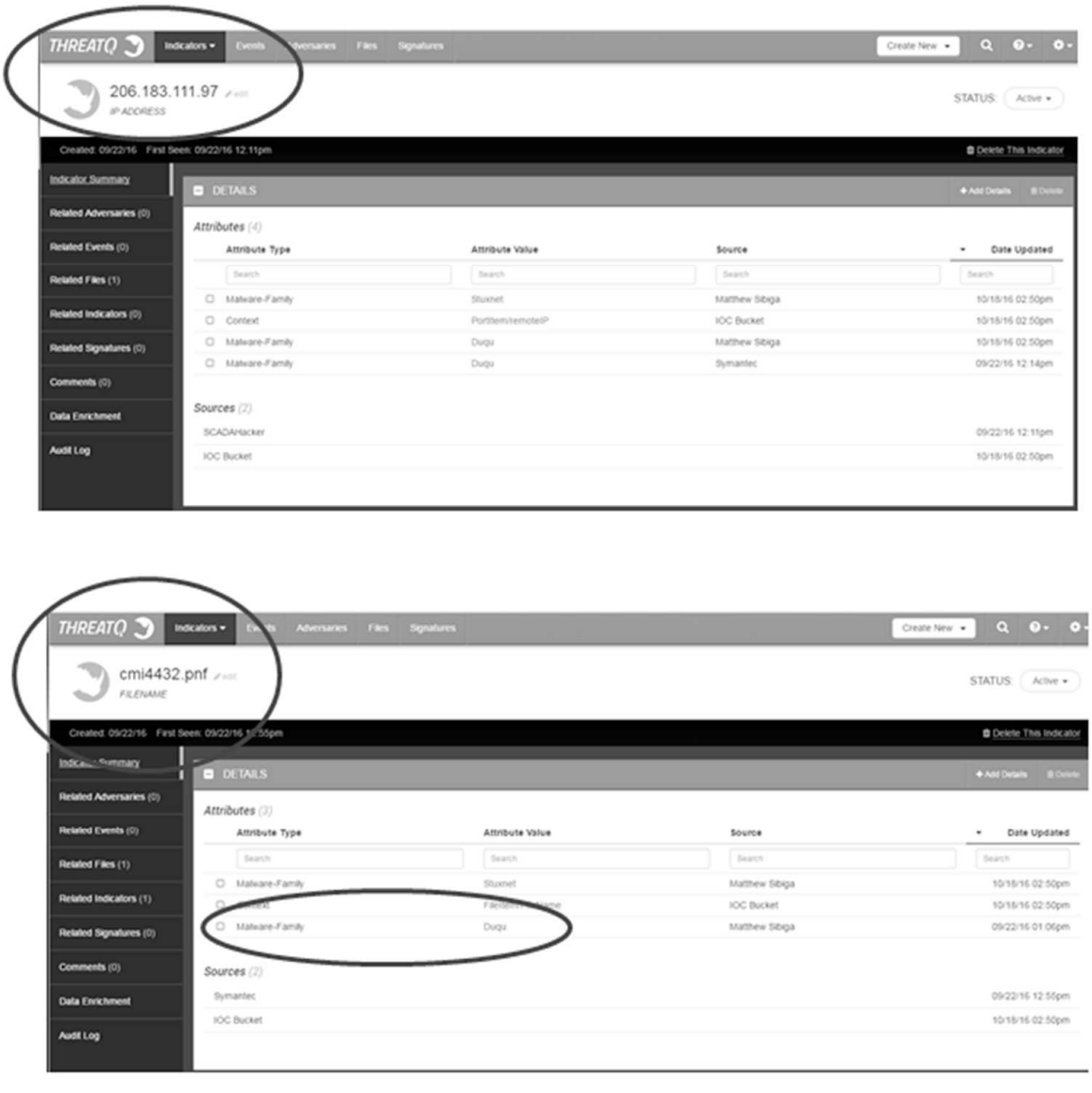
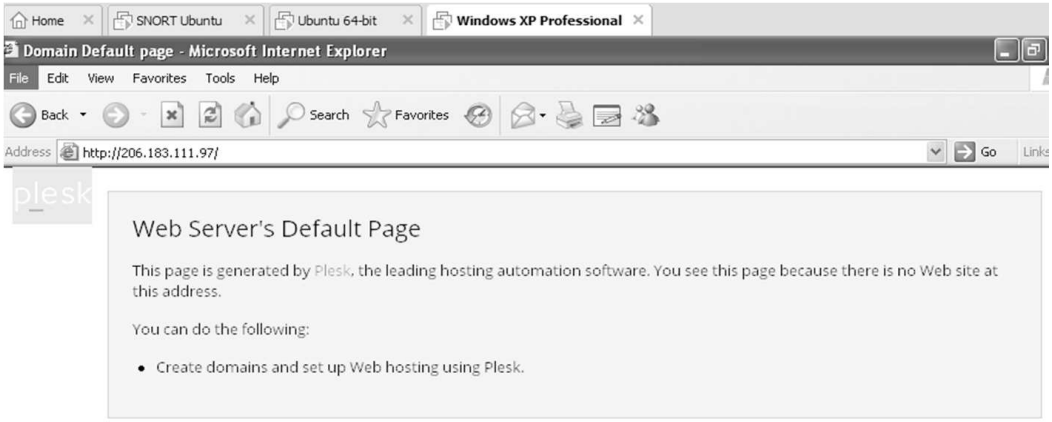


Figure 7. Duqu screenshot - ThreatQ record.




```
10/25-11:20:48.484187  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1218
10/25-11:20:48.484187  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1218
10/25-11:20:48.484407  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.484407  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.484860  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.484860  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.749591  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1218
10/25-11:20:48.749591  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1218
10/25-11:20:48.901795  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.901795  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.904542  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.904542  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:48.905098  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:48.905098  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.120833  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.120833  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.120921  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.120921  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.121228  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.121228  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.137549  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:49.137549  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1218 -> 206.183.111.97:80
10/25-11:20:49.350910  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350910  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350927  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350927  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350930  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350930  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350939  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.350939  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.351133  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.351133  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.351313  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.351313  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.566920  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.566920  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.567071  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.567071  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.567163  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.567163  [**] [1:500003:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
10/25-11:20:49.567174  [**] [1:500002:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.567174  [**] [1:500000:1] Malicious IP discovered [**] [Priority: 0] {TCP} 206.183.111.97:80 -> 10.1.5.103:1219
10/25-11:20:49.567474  [**] [1:500005:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1219 -> 206.183.111.97:80
```

Figure 8. Duqu screenshot - Visiting IP and SNORT alerting.

Found 1 Result(s) for 0a566b1616c8afeef214372b1a0580c7:

MD5:	0a566b1616c8afeef214372b1a0580c7
SHA1:	192f3f7c40fa3aaa4978ebd312d96447a061a473
SHA256:	84116fffa72a50d4c5f63f284c589dfd7afa0a2954fb6408a440dd673b88aa91
OCID:	4039405883
Original Filename:	0a566b1616c8afeef214372b1a0580c7
Added:	2011-11-08 12:40:37.93579
AV Results:	**ClamAV:** Trojan.Duqu-2
Other Information:	Virustotal ThreatExpert
Download:	Download Sample - Authentication Required. Sample password is "infected"

Figure 9. Duqu screenshot - Downloading malicious filename.

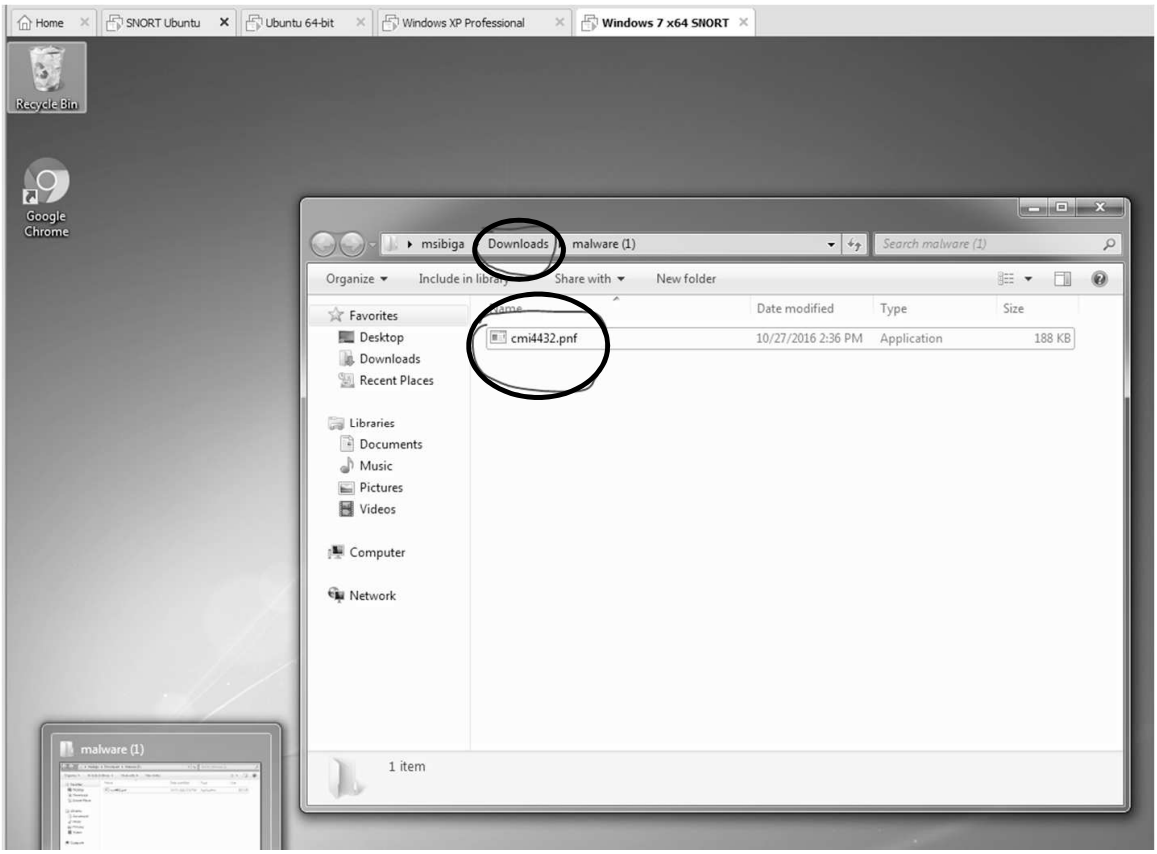


Figure 10. Duqu screenshot - File on Windows 7 machine.

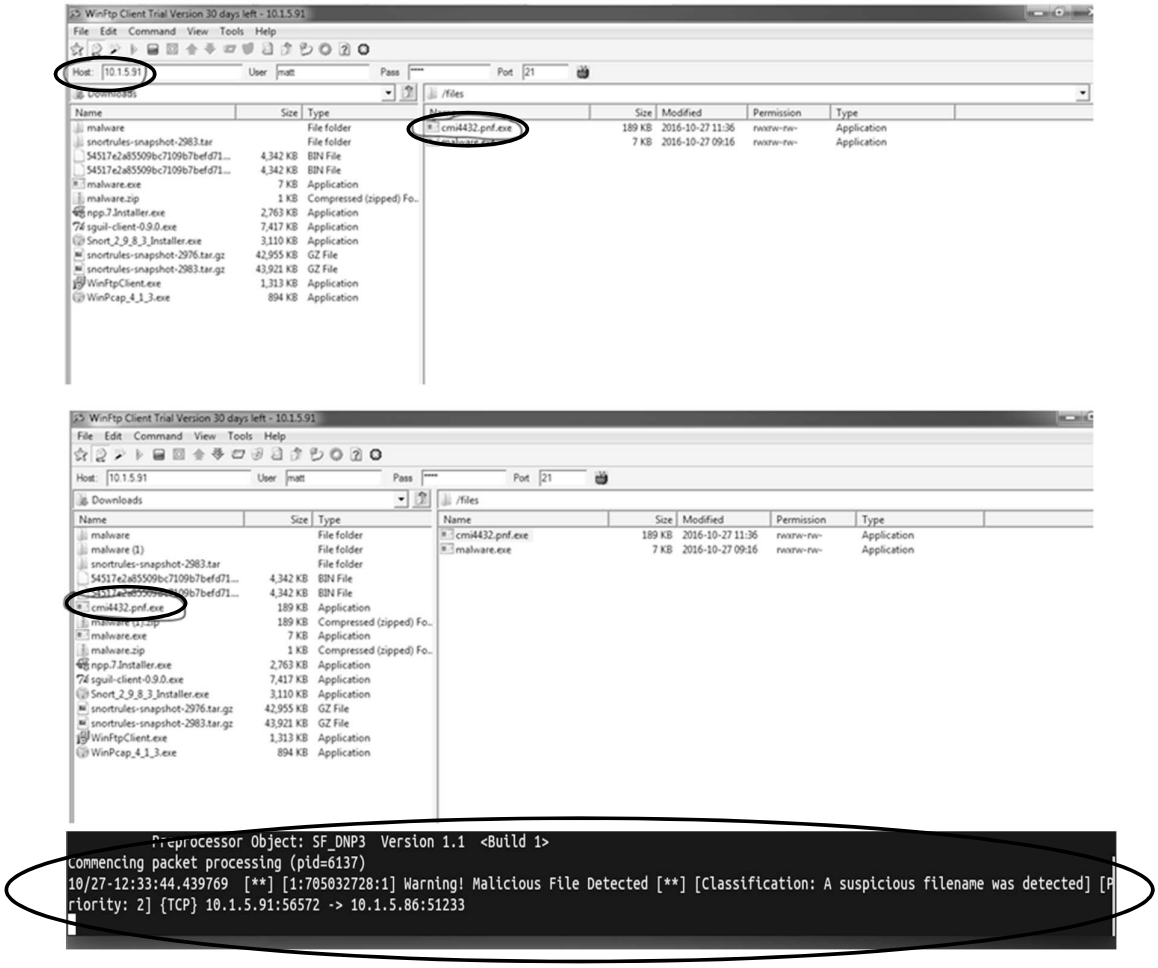


Figure 11. Duqu screenshot - FTP and SNORT alerting.

Appendix C. Screenshots of Havex Expirement

C.1 Havex

The following screenshots were taken during the Havex experiment. Here is a brief description of each:

- **Figure 12**

  Part of Havex's all-inclusive IOC spreadsheet from ICS-CERT's secure portal with a FQDN circled. ThreatQ's record of the IOC and it's association to Havex.

- **Figure 13**

  Using the Windows 7 virtual machine and visting the FQDN with an Internet browser. At the same time, SNORT is alerting to the malicious activity.

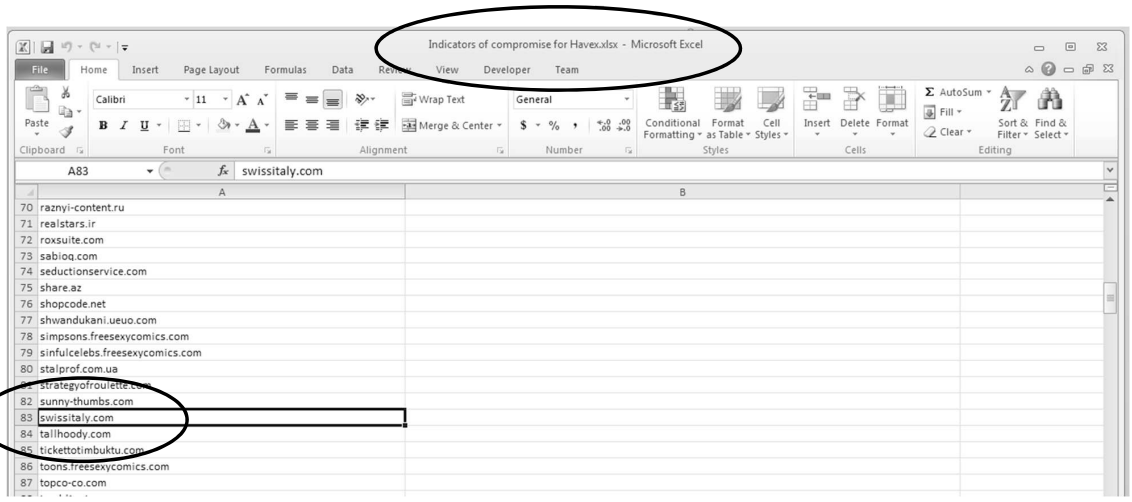


Figure 12. Havex screenshot - ThreatQ record.

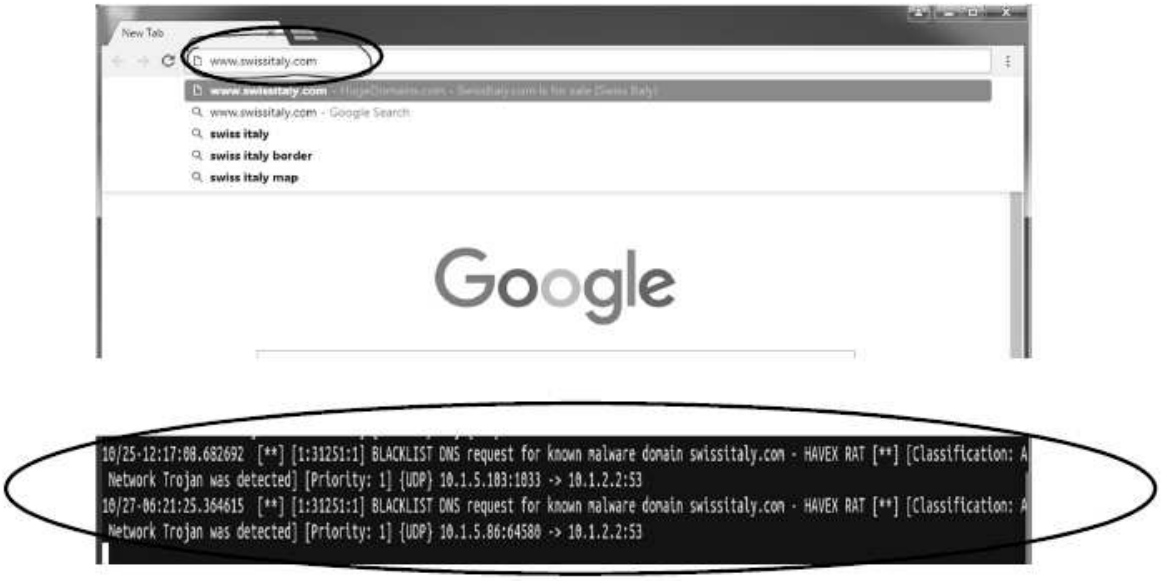


Figure 13. Havex screenshot - Visiting FQDN and SNORT alerting.

Appendix D. Sample of SNORT Rules

The following screenshots are a small sample of SNORT rules that were created by scripts and ThreatQ's export tool. Here is a brief description of each:

- **Figure 14**

  Sample rules for any TCP, UDP and IP protocol connection to any noted bad IP address. Connections from either inside or outside the trusted network on any port is evaluated.

- **Figure 15**

  Sample rules for any noted bad filenames. Connections from either inside or outside the trusted network on any port is evaluated.

```
 1 # Block bad IP
 2 alert tcp 206.183.111.97 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500000; rev:1;)
 3 alert udp 206.183.111.97 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500001; rev:1;)
 4 alert ip 206.183.111.97 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500002; rev:1;)
 5 alert tcp $HOME_NET any -> 206.183.111.97 any (msg: "Malicious IP discovered"; sid:500003; rev:1;)
 6 alert udp $HOME_NET any -> 206.183.111.97 any (msg: "Malicious IP discovered"; sid:500004; rev:1;)
 7 alert ip $HOME_NET any -> 206.183.111.97 any (msg: "Malicious IP discovered"; sid:500005; rev:1;)
 8 alert tcp 77.241.93.160 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500006; rev:1;)
 9 alert udp 77.241.93.160 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500007; rev:1;)
10 alert ip 77.241.93.160 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500008; rev:1;)
11 alert tcp $HOME_NET any -> 77.241.93.160 any (msg: "Malicious IP discovered"; sid:500009; rev:1;)
12 alert udp $HOME_NET any -> 77.241.93.160 any (msg: "Malicious IP discovered"; sid:500010; rev:1;)
13 alert ip $HOME_NET any -> 77.241.93.160 any (msg: "Malicious IP discovered"; sid:500011; rev:1;)
14 alert tcp 111.248.118.89 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500012; rev:1;)
15 alert udp 111.248.118.89 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500013; rev:1;)
16 alert ip 111.248.118.89 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500014; rev:1;)
17 alert tcp $HOME_NET any -> 111.248.118.89 any (msg: "Malicious IP discovered"; sid:500015; rev:1;)
18 alert udp $HOME_NET any -> 111.248.118.89 any (msg: "Malicious IP discovered"; sid:500016; rev:1;)
19 alert ip $HOME_NET any -> 111.248.118.89 any (msg: "Malicious IP discovered"; sid:500017; rev:1;)
20 alert tcp 115.28.45.82 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500018; rev:1;)
21 alert udp 115.28.45.82 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500019; rev:1;)
22 alert ip 115.28.45.82 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500020; rev:1;)
23 alert tcp $HOME_NET any -> 115.28.45.82 any (msg: "Malicious IP discovered"; sid:500021; rev:1;)
24 alert udp $HOME_NET any -> 115.28.45.82 any (msg: "Malicious IP discovered"; sid:500022; rev:1;)
25 alert ip $HOME_NET any -> 115.28.45.82 any (msg: "Malicious IP discovered"; sid:500023; rev:1;)
26 alert tcp 118.174.39.154 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500024; rev:1;)
27 alert udp 118.174.39.154 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500025; rev:1;)
28 alert ip 118.174.39.154 any -> $HOME_NET any (msg: "Malicious IP discovered"; sid:500026; rev:1;)
29 alert tcp $HOME_NET any -> 118.174.39.154 any (msg: "Malicious IP discovered"; sid:500027; rev:1;)
30 alert udp $HOME_NET any -> 118.174.39.154 any (msg: "Malicious IP discovered"; sid:500028; rev:1;)
```

Figure 14. Sample of SNORT bad IP rules.

```
1 # Malicious Filenames
2 alert tcp any any -> $HOME_NET any (sid:5000000000; rev:1; msg:"Warning! Malicious File Detected"; content:"
  nred961.sys"; classtype:suspicious-filename-detect;)
3 alert udp any any -> $HOME_NET any (sid:5000000001; rev:1; msg:"Warning! Malicious File Detected"; content:"
  nred961.sys"; classtype:suspicious-filename-detect;)
4 alert tcp any any -> $HOME_NET any (sid:5000000002; rev:1; msg:"Warning! Malicious File Detected"; content:"
  cmi4464.pnf"; classtype:suspicious-filename-detect;)
5 alert udp any any -> $HOME_NET any (sid:5000000003; rev:1; msg:"Warning! Malicious File Detected"; content:"
  cmi4464.pnf"; classtype:suspicious-filename-detect;)
6 alert tcp any any -> $HOME_NET any (sid:5000000004; rev:1; msg:"Warning! Malicious File Detected"; content:"
  allide1.sys"; classtype:suspicious-filename-detect;)
7 alert udp any any -> $HOME_NET any (sid:5000000005; rev:1; msg:"Warning! Malicious File Detected"; content:"
  allide1.sys"; classtype:suspicious-filename-detect;)
8 alert tcp any any -> $HOME_NET any (sid:5000000006; rev:1; msg:"Warning! Malicious File Detected"; content:"
  nfred965.sys"; classtype:suspicious-filename-detect;)
9 alert udp any any -> $HOME_NET any (sid:5000000007; rev:1; msg:"Warning! Malicious File Detected"; content:"
  nfred965.sys"; classtype:suspicious-filename-detect;)
10 alert tcp any any -> $HOME_NET any (sid:5000000008; rev:1; msg:"Warning! Malicious File Detected"; content:"
  netp191.pnf"; classtype:suspicious-filename-detect;)
11 alert udp any any -> $HOME_NET any (sid:5000000009; rev:1; msg:"Warning! Malicious File Detected"; content:"
  netp191.pnf"; classtype:suspicious-filename-detect;)
12 alert tcp any any -> $HOME_NET any (sid:5000000010; rev:1; msg:"Warning! Malicious File Detected"; content:"
  keylogger.exe"; classtype:suspicious-filename-detect;)
13 alert udp any any -> $HOME_NET any (sid:5000000011; rev:1; msg:"Warning! Malicious File Detected"; content:"
  keylogger.exe"; classtype:suspicious-filename-detect;)
14 alert tcp any any -> $HOME_NET any (sid:5000000012; rev:1; msg:"Warning! Malicious File Detected"; content:"
  netp192.pnf"; classtype:suspicious-filename-detect;)
15 alert udp any any -> $HOME_NET any (sid:5000000013; rev:1; msg:"Warning! Malicious File Detected"; content:"
  netp192.pnf"; classtype:suspicious-filename-detect;)
```

Figure 15. Sample of SNORT bad filenames rules.

Appendix E. Validation Screenshots

The following screenshots are provided to show that SNORT was configured and set up correctly and that it analyzed network traffic packets correctly.

- **Figure 16**

  By using the command 'sudo snort -c /etc/snort/snort.conf -T', SNORT will test configuration. The rules will be tested along varies other components. A message stating that SNORT successfully validated configuration will appear and then will promptly exit when test is complete.

- **Figure 17**

  A local rule was inputted into SNORT to test packet analysis; 'alert tcp $HOME_NET any ->$EXTERNAL_NET any (msg: "Out Traffic detected"; sid: 1000000000000)'. The command 'sudo snort -c /etc/snort/snort.conf -A console -i eth0' will initialize packet capture and analysis on the first ethernet interface. By visiting google.com, the SNORT console displayed the traffic. Upon exiting SNORT, statistics were shown to the user regarding packet analysis.

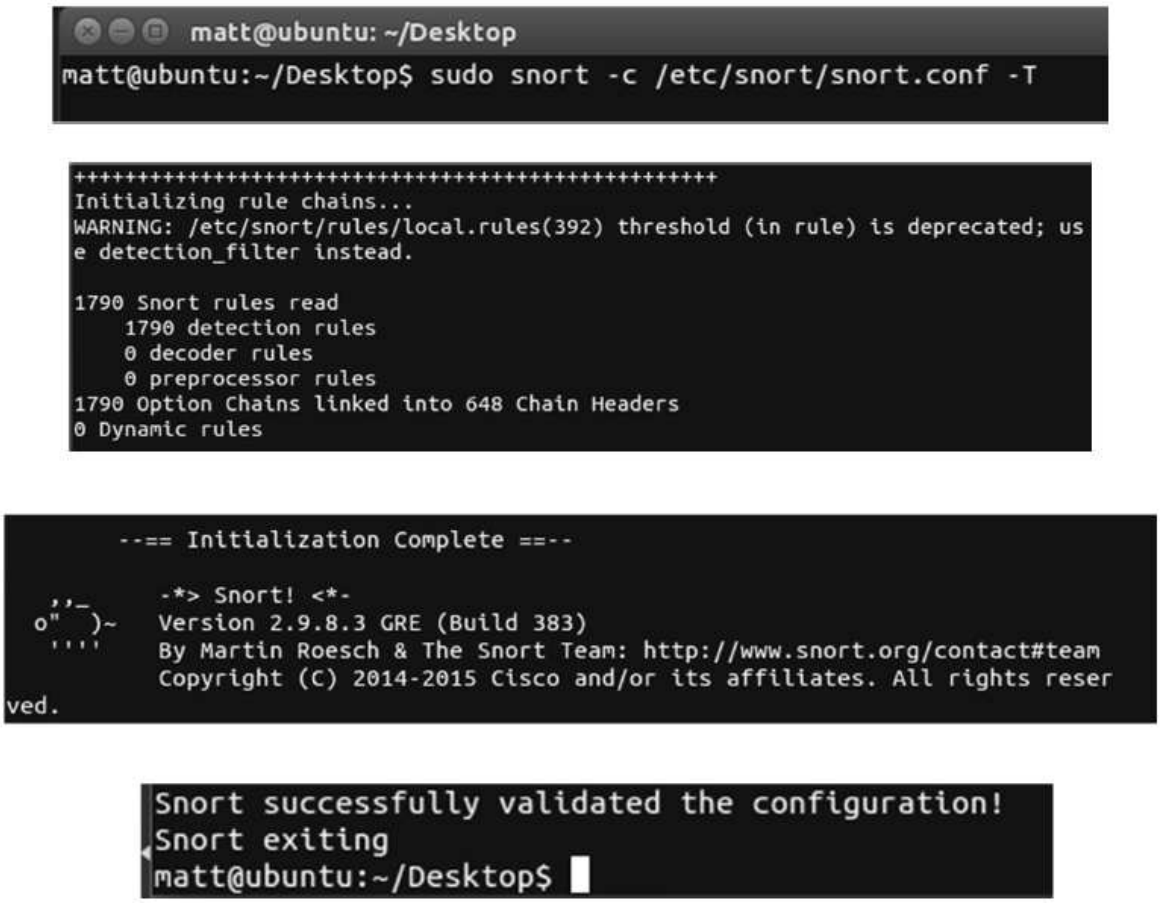


Figure 16. SNORT validation.

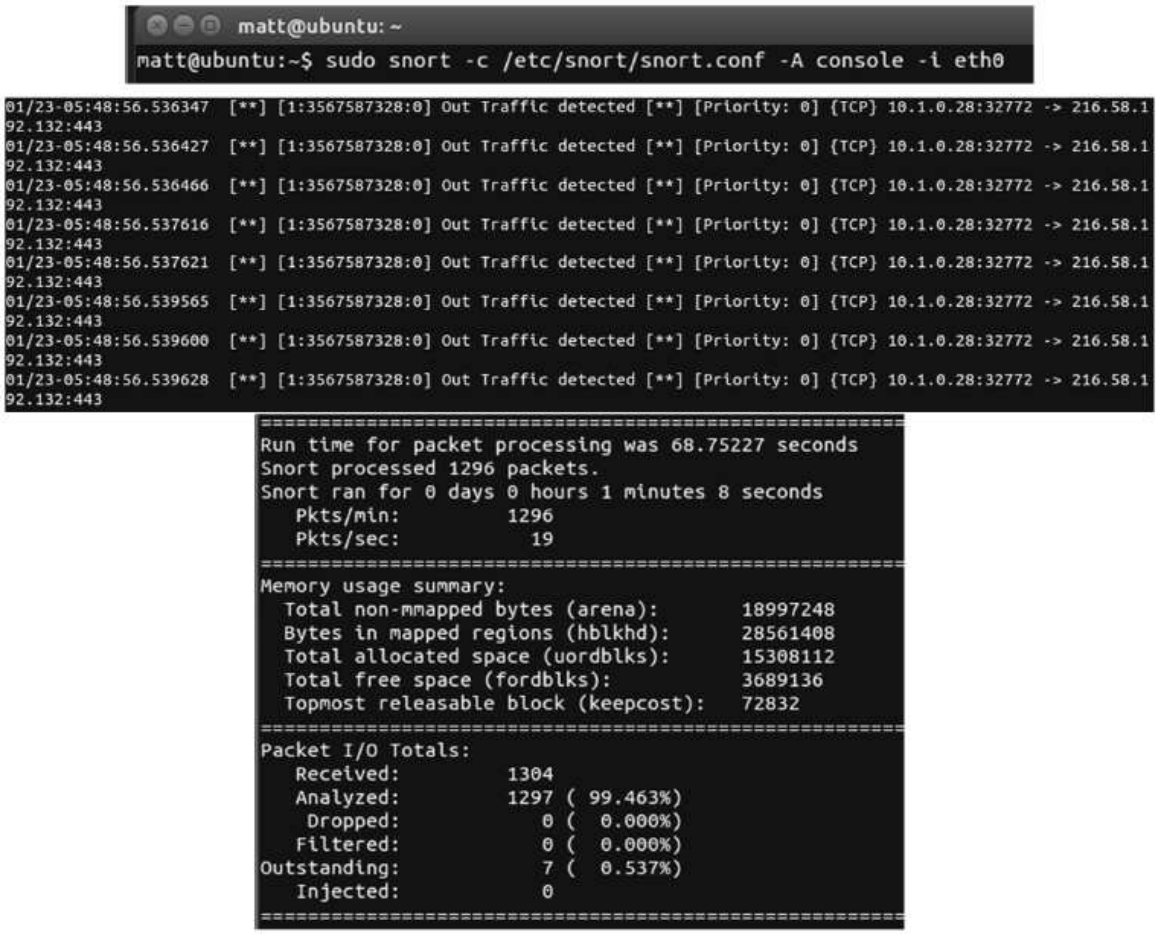


Figure 17. Packet validation.

Bibliography

1. O. Andreeva, S. Gordeyshik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. Sidorov and A. Timorin, Industrial Control Systems Vulnerabilities Statistics, Kaspersky Lab, Moscow, Russian Federation (kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf), 2016.

2. M. Assante and R. Lee, The Industrial Control System Cyber Kill Chain, InfoSec Reading Room, SANS Institute, Bethesda, Maryland (www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297), 2015.

3. T. Bartman and J. Kraft, An introduction to applying network intrusion detection for industrial control systems, presented at *AISTech*, 2016.

4. M. Chipley, Cybersecuring DoD industrial control systems presentation, presented at the *Ninth Annual ICS Security Summit*, 2014.

5. Earnest and Young, Cyber Threat Intelligence – How to Get Ahead of Cybercrime, London, United Kingdom (www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime//$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf), 2014.

6. J. Friedman and M. Bouchard, *Definitive Guide to Cyber Threat Intelligence*, CyberEdge Group, Annapolis, Maryland, 2015.

7. C. Geyer, OASIS Advances Automated Cyber Threat Intelligence Sharing with STIX, TAXII, CybOX, OASIS, Burlington, Masssachusetts

(www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox), 2015

8. W. Gragido, Understanding Indicators of Compromise (IOC) Part I, RSA Blogs, RSA, Bedford, Massachusetts (blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i), 2012.

9. R. Holland, State of Cyber Threat Intelligence Address, presented at the *Cyber Threat Intelligence Summit*, (digital-forensics.sans.org/summit-archives/cti2015/State-of-Cyber-Threat-Intelligence-Address--Rick-Holland-Forrester-Research.pdf), 2015.

10. M. Horkan, Challenges for IDS/IPS Deployment in Industrial Control Systems, InfoSec Reading Room, SANS Institute, Bethesda, Maryland (www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127), 2015.

11. Industrial Control Systems Cyber Emergency Response Team, Advisory (IR-ALERT-H-16-043-01BP), Cyber-Attack Against Ukrainian Critical Infrastructure, U.S. Department of Homeland Security, Washington, DC, 2016.

12. iSight Partners, What Is Cyber Threat Intelligence and Why Do I Need It? Dallas, Texas, 2014.

13. Joint Improvised Explosive Device Defeat Organization, Counter-Improvised Explosive Device Strategic Plan, Washington, DC (www.defenseinnovationmarketplace.mil/resources/20120116_JIEDDO_C-IEDStrategicPlan.pdf), 2012.

14. Kaspersky Lab, Energetic Bear – Crouching Yeti, Moscow, Russian Federation (securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf), 2014.

15. E. Kovacs, Critical Infrastructure Incidents Increased in 2015: ICS-CERT, Security Week, Charlestown, Massachusetts (www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert), 2016.

16. J. Langill, Defending Against the Dragonfly Cyber Security Attacks, Belden, Saint Louis, Missouri (www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf), 2014.

17. C. Lawson and R. McMillan, Technology Overview for Threat Intelligence Platforms Training, Gartner, Stamford, Connecticut, 2014.

18. R. Lee, M. Assante and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity – Information Sharing and Analysis Center, Washington, DC (ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf), 2016.

19. N. Nelson, The Impact of Dragonfly Malware on Industrial Control Systems, InfoSec Reading Room, SANS Institute, Bethesda, Maryland (www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672), 2016.

20. B. Obama, Fact Sheet: Cyber Threat Intelligence Integration Center, The White House, Washington, DC (www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center), 2015.

21. Phantom Cyber, Apps, Palo Alto, California (my.phantom.us/2.0/apps/), 2016.

22. D. Shackleford, Whos Using Cyberthreat Intelligence and How? InfoSec Reading Room, SANS Institute, Bethesda, Maryland (www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767), 2015.

23. Symantec, W32.Duqu: The Precursor to the Next Stuxnet, Mountain View, California (www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf), 2011.

24. ThreatConnect, Go Deeper and Discover New Intelligence With ThreatConnect, Arlington, Virginia, (www.threatconnect.com/wp-content/uploads/ThreatConnect-Case-Study-Go-Deeper-and-Discover-New-Intelligence-with-ThreatConnect1.pdf), 2016.

25. ThreatConnect, This Is How We Do It: A Financial Giant's Threat Intel Success Story, Arlington, Virginia (www.threatconnect.com/wp-content/uploads/ThreatConnect-CaseStudy-FSV1-1.pdf), 2016.

26. ThreatConnect, Threat Intelligence Platforms: Everthing You've Ever Wanted to Know But Didnt Know to Ask, Arlington, Virginia (cdn2.hubspot.net/hubfs/454298/ebook/Threat-Intel-Platform-ebook-ThreatConnect.pdf), 2015.

27. T. Townsend, M. Ludwick, J. McAllister, A. Mellinger and K. Sereno, SEI Innovation Center Report: Cyber Intelligence Tradecraft (Summary of Key

Findings), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2013.

28. R. Trost, ThreatQ's Instant ROI to Standardize Intelligence Workflows in the Enterprise, ThreatQuotient, Reston, Virginia (www.infosecurityeurope.com/__novadocuments/242948?v=636008140463830000), 2016.

29. U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center, Washington, DC (www.dhs.gov/national-cybersecurity-and-communications-integration-center), 2016.

30. U.S. Department of Homeland Security, TRIPwire Fact Sheet, Washington, DC (www.dhs.gov/sites/default/files/publications/OBP-TRIPwire-Fact-Sheet-508.pdf), 2013.

31. K. Wilhoit, Who's Really Attacking Your ICS Equipment?, Trend Micro, Irving, Texas (www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf), 2013.

32. B. Zhu, A. Joseph and S. Sastry, A taxonomy of cyber attacks on SCADA systems, *Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing*, pp. 380-388, 2011.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
23–03–2017	Master's Thesis	May 2015 — Mar 2017

4. TITLE AND SUBTITLE

Applying Cyber Threat Intelligence to Industrial Control Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sibiga, Matthew, P, Major, USAF

5d. PROJECT NUMBER

17G310

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-17-M-069

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of Homeland Security ICS-CERT
POC: Neil Hersheld, DHS ICS-CERT Technical Lead
ATTN: NPPD/CSC/NCSD/US-CERT Mailstop: 0635
245 Murray Lane, SW, Bldg 410, Washington, DC 20528
Email: ics-cert@dhs.gov Phone: 1-877-776-7585

10. SPONSOR/MONITOR'S ACRONYM(S)

DHS ICS-CERT

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subjtect to copyright protection in the United States.

14. ABSTRACT

A cybersecurity initiative known as cyber threat intelligence (CTI) has recently been developed and deployed. The overall goal of this new technology is to help protect network infrastructures. Threat intelligence platforms (TIPs) have also been created to help facilitate CTI effectiveness within organizations. There are many benefits that both can achieve within the information technology (IT) sector. The industrial control system (ICS) sector can also benefit from these technologies as most ICS networks are connected to IT networks. CTI and TIPs become resourceful when using indicators of compromise (IOCs) from known ICS malware attacks and an open source intrusion detection system (IDS). This research shows how these IT-based technologies may help protect ICS. Three known malware attack scenarios are used to showcase its likely deployment. These scenarios are well-documented campaigns that targeted ICS environments and consisted of numerous IOCs. Equipped with this data, critical asset owners can obtain situational awareness on potential attacks and protect their devices with the proper implementation of CTI and TIP technologies.

15. SUBJECT TERMS

Cyber threat intelligence, threat intelligence platform, ICS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert Mills, AFIT/ENG
U	U	U	U	67	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4527; rmills@afit.edu