Carnegie Mellon University
Software Engineering Institute

AN UPDATED FRAMEWORK OF DEFENSES AGAINST RANSOMWARE

Timur D. Snoke
Timothy J. Shimeall
CERT Situational Awareness Group
May 2020

Table of Contents

Executive Summary

The proliferation of tools and techniques to disrupt enterprise systems has evolved from those capable of supporting merely opportunistic attacks to those enabling targeted attacks. Furthermore, attackers continue to develop methods for monetizing their efforts, resulting in ransomware, a very disruptive threat to business as well as governmental departments and agencies. Ransomware developers are now selling their tools as a service, enabling attackers (individual criminals, organized crime, ideological hackers, or nation-state teams, all hereafter referred to as *affiliates*) to use tools they do not build or maintain to attack vulnerable systems.

In the last few years we have seen a rise of successful ransomware affiliates that purchase the malware that they use and incorporate it into a ransomware tool chain that is targeted to a specific victim. These

attackers lock victims out of their own data, usually by encrypting it, and attempt to extort money to restore the victim's access to the enterprise data under threat of data destruction or disclosure as a response for non-payment. Recent high-profile cases, including attacks on FedEx subsidiary TNT Express, shipping company Pitney Bowes, and national postal service Pos Malaysia, all attest to the seriousness of the problem. In each case, the victims suffered operational disruptions (delayed mail, abandoned mail, or mail referred to other carriers) with monetary losses (both lost revenue and large recovery expenses).

This report, loosely structured around the *NIST Cybersecurity Framework*, seeks to frame an approach for defending against Ransomware-as-a-Service (RaaS) as well as direct ransomware attacks. The recommendations from this report, listed with the *NIST Cybersecurity Framework* functions, are as follows.

- Identify
  - Perform asset management for physical devices, clients, servers, data, software platforms, and applications. Ensure that the documentation reflects current inventory status and includes information about business use and stakeholders.
  - Document possible infection vectors, malware propagation mechanisms, and access methods for the assets that are publicly exposed in a way that allows estimation of the downstream risk to the internal assets in the organization.
  - Assign priority to assets based on their business value, criticality, and classification. Ensure a strategy that allocates resources (e.g., skilled personnel and time) in alignment with asset priority and assumed risk when issues arise.
- Protect
  - Perform regular backup, augmented with validation and encryption. Ensure that data content is clean and accurate, that recovery works as desired, and that media is protected from loss and corruption.
  - Mitigate against social engineering attacks, which allow attackers to gain a foothold in the organization network. Train users against probable methods, and supplement training with exercises.
  - Practice proactive software hygiene, including maintaining user awareness, performing regular vulnerability management, hardening deployed systems, and improving network defenses. Focus these activities around public (likely targeted) hosts, mission-critical servers, and workstations of personnel serving in a public-facing manner.
- Detect
  - Inform and motivate users to report social engineering, reconnaissance activity, and ransomware-indicative network activity. Provide training that builds on the social engineering awareness training recommended in the Protect function and supplement the training with exercises.
  - Deploy and maintain robust malware detection applications, including anti-malware software, host-based intrusion detection software (IDS), and host-based intrusion prevention software. Deploy these applications throughout the organization and configure them to report

to a central logging location. Update rule sets, signature databases, and clock settings to provide coordinated alerts.
  - With the centralized logging information, analyze for behavioral indicators relevant to ransomware. Correlate positive analytic results to generate appropriate alerts for Respond and Recover actions.
- Respond
  - Develop a plan that guides incident response to protect data integrity and support business continuity.
  - Develop communications channels in which stakeholders can safely express updates and move forward on their piece of the response.
  - Establish standards for creating tickets that include all of the information needed to support decision makers and communication with other stakeholders. Use the standards for help in scoping and understanding the impact of the incident.
- Recover
  - Restore lost data from recent backups or collateral storage if at all possible, paying the ransom only as a last resort. Inform this restoration using the relationships documented through the Identify function.
  - Restore lost software from known-good install media, applying sufficient updates to deal with all currently known vulnerabilities. Move the network into a known and defensible state before doing other recover activities.
  - Report any attack to appropriate law enforcement. Report through trusted channels to help to protect other organizations, including your vendors and customers.
  - Revise software configurations, network defenses, traffic and host monitoring, user training, and operational procedures. Proactively strengthen the network to deal with predictable attacks after a successful ransomware attack.

Overview and Introduction

Of the many threats facing corporate networks, ransomware deserves attention as a notable vector for a variety of attacks on data. Several recent high-profile cases highlight the magnitude of the problem. In 2017, FedEx subsidiary TNT Express suffered a ransomware attack when that subsidiary became infected by installing a tax software update that contained malware [BBC 2017]. The attack reduced the company to manual pickup, sort, and delivery processes, and FedEx projected $300 million in losses. In 2019, the large shipping company Pitney Bowes suffered a ransomware attack that disrupted operations among its 1.5 million customers and tarnished the shipper's reputation. Also, in 2019, national postal service Pos Malaysia suffered a ransomware attack that knocked out a number of its online services [E Hacking News 2019]. The attack disrupted Pos Malaysia's internal services as well as online services to its customers. Recovery was gradual and painstaking.

Ransomware is a form of malicious software (called malware) that encrypts data on an infected system and sends a ransom notice to the victim demanding payment for the decryption key. Ransomware is a class of malicious code that is considered a data integrity threat. The infection vector for ransomware is often delivered through spear phishing campaigns, malvertising, or targeted exploit kits [Cisco 2017].

Attackers generally deploy ransomware after gaining a foothold on the network to encrypt specific files on the local system or network shares. The attackers notify the victim of their actions and communicate their demands for unencrypting the data. Frequently those demands have included payment via cryptocurrency, such as bitcoin, to produce a decryption key and method for recovery. Some attackers have used malicious code that would look like ransomware, but instead of decrypting the files would wipe the files. This class of malicious code is called a wiper. Some examples of poorly written ransomware have been observed, and recovery is not guaranteed even if given the right key and process.

Attackers apply many different attack patterns that include ransomware. For instance, in addition to data encryption, ransomware may include capabilities of other malware, such as keylogging, data exfiltration, and automated propagation of the attack to other systems. For a detailed look at ransomware attacks and common ransomware varieties, see the report *Current Ransomware Threats* [Midler 2020].

Ransomware is not a single malicious tool; rather, it is a part of a tool chain. This chain starts with tools that breach company networks and establish a foothold (known as a *vector of compromise* or *infection vector*). The chain continues to perform actions on victim company networks by compromising data assets, involving encryption or exfiltration of the assets. Finally, the chain includes capabilities to extort a business or individual, including notification to the victim, payment processing, and possibly restoration once payment is made. So to protect against ransomware, an organization needs to decrease the attack surface that allows the attacker a foothold in the network. Given that attackers employ multiple vectors of compromise to get ransomware on the network, the organization must understand the network. Such understanding allows the organization to track risk and maintain the dependencies on the network that support business continuity.

Ransomware capabilities are evolving at an ever-increasing pace. The first known ransomware, called AIDS TROJAN, from 1989 was spread by floppy disks. Modern ransomware incorporates characteristics of worms, making them self-propagating. Recently, a version of the ransomware Ryuk was reported using Wake-on-LAN to spread code to systems that are turned off [Hanel 2019]. Ryuk was also in the news as being the version of ransomware that hit Pitney Bowes at the end of 2019 [Kim 2019]. Another recent version of the EKANS ransomware was seen with crude abilities to impact industrial control systems (ICS) [Dragos 2020]. The threat of ransomware targeting ICS could have severe implications for business automation and systems, such as in a mail processing center. The ransomware Sodinokibi, also known as REvil and Sodin, started by exploiting flaws in vulnerable Oracle Weblogic systems and now are also targeting two different types of remote access services, Pulse and Fortinet VPN clients [Tung 2020]. As mentioned earlier, the combined set of features in modern ransomware allows attackers multiple paths to monetize their compromises and to evade network defenses.

Some attackers recently started to apply a Ransomware-as-a-Service (RaaS) work flow, in which affiliate groups (*affiliates* are not the ransomware creators, but individual criminals, organized crime, ideological hackers, or nation-state attackers) license and use it as part of a ransomware tool chain, along with money laundering services, data brokers, and other malicious capabilities (see **Error! Reference source not found.** for a visualization of the relationships involved). This model shields the ransomware creators from the risks of performing attacks and reduces the affiliates' cost to mount attacks. From the victim's point of view, the threat is only part of a larger threat ecosystem: attacks may involve components from a variety of developers, and multiple affiliates may be competing to compromise security. All of this makes identifying, protecting, detecting, responding, and recovering from a ransomware attack much more difficult.

In this report, we explain the requirements for mitigating the ransomware threat. We use the *NIST Cybersecurity Framework* to organize the content [NIST 2018b]. For each of the five functions of the framework, we present a set of activities that should be completed, or capabilities that should be implemented, as part of an organization's ransomware mitigation. The functions are Identify, Protect, Detect, Respond, and Recover. We will look at each of these in turn.

Model Ransomware-as-a-Service (RaaS)

As noted, the advent of RaaS means that affiliate attackers do not create or maintain the tools they deploy against the target network. Ransomware affiliates purchase the license to use the ransomware binaries and any other malware that they want to use on their campaign against an enterprise. This financial incentive on malware developers is resulting in a decreased development cycle and a more effective threat. This is resulting in newly disclosed proof-of-concept exploits being incorporated into malware within hours of disclosure.

Ransomware is now being bundled with additional capabilities beyond file encryption. These include key logging, screen grabs, data aggregation and exfiltration, cryptomining, and the means for automating their propagation throughout the network. Many of the attackers that are using ransomware are now creating data leak sites to punish the victims who do not pay [Abrams 2020a]. The adaptability of the ransomware tool chain makes it more successful against well-defended networks.

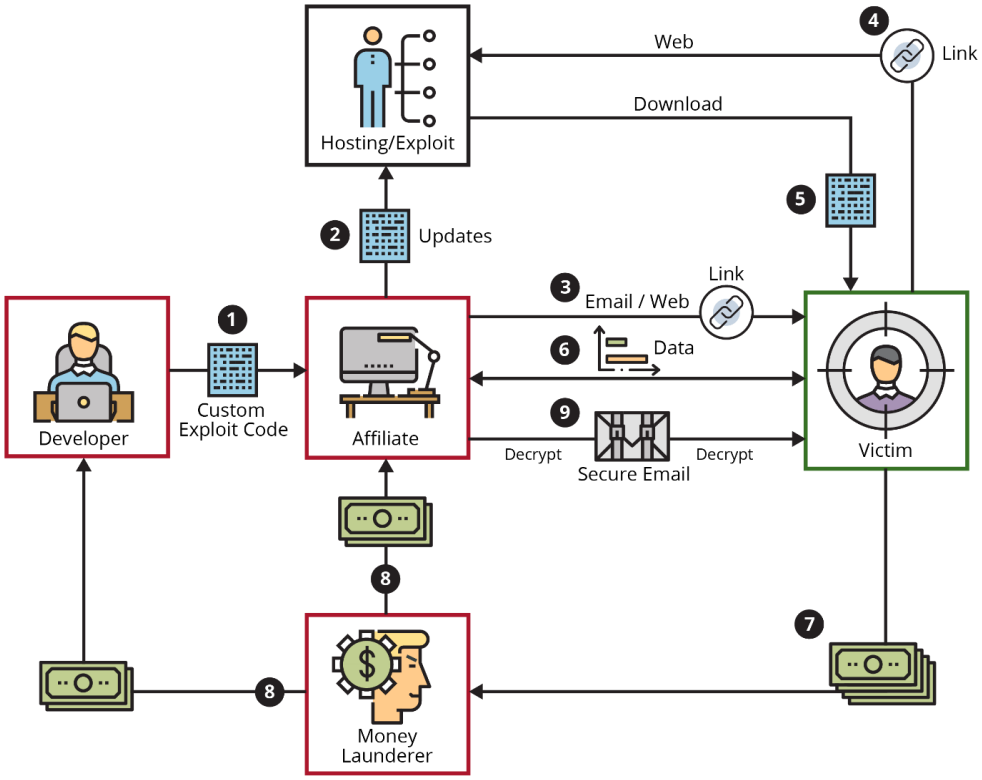

Figure 1: Ransomware-as-a-Service Workflow

Figure 1 portrays a workflow for an attack performed through RaaS. In this workflow the following steps occur:

1. The ransomware developer creates custom exploit code (leveraging specific vulnerabilities and targeting particular types of data), which is then licensed to a ransomware affiliate for a fee or a share in the proceeds from the attack.
2. The ransomware affiliate[1] takes the custom exploit code and updates the site that is hosting the exploit.
3. The ransomware affiliate identifies and targets an infection vector and delivers it to the victim. Such a vector could be an email to which a document embedded with malicious code it is attached, a link to an external site hosting the malicious code, a compromised website, code embedded in an otherwise-innocuous website, compromised adware (also known as malvertising), or abuse of some other service.

---

1 While this description will speak of "the affiliate," in practice a given developer may have multiple affiliates, and a given affiliate may use exploits and code from multiple developers. It is also true that multiple affiliates may attack the same victim organization, coordinating their attacks to a greater or lesser degree.

4. The vector entices the victim to open a link, and malicious content directly transfers from the hosting site. Or a user is induced to access the hosted exploit code (for instance, by opening an email attachment).
5. The ransomware is downloaded and exploits a system vulnerability to gain control, establishing a foothold in the network.
6. The ransomware affiliate uses the ransomware to access the enterprise systems. The attacker seeks local administrative rights, identifies files to extract and encrypt in place, scans the network to identify additional targets, modifies configurations to establish permanency, disrupts or destroys backups, and covers their tracks.
7. The attacker instructs the victim to pay a ransom using untraceable funds, such as a cryptocurrency, to a money launderer, also known as a tumbler. Often, the attacker may also threaten to publish the data as a consequence for non-payment, further motivating the victim to pay the ransom.
8. The money launderer will move the money through multiple transformations to obscure and protect the identities of the participants and split out shares to the ransomware developer and the affiliate.
9. On receiving payment, the ransomware affiliate might securely send the victim a means to decrypt and recover the affected files. Or it might make additional demands on the victim. Sometimes the affiliate takes no further action and leaves the victim with encrypted files.

Terminology

Ransomware refers to the specific type of cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid [Young 1996].

Cryptomining is "a process in which transactions for various forms of cryptocurrency are verified and added to the blockchain digital ledger" [Stroud 2020].

Data aggregation is "the process of gathering and combining data from different sources" [Schober 2020].

Exfiltration is "the unauthorized copying, transfer or retrieval of data from a computer or server" [Techopedia 2020].

Malvertising is "the use of online advertising to spread malware" [Salusky 2007].

Scanners are surveillance software that performs port or service enumeration. This activity is at least potentially observable on the victim network. Other forms of surveillance (human, open-source, electronic, physical, etc.) may not be as observable but may be used by ransomware affiliates to prepare for targeted attacks.

A *tumbler* is a money laundering resource that mixes cryptocurrency tokens to obscure transactions to the affiliate and ransomware developer [Phillips 2019].

Vector is "a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome" [Rouse 2012].

Identify

Recommendation 1: Perform asset management for physical devices, clients, servers, data, software platforms, and applications. Ensure that the documentation reflects current inventory status and includes information about business use and stakeholders.

Recommendation 2: Document possible infection vectors, malware propagation mechanisms, and access methods for the assets that are publicly exposed in a way that allows estimation of the downstream risk to the internal assets in the organization.

Recommendation 3: Assign priority to assets based on their business value, criticality, and classification. Ensure a strategy that allocates resources (e.g., skilled personnel and time) in alignment with asset priority and assumed risk when issues arise in alignment with asset priority and assumed risk.

The Identify function in the *NIST Cybersecurity Framework* seeks to define the known state of the enterprise, and the policy that governs it, to enable risk containment and mitigation. There are three main activities that need to be addressed in the Identify function to limit the impact of a ransomware-toolchain attack:

1. Identify the business services, functions, and data dependencies within the organization.
2. Document the assets[2] that support each of the business services and functions. This documentation should capture how the assets operate, who owns them, and how they should interconnect.
3. Determine the stakeholders for each asset, business service, and business function, both internal and external.

Though nothing in these steps is unique for ransomware threats, ransomware increases the emphasis needed on identifying the enterprise data, the devices that store and process it, and the business services and functions that use it.

In 2017, FedEx fell victim to a ransomware attack indirectly when a recent acquisition, TNT Express, was targeted as part of a campaign meant to disrupt the businesses active in Ukraine. Reports indicated the initial infection vector was an update to the tax software used in the Ukrainian office [BBC 2017]. This initial vector of compromise was a supply-chain attack wherein a malicious payload was placed where it would be accessed by the target and run in the targeted environment without being vetted. To respond to this threat, FedEx was forced to use external methods for communicating internally. Yet it decided to not turn away business, even though it was reduced to manual processes for pickup, sort, and delivery. FedEx projected $300 million in losses as a result of this attack, and it believed that the objective was data destruction rather than merely holding the data for ransom [Palmer 2017].

---

[2] Organizations must consider not only their traditional assets in these activities but also devices and systems such as employee laptops and phones in bring-your-own-device (BYOD) settings and Internet of Things (IoT) devices like video cameras and smart thermostats.

Organizations should plan the Identify function as a recurring process. As the organization evolves over time due to changing business needs, acquisitions, and the retirement or replacement lifecycle, all of the asset information needs to be maintained, whether refreshed (prior information is still valid) or updated (current information replaces prior information). Business evolution makes asset identification, governance, and risk management continual activities. Even the more stable pieces of the Identify function—governance and risk management strategy—require organizations to regularly update asset information to reflect changes in each organization and its threat landscape.

The Identify activities produce information necessary to accomplish effectively the four other functions (Protect, Detect, Respond, and Recover). Furthermore, the information helps decision makers to prioritize their cybersecurity efforts.

Protect

Recommendation 1: Perform regular backup, augmented with validation and encryption. Ensure that data content is clean and accurate, that recovery works as desired, and that media is protected from loss and corruption.

Recommendation 2: Mitigate against social engineering attacks, which allow attackers to gain a foothold in the organization network. Train users against probable methods, and supplement training with exercises.

Recommendation 3: Practice proactive software hygiene, including maintaining user awareness, performing regular vulnerability management, hardening deployed systems, and improving network defenses. Focus these activities around public (likely targeted) hosts, mission-critical servers, and workstations of personnel serving in a public-facing manner.

The Protect function of the cybersecurity framework supports the organization's ability to limit or contain the impact of a potential cybersecurity event [NIST 2018a]. The protective measures need to be effective against the diverse forms of attack employed by ransomware affiliates. In general, there are three requirements for understanding protection against a ransomware attack:

1. Provide an available option for continuing business operations, including the assurance of at least minimal known-good data with which to proceed.
2. Protect through people, since modern attacks are focused on personnel as much as technology.
3. Populate your network with defenses that make gaining a foothold as difficult as reasonable and that render further malicious action subject to detection, response, and recovery.

While backup, social engineering awareness, and software hygiene are general security measures, the specific threat posed by ransomware affiliates motivates applying them in a targeted manner. Of particular note are the following behaviors:

- Affiliates have compromised backup credentials and contaminated backups that lacked content protection [Abrams 2020b].

- Affiliates have used spear phishing email to acquire a foothold on networks, then dropped malware to spread through the network and compromise data [Moffat 2020].
- Affiliates have abused group policy objects to distribute malware (in addition to exploiting a variety of system and network vulnerabilities), which suggests that software hygiene is needed to address this threat [Sophos 2020].

These protective measures serve as a baseline that supports further activities in the cybersecurity framework. By constraining the attacker's options and at least slowing the attack, more opportunities for detection exist, and the number of response and recovery activities needed are reduced.

As an example of how these practices apply, consider this scenario based on a common attack timeline where a fictitious organization is attacked by a ransomware variant.[3] The ransomware affiliate sent an attachment via a spear phishing email message to a postal agent within the organization. The attachment appeared to be an invoice. If opened, the malicious content would download a malicious application that would immediately seek to collect and encrypt files, both on the local host and on mapped file shares. In addition, it would send copies of itself via email, using the initial recipient's identity, to all individuals on the recipient's contact list. Once the data was collected, the malware would exfiltrate it via third-party cloud storage, and ransom demands would be sent to the original recipient, including a threat of disclosure if the ransom was not paid.

In this case, the organization was prepared for the attack in several ways:

Users, including the postal agent who was the recipient of the spear phishing message, had been trained to be aware of ransomware threats. In this case, the agent noted that the wording and naming of the message were not similar to normal traffic, and the agent chose not to open the malicious attachment. Instead, the phishing email was stored and the organization's security operations center (SOC) was notified.

The shipping data accessed by the agent was stored in an encrypted file share. Since the agent had not yet entered the key, the malicious software would not have been able to gather the data in a form useful for disclosure.

The SOC isolated the attacked environment, then used a sandbox environment to open the attachment, intercepting its attempts at propagation and file gathering. The SOC noted that while data on the file share would potentially be able to be gathered (although encrypted), restrictions on the write permissions on that data would prevent the malware from overwriting the data with malicious encryption. In addition, regularly maintained backups would have permitted restoration of all but the most recently modified data. However, since the system was attacked, the SOC did a thorough examination of that system, in coordination with local law enforcement, to ensure that no other attempt had been successful and that all evidence was properly collected. No further damage was found, but the investigation took several days, during which no packages could be shipped.

---

3 This example is modified from an account [E Hacking News 2019] of an unsuccessful ransomware attack that nonetheless was damaging to the postal delivery service in Malaysia.

The SOC also updated the anti-malware software running on the email server and the user workstations with signatures derived from its analysis of the attachment.

Detect

Recommendation 1: Inform and motivate users to report social engineering, reconnaissance activity, and ransomware-indicative network activity. Provide training that builds on the social engineering awareness training recommended in the Protect function and supplement the training with exercises.

Recommendation 2: Deploy and maintain robust malware detection applications, including anti-malware software, host-based intrusion detection software, and host-based intrusion prevention software. Deploy these applications throughout the organization and configure them to report to a central logging location. Update rule sets, signature databases, and clock settings to provide coordinated alerts.

Recommendation 3: With the centralized logging information, analyze for behavioral indicators relevant to ransomware. Correlate positive analytic results to generate appropriate alerts for Respond and Recover actions.

The focus of the detect actions is to develop and implement appropriate activities to identify the occurrence of a ransomware attack [NIST 2018a]. Since ransomware developers often test their exploit code against anti-malware software, it is important to rely on more than this software to detect this threat. In general, there are three requirements for performing detection of a ransomware attack:

1. Deploy your people as a line of detection. Humans, once informed, are more flexible and motivated than any automated option.
2. Provide multiple points of sensing, but a single point of archiving. Diversity of sensing (network and host, rule-based and exploratory) offers repeated opportunities for finding the affiliate's attack. A single archive provides a base for improving the accuracy of detection through correlation of alerts.
3. Analyze the traffic on your network, looking for unusual events. Recognize that not all attacks will generate the same type of event and not all events of a given type will indicate an attack. Base detection relies on finding indicative events resulting in alerts. Modern network traffic is dynamic enough that false alarms may occur, so corroboration between differing types of alerts improves confidence.

Events to monitor for include the following:

- look-ups for DNS records, especially MX records, coupled with resolution of the host names involved, followed by email from unusual locations (including locations sending email tagged as spam by anti-spam software); NX responses to queries occurring in larger-than-normal bursts or on requests from internal hosts

- unusually large bursts of incomplete network connections on a specific group of network addresses and service ports, or similar unusual traffic coming from unexpected internal hosts, found by analysis of network flow records, often an indicator of scanners
- bursts of email from unusual sources, found by analysis of network flow records, with follow-on contact to unusual locations as web or DNS activity
- web downloads, followed rapidly by web redirects or new web connections to unknown locations or those identified as malicious by threat intelligence sources
- attempts to start unusual software, triggering host-based IDS alerts
- attempts to escalate privilege, triggering host-based IDS alerts
- unusual file transfer, particularly from unknown locations or those identified as malicious by threat intelligence sources
- periodic DNS requests or web GET requests to unusual locations
- unusual contacts between hosts on the network, identified by network flow records collected internally
- unusual traffic to email destination ports from internal hosts that are not email servers
- unusual responses to web requests by internal hosts that are not web servers

While it is unlikely that a single indicator will be usefully specific to a ransomware attack, combinations of indicators, such as those listed above, may provide alerts with sufficiently low false-positive rates.

To understand how these practices apply, consider the increasing use of remote desktop protocol (RDP) attacks to gain a foothold on the targeted network [Sophos 2020]. Attempts to gain access to RDP have been viewed as "Internet background traffic," but RDP clients and servers are viewed by attackers as useful entry points. Monitoring solutions that track where RDP clients and servers contact can offer immediate warning should compromise occur. The RDP collection logs (if centralized in a secure manner) can provide insight into what credentials have been exploited. Further network and host log analysis, using the detected compromise as a starting place, may be able to diagnose and isolate activity before the enterprise incurs further damage. Should attempts at propagation occur, RDP logs, email logs, and web logs may provide useful content to analyze the impact and guide corrective actions by the defenders.

Respond

Recommendation 1: Develop a plan that guides incident response to protect data integrity and support business continuity.

Recommendation 2: Develop communications channels in which stakeholders can safely express updates and move forward on their piece of the response.

Recommendation 3: Establish standards for creating tickets that include all of the information needed to support decision makers and communication with other stakeholders. Use the standards for help in scoping and understanding the impact of the incident.

The Respond function is intended to prepare an enterprise to establish a response plan that can be practiced ahead of an actual event. The most effective response is one that is planned before an incident. Some of the Respond activity requirements that support a successful response include the following:

- Develop a response plan that identifies roles and responsibilities for all participants expected to be part of the incident response.
- Identify communications channels for stakeholders and their dependents before an event.
- Develop relationships with counterparts on different teams and with the federal, state, and local authorities to which the enterprise has reporting responsibilities. (These relationships are described further in the discussion on the Recover function.)
- Develop a reporting process that consolidates progress information for key stakeholders during recovery.

To understand these recovery practices, consider this scenario based on common attack patterns and accepted best practices. In this case, a local website had third-party ads that included malicious scripts, known as malvertising, which on viewing compromised the user's browser and downloaded the ransomware tool chain. After spreading silently within the organization's network for three days, the ransomware encrypted a variety of proprietary data, including the customer database and the accounts receivable records. The malware issued a ransom demand for $45,000 payable via a bitcoin transaction.

In advance of this attack, the organization had in place a response plan. The plan outlined the major stakeholders for key systems (in this example, the Customer Relations VP and the Chief Financial Officer) and the resources (people and equipment) for responding to security attacks. In accordance with the response plan, the designated technical manager rapidly messaged the responsible stakeholders, identifying the then-known affected systems and laying out the process to move forward.

In accordance with the plan, affected systems were isolated, and standby systems were rapidly configured with reduced (but minimally sufficient) capability and deployed to support continuity of operations while response proceeded.

Detailed analysis of the affected systems revealed both the location of the initial intrusion and a list of systems probed by the malware. The affected stakeholders were notified and made aware of the results of the analysis. Other systems were isolated, and critical services were replaced with temporary systems. Once the extent of the damage was known, and as response proceeded, an interim report was provided to senior management.

Once analysis and diagnosis were complete (in this case, also involving FBI assistance in securing forensic data copies), the affected systems were completely wiped back to factory configurations. The operating system and application software were reloaded from authorized known-clean copies, and

additional patches and security software were installed. Backup tapes were used to restore the database and financial records to a recent state, and transaction records were used to bring the data sufficiently close to current. The reconstituted systems were then returned to service.

Recover

Recommendation 1: Restore lost data from recent backups or collateral storage if at all possible, paying the ransom only as a last resort. Inform this restoration using the relationships documented through the Identify function.

Recommendation 2: Restore lost software from known-good install media, applying sufficient updates to deal with all currently known vulnerabilities. Move the network into a known and defensible state before doing other recover activities.

Recommendation 3: Report any attack to appropriate law enforcement. Report through trusted channels to help protect other organizations, including your vendors and customers.

Recommendation 4: Revise software configurations, network defenses, traffic and host monitoring, user training, and operational procedures. Proactively strengthen the network to deal with predictable attacks after a successful ransomware attack.

The focus of the Recover actions is to develop and implement the appropriate activities to maintain resilience and restore any capabilities or services impaired by the ransomware attack [NIST 2018a]. Since ransomware affiliates are highly motivated to continue or restart their attack once a successful compromise has occurred, improving network resilience is essential. Some key requirements for recover actions include the following:

- Deny the attackers benefit from their compromise to the extent possible. If an attack has succeeded in compromising hosts in the network, recover without paying the ransom for your data.
- Eliminate vulnerability by placing affected systems in a good state, based on reliable software distributions, and correcting known issues.
- Notify law enforcement—since affiliates attack multiple victims—so that these campaigns can be tracked and traced. Doing so provides for appropriate warning to other victims, possibly including your clients and vendors. Proactively form relationships with appropriate law enforcement agencies (many have programs facilitating this[4]) to provide a trusted communication channel before attacks occur.

---

4 In the United States, the National Cyber-Forensics and Training Alliance (https://www.ncfta.net/) has many local chapters that facilitate cooperation with law enforcement. The European Cybercrime Centre (https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3) provides useful points of contact in the European Union. Other locales are building similar capabilities.

- Prepare for follow-on attacks—since victim organizations report an average of five attacks in a 12-month period—to reduce further loss to the organization [SentinelOne 2018]. If necessary, involve outside expertise to secure the network and personnel.

To understand how these practices might work, consider a medical practice attacked by Cryptolocker (a ransomware variant) [Moffat 2020]. The attackers delivered the ransomware through a phishing message, and it successfully intruded on the organization's network, encrypting files mounted through file shares.

The organization continued to operate using manual (paper) methods for critical prescriptions and medical records. Using its off-line backup, the IT department was able to restore the organization's data. This days-long process required transporting data, clearing affected computers, restoring critical files, and making configuration changes. The process was successful but required hiring an IT service provider to upgrade the organization's data security. IT also installed an email filter.

The organization submitted an incident report electronically to the FBI and physically to its local police department. It also submitted a claim to its insurance company, but coverage was declined.

The procedural, managerial, and technical safeguards limited the organization's losses and prevented the ransom payment. An after-action analysis was used to guide the reconfiguration of network defenses and to support the work of the outside IT service provider.

The business impact of a ransomware attack may prevent a full and immediate recovery. Affected organizations may need to consider intermediate recovery stages to mitigate business losses. For example, during the FedEx ransomware attack, the organization had to reallocate and deploy resources to the targeted unit [BBC 2017]. For some customers, FedEx had to arrange for shipping via a competitor. The diversion of resources and loss of customers magnified the impact of the ransomware attack. Planning for continuity of operations via other business units may reduce such losses until the targeted unit achieves full recovery.

Conclusions

Ransomware is a multifaceted threat. The ransomware affiliates incorporate a wide range of attacks with the goal of monetizing the compromise in multiple ways. This range of attacks helps them evade common network defenses. These affiliates have been wildly successful across multiple years and a wide variety of victim organizations [Sophos 2020].

No single defense will be effective, since affiliates or attackers use whatever vulnerability is present on the network and suits their attack. They have demonstrated facility with multiple methods of compromise and have been known to purchase exploit kits as needed. Some attackers have shown ability to incorporate compromises within hours of release of a proof of concept.

To gain ground against this ambitious threat, organizations need to control and understand the attack surface of public-facing resources. This attack surface is the set of network dependencies that can be

contacted and used by attackers. Within those dependencies, the organization needs to be aware of, and rapidly respond to, exposure of vulnerabilities.

This report has described multiple overlapping defenses, applicable both prior to and following an attack. Even unsuccessful attacks should be evaluated for the exploits attempted, and corrective action performed where meaningful.

The decision makers' goal is to assure that policy, personnel, and procedure all align for defense, and all support a known state. This known state provides for reliable continuity of organizational operations.

Bibliography

URLs are valid as of the publication date of this document.

[Abrams 2020a]

Abrams, Lawrence. Nemty Ransomware Punishes Victims by Posting Their Stolen Data. *BleepingComputer*. March 2, 2020. https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/

[Abrams 2020b]

Abrams, Lawrence. Ransomware Attackers Use Your Cloud Backups Against You. *BleepingComputer*. March 3, 2020. https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

[BBC 2017]

BBC News. NotPetya cyber-attack cost TNT at least $300m. *BBC News: Technology*. September 20, 2017. https://www.bbc.com/news/technology-41336086

[Cisco 2017]

Cisco. SAFE Design Guide. Security Domain: Threat Defense; Use Case: Cisco Ransomware Defense; Added Advanced. Updated August 2017. https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/ransomware-defense-dig.pdf

[Dragos 2020]

Dragos. EKANS Ransomware and ICS Operations. *Dragos Blog*. February 3, 2020. https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[E Hacking News 2019]

E Hacking News. Pos Malaysia: Malware Attack Disrupts Internal Systems and Online Services. *E Hacking News*. October 26, 2019. https://www.ehackingnews.com/2019/10/pos-malaysia-malware-attack-disrupts.html

[Hanel 2019]
Hanel, Alexander & Stone-Gross, Brett. WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN. *Crowdstrike.com*. November 1, 2019. https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/

[Kim 2019]
Kim, Allen. Yet Another Company Has Been Hit by a Ransomware Attack. *CNN Business*. October 15, 2019. https://www.cnn.com/2019/10/15/business/pitney-bowes-ransomware-trnd/index.html

[Midler 2020]
Midler, Marisa; O'Meara, Kylem; & Parisi, Alexandra. Current Ransomware Threats. Technical Report (number pending). Software Engineering Institute, Carnegie Mellon University. May 2020.

[Moffat 2020]
Moffat, Wiks. Ransomware Attack on a Medical Practice: A Case Study with Guidance. *Coventus Website*. May 5, 2020 [accessed]. https://www.conventusnj.com/practice-resources/regulatory/ransomware-attack-medical-practice-case-study.aspx

[NIST 2018a]
National Institute of Standards and Technology. Framework Documents: Cybersecurity Framework Version 1.1. *NIST Website*. April 2018. https://www.nist.gov/cyberframework/framework

[NIST 2018b]
National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. V1.1. August 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[Palmer 2017]
Palmer, Danny. NotPetya Cyber Attack on TNT Express Cost FedEx $300m. *ZDNet*. September 20, 2017. https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/

[Phillips 2019]
Phillips, Gavin. What Is a Bitcoin Tumbler? Are They Legal? *BlocksDecoded Website*. May 5, 2020 [accessed]. https://blocksdecoded.com/what-is-bitcoin-tumbler/

[Rouse 2012]
Rouse, Margret. "Attack Vector" Definition. *Search Security TechTarget Website*. May 5, 2020 [accessed]. https://searchsecurity.techtarget.com/definition/attack-vector

[Salusky 2007]
Salusky, William. "Malvertising" Definition. *ISC: SANS*. December 6, 2007. https://isc.sans.edu/diary/Malvertising/3727

[Schober 2020]
Schober, Scott. Glossary of Cybersecurity Terms. *ScottSchober.Com*. May 7, 2020 [accessed]. https://scottschober.com/glossary-of-cybersecurity-terms/#d

[SentinelOne 2018]
2018 Global Ransomware Research Report. *SentinelOne Website*. https://go.sentinelone.com/rs/327-MNM-087/images/Ransomware%20Research%20Data%20Summary%202018.pdf

[Sophos 2020]
SophosLabs research team. 2020 Threat Report. *Sophos Website*. May 7, 2020 [accessed]. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

[Stroud 2020]
Stroud, Forrest. "Cryptocurrency Mining" Definition. *Webopedia Website*. May 5, 2020 [accessed]. https://www.webopedia.com/TERM/C/cryptocurrency-mining.html

[Techopedia]
"Data Exfiltration" Definition. *Techopedia Dictionary Website*. May 5, 2020 [accessed]. https://www.techopedia.com/definition/14682/data-exfiltration

[Tung 2020]
Tung, Ling. VPN Warning: REvil Ransomware Targets Unpatched Pulse Secure VPN Servers. *ZDNet*. January 6, 2020. https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/

[Young 1996]
Young, A. & Young, Moti. Cryptovirology: Extortion-Based Security Threats and Countermeasures. Pages 129–140. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*. Oakland, California. May 1996. http://www.syros.aegean.gr/users/tsp/citations_dnl/ieee96.pdf

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM20-0361