INSTITUTE FOR
HOMELAND SECURITY

Sam Houston
State University

RANSOMWARE PREVENTION AND DEFENSE:

A HARDENING GUIDE FOR SMALL AND MEDIUM-SIZED BUSINESSES

Institute for Homeland Security

Sam Houston State University

Narasimha Shashidhar, Cihan Varol

Ransomware Prevention and Defense: A Hardening Guide for Small and Medium-Sized Businesses

Authors: Narasimha Shashidhar, and Cihan Varol

Email: *{karpoor, cvarol}@shsu.edu*

Contents

1 Introduction and Overview

Small businesses typically don't expend as much time, energy, and resources on cybersecurity and information assurance protocols as large corporations do. To this end, they often fall prey to malware and related cyber-attacks. *Ransomware* is a specific type of malware that threatens the victim's access to her data unless a ransom is paid. It is also known as a *cryptovirus* due to its method of operation. Typically, ransomware encrypts the contents of the victim's hard drive thereby rendering it inaccessible to the victim. It might also threaten to publish sensitive data if the victim refuses to pay up. Upon payment of the ransom, the decryption key is released to the victim, with no guarantees that the data will indeed be recovered. This means of attack is therefore also sometimes aptly called *cryptoviral extortion*. The ransomware itself is delivered to the victim using several channels. The most common channel of delivery is by masquerading the malware as a Trojan horse via an email attachment.

Ransomware is projected to reach $40 billion by 2025 and exhibits a growing trend for cyber extortion - data being held for ransom. A small business involved in finance, healthcare, or online retail, is more likely to be targeted than others, such as a small-sized restaurant. It can be recognized as either crypto-ransomware or locker-ransomware. Locker-ransomware locks up systems and demands a ransom to make the system usable; this type is commonly seen in mobile devices. The focus of this whitepaper will be on *crypto-ransomware* in which a system is encrypted with an asymmetric or symmetric key and the only method of recovery is to pay a ransom for a decryption tool. With this in mind, we study this issue and put forth a hardening guide for Small to Medium Size Businesses (SMBs) to best defend and thwart such attacks.

2 How to Use This Whitepaper

Most articles and published reports in the scholarly literature are inaccessible to the average small and medium-sized business proprietor. This is either because the contents of these materials are highly technical, or the solutions presented are time-consuming or prohibitively expensive to deploy. This has motivated us to write this whitepaper in plain English with minimal technical jargon to reach a broad audience. Furthermore, we put forth solutions that are open source and can be deployed effectively with minimal expense and technical expertise. This whitepaper is meant to be read sequentially, from beginning to end. However, the advanced reader may skip to specific sections to best suit their individual needs. This report is accompanied by a descriptive video by the authors that addresses the best industry standards and approaches to take to harden an SMB network and infrastructure from malware, and more specifically the current generation of ransomware.

In addition to proposing hardening defense postures for the SMB, we also develop prevention and mitigation strategies. Lastly, we understand that despite best efforts, some attacks can't be thwarted. To this end, we also propose business continuity and disaster recovery techniques, aimed at getting an SMB back operational and minimizing downtime and lost profits.

2.1 Economic Loss

Ransomware costs small and medium-sized businesses more than just economic loss. Forbes reports that a new ransomware attack will be launched every 11 seconds in 2022 and is expected to reach $40 billion by 2025. About 50% of victims end up paying the ransom but are never fully recovered after the incident. The indirect costs which include rebuilding the servers, lost customer base, tarnished reputation, brand erosion, legal costs, regulatory challenges, and lost employee productivity can, in many instances, never be recouped. Thus, a ransomware attack has the potential to devastate small and medium sized businesses. Our hope in this whitepaper is to present tangible techniques and strategies to mitigate this threat.

3 Most Well-Known Types of Ransomware and Their Modus Operandi

Ransomware and related malware come in many different varieties with as many distinct payloads. Kaspersky[1] identifies the following malware, that have infected both individuals and corporations over the years, to be the most well-known in history:

- Bad Rabbit
- Cryptolocker
- GoldenEye
- Jigsaw
- Locky
- Maze
- NotPetya
- Petya
- Ryuk
- Wannacry

Without loss of generality, most of the ransomware in existence can be classified into two primary categories, based on their modus operandi. While both these classes of ransomware ultimately extort their victims, the subtle difference lies in their degree of data destruction.

a) *Denial-based Extortion Ransomware:* The primary motivation for the perpetrator in this scenario is to ensure that the victim's computing system remains partially operable. This is so that the victim can continue to interact with the perpetrator with minimal computing functions to pay the ransom. To this end, often the most critical system files and software are left unaffected.

[1] https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

b) *Cryptoviral-based Extortion Ransomware:* The primary motivation in this instance is to encrypt the victim's drive contents using strong symmetric or asymmetric cryptographic algorithms. In most cases, without payment in a specified time frame, the system is left completely crippled.

StopRansomware.gov[2] is the U.S. Government's official one-stop location for resources to tackle ransomware effectively and contains a wealth of information for SMB.

4 Common Delivery Vehicles/Mechanisms - Propagating Ransomware

While there are several vectors of attack for ransomware to gain a foothold at an enterprise level, typically the three most common vectors are: a. Phishing and spear phishing email attacks, b. exploiting unpatched software vulnerabilities, and c. trojan horses.

1. Social Engineering Attacks, such as phishing and spear phishing campaigns: Phishing is a form of social-engineering attack designed to trick the recipient into revealing sensitive information. The attack is usually delivered via email and embedded spurious links in an effort to steal credentials, financial information, and other data. Spear phishing is a particularly devious sub-technique of phishing where specific high-profile individuals of an organization are targeted as victims and the emails are custom designed to deceive them into revealing company secrets.
2. Exploit of unpatched software vulnerabilities: Most businesses are dependent upon a slew of software systems and servers for their daily operations. These include operating systems, application software, internet-facing servers, and software daemons with open ports and protocols. Each of these software products needs to be scanned routinely for vulnerabilities and patched in a timely manner.
3. Trojan horses: A Trojan horse, whose name is derived from the Greek story that led to the downfall of the city of Troy, is generally any piece of software that masquerades its true form and disguises itself as a legitimate program. It is generally propagated primarily using social-engineering techniques.

5 Equipping Small Businesses with Appropriate Defense Strategies

In this section, we discuss some strategies for SMBs to defend themselves against ransomware attacks. In particular, let's look at defense strategies against ransomware attack vectors and threats discussed in Sections 3 and 4 above. At the very outset, a well-trained, and informed workforce is the first line of defense against malware. This includes periodic cybersecurity training and awareness programs, and appropriately designed tests and challenges to ascertain the level of preparedness of the organization. In the subsections below, we delve into specific defense mechanisms on several important domains. But before doing so, given the prevalence of Microsoft software and products in the marketplace we'd be remiss if we did not mention Microsoft's

[2] https://www.cisa.gov/stopransomware

Security Compliance Toolkit[3]. The toolkit permits security professionals to test and apply security recommendations for most Microsoft products within their corporate network.

5.1 Firewall Hardening Using Open-Source Software

It is common knowledge that ransomware makes its way into an organization via file download, watering hole attacks, unsecured backdoors, email, malicious attachments, or via remote network protocols. To this end, it behooves the security professionals to harden firewall measures including, but not limited to (Sophos White Paper, 2021):

- Limiting or locking down remote desktop protocol, remote access, and management applications.
- Eliding all unwanted port forwarding and open ports in the firewall rules table.
- Support the latest TLS cipher suites and standards for ingress and egress traffic.
- Upgrading firewall equipment and related IT security devices to the current security standards.
- Ability to isolate traffic from infected systems.

Small and medium-sized businesses would be hard-pressed to find better solutions than the open-source offerings put forth by *pfSense*[4] and *OPNsense*[5]. Both these providers have teamed up with hardware manufacturers to develop turn-key solutions for businesses of all sizes. Finally, we conclude this subsection on firewalls by pointing the reader to the special publication 800-41, by NIST SP 800-41 Rev. 1, "*Guidelines on Firewalls and Firewall Policy*" from the computer security resource center (Karen Scarfone, 2009). Despite being dated, this publication offers a detailed treatment of firewall technologies, architectures, and policies that will assist security administrators at SMBs as they deploy their network infrastructure.

5.2 Deploying Host and Network Intrusion Detection Systems

The increase in ransomware specifically targeted individuals in organizations and SMBs. Since such targeted attacks may bypass perimeter defenses such as firewalls, defense-in-depth strategies are necessary. Cyber threats, including ransomware, can be countered with intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). When used against known, less sophisticated attacks, such as those carried out by activist groups or large-scale email scams, they can be reasonably effective. These attacks are likely to be less effective against sophisticated, targeted attacks by criminals or state-sponsored hackers since they are more likely to use zero-day exploits and conceal their activities. This implies that they may also need to be part of a defense-

[3] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

[4] https://www.pfsense.org/

[5] https://opnsense.org/

in-depth strategy that involves encrypting sensitive information, maintaining detailed audit trails, implementing strong authentication and authorization controls, and actively managing the operating system and application security. The SMB should deploy a hybrid IDS which combines information from a number of sensors. Specifically:

a. In a host-based IDS (HIDS), suspicious activity is detected via examining the characteristics of a host and events occurring on that host, such as process identifiers and system calls. The primary advantage of a host-based IDS is that it can detect both external and internal intrusions, which is not possible either with network-based IDSs or firewalls.

b. In a network-based IDS (NIDS), monitoring and analysis are conducted on the network traffic and application protocols in order to detect suspicious activity.

A combination of *Sagan*[6], a free HIDS tool long with *Snort*[7], a free NIDS tool will be a powerful combination tool for IDS.

5.3 Best Practices for Business Recovery and Disaster Recovery Procedures

Risk mitigation and disaster recovery are components of most business continuity strategies to recover from a disaster, including ransomware. Lack of security controls and disaster recovery strategies may cause a financial impact on the business, which is almost impossible to recover. Generally, the complexity and development of such business continuity plans are handled by experts from a third party. However, having a consultant external to the organization can be an expense that is not justifiable for SMBs. The operating budget for this type of business is uncertain when it comes to protecting technology assets. More and more organizations, including SMBs, are migrating towards cloud computing due to its advantages and ease of maintenance. However, consumers and SMB users are worried about their loss of data on the cloud and data backup to their premises. No doubt, the cloud provides redundancy, but even this data is all, offsite. Consumers need to have their own data on-premises to eliminate dependency on CSP and need to secure this data. The proposed solution is a user deployment scenario by incorporating an application on a Linux box that will perform the backup of the cloud onto local drives. The application will interface with the cloud on a secured channel, check for updates and sync them with local storage. The data transmission will be secure and encrypted. This will provide a few advantages for the SMB.

1. Daily and monthly full backups can be done locally.
2. Since storage space in the cloud can be downsized because of local storage, the cost of the cloud can be reduced.

[6] https://quadrantsec.com/sagan_log_analysis_engine/

[7] https://www.snort.org/

3. Migration from one cloud to another or from public to private or vice versa would be easier since the data is also available locally.

5.4 Limiting the Number of Services/Daemons on the SMB network

Recon is the first step of the Computer Network Attack (CNA) stage. During this stage, the attacker attempts to gather as much data as possible about the target in hopes of using it in subsequent stages of an attack, including Ransomware. Methods and tools used can vary from collecting data via Open-Source Intelligence (OSINT) tools such as search engine results, social media searches, and domain name registry data lookups, to social engineering attempts such as in-person or phishing attacks, and dumpster diving. Technical reconnaissance such as ping, Nmap, and Tracert can also be used. Some techniques, such as planting key loggers and sniffing the network for plain-text credentials, can take a varied amount of time before producing results. In addition to the ones listed above, resources available at *centralops.net*, *osintinsight.com*, and *onstrat.com* contain a multitude of online tools for OSINT data collection. Network reconnaissance, or the process of mapping the network using available tools, requires access to available information as well as the network. Generally speaking, the less information that is made available, the fewer the attackers are able to deduce. For starters, one can limit the information available in the domain registration records, which are public. Using generic role accounts eliminates names and protects against social engineering attacks. Prohibiting zone transfers on your DNS servers limits the amount of detail regarding your hostnames/IP addresses an attacker may receive. Moving on to actual active scanning, the general rule is to disable all unused services, ports, and protocols, as well as protecting any servers and applications that do not specifically need to be publicly accessed. Access to the network (physically and wireless) should be prohibited (such as 802.1X) unless specifically allowed. This will prevent the attacker from accessing the network. After these steps are taken, ongoing internal network reconnaissance should be performed in order to identify exactly what an attacker would see and make adjustments if necessary.

Scan is the next step and builds upon the port scanning and network mapping that may have been completed during the Recon phase. By looking for more detailed information regarding in-use applications and operating system specifics, the attacker may better identify vulnerabilities with which to focus their efforts on. This stage will include tools for network discovery and security auditing such as Wireshark, Nmap (also referenced in the prior stage), Nessus or OpenVAS, Metasploit, Microsoft Baseline Security Analyzer, eEye’s Retina, and GFI Languard. For example, the ability to assess web server and database versions may allow for the identification of known vulnerabilities, such as a SQL injection attack. Defending against scanning is approached most often by not allowing the scanner/attacker on the network, closing/disabling ports that will provide data to the scanner, or in some cases it is even possible to invalidate scanner results by moving services to a port other than what their services are generally accepted to be run on, such as moving ftp services off port 21, or moving another service to port 21. This can confuse the attacker and cause additional effort.

5.5 Antivirus and Related Software

Anti-virus software needs to be used on each end system. This gives the software maximum access to information on not only the behavior of the malware as it interacts with the targeted system but also the smallest overall view of ransomware activity. Fourth-generation antivirus programs, such as Malwarebytes and Windows Defender consist of a variety of anti-virus techniques, including scanning and activity trap components that are required. In addition, such a package includes access control capability, which limits the ability of ransomware to penetrate a system and then limits the ability of ransomware to update files in order to propagate.

6 Prevention Techniques

In this section, we outline some of the most prevalent approaches used in preventing some of these attacks.

6.1 Creation of a Security Policy and Appropriate Awareness Training

It is important to develop an organizational security policy that describes the objectives and strategies to thwart ransomware attacks and how they will be achieved. It is more common to have a set of related documents in an organizational or corporate security policy. This policy should cover:

1. The policy's intent and scope.
2. The interrelationship between the organization's business goals, legal and regulatory duties, and security goals.
3. IT security needs for privacy, availability, accountability, authenticity, and dependability, especially in light of asset owners' perspectives.
4. The delegating of duties for the administration of IT security and the organizational infrastructure.
5. The organization's strategy for managing risk.
6. How to handle security awareness and training concerns with general employees, particularly for those in positions of trust.
7. Any potential legal consequences for staff members and the circumstances in which they would be applicable.
8. Security integration in system development and acquisition.
9. Contingency and business continuity planning.
10. Incident detection and handling processes.
11. How and when this policy should be reviewed.
12. The method for controlling changes to this policy.

The intent of the policy is to provide a clear overview of how an organization's IT infrastructure supports its overall business objectives in general, and more specifically what security requirements must be provided to do this most effectively.

6.2 Weakest link: The Human Factor - Social Engineering Attacks

Social engineering assaults are one of several avenues for launching ransomware-attacks, and as it turns out, also the most effective technique. The best line of defense against social engineering fraud in the SMB is awareness raised through the company cultures, training programs, and education. To become a "*human firewall*," a workforce must be taught how to identify and respond to an attacker's tactics. Simply following policy guidelines is not enough. The following actions should be included in a thorough countermeasure training program:

- Carry out a data classification evaluation to determine which workers have access to what categories and levels of private company data. Be aware of who a social engineering strategy is likely to use as its main target. Keep in mind that every employee faces a risk.
- Even if the individual claims to be a coworker, boss, or IT representative, never provide private or sensitive information to someone you don't know or who doesn't have a good reason to obtain it. If a password needs to be provided, it should never be communicated over email or phone.
- Refrain from conducting all financial transactions via email. Establish call-back policies with clients and vendors for all outgoing fund transfers to a pre-established phone number, if email must be used, or put in place a customer verification system with comparable dual verification capabilities.
- Create processes for independently verifying any modifications to vendor or customer information.
- Prevent utilizing or investigating "rogue devices" such as software on a computer or network or unauthenticated thumb/flash drives.
- Be wary of unsolicited emails and only open those that come from reliable sources. Never respond to or view links or attachments in such emails; instead, quarantine or delete them.
- Refrain from reacting to any offers received by phone or email. If something seems too good to be true, it most likely is. Unsolicited offers to help with a problem, such as a computer problem or other technical difficulty, could fall under this category.
- Be wary of anyone who tries to rush a conversation (act now, think later), refuses to offer basic contact information, uses threatening language, or demands confidential information. Before being disposed of in any on-site containers, such as dumpsters, physical documents and other tangible materials like computer hardware and software should always be shredded and/or destroyed.
- Actively address workplace information security complacency by putting in place internal awareness and training programs that are regularly reviewed with staff members. This entails creating an incident reporting and tracking program to keep track of social engineering incidents and putting an incident response plan into practice.

- Teach customer service representatives to spot the psychological tricks that social engineers employ, including pressure, speed, enticement, and power. If something is crucial enough to move on fast, it is crucial enough to confirm.
- Consider running a periodic, independent penetration test to evaluate the vulnerabilities in your company, such as unauthorized calls or emails to staff members asking for private information.
- Prevent unlawful physical access by adhering to rigorous rules for the display of security badges and other identification, and by ensuring that all visitors are escorted. Please turn away anyone who is "tailgating." Secure all important places, including executive offices, mail rooms, phone closets, and server rooms, always.
- To avoid sensitive information being exposed online, keep an eye on how social media platforms, public sources, and online commercial information are used.

6.3 Two-factor Authentication Techniques

The employment of multiple authentication methods in a system is referred to as multifactor authentication. The quantity of factors an authentication system incorporates heavily influences the system's strength. Systems that combine three elements are stronger than systems that just contain two of the components, and so on. Implementations that employ two factors are thought to be more effective than those that use just one factor.

While the primary authentication mechanisms are based on something that the individual knows, such as password and pin numbers, there are three other mechanisms that can be employed as part of the two-factor authentication techniques.

a) Something the individual possesses (token), such as electronic keycards, fobs, smart cards, and physical keys.
b) Something the individual is (static biometrics), such as getting recognition by fingerprint, retina, and face.
c) Something the individual does (dynamic biometric), such as getting recognized by voice pattern, handwriting characteristics, and typing rhythm.

When implemented and used correctly, each of these techniques can offer safe user authentication. Each approach, though, has drawbacks. A password could be susceptible to guessing or theft by an attacker. Similarly, an adversary may be able to steal or counterfeit a token. A user might misplace a token or forget their password. Additionally, maintaining and protecting the password and token information on systems entails a considerable administrative burden. There are many issues with biometric authenticators, such as handling false positives and false negatives, user acceptance, cost, and convenience. However, considering the cost factor and easy of access/use, the SMB should rely on face-recognition done by a mobile device (smartphone) of the user to provide authorization and authentication.

6.4 Principle of Least Privilege and Network Segmentation

The sorts of users on the system, their rights, the kinds of information they can access, and how and where they are defined and validated should all be taken into account during the system planning process. There will be users with enhanced privileges who can manage the system, typical users who can share appropriate access to files and other data as needed, and possibly even guest accounts with very restricted access. Restricting elevated rights to only those people who need them is a crucial mitigation technique for ransomware attacks. Furthermore, it is ideal for such individuals to only utilize systems with elevated rights when necessary to complete a task and to use them normally otherwise. By giving an attacker a limited window of opportunity to take advantage of the actions of such privileged users, increases the security profile of the system. In order to help administrative users, elevate their privileges only when necessary and properly track these operations, certain operating systems offer specialized tools or access mechanisms.

6.5 Updating Operating systems and Software: Timely Security Patches

Securing the base operating system, which serves as the foundation for all other applications and services, is a crucial initial step in system security. An appropriately installed, patched, and configured operating system is necessary for a strong security foundation. Unfortunately, convenience and utility are frequently prioritized over security in many operating systems' default configurations. Additionally, as every firm has different security requirements, so will the proper security profile and, consequently, configuration.

It is essential that the system be kept as current as possible, with all crucial security-related patches implemented, given the ongoing discovery of software and other vulnerabilities for widely used operating systems and applications. This is undoubtedly one of the most important ransomware mitigation techniques. Today, almost every system that is frequently used comes with programs that can download and apply security updates automatically. To reduce the amount of time any system is exposed to vulnerabilities for which patches are available, these tools should be set up and used. It may be necessary to stage and validate all patches on test systems before deploying them in production for systems where availability and uptime are crucial. However, this procedure ought to be completed as soon as possible.

7 Lifecycle of a Ransomware Attack

In this section, we briefly outline the lifecycle of a ransomware attack as illustrated in Figure 1 below. As expected, once the malware has found a foothold using any of its attack vectors (phishing, trojan, or software vulnerability), it launches its attack. This is then followed by the infection phase, whereupon the malware contacts the command center to download the encryption key from the perpetrator. Once downloaded, this key is used to encrypt the victim’s system which permits the next phase, the encrypt and extort phase. In this phase, a ransom message is made available on the victim’s machine with directions on how the ransom is to be paid. Typically, this is done via Bitcoin or other unregulated mechanisms of cryptocurrency, for obvious reasons. Once the ransom is paid, the hope is that the victim is permitted to decrypt their data and proceed to the post-attack and data-recovery phase. It is of course in the interest of the attacker to propagate the virus and to this end, the virus continues to search for new victims and spread this cycle all over again.

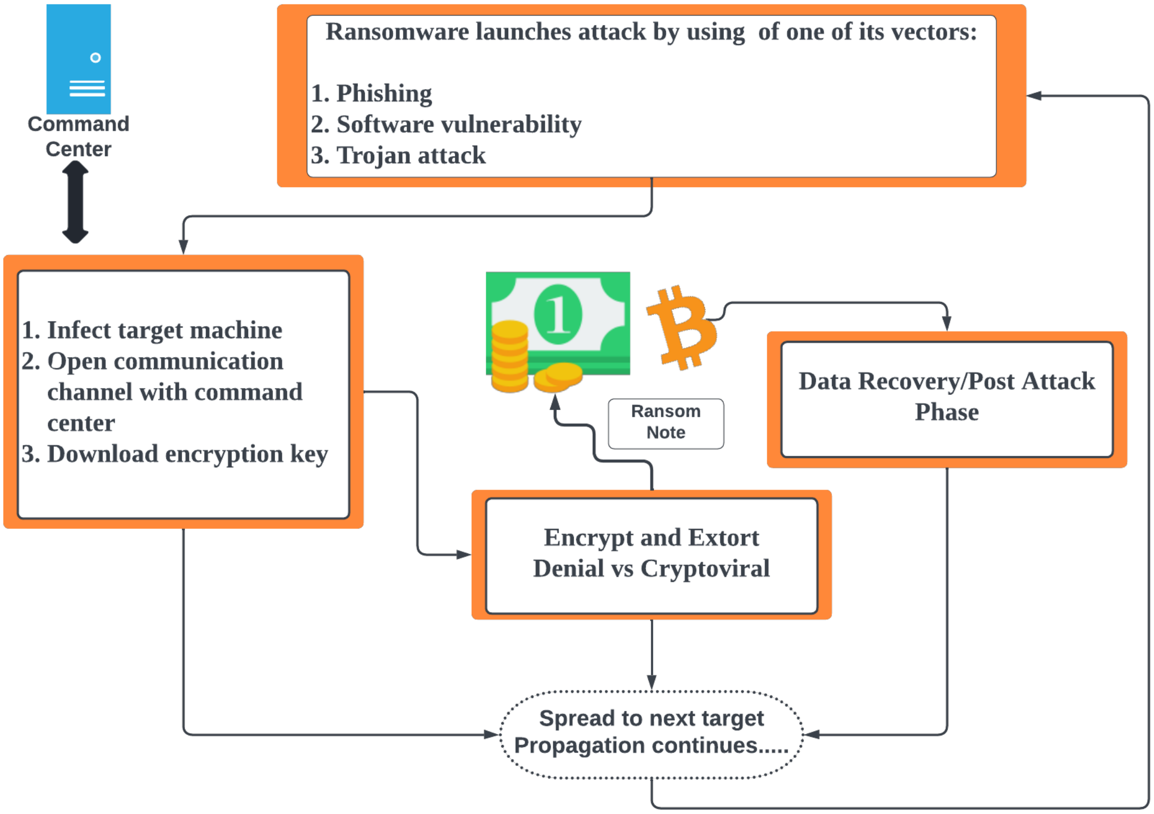
Command Center
Ransomware launches attack by using of one of its vectors:
1. Phishing
2. Software vulnerability
3. Trojan attack
1. Infect target machine
2. Open communication channel with command center
3. Download encryption key
Ransom Note
Data Recovery/Post Attack Phase
Encrypt and Extort Denial vs Cryptoviral
Spread to next target Propagation continues.....

Figure1: Lifecyle of a ransomware attack

8 Planning a Response/Recovery After an Attack

We've spent quite a bit of time discussing various security measures to protect an SMB from ransomware attacks. Despite best efforts, attacks do indeed succeed and in this section, we briefly touch upon recovery techniques after an attack. Often, depending on the specifics of the attack, a victim does not have the luxury of time. To prevent further damage, the first response ought to be limiting the spread of the malware through the SMB network. To this end, isolation of infected hosts, disconnecting them from the network, disabling Wi-Fi, Bluetooth, and other communication channels is paramount. Having isolated the infected machines, identify the strain of malware that is plaguing these systems and report this to the authorities. In particular, victims are encouraged to file a complaint with the Internet Crime Complaint Center (IC3) by the FBI. Details on the procedure and what is to be included in the complaint are available here: *https://www.ic3.gov/*. Subsequently, use any of the above-mentioned strategies to restore affected systems and get the business running again.

8.1 The Future of Ransomware: Internet and the IoT

In this whitepaper, we asserted that an adaptive approach is necessary when dealing with ransomware as malware authors continually evade security software and deployed hardening measures. Ransomware is here to stay, and it can be forecasted to affect other systems and technologies like IoT. IoT, the Internet of things, encompasses all objects that are embedded with sensors, processing, and other tools that network them to other devices over the Internet or other large/small-scale networks. With the pervasiveness of the Internet and IoT, a far greater number of hosts are now in jeopardy from ransomware. For example, the connected-car can become a primary target as commands can be sent to essentially render the car inoperable until a ransom is paid. A similar fate could await our mobile devices as well. In conclusion, ransomware defense tactics require a new approach that uses behavioral analysis and key traits common to ransomware to thwart their advance. To this end, the solutions we have put forth will therefore be applicable in many distinct applications and several different small and medium-sized business arenas to minimize downtime and lost profits/revenue to ransomware.

9 Conclusion

In conclusion, it is unfortunate that ransomware has now become an ever-present threat in our current marketplace. Several federal and state agencies have recognized this issue. In particular, ransomware is now classified as a federal crime and is reportable to the FBI as discussed in Section 8. The Federal Trade Commission, FTC, has a few publications "*Cybersecurity for Small Business*"[8] and "*Ransomware prevention: An update for businesses*"[9] aimed at helping small and medium-sized businesses. These publications have been created with input from NIST[10] (The National Institute of Standards and Technology), the SBA[11] (The U.S. Small Business Administration), and DHS[12] (United States Department of Homeland Security). We hope that this whitepaper and the resources mentioned herein help SMBs thwart any future ransomware attacks.

10 Acknowledgement

The authors would like to thank the Homeland Security Institute, and The Department of Computer Science at Sam Houston State University, for funding and support in developing this whitepaper.

[8] https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

[9] https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses

[10] https://www.nist.gov/

[11] https://www.sba.gov/

[12] https://www.dhs.gov/

11 References

Karen Scarfone, P. H. (2009). *Guidelines on Firewalls and Firewall Policy; Recommendations of the National Institute of Standards and Technology.* Information Technology Laboratory, Computer Security Resource Cente. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved July 27, 2022, from https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Sophos White Paper. (2021). *Firewall best practices to block ransomware.* Sophos. Retrieved July 28, 2022, from https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/firewall-best-practices-to-block-ransomware.pdf

INSTITUTE FOR
HOMELAND SECURITY

Sam Houston
State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Shashidhar, N. & Varol, C. (2022). **Ransomware Prevention and Defense: A Hardening Guide for Small and Medium – Sized Businesses** (Report No. IHS/CR-2022-2037). The Sam Houston State University Institute for Homeland Security. https://ihsonline.org/Research/Technical-Papers/Ransomware-Prevention-and-Defense-A-Hardening-Guide-for-Small-and-Medium-Sized-Businesses