Fall 11-23-2021

Ransomware Education: Availability, Accessibility, and Ease of Use

Judson Gager

Judson Gager

Murray State University Honors College

HONORS THESIS

Certificate of Approval

Ransomware Education: Availability Accessibility, and Ease of Use

Judson Gager

December/2021

Approved to fulfill the
requirements of HON 437 or 438

_____
Dr. Randall Joyce, Instructor
[Cybersecurity and Network Management]

Approved to fulfill the
Honors Thesis requirement
of the Murray State Honors
Diploma

_____
Dr. Warren Edminster, Executive Director
Honors College

Examination Approval Page

Author: Judson Gager

Project Title: Ransomware Education: Availability Accessibility, and Ease of Use

Department: Cybersecurity and Network Management

Date of Defense: 11/23/2021

Approval by Examining Committee:

_____ _____

(Dr. Randall Joyce, Advisor) (Date)

_____ _____

(Mr. Brandon Dixon, Committee Member) (Date)

_____ _____

(Mr. Carlos Lopez, Committee Member) (Date)

Ransomware Education: Availability, Accessibility, and Ease of Use

Submitted in partial fulfillment

of the requirements

for the Murray State University Honors Diploma

Judson Gager

November/2021

Abstract

With cybersecurity constantly in the media outlets with breaches, cybercrime, and cyberwarfare, it has become a significant concern for all. One of the most recent breaches in the summer of 2021 was the Colonial Pipeline breach, which has proven the country's reliance on these industrial control systems and networking. The systems were taken for ransom by a new type of ransomware written in a different programming language. Although the Colonial Pipeline breach was quickly addressed, the impact of the gas shortage and the response time were alarming at triaging the breach. However, this attack showed the public how dangerous ransomware could be, mainly when groups target crucial supply chains and infrastructure critical to the functioning of a nation's economy. The only proper "solution" to these attacks is a standard solution to many information security issues, user training. However, the reality of the problem is that even if computers were one hundred percent secure and infallible machines, which they are not, user error could still compromise an entire system.

Table of Contents

LIST OF FIGURES

Introduction

In order to start educating users about ransomware, users must know what it is in the first place. NIST, the National Institute of Standards and Technology, defines ransomware as "A type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom, is paid," (NIST, "Glossary," 2019). In recent years ransomware groups have also begun exfiltrating data in addition to encrypting it. Ransomware gives them more leverage over the victims, giving attackers the options of leaking the data over time to encourage a ransom payment or outright selling the data to the highest bidder if the victim refuses to pay the ransom. These core principles remain relatively constant regardless of the particular company that was a victim or the ransomware group that performed the attack. In order to gain a more in-depth understanding of how ransomware works in the real world, this research will first create a demo for users unfamiliar with ransomware to get firsthand experience with it in a safe and secure environment. While simple compared to ransomware used in real-world attacks, it should give anyone who follows along with a general understanding of the mechanics of ransomware. Next, the research will provide an example of ransomware used in real-world attacks and analyze its methods to compromise a system using various malware analysis tools. Lastly, this research will recommend solutions for creating a layered approach to security against threats like ransomware.

Background Research

MITRE ATT&CK Framework

According to the official website, the MITRE ATT&CK framework (may also be referred to as Mitre Attack) "is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base serves as a foundation for the development of specific threat models and methodologies in the private sector, in government, and the cybersecurity product and service community" ("MITRE ATT&CK®"). The Mitre Att&ck framework includes Tactics and Techniques. Tactics are the categories under which Mitre Att&ck classifies Techniques. Tactics are common steps taken by attackers in order to accomplish whatever their goal may be. Techniques (and sub-techniques) are the nitty-gritty details of how a specific tactic works. An attacker may deploy many techniques within a singular tactic or might not use a particular tactic at all; it depends entirely on the attack's goal. For those unfamiliar with this topic, I have supplied a table below of all enterprise tactics, taken from the official Mitre Att&ck website:

Figure 1

Mitre ATT&CK Enterprise Tactics

Enterprise tactics

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Note: ("MITRE ATT&CK®").

Mitre attack will be used throughout this research to define actions taken by attackers (Tactics) and how they accomplish those actions (Techniques). Defining the methodology is critical to the research because it provides a method to define the risks posed by any form of malware and the suggested prevention and mitigation measures for each risk. By doing this, the framework provides a straightforward solution to creating a layered security approach to counter, or at the very least, detect any attack.

Joe's Sandbox

Joe's sandbox is a web-hosted cloud application that offers the ability to detect and analyze potential malicious files. This research will be conducted using the Community Edition of Joe Sandbox Cloud. According to its website, "It performs deep malware analysis and generates comprehensive and detailed analysis reports" (LLC, Automated malware analysis). This tool allows one to perform malware analysis without taking on many of the risks associated with doing so. Joe Sandbox is incredibly helpful because it makes malware analysis more accessible and safer simultaneously. For example, the user can supply malware, or the user can search through the database of malware that has already been submitted for analysis by other community members.

ShinoLocker

According, to the official website "ShinoLocker is ransomware simulator. The difference between ShinoLocker and real ransomware is that it never asks for ransom; you do not have to pay to get the decryption key" (Sh1n0g1 Inc., 2016). During this research, ShinoLocker will be

a safe and effective means to demonstrate how ransomware works to everyday users. The safety features are the main factor in the decision to use this software. Executing, Shino Locker provides you with the encryption key to decrypt your files, and even if it does not work for some reason, the files are not deleted as they are with actual ransomware. Instead, they are moved to the recycle bin, restoring them even without the encryption key.

Virus Total

According to the official website, “VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers several file submission methods, including the primary public web interface, desktop uploaders, browser extensions, and a programmatic API” (VirusTotal, How it works – virustotal). Throughout this research, VirusTotal will be used in conjunction with Joe’s Sandbox to analyze malware that has been deemed too risky to handle using conventional means.

Virtual Machines (VMware)

VMware is virtualization software that allows for the creation of and use of virtual machines. According to the NIST Glossary, "A simulated environment created by virtualization" (NIST CSRC, Virtual machine (VM) - glossary). Essentially, a virtual machine is a simulated computer running off of the resources of a physical computer. This is helpful when dealing with malware because it creates a logical barrier between the physical machine and the simulated environment. Therefore, while it is not advisable to use Virtual Machines as a primary defense mechanism against malware, it is advisable to use them as a secondary defense mechanism in a lab environment.

Safety/Security Protocols

The biggest security concern in this research is to ensure that it is done safely, without risking any damage to the University's IT environment. This research has a lot of inherent risks due to the nature of the subject. In order to ensure user safety, the safety and security protocols designated here will be used throughout the research. There are a few different phases to this research, and each phase will have slightly different security guidelines. The guidelines are as follows:

Phase 1: Demonstration

To follow along with the demonstration, these guidelines must be adhered to in order to ensure the security of your machine and network:

- Only download ShinoLocker from the official website. Other sources could have the safety features removed
- The demonstration should be in a inside a virtual machine
- The virtual machine should only be connected to a network to download ShinoLocker and retrieve the encryption key.

- The network should be behind a firewall

Phase 2: Finding Ransomware on the open internet

- Only browse the internet from well-secured machines (firewall on the network, antivirus running, etc.)
- Avoid known black-hat hacker sites as well as sites that are known to be dangerous.
- DO NOT download anything. Due to the nature of the tools and research, all required to analyze the ransomware is a link to the file download.

Phase 3: Ransomware Analysis

- DO NOT download anything.
- Only use reputable sites to corroborate code analysis.

Hypothesis

This research seeks to answer the following questions:

- How hard is it to find ransomware on the open internet?
- How easy is ransomware to deploy?
- How does ransomware work?
- What tools and methods are available and effective for the detection and prevention of a ransomware attack?
- How do you train the general public to help prevent ransomware attacks?

Given these questions, this research seeks to accomplish these objectives:

- First, create a reproducible demonstration of how ransomware works for educating the general public.
- Perform analysis on an example of ransomware from the real world to demonstrate the tactics and techniques commonly used throughout different strains of ransomware
- Discuss prevention and mitigation measures to create a layered security approach to detect and respond to ransomware incidents.

Demonstration/Project Setup

Equipment and Software Required

For the demonstration, there are only a few necessary things:

- Virtualization Software
- Windows License Key or VM snapshot
- ShinoLocker
- Some form of antivirus (Windows Defender will work)

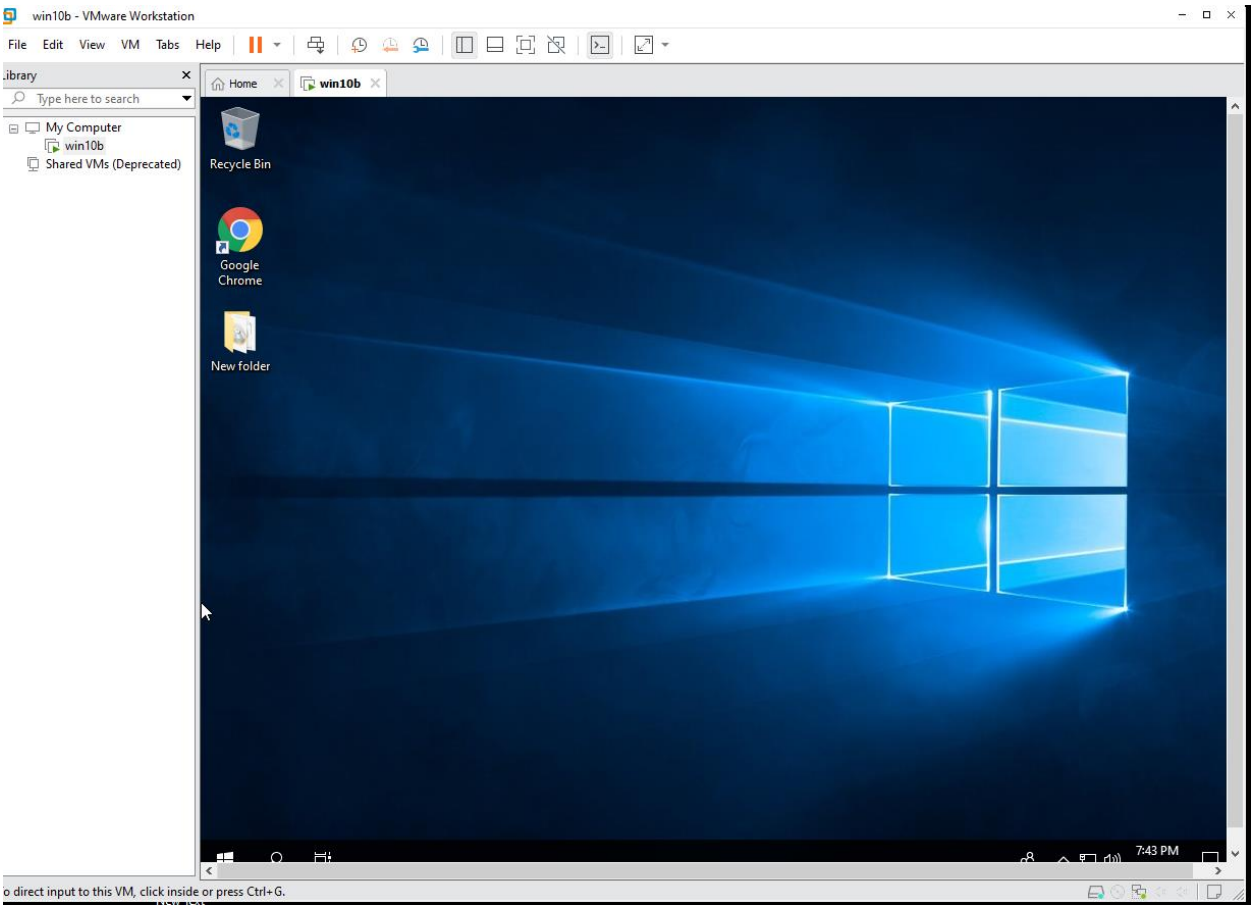
The virtualization software allows one to create a virtual machine for the demonstration, and ShinoLocker is the ransomware we will be using. The Virtualization software used in this research will be a VMware workstation, but any virtualization software will work.

How to Implement/operate

First, open a virtual machine using your preferred virtualization software.

Figure 2

VMware Screenshot



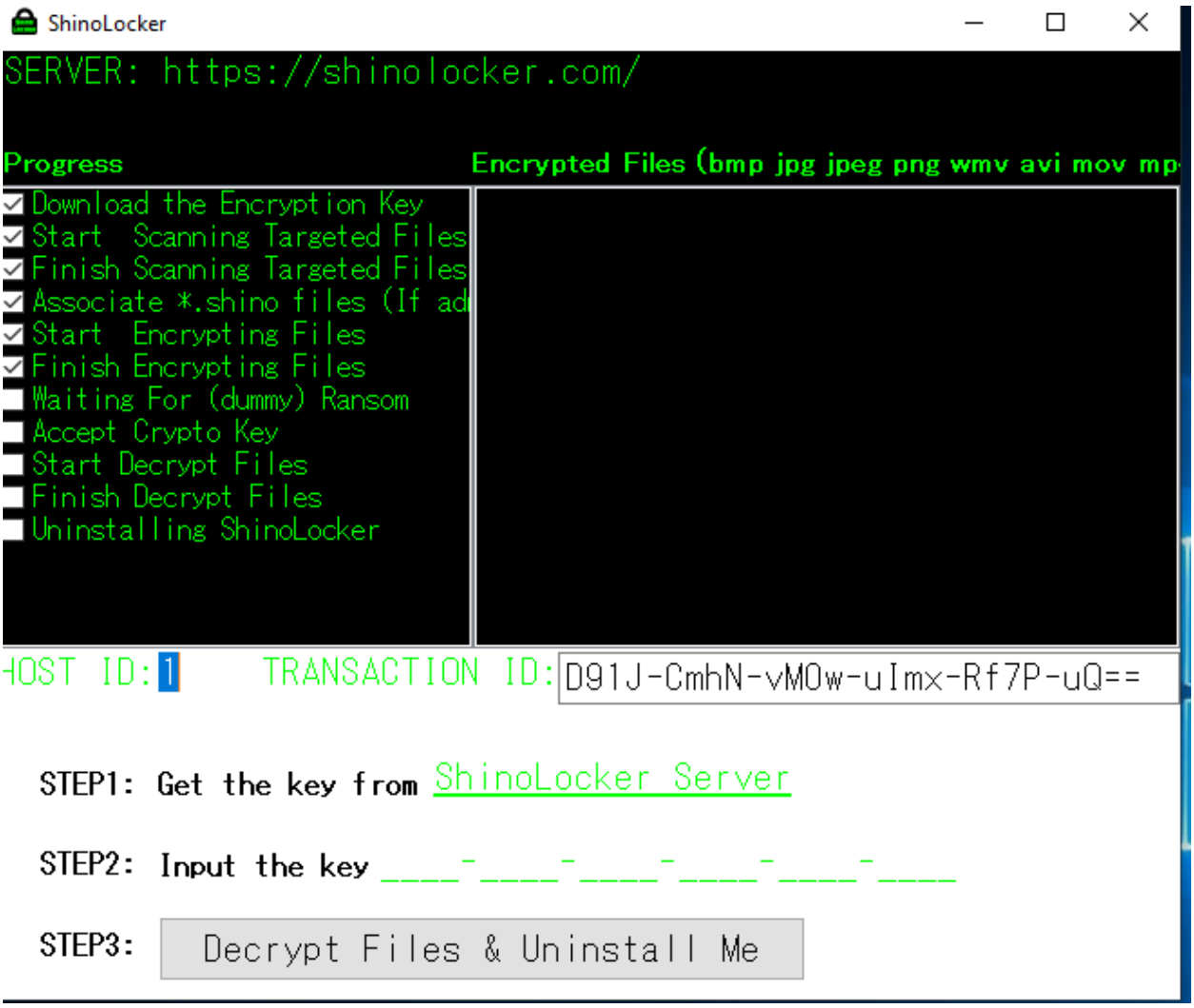
Next, connect to a network so that you can access the internet to download ShinoLocker.

Downloading Shinolocker may give you some issues since it is known as ransomware. You may have to disable windows defender. You can do this by clicking more details when you are alerted to the security issue by windows defender and then disabling your Real-time protection. Only do this if you intend to have your files encrypted.

Next, launch ShinoLocker and run it as administrator. You can see the program below.

Figure 3

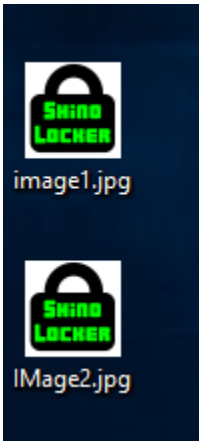
Screenshot of Shinolocker program



At this point, any files matching the file extensions specified when you downloaded ShinoLocker will be encrypted. Encrypted files will look like those shown below:

Figure 4

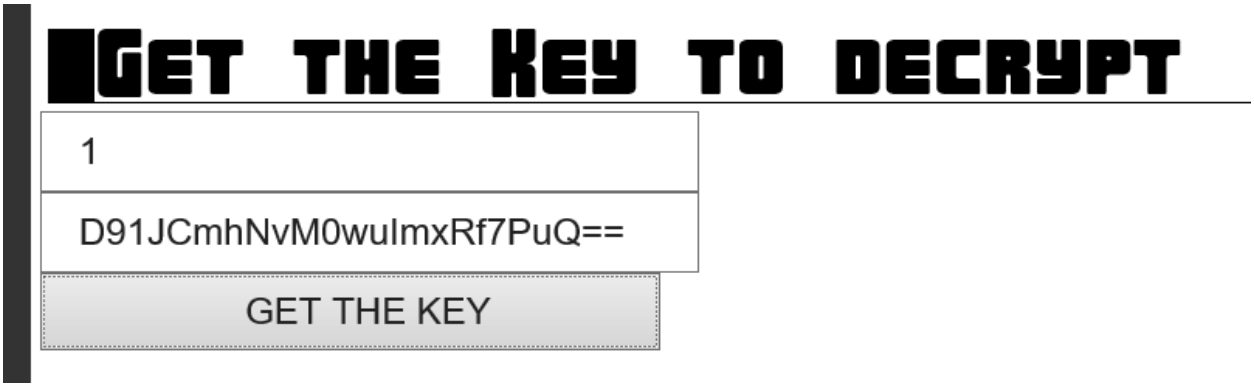
Screenshot of Encrypted Files



You should now see the program above. From here, you can click the Get the key from the ShinoLocker Server button. Next, click the Get the Key button on the ShinoLocker website.

Figure 5

Screenshot of decryption key retrieval



From here to the key will be displayed in a pop-up box.

Figure 6

Screenshot of decryption key pop-up box

Copy and paste this key into the Shinolocker program to decrypt your files

Figure 7

Screenshot of decryption key input

Click the Decrypt Files and Uninstall Me button.

Figure 8

Screenshot of Decrypt Files and Uninstall me button

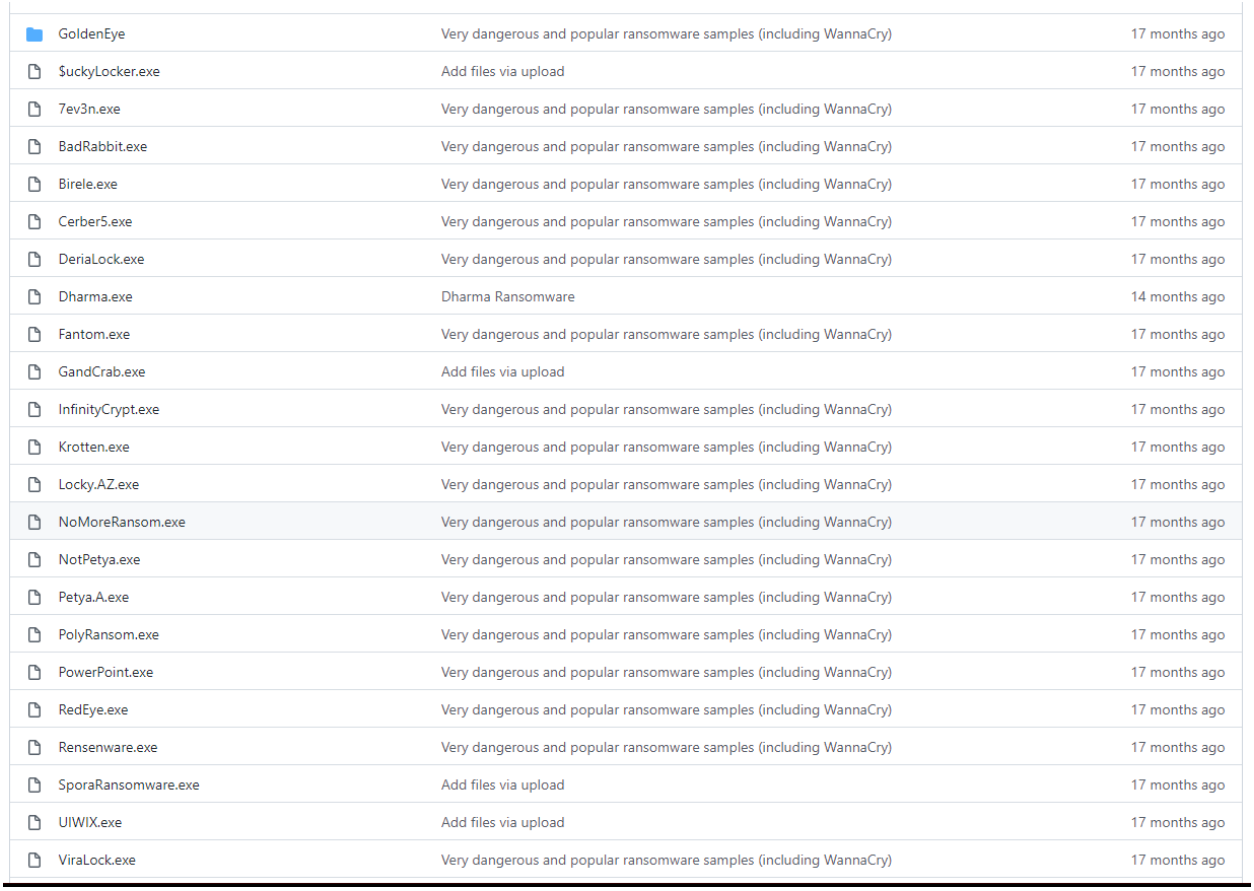
Once your files are decrypted, Shinolocker will disappear/uninstall, and your files will be restored.

Finding Ransomware on the Open Internet

Finding ransomware on the internet has become an almost trivial task due to the sheer volume of attacks we have seen over the past few years. A simple google search for "GitHub ransomware repository" will yield many results. However, it is not recommended to download these programs as they can be highly unpredictable. The purpose of Joe's Sandbox and Virus Total. These cloud-based malware analysis tools allow someone to analyze malware without potentially risking their machine in the process. The first repository this research will analyze is the Malware Repo public repository on GitHub hosted at https://github.com/Da2dalus/The-MALWARE-Repo. This research will be analyzing some of the different ransomware included in this repo under the ransomware directory. Below is a screenshot of just some of the ransomware included in this repository

Figure 9

Screenshot of GitHub Ransomware Repository

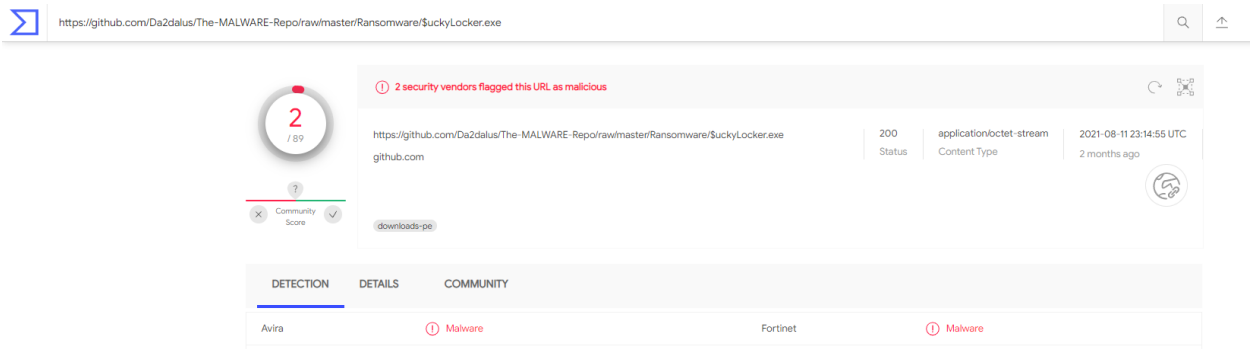


GoldenEye	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
$uckyLocker.exe	Add files via upload	17 months ago
7ev3n.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
BadRabbit.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Birele.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Cerber5.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
DeriaLock.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Dharma.exe	Dharma Ransomware	14 months ago
Fantom.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
GandCrab.exe	Add files via upload	17 months ago
InfinityCrypt.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Krotten.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Locky.AZ.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
NoMoreRansom.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
NotPetya.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Petya.A.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
PolyRansom.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
PowerPoint.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
RedEye.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
Rensenware.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago
SporaRansomware.exe	Add files via upload	17 months ago
UIWIX.exe	Add files via upload	17 months ago
ViraLock.exe	Very dangerous and popular ransomware samples (including WannaCry)	17 months ago

To confirm these files are ransomware, I will run one of the files through the virus total using its download URL. The results are shown below:

Figure 10

Screenshot of VirusTotal scan results



Now that it is confirmed that this repository includes actual ransomware, is it usable? For most users, this sort of ransomware would not be very usable. To serve an individual's purposes, it would require a high level of technical expertise to modify ransomware source code, like the files found in the git hub repository above. It would probably be easier for someone with the required technical expertise to just write their original malware.

There are other options for an aspiring threat actor available on the open internet. RAASNet is another repository that can be found on GitHub. RAASNet is a set of scripts that can generate encryptor payloads, send them to targets, and decrypt a target's machine. It includes a GUI Admin Dashboard with all sorts of statistics available for the threat actor to see about their victims. The Github page even includes a link to an onion site that claims to host a complete command and control system for aspiring threat actors to use. To conclude, the resources are out there for those with the technical expertise to use them.

Real-World Ransomware Analysis

Introduction to Revil

Revil is the specific strain of ransomware chosen for analysis for this research. Throughout this research, the term "Revil" will refer to a specific strain of ransomware. The ransomware group that uses Revil goes by that name. The Revil ransomware group is thought to be based out of eastern Europe. The group disappeared for a short stint back in July of 2021 (Tidy, 2021), only to reappear a few months later in September of 2021 (Abrams, 2021).

Background Information

The specific attack this research will analyze is the Kaseya VSA attack in July of 2021 that affected over 1000 different companies. The Kaseya VSA attack is unique due to the vast number of compromised machines and organizations, with just one attack carried out by one group. Additionally, the absurdly large scope of this attack is due to the nature and purpose of Kaseya VSA software. Kaseya VSA is a remote monitoring and management solution marketed to and used by IT managed service providers or MSPs. MSPs are third-party companies that provide businesses with networking infrastructure, applications, and network security through ongoing support and administration of systems per their service level agreement. Essentially MSPs are a third party that businesses may contract to provide them with IT services. Understanding this attack vector is important because ransomware attacks with a Third-Party Liability are almost sure to involve insurance, increasing the chances of attackers receiving a payout. These two factors combined, third party liability and many users affected, made Kaseya VSA an incredibly enticing target for attackers.

Initial Access/Zero-Day

The Kaseya VSA attack leveraged an unpatched zero-day vulnerability in the Kaseya VSA software to accomplish its objectives. According to the Spider Labs Blog, “This vulnerability has been issued CVE-2021-30116 and was discovered and reported to Kaseya by a researcher for the

Dutch Institute for Vulnerability Disclosure (DIVD). Kaseya was actively working on a patch. According to the DIVD, but not finalized before REvil discovered and exploited the issue. At this point, it is still not clear what the actual issue is or how the exploit may work, although initial reports suggest a potential authentication bypass." (Mendrez & Kazymirskyi, 2021)

Further details into the inner mechanisms of the zero-day vulnerability are hard to find and for a good reason. According to the Dutch institute for Vulnerability Disclosure (the original research organization that identified the vulnerability), "One of our researchers found multiple vulnerabilities in Kaseya VSA. The researchers were in the process of responsible disclosure (or Coordinated Vulnerability Disclosure) with Kaseya; before all these vulnerabilities could be patched, a ransomware attack happened using Kaseya VSA. Ever since we released the news that we indeed notified Kaseya of a vulnerability used in the ransomware attack, we have been getting requests to release details about these vulnerabilities and the disclosure timeline. However, in line with the guidelines for Coordinated Vulnerability Disclosure, we have not disclosed any details so far. Furthermore, while we feel it is time to be more open about this process and our decisions regarding this matter, we will still not release the full details" (Oudshoorn, 2021).

While it may be challenging to get specific details about the vulnerability due to the coordinated vulnerability disclosure guidelines, some information can still be gleaned from the official disclosure documents. For example, according to the official CVE list hosted at cve.mitre.org, for CVE-2021-30116, the vulnerability description is, "Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021" (CVE-2021-30116, 2021). Furthermore, in another document produced by the Dutch Institute for Vulnerability Disclosure, CVE-2021-30116 is referred to as "a credentials leak and business logic flaw, to be included in 9.5.7" (Oudshoorn, 2021). By corroborating the information from these two sources, one can infer that the attackers acquired valid credentials with high-level access to the Kaseya VSA servers. Therefore, this vulnerability would fall under TA0001 Initial Access and T1078 Valid Accounts in MITRE Attack Classification.

After the initial authentication bypass has been achieved using the zero-day vulnerability discussed above, the attacker then uses the Kaseya VSA platform to drop a file (agent.crt) that is base64 encoded to the Kaseya Working directory (C:/kworking), which will then be delivered as part of a malicious hotfix update to the VSA agents running in managed Windows systems. This would be classified as Technique T1195.002 Supply Chain Compromise: Compromise Software Supply Chain and fall under TA0001 Initial Access for its MITRE classification.

Execution/PowerShell

The attack moves from the Kaseya VSA servers to the VSA Agents running in managed Windows systems.

First, a PowerShell command is launched by the C:/Program Files (x86)\Kaseya\[id]\AgentMon.exe process. The AgentMon.exe process is a component of the Kaseya VSA Agent Software, and as such, it has full administrator access. This action is a component of the malicious update that was dropped in the previous section. PowerShell for command execution would be classified as MITRE Attack Execution Technique T1059.001 Command and Scripting Interpreter: PowerShell. The PowerShell command is quoted below:

"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul & C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe" (Özarslan, 2021)

While this command may look like an impenetrable wall of text, it is easier to understand if broken down into sections. The first section of the command, "/c ping 127.0.0.1 -n 4979 > null &" may actually be " /c ping 127.0.0.1 -n #diffSec# >> null", but this varies depending on the source. However, the intent of this section of the command remains the same regardless of the source. It is a ping to the default loopback address that sleeps for the time defined by the diffs variable determined by a calculation made when the malicious update initially infects the machine. According to the huntress rapid response blog on the Kaseya VSA Incident, this command "effectively coordinates a synchronized attack at exactly 1630 UTC across all victims" (Hammond, 2021).

Next, the command disables Windows Defender's Real-Time Protection feature. This technique is a well-known Defense Evasion Tactic, and it would be classified as TA0005 Defense Evasion T1562.001 Impair Defenses: Disable or Modify Tools. This is done with the following section of the command:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true

Next, the command disables other features of windows defender, such as scanning of downloaded files, scanning of scripts during malware scans, the intrusion prevention system, and more. This is done with the following section of the command:

-DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend

After impairing Windows Defender, the PowerShell command copies the certutil.exe file from the C:\Windows\System32 directory and pastes it in the C:\Windows\ directory as cert.exe. Once cert.exe has been created, the PowerShell command appends a random number to the end of the cert.exe filename to evade hash-based detection rules. The alteration of the location and file name of cert.exe would be classified as MITRE Attack Defense Evasion Tactics. Specifically, this action is Technique T1036 Masquerading. This is done with the following section of the command:

& copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe

Next, the PowerShell command decodes the base64 encoded agent. crt file dropped earlier and saved it as agent.exe. Decoding an obfuscated file would be classified as MITRE Attack Technique T1140 Deobfuscate/Decode Files or Information during the initial obfuscation of the agent. crt file would be classified as MITRE Attack Defense Evasion Technique T1027 Obfuscated File or Information. The decoding is done with the following section of the command:

& C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe

Next, the PowerShell command removes the agent.crt and cert.exe files. This action falls under MITRE Attack Defense Evasion Technique T1070.004, Indicator Removal on Host: File Deletion. This action is taken to minimize the attacker's footprint. This is done with the following section of the command:

& del /q /f c:\kworking\agent.crt C:\Windows\cert.exe

Lastly, the PowerShell command executes the now decoded/deobfuscated agent.exe file. The agent.exe file is digitally signed using a valid certificate from "PB03 Transport LTD". The use of a valid certificate falls under MITRE Attack Defense Evasion Technique T1553.002 Subvert Trust Controls: Code Signing. This bypasses potential security policies that require a program to be signed with a valid certificate to run on a system. It is currently unknown how the attacker acquired the key required to sign the code. This is done with the following section of the command:

& c:\kworking\agent.exe”

Persistence, Privilege Escalation, and Impact

The launching of the agent.exe file concludes the PowerShell section of the attack. Next, the Agent.exe file extracts two different embedded binaries. These files are named MsMpEng.exe and mpsvc.dll. When the agent.exe file is executed, these files are extracted to the C:\Windows directory. The file MsMpEng.exe is a legitimate Microsoft Defender executable file. To be specific, it is version 4.5.218.0 signed by Microsoft on March 23, 2014. (Columbia SPS, 2021).

Why would attackers want to install an antivirus program on a target machine during their attack? The answer is simpler than you would think. This specific version of Windows Defender has a vulnerability to DLL side loading, and as such, it is used to launch the other file previously embedded in Agent.exe, mpsvc.dll. The action would be classified as MITRE Attack Persistence, Privilege Escalation, and Defense Evasion Technique T1574.002 Hijack Execution Flow: DLL Side-Loading. When MsMpEng.exe runs, it uses the mpsvc.dll to load an exported function from a Malicious library. Next, the function loads the ransomware payload into the system memory and executes it. This action would be classified as MITRE Attack Impact Technique T1486 Data Encrypted for Impact.

MITRE ATT&CK Breakdown

Below is a list of the MITRE ATT&CK Techniques and Tactics used in this attack:

Initial Access:

- T1078 Valid Accounts
- T1195.002 Supply Chain Compromise: Compromise Software Supply Chain

Execution

- T1059.001 Command and Scripting Interpreter: PowerShell.

Persistence

- T1574.002 Hijack Execution Flow: DLL Side-Loading

Privilege Escalation

- T1574.002 Hijack Execution Flow: DLL Side-Loading

Defense Evasion

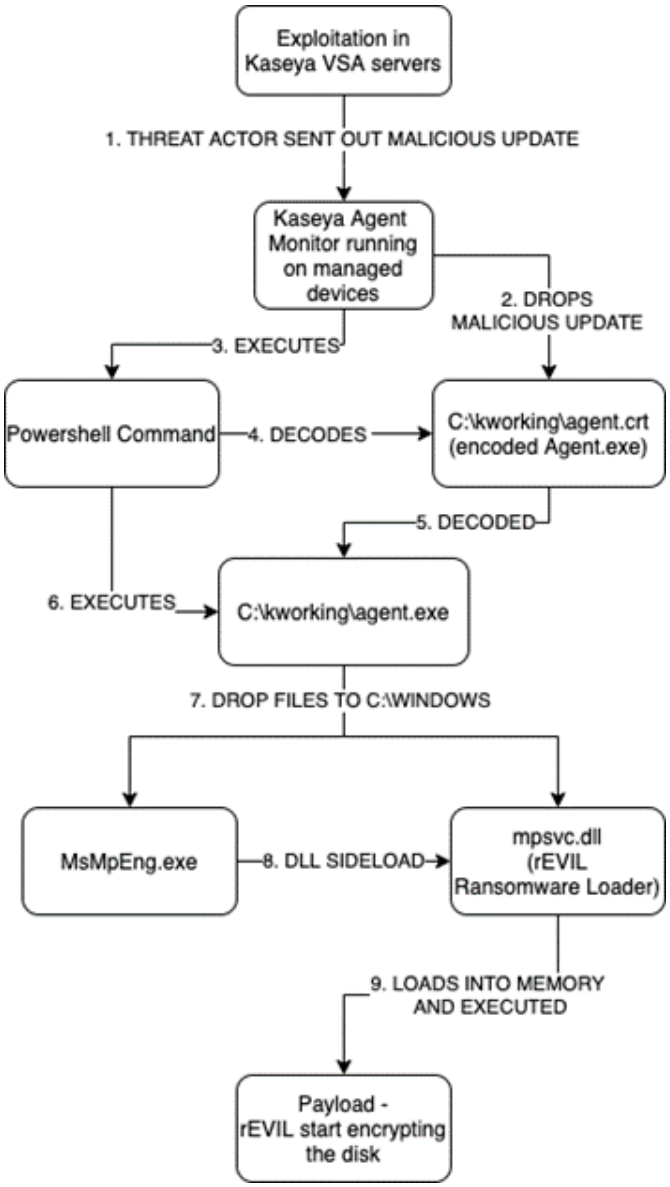
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1036.003 Masquerading: Rename System Utilities
- T1027 Obfuscated File or Information.
- T1140 Deobfuscate/Decode Files or Information
- T1070.004, Indicator Removal on Host: File Deletion
- T1553.002 Subvert Trust Controls: Code Signing.

Summary

The Kaseya VSA attack is characterized primarily by its emphasis on defense evasion techniques and its wholly automated process for infecting a machine. This approach comes with positives and negatives for the attackers. The positive aspect of this approach is that due to its automated and synchronized nature, all systems are infected simultaneously, reducing the chance for countermeasures to be developed. The negative aspect of this approach is that the lack of "touch" involved in this attack means that only a small percentage of vulnerable servers were compromised. Many vulnerable systems avoided the attack simply due to misconfigurations. The following graphic was taken from the Spider Labs Blog,

Figure 11

Post-Exploitation Execution Flow Chart



Note: (Mendrez & Kazymirskyi, 2021)

This graphic does a good job of creating a visual representation of the process flow of the Kaseya VSA attack. First, the compromised Kaseya VSA Update servers send out a malicious update to a Kaseya Agent Monitor. This update drops the agent.crt file and then executes the PowerShell command. Once the agent. crt file is decoded; it is then executed. Next, agent.exe drops MsMpEng.exe and mpsvc.dll and then use MsMpEng.exe to dll sideload mpscd.dll. Mpsvc.dll then loads into memory and executes the encryptor payload.

Technology Based Solutions

In this section, this research will recommend solutions and prevention, and mitigation measures regarding ransomware attacks. The topics covered within this section will include backups, Endpoint Detection, Least Privilege Access, Antivirus software, Intrusion Prevention Systems, and User training.

Backups

Backups have always been the number one solution to dealing with ransomware attacks. Since a ransomware attack aims to encrypt your systems to deny you use, a simple solution is to back up all your business's critical resources. However, ransomware has been developed in recent years that targets your central systems resources and any potential backups on-site. Due to the uptick in this recent trend, the new recommendation is to have Air-Gapped Backups. Air gapped backups are kept in a system disconnected from the internet and all networks except a local/private internal network. By storing backups in this manner, an administrator can ensure that the backups will not be tampered with even if the primary network/system has been compromised.

Endpoint Detection and Response

Endpoint Detection and Response sometimes referred to as an EDR, is a software solution that continually monitors and responds to mitigate security threats. This is done by installing an agent on each endpoint, and the agent then sends behavioral data to the central database for analysis. Modern Day EDR's have started to use Artificial Intelligence to assist in the analysis of behavioral data. First, Artificial Intelligence analyzes an extensive data set to establish a baseline for endpoint behavior. Once the baseline has been set, any endpoint behavior that goes outside of the established baseline sends an alert to an administrator.

Antivirus

This point cannot be stressed enough, primarily because of how effortless it is. First, an organization must keep whatever antivirus software they choose to use up to date. This is usually done through a scheduled task that runs at the end of the week to check for updates. Keeping antivirus up to date helps to prevent users from unintentionally installing malicious software, and as such, the value of it cannot be overstated. During the demonstration section of this research,

the value of antivirus software is quite evident due to how difficult it is to install malicious software even when it is done intentionally.

User Training

User Training is of paramount significance in today's current landscape of cybersecurity. The importance of User Training is due to the prevalence of phishing tactics used by threat actors. NIST defines phishing as " A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person" (NIST CSRC, *Phishing - glossary*). Phishing is one of the most common ways for a threat actor to steal a target's credentials. Threat actors commonly use phishing because it does not rely on any technical vulnerabilities; it relies on the so-called Human Vulnerability of a system. A threat actor does not need to use complicated tactics to acquire credentials when they can easily acquire them through phishing. Since phishing is an entirely human vulnerability, the only solution for it is user training. This can be done in a variety of ways. A prevalent user training method is for the security team to conduct phishing campaigns to test the users in an organization. You can identify users requiring more training and reward those who successfully identify the phishing emails by conducting phishing campaigns.

Intrusion Prevention Systems

An Intrusion Prevention System, often referred to as an IPS, is defined by NIST as "a system which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches the target." (NIST, Intrusion prevention system (IPS) - glossary) An IPS can help to prevent malicious software from spreading throughout your network. Most IPSs continuously monitor the network and compare it to an established network performance/statistics baseline. Whenever the IPS detects something malicious, it alerts a security analyst and takes what actions it can to prevent the event from impacting the network. Many of the newer ransomware strains have some form of self-propagation. The only way to detect and respond to these incidents quickly is by using an Intrusion Prevention System or an Intrusion Detection System. IPS/IDS systems come in various forms, some are network-based, and others are host-based. The decision between a host-based and a network-based IPS entirely depends on the sorts of systems you are trying to secure. It is not uncommon to see an organization implement both types of IPS in a large-scale enterprise environment.

Policy Based Solutions

Almost any organization that uses computer in the modern-day landscape can benefit from having a security policy. Security Policy is a very broad topic so this research will not attempt to cover it in its entirety. Instead, this research aims to address the specific pieces of security policy that are helpful in countering ransomware attacks.

Least Privilege Access

Least Privilege Access is the concept of giving users the least amount of privilege they need to do their job. This is typically done by giving read-only access to everyone other than designated power users. By implementing a policy of least privilege access, an organization can drastically reduce the attack surface of their systems. Least Privilege Access also ensures that if standard user accounts are compromised, the damage will be minimal. Suppose an attacker wants to gain meaningful access to a system with a least privilege access policy to do any real damage. In that case, they must target an administrator, or some other kind of power used to get sufficient credentials. This policy will not prevent an attack from happening, but it helps put more obstacles in an attacker's path.

Security Audits

Security Audits have only recently become standard practice for all organizations. A security audit is defined by NIST as an, “Independent review and examination of a system’s records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.” (NIST, Security Audit - Glossary) Essentially the purpose of an audit is to ensure that an organization is following its own security policy as well as any laws and or regulations that may apply to the organization. By conducting audits on a regular basis an organization can ensure that it is following its own guidelines and best practices dictated in the security policy as well as any legal requirements the organization might have. An audit is also helpful for identifying areas in which a company can improve its security policy to fit better within industry standards. Annual security audits should be conducted by a licensed and certified third-party contractor. Internal security audits can also be performed by the internal security team, however an external organization must conduct security audits if they are for the purposes of Governance, Risk, and Compliance or legal requirements. Different industries have different legal requirements based on a variety of factors such as the sensitivity of the data that they are handling or the organizations status as a contractor for the federal government.

Incident Response Plan

An Incident Response Plan is defined by NIST as, “The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information systems(s).” (NIST, Incident response plan - glossary) An Incident Response Plan should contain all of the materials your organization requires should an incident occur. An Incident Response Plan should contain the structure of the incident response team, the roles of each member on the team, and the assigned responsibilities for each role. In addition to this it should also include a framework to abide by during the incident response process, the standard frameworks used are the NIST Incident Response Process and the SANS Incident Response Process. These Frameworks define the stages and

procedures within an incident response plan. The incident response plan should also include examples of incidents and definitions of incident severity ratings.

Disaster Recovery Plan

A Disaster Recovery Plan is similar to an incident response plan but also quite different. The purpose of a Disaster Recovery Plan is not to respond to an incident, instead its purpose is to get your systems back online in a timely and orderly fashion. An Incident Response Plan defines how an organization will respond to an incident; Disaster Recovery defines how the organization will go about getting it systems back online. NIST defines Disaster Recovery as, "A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities." (NIST, Disaster recovery plan (DRP) - glossary) It is hard to define what a normal disaster recovery plan contains because it is almost entirely dependent on the context and circumstances of the particular organization in which it applies. A Disaster Recovery Plan may attempt to provide a blueprint to recovering from service disruptions such as Ransomware, Environmental Catastrophes (tornados, hurricanes, earthquakes, fires), Building Accessibility, Power Disruption, Hardware Failures, Software Failures, and Employee Errors. A disaster recovery plan should be tested at least once yearly to ensure that it will function properly.

Backup Testing

If an organization uses backups to mitigate security risk, then it should also test its backups. If the backups aren't tested, then how can anyone know if they will work? Backup testing has been around for a while, but only recently became relevant due to the threat of ransomware. If an organization has backups, it is recommended to test them at least once yearly. This will ensure that if a situation arises in which you need to use your backups, they will work. Without backup testing it is impossible to know if your backups will work when you need them to. If your organization is heavily reliant on backups for disaster recovery it advisable to recommend backup testing semiannually or even quarterly. Guidelines for how often an organization should test their backups should be dictated within either the organizations general security policy or the disaster recovery plan. Back Up Testing should ideally be a component of an organization's Disaster Recovery Testing.

Vulnerability Scanning

Vulnerability scanning is an incredibly useful tool for an organization's security team. Vulnerability scanning is defined by NIST as, "A technique used to identify hosts/host attributes and associated vulnerabilities." The reason vulnerability scanning is such a valuable tool is because it gives an organization security team a rare opportunity to examine the network from the perspective of an attacker. Vulnerability scanning may also help with patch management which will be discussed in the next paragraph. By routinely running vulnerability scans on the network an organization's security team can ensure that it is at the very least aware of all

vulnerabilities throughout the systems. Vulnerability scanning tools are available for free, but there are also organizations that sell proprietary vulnerability scanning software. Free vulnerability scanning programs should be sufficient for most small and medium sized organizations. An organization should have a section in its security policy for vulnerability scanning. The policy should include how often scans will be conducted, roles, responsibilities, and identification of the vulnerability scanning team, the systems to be scanned, and documentation identifying current vulnerabilities in the system as well as ranking them on levels of severity.

Patch Management

Many vulnerabilities are the result of unpatched software. Whenever a vulnerability is discovered by a security researcher it is reported to the supplier who then works on fixing the software. Once they have fixed the vulnerability, the supplier releases what is known as a patch. A patch is an update to the software that aims to fix newly discovered issues. A patch may sometimes also be referred to as a bug fix or a hot fix in popular media. The distribution and application of these patches throughout an organizations network is called Patch Management. An organization security policy should have a section addressing patch management. The section should include an inventory of your systems, roles, responsibilities, and identification of the patch management team, details on the patch management software and deployment, a patch testing policy, a patching schedule, and documentation of the process. By implementing a robust patch management policy an organization can ensure that its systems will not be running vulnerable patches of software unless absolutely necessary.

Hypothesis Analysis

Accessibility/How easy is it to find ransomware?

This was discussed briefly in a previous section but finding ransomware on the internet is quite an easy task if you know where to look. The most obvious and easy answer to finding an example of actual ransomware is to look on google search "GitHub ransomware repositories," and you will find what you are looking for. If the goal is to find a specific strain on ransomware, then the task is not beginner-friendly, but the information is still there. A minor detail worthy of consideration is that any ransomware found on the internet with ease will be detected by the most recent Antivirus Solutions and EDR systems. Threat intelligence is the cybersecurity sector responsible for supplying antivirus software and EDR solutions with large amounts of data on nearly all malware used in recent times. In summary, if you can find a piece of pre-written malware on the internet, it will probably set off some alarm.

Ease of Use

So, it has been established that finding ransomware is a trivial task. However, this poses the question, what can the average person do with access to this malicious software? Unfortunately, the answer is not much. The average user has no business attempting to deploy malware. The

only way an average person could successfully deploy ransomware is with someone with expertise supplied pre-written software. While this may sound like something out of a spy thriller, there is some precedence for insider attacks in the real world. However, insider attacks can be countered by following best practices like least privilege access and physical access control and software like a Behavior-Based XDR Solution.

How Dangerous?

Ransomware poses a unique and ever-evolving threat in the cybersecurity sector. Prior to the ransomware threat, there was no substantial financial incentive to become a threat actor. Nevertheless, ransomware has existed since the 1990s, so how does that make any sense? Cryptocurrency. The proliferation of cryptocurrency is the primary reason for the new interest in ransomware by threat actors across the globe. It represents a way to get paid without dealing with banks, police, or anything representing a traditional institution. A hacker can infect a target's system, receive the ransom payment, and decrypt the system without leaving their seat, and it is thanks, at least in part, to cryptocurrency. Many governments have begun to crack down on cryptocurrency, but that is easier said than done due to the technology's decentralized nature.

In summary, due to the significant financial incentives, it is expected that ransomware will continue to proliferate and pose a sizeable economic threat to developed nations. Systems will always have vulnerabilities, and someone will always click a link they know they should not; this is why having a layered security approach is essential. The risks posed by ransomware will continue to grow if the financial incentive remains.

Discussion

There is a political aspect to the issue of ransomware that is seldomly talked about in public circles and is generally only known to those in the cyber security field. However, it is an essential detail when addressing the threat of ransomware on a global level. It is all but confirmed that Russia and other Eastern European countries in the Russian Sphere of influence are giving ransomware operators safe harbor if they refrain from targeting entities that would be considered allies. This conclusion is supported by a common feature of any Ransomware that comes out of Eastern Europe. There are a variety of forms of ransomware written by Revil that will not run on a system that has a default language that is native to eastern Europe. By including this threat, actors ensure that they do not jeopardize their haven in Russia. By implementing this all but confirms that the ransomware operators are government-sanctioned. If these operators indeed are sanctioned on some level by the Russian government, then Russia represents the most significant roadblock to apprehending ransomware operators in the entire world. The FBI can take down as many dark-web websites as they want to, but their efforts amount to nothing if they cannot apprehend the individuals responsible for the operation. If these criminals cannot be apprehended, then ransomware will continue to be a sizeable threat for the foreseeable future.

Conclusion

To conclude, the threat of ransomware only grows day by day. While it may be easy to find, the creation, implementation, and configuration require significant technical expertise. Your first line of defense against ransomware and any malware should be user training. Many IT professionals see users as a vulnerability. However, well-trained users are an invaluable asset. Well-trained users help make the job of a system administrator easier by helping to alert the system administrator when they notice something is off. User-Training is the difference between having users that serve as vulnerabilities to your system's security and having users that serve as an asset to the security of your system. Backups are your last line of defense. Backups alone do not make you immune to ransomware attacks, as many would lead you to believe. If you want your backups to be "ransomware-proof," they need to either be air-gapped on-site or stored off-site in a completely different location. If Backups are integral to an organization's disaster recovery plan, it is conceivable to recommend both. Antivirus is the standard defense against malware; it is inconceivable to use computers without antivirus in today's world of cyber security. If cybersecurity is integral to your organization, it is recommended that you implement some form of EDR solution and some form of IPS solution. These two technologies are at the core of a modern cyber security architecture. To summarize, ransomware is incredibly dangerous in the right hands, and to defend against it, an organization must take a layered approach to security. Additionally, ransomware will continue to be a problem in the foreseeable future as long as Russia gives operators safe harbor and allows anonymous financial transfers.

References

LLC, J. S. (n.d.). Automated malware analysis. Joe Sandbox Cloud Basic. Retrieved September 11, 2021, from https://www.joesandbox.com/#windows.

MITRE ATT&CK®. (n.d.). Retrieved from https://attack.mitre.org/

Glossary. (2019, February 28). Retrieved November 2021, from https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

Abrams, L. (2021, September 11). *Revil ransomware is back in full attack mode and leaking data*. BleepingComputer. Retrieved November 11, 2021, from https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/.

Tidy, J. (2021, July 13). REvil: Ransomware gang websites disappear from the internet. Retrieved from https://www.bbc.com/news/technology-57826851

Mendrez, R., & Kazymirskyi, N. (2021, July 7). *Diving deeper into the Kaseya VSA attack: Revil returns, and other hackers are riding their coattails*. Trustwave. Retrieved November 11, 2021, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/.

Gevers, V. (2021, July 3). *Kaseya Case updates 2*. DIVD CSIRT. Retrieved November 11, 2021, from https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/.

Oudshoorn, L. (2021, July 7). *DIVD-2021-00011 - Kaseya VSA Limited disclosure*. DIVD CSIRT. Retrieved November 11, 2021, from https://csirt.divd.nl/cases/DIVD-2021-00011/.

CVE-2021-30116. CVE. (2021, July). Retrieved November 11, 2021, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116.

Özarslan, S. (2021, July 4). *TTPs used by Revil (Sodinokibi) ransomware gang in Kaseya MSP Supply-Chain attack*. Picus Security. Retrieved November 11, 2021, from https://www.picussecurity.com/resource/blog/revil-sodinokibi-ransomware-kaseya-vsa-msp-supply-chain-attack.

Hammond, J. (2021, July 3). *Rapid response: Mass MSP ransomware incident*. Huntress. Retrieved November 11, 2021, from https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-incident.

Columbia SPS, (2021, August 12). *REvil Ransomware Kaseya Supply-Chain Attack: Analysis and Countermeasures* [Video]. YouTube. https://www.youtube.com/watch?v=WHqXZcXgpjs&ab_channel=ColumbiaSPS

Sh1n0g1 Inc. (2016). ShinoLocker. Retrieved November 15, 2021, from https://shinolocker.com/

VirusTotal. (n.d.). How it works – virustotal. VirusTotal. Retrieved November 15, 2021, from https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works.

NIST CSRC. (n.d.). *Virtual machine (VM) - glossary*. CSRC. Retrieved November 15, 2021, from https://csrc.nist.gov/glossary/term/virtual_machine.

NIST CSRC. (n.d.). *Phishing - glossary*. CSRC. Retrieved November 15, 2021, from https://csrc.nist.gov/glossary/term/phishing.

NIST CSRC. (n.d.). *Intrusion prevention system (IPS) - glossary*. CSRC. Retrieved December 9, 2021, from https://csrc.nist.gov/glossary/term/intrusion_prevention_system.

NIST CSRC. (n.d.). *Disaster recovery plan (DRP) - glossary*. CSRC. Retrieved December 9, 2021, from https://csrc.nist.gov/glossary/term/disaster_recovery_plan#:~:text=2%20under%20Disaster%20Recovery%20Plan,failure%20or%20destruction%20of%20facilities.

NIST CSRC. (n.d.). *Incident response plan - glossary*. CSRC. Retrieved December 9,2021, from https://csrc.nist.gov/glossary/term/incident_response_plan#:~:text=Definition(s)%3A,NST%20SP%20800%2D34%20Rev.

NIST CSRC. (n.d.). *Security Audit - Glossary*. CSRC. Retrieved December 9, 2021, from https://csrc.nist.gov/glossary/term/security_audit.