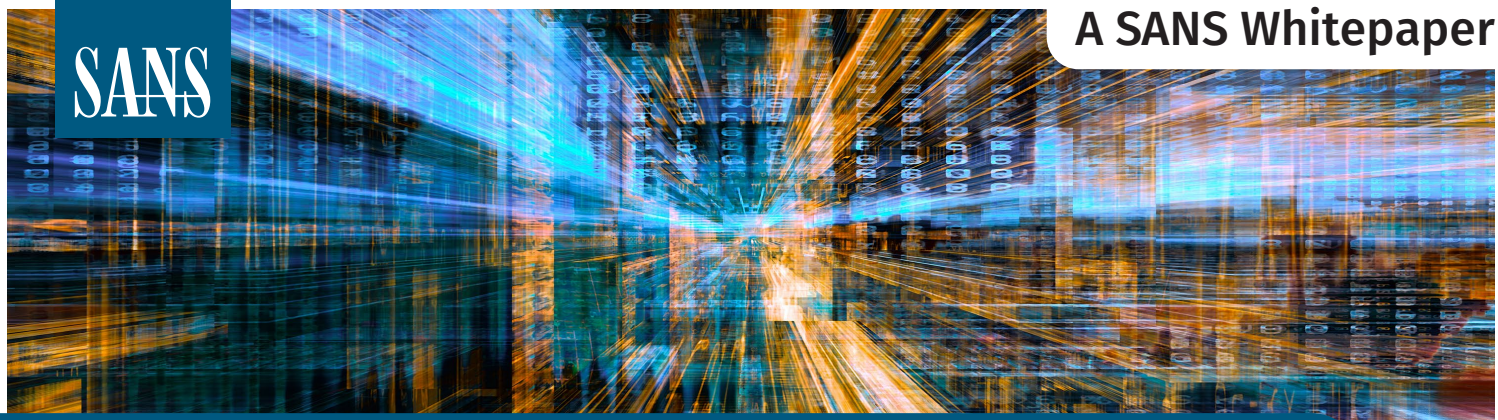
SANS

A SANS Whitepaper



Ransomware Prevention Special Report: How to Address a Pervasive and Unrelenting Threat

Written by **Justin Henderson**

November 2020

Sponsored by:

ExtraHop

Ransomware is a fast-growing threat affecting organizations of all sizes and industries. Quick spreading and highly interruptive, ransomware damage ranges from profoundly impacting a business's finances to threatening proper healthcare by disabling access to critical data needed for medical systems and interrupting operations. Organizations need to assess the potential impact and damage from ransomware and establish a balance between prevention, detection and response capabilities. For this report, we will focus on actions that organizations can take to protect themselves from ransomware and the far-reaching damage it causes.

The critical challenge when facing ransomware is that there is no silver bullet. In fact, ransomware symbolizes the ongoing challenges organizations face in information security. A combination of proper security hygiene, detection, prevention techniques, and detection and response capabilities is required to combat ransomware successfully. This paper aims to help organizations identify what ransomware is, the threats it might pose and how to defend against it.

This paper initially covers common infection vectors and how ransomware spreads. Both aspects provide an understanding that is helpful to know before covering prevention and detection techniques. As such, the recommendation is to read the paper from start to finish. However, if you already know the history of ransomware, feel free to move throughout the paper at your leisure—although one exception is the deep dive into RIPlace, which may clarify how ransomware changes over time.

Analyst Program

The History of Ransomware

Ransomware is a form of digital extortion executed via malware that prevents recipients from accessing their own data, often by encrypting the data. After a victim's access has been removed, the victim is presented with a ransom demand. The ransom demand is usually a request for money, often in the form of cryptocurrency, such as Bitcoin.

Initial ransomware attacks started in 1989 in the form of mass-spreading drive-by downloads that targeted anyone and everyone. These early forms of ransomware were more akin to viruses or worms, except for the added ransom demand. Starting in 2018, the trend began to change. Previously, organizations faced automated broad-based attacks, but now they encounter highly targeted and more sophisticated ransomware attacks.[1] Modern ransomware attacks might involve human-operated ransomware (also referred to as "ransomware-as-a-service [RaaS]") or multistage ransomware, such as double extortion. Double extortion refers to ransomware that exfiltrates, encrypts and extorts. With this type of ransomware, the attacker demands payment not only to decrypt the data, but also to prevent the data from being publicly leaked. The latter method has serious consequences for organizations because having backups does not protect them against potential data leakage.

Generally speaking, there are two types of ransomware: broad and targeted. Broad-based ransomware is indiscriminate about the victims it chooses. The end goal is to spread and infect, then simply demand ransom. In contrast, targeted ransomware focuses on a specific victim or industry. Both types are multistage, but the level of effort and sophistication changes. In the 1980s, the AIDS Trojan was distributed to members of the World Health Organization (WHO) via floppy disks. Soon after, ransomware began to take on familiar forms of drive-by downloads, mass email campaigns and internet-based worms.

In 2017, ransomware attacks started to evolve rapidly, and the attacks became more sophisticated. They were spread not only via social engineering, but also by using server-side exploits and stolen credentials. For example, NotPetya can compromise one unpatched machine and put an entire organization at risk. After compromising the initial machine and stealing credentials, NotPetya then uses those credentials against the rest of the organization to lock out systems and demand ransom. Also in 2017, criminals began to pay for RaaS, as we saw in the Cerber ransomware attacks.

Each year, new variations of ransomware are found. For example, in 2019, RIPlace became a serious threat because it found new methods of encrypting files that evaded antivirus and endpoint detection and response (EDR) solutions. In 2020, double extortion attacked universities. While some were able to restore their data from backups, these universities still had to pay the ransomware gang to prevent them from leaking student data.[2] Figure 1 on the next page provides a timeline of some of the known ransomware variants and their characteristics.

---

[1] "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," FBI Public Service Announcement, Alert Number I-100219-PSA, www.ic3.gov/media/2019/191002.aspx

[2] "University of Utah pays $457,000 to ransomware gang," www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang

Damage from ransomware is something all organizations need to consider. Small businesses and large enterprises alike have been infected with ransomware. Merck, the pharmaceutical giant, lost more than $300 million in the third quarter of 2017 due to NotPetya and is currently in litigation with insurers for $1.3 billion.[6] Researchers at Vanderbilt University's Owen Graduate School of Management conducted a study of patient mortality rates at more than 3,000 hospitals, 10% of which had experienced a data breach. Based on this study, a possible correlation showed that as many as 36 additional patient deaths per 10,000 heart attacks occurred at the hospitals that reported being a victim of ransomware.[7] Other healthcare-related reports arose, such as a woman dying at a hospital in Düsseldorf, Germany, where it is believed that ransomware contributed to a lack of ability to provide proper healthcare treatment.[8] The Heritage Company, a telemarketing firm, was forced to suspend operations for 300 employees right before Christmas 2019 due to ransomware.[9]

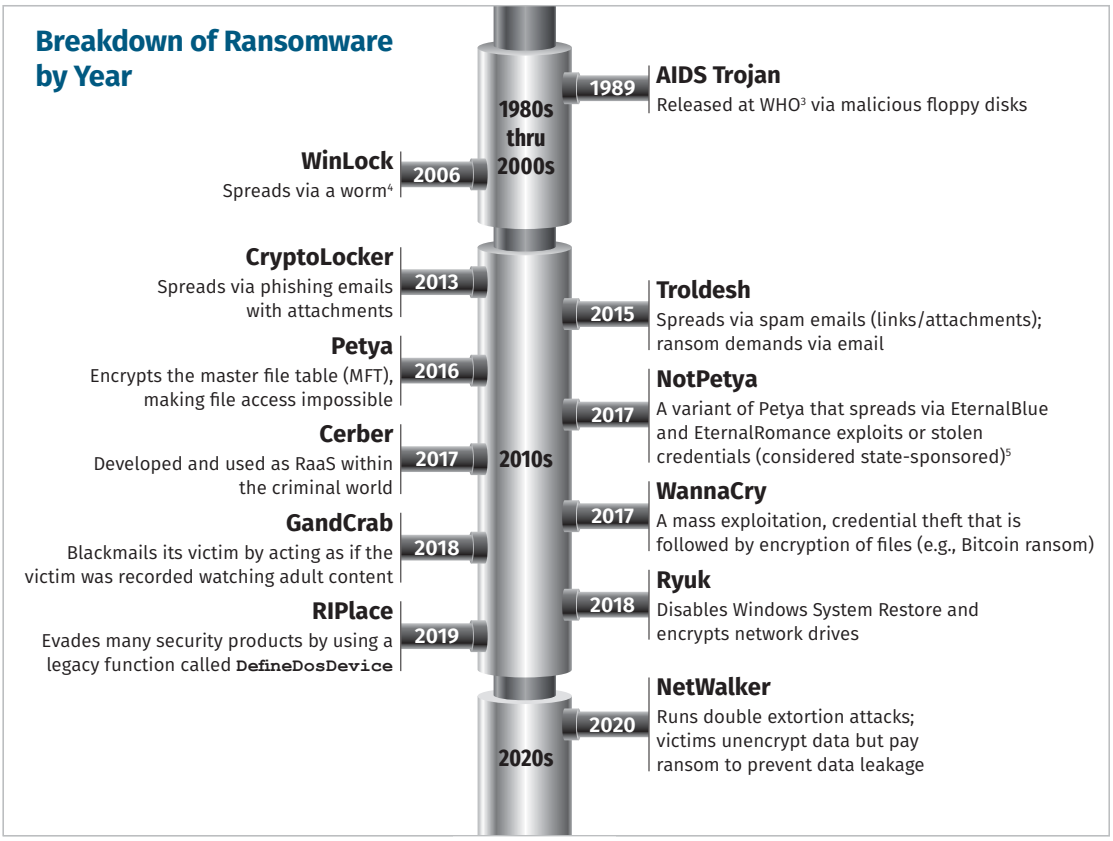


Figure 1. Ransomware Evolution Timeline

In many cases, organizations have chosen to pay the ransom to regain access to their data or stop the attackers from leaking it due to payment demands from double extortion. However, advisories posted in the third quarter of 2020 by the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) may affect the decision to pay ransoms in the future. The OFAC advisory,[10] in particular, warns that companies might be sanctioned for paying the ransom, because it encourages terrorism and other criminal activities.

---

[3] "Case Study: AIDS Trojan Ransomware," www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware

[4] "WinLock Ransomware," www.knowbe4.com/winlock-ransomware

[5] "Petya ransomware and NotPetya malware...," www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[6] Merck in $1.3B showdown with insurers over 2017 ransomware attack," https://endpts.com/merck-in-1-3b-showdown-with-insurers-over-2017-ransomware-attack-bloomberg

[7] "Study: Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks," https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks

[8] "A Patient Dies After a Ransomware Attack Hits a Hospital," www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital

[9] "Ransomware Attack Topples Telemarketing Firm, Leaving Hundreds Jobless," https://threatpost.com/ransomware-attack-topples-telemarketing-firm/151530

[10] "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Evolution of Ransomware: A Case Study of RIPlace

Cyber defense is an ongoing game of cat and mouse where attackers come up with new tools and methodologies while defenders, in turn, develop new security tools and controls. That holds true with ransomware. Early variants of ransomware used encryption tools to find and replace files, or even an entire OS, with encrypted content. However, modern endpoint suites, including antivirus and EDR, quickly adapted and do well with preventing and detecting ransomware. The problem, as always, is that attackers continue to evolve in order to bypass such controls. RIPlace is an example of malware that has evolved to include evasive measures.

In early 2019, Nyotron's security research team identified a new ransomware technique that appears to be undetectable by many security products.[11] The lack of detection is due to the ransomware's encryption method, which is unlike prior ransomware. Prior to RIPlace, ransomware encrypted files by reading the original file, encrypting the contents in memory and then destroying the original file with one of the methods shown in Figure 2.

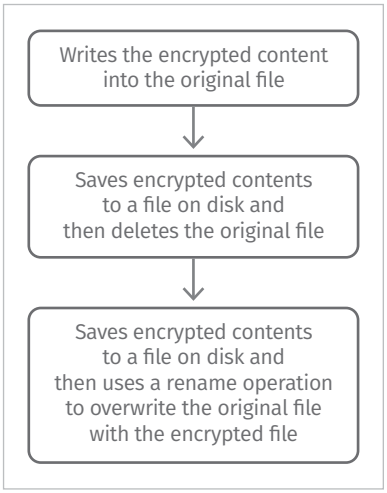


Figure 2. Encryption Prior to RIPlace

Most security products focus on various file operations in an attempt to identify ransomware behavior. For example, when an encrypted file is being renamed over an existing file, there is a call to **`IRP_MJ_SET_INFORMATION`** with the **`FileInformationClass`** set to **`FileRenameInformation`**. Such a process can be monitored with tools such as Sysinternals Process Monitor (ProcMon) or various security products. However, RIPlace adds a step in front of the system call for issuing a rename. RIPlace first calls **`DefineDosDevice`**, which allows passing any value as a device name followed by the file path such as a symlink. By doing so, the rename operation returns an error rather than the file path of the rename. Yet, the rename operation succeeds. Figure 3 shows the output of the rename operation.

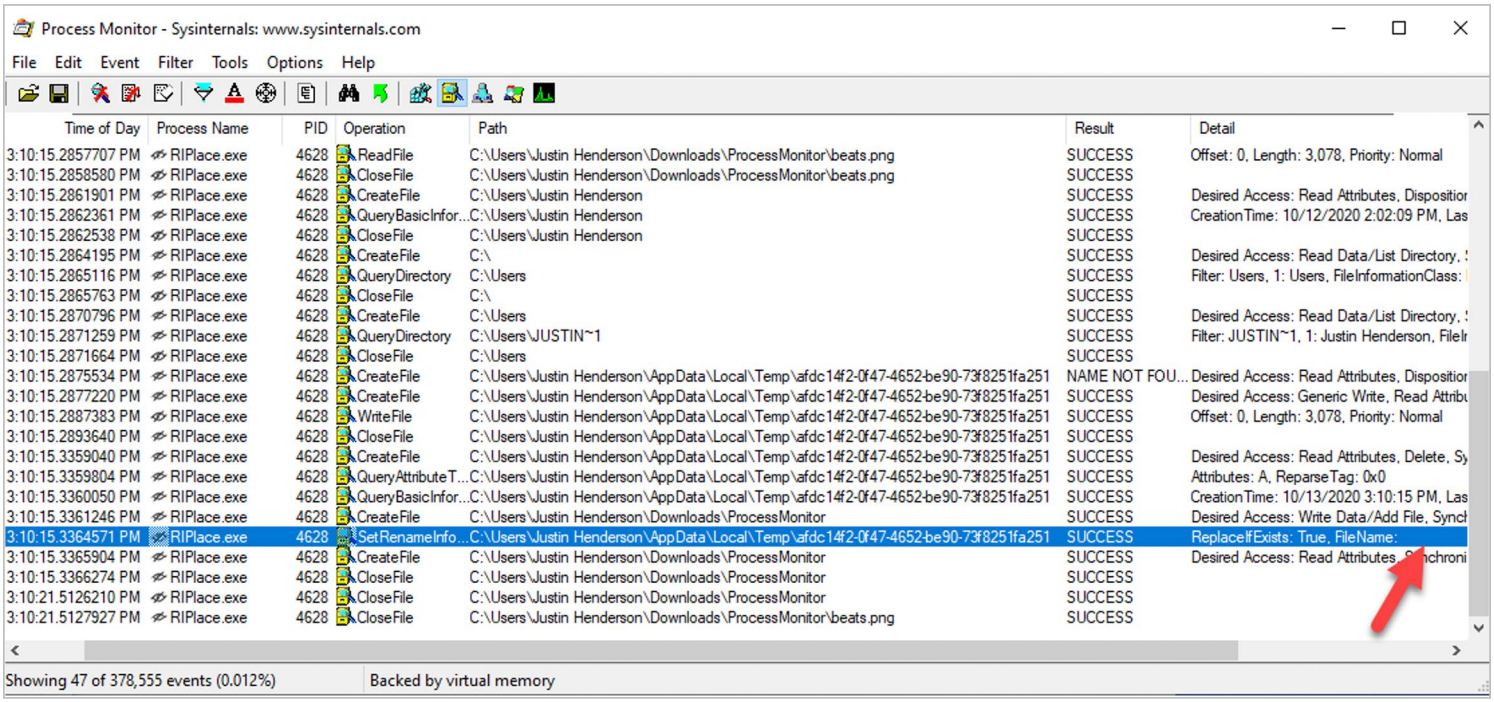


Figure 3. RIPlace File Rename Operation

[11] "RIPlace Evasion Technique," www.nyotron.com/collateral/RIPlace-report_compressed-3.pdf

Due to the failure to return a destination file path, the result is a lack of visibility into a file rename operation. In turn, many security solutions—including dedicated anti-ransomware products—are unable to detect RIPlace. Thus, security controls again must adapt to new ways of identifying such an attack. The next sections will focus on areas to prevent and detect both traditional and modern ransomware variants, such as RIPlace. Organizations can download RIPlace, a free tool from Nyotron, to evaluate if this evasion technique will succeed against their computer systems.

Mitigating the Widespread Damage of Ransomware

Because there are multiple variations of ransomware and various delivery methods, there is no single method to prevent ransomware from executing. To provide guidance, the Computer Emergency Readiness Team (US-CERT) released Security Tip (ST19-001), "Protecting Against Ransomware."[12] The recommendations given in this section align with US-CERT's guidance. The goal is to implement various processes or controls that will stop ransomware from successfully operating.

Vulnerability Management (VM)

Some variants of ransomware exploit server-side code, including flaws in the Windows operating system or vulnerabilities in internet-facing services, such as Remote Desktop Protocol or VPN appliances. Even ransomware attacks via drive-by downloads or email attachments include exploits against client-side software, such as Adobe Reader. As a result, proper vulnerability management can significantly aid in preventing ransomware from running. Vulnerability management should include the following best practices:

- Apply software and operating system patches or use firmware to prevent spread via known exploit vectors, such as EternalBlue.
- Ensure secure coding and web development to prevent ransomware via web application abuse.
- Remove unnecessary and high-risk services, such as SMB1, SSDP and LLMNR, to prevent attack vectors relying on legacy or unused services.
- Secure high-risk services, such as RDP, through the use of restricted IP addresses, IPSec, placement behind VPNs, enabling network level authentication and other service-related controls.
- Implement hardening and security baselines, such as CIS Benchmarks,[13] to prevent attacks by adding defense-in-depth mechanisms such as preventing credential theft and reuse by ransomware.
- Remove administrative accounts to prevent the spread of infections by limiting credential theft capabilities or use, as well as limit overall ransomware capabilities.
- Implement two-factor authentication to limit the damage of stolen credentials.
- Consider Microsoft attack surface reduction (ASR) rules to limit Microsoft Office and other common programs, such as Adobe Reader, from running executables, macros or other dangerous functions.

Ransomware prevention is part good practice and part of software controls. Keep in mind that some of the most effective prevention capabilities are free.

[12] "Security Tip (ST19-001) Protecting Against Ransomware," https://us-cert.cisa.gov/ncas/tips/ST19-001

[13] "CIS Benchmark Hardening/Vulnerability Checklists," www.newnettechnologies.com/cis-benchmark.html?keyword=Cis%20Benchmarks&gclid=CjwKCAjw_Y_8BRBiEiwA5MCBJgfa73LE6jLJ48RYHpubTCZ3kTe9wd3-uT_rXnRhvAUFx7nwgdydGxoCFLQQAvD_BwE

The primary infection vectors for ransomware are social engineering via web requests or email. As such, there are multiple web- and email-based protection mechanisms that can prevent the initial ransomware infection. These range from proxy-based controls, such as email gateways or web proxies, to endpoint controls, such as browser isolation.

Network Segmentation

Network controls should be in place to limit and detect the spread of ransomware. There are multiple mature forms of segmentation, such as network firewalls or access controls, private VLANs, host-based firewalls and denying logon rights within an operating systems.

Browser Isolation

One significant preventative control that organizations should consider is the implementation of browser isolation. With browser isolation, web access is achieved via either a local or remote process that separates the browser from the host operating system. Local isolation works by using an application-level container or sandbox. Remote browser isolation (RBI) involves moving the browser to a remote service, such as a cloud provider or on-premises server. See Figure 4.

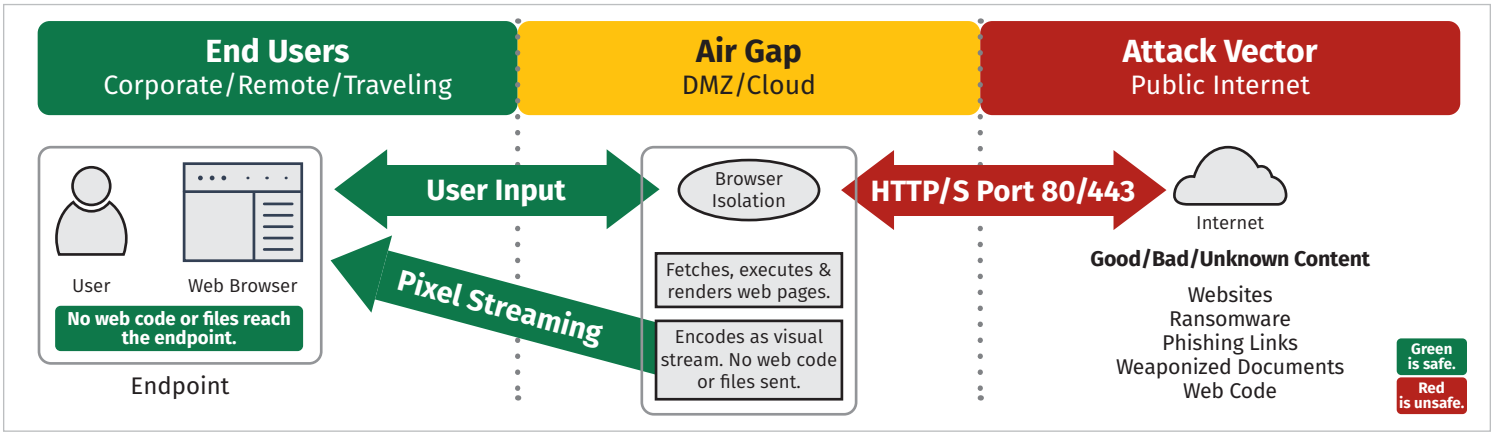


Figure 4. Browser Activity Workflow for Typical User with Isolation Implemented[14]

With browser isolation, if an end user accesses a malicious site and gets infected, the malware is captured within the local or remote isolation environment and cannot escape to the host files or operating system without first performing container escape. If the infection were ransomware, the malware is likely limited to only what the isolated browser has access to. In RBI, the remote browser is disposable, providing an extra layer of protection against persistent threats, such as ransomware, because RBI creates a new container at session startup and then disposes of the container at session end. Thus, attacks such as NotPetya, which would run Mimikatz to steal credentials and pivot, could be rendered harmless. Browser isolation is available in endpoint suites, RBI products and standalone commercial products, as well as part of Microsoft Edge within Windows 10 Pro or later (version 1709 or later). See Figure 5 on the next page. For more in-depth coverage on local and remote browser isolation check out "All Roads Lead to the Browser: A SANS Buyer's Guide to Browser Isolation."[15]

[14] "All Roads Lead to the Browser: A SANS Buyer's Guide to Browser Isolation," May 2020, www.sans.org/reading-room/whitepapers/analyst/roads-lead-browser-buyers-guide-browser-isolation-39555, p. 5, Figure 3. [Registration required.]

[15] "All Roads Lead to the Browser: A SANS Buyer's Guide to Browser Isolation," May 2020, www.sans.org/reading-room/whitepapers/analyst/roads-lead-browser-buyers-guide-browser-isolation-39555 [Registration required.]

Web Proxy

To further increase protection against malicious web traffic, web proxies can be utilized in conjunction with local or remote isolated browsers. Modern web proxies combine signature-based payload inspection, reputation scoring and behavioral analysis, as well as possible TLS inspection and malware detonation integration. As such, web proxies are well positioned as a last-ditch effort to protect against an employee who might have clicked on a phishing link. Additional web proxy capabilities that may help prevent ransomware include:

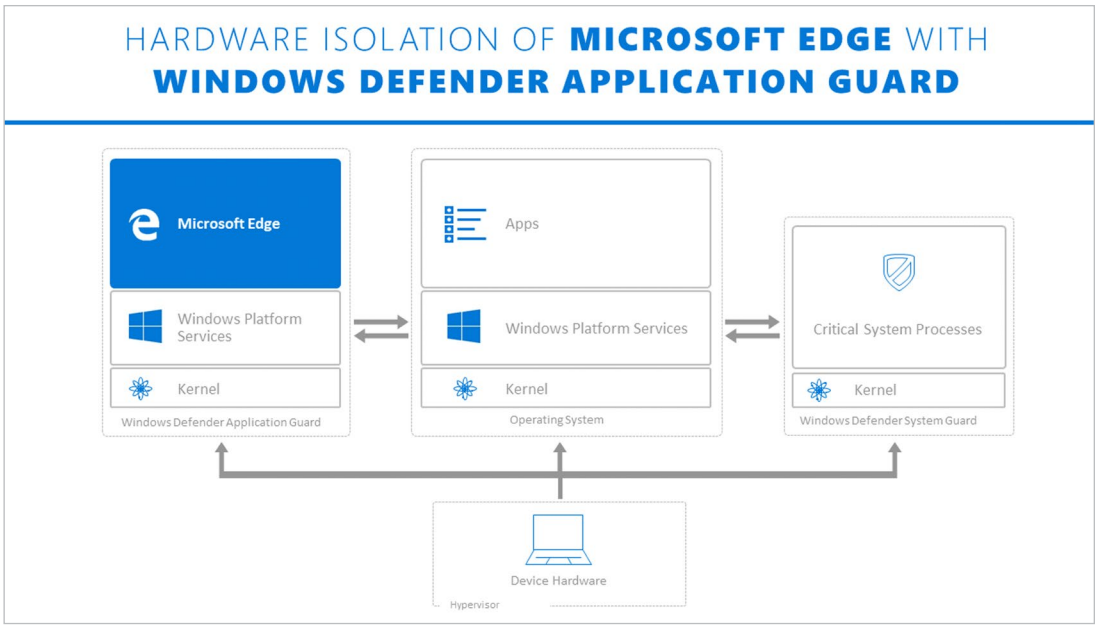


Figure 5. Browser Isolation with Microsoft Defender Application Guard[16]

- Blocking new domains
- Blocking unrated sites
- Implementing splash proxies, which warn users that they are accessing a site that the organization has not previously contacted

Email Gateway

Email continues to be one of the most common social engineering vectors. An SMTP proxy, such as an email gateway, should be in place to block malicious content and attachments. Special attention should be paid to areas with which phishing emails commonly are associated. This includes enabling sender validation frameworks, such as SPF, DKIM and DMARC. It can also include creating anti-display name spoof rules within the email security gateway to detect emails that attempt to spoof employee display names. Integration with a malware detonation system can help identify and prevent ransomware URLs or attachments.

Malware Detonation

A malware detonation system is a piece of software that runs potentially malicious tasks and observes the behavior. Execution takes place in either a virtual environment, container or emulation software so that any potential infection cannot escape. By performing behavior monitoring in conjunction with standard signature-based analysis, a malware detonation system is likely to catch ransomware because the behaviors are aggressively abnormal. For example, ransomware crawls the drive and/or network looking for files, reads them, and then encrypts and renames or deletes original files.

[16] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview

EDR Soultions

Machine learning within EDR products can identify and block ransomware with on-the-fly analysis of file attributes. If that fails and the program begins to execute, EDR falls back to the monitoring of indicators of attack (IoAs). If ransomware attempts to delete shadow copies or mass read and encrypt files, EDR should identify those behaviors and stop the executable, but it is still possible that some behaviors will remain unidentified. For example, RIPlace initially could bypass antivirus and EDR vendors. Since RIPlace's release, multiple EDR vendors have added the technique as an IoA.

Securing Backups

Ransomware is a direct attack against the integrity and availability of data. Therefore, logic dictates that having backups of data goes hand in hand with protecting against ransomware. However, targeted ransomware attacks commonly include compromising backup systems. Organizations often find themselves ill-prepared for both their data and backups of their data to be compromised during a ransomware attack. To prepare for such an attack, consider the following best practices:

- Do not join your backup systems to your domains. (Ransomware credential theft can allow spreading into the backup system.)
- Consider a backup method that leaves successful backups in an offline state.
- Test backups to make sure they work.
- Rename **`vssadmin.exe`** to prevent deletion of volume shadow copies.

Security Awareness Training

The most common attack vectors for ransomware are via phishing emails and web links. To combat this method of attack, organizations should establish a security awareness training platform to educate users about identifying and reporting phishing. Training should include concepts such as ransomware attempting to trick a user into running a file with elevated privileges.

Controlled Folder Access

Windows 10 comes with built-in ransomware protection. This protection is found under virus and threat protection settings and is called "Ransomware Protection." It is also referred to as "Controlled folder access." *Controlled folder access* audits or blocks executables from accessing certain files, folders and memory areas on a device. While this feature is turned off by default, it is easy to enable manually or centrally with group policy, Microsoft Intune or another asset management agent. While an effective ransomware control, *Controlled folder access* does not protect against all variants. For example, RIPlace works even with *Controlled folder* access in block mode.

Detecting Ransomware Attacks

Preventing ransomware is ideal. Unfortunately, unknown or new ransomware techniques will still break through the best defenses. RIPlace is an example of a technique that continues to evade endpoint protections, even though it is known and documented. Fortunately, organizations can implement additional detection techniques in an attempt to quickly identify ransomware should it happen. NIST has released special publication 1800-26, which explores methods for detecting and responding to ransomware.[17] This publication aligns well with the following detection techniques, which can aid in catching ransomware:

- **File Integrity Monitoring (FIM)—**FIM technology establishes a baseline on a given system. The baseline is created by creating a checksum of files. The baseline usually includes system files, but can further extend to baseline user data. Then, if ransomware modifies files within the baseline, an alert is generated. Not all FIM solutions are equal, however. Some provide real-time notification, while others are based on scheduled scans.
- **Logging and analysis—**The core capabilities to detect ransomware lie in an organization's logging and analysis platform. The platform can include solutions such as EDR or SIEM. To detect ransomware, the organization must first identify what data sources can help them gain visibility into the attack and then couple that with detection techniques and analytics. Examples of data sources and techniques that aid in identifying ransomware include:
  - **File auditing—**Events such as Windows event ID 4663 or Sysmon file event IDs can identify that files are being accessed, modified, deleted and so on. High volumes of access can be an indicator of ransomware. An alternative is to place a fake file (or files) within an operating system and specifically look for access requests to the file. This technique is known as using "honey tokens" or "honey files." Honey tokens act as early indicators of malicious access, such as those associated with ransomware.
  - **Process creation events—**Windows process creation events such as event ID 4688, Sysmon event ID 1 or EDR process creation logs can identify running processes, parent processes and their corresponding commands. By collecting one of these data sources, an organization gains the ability to look for ransomware. For example, an organization could be alerted if a process attempts to launch `vssadmin.exe` to delete volume shadow copies.
  - **Network events—**Microsoft Sysmon event ID 3 or EDR log what process and which user is behind a network connection. Organizations should monitor which application processes make network connections related to file access. This includes identifying processes that connect to file shares, such as SMB, CIFS or older NetBIOS ports.

If you only focus on ransomware prevention, be prepared to stare at an adversary-provided detection technique: the ransom request. At some point, prevention will fail, and detection will take over.

[17] "NIST Special Publication 1800-26," www.nccoe.nist.gov/sites/default/files/library/sp1800/di-detect-respond-nist-sp1800-26-draft.pdf

- **Image loading—**Ransomware can attempt to load custom code into running software. By doing so, ransomware gains capabilities such as stealing credentials or accessing PowerShell scripting functions. Some ransomware variants do so by loading DLLs into a running process. Data sources such as Sysmon event ID 7 or endpoint security suites record image loading. If unknown or dangerous DLLs are loaded into a process, an alert should be generated. For example, if **`System.Management.Automation.ni.dll`** is loaded into a process such as **`notepad.exe`**, that process can now issue PowerShell commands.
- **PowerShell logs—**PowerShell is increasingly being utilized as an offensive tool, due to its capabilities and pre-existence on Windows computers. Organizations should enable, collect and monitor PowerShell logs, such as Script Block logs, to identify malicious PowerShell code execution. Doing so can identify ransomware infections or spread using PowerShell.

- **Successful and failed authentication—**Broad-based ransomware might crawl and encrypt files through accessible network shares. When this happens, there are multiple successful impersonation-level logins. The number of logins might be higher than normal and warrant an investigation. Targeted ransomware attacks can instead deal with stolen credentials being used to access other servers. In this case, multiple logins might deal with delegation tokens, yet the volume of logins dealing with delegation tokens can exceed a threshold normal for the stolen account. Also, multiple failed authentication attempts could indicate on an instance of ransomware attempting to spread.
- **Forensics and reporting—**In the off chance that a ransomware attack succeeds, it is imperative that organizations have forensics and reporting capabilities to identify the extent of the attack and respond quickly. The time to respond can be directly related to the damages accrued by a ransomware attack.
- **Network detection and response (NDR)—**While endpoint controls provide visibility beyond networking, these controls are not foolproof. A compromised asset may be tampered with so that endpoint prevention and detection capabilities fail to catch ransomware. By including NDR, organizations can use passive network data to identify abnormal or unauthorized connections. For example, if ransomware steals credentials and begins to spread from a workstation, it would exhibit anomalous use of network protocols and connections. NDR may further help identify such activity by using machine learning or automatic baselining techniques. Packet captures further aid to provide a source of truth during a forensics investigation.

With ransomware constantly evolving, organizations must pursue a proper level of prevention technologies. Finding the right prevention and detection capabilities involves staying current with ransomware techniques, then assessing which control(s) are best suited to combat ransomware.

Conclusion

Ransomware is a fast-moving threat for organizations small and large. As discussed throughout this paper, combatting ransomware requires a combination of proper security hygiene as well as defense-in-depth via multiple prevention and detection capabilities. Balancing prevention, detection and response can be difficult, but organizations should assess the risk of not including each in their strategy against ransomware.

There is no one technique or tool that deals with ransomware. Instead, defense-in-depth is the only strategy that properly aligns with an acceptable risk-tolerance level. Knowing this, organizations should perform a self-assessment on their approach to dealing with ransomware. Here are a few questions worth asking:

- Is there focus on hardening, patching and general system configuration?
- Are prevention controls in place for both network and endpoints?
- Are backups secure from ransomware?
- Are logs that are specific to ransomware being collected and analyzed?
- If ransomware were to succeed, are controls in place to detect and stop its spread?

If the answer to any of the preceding questions is “no,” then you might want to sit down and rethink your overall strategy. A combination of built-in capabilities plus commercial tools can help solve these issues. As ransomware continues to evolve, so too should your strategy.

Note: We appreciate the opportunity to present this information and the contributions provided by US-CERT and NIST in their respective publications.

About the Author

Justin Henderson is a certified SANS instructor who authored the SEC555: SIEM with Tactical Analytics course and co-authored SEC455 SIEM Design and Implementation and SEC530: Defensible Security Architecture and Engineering. He is a member of the SANS Cyber Guardian Blue Team who is passionate about making defense fun and engaging. Justin specializes in threat hunting via SIEM, network security monitoring and ad hoc scripting.

Sponsor

SANS would like to thank this paper's sponsor: