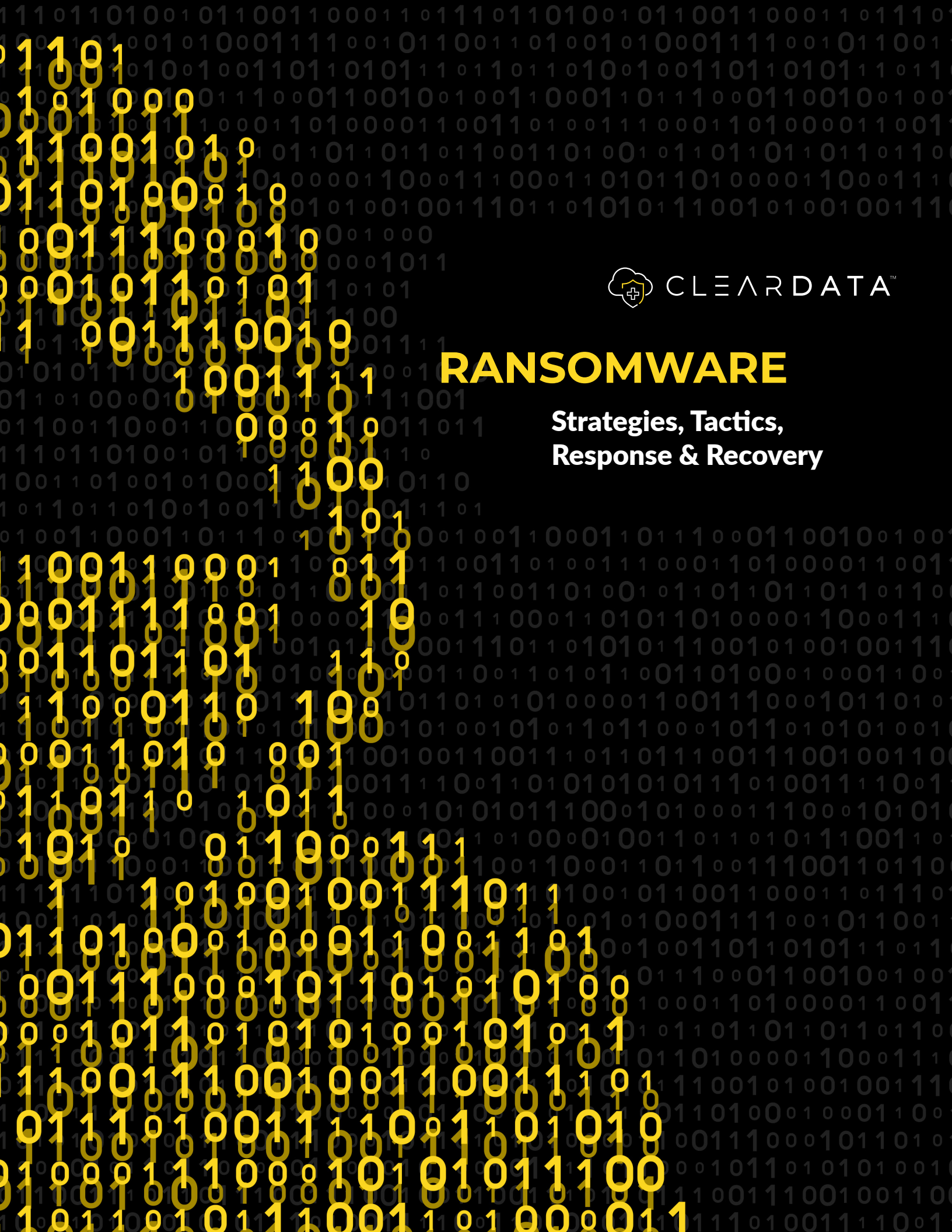


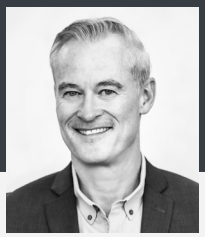
CLEARDATA™

RANSOMWARE

Strategies, Tactics, Response & Recovery

RANSOMWARE

Strategies, Tactics, Response & Recovery



CHRIS BOWEN

CISSP, CCSP, CIPP/US, CIPT
ClearDATA Founder &
Chief Privacy & Security Officer

Chris Bowen is Founder and Chief Privacy and Security Officer at ClearDATA. He leads ClearDATA's internal privacy, security and compliance strategies. He currently advises on the security and privacy risks faced by customers, including global healthcare organizations, payers, providers, life science companies, and market leading innovators from Asia Pacific, North American, and Europe. Mr. Bowen also leads ClearDATA's international security risk consulting practice and has provided counsel to some of the world's largest healthcare organizations.

He is a Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Technologist (CIPT) from the International Association of Privacy Professionals (IAPP), and Certified Information Systems Security Professional (CISSP) and Certified Cloud Security Professional from (ISC)2. As one of the leading experts on patient privacy and health data security, Mr. Bowen has authored dozens of articles and is a frequent speaker at national healthcare industry events.

Contents

If your organization creates, processes, transmits, or stores Protected Health Information (PHI), **you and your organization are a target for ransomware**

Executive Summary

This ransomware guidance whitepaper describes the business and technical aspects of preparing for and responding to a ransomware attack. The author intends for this paper to be used by risk, compliance, security, and operational personnel responsible for creating, configuring, and operating HIPAA- and GDPR-regulated environments.

This whitepaper contains information to:

- Plan for a ransomware attack.
- Architect a cloud environment capable of thwarting and recovering from an attack.
- Detect the indicators that could lead to a ransomware attack.
- Appropriately respond to a successful attack.
- Conduct the required analysis to determine whether the attack is reportable.
- Recover from the attack.

If you search for "ransomware guidance" you'll find about 6,000,000 results. So, great! Here is yet another ransomware guidance paper. Why is this one any different than the others?

This paper has particular credence because ClearDATA defends and continuously gains insights to 240 healthcare organizations in the U.S., E.U., Canada, and Asia Pacific. We perpetually consume system information and identify common attack vectors and threats targeting our customers. This paper shares our observations, including how to thwart attacks and how resiliency should be a primary factor in your defense and preparation.

At the core of what we do is turning policy into code. We take thousands of lines of healthcare privacy legislation and regulations and risk and security standards and translate them into the technical controls and reference architectures that power our platform and services. This "Policy-as-Code Engine" enables us to quickly automate compliance and security in the public cloud and provide the latest healthcare-specific protection. We continually update our Policy-as-Code Engine with aggregated data from regulatory enforcement actions, insurance settlements, and confirmed threat data experienced by our healthcare customers.

This guidance contains real-world intelligence from our daily efforts to keep patient data protected.

In addition to gleaning insights from our customers, ClearDATA monitors the healthcare industry and readies our battle stations as targeted attacks on healthcare continue—attacks orchestrated, for example, by Wizard Spider/UNC1878/Ryuk, which in late 2020 resumed operations using Trickbot, Cobalt Strike, BazarLoader/Kegtap, and Ryuk ransomware. These may be perpetuated by the REvil/Sodinokibi Kaseya supply chain compromise that paralyzed hundreds of companies in five continents, affecting 1,500 companies. Don't get me started about the Solarwinds attack—nobody knows the full impact of that supply chain disaster.

The news shares the dirty deeds of the cyber underworld daily. But beyond the news reports are the everyday heroes sifting through millions of alerts coming at them from threats located around the globe.

In July through September 2021, for example, we observed:

- Millions of connection attempts from known malicious hosts, including the Egregor, Ryuk, and Conti ransomware families.
- Hundreds of thousands of attempts to exploit known vulnerabilities in customer cloud environments.
- Sysrv-hello cryptojacking botnets which continue to be highly active, targeting exposed Jenkins servers.
- Hundreds of thousands of brute force attempts against SSH and RDP.

In a given month, ClearDATA will:

- Block **1,100+** ransomware-related threats.
- Evaluate **10M+** automated controls.
- Conduct **50,000+** risk remediations using automated controls.
- Enforce **6,000+** controls with managed services.

The Ransomware Crisis

About 15 ransomware attacks occurred while you read the introduction to this whitepaper. That's almost one every 10 seconds! Sadly, hospitals are the primary target.

Our inboxes are overflowing with new warnings about new malware variants designed to destroy your data. Alerts like the one in October 2020 warned of a widescale attack targeting 400 U.S. hospitals. Three U.S. government agencies joined forces to warn healthcare providers about a cybercrime operation called Ryuk.

The potential harm to patients, the operational damage strain on the healthcare system, the threat to human life due to lack of information, and the astounding recovery costs can be catastrophic to any organization. In the most severe scenarios, an attack can effectively bring the hospital's entire system down. This type of disruption causes scheduled surgeries to cancel, ambulances to reroute, or critical patients to be transferred to another facility or provider mid-treatment.

Ransomware attacks against the healthcare industry are reaching crisis levels.

We all know the ransomware problem is enormous, and we cannot ignore it. Organized crime, and now in some cases, nation-state actors, have amassed substantial financial gain by taking healthcare networks hostage. With each success and ransom paid, more ransomware attacks are guaranteed. While this may sound like a technology problem—and it is—it's more than that. In healthcare, there are downstream effects for every event. Whatever happens with data eventually affects a human being.

In the case of ransomware, knowledge is power. Gaining insights into how you can detect intruders and know the methods they use to gain access is necessary if you are to stop them before the harm is substantial. Ransomware attacks have warning signs and attackers leave trails.

Market Dynamics of the Ransomware Economy

To understand the "why," we must delve into the greater context surrounding the ransomware market. Typically, the attacker is part of a criminal syndicate, leveraging the tools provided by the illicit economy. This economy sells easy-to-use software designed to yield the user the most money possible in the shortest time.

Like a "normal" business, the ransomware attacker strives to generate consistent revenues leveraging global automation and cloud services. The attacker even leverages at-scale services provided by the syndicate, such as "customer support" for attackers to scale and to victims struggling to recover from the attack.

The ransomware underworld thrives from these variables:

- Novice criminals can easily buy and use ransomware software (See Figure 2, below).
- Profit from attacks is predictable.
- There is less risk in the payoff than other hacking methods with little or no direct contact with the victim.
- The ransomware model comes with a "built-in" buyer of the data meaning the criminal doesn't have to find a buyer.
- Ransomware is rapidly scalable – it can be globally automated.
- It is less trackable using cryptocurrency.

However, those who pay the ransom may think they have recovered, only to be attacked again because they've now become a "known payer." Becoming a known payer of ransoms puts a long-term target on the organization and contributes to the cybercriminal economy. For this reason, the FBI discourages the payment of a ransom.[1]

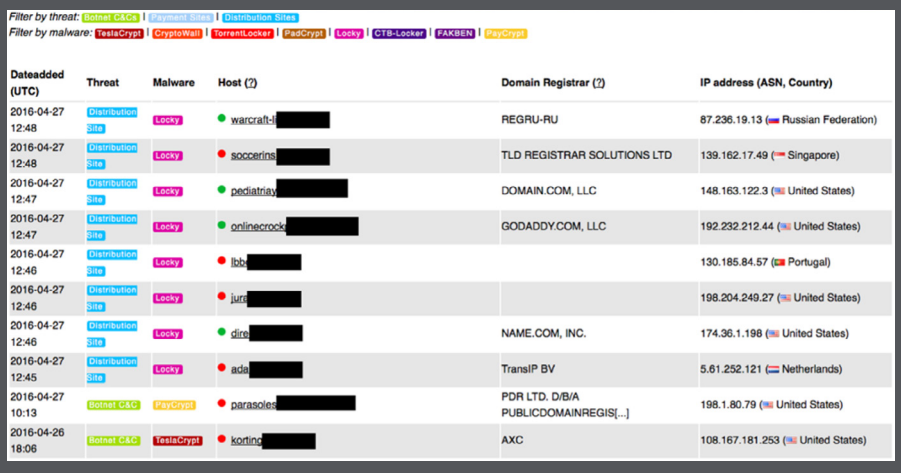


Figure 2 Ransomware Tracker[2]

1. High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations." High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, Internet Crime Complaint Center (IC3), 2 Oct. 2019, www.ic3.gov/Media/Y2019/PSA191002.
2. Ransomware Tracking Database." Ransomwaretracker abuse.ch, 2021, ransomwaretracker.abuse.ch/

Ransomware Has Evolved

Ransomware is a for-profit industry that evolves with technology and societal trends. Some variants fail while some dominate on a global scale. Regardless, ransomware criminals adopt new techniques quickly, favoring approaches that make payment more likely and faster.

The later years of ransomware have exposed troubling patterns, including the expansion of double-extortion techniques, which expanded from Maze in 2019 to 18 different ransomware operators in 2020. Double extortion begins when a crypto-malware strain steals information stored on a victim's machine before launching its encryption routine. The ransomware then encrypts the victim's data and demands payment for a decryptor in the ransom note. However, the threat actor then makes the additional demand that victims pay the additional ransom to prevent the attackers from publishing their data online.

We can prevent ransomware if we understand how it works. While reading the brief history of the ransomware evolution (below), please observe common attack patterns.

Year	Variant	Also Known As	Characteristic
1989	PSCyborg[3]	AIDS Trojan	After 90 reboots, the Trojan hid directories and encrypted the names of the files on the customer's computer. To regain access, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panama.
2005	GPCoder[4]		GPCoder infected Windows systems and targeted files with a variety of extensions. Once found, it copied files in encrypted form and deleted the originals from the system.
2009	Vundu[5]		Vundu encrypted files on the victim's computer and sold a genuine antidote to unlock them. This ransomware was the first indication that hackers felt that they could make more money from ransomware.
2011	Trojan WinLock[6]	Locker	Trojan WinLock was the first widespread example of what became known as "Locker" ransomware. Rather than encrypt files on a victim's device, a Locker makes it impossible to log into the machine. This ransomware started a trend that imitated genuine products.
2012	Reveton[7]	Police Malware	Reveton was a police-style malware that would target infected systems with messages claiming to be from law enforcement agencies and state authorities. The device would be locked as "confiscation" until the victim paid some bribe or fine.
2013-2014	CryptoLocker[8]	TorrentLocker	CryptoLocker propagated via infected email attachments and an existing Gameover ZeuS botnet. It marked the first example of ransomware spreading via infected websites. It was also distributed via spear phishing, specifically email attachments sent to businesses that cybercriminals made to look like a customer complaint. When activated, the malware encrypted certain types of files stored on local and mounted network drives.

3. 6/19/2020, Kieran Laffan Updated: "A Brief History of Ransomware." Inside Out Security, 20 June 2020, www.varonis.com/blog/a-brief-history-of-ransomware/.
4. "A History of the Ransomware Threat: Past, Present and Future." VpnMentor, 27 July 2021, www.vpnmentor.com/blog/history-ransomware-threat-past-present-and-future/.
5. Ibid.
6. Ibid.
7. "Threat Landscape Dashboard." McAfee, 9 Apr. 2019, www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.reveton-ransomware.html.
8. "CryptoLocker." Wikipedia, Wikimedia Foundation, 8 Aug. 2021, en.wikipedia.org/wiki/CryptoLocker.

Year	Variant	Also Known As	Characteristic
2014	TorLocker[9]		Cybercriminals first deployed TorLocker in 2014 against Japanese users. TorLocker was marketed and sold on the now-defunct Evolution Market.
2014	CTB-Locker[10]		CBT-Locker is a virus that infiltrates operating systems via infected email messages and fake downloads (e.g., rogue video players or fake Flash updates). After successful infiltration, this malicious program encrypts various files stored on computers. It demands a ransom payment of Bitcoins to decrypt them.
2014	Kryptovor[11]		Kryptovor is modular malware, which makes it easy for the creator to add more functionality. Cybercriminals used this ransomware to steal cryptocurrency wallets from its victims. Over time it evolved to include a ransomware component.
2015	TeslaCrypt[12]	Alpha Crypt	After a successful infection, the malicious program demanded a $500 ransom for the decryption key. If the victim delays, the ransom doubles.
2015	Cryptowall		Attackers widely distribute Cryptowall using exploit kits, spam campaigns, and malvertising. It uses I2P network proxies and Tor networks for payments using Bitcoin.
2015	CRYPVAULT[13]		CRYPTVAULT makes encrypted files appear as if they were quarantined files. These files are appended by a *.VAULT file extension, an antivirus software service that keeps any quarantined files for a specific time period.
2016	Locky[14]		Cybercriminals aggressively distribute Locky via phishing attacks. It set a precedent followed by the likes of WannaCry for the sheer speed and scale of its distribution. Locky specifically targeted healthcare providers because its originators noticed that essential public services quickly paid ransoms to get their systems up and running again.
2017	WannaCry[15]		North Korea launched WannaCry, which used EternalBlue, a leaked NSA hacking tool, to spread as far and wide as possible. The ransomware trawled the internet for computers operating on older versions of Windows Server – which had a known security flaw – to infect them. It does not use phishing scams or downloads from compromised botnet sites.
2017	Petya & NotPetya[16]		After encrypting the file or data, Petya ransomware flashes a request to pay a Bitcoin ransom to get access to the data. A NotPetya spreads in a computer independently, while a Petya requires the victim to open the file and download it.

9. Villeneuve, Nart. "TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware." FireEye, 15 May 2015, www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html.
10. Heinbach, Courtney. "What MSPs Need to Know About CTB-Locker." What MSPs Need to Know About CTB-Locker, 21 Mar. 2021, www.datto.com/blog/what-is-ctb-locker-ransomware.
11. Hernandez, Erye. "Analysis of Kriptovor: Infostealer+Ransomware." FireEye, 8 Apr. 2015, www.fireeye.com/blog/threat-research/2015/04/analysis_of_kriptovo.html.
12. Kaspersky. "Teslacrypt Ransomware Attacks." Usa.kaspersky.com, 13 Jan. 2021, usa.kaspersky.com/resource-center/threats/TeslaCrypt.
13. "CRYPVAULT: New CRYPTO-RANSOMWARE Encrypts and 'QUARANTINES' Files." CRYPVAULT: New Crypto-Ransomware Encrypts and "Quarantines" Files, TRENDLABS Security Intelligence Blog, 6 May 2016, blog.trendmicro.com/trendlabs-security-intelligence/crypvault-new-crypto-ransomware-encrypts-and-quarantines-files/.
14. "What Is Locky Ransomware? Locky Definition, LOCKY Prevention 2021." CyberTalk, 27 July 2021, www.cybertalk.org/what-is-locky-ransomware/.
15. "A History of the Ransomware Threat: Past, Present and Future." VpnMentor, 27 July 2021, www.vpnmentor.com/blog/history-ransomware-threat-past-present-and-future/.
16. "Petya Ransomware AND NotPetya Malware." Cyber Security Solutions, Compliance, and Consulting Services - IT Security, 13 Nov. 2019, www.infoguardsecurity.com/petya-ransomware-and-notpetya-malware/.

Year	Variant	Also Known As	Characteristic
2018	SamSam[17]		SamSam exploits Windows servers to gain continued access to a victim's network and infect all reachable hosts. It then escalates privileges for administrator rights, drops malware onto the server, and runs an executable file; all without victims' action or authorization.
2019	Ryuk[18]		Threat actors use Ryuk in targeted attacks. They make sure that essential files are encrypted and then ask for large ransom amounts.
2019	MAZE[19]		MAZE ransomware was initially distributed directly via exploit kits and spam campaigns through late 2019. These emails use tax, invoice, and package delivery themes with document attachments or inline links to download and execute Maze ransomware.
2020	Conti[20]		Conti is a human-operated "double extortion" ransomware that, in addition to encrypting the data, steals it and threatens to expose information.
2021	BlackMatter[21]		BlackMatter leverages the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network. BlackMatter then remotely encrypts the hosts and shared drives as they are found.

Ransomware Spreader Events

Ransomware has evolved in the way it permeates victim environments and in the infection of new victims. The early days of ransomware were simpler than now. The creator of the AIDS Trojan handed out 20,000 infected disks to attendees of the World Health Organization's AIDS conference in the mid 1980s, whereas now automation rules the day with targeted phishing campaigns preying on the mindless actions of email recipients. There are even cyborg-style attacks of ransomware autonomously seeking and destroying data using known exploits.

By far, the most prolific attack vectors are nefarious email attachments aimed at employees or a visit to an infected website programmed to drop a destructive payload on the first visit.

Some of the most popular ways of spreading include:

- Emailing malware to huge numbers of people, targeting mainly the U.S. and U.K. using the "spray and pray" approach (see Figures 3 and 4, next page).
- Loading a website with browser exploit kits, known as drive-by downloads.
- Downloading an installer masquerading as a legitimate tool that downloads ransomware as an additional component.
- Violating RDP ports that have been left open to the internet.
- Navigating to mapped or connected storage volumes.
- Compromising outdated or unpatched operating systems.
- Using unauthorized thumb drives, online storage accounts, or storage shares.

17. "SamSam Ransomware - Alert (aa18-337a)." CISA, Cybersecurity and Infrastructure Security Agency CISA, 3 Dec. 2018, us-cert.cisa.gov/ncas/alerts/AA18-337A.
18. "Ryuk - What IS Ryuk Ransomware?" Ryuk - What Is Ryuk Ransomware?, www.malwarebytes.com/ryuk-ransomware.
19. "What Is Maze Ransomware?" Crowdstrike.com, CrowdStrike, 13 July 2021, www.crowdstrike.com/blog/maze-ransomware-analysis-and-protection/.
20. "Conti Ransomware." Nhs Choices, NHS, 9 July 2020, digital.nhs.uk/cyber-alerts/2020/cc-3544.
21. "Alert (AA21-291A)." Cybersecurity and Infrastructure Security Agency, CISA, 18 Oct. 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-291a.

Figure 3 Phishing Email Impersonating the IRS

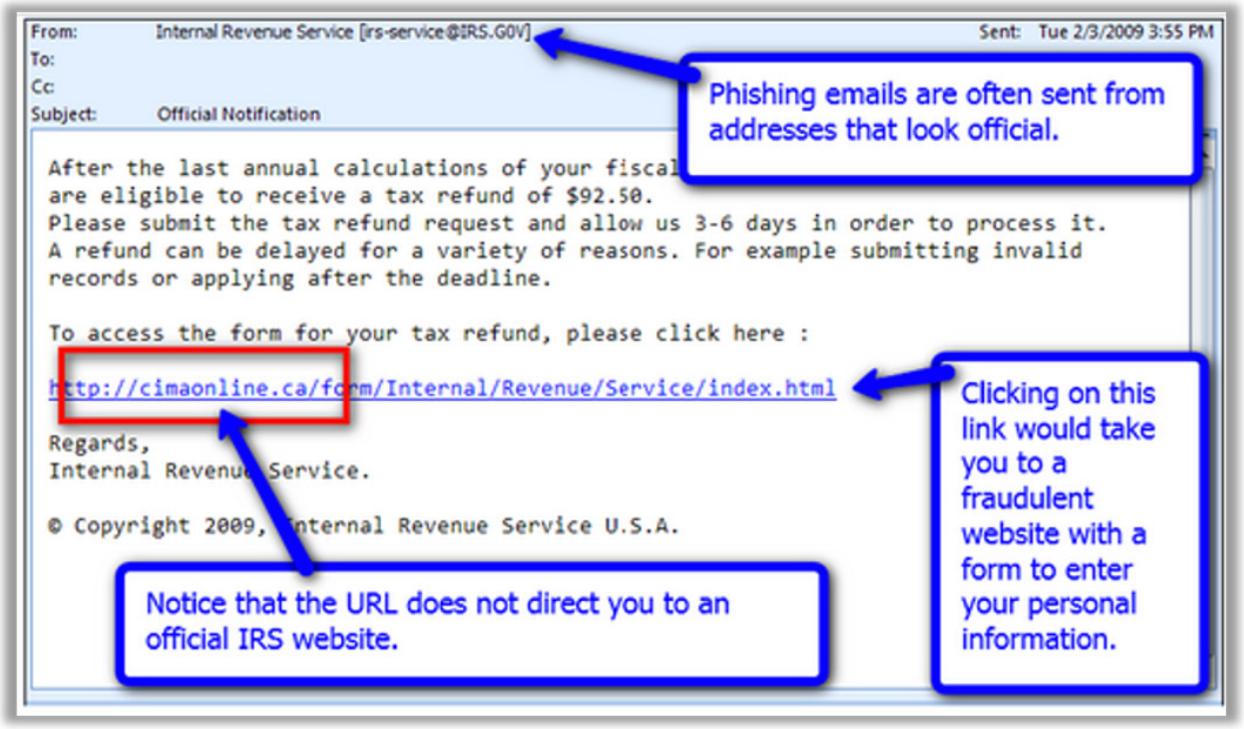
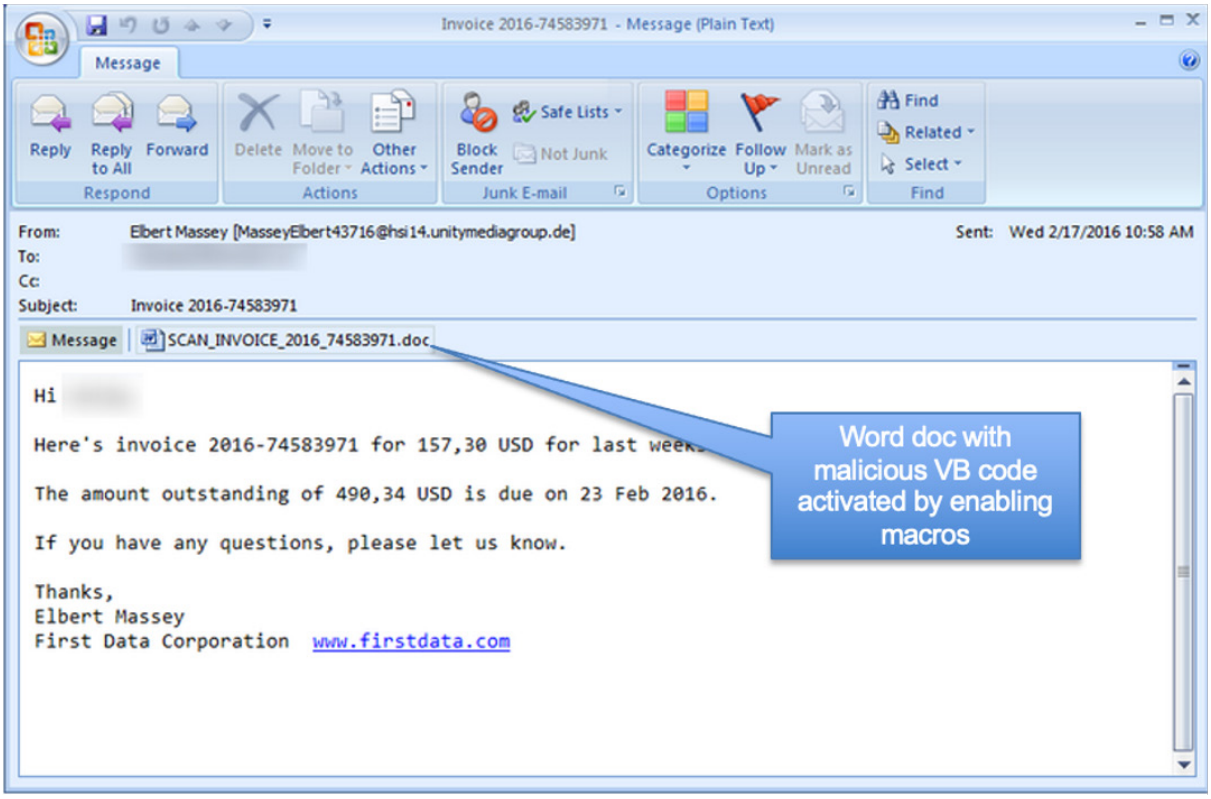


Figure 4 Phishing Email Impersonating the IRS



Phishing Has Become Big Game Hunting

Phishing and drive-by downloads – ah, the good old days!

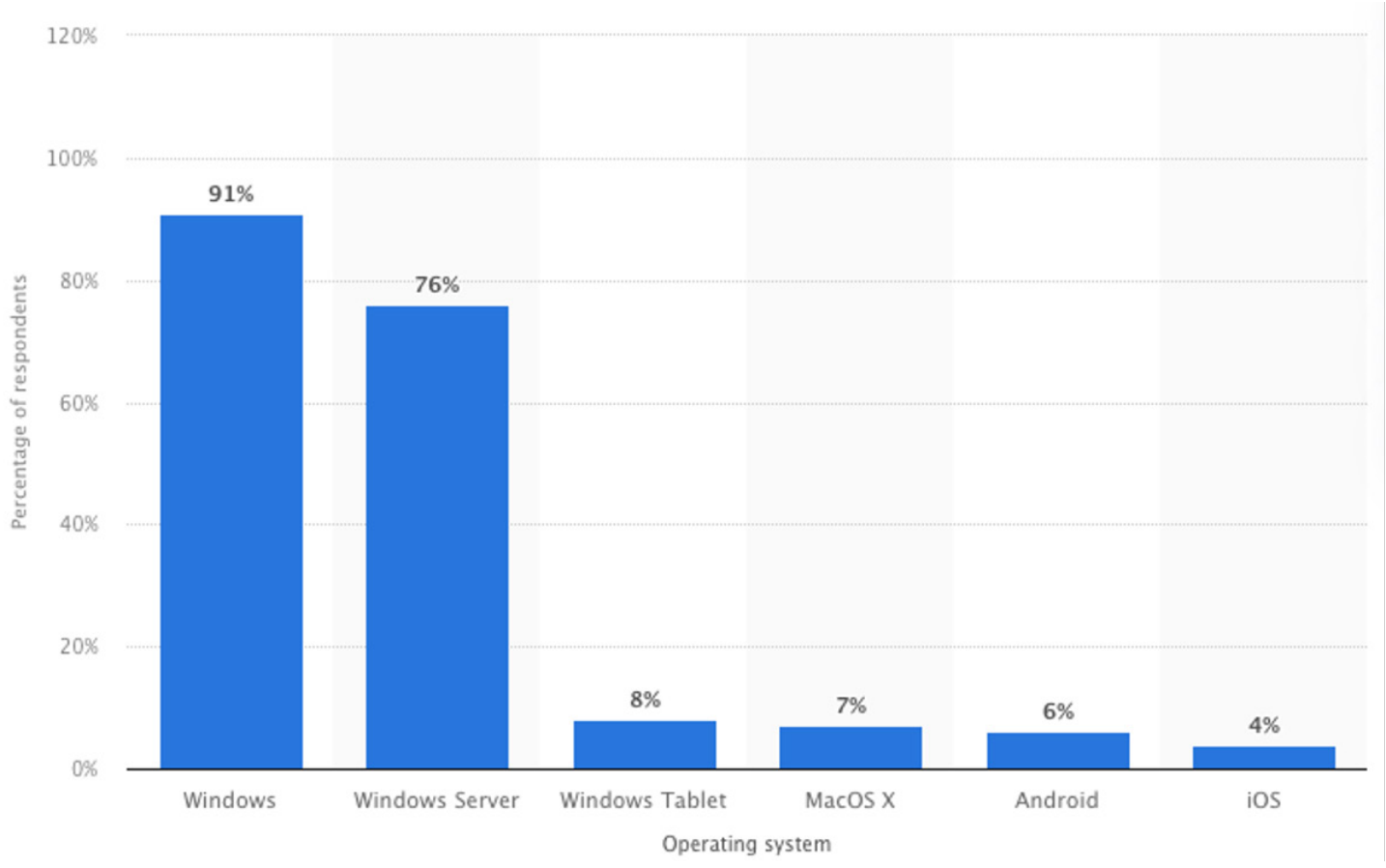
Big game hunters search for industries that depend on information technology and industries with resource or talent constraints. The greater the constraints, the more likely a vulnerability exists that they can exploit.

Like an actual hunt, once actors have gained access to a target network, they are more likely to take their time before striking.[22]

The FBI cited three significant modes of attack:

1. Email phishing campaigns: A threat actor uses an email to entice the victim to provide credentials or other access tools.
2. Network edge vulnerability: Unpatched vulnerabilities in the network create opportunities for compromise.
3. Exploitation of remote desktop protocols (RDP): A remote desktop software tool that already has access to a machine is exploited, then uses the access to the device to steal information.
4. Known vulnerabilities in software: Mostly Microsoft operating systems, although others can be vulnerable as well (see Figure 5).

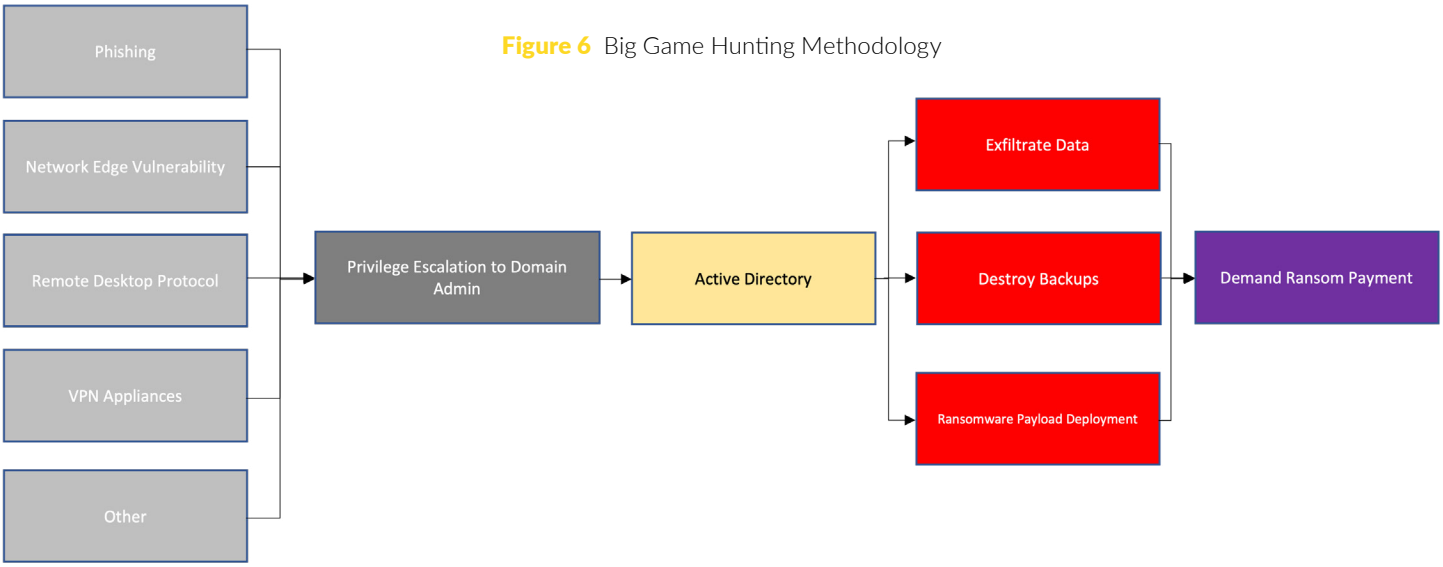
Figure 5 Commonly Vulnerable Operating Systems Targeted by Ransomware (Source: Statistica[23])



22. "2021 Forecast: The Next Year of Healthcare Cybersecurity." Department of Health & Human Services, 11 Mar. 2021.
23. Johnson, Joseph. "Major Operating Systems Targeted by Ransomware 2020." Statista, 16 Feb. 2021, www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/.

Big game hunters typically cast a wide net, seeking a way to gain access to an environment to deploy their wares. Once they obtain access, they work to elevate their access rights to become a domain administrator. Then the nightmare begins for the victim organization. The hunters deploy ransomware, destroy backups, and exfiltrate the data. The final step in this scheme is the ransom note – electronically, of course (see Figure 6 below).

Figure 6 Big Game Hunting Methodology



Not surprisingly, the healthcare industry is a prime target of big game hunters. Which begs the question…

Why Is Healthcare Such a Target?

The attacks are plentiful and expensive. Consider dramatic examples of these successful attacks on healthcare organizations:

- The University Medical Center Southern Nevada suffered a ransomware attack during the summer of 2021 that affected the data, including PHI, of 1.3M people. Analysts pointed to REvil, a Russia-linked ransomware group, as the culprit.[24]
- The United Kingdom's National Health Service (NHS). The WannaCry outbreak of 2017, which afflicted over 200,000 computers in over 150 countries, brought hundreds of NHS facilities to a standstill for several days. This disruption resulted in the cancellation of thousands of operations and appointments and the frantic relocation of emergency patients from stricken emergency centers. The NHS Trusts that patched EternalBlue avoided becoming WannaCry victims. This attack was, and still is, the most significant cyberattack to hit the U.K.[25]
- The Hollywood (California, USA) Presbyterian Medical Center was hit with Locky ransomware, which locks users from their systems until victims pay a ransom. The medical center reverted to manual pen-and-paper operations for four days in response to the attack. Cybercriminals demanded $3.6M but ultimately paid a $17,000 ransom to bring systems back online after a week of resorting to internal emergency measures. The medical center had to cancel surgeries and transfer patients to other hospitals.[26]
- Hancock Health (Indiana, USA) lost access to its email, electronic health records, and internal operating systems. It operated on pen-and-paper for days before paying a $55,000 ransom.
- Erie County Medical Center (New York, USA) lost access to 6,000 computers to a SamSam ransomware attack. Refusing to pay the ransom demand of 24 bitcoins (valued at $1,250 each totaling approximately $30,000,) six weeks of manual operations and a recovery process ultimately cost Erie County Medical Center $10M.[27]

24. "Nevada Hospital Ransomware Attack Could Affect Data of 1.3M Patients." Healthcare IT News, Healthcare IT News, 24 Aug. 2021, www.healthcareitnews.com/news/nevada-hospital-ransomware-attack-could-affect-data-13m-patients.
25. Palmer, Danny. "Ransomware: How the NHS Learned the Lessons of WannaCry to Protect Hospitals from Attack." ZDNet, ZDNet, 13 May 2021, www.zdnet.com/article/ransomware-how-the-nhs-learned-the-lessons-of-wannacry-to-protect-hospitals-from-attack/.
26. Zetter, Kim. "Why Hospitals Are the Perfect Targets for Ransomware." Wired, Conde Nast, 30 Mar. 2016, www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.
27. Davis, Henry L. "ECMC Spent Nearly $10 Million Recovering from MASSIVE CYBERATTACK." The Buffalo News, 26 July 2017, buffalonews.com/business/local/ecmc-spent-nearly-10-million-recovering-from-massive-cyberattack/article_1786edc7-214e-5c48-84c5-8823a2a38e91.html.

The U.S. healthcare delivery system is particularly vulnerable to ransomware attacks due to several factors:

1. Outdated, disparate, and vulnerable systems — Most healthcare providers use outdated IT infrastructure. For example, Forescout reported that more than half of medical devices operate on legacy systems and 83% of medical imaging devices use outdated operating systems.[28] Many healthcare organizations use outdated operating systems that can no longer be patched, such as Microsoft 7 and Windows Server 2008.[29]

2. Data sprawl and a lack of accurate, up-to-date data maps and inventories — Healthcare consumerization is accelerating in the post-pandemic world, driving up the demands for data liquidity, or the need for health data flow and access. Key drivers are virtual care expansion, the acceleration of interoperability standards, the realities of the digital front door, and the rise of retail health providers.

In this complex setting, one of the first things privacy officers in healthcare organizations attempt is to create a map of sensitive data that they must protect. Now a petabyte problem[30], this effort quickly becomes futile as data sprawl expands beyond the boundaries of the providers' systems. In both structured and unstructured formats, the data journey takes on a life of its own as it traverses healthcare treatment, payment, and operations activities.

Adding to that unpredictable data flow, the journey to the cloud adds additional complexities, such as automated scalability. Quickly the privacy officer is left with limited information about the data lifecycle, including where the data flows and who or what has access.

3. The perception that "bad guys" can get paid more quickly than other sectors — Healthcare data shared at the right time with the right users saves lives. Disrupt that flow, and you have the makings of a human disaster where death can occur, as was the case in the successful ransomware attack in 2020 on a German hospital that crippled the provider. One patient died as a direct result of being redirected to an alternate facility. Most recently a lawsuit surfaced from a U.S. ransomware attack in 2019 that attributed to the death of a baby several months later. The attack made critical information and technology unavailable during the child's birth. We know this, and unfortunately, so do the cybercriminals.[31]

Because the cybercriminals' mission is to generate revenue from their crimes, they want their money fast, with certainty and consistency. In addition to being vulnerable, the healthcare sector is motivated to recover from an attack as quickly as possible. But due to antiquated IT systems, many healthcare organizations cannot recover well at all. So, criminals attack healthcare organizations believing they will receive payments more quickly than other sectors of the economy.

4. Lack of in-depth employee security awareness training — Hospitals in the past have not focused on cybersecurity in general, but rather focused more on general HIPAA compliance, ensuring that employees meet the federal requirements for protecting patient privacy.[32]

28. Davis, Jessica. "Majority of Healthcare Medical Devices Operate on Legacy Systems." HealthITSecurity, 15 May, 2019, https://healthitsecurity.com/news/majority-of-medical-devices-are-running-on-legacy-systems
29. "Microsoft Ending Support for Windows 7 and Windows Server 2008 R2." Cybersecurity & Infrastructure Security Agency, 17 Oct., 2019. https://us-cert.cisa.gov/ncas/alerts/aa19-290a
30. Speciale, Paul. "The Explosion of Healthcare Data: How Providers Are Managing Growth without Breaking the Bank." SOLVED, SOLVED Magazine, 8 June 2020, www.scality.com/solved/explosion_of_healthcare_data/.
31. Millard, Mike. "Hospital Ransomware Attack Led to Infant's Death, Lawsuit Alleges." HealthcareITNews, 1 Oct. 2021, https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges
32. Zetter, Kim. "Why Hospitals Are the Perfect Targets for Ransomware." Wired, Conde Nast, 30 Mar. 2016, www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

Preventative Measures

We are at a point with technology where prevention cannot just be the sole strategy. Organizations need to plan as if an attack will happen, not just try to prevent it. Security professionals know that we cannot stop every attack. We must prepare to avoid as many as possible and minimize the damage when one is successful. There are many things we can do to prevent ransomware. Below are recommendations grouped by **People, Process,** and **Technology.**

PEOPLE

Train your workforce for security awareness. Incorporate phishing, safe browsing, irregular system activity, social engineering, remote working, and working in public places.

Continually learn from what others experience. Learn from real-world incidents, attend webinars and conferences that further educate the industry, and read relevant articles weekly. Consume threat intelligence from these and automated sources such as the Cybersecurity & Infrastructure Security Agency (CISA), MITRE ATT&CK, FBI: InfraGard, the SANS Institute, (ISC)2 and many others. A few notable partnerships that share high-quality information include:

- Multi-State Information Sharing and Analysis Center (MS-ISAC): https://learn.cisecurity.org/ms-isac-registration
- Sector-based ISACs – National Council of ISACs: https://www.nationalisacs.org/member-isacs
- Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups

Be aware of regular system activity. Observing changes to the behavior of your laptop or the observance of spikes in storage or memory use can be an incident underway.

Test business resiliency. Conduct disaster recovery tests on a frequent, regular basis. These tests include technology testing and evaluation and the reaction, response, and knowledge of the team responsible for ensuring business continuity.

Know how to report security incidents. And report them quickly and with as much specific information as possible.

Be prepared for incident response. Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident. Build runbooks that contemplate ransomware attack scenarios and define in advance how to prioritize threats to your organization. Share the plans and runbooks with the executive suite and practice your incident response plan before an attack happens.

PROCESS

Maintain offline, encrypted backups and regularly test them. Conduct backup procedures regularly. Backups must be maintained offline as many ransomware variants attempt to find and delete any accessible ones and because there is no need to pay a ransom for data readily accessible to your organization. There are several approaches to the backup strategy. Some organizations swear by the 3-2-1 rule, which is three copies, with one offsite copy on two types of media. For more critical data, we recommend a 3-2-2 rule. Some even use a 3-2-3 rule. For more information, visit https://www.unitrends.com/blog/3-2-1-backup-sucks and read the section below titled, "Immutable Backups."

Maintain regularly updated "gold images" of critical systems if they need to be recovered from a ransomware attack. This approach entails maintaining image "templates" that include a prebuilt, hardened operating system (OS). It also includes associated software applications that your organization can quickly deploy to rebuild a system, such as a virtual machine or server.

Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. Hardware newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.

Ensure the availability of application source code or executables should be stored with backups, escrowed, or other air-gapped means. Taking this action will allow you to obtain pristine, up-to-date copies of the code safely. Recovery by rebuilding images is more efficient than reinstalling directly to hardware. Still, some images may not install correctly on different hardware or platforms.

Scan for vulnerabilities on an ongoing basis to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

Ensure devices are properly configured and hardened to ensure security features are enabled and other features tuned for limited use. For example, disable ports and protocols not used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389). Threat actors often gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware. After auditing networks for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts. For more information review CISA Alert AA20-073A, Enterprise VPN Security at: https://us-cert.cisa.gov/ncas/alerts/aa20-073a.

Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Consider disabling SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled. Then remove dependencies through upgrades and reconfiguration. Upgrade to SMBv3.1.1 (or most current version) along with SMB signing. Finally, block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Regularly patch and update software and operating systems to the latest available versions. Prioritize timely patching of internet-facing servers and software processing internet data, such as web browsers, browser plugins, and document readers for known vulnerabilities. Understand and know your patch health for all devices. Deploy those critical patches as soon as possible. WannaCry leveraged the Microsoft EternalBlue vulnerability. Those who patched this did not face the WannaCry threat.

Establish baseline system behavior patterns by defining key indicators that measure normal system behavior. These could be user access patterns, network traffic, endpoint locations, email patterns, compliance score patterns, and most importantly, data flow and permission patterns.

Enforce strong password security. CIS password guidance is found in its online policy guide, free to download at: https://www.cisecurity.org/white-papers/cis-password-policy-guide. These recommendations are robust and include the following:

- Enforce password history set to 24 or more passwords.
- Maximum password age set to 60 or fewer days, but not zero.
- Minimum password age set to one or more days.
- Minimum password length set to 14 or more characters.
- Enable – password must meet complexity requirements.
- Disable — store password using reversible encryption.
- Account lockout duration set to 15 or more minutes.
- Account lockout threshold set to 10 or fewer invalid login attempts, but not zero. 'Reset account lockout counter after' set to '15 or more minutes.' NIST SP-800-63B also provides excellent guidance found online at: https://pages.nist.gov/800-63-3/sp800-63b.html.

Leverage multifactor authentication (MFA). Wikipedia explains that MFA, "is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism,"[33] for all external connections to your network. In combination with password and MFA, healthcare providers could thwart most ransomware attacks.

Whitelisting applications helps you determine which application has the right to run in your environment. Like being on the authorized guest list at a dinner party, a software application should be on the authorized software list to instantiate in your network. Restricting privileges this way is a substantial countermeasure to a ransomware installer.

Employ the principle of least privilege. If a user does not need access to a tool, don't give him/her access. If a user changes roles and needs greater access, review and document the request before granting it. Conversely, if that user role no longer needs access, reduce it. And by all means, departed employees should have no access after the moment they leave.

Label assets associated with sensitive data. In a sea of cloud assets (or on-premises assets), identifying which assets can touch sensitive data is essential to placing appropriate safeguards with those assets. You must follow a suitable data labeling procedure to protect data successfully.

Map data flows as they flow through your systems, including expected ingress and egress points, storage locations, API connection, and associated data calls. Not knowing where your data flows could leave you vulnerable to data exfiltration tactics common in today's double-extortion ransomware attacks.

Know and manage the data lifecycle. Effectively doing this requires knowing how and where your sensitive data is created, who accesses it, where it is distributed, and how and who maintains it. (See Figure 7, next page.)

33. Wikipedia contributors. "Multi-factor authentication." Wikipedia, The Free Encyclopedia. 5 Sep. 2021. Web. 13 Oct. 2021.

Figure 7 Sample Data Lifecycle

TECHNOLOGY

Tune your SIEM (Security Information and Event Monitoring System) to watch for known Indicators of Compromise (IOCs) with automation if possible. Loading IoC information as quickly as possible can alert your security team early, trigger firewall rules, access and permission changes, fire off storage air-gapping rules, and keep you ahead of the attack.

Deploy and use a VPN for remote connectivity to hide your IP address and it allows you to access the web anonymously, making it more challenging to target your computer. When you share or access data online using a VPN, that data is encrypted, and it remains largely out of reach for malware creators. Reputable VPN services also blacklist URLs that may be associated with illicit activity.

Maintain VPN appliances. VPN servers should be hardened, maintained, and regularly patched. As was the case with PulseSecure and VMWare, which recently had major VPN vulnerabilities[34], VPNs can become vulnerable to compromise.

Segment your network to provide greater security and to increase performance. Network segmentation splits a network into zones that contain data with similar security, privacy, and compliance requirements. In today's world, ransomware spreads quickly through a network. Complete isolation of one network from another can save critical backups, or mission critical infrastructure from destruction.

Endpoint protection can be critical in preventing ransomware loaders from infecting a user's laptop or a production server. In fact, not having endpoint protection is like playing Russian Roulette. The odds are that serious injury will occur without it.

Harden email. Phishing is the number one attack vector for ransomware attacks. IT administrators can easily misconfigure email infrastructure. One mistake could make it possible for the unwitting user to double-click that "Urgent Invoice" carrying a secret executable payload ready to decimate your system.

Use ad blockers and block script executions. Ransomware cannot launch if you block the ability to execute.

Display file extensions to help you identify ransomware variants when responding to an attack. Because time is of the essence in these kinds of investigations, having instant visibility can help you in the moment.

Ensure that devices go offline automatically in case of a threat. In some scenarios, an application or asset can automatically halt activity. If you can enable this safely, do so.

Deploy edge and host-based firewalls. Firewalls are network security applications that monitor and filter traffic to and from your network or your host. Good firewalls automatically deploy rules based on threat patterns leveraging artificial intelligence and machine learning (AI and ML).

34. Alert (aa21-110a)." Cybersecurity and Infrastructure Security Agency, CISA, 20 Apr. 2021, us-cert.cisa.gov/ncas/alerts/aa21-110a.

Immutable Backups

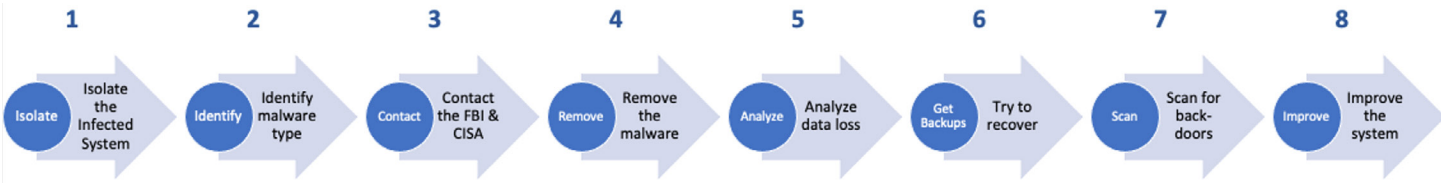
Advanced ransomware now targets backups by modifying or completely erasing them. Primary storage systems should be designed for accessibility and be available to other assets, services, APIs, and protocols in your system. When a ransomware attack attempts to destroy its way through your network, having untouchable backups that are untouched and pristine are critical for recovery. Immutability means unchanging or unchangeable. The immutable backup cannot be read, modified, or deleted by other assets or services in your system. To recover from a ransomware attack, using an immutable backup approach is the only way to succeed.

Immutable backups must be a core part of a disaster recovery architecture.

To ensure immutability in your backups, you must move beyond permission-based strategies or access control list approaches. Below are some architectural suggestions to consider in creating your ransomware-evading backup objectives:

- Never expose backup data to external clients through insecure means, such as Network File System (NFS) or Server Messaging Protocol (SMB). Every action performed on data should be authenticated through multiple means. Old school approaches use standard protocols that allow the malware to evade weak authentication mechanisms found in NFS or SMB.
- Never allow writes to touch data written earlier. Companies that take a more vulnerable approach to ensure that writes are done in-place. This approach cannot guarantee that data has not changed since the data was ingested.
- Never allow writes to touch data written earlier. Companies that take a more vulnerable approach to ensure that writes are done in-place. This approach cannot guarantee that data has not changed since the data was ingested.
- Data still must be transferred to your disaster recovery-hardened, air-gapped infrastructure. By all means, use secure transit protocols to ensure end-to-end encryption – leverage TLS 1.2 to encrypt traffic.
- Test your backups to ensure that they have not been altered, even as additional backups are created on a r egular cadence.
- Like any sensitive environment, administrators should use credentials that bear no resemblance to credentials used in other tasks or duties that are less sensitive.
- Restrict access to this environment to only those with a need. Implement a least privilege strategy and implement segregation of duties where it makes sense into your process.

Figure 8 Eight-Step Ransomware Response



Incident Response

Responding to a ransomware attack requires a different response than other cyberattacks. Time is of the essence. The response should be methodical and rapid. The following eight steps can guide you to a successful outcome if you are prepared for an attack (see Figure 8 above).

There are many ransomware incident response playbooks available on the web. This playbook comes from Chris Hendricks, a cybersecurity expert and incident responder from San Antonio, Texas. This is one of the most "human" playbooks we've seen. We added a few more steps here and there, and we recommend that you take this work from Hendricks and modify it to work for your organization.

Take a Deep Breath – Quickly

Find a way to stay calm, cool, and collected. You'll need to be calm to think clearly.

As soon as humanly possible, **isolate the infected system** by disconnecting from the network.

Report the attack to your helpdesk team. They should be trained to escalate the issue to the incident response team.

Take pictures of your screen, ransom messages, encrypted files and their extensions, system error messages, and anything else that doesn't look right. **Make sure you are using your smart phone and not taking screenshots – your computer may cease to exist soon!**

Take notes about the issues. Try to answer as many of these questions as possible, including:

- What did you notice?
- Why did you think it was a problem?
- What were you doing at the time you detected it?
- When did it first occur and how often since?
- Where were you when it happened, and on what network? (Office, home, wired, wireless, with/without VPN, etc.)
- What systems are you using? (Operating system, hostname, etc.)
- What account were you using?
- What data do you typically access?
- What were you doing when this occurred?
- Who else have you contacted about this incident, and what did you tell them?

Be aware that your incident response team may be available to assist with answering these questions.

Early in the investigation, contact your CISO. He or she will likely contact the cyber insurance provider to give them a heads up. This is important because they only pay settlements from the time they are notified. Insurance providers can also leverage security experts to assist in the investigation, as covered by your cyber policies.

Investigate

DETERMINE THE TYPE OF RANSOMWARE

1. Find any related messages. Check the following:

- Application screens [or graphical user interfaces (GUIs)] for the malware itself,
- Text, HTML files, or executable files, sometimes open automatically after encryption (make sure you also look behind existing, open screens),
- Look for new image files; they often appear as wallpaper on infected systems,
- Take photos of contact emails in encrypted file extensions,
- Observe and document pop-ups after trying to open an encrypted file, and
- Check your system for any voice messages that could be irregular.

2. Analyze the messages looking for clues to the ransomware-type:

- Ransomware name,
- Language, structure, phrases, artwork,
- Contact email addresses,
- Format of the user ID,
- Ransom demand specifics (e.g., digital currency, gift cards),
- Payment address in case of digital currency, and
- Support chat or support page.

3. Analyze affected and/or new files. Identify which data the attacker managed to encrypt. Check for:

- File renaming scheme of encrypted files including extensions (e.g., .crypt, .cry, .locked) and base name.
- Files that have been corrupted or encrypted.
- Targeted file types and locations, if possible.
- Who the user of the system should be (the "owning user") and determine the group of affected files.
- Any icons for encrypted files.
- Existence of file markers.
- Existence of file listings, key files, or other data files.

Continued — Determine the Type of Ransomware

4. **Analyze affected software or system types.** Some ransomware variants only affect certain tools (e.g., databases) or platforms (e.g., NAS products).

5. **Upload indicators to automated categorization services** like Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php), ID Ransomware (https://id-ransomware.malwarehunterteam.com), or similar.

DETERMINE THE SCOPE OF THE INFECTION

1. Which systems are affected?

- Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc.
- Use endpoint protection/EDR, endpoint telemetry, system logs, cloud logs, netflow logs, and other sources of information where possible.
- Check similar systems for infection such as similar users, groups, data, tools, department, configuration, and patch status.
- Check Identity Access Management (IAM) tools, permissions management tools, directory services, secrets managers, etc.
- Find external command and control (C2) traffic. If present, find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, NetFlow or router logs.

2. Find out what data is affected, such as file types, department, or group, affected software, customer environments, management planes, scanning tools, etc.

- Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools.
- Find changes to normally stable or critical data files. Check file integrity monitoring tools.

ASSESS THE IMPACT

Prioritize and motivate resources.

1. Assess functional impact and the impact to business.

- How much money is lost or at risk?
- How is the business degraded or at risk?

2. Assess information impact: impact to confidentiality, integrity, and availability of data.

- How critical is the data to the business? And to your customers?
- How sensitive is the data (e.g., trade secrets)?
- What is the regulatory status of data (e.g., PII, PHI)?

FIND THE INFECTION VECTOR

Check the tactics captured in the Initial Access tactic of MITRE ATT&CK. (https://attack.mitre.org/tactics/TA0001)

Common specifics and data sources include:

- Email attachment: check email logs, email security appliances and services, e-discovery tools, etc.
- Insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, etc.
- Self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, etc.).
- Infection via removable drives (worm or virus).
- Delivery by other malware or attacker tool: expand investigation to include additional attacker tools or malware.
- Scan all IT environments for potential entry points.

Remediate

- Plan remediation events where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- Consider the timing and tradeoffs of remediation actions: your response has consequences.

Contain

In ransomware situations, containment is critical. Inform containment measures with facts from the investigation. Prioritize quarantines and other containment measures higher than during a typical response.

Quarantines (logical, physical, or both) prevent spread from infected systems and prevent spread to critical systems and data. Quarantines should be comprehensive: include cloud/SaaS access, single-sign-on, system access such as to enterprise resource planning (ERP) or other business tools, etc.

- Quarantine infected systems.
- Quarantine affected users and groups.
- Quarantine file shares (not just known infected shares; protect uninfected shares too).
- Quarantine shared databases (not just known infected servers; protect uninfected databases too).
- Quarantine backups, if not already secured.
- Block command and control domains and addresses.
- Remove vector emails from inboxes.
- Confirm endpoint protection (AV, NGAV, EDR, etc.) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, operating systems, software, etc.).
- Deploy custom signatures to endpoint protection and network security tools based on discovered indicator of compromise (IOC).

Eradicate

- Rebuild infected systems from known-good media.
- Restore from known-clean backups.
- Confirm endpoint protection (AV, NGAV, EDR, etc.) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, operating systems, software, etc.).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs.
- Watch for re-infection – consider increased priority for alarms/alerts related to this incident.

Communicate

1. Escalate the incident and communicate with leadership per procedure.
2. Document the incident per procedure.
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, etc.
4. Communicate with internal users:
    i. Communicate incident response updates per procedure.
    ii. Communicate impact of incident and incident response actions (e.g., containment: "Why is the file share down?"), which can be more intrusive/disruptive during ransomware incidents.
    iii. Communicate requirements: "What should users do and not do?" See "Reference: User Actions for Suspected Ransomware" below.
5. Communicate with customers:
    i. Focus particularly on those whose data was affected.
    ii. Generate required notifications based on applicable regulations (particularly those that may consider ransomware a data breach or otherwise requires notifications, such as with HIPAA, or GDPR).
6. Contact insurance provider(s):
    i. Discuss what resources they can make available, what tools and vendors they support and will pay for, etc.
    ii. Comply with reporting and claims requirements to protect eligibility.
    iii. Communicate with regulators, including a discussion of what resources they can make available (not just boilerplate notification: many can actively assist).
7. Consider notifying and involving law enforcement:
    i. Local law enforcement,
    ii. State or regional law enforcement, and
    iii. Federal or national law enforcement. (https://www.nomoreransom.org/en/report-a-crime.html).
8. Communicate with security and IT vendors:
    i. Notify and collaborate with managed providers per procedure.
    ii. Notify and collaborate with incident response consultants per procedure.

Recover

- Launch business continuity/disaster recovery plan(s): e.g., consider migration to alternate operating locations, fail-over sites, backup systems.
- Recover data from known clean backups to known clean, patched, monitored systems (post-eradication), in accordance with our well-tested backup strategy.
- Check backups for indicators of compromise.
- Consider partial recovery and backup integrity testing.
- Find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page. (https://www.nomoreransom.org/en/decryption-tools.html)
- Consider paying the ransom for irrecoverable critical assets/data, in accordance with policy.
- Consider ramifications with appropriate stakeholders.
  - Understand finance implications and budget.
  - Understand legal, regulatory, and insurance implications.
  - Understand mechanisms (e.g., technologies, platforms, intermediate vendors/go-betweens).
  - Remove the malware by uninstalling everything on the infected device and reinstalling the operating system.
  - Restore data from the most recent backup available.
  - Determine how the intruder breached the system and make improvements to ensure the same attack does not happen again.
  - Remember, those who pay the ransom may think they have recovered, only to be attacked again because they've now become a "known payer." Becoming a known payer of ransoms puts a long-term target on the organization and contributes to the cybercriminal economy. For this reason, the FBI discourages the payment[35] of a ransom.

35. High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations." High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, Internet Crime Complaint Center (IC3), 2 Oct. 2019, www.ic3.gov/Media/Y2019/PSA191002.

Conclusion

Ransomware is going to continuously evolve and become more sophisticated and prolific. The consequences are costly, and more importantly, in healthcare it is a threat to patient safety. Right now is the time to prepare your organization for when, not if, an attack occurs.