MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD®

EVOLUTION OF RANSOMWARE

Kellyn A. Wagner Ramsdell and Kristin E. Esbeck

The MITRE Corporation

JULY 2021

Contents

Introduction

Modern ransomware is a business. Threat actors access victim networks through email or network vectors, exfiltrate data in some cases, and encrypt or otherwise block access to the original data. They then demand money to unlock a victim's data. In some cases, the phases of a ransomware infection are outsourced to other actors, often resulting in increased specialization and skill in ransomware attacks. Increased skill and other developments have enabled major changes in ransomware since it was first observed in 1989. Profit remains the primary motive, but ransomware is now a sophisticated threat capable of broader disruption.

The two main types of ransomware are locker and crypto. Locker ransomware locks a victim system and denies users access to data. Crypto ransomware encrypts the data on a target system. In both cases, the ransomware operators demand payment to unlock or decrypt the files. [1] Some threat actors may layer locker and crypto ransomware in hybrid attacks. In a less common third type of ransomware, threat actors demand a payment, but either never provide a decryption key or lack the technical ability to produce one. Called wiper ransomware, these attacks are either intended to be destructive attacks or are the result of technical flaws in the ransomware. Crypto ransomware is the dominant form of ransomware observed since 2013. Regardless of type, ransomware can be highly disrupting to any victim organization and has proven to be significantly disruptive in healthcare environments.

Evolution of Ransomware

The 1989 AIDS trojan was the first malware to encrypt data and demand a ransom payment for decryption. The malware was initially distributed on floppy disks, and it only encrypted the names of the files on a victim computer. Additionally, the malware only used symmetric encryption, meaning the decryption information was available on the victim device. [2]

General computer-enabled extortion attacks continued through the 1990s, where threat actors gained access to data – or claimed to – and demanded payment to decrypt data, prevent its encryption, or even prevent its public release. In 1996, Columbia University researchers proposed the idea of combining symmetric and asymmetric cryptography for use in "data kidnapping attacks." [3] Many ransomware variants now combine asymmetric and symmetric key encryption in multi-step key generation processes. This hybrid encryption is the dominant key generation method used in modern ransomware infections. The development of these encryption strategies enabled the rise of highly damaging ransomware by creating strong, secure decryption keys only accessible to the perpetrators. [4,5] Most modern ransomware leverages *Data Encrypted for Impact* [T1486] to force ransom payments.

From the 1990s to early 2010s, ransomware often either only pretended to encrypt data or the encryption was implemented incorrectly. As a result of these flawed implementations, early ransomware often did not result in data loss. [6] Threat actors still sometimes incorrectly implement encryption in ransomware; this is typically how researchers create decryption tools posted to No More Ransom or security vendor sites.

The next major evolution occurred in 2013 when CryptoLocker ransomware began infecting victims.

CryptoLocker combined public-key encryption and bitcoin ransomware payments. [7] Prior to CryptoLocker, ransomware payments were facilitated using e-wallets, prepaid debit cards, money transfers, gift cards, and other forms of payment that were difficult for threat actors to monetize at scale. Bitcoin's emergence in 2009 allowed rapid, pseudo-anonymous payments. [8] This shift then enabled the modern ransomware business model.

CryptoLocker's combination of bitcoin ransom demands and strong encryption allowed the operators to steal an estimated $27 million before the Federal Bureau of Investigation (FBI) disrupted the gang's operations in 2016. [9] CryptoLocker used "spray and pray" tactics to infect as many of victims as possible and they demanded smaller ransom payments of a few hundred dollars per victim. Spray and pray ransomware was the dominant model of ransomware prior to 2015 and some threat actors continue to use this infection strategy.

In the mid-2000s, ransomware was typically used against individuals and a few businesses. However, in 2015, threat actors began to recognize the value of ransomware in disrupting business operations. They began to demand ransoms based on ransomware's impact on operations, not just the inconvenience of data encryption. Instead of default amounts, threat actors began estimating the value of a victim's critical functions to determine the ransom demand. This shift drove the widespread targeting of businesses and critical industries seen with modern ransomware attacks.

Strong encryption. Rapid, anonymous payments. Value in business disruption. These incremental advancements in ransomware operations contributed to the emergence of the modern ransomware business model. The next business paradigm adopted was the services operating model.

In 2014, ransomware operators began selling ransomware in online forums as ransomware-as-a-service (RaaS). The first RaaS identified, CTB-Locker, operated an affiliate model RaaS in which ransomware creators hosted the malware, and affiliates deployed the malware on victim systems. The creators then got a portion of the ransom demanded from the victim. This reduced the risk to the affiliate and increased the profits for ransomware creators. [10] The affiliate model is the primary RaaS offering, but several other offerings exist. Some RaaS offer access methods alongside ransomware offerings, while others give customers the malware and do not require profit sharing with the ransomware creators. A fourth type of RaaS offering involves a subscription fee for "customers" who use the ransomware payload. [11] All four RaaS models lowered the technical ability required to conduct ransomware attacks, driving increased victim infections. [12]

As an extension of RaaS, some ransomware creators began outsourcing parts of their *Resource Development* [TA0042] to other skilled threat actors. In 2017, Jaff ransomware began renting the Necurs spam botnet to send malspam to millions of potential victims. [13] In 2018, *Ryuk ransomware* [S0446] began working with the Emotet [S0367] botnet to send infected Word documents to victims from compromised email accounts and then spread laterally. Ryuk operators then used this access to infect victims with ransomware in damaging ransomware attacks. This type of mutually beneficial partnership between multiple skilled threat actors continues and is associated with several of the most damaging modern ransomware variants.

RaaS insulates ransomware creators from law enforcement. When faced with law enforcement pressure, ransomware operators can quickly dissolve and reform under a new name. They can then contact known initial access brokers and resume operations. As a result, when ransomware groups declare retirement or disbanded operations, any reduced activity may only last until the gang can change the name of their product and resume sales. The RaaS operating model reduced the risk faced by operators, resulted in increased profits, and allowed for specialization between ransomware creators and initial access brokers.

For defenders, one of the most significant consequences of RaaS was that many ransomware variants became associated with a wide variety of infection vectors. Prior to the affiliate business models, most variants were associated with a limited number of infection vectors. This allowed victims to more quickly identify ransomware's infection vectors and begin remediation faster during incident response.

Customer service support is another common feature of the modern ransomware business model. CryptoLocker was one of the first groups to respond to victims' requests for help in public forums. Other ransomware groups have since negotiated with victims or offered guidance on acquiring bitcoin to pay the ransom. [14] Various ransom demands even offer to disclose how the threat actor compromised the victim, for an additional fee. These features show ransomware groups' business interest in ensuring victims pay the ransom.

The ransomware business model also drives threat actors to pursue other monetization strategies during the attack. These strategies can be broken into three broad categories: identification of additional victims; layering of cyberattacks; and data theft and/or public release of information.

Some early ransomware payments demanded victims either pay a ransom or infect two other victims to unlock their data. [15] This identification of additional potential victims continues to be a common monetization strategy, although the format has changed. When threat actors are in victim networks, they may use compromised email accounts to email malware to a victim's contacts. In the case of managed service providers (MSPs) infected with ransomware, threat actors may use the victim's *Trusted Relationship* [T1199] access to infect additional victims.

Other monetization strategies include layering multiple types of cyberattacks. Some threat actors install cryptocurrency miners on victim systems prior to encryption to enable *Resource Hijacking* [T1496]. If these miners are present in backups or systems where victims pay the threat actors, they will remain on a system after a victim thinks they have remediated the infection. Other groups have simultaneously launched *Network Denial of Service* [T1498] attacks to disrupt a victim's ability to communicate with their customers or stakeholders. These threat actors then demand a second ransom to end the denial of service. Since 2020, in a third type of layering, several ransomware gangs have reportedly layered either the same ransomware or multiple ransomware variants. [16] Impacted victims are then forced to pay multiple ransom demands if they choose to pay threat actors to regain access to their systems.

The final category of monetization strategies involves data *Exfiltration* [TA0010] or public release of information. One of the enduring monetization strategies is the resale of credentials stolen during initial infection. After the victim restores operations, if passwords are not reset enterprise-wide, these credentials can then be used by new threat actors to gain access. In other cases, threat actors steal victim data and auction it to the highest bidder on underground marketplaces.

As ransomware infections became more common starting in 2018, threat groups also began to extort money from victims seeking to keep ransomware attacks from the public view. Given the perceived reputational and regulatory ramifications of ransomware infections, many organizations chose to pay rather than have their attack publicized. The most damaging secondary monetization strategy with modern ransomware, however, is double extortion. In these cases, threat actors demand a second ransom payment to prevent the public release of stolen data. This escalation became a mainstream ransomware technique in 2019 when the Maze cartel announced a blog site for threat actors to post stolen data. [17] Multiple other ransomware groups adopted the same method and currently operate leak sites on the dark web.

The RaaS operating model is the dominant business model for some of the most disruptive ransomware in 2021, but it is not the only model. Some variants are still privately operated, and others are available for a one-time purchase on forums with bundled infection vectors. Select ransomware gangs still pursue spray and pray tactics, leveraging common vulnerabilities to infect a high number of victims. These many operating models means even victims who do not believe they are targets may still be victimized by ransomware.

Ransomware Threat Actors

Most ransomware operators are criminal groups seeking money from victims. The use of affiliates in some RaaS operations, however, create opportunities for overlap between state-sponsored threat actors and criminal affiliates. While there are no documented cases of foreign government threat actors serving as ransomware affiliates, Russian national Maksim Yakubets helped develop a trojan later used to deliver ransomware. Since 2017, he has also provided direct assistance to the Russian government. [18] This type of overlap can create the appearance that ransomware is state-sponsored activity, but this is often not the case.

The 2017 *WannaCry ransomware* [S0366] attack was the first ransomware attack attributed to a foreign government. That attack was an official North Korean government operation attempting to raise funds for their nuclear program. [19] Also in 2017, the widespread *NotPetya wiper ransomware* [S0368] was attributed to Russian government threat actors. [20] Finally, in 2020 and 2021, researchers associated Thanos and "Project Signal" ransomware with the Iranian government. [21,22] These are some of only cases of ransomware being directly attributed to a foreign government. It is primarily a tool used by cyber criminal threat actors.

The typical operating locations of many ransomware groups can also create the appearance of foreign government involvement in ransomware operations. Many cybercriminal groups operate in jurisdictions where they are unlikely to face prosecution. In many cases, groups will also avoid targeting businesses and individuals in their host country to avoid becoming a law enforcement target. This dynamic leads several groups to base their operations out of Russia, creating the appearance of Russian state involvement in some ransomware operations. Despite the appearance, there is no evidence of more direct collaboration beyond the cases above.

Common Initial Access Tactics, Techniques, and Procedures

Ransomware infections are multi-phase attacks where the initial steps often occur long before encryption. Preventing and detecting initial access is therefore one of the most significant parts of mitigating a ransomware infection. Most ransomware gangs gain initial access by sending phishing or spam emails, infecting websites, or exploiting network vulnerabilities.

Phishing and spam emails are a common malware delivery method. Threat actors send *Spearphishing Attachments* [T1566.001] or *Spearphishing Links* [T1566.002] to websites hosting malicious content. This malicious content then downloads malware onto a victim system. In many cases, the first malware on a system is a "loader" that serves to download secondary malware like banking trojans. These trojans conduct *Lateral Movement* [TA0008] through victim networks and often steal password *Credentials from Password Stores* [T1555]. Ransomware operators then leverage the trojans' access to infect victim networks.

Infected and compromised websites can be used to download malicious documents or steal user information that can later be used to gain access to victim systems. In some cases, malicious advertisements on websites are used to deliver malware. SocGholish is a well-known tool that uses *Drive-by Compromise* [T1189] to infect victims and gain a foothold for ransomware. The tool displays fake browser update windows. If a user clicks on the fake update, SocGholish downloads malware which can then serve as an entry point for later ransomware infections. [23]

One of the earliest and most common network-based infection vectors exploits open or weakly protected *Remote Desktop Protocol* (RDP) [T1021.001] ports. Other threat actors may *Exploit Public-Facing Applications* [T1190]. Recently targeted systems include virtual private networks (VPNs) and Microsoft SharePoint servers with critical vulnerabilities. A vulnerability in the Microsoft's *Server Message Block version 1 (SMBv1)* [T1021.002] enabled the *WannaCry ransomware* [S0366] infections starting in 2017. WannaCry demonstrated how network vulnerability-based infection vectors can enable the most widespread ransomware infections when the exploited vulnerability is wormable. Wormable exploits do not require user interaction to infect devices. These types of exploits enable malware on internet of things (IoT) devices, industrial control systems, and medical devices that would not typically be impacted in a ransomware infection.

Increased ransomware demands have greatly increased ransomware groups' operational budgets. This money is giving ransomware operators the budget to purchase or develop exploits for zero-day vulnerabilities, those for which patches do not exist. Since late 2020, three different ransomware groups have exploited zero-day vulnerabilities in three different types of software. [24,25,26] Although ransomware threat actors used zero-day vulnerabilities prior to these events, those vulnerabilities were first exploited by state-sponsored threat actors. In late 2020 and 2021, ransomware operators began originating zero-day vulnerabilities. This is a significant development in the skill of ransomware groups, likely made possible by massive profits from successful ransomware attacks.

There are other infection vectors and sometimes multiple infection vectors are used in the same attack. Organizations can begin their cyber threat intelligence journey by reviewing the tactics, techniques, and procedures (TTPs) of various ransomware groups and variants documented in the MITRE ATT&CK™ Framework. Click on the links below to view specific TTPs tied with each type of ransomware.

Researchers believe *Ryuk Ransomware* [S0446] is related to *Conti Ransomware* [S0575]. Both are distributed by *Trickbot* [S0266] and, before its takedown, *Emotet* [S0367]. Bazar *malware* [S0534] has also recently been used by Ryuk. Ryuk, Emotet, and Trickbot are all associated with Wizard Spider [G0102].

REvil (Sodinokibi) Ransomware [S0496] is operated by the GOLD SOUTHFIELD *group* [G0115].

Indrik Spider [G0119] has delivered multiple different ransomware variants.

Pysa (Mespinoza) Ransomware [S0583] is known to abuse *Remote Desktop Protocol* [T1021.001] to access victims.

BitPaymer Ransomware [S0570] is commonly delivered by the *Dridex banking Trojan* [S0384].

LockerGoga Ransomware [S0372] and *MegaCortex Ransomware* [S0576] used to target industrial targets.

The variants below are no longer active, but other threat actors may use similar infection vectors.

- *SamSam Ransomware* [S0370]
- *Maze Ransomware* [S0449]
- *JCry Ransomware* [S0389]

on evolving threat conditions. Automation and Orchestration, such as SOAR, improve cybersecurity posture by automating response actions in a more efficient manner across the enterprise.

Healthcare Case Study – Ransomware Attacks Impacting Radiology Services

In May 2021, the Conti ransomware group infected the Irish Health Services Executive (HSE) with ransomware. [27] Upon detecting the infection, HSE took all systems offline to protect patient data. The National Integrated Medical Imaging System (NIMIS) was one of the systems take offline. Ireland uses NIMIS to "electronically capture and store diagnostic images on a picture archiving and communication system (PACS)." [28] This resulted in delayed or postponed imaging, including oncology staging and surveillance scans. Radiotherapy treatments were also postponed and HSE is still investigating the long-term consequences of those delays. [29]

Tallaght University Hospital in Dublin moved to using handwritten radiology requests and formal reports for emergent care. To address concerns of incorrectly scanning a patient twice, secretaries began developing spreadsheets to track all imaging and imaging requests. The hospital also altered their policies for scanning, often performing multiple scans at the same time to reduce the risk of duplicate scanning. [30] Although critical care was maintained, ransomware had a broad impact on patients.

The attack against HSE is consistent with the increased targeting of healthcare entities observed during the COVID-19 pandemic and although it took place in Ireland, many US providers are similarly vulnerable. In January 2021, a former PACS administrator shared the details of her experience when the multi-hospital system she worked for was infected with ransomware. Sylvia Devlin report how ransomware forced the system to shutdown all electronic health record (EHR) systems and email. Radiology and imaging were severely impacted by the ransomware and the hospital's most recent hard copy downtime procedures were outdated. During remediation, the hospital system also discovered the ransomware impacted all the PACS workstations. They had to work with the vendor to identify how to get those systems to resume, meanwhile cardiology and fetal assessment were also impacted by the disrupted radiology and imaging systems. [31] Here again, ransomware had a significant impact on patient care.

To address concerns against PACS specifically, the National Institute of Standards and Technology (NIST) produced security guidance available here: https://www.nist.gov/publications/securing-picture-archiving-and-communication-system-pacs-cybersecurity-healthcare. These examples focus on a specific healthcare department, but they illustrate the broader impact of ransomware within healthcare environments.

References

1. S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi and R. Khayami, “Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence,” in I*EEE Transactions on Emerging Topics in Computing*, vol. 8, no. 2, pp. 341-351, 1 April-June 2020, doi: 10.1109/TETC.2017.2756908.
2. S. Davidoff, *Data Breaches: Crisis and Opportunity*, Boston, MA: Addison-Wesley Professional, 2019.
3. A. L. Young and M. Yung, “Cryptovirology: The Birth, Neglect, and Explosion of Ransomware,” *Communications of the ACM*, vol. 60, no. 7, pp. 24-26, July 2017. Available: https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext.
4. M. A. Aboud and K. Mariyappn, “Investigation of Modern Ransomware Key Generation Methods: A Review,” in 2021 *International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402680. Available: https://ieeexplore.ieee.org/document/9402680.
5. F. Cicala and E. Bertino, “Analysis of Encryption Key Generation in Modern Crypto Ransomware”, *IEEE Transactions on Dependable and Secure Computing*, pp. 1, 2020. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9130140.
6. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, “Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks,” in M. Almgren and F. Maggi, *Detection of Intrusions and Malware, and Vulnerability Assessment, Lecture Notes in Computer Science*, 2015, doi: https://doi.org/10.1007/978-3-319-20550-2_1.
7. S. Greengard, “The worsening state of ransomware,” in *Communications of the ACM*, vol. 64, no. 4, pp. 15-17, April 2021, doi: https://doi.org/10.1145/3449054.
8. M. Fuentes, F. Hacquebord, S. Hilt, I. Kenefick, V. Kropotov, R. McArdle, F. Merces, and D. Sancho, “Modern Ransomware’s Double Extortion Tactics and How to Protect Enterprises Against Them,” Trend Micro, Irving, TX, USA, 2021. Available: https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf.
9. B. Krebs, “2014: The Year Extortion Went Mainstream,” KrebsonSecurity.com. https://krebsonsecurity.com/2014/06/2014-the-year-extortion-went-mainstream/ (accessed Jun. 16, 2021).
10. J. Wyke and A. Ajjan, “The Current State of Ransomware,” Sophos, Boston, MA, USA, December 2015. Available: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf.
11. CrowdStrike, “Ransomware as a Service (RAAS) Explained,” CrowdStrike, Sunnyvale, CA, USA, January 28, 2021. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.
12. Trend Micro, “Ransomware as a Service,” Trend Micro, Irving, TX, USA, 2016. Available: https://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf.
13. D. Palmer, “This new ransomware nightmare demands a big payday to decrypt your files,” ZDNet, May 12, 2017. Available: https://www.zdnet.com/article/this-new-ransomware-nightmare-demands-a-big-payday-to-decrypt-your-files/.

14. D. Turkel, “Hackers are now offering ‘customer support’ to the victims they extort money from,” Business Insider, New York, NY, USA, January 9, 2016. Available: https://www.businessinsider.com/ransomware-writers-offer-customer-support-to-victims-2016-1.
15. T. Spring, “Ransomware Gives Free Decryption Keys to Victims Who Infect Others,” Threatpost, Woburn, MA, USA, December 9, 2016. Available: https://threatpost.com/ransomware-gives-free-decryption-keys-to-victims-who-infect-others/122395/.
16. L. Hay Newman, “Ransomware’s Dangerous New Trick Is Double-Encrypting Your Data,” Wired, San Francisco, CA, USA, May 17, 2021. Available: https://www.wired.com/story/ransomware-double-encryption/.
17. J. Agcaoili, M. Ang, E. Earnshaw, B. Gelera, and N. Tamana, “Ransomware Double Extortion and Beyond: REvil, Clop, and Conti,” Trend Micro, Irving, TX, USA, June 23, 2021. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.
18. United States Department of the Treasury, “Press Release: Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware,” December 5, 2019. Available: https://home.treasury.gov/news/press-releases/sm845.
19. United States Department of Justice, “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe,” February 17, 2021. Available: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.
20. United States Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” October 19, 2020. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.
21. C. Cimpanu, “Iranian state hacker group linked to ransomware deployments,” ZDNet, October 15, 2020. Available: https://www.zdnet.com/article/iranian-state-hacker-group-linked-to-ransomware-deployments/.
22. Flashpoint, “A Second Iranian State-Sponsored Ransomware Operation “Project Signal” Emerges,” Flashpoint, New York City, NY, USA, April 30, 2021. Available: https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/.
23. Proofpoint, “Fake Browser Updates Awareness Training – Attack Spotlight,” Proofpoint, Sunnyvale, CA, USA, 2020. Available: https://www.proofpoint.com/us/learn-more/attack-spotlight-fake-browser-updates.
24. A. Moore, G. Stark, I. Ibrahima, V. Ta, K. Goody, “Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion,” FireEye, Milpitas, CA, USA, February 22, 2021. Available: https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html.
25. J. Fleischer, C. DiGiamo, and A. Pennino, “Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise,” FireEye, Milpitas, CA, USA, April 20, 2021. Available: https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html.
26. Kaseya, “Incident Overview and Technical Details,” Kaseya, Miami, FL, USA, July 2021. Available: https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961.

27. L. Abrams, “Conti ransomware gives HSE Ireland free decryptor, still selling data,” *Bleeping Computer*, Melville, NY, USA, May 20, 2021. Available: https://www.bleepingcomputer.com/news/security/conti-ransomware-gives-hse-ireland-free-decryptor-still-selling-data/.
28. T. Anderson and W.C. Torreggiani, “The Impact of the Cyberattack on Radiology Systems in Ireland,” in *Irish Medical Journal*, vol. 114, no. 5, 2021. Available: http://www.imj.ie/wp-content/uploads/2021/05/The-Impact-of-the-Cyberattack-on-Radiology-Systems-in-Ireland.pdf.
29. Ibid.
30. Ibid.
31. D. Raths, “Imaging Informatics Exec: What It’s Like to Respond to a Ransomware Attack,” *Healthcare Innovation*, January 28, 2021. Available: https://www.hcinnovationgroup.com/cybersecurity/disaster-recovery-business-continuity/article/21207923/imaging-informatics-exec-what-its-like-to-respond-to-a-ransomware-attack.

Appendix A: Abbreviations and Acronyms

DDoS	Distributed Denial of Service
EHR	Electronic health record
FBI	Federal Bureau of Investigation
HSE	Irish Health Services Executive
IoT	Internet of Things
MSPs	Managed Service Providers
NIMIS	National Integrated Medical Imaging System
NIST	National Institute of Standards and Technology
PACS	Picture archiving and communication system
RaaS	Ransomware as a Service
RDP	Remote Desktop Protocol
SMBv1	Server Message Block version 1
TDoS	Telephony Denial of Service
TTPs	Tactics, Techniques, and Procedures
VPN	Virtual Private Network

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™