Ransomware Response, Safeguards and Countermeasures

It is time to reassess cybersecurity because current efforts to prevent ransomware events are porous and are not fulfilling their purpose. The facts are clear. Ransomware is distributed by a variety of methods,[1] including infected websites, online advertisements and Universal Serial Buses (USBs); direct attacks; phishing[2] (e.g., through email and more than 1.5 million unique phishing URLs[3]); and "Ransomware as a Service"[4] (e.g., malware, criminal activity). In 2019, ransomware from phishing emails increased 109 percent over 2017.[5] One report predicts that by 2021, an enterprise will fall victim to a ransomware attack every 11 seconds,[6] and according to another, "only 47% of people who pay ransom get their files back."[7] The potential targets are too numerous to mention, but they include local governments, financial services, law enforcement, academia, European agencies and healthcare organizations. And this is just the tip of the iceberg.

Ransomware

"Ransomware is malicious software (malware) used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment (usually cryptocurrency, such as Bitcoin) is made by the victim."[8] Ransomware can encrypt data files, system files and the entire disk. Attacks can stop or delete antivirus software, prevent system programs from working, make it impossible to boot from safe mode, block system updates and remove data rollback points. Malware can have many variations.

Infection vectors include email (script files, malicious attachments and links to malicious software), drive-by downloads (web exploit scripts and advertisements or malvertisements), social engineering via offers for free software (e.g., games, screensavers), vulnerable or unpatched software, and Remote Desktop Protocol (RDP). Threats are everywhere.

Cyberinsurance

Cyberinsurance is a consideration when planning for contingencies and disaster recovery, and a ransomware event falls into this category. Cyberinsurance provides some level of security in that it gives the enterprise the ability to recover from or respond to a cyberevent. Insurance can cover investigations, privacy alerts and notifications, lawsuits and extortion, legal fees and expenses, customer notification of data breaches, restoration of personal identities of affected customers, recovery of compromised data, and repair of damaged computer systems.[9] Enterprises should be able to obtain insurance that can be used to pay for Decryption as a Service (DaaS).

Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL V3, PMP
Is a senior consultant at Coalfire-Federal. He has more than 20 years of experience in IT security and privacy and has spoken at US government and professional conferences on these topics. He has written numerous magazine and newspaper articles, reviewed various ISACA® publications, and written questions for the Certified Information Security Manager® (CISM®) examination.

However, cyberinsurance typically does not cover everything. Uncovered losses and events typically include the following:[10]

- Anything above the enterprise's limit and sublimit caps
- Loss of intellectual property or trade secrets
- Brand damage
- Business interruption
- Lost revenue
- Negligence-induced incidents
- Nation-state attacks
- Postbreach remediation
- Physical damage

General liability is not adequate to ensure protection. Additionally, there is the risk that if the insurance is used to pay the perpetrators, they will not provide the decryption key needed to decrypt the affected data or files.

Response Options

During any ransomware event, a number of actions need to be performed immediately to identify the malware, contain the damage and determine a course of action.[11, 12] There are several possible responses to an enterprise-level ransomware event. Any of the following options can be used alone or in combination to manage a ransomware event.

Restore From Backups

Once a ransomware attack has been identified and contained, the typical response is to restore the affected files using the backups. The problem with this option is that the ransomware may have infected the network prior to activation, and during that time, the backup or archive files may have been encrypted as well.

Decrypt the Files

Decrypting the files is another response. As one option, the enterprise can try to do this itself using one of the numerous decryption tools available on the market, some of which are free.

A second option is to obtain help from a security vendor. Some security vendors provide DaaS to decrypt files. One decryption technique is to use a file of password variations to feed a script that uses them to decrypt a sample ransomware file back to its baseline.

A third option is to ask the government for help.[13, 14] If an enterprise chooses this option, it should be prepared (depending on the country) to provide the following information:

- Date of infection and victim information (e.g., industry type and business size)
- Ransomware variant (identified on the ransom page by the encrypted file extension)
- How the infection occurred (e.g., email link, browsing the Internet, social engineering)
- Requested ransom amount
- Amount paid (if any)
- Attacker's Bitcoin wallet address (which may be listed on the ransom page)
- Overall losses associated with a ransomware infection (including the ransom amount and victim impact statement)

Do Not Pay

The "do not pay" response puts the enterprise at risk of not recovering the data and being unable to resume business operations. This option may be taken for a number of reasons:

- The enterprise lacks the money (or insurance) to pay the attackers.
- The enterprise's policy does not allow payment.
- The board of directors has decided not to pay.
- The enterprise fears that if it pays, the perpetrators will attack again in the future.
- The enterprise fears the perpetrators will not provide the key to decrypt the system or data.

"THE "DO NOT PAY" RESPONSE PUTS THE ENTERPRISE AT RISK OF NOT RECOVERING THE DATA AND BEING UNABLE TO RESUME BUSINESS OPERATIONS."

- The enterprise has confidence in its IT operations.
- The enterprise has contacted vendors for help.

The decision to take this option may be made by enterprise management or, in the case of governments, by policy, law or directive. When choosing this option, recovery is difficult and may take a very long time. Using cyberinsurance that avoids paying the attacker may also be part of this option.

Pay the Attackers
This option entails the risk of being targeted again, being denied the decryption key despite paying the ransom, being forced to pay more for the promised decryption key and encouraging criminal behavior. However, for those who choose this option, there is a helpful guide available.[15]

Safeguards and Countermeasures

Ransomware safeguards can be broken down into the following areas: prevention, protection, detection, response and recovery. This section covers current and new recommendations, vendors that can help, and guidance available online.

Prevention
Prevention involves implementing safeguards viewed as best cyberpractices in the areas of network architecture, configuration and operations.

Architecture
Improvements in network architecture include categorizing data based on value and physically and logically separating networks and data accordingly. Reducing the attack surface by means of network segmentation results in better protection of high-value assets. Data can be protected either by not connecting sensitive data to the Internet or by creating a hidden storage area. To back up data twice, consider opening a temporary port and making secondary backups from primary backups. Cloud storage may be a good option.

Install and maintain software-based protection and detection, such as antivirus, antispam, and antiphishing software and filters, and multiple firewalls (to handle the volume). Develop containment strategies to make it difficult to exfiltrate data. One option is to implement a zero-trust environment for data egress. Also, consider executing operating systems or specific programs in a virtualized environment that has protections not available to dedicated hardware devices.

Local governments can standardize software within a jurisdiction so that if a ransomware attack occurs at one location, it can obtain a copy of the software from another site. This, however, is only a partial solution; although the government would be able to continue operations, data recovery is a separate concern (discussed later). Other institutions (e.g., healthcare enterprises) can implement similar types of architecture. The European Union,[16] the Center for Internet Security (CIS),[17] KnowBe4[18] and the National Cyber Security Centre[19] can provide guidance and assistance.

> "AN ENTERPRISE'S INFORMATION SECURITY POSTURE CAN BE IMPROVED BY IMPLEMENTING BEHAVIOR-MONITORING SOFTWARE AND NEW TECHNOLOGIES."

Configuration
Configuration safeguards include not mapping drives and hiding network shares so perpetrators cannot find key assets. Configure access and account controls to work on the principle of least privilege.

Implement software restriction policies (use whitelists instead of blacklists) and a zero-trust access policy (with access based on user role and device, not Internet Protocol [IP] address). The latter is a fairly new concept, but it has the advantages of limiting access to only those who have been vetted and restricting access to only approved and registered devices. If would-be attackers cannot get in, they may not be able to encrypt data files or application software.

Restrict the exfiltration of high-value data, such as monitoring egress activity and requiring a manual approval response. Block advertisements, proxy services, NoScript browser add-ons and known malicious IP addresses. Disabling macro scripts

> FOR SOME INDUSTRIES, SUBSCRIPTION SERVICES THAT CAN MONITOR AND SCREEN FOR MALICIOUS ACTIVITY AT THE PERIMETER, CAN BE AN ALTERNATIVE TO A ZERO-TRUST ENVIRONMENT.

reduces the ability to use utility programs or routines in memory. Disabling the RDP eliminates another potential means of entry. Configure the network to block file extensions in email (e.g., .js, .wsf, .zip). Also consider password-protecting archived files.

Operations

Operational safeguards should include patching operating systems, software and firmware. An enterprise's information security posture can be improved by implementing behavior-monitoring software and new technologies (e.g., artificial intelligence) and by using secure Hypertext Transfer Protocol Secure (HTTPS) filtering on all web traffic. The Host Intrusion Prevention Service (HIPS) and other signatureless technologies are essential to a strong cyberdefense, along with reviewing and exercising the enterprise's incident response plan (IRP) and practicing good cyberhygiene.[20]

The user interface should never be overlooked because users may be the weakest link when it comes to security. Provide security awareness training combined with simulated phishing attacks on a regular basis, and train users to connect only to sites that use cryptography (HTTPS) and to employ a virtual private network (VPN) connection for remote access.

Penetration testers can determine whether attackers will be able to find backups (regular and hidden). Backup data files are targets for ransomware attacks, but if they cannot be found, an enterprise will be able to recover from an attack.

Enterprises should consider increasing the security requirements of business partners and any entity with which they exchange high-value data. Sometimes the business partner is the weakest security link.

Developers and maintainers of operating systems should consider adding a new feature whereby sample files are created in the same space as the production environment. These sample files serve as baselines with known nonproduction data that can be used to break the ransomware's encryption code. To support this feature, software vendors need to create software scripts that can try unlimited variations of a decryption key to unlock the sample files. Once the key is found, the enterprise is informed.

Ransomware prevention software can monitor for unauthorized/hidden use of encryption software on files and directories, deactivation of device protective software, and for changes to the master boot record and master file table.

Guidance is available from BackBlaze[21] and Cisco[22] to help safeguard enterprises from ransomware attacks. One document from Cisco covers Domain Name System (DNS)—level security, email security, malware protection for endpoints and IRPs.[23]

Protection

Cybersoftware is one type of protection that can be implemented. Subscription services are available that can supplement an enterprise's cybersecurity safeguards. Software as a Service (SaaS) is a growing industry in which enterprises (e.g., payroll systems, alert notification systems) subscribe to these services, which can be viewed as enterprise-level systems. For some industries, subscription services that can monitor and screen for malicious activity at the perimeter, can be an alternative to a zero-trust environment.

Enterprises should develop business continuity plans and disaster recovery plans because ransomware is a viable threat with potentially catastrophic consequences. A ransomware event that is not handled properly can cause an enterprise's demise. Disaster recovery goals and procedures need to be reviewed and validated with executives to ensure business continuity.

A noteworthy US Department of Justice document that offers guidance on protecting networks from ransomware contains descriptions of ransomware, to help determine what the actual malware is. It also contains guidance on what to do if an organization is infected with ransomware and how law enforcement can help. [24]

The US National Institute of Standards and Technology (NIST) has issued Special Publication (SP) 1800-25, which contains identification and protection guidance related to network architecture (volume a), handling of attack scenarios (volume b) and how-to product installation guides (volume c).[25]

Detection
It is critical to detect attacks quickly and respond immediately. Activities and tools to improve the detection of malware include identifying, inspecting and tracking incoming and outgoing network traffic to see who is attempting to gain access and from where. This can be part of a zero-trust environment, or artificial intelligence (AI) software can be deployed to prevent unknown or suspicious network traffic.

An event logging program can be implemented. This includes reviewing the log reports daily and configuring them to send alerts for intrusive and suspicious activity. The event alert requirements should not be set so high that alerts are issued only after network entry has been gained. Unusual and suspicious activity can include long network connections, spikes in central processing unit (CPU) activity, types of files downloaded and network tasks not run by the system administrator. It is always better to prevent a network intrusion than to recover from an attack, although both should be part of a comprehensive plan.

Deploy AI software for monitoring, analysis and response, and conduct regular and frequent vulnerability scanning of key assets to identify weaknesses that require immediate resolution. Conducting annual penetration testing can identify weaknesses that other tools may not uncover. Additionally, security teams should periodically search for malware hiding places (e.g., archived data, email), and conduct annual security and privacy assessments.

NIST's SP 1800-26 contains similar guidance to SP 1800-25 but is oriented toward detecting and responding to adverse events.[26] This guidance can also be consulted for secure configuration settings. Administrators sometimes miss them during installation, and they may be unaware of upgrades to software.

Tools to help detect malware events may have scanners designed to locate systems on a network that are vulnerable to attack.[27] They may also automate the process of finding files encrypted by ransomware and provide the option of copying or moving the files to a new location.[28] Victims who have been impacted by a variant for which there is no free decryption tool could use another program to locate and store encrypted files until a later date, when a decryption solution may become available.

Response
Responses to a ransomware attack include having multiple versions of data; testing backups of data, system images and configurations; and storing backups on a separate offline device.

It is important to know the system's baseline for recovery and to test its reliability. The contingency plan for functional testing should be expanded to include verification that data files are usable, not just restorable, and that their integrity has not been compromised. Increasing the testing frequency (e.g., quarterly or even monthly) may be a good practice, especially for high-value data. Conducting simulated attacks to find weaknesses and identifying lessons learned are important when responding to all types of cyberattacks and for implementing appropriate countermeasures.

If the enterprise cannot determine how the ransomware was able to enter the network, help from outside experts who specialize in threat hunting and forensic analysis can be obtained. There are websites that provide guidance in the areas of response planning,[29] understanding the malware and ransomware removal.[30]

Recovery
Recovery from a ransomware attack is not always certain. However, there are some actions an enterprise can take:

- Obtain DaaS, if possible. Some software vendors provide this service, which decrypts a sample ransomware file back to its baseline.
- Remember that cloud providers may have files from a previous state. Make sure that system recovery and data recovery are covered in the service agreement.
- In an emergency or crisis, key data may be found in email attachments that are cloud based. This type of storage can help save part of the business (e.g., critical clients).

> "ONE WEAK LINK CAN ALLOW AN ATTACKER TO CIRCUMVENT CYBER SAFEGUARDS AND GAIN A FOOTHOLD IN AN ENTERPRISE'S ENVIRONMENT."

Conclusion

Despite all the safeguards and countermeasures put in place to prevent ransomware attacks, one of the biggest threats is social engineering. One weak link can allow an attacker to circumvent cyber safeguards and gain a foothold in an enterprise's environment. It is critical to implement a social-engineering awareness program that covers ways to recognize suspicious email links and attachments and to test staff frequently. Opening links and attachments in email and accessing infected websites are two common methods criminals use to gain access into the enterprise's digital infrastructure.

Social-engineering tricks that can be used to motivate an individual to unknowingly install malicious software include email notifications about antivirus protection expiring, popups and email concerning the need to install an update, and email requests for package delivery confirmation. Enterprises should implement filtering programs that can minimize this threat vector.

Endnotes

1 Eichner, J.; "Stop Ransomware 2—Where Does Ransomware Come From?" Kogo, *https://kogo.co.uk/stop-ransomware-2-where-does-ransomware-come-from/*

2 MacDougall, M.; "2018: A Reverse-Course for Ransomware," Cofense, 5 December 2018, *https://cofense.com/2018-reverse-course-ransomware/*

3 Webroot, "2019 Webroot Threat Report Mid-Year Update," September 2019, *https://mypage.webroot.com/rs/557-FSI-195/images/Threat_Report_Mid-Year_Update_Sept_US.pdf*

4 Unterfingher, V.; "Ransomware as a Service (RaaS)—Contemporary Mal du Siècle?" Heimdal Security, 11 November 2019, *https://heimdalsecurity.com/blog/ransomware-as-a-service/*

5 Cofense, "Ransomware Delivered by 97% of Phishing Emails by End of Q3 Supporting Booming Cybercrime Industry," Phishme, 17 November 2016, *https://phishme.com/ransomware-delivered-97-phishing-emails-end-q3-2016-supporting-booming-cybercrime-industry/*

6 Morgan, S.; "The 2019 Official Annual Cybercrime Report," Herjavec Group, *https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/*

7 Symantec, "Internet Security Threat Report (ISTR) Government," vol. 22, June 2017, *https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf*

8 Miller, L.; *Ransomware Defense for Dummies, 2nd Edition*, Cisco, *https://learn-umbrella.cisco.com/ebooks/ransomware-defense-for-dummies-2nd-edition*

9 Lindros, K.; E. Tittel; "What Is Cyber Insurance and Why You Need It," *CIO*, 4 May 2016, *https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html*

10 Chickowski, E.; "10 Things Cyber Insurance Won't Cover," *Information Week Dark Reading*, 14 April 2016, *https://www.darkreading.com/vulnerabilities—-threats/10-things-cyber-insurance-wont-cover/d/d-id/1325123?image_number=1*

11 KnowBe4, *Ransomware Hostage Rescue Manual*, 2019, *https://info.knowbe4.com/ransomware-hostage-rescue-manual-0*
12 ID Ransomware, *https://id-ransomware.malwarehunterteam.com/index.php*
13 US Federal Bureau of Investigation, "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," 2 October 2019, *https://www.ic3.gov/media/2019/191002.aspx*
14 US Federal Bureau of Investigation, "Ransomware Victims Urged to Report Infections to Federal Law Enforcement," 15 September 2016, *https://www.ic3.gov/media/2016/160915.aspx*
15 Zelonis, J.; T. Lyness; S. Balaouras; M. Cyr; P. Dostie; "Forrester's Guide to Paying Ransomware," Forrester, 5 June 2019, *https://reprints.forrester.com/#/assets/2/1666/RES154595/reports*
16 European Union, "Cracking Code: How the EU Protects Our Computers, Cybercriminals," *https://europa.eu/euprotects/our-safety/cracking-code-how-eu-protects-our-computers-cybercriminals_en*
17 Center for Internet Security (CIS), "Ransomware: Facts, Threats, and Countermeasures," *https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/*
18 KnowBe4, "Ransomware," *https://www.knowbe4.com/ransomware*
19 National Cyber Security Centre, "Mitigating Malware and Ransomware Attack," 13 February 2020, *https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks*
20 Wlosinski, L. G.; "Cybersecurity Takedowns: A Primer for Success," *ISACA® Journal*, vol. 6, 2019, *https://www.isaca.org/archives*
21 Bauer, R.; "Ransomware: How to Prevent Being Attacked and Recover After an Attack," BackBlaze, 18 April 2019, *https://www.backblaze.com/blog/complete-guide-ransomware/*
22 Cisco, "SAFE Design Guide," August 2017, *https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/ransomware-defense-dig.pdf*
23 Cisco, "Ransomware Galore: The Four You Shouldn't Ignore," 2018, *https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/ransomware-defense/ransomware-four-shouldnt-ignore.pdf*
24 Justice.gov, "How to Protect Your Networks From Ransomware," *https://www.justice.gov/criminal-ccips/file/872771/download*
25 National Institute of Standards and Technology (NIST), "Data Integrity—Identifying and Protecting Against Ransomware and Other Destructive Events," Special Publication (SP) 1800-25, USA, January 2020, *https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect*
26 National Institute of Standards and Technology, "Detecting and Responding to Ransomware and Other Destructive Events," SP 1800-26, USA, January 2020, *https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond*
27 Erez, E.; "Eternal Blues," Omerez, 28 June 2017, *http://omerez.com/eternalblues/*
28 Cimpanu, C.; "Cryptosearch Finds Files Encrypted by Ransomware, Moves Them to New Location," *BleepingComputer*, 15 January 2017, *https://www.bleepingcomputer.com/news/security/cryptosearch-finds-files-encrypted-by-ransomware-moves-them-to-new-location/*
29 New Jersey Cybersecurity and Communications Integration Cell, "Cyber Threat Profiles," USA, *https://cyber.nj.gov/threat-center/threat-profiles/#ransomware*
30 Avast, "Ransomware," *https://www.avast.com/c-topic-ransomware*