Ransomware Protection Strategies

Cyber Hygiene for Digital Resilience

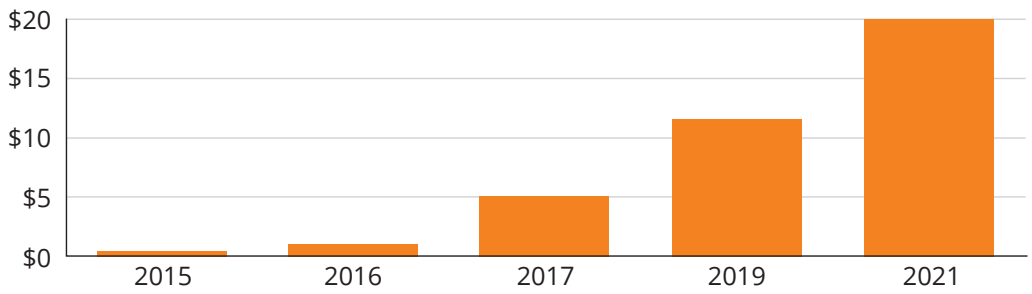
By Debra Baker, CISSP CCSP

Introduction

Ransomware attacks have been occurring at an alarming rate. From the estimated $10 million payout from Garmin to the Evil Corp Ransomware gang to the attack on a major United States (US) hospital chain that forced the hospital system to use an all-paper system, the devastating effect of ransomware can be seen. The ransomware attack on Colonial Pipeline caused massive disruption of gasoline supply throughout the US South and Northeast. These attacks are not only costly but can bring a company's operations to a halt. The below chart illustrates the exponential cost of ransomware attacks over time.

Ransomware gangs have become more sophisticated in their attacks to ensure they receive a payout. Before 2020, most ransomware attacks were delivered via a malware payload in email. A bogus link would lure the unsuspecting victim into downloading something from a website, or the malware would be attached to the email. Once the malware was launched, the victim's computer hard drive would be encrypted. The victim's computer screen would alert them that their computer hard drive was now encrypted and that they had to pay a ransom to receive the encryption key. In the background, the malware self-propagates using remote desktop protocol (RDP) port 3389 or Server Message Block (SMB) ports 139 & 445 infecting other computers on the same network segment.

Figure 1: Ransomware cost - courtesy of CyberVentures Cybercrime Magazine[1]



STEEP PRICE

In 2021, the largest Ransomware payout was $40M and average downtime is 21 days.*

[1] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

[2] https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

REDSEAL

Figure 2: Pre-2020 Ransomware Attack

In 2020 and beyond, the ransomware gangs have upped their game by hacking into a potential victim's network primarily using Internet Aggregator sites such as Shodan or Censys to find exposed RDP and SMB ports on a victim's network. Additionally, attackers may leverage unpatched externally facing hosts and devices or send malware or a bogus link via email. Once inside a company's network, the attacker will quietly move about trying to find the critical assets where the Personally Identifiable Information (PII) and intellectual property reside. Next, the attackers will exfiltrate the sensitive data offsite to a server that the ransomware gang controls. Once they have a copy of the sensitive data, the attackers will launch the ransomware attack.

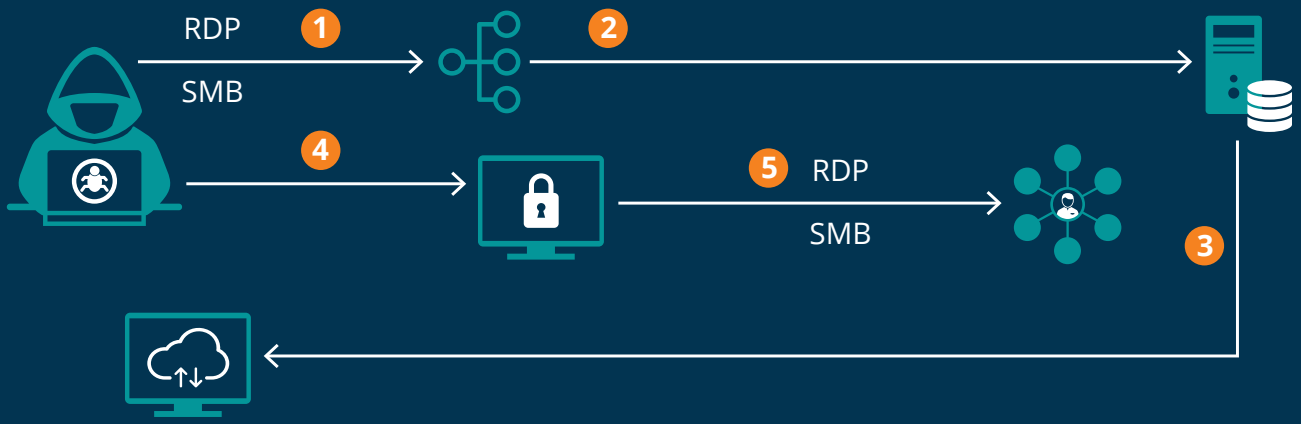


Figure 3: 2020 and beyond Ransomware Attack

Ransomware attacks are paid because of two reasons. One the cost of paying the ransom is less that the cost to restore operations. The second reason is extortion. The attackers threaten to release the victim's sensitive information. The ransomware gang exfiltrates unencrypted sensitive data to ensure the company will pay the ransom even if they have good backups. Today, good backups in itself will not prevent the company from paying the ransom. If a few days or weeks go by and the ransom has not been paid, then the ransomware gang will notify the company that they have sensitive information belonging to the company. The ransomware gang will explain that they will post the company's sensitive data on the dark web, unless the company agrees to pay the ransom. This is a reason the value of ransomware payouts has gone up exponentially. This also means the ransomware gang now knows the victim company's network, so ensuring the company has good cyber hygiene is paramount not only to prevent the disruption of being a victim, but to ensure the attackers can't easily gain reentry into the victim's network.

How to Protect Your Network

Having good cyber hygiene is your best defense against ransomware. As a quick reference, see Figure 4 below

Know Your Network

You can't protect what you don't know about, and this is precisely where RedSeal can help. One of the biggest threats to your company are unknown network devices and hosts connected to your on-premises network or in the cloud. You must know what is on your on-prem and cloud networks to protect them. Tanium recently published a white paper that was based on an independent study of 750 Information Technology (IT) decision-makers.

"Nearly all (94 percent) of the IT decision-makers surveyed have discovered endpoints in their organization of which they were previously unaware. And nearly three-quarters of CIOs (71 percent) say their teams discover new [unknown] endpoints weekly." It's the unknowns that puts your network at risk. The reason is that unknown endpoints and devices on your network are not being actively managed. If it's a host or server it may not be patched or running corporate approved software and configured according to your company's secure configuration baseline. If it's a network device, then it may not be patched or configured according to your company's security policy.

Figure 4: Quick Reference for Cyber Hygiene

1. Know Your Network
   - 1.1. Network Inventory
   - 1.2. Discovery
2. Segmentation
   - 2.1. Identify Your Critical Assets
   - 2.2. Place Critical Assets into High Value Segments
3. Vulnerability Management
   - 3.1. Vulnerability Prioritization with Network Context
4. Secure Configuration Network Devices
   - 4.1. Center for Internet (CIS)
   - 4.2. Security Technical Implementation Guidance (STIGS)
5. Multi-factor Authentication
6. Data Protection
   - 6.1. Encryption
   - 6.2. Offline Backups
7. Security Awareness

You need an asset management system to track all the assets on your network from when they are first purchased through the disposal. Having a good network inventory and understanding where your PII data resides is critical to ensure the data is securely encrypted and on a protected network. There are many products that can provide asset management capabilities to your company such as ServiceNow, Remedy, or RSA Archer. The tricky part is tracking the endpoints you don't know about such as unauthorized devices and unknown hosts. This is where RedSeal can help. RedSeal is able correlate data from your Asset Management System, Vulnerability Scanners, and Network Device Configurations to discover unknown devices, hosts, and coverage gaps in your vulnerability scanning program.

In addition, RedSeal provides visibility of access into your network from the internet and untrusted subnets. Discovering and validating the access to critical assets from other segments within your network are critical to securing your sensitive data from attackers. The reason is any network device or endpoint visible to the internet or untrusted network could have an open port, unauthorized protocol, or vulnerability allowing

an attacker access into your network. Ensure you deploy an endpoint detection and response (EDR) such as Windows Defender on hosts to ensure an alert is created when ransomware or associated malware is detected.

Segmentation

Once an attacker gains access to your on-prem and/or cloud networks, if your network is flat (unsegmented), then the attacker can easily move laterally on your network to find hosts that store PII and other sensitive data. Therefore, network segmentation is paramount to securing your network. Network Segmentation ensures that there is not a free flow of network traffic on your general network. Ideally, the following endpoints should be on separate segments:

- Internet of Things (IoT)
- Critical Assets storing sensitive data
- Systems supporting critical business functions
- Printers
- Workstations

Network segmentation will ensure that if a workstation has ransomware, then the malware can only self-replicate on a particular segment where it resides. This will ensure the ransomware gang is unable to gain access to critical assets and PII data that can force your company to pay the ransom even if you have good backups because the PII data can be sold on the dark web. Every commercial customer network has thousands of vulnerabilities and security holes. It is not possible to eradicate all the vulnerabilities. Having a single host or server being hacked or compromised is not the end of the world. The real issue is when your network is not segmented, so one compromised host will lead to several more compromised hosts and servers, to a point where a ransomware situation is mature and deep enough, you are not able to restore to a basic operational state which is the real threat.

Vulnerability Management

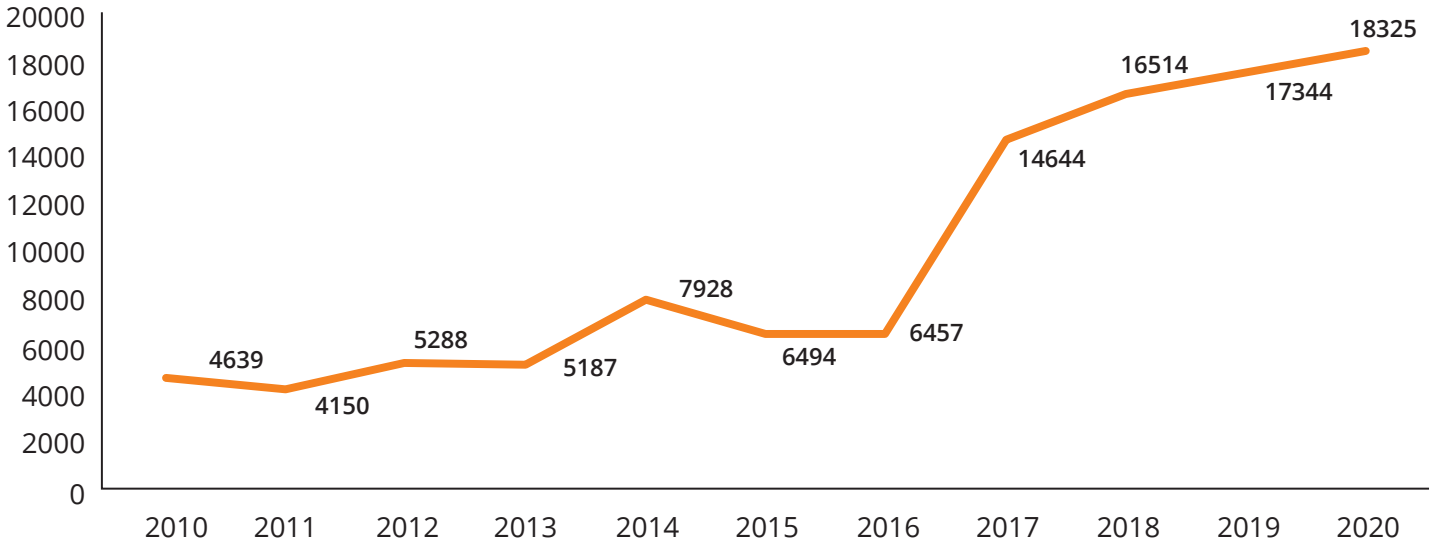
See Figure 5 below, to see all Common Vulnerability and Exposures (CVE) which are software vulnerabilities from 2010 to 2020. The dramatically increasing number of vulnerabilities means that vulnerability management teams need to work smarter. RedSeal can help by prioritizing software vulnerabilities, not just by the Common Vulnerability Scoring System (CVSS) which is commonly done, but by factoring in network location and asset value. RedSeal can prioritize the software vulnerabilities on your network, so that your Vulnerability Management team can focus on patching critical assets and hosts that are exposed to the internet first. Since attackers are scanning your perimeter for exposed vulnerabilities, you want to prioritize patching these hosts first.

Secure Configuration Network Devices

Secure configuration of your company's network devices is key to securing your network from ransomware attackers. Good cyber hygiene begins with the secure configuration baseline of your network devices. Using RedSeal to audit the network device configurations on a continual basis will alert you of misconfigurations and being out of compliance. To protect from ransomware, you must limit the use of high risk ports such as remote desktop protocol (RDP) port 3389 or Server Message Block (SMB) ports 139 & 445.

According to the Gartner, "through 2023, 99% of firewall breaches will be caused by **firewall misconfigurations**, not firewall flaws."[3]

Figure 5: All CVEs 2010-2020[2]



Multi-Factor Authentication

Multi-Factor Authentication (MFA) is one of the single most important security features you need to use to protect yourself and your company. Using passphrases such as a sentence with spaces is recommended with a minimum password length of 12 characters. For Administrator accounts, a minimum password length of 14 characters or higher is recommended. Adding a second factor authentication, such as google authenticator is paramount to protecting your accounts. Using a password wallet such as LastPass or Okta that stores all your passwords and creates long complex passwords for each account is recommended. Also, ensure you turn on two-factor authentication for the password wallet account. You can harden your devices and cloud services using MFA and check against the compliance using Center for Internet Security (CIS) benchmark libraries using RedSeal.

Data Protection

Your last defense in protecting your organization from ransomware attacks are good offline backups and data encryption. If the ransomware attackers are not sophisticated, many times the encryption key is available from a trusted site such as nomoreransom.org which may have the decryption key.[4] If you have good offline backups, then you may be able to just restore from backup. The backups need to be offline because all online connected drives on a ransomware infected host will be encrypted by the ransomware. When all else fails, encrypting your data will secure it from hackers. Data encryption is the last defense of your PII and sensitive data. If an attacker gains access to your critical assets, but the data is securely encrypted, then they won't be able to access the data ensuring it is safe from extortion.

Security Awareness

Your company needs to ensure there is a security awareness training program that teaches employees how to spot a bogus email or link. There are plenty of video learning programs like KnowBe4 or Infosec Institute that can be used to train your employees. In addition, having an email filter service like Mimecast is recommended.

Footnotes

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.cvedetails.com/browse-by-date.php

[3] https://www.guardicore.com/blog/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them/

[4] https:// nomoreransom.org; https://www.barkly.com/ransomware-recovery-decryption-tools-search

How RedSeal Can Help

- RedSeal is able correlate data from your Asset Management System, Vulnerability Scanners, and Network Device Configurations to discover unknown devices, hosts, and coverage gaps in your vulnerability scanning program. The vulnerability scan results are augmented with RedSeal's Threat Reference Library (TRL). The comprehensive vulnerabilities are overlayed with a 3D map of the network (cloud, Datacenters, On-Prem, and remote sites.)
- The addition of location data allows RedSeal to go beyond vulnerability and create a threat map of the network. In addition, understanding access into your network from the internet and within your general network is critical for securing your network.
- RedSeal can give you visibility of unintended access from the internet and untrusted subnets into your general network using access queries and detailed path queries. RedSeal can identify critical assets on your network and those assets can be segmented from the general network using Zones and Policies. RedSeal will monitor and send alerts if unintended access is allowed into the segment.
- RedSeal provides Vulnerability Prioritization based on access, making hosts that are externally visible to the internet and critical assets that can be exploited for lateral movement a higher priority, so they get patched quicker.

Ransomware Protections Checklist

☐ Scheduled Backups; Keep offline backups

☐ Use Host Defender i.e. Windows Defender, Crowdstrike, Tanium

☐ Turn it off! Remove infected host from Wired and Wireless Network

- Quickly identify the kill chain

☐ Don’t use Windows 98, XP, Windows 7 and Windows Server 2008

- No longer patched and frequently exploited
- Win 7 and 2008 stopped receiving security updates as of January 14, 2020

☐ Turn off Remote Desktop Protocol (RDP) port 3389

- Frequently exploited by Ransomware

☐ Block port Ports 137-139, 445, & 3389 from external networks

- Don’t use SMB 1.0, should be using SMB 3.0 >> WannaCry
- If have SMB 3.0 in use, but have not disabled SMB 1.0, hackers could use SMB 1.0

☐ Check well known site like nomoreransom.org which may have the decrypt key

- https://www.nomoreransom.org
- https://www.barkly.com/ransomware-recovery-decryption-tools-search

References

https://www.ibmsystemsmag.com/Power-Systems/03/2020/Ransomware-Attacks-on-the-Rise

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-20th-2019-attacks-everywhere/

https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

https://threatpost.com/ransomware-attack-new-jersey-largest-hospital-system/151148/

https://www.cnn.com/2019/11/12/tech/google-project-nightingale-federal-inquiry/index.html

https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Decryption Key Websites:

https://www.barkly.com/ransomware-recovery-decryption-tools-search

https://nomoreransom.org

https://id-ransomware.malwarehunterteam.com/

ABOUT REDSEAL (redseal.net)

RedSeal – through its cloud security solution and professional services -- helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises – into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL

1600 Technology Drive, 4th Floor, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net

SEPTEMBER 2021