NETSPI™

The Ultimate Guide to Ransomware Attacks

What is Ransomware?

Ransomware, a type of malware, is top-of-mind for all organizations today as attacks become more sophisticated and its impact increasingly detrimental. When infected with ransomware, organizations lose access to their systems and/or data and the cybercriminals demand a ransom in exchange for releasing the data.

One in four companies worldwide pay the ransom to regain access to their files. However, paying up does not always pay off. The likelihood of getting all your data back after paying is slim. In 2021, only 8% of companies that paid received all their encrypted files, according to SonicWall's Cyber Threat Report.

To stop ransomware attacks, collectively we need to cut off the cybercriminal's source of income – that means not paying the ransom and understanding the alternative steps to take to prevent and respond to a ransomware attack.

IN THIS ULTIMATE GUIDE TO RANSOMWARE ATTACKS, **EXPLORE:**

1. RANSOMWARE TRENDS, TARGETS, AND FAMILIES
2. HOW RANSOMWARE WORKS
3. HOW TO PREVENT AND DETECT A RANSOMWARE ATTACK

Ransomware Trends, Targets, and Families

Before arming your organization with the right security protocols and tools to prevent a ransomware attack, it is important to understand the ransomware ecosystem. This includes the latest trends, understanding who a prime target is, and which of the 400+ ransomware families to watch.

Ransomware trends:

- The ransomware-as-a-service (RaaS) model is on the rise. With RaaS, attackers do not write the malware, they purchase and spread it. Commissions are paid to the developers for the use of the malware.
- With COVID, remote worker entry points are being targeted much more, including remote desktop, employee access gateways, and VPN access portals.
- Operational technology is a prime target. According to IBM Security X-Force, 41% of all ransomware attacks targeted organizations with operational technology (OT) networks.
- Email phishing, admin interfaces, and exploits are common entry points, and drive-by downloads (malvertising, force download, or exploit browser) are becoming more popular.
- Many threat actors that deploy ransomware attempt to disable backup/recovery capabilities so victims are forced to pay if they want access to their systems and data.
- Once ransomware is deployed, IBM X-Force estimates 70% of victims are paying ransoms.
- Ransom demands are increasing exponentially. We are now seeing ransom demands of more than $40 million. IBM Security's X-Force data shows that 20 percent of compromised organizations have paid ransoms of more than $40,000, and 25 percent have paid between $20,000 and $40,000.

Who is a target?

Attackers consider many variables when choosing which organizations to target with ransomware. It is important to understand that ransomware attacks are both opportunistic and targeted – and no industry is exempt from being targeted. Opportunistic attacks may target the public utilities sector knowing that it historically has immature and underfunded security programs.
They may also target organizations that cannot afford downtime and are more likely to pay the ransom faster.
This includes healthcare organizations, where they rely on their systems to provide patient care.

Ransomware families to watch:

Ransomware Family	RaaS Support	Initial Access Vectors	First Seen	MITRE Software TTP's
MAZE	Yes	Phishing, Macro, VDI, RDP, Exploits	2019-Present	https://attack.mitre.org/software/50449
Sodinokibi	Yes	Phishing, Macros, VDI, RDP, Exploits, Malvertising, WaterHoling	2019-Present	https://attack.mitre.org/software/50496
Ryuk	Yes	Phishing, Macro, VDI, RDP, Exploits	2018-Present	https://attack.mitre.org/software/50446
Netwalker	Yes	Phishing, Macro, VDI, RDP, Exploit	2020-Present	https://attack.mitre.org/software/50457
SamSam	Unknown	Phishing, Macros, VDI, RDP, Exploits,	2019-Present	https://attack.mitre.org/software/50370

How Ransomware Works:

Step 1: Getting in

Adversaries can get into a network in numerous ways. Here are four vectors used to gain initial access:

1. Phishing links and attachments.
2. Using weak or default credentials to log into single factor remote management interfaces and desktop platforms such as Citrix, Remote Desktop, and VPN access points.
3. Exploitation of common security vulnerabilities, including SQL injection, broken authentication, broken access control, and insufficient logging and monitoring.
4. Unintentional download and execution of malware through obfuscation and/or social engineering techniques (drive-by downloads, malvertising, forced download, or browser exploits).

Step 2: Privilege escalation

Once in, adversaries work to exploit bugs, design flaws, or configuration oversights in an operating system or application to gain access to protected databases, file shares, and business sensitive data. They often use Server Message Block (SMB) exploits, weak passwords, and insecure Active Directory configurations.

Step 3: Find and exfiltrate sensitive data

Attackers leverage well known techniques to quickly identify servers that may contain sensitive data and upload the data to systems on the internet. Threat actors often follow this workflow:

1. Perform Active Directory reconnaissance for all domain computers, SQL Servers, and SMB shares.
2. Attempt access to file servers and SQL Servers with privileged accounts.
3. Search for sensitive data patterns across file servers and SQL Server databases.
4. Package data for export (this often includes encrypted and compressing data).
5. Upload data to systems on the internet in one large file or in parts using common protocols such as SMB, Secure Shell (SSH), file transfer (FTP), and HTTP/HTTPS.

Step 4: Ransomware deployment

Now it is time to deploy the ransomware. Ransomware can take many forms, including: locker (uses screen locking to block basic computer functions), wiper (deletes files on a timer), or crypto (encrypts important data and often includes a kill switch to delete data if the ransom is not paid by a specific time).
Here are the steps ransomware families often take to deploy the malicious code:

1. Verify correct platform, language, and time zone
2. Disable or bypass detective security controls
3. Remove system restore capabilities
4. Encrypt files, often targeting specific file types and resulting in central processing unit (CPU) spikes
5. Overwrite MBR (less common, but growing in popularity)
6. Propagate over SMB to spread through the environment

Standard file encryption process:

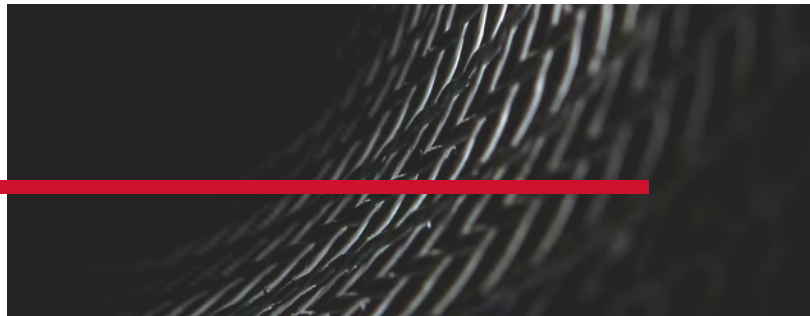
1. Hardcoded or generated RSA key pair
2. Generate Advanced Encryption Standard (AES) key
3. Encrypt files with AES
4. Encryption AES key with public key
5. Only a private key can be used to decrypt the AES key required to decrypt the files

Step 5: Get paid for the decryption key

Often ransomware attackers request the ransom is paid in Bitcoin. Once paid, the likelihood of recovering the money is low. Even when money is returned you're not likely to get all of it back. For example, in 2021 the FBI recovered $2.3 million of the $5 million from the Colonial Pipeline attackers.

Step 6: Extort additional money by threating to publish exfiltrated data

Adversaries exfiltrate sensitive data early in the ransomware deployment process so that, even if a ransom is paid, they can continue to threaten the organization and make more money.

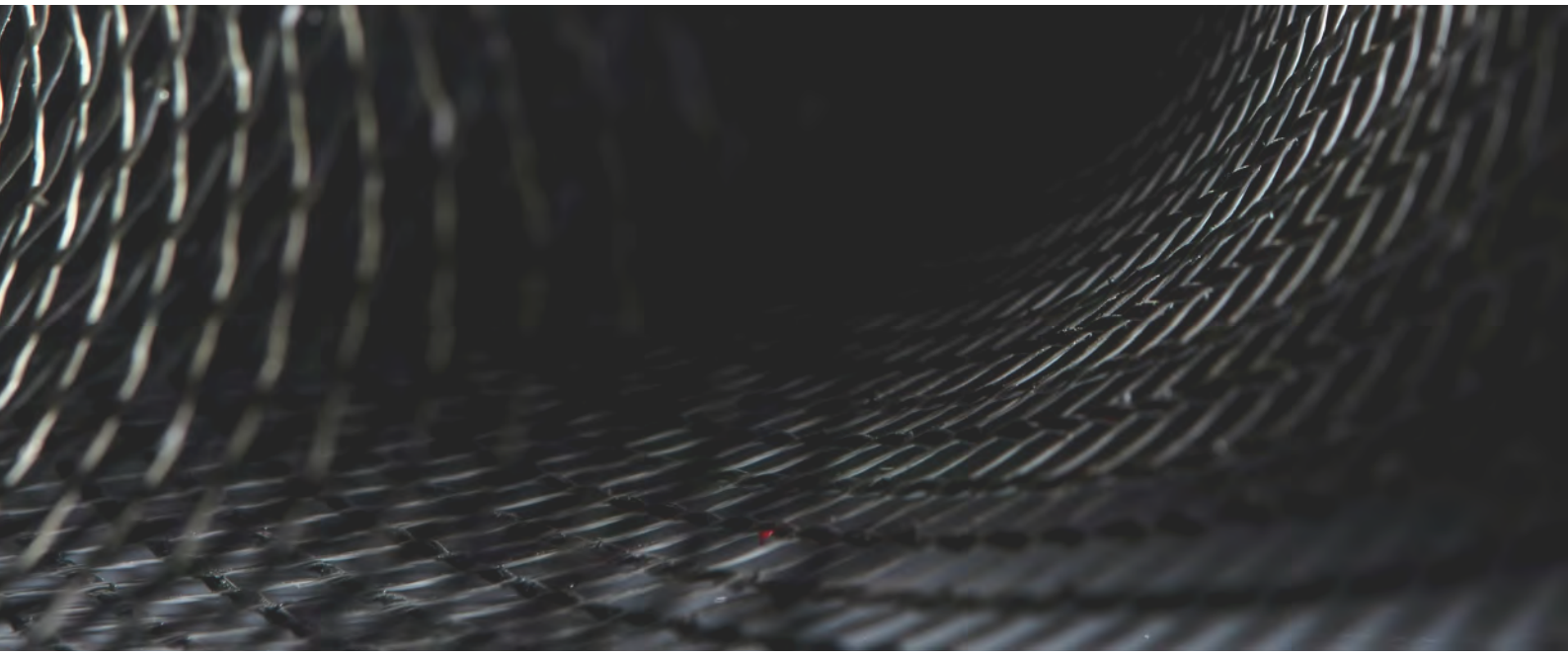


How to Prevent and Detect a Ransomware Attack:

Remember, paying a ransom is a losing game. Invest in security now to avoid paying a ransom later. Leverage the following checklists to proactively prevent ransomware and ensure your ransomware detective controls are working as intended.

Ransomware prevention checklist:

- [ ] Continue to build and maintain robust asset management, vulnerability management, patch management, and configuration management programs.
- [ ] Reduce and monitor all internet facing attack surfaces.
- [ ] Enable multi-factor authentication on all internet-facing interfaces.
- [ ] Ensure least privilege is enforced across applications, cloud platforms, systems, and databases.
- [ ] Isolate sensitive networks, systems, and data.
- [ ] Isolate and validate backup and restore capabilities.
- [ ] Perform a comprehensive evaluation of how your preventative and detective controls hold up to TTPs used by real-world ransomware.



Ransomware detection checklist:

- [ ] Ensure data sources are available to provide your security operations teams and/or partner with enough information to develop detections for common malicious behavior. This should include file modification events, registry modification events, process creation events, image load events, network connection events, Windows endpoint security event logs, command line event logs, PowerShell event logs, Netflow/Pcap data, and security event data from third party software or devices.
- [ ] Ensure your security operations team and/or partner have the capability to tune or create new detections. NetSPI found that most endpoint detection and response and security information and event management (SIEM) solutions only identify around 15% of the most common TTPs used by real world attackers out of the box.
- [ ] Ensure that alert levels trigger response for high-risk behavior associated with high fidelity detections.
- [ ] Ensure detections cover common defensive evasion techniques and are not limited to known bad script and executable behavior.
- [ ] Deploy or configure monitoring for high-risk command execution related to scheduled tasks, service manipulation, and lolbins (living off the land binaries) execution.
- [ ] Monitor for the deletion of shadow copies.
- [ ] Monitor for modifications to SafeBoot and similar restore capabilities.
- [ ] Ensure security tool tampering logs are enabled and forwarded to the SIEM.
- [ ] Monitor for high CPU utilization on individual systems and the average across the network.

During NetSPI's ransomware attack simulation engagement, we closely collaborate with organizations to simulate sophisticated ransomware modules using our custom-built attack and breach simulation technology.

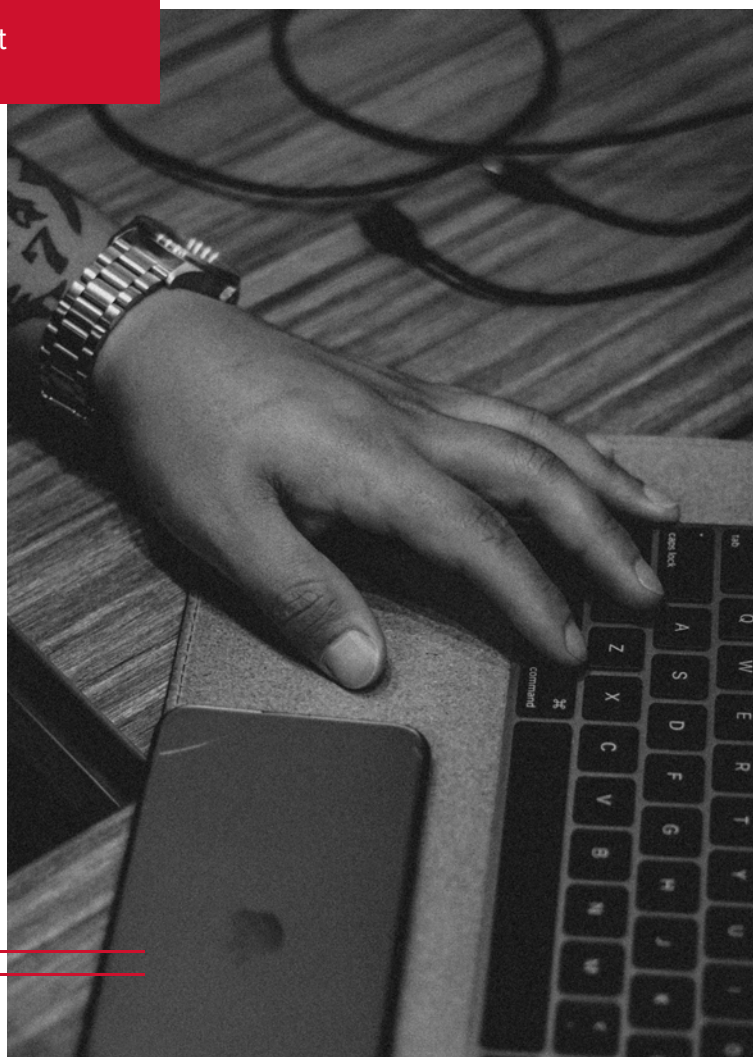
Then, we enable you to continue testing and develop custom attack plays and playbooks on your own. Gain a greater understanding of your ransomware prevention and detection capabilities and learn where gaps exist in your program.

Looking forward:

Many governments are discouraging ransomware payments because they naturally fuel a threat actor's ability to conduct future ransomware attacks. However, right now, no one is outright prohibiting direct ransomware payments or ransomware insurance claims. If we do not see new regulations restricting ransomware payment, hopefully, we will see governments offering some subsidies to small and medium businesses that can't afford to partner with security firms but may be considered high-risk targets. While we wait for the global cybersecurity community to work toward solutions, Ransomware Resiliency Planning is going to become a priority for everyone. We hope this guide helped provide you with a jump start in the right direction.

For continued reading on the state of ransomware attacks, read:

- Red Canary 2021 Threat Detection Report
- CrowdStrike® 2021 Global Threat Report
- FireEye and Mandiant M-Trends 2021
- Verizon 2021 Data Breach Investigations Report



About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable guidance allowing our customers to find, track, and fix their vulnerabilities faster.

Email **sales@netspi.com** to learn more or call us at **612-465-8880**