secpod

THE DEFINITIVE GUIDE TO

Prevent Ransomware Attacks

www.secpod.com

Introduction

Not one cybersecurity professional in the world would like to see the below image in one of the devices they manage.

The image is the end result of a ransomware cyberattack, and the impact it can have on your organization can be fatal and crippling.

Ransomware isn't just a buzzword in the cybersecurity world; it's one of the most pressing threats businesses face today. With attacks occurring every 11 seconds and resulting in billions of dollars in damages annually, understanding ransomware is more than a necessity; it's a business imperative. It's a problem of today!

But the biggest challenge?

We react to ransomware instead of trying to find ways to prevent it.

This ebook will help you answer the most important question.

How do you prevent a ransomware attack?

Understanding the Ransomware Threat Landscape

Before we discuss the prevention aspect of ransomware attacks, it's critical to dissect, analyse, and autopsy the attack itself. Understanding ransomware and how it works will help us develop the right strategies to combat it.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that locks or encrypts data, holding it hostage until a ransom is paid. Hackers and attackers aim to extort money by rendering critical systems and information inaccessible.

Ransomware can typically infiltrate your systems via phishing emails, RDP brute-force attacks, drive-by downloads, software vulnerabilities, and malicious ads (malvertising).

Types of Ransomware

Crypto Ransomware
These attacks typically encrypt files and demand payment for the decryption key, usually cryptocurrency. Some of the biggest ransomware attacks have asked for payments through crypto due to its anonymity. Example: LockBit, Conti, Revil.

Locker Ransomware
These attacks lock users out of their entire system, but the key differentiator is that they don't encrypt files. Example: WinLocker

Scareware
Another ingenious type of ransomware, Scareware creates fake software alerts claiming a malware infection, demanding payment for a "fix." In reality, there's no infection, and you pay for nothing! Example: Rogue antivirus tools

Doxware (or Leakware)
These attacks go a step further from a typical ransomware by threatening to publish or leak the stolen data if the ransom isn't paid. Often, attackers target establishments that work with sensitive data or IPs for more effectiveness.
Example: Maze, Babuk

ATTACK VECTORS OF RANSOMWARE AND MOTIVATIONS

Attack vectors are paths or ways for an attacker to get into your system and do damage. Like most attacks, ransomware leverages multiple attack vectors to breach your system. Ransomware attacks commonly originate through phishing emails, software vulnerabilities, remote desktop protocol (RDP) exploits, and even infected USB drives.

Ransomware attacks can happen for various reasons, but typically, the motivations are monetary. But threat actors can also leverage these attacks for corporate espionage, cyber warfare, and more.
Let's take a look at some of the biggest ransomware attacks and the motivations behind them.

High-Profile Case Studies

1. Colonial Pipeline Ransomware Attack

In May 2021, Colonial Pipeline, a critical U.S. fuel infrastructure operator, fell victim to a devastating ransomware attack by the cybercriminal group DarkSide. The attack forced the company to shut down operations for six days, disrupting nearly 45% of the East Coast's fuel supply and causing widespread panic buying, fuel shortages, and price spikes. Colonial Pipeline ultimately paid a $4.4 million ransom in Bitcoin to restore systems, though authorities later recovered $2.3 million of the payment.

The attack exposed vulnerabilities in critical infrastructure, with estimated economic losses exceeding $100 million. DarkSide, a Russia-linked group, operated under a ransomware-as-a-service (RaaS) model, targeting high-value victims for financial gain. The incident prompted the US administration to issue an executive order strengthening federal cybersecurity standards and spurred renewed focus on protecting energy grids and supply chains from cyber threats.

MAY 2021
Critical US Infra Operator fell victims to ransomware attack by Darkside

Shut down operations for 6 days

Operator paid $ 4.4 million ransom in Bitcoin

Exposed vulns with economic loss exceeding $100 million

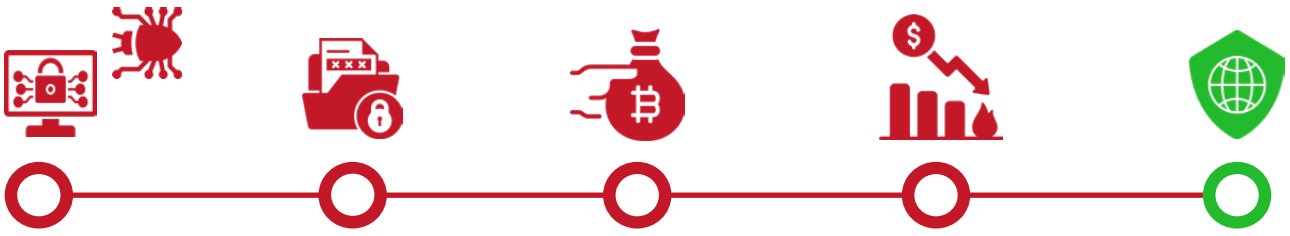
US Admin ordered to strengthen federal cyber security standards

2. WannaCry Ransomware Attack

In May 2017, the **WannaCry ransomware** attack infected over **200,000 systems** across **150 countries,** causing widespread disruption. The malware exploited a **Windows vulnerability** (EternalBlue) leaked from the NSA, encrypting files and demanding **$300-$600 in Bitcoin** per device. High-profile victims included **Britain's NHS,** forcing hospitals to cancel surgeries and rely on paper records.

WannaCry's rapid spread was due to its **self-replicating worm** capability, affecting unpatched systems. A kill switch, discovered by a cybersecurity researcher, slowed its progress. Estimated damages exceeded **$4 billion,** highlighting risks of outdated software and government-held exploits.

The attack was linked to **North Korean hackers (Lazarus Group)**, blending cybercrime with geopolitical motives. It spurred global emphasis on **patching systems, network segmentation, and ransomware preparedness,** influencing corporate and government cybersecurity policies.



MAY 2017
WannaCry ransomware infected 200,000 systems across 150 countries

Windows vulnerability (EternalBlue) leaked from NSA & encrypted files

Demanded $300 to $600 in Bitcoin per device

Estimated damages exceeded $4 billion

Global emphasis & influence of corp. & gov. cybersecurity policies

Anatomy of a Ransomware Attack

Understanding how ransomware attacks unfold is critical to designing robust defenses. While not every attack might have all these steps, most ransomware attacks typically have these five broad steps:

1. INITIAL ACCESS & INFECTION

What's the Objective?

Gain a foothold in your network by gaining access to your network.

How does the hacker achieve it?

Phishing Emails
Malicious attachments or links deliver ransomware payloads that you might unknowingly click and download.

Exploiting Vulnerabilities
Unpatched software that contains critical vulnerabilities is exploited to provide entry to your network

Brute-force Attacks
Weak passwords on your network can be used to brute-force and break into it!

Malvertising & Drive-by Downloads
Compromised websites trigger malware downloads that can infect your network and provide access to your network.

Third-party Compromises
Supply chain attacks or breaches in vendors themselves, leading to a cascading effect on your own network if you're using the infected software or service.

2. LATERAL MOVEMENT

What's the Objective?

Expand control across your network infrastructure to maximize impact.

How does the hacker achieve it?

Pass-the-Hash/Pass-the-Ticket
After gaining access, hackers try to steal credentials to move between systems.

Exploiting Active Directory (AD) Weaknesses
By leveraging weaknesses in your Active Directory, attackers can escalate privileges.

ARP Spoofing & Network Scanning
By spoofing your ARP or scanning your network, attackers can identify high-value targets (e.g., file servers, backups) and target them first.

RDP & SSH Hijacking
Additionally, hackers can also use stolen credentials to access other machines and spread the ransomware.

3. PRIVILEGE ESCALATION

What's the Objective?

Gain higher-level permissions (e.g., Domain Admin) to disable defenses and get greater control over your network.

How does the hacker achieve it?

Exploiting Zero-Day Vulnerabilities
Hackers leverage unpatched OS/software flaws to escalate privilege.

Dumping Credentials
Hackers extract cached passwords from memory and try to gain administrative privileges for more damage.

Modifying Group Policies
Threat actors try to disable security tools (AV, EDR, backups) to infect more devices and do more damage.

4. DATA ENCRYPTION AND EXFILTRATION

What's the Objective?

Lock your files or sensitive data and steal it for double extortion.

How does the hacker achieve it?

Deploying Ransomware Payload
Hackers encrypt files with a strong algorithm that can't be cracked easily.

Disabling Backups
Backups are the bane of hackers, so once in, hackers try to delete them so they don't lose their leverage.

Exfiltrating Data
For double extortion, hackers often upload the sensitive files to attacker-controlled servers and hold them for leverage.

5. RANSOM DEMAND

What's the Objective?

Demand ransom for your encrypted data and extort money, typically in cryptocurrency.

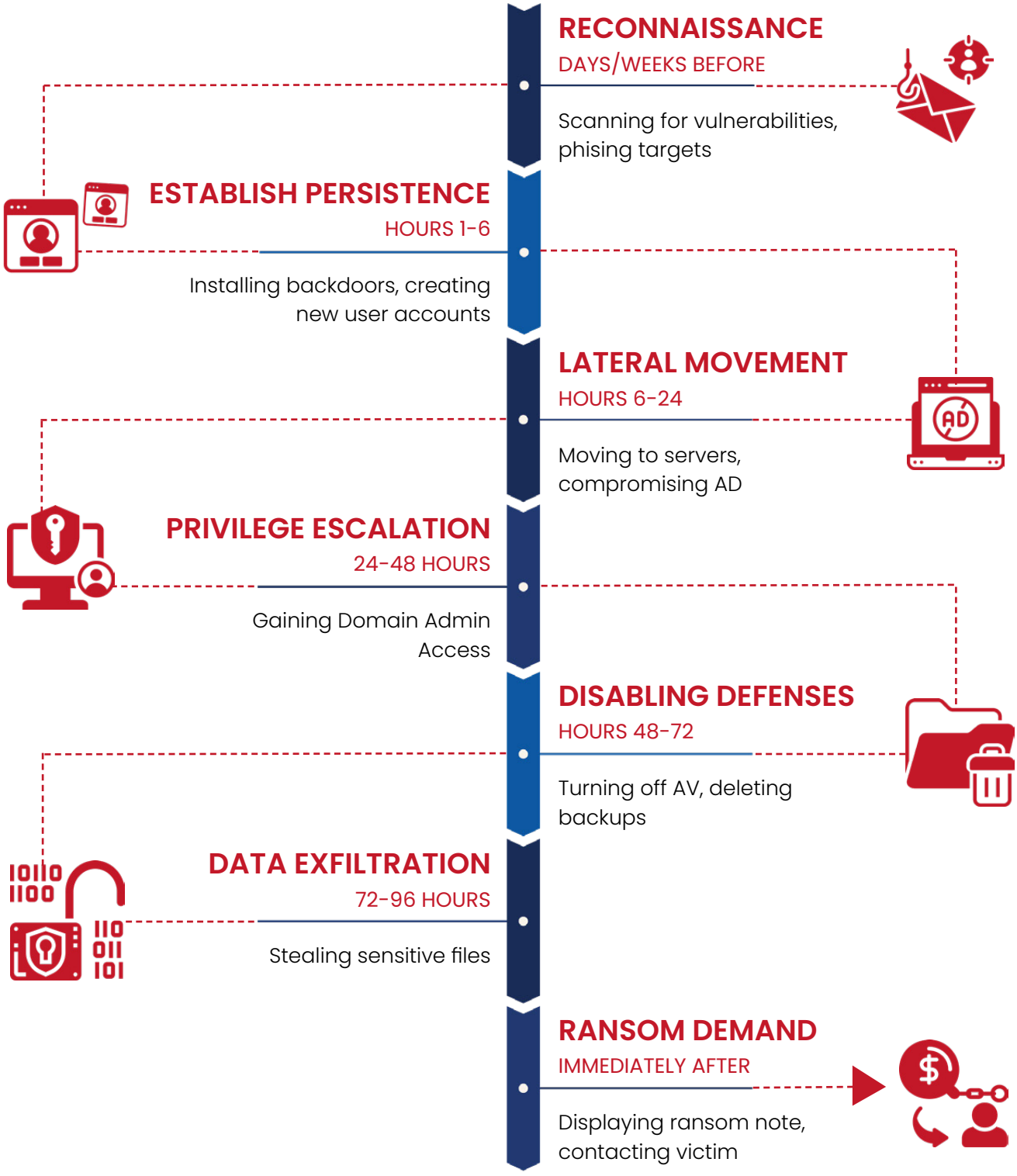
How does the hacker achieve it?

Bitcoin/Monero Demands
To maintain anonymity, hackers ask you to pay via cryptocurrency.

Negotiation Tactics
To create fear as well, hackers try to offer discounts for quick payment, but often don't hold up to their promises.

Follow-up Extortion
Taking a step further, threat actors demand more money to prevent future leaks.

Typical Ransomware Attack Timeline



Nine Golden Rules to Prevent Ransomware

You know the what and the how of ransomware. However, the most important thing is how to prevent ransomware cyberattacks effectively. Here are the 10 golden rules you must follow and implement to drastically reduce your attack surface and chance of preventing ransomware.

1. IDENTIFY CRITICAL ASSETS

Understanding which systems and data are most vital to your business is the first step toward protection. Identify the most important and sensitive assets and information, such as customer data, financial systems, proprietary information, and the servers. Document their location, access patterns, and dependencies. This insight helps prioritize security efforts and ensures limited disruption if ransomware strikes.

Asset classification also enables you to:

1. Plan your risk management
2. Make informed backup strategies
3. Plan for a faster response

Without knowing what to protect, defending effectively becomes nearly impossible.

2. UNDERSTAND YOUR ATTACK SURFACE

Do you know your attack surface? Do you know all its components? So, understanding your attack surface could be the difference between a successful breach and effective prevention. Your attack surface includes all entry points an attacker could exploit, including endpoints, servers, apps, cloud instances, users, and even third parties.

So, visibility into your attack surface is key. Here are two points you must remember:

1. Unknown assets are unprotected assets and gateways to a threat actor.
2. Periodic detection of shadow IT or unpatched devices is a must.

Understanding this landscape helps prioritize defenses and block attack paths before ransomware can find them.

3. VULNERABILITY MANAGEMENT

Closely linked to the previous two rules, vulnerability management is an often overlooked but most critical aspect of attack prevention. Ransomware often exploits known, unpatched vulnerabilities.

So, to combat these exploits and prevent ransomware, you must:

1. Implement a structured vulnerability management program to scan regularly, automatically, and quickly patch the detected risks.
2. Use automated scanning tools supplemented by manual testing for deeper insights.
3. Analyze the results to prioritize remediation based on risk, business impact, and risk appetite.
4. Beyond CVEs, scan for misconfigurations, legacy systems, and third-party software risks.
5. Prioritize vulnerabilities using risk-based frameworks (e.g., CVSS, EPSS, or CISA KEV list).
6. Automate patch deployment for operating systems, apps, and firmware.

Think bigger and don't just focus on the critical ones alone. Many ransomware attacks use medium-severity risks to breach your network, and vulnerability management is the most important weapon in your security arsenal. **Vulnerability management is the core to your security posture.**

4. ENDPOINT AND NETWORK SECURITY

Every endpoint in your network is a potential entry point for a hacker, so treat it as part of your security responsibility.

That's where endpoint and network security come into play.

1. Secure endpoints with EDR tools that detect suspicious behaviour, not just known malware.
2. Segment your network to limit ransomware's ability to spread and keep user workstations separate from critical systems.
3. Implement zero-trust principles & use next-gen firewalls to inspect traffic and block malicious payloads.

5. SECURE CONFIGURATIONS & NORMALIZE ANOMALIES

Misconfigurations and posture anomalies in your network can be an open invitation for attackers.

Here are a few pointers to keep in mind:

1. Enforce the principle of least privilege so that users have only the access they need.
2. Disable unused services and restrict administrative privileges to prevent misuse.
3. Detect posture anomalies and misconfigurations with scanners and mitigate them immediately.

A good place to start would be compliance policies like CIS Benchmarks and NIST guidelines, which provide strong baselines. A well-configured, normalized, and compliant system is much harder for ransomware to compromise.

6. BACKUP AND RECOVERY

Backups are your last line of defense and must be ransomware-proof and completely secure. **Follow the 3-2-1 rule: three copies, two different storage types, one off-site and one offline.** Once you are set with the backups, regularly test restoration to ensure data integrity and recovery speed. In a ransomware event, fast recovery can be the difference between hours and weeks of downtime.

7. FOLLOW COMPLIANCE GUIDELINES

Compliance helps enforce good security hygiene and reduce ransomware exposure. Ensure your ransomware response plan includes regulatory notification requirements. Conduct audits to stay compliant and align with evolving laws. While compliance isn't security by itself, it's a foundation, and non-compliance during or after a ransomware event adds legal and financial risk.

8. LEVERAGE INTEGRATION & CENTRALIZATION

Too many tools can cause you more problems than required. In this modern era, with multiple tools and platforms for each and every aspect of security, tracking tools themselves can be painful.

That's where integration and unification come into play. A unified approach to cybersecurity can drastically improve your security posture and process. If you have a single tool for vulnerability detection and remediation, then the manual process of correlating risks to patches is completely eliminated, and remediation becomes faster and better. Another benefit of integrating your entire security process is that it becomes easier to get a single view of your IT landscape and take control of what is important!

9. SECURITY AWARENESS AND TRAINING

Human error remains the biggest enabler of ransomware. It is also the biggest challenge and hurdle you might not really have complete control over.

So, creating a security-first culture where employees feel accountable is key.

1. Train employees to spot phishing, suspicious links, and social engineering tactics.
2. Simulate attacks regularly to reinforce awareness and identify risky users.
3. Teach basic cyber hygiene: strong passwords, MFA, and secure browsing.

Awareness isn't a one-time event; you must make it a continuous process. So, be proactive, teach proactive, and empower users to report threats and respond quickly.

LET'S RECAP

- **Identify Critical Assets**
- **Understand Your Attack Surface**
- **Vulnerability Management**
- **Endpoint and Network Security**
- **Secure Configurations & Normalize Anomalies**
- **Backup and Recovery**
- **Follow Compliance Guidelines**
- **Leverage Integration & Centralization**
- **Security Awareness and Training**

The Future of Ransomware Attack Prevention: Emerging Defenses

A good sign in the cybersecurity market is that more and more vendors are leaning towards preventing attacks instead of reacting to them. So, here are the two biggest emerging pillars in ransomware attack prevention that you must keep a tab on and try to implement for improved security.

AI-DRIVEN SOLUTIONS

AI is the talk of the town. Every town. In cybersecurity, AI models are being trained on threat behavior and are revolutionizing ransomware prevention. We can leverage AI to detect and stop encryption attempts, lateral movement, or unusual privilege escalations before data is compromised. So, by observing, analysing, and constantly improving, AI cuts reaction times from hours to milliseconds, reducing your attack surface and the breach impact drastically.

ZERO TRUST ARCHITECTURE

Another impactful new development, Zero Trust security ensures every user and device is continuously authenticated, authorized, and validated. The keyword here is segmentation. Segmenting your network's access, you reduce chances of lateral movement which in turn contains ransomware spread. In ransomware defense, this model stops compromised credentials or devices from accessing critical assets without passing stringent checks.

Ransomware Prevention with Saner Platform

Combating ransomware attacks in today's landscape requires a sophisticated and integrated strategic approach.

The Saner platform is a state-of-the-art cyberattack prevention platform that leverages the Continuous Vulnerability and Exposure Management (CVEM) framework, providing comprehensive detection, assessment, and mitigation of security risks.

It streamlines the risk management process, seamlessly integrating detection, remediation, and beyond for both cloud and endpoint infrastructures.

It detects vulnerabilities, misconfigurations, exposures, and more in your cloud and IT infrastructure. With the power of automation and a continuous approach to risk management, the Saner platform significantly accelerates the mitigation process, reduces the attack surface, and proactively guards against cyberattacks.

Especially ransomware!

Conclusion

Cyberattackers use clever and increasingly complex methods to launch ransomware into your network. So, you need all the help you can get to stop them!

Vulnerability management paired with effective security controls are the most powerful weapons in your arsenal to combat and prevent ransomware cyberattacks.
Further, establishing a proactive and effective strategy and strengthening your security posture will help you achieve what matters most.

A cyberattack-free organization.

About SecPod

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

www.secpod.com | info@secpod.com