SpyCloud

RANSOMWARE PREVENTION CHECKLIST

A proactive approach to combating ransomware attacks

Ransomware continues to be a top cybersecurity challenge for organizations of all sizes and industries.

While phishing and social engineering remain some of the most common entry points for ransomware, criminal technology is advancing to leverage hard-to-detect infostealer malware technologies that infect both corporate and personal devices.

As cybercriminals increasingly use infostealer malware as the starting point for follow-on ransomware attacks, it's important to adapt our prevention measures accordingly. Resulting attack patterns can slip through gaps in traditional security measures, so understanding the current state of ransomware can help us form the best defense strategies to prevent these costly cyberattacks.

RANSOMWARE IMPACT REMAINS HIGH

81% of surveyed organizations experienced at least one ransomware attack in the past 12 months. Of these organizations, 39% reported cumulative costs of at least **$1 million.**

INFOSTEALER INFECTIONS ARE A WARNING SIGN

Of 2600+ North American and European companies impacted by ransomware,

30% had 1 or more infostealer infections prior to being attacked.

TIME TO ATTACK IS SHRINKING

The average duration of a ransomware attack – from initial access to ransomware deployment – is now less than **24 hours**

STANDARD DEFENSES DON'T CUT IT

Relying on antivirus software deployed on employee devices isn't enough. Over

20% of companies had antivirus installed at the time of data exfiltration.

Use this ransomware prevention checklist to adapt your prevention strategy in the face of the evolving ransomware threat.

RANSOMWARE PREVENTION CHECKLIST

- [ ] **Educate employees on malware threats**

Continuously train and educate employees on common ransomware attack vectors like phishing emails and malicious attachments. Be aware of new infostealer malware technology that has the ability to exfiltrate active sessions and cookies, passwords, cookies, autofill information, and even desktop files like the **LummaC2 Stealer**.

- [ ] **Improve VIP and executive hygiene**

Detect exposures for **high-profile employees' personal accounts** as they are increasingly targeted for cyberattacks. Guide VIPs on how to create and manage strong passwords and reset exposed credentials to prevent targeted attacks.

- [ ] **Enforce strong passwords to protect accounts**

Enforce **strong password practices**, like banning commonly-used or easily guessable passwords that include things like your company name. Encourage the use of a password manager to create and store passwords for corporate accounts, and automatically detect and reset exposed passwords.

- [ ] **Automate software patching**

Leverage **automated patch deployment** to keep employee systems and applications up to date and prevent vulnerabilities from being exploited. Start small by prioritizing the most critical applications and identify which workflows are well-suited for automation.

- [ ] **Remove blindspots in personal devices**

If you can't implement security policies to prevent network access from personal devices, **detect any malware-infected devices** outside corporate control that are being used by employees, contractors, and vendors. Hidden infostealers could grab corporate application credentials and open up attack vectors.

- [ ] **Shut down application entry points**

Research shows that a single malware infection can expose access to **up to 26 business applications**. Prevent criminals from exploiting this access by resetting compromised credentials of applications beyond your primary domain, including password managers, CRMs, chat programs, ticketing systems, HR and payroll platforms, and other jumping-off points that could be used to gain access and escalate privileges across the network.

- [ ] **Prevent session hijacking**

Stolen session cookies can give cybercriminals access to critical applications, allowing them to bypass SSO, MFA, and even passwordless technologies. It's crucial to have access to **compromised cookie data** associated with your domains so you can invalidate active sessions and prevent session hijacking that could precede a ransomware attack.

- [ ] **Automate remediation workflows**

Embrace automation to move faster than attackers. Where possible, integrate high-priority breach and malware record data into automated workflows within your **SIEM / SOAR platforms** to remediate and reset exposed credentials – before criminals can use them for follow-on attacks.

- [ ] **Shift towards an identity-centric response**

Follow all the steps above, and be sure to expand your malware infection response beyond just the device level by monitoring employee, contractor, and vendor accounts for credential and cookie exposure – and taking rapid action. **Early detection and remediation** of these exposures will holistically protect your employees' digital identities and your sensitive data from ransomware attacks.

And remember, don't get caught being overconfident!

Ransomware is constantly evolving. Measuring your confidence in your ability to prevent ransomware attacks based on the past can be dangerous. **SpyCloud's Ransomware Defense Report** showed that 79% of organizations are confident in ransomware defenses today, but only 19% are prioritizing improved visibility and remediation of exposed credentials of malware-exfiltrated data. Continue investing in training and tooling to shut down ***all*** entry points for ransomware, including emerging threats.

A NOTE ON EMERGING MALWARE TRENDS THAT CAN FUEL RANSOMWARE

At SpyCloud, our research team tracks the latest trends in malware technology to provide teams with guidance and tools to stay ahead of ransomware and other targeted follow-on attacks. Here's some rising trends we are actively monitoring.

MOBILE MALWARE

Mobile malware technology is advancing, giving bad actors new ways to exploit vulnerabilities and steal personal data, passwords, and financial information. Mobile malware infections and the rise of personal device use for transmitting corporate data increases the risk of follow-on attacks.

SPYCLOUD INSIGHT

We're seeing bad actors launch targeted financial attacks where they access banking applications via SMS or MFA bypass. Read about it >

macOS MALWARE

Malware is no longer a concern for just Windows users. We're seeing malware infections on macOS devices increase, compounded by frequent personal device use at home – often MacBooks – to access corporate networks and business applications.

SPYCLOUD INSIGHT

We're seeing a rise in attacks from malware called Atomic macOS Stealer that can exfiltrate keychain data.

INFOSTEALER TECHNOLOGY

Malware-as-a-service technology like LummaC2 stands out because it can steal extremely sensitive data – like browser-based 2FA, remote desktop software configs, and passwords saved in vaults. These features are in addition to its ability to exfiltrate local files, steal saved credentials and cookies, and parse local cached browser data like autofills.

SPYCLOUD INSIGHT

Cybercriminals don't embrace new tools frequently, but we're seeing LummaC2 quickly gain popularity in the criminal underground. Learn more about it >

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

Get started protecting your business from ransomware today: spycloud.com/request-a-demo/