Cybersecurity 101: The Fundamentals of Cybersecurity > What is Ransomware? > How To Prevent Ransomware: 10 Pro Tips

HOW TO PREVENT RANSOMWARE: 10 PRO TIPS

Kurt Baker - October 24, 2023

Ransomware is a type of malware attack that blocks access to important files or your device until a ransom is paid. A ransomware attack is usually conducted through social engineering, such as a phishing attack, that convinces the victim to click on a malicious attachment in an email. The malicious attachment then downloads the ransomware on the device and encrypts the victim's files.

CrowdStrike has written about a number of very effective security controls and practices that you can put in place to drastically reduce your risk of a ransomware infection.

What Are 10 Pro Tips to Prevent Ransomware?

The following tips are supported by what CrowdStrike has found to successfully prevent and combat ransomware:

1. Practice Good IT Hygiene
2. Improve Resiliency of Internet Facing Applications
3. Implement and Enhance Email Security
4. InfrastructureHarden Endpoints
5. Ransomware-Proof Data with Offline Backups
6. Restrict Access to Virtualization Management Infrastructure
7. Implement zero trust architecture
8. Develop and Pressure-Test an Incident Response Plan
9. Implement a Comprehensive Cybersecurity Training Program
10. Know When to Ask for Help

1. Practice Good IT Hygiene

Minimizing the attack surface is critical for every organization — it's crucial that you gain visibility into every endpoint and workload running in your environment and then keep any vulnerable attack surfaces updated and protected.

IT hygiene's primary benefit is to give you complete network transparency. This perspective provides a bird's eye view, as well as the power to drill down and proactively clean out your environment. Once you achieve this level of transparency, the understanding of "who, what and where" that IT hygiene provides has tremendous benefits for your organization.

2. Improve Resiliency of Internet-facing Applications

CrowdStrike has observed eCrime threat actors exploiting single-factor authentication and unpatched internet-facing applications. BOSS SPIDER, one of the initial big game hunting (BGH) ransomware threat actors, routinely targeted systems with Remote Desktop Protocol (RDP) accessible from the internet. Less sophisticated threat actors operating ransomware variants such as Dharma, Phobos and GlobeImposter frequently gain access through RDP brute-force attacks.

3. Implement and Enhance Email Security

Gaining an initial foothold into a victim organization through a phishing email is the most common tactic for BGH ransomware groups. Typically, these suspicious emails contain a malicious link or URL that delivers the ransomware payload to the recipient's workstation.

CrowdStrike recommends implementing an email security solution that conducts URL filtering and also attachment sandboxing. To streamline these efforts, an automated response capability can be used to allow for retroactive quarantining of delivered emails before the user interacts with them. In addition, organizations may want to restrict users from receiving password-protected zip files, executables, javascripts or Windows insta package files unless there is a legitimate business need. Adding an "[External]" tag to emails originating from outside of the organization and a warning message on top of the email's body can help remind users to use discretion when handling such emails.

Are you ready to combat the rise of cross-domain cyberattacks?

4. Harden Endpoints

Throughout an attack lifecycle that ultimately culminates in a ransomware deployment, threat actors will often leverage a number of endpoint exploitation techniques. These exploitation techniques vary from exploiting poor AD configurations to leveraging publicly available exploits against unpatched systems or applications.

The list below includes some key system-hardening actions for defenders to implement. It is important to note this is not an exhaustive list, and system hardening should be an iterative process.

- **Ensure full coverage across all endpoints on your network for endpoint security products**, and for the endpoint detection and protection (EDR) platform. Each endpoint security platform should have strict anti-tampering protections and alerting in place if and when a sensor goes offline or gets uninstalled.
- **Develop a vulnerability and patch management program**. Doing so will ensure that all endpoint applications and operating systems are kept up-to-date. Ransomware actors leverage endpoint vulnerabilities for many purposes, including but not limited to privilege escalation and lateral movement. Existing Falcon customers can leverage CrowdStrike Falcon Spotlight™ vulnerability management for a near real-time way to understand exposure to a particular vulnerability across the environment, without the need to deploy additional agents and security tools.
- **Follow** Active Directory security best practices based on some of the most common AD downfalls observed by CrowdStrike Services during ransomware engagements.

5. Ransomware-proof Data with Offline Backups

In recent years, and since the emergence of ransomware as a top method of monetizing attacks, the developers behind malicious code have become very effective at ensuring victims and security researchers cannot decrypt affected data without paying the ransom for the decryption key. Further, when developing a ransomware-proof backup infrastructure, the most important idea to consider is that threat actors have targeted online backups before deploying ransomware to the environment.

For these reasons, the only sure way of salvaging data during a ransomware attack is through ransomware-proof backups. For example, maintaining offline backups of your data allows for a quicker recovery in emergencies. The following points should be considered when developing a ransomware-proof offline backup infrastructure:

- Offline backups, as well as the indexes (describing which volumes contain which data) should be completely separate from the rest of the infrastructure.
- Access to such networks should be controlled via strict access control lists (ACLs), and all authentications should be performed using multifactor authentication (MFA).
- Administrators with access to both offline and online infrastructures should avoid reusing account passwords and use a jump box when accessing the offline backup infrastructure.
- Cloud storage services, with strict ACLs and rules, can also serve as offline backup infrastructure.
- Emergency situations such as a ransomware attack should be the only time the offline infrastructure is allowed a connection to the live network.

6. Restrict Access to Virtualization Management Infrastructure

As mentioned earlier, threat actors engaged in big game hunting ransomware campaigns are continuously innovating to increase the effectiveness of their attacks. The most recent such development includes the ability to attack virtualized infrastructure directly. This approach allows for targeting of hypervisors that deploy and store virtual machines (VMDK). As a result, the endpoint security products installed on the virtualized machines are blind to malicious actions taken on the hypervisor.

7. Implement a Robust Zero Trust Architecture

Organizations can improve their security posture by implementing a robust zero trust architecture. By enabling a zero trust security model, users inside and outside the organization are required to be authenticated and authorized before being granted access to its network and data. As part of the architecture, you could implement an identity access management (IAM) program. This allows IT teams to control access to all systems and applications based on each user's identity.

There are various identity protection tools that help understand on-premises and cloud identity store hygiene (for example, Active Directory, Entra ID). Ascertain gaps, and analyze behavior and deviations for every workforce account (human users, privileged accounts, service accounts), detect lateral movement, and implement risk-based conditional access to detect and stop ransomware threats.

8. Develop and Pressure-test an Incident Response Plan

Organizations sometimes become aware of threat actor activity within their environment, but they lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Recognizing the threat and responding quickly and effectively can be the difference between a major incident and a near miss.

Incident response plans and playbooks help facilitate that speedy decision making. Plans should cover all parts of the response effort, across the organization. For the security team, they should provide aids to decision-making so that front-line responders don't overlook important details while triaging alerts. They should also outline the extent of the security team's authority to take decisive actions — such as shutting down business-essential services — if a ransomware attack appears imminent.

9. Implement a Comprehensive Cybersecurity Training Program

One of the key ideas behind installing a comprehensive cybersecurity training program within your organization is to protect against cyber threats like ransomware. Employees will take a proactive approach when performing routine tasks such as checking an email for a phishing attempt or using vpn when logging into the organization's network from a public wifi. The training program should also include a list of policies regarding cybersecurity and how essential it is for every stakeholder to follow them.

10. Know When to Ask for Help

In the event that you believe your organization may be impacted by ransomware, calling in experts to help investigate, understand and improve the situation can make the difference between a minor incident and a major breach. In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Getting educated about the latest threats and seeking help by activating an incident response team or retainer, such as those offered by CrowdStrike Services, may allow for detection and remediation before the threat actor is able to deploy ransomware or exfiltrate data from the environment.

It's better yet to seek out expert assistance before you truly need it. A technical assessment can help you to proactively identify and understand factors about your organization's network that could make future ransomware incidents more or less likely. It may take different forms, depending on your current needs and security maturity. For instance, if you experience an intrusion that was confined to a specific network segment or specific business unit, an enterprise-wide compromise assessment can give confidence that the attacker did not move into parts of the environment that were beyond the scope of the initial investigation. Alternatively, an IT hygiene assessment can identify weak passwords, Active Directory configurations or missed patches that could open the door to the next attacker.

Kurt Baker is the senior director of product marketing for Falcon Intelligence at CrowdStrike. He has over 25 years of experience in senior leadership positions, specializing in emerging software companies. He has expertise in cyber threat intelligence, security analytics, security management and advanced threat protection. Prior to joining CrowdStrike, Baker worked in technical roles at Tripwire and had co-founded startups in markets ranging from enterprise security solutions to mobile devices. He holds a bachelor of arts degree from the University of Washington and is now based in Boston, Massachusetts.

Featured Articles

Types of Ransomware

What Does **Ransomware Allow Hackers to** Do?

Ransomware Detection

1. IT Hygiene
2. App Resiliency
3. Email Security
4. Endpoints
5. Backups
6. VMI
7. Zero Trust
8. Incident Response
9. Training
10. Ask For Help

ur free trial now.

er been easier. Take advantage of our free 15-day trial and explore the most popular solutions for your business:

alware with next-gen antivirus.

ility with USB device control.

st threats on your mobile devices.

Request free trial →

About the Platform

Explore Products

Services

Why Choose CrowdStrike?

CrowdStrike Financial Services

Cyber Monday deals

Company

About CrowdStrike

Careers

Events

Newsroom

Partners

CrowdStrike Marketplace

Learn with CrowdStrike

2024 Global Threat Report

Cybersecurity 101

Your Threat Landscape

Tech Hub

View all resources

Contact Us →

Experienced a breach? →

Contact Us Privacy Cookies Your Privacy Choices Terms of Use Accessibility

Copyright © 2024