ADVISORY REPORT FOR SECURITY TEAMS

Top Recommendations to Prevent Ransomware

Ransomware has evolved from a low-grade nuisance to a sophisticated multimillion-dollar criminal business that now targets both individuals and corporations. It is a criminal business model that uses malicious software to cryptographically hold your personal data hostage. While an increasingly urgent challenge, ransomware can be prevented through proper training, specific adjustments to the current IT environment, and advanced endpoint technology.

What Is Ransomware?

Attackers must execute five steps for a ransomware attack to be successful:

1. **Compromise and control of the system.** Most attacks begin with spear-phishing, tricking a user with a fraudulent email to open an infected attachment that compromises the system. This may impact a single computer, mobile phone or an entire enterprise.
2. **Prevent access to the system.** Once infected, an attacker either identifies and encrypts certain files types likely to be of value to the victim, such as business documents like .doc, .xls and .pdf, or totally denies access to the entire system through lockout screens or scare tactics.
3. **Alert the owner of the device about the compromise, ransom amount, and steps to be taken.** Though seemingly obvious, attackers and victims often speak different languages and have different levels of technical capabilities, so attackers must explain to victims in terms they can understand what has happened as well as the steps to be taken to unlock their devices.
4. **Accept ransom payment.** An attacker must have a way to receive ransom payments while evading law enforcement, which explains the use of anonymous crypto-currencies, such as bitcoin for these transactions.
5. **Promise to return full access upon payment receipt.** Failure to restore compromised systems will destroy the effectiveness of the scheme, as no one pays a ransom without confidence that their valuables will be returned.

WHO'S AT RISK?

Corporations in the crosshairs. Ransomware attacks can have very public impact, as victim organization operations may be severely degraded or shut down entirely, which is illustrated by recent attacks on hospitals across the United States. Criminals have realized that this is a lucrative business with low barriers to entry. Consequently, ransomware is displacing other cybercrime business models. Moreover, attackers will grow more sophisticated in their ability to determine the value of compromised information, assess the victim organization's willingness to pay, and demand higher ransoms.

More platforms. While historically attackers focused exclusively on Microsoft® Windows® systems, the emergence of ransomware for Android™ and – as Palo Alto Networks® most recently discovered – Mac® OS X® demonstrates that no system is immune from these attacks. Nearly all computers or devices with an internet connection are potentially victims of ransomware, which will be a more urgent concern with the coming rise of the internet of things (IoT) and the proliferation of additional devices, such as wearable tech and home appliances, connected to the Internet.

PREPARE AND PREVENT

Ransomware attacks act quickly – typically within minutes of an infection – so it is critical to take action and deploy controls that either mitigate or prevent ransomware attacks. The next two sections summarize the top recommendations to do both.

TOP RECOMMENDATIONS TO MINIMIZE THE IMPACT OF RANSOMWARE

1. Develop and execute a plan for an end-user awareness program

- It can be difficult to get approval to send regular company-wide security reminders, but smarter end users will surely result in fewer ransomware incidents.

2. Review/Validate server backup processes

- Some organizations don't realize their backups are compromised, or were configured improperly, until it's too late. You may need them to restore service.
- Start with your file servers that host network shares for critical departments.

3. Review network drive permissions to minimize the impact a single user can have

End User Privilege Reviews

- Assign a project manager to organize an effort to evaluate permissions that users have on mapped network drives. Implement the principle of least privilege to minimize the impact that any single user can have on the organization's network-shared drives.
- Depending on the size of the organization, this process could be a large, complex effort, so start with network drive locations used by critical departments.

Administrator User Privilege Reviews

- Audit privileged roles used by the server, backup and network teams to validate appropriate access.
- Ensure administrators are assigned normal, restricted accounts, separate from their highly privileged accounts.
- Require administrators to use their highly privileged accounts only when they need them.
- Remove automatic network drive mappings from administrative accounts, where possible.
- Restrict administrative accounts from receiving email.

4. Document your incident response plan for ransomware

- You probably already have a generic incident response plan, but you need to be ready for ransomware, in particular, because it requires a very specific process to recover, very different from other malware incidents.
- Cases where all the files on an entire department drive are encrypted can become quite complex as multiple teams need to be engaged – backup team, file-server team, endpoint, directory team and others. The more you plan now, the quicker your response time will be.

TOP RECOMMENDATIONS TO PREVENT RANSOMWARE

1. Disable macro scripts from MS Office files using AD Group Policy

- According to Microsoft, 98 percent of Office-targeted threats use macros. Disabling macro scripts from MS Office files will stop ransomware, such as Locky.
- The entire organization may not require Office macros, but some will. Enable macros only for exceptions or certain departments.
- Office 2016 has a new feature that allows administrators to block macros from running in Word, Excel and PowerPoint documents that originate from the internet. So, if you can upgrade, do it and enable this feature.

2. Scrutinize your monthly patch management processes

- Many organizations struggle to patch their systems within 30 days of Microsoft's "Patch Tuesday" monthly patch release.
- Review your patching processes and look for opportunities to remove roadblocks.
- Consider deploying an advanced endpoint product that prevents exploits due to missing patches and malware.

3. Scrutinize your inbound spam/malware protection

- Ensure you are configured to block inbound mail as per recommendations from your email server vendor (block executables in attachments, etc.).

4. Deploy a next-generation firewall to protect the network

- Ensure your firewall automatically blocks known threats based on a threat feed that constantly updates.
- Ensure your firewall provides sandboxing capabilities so you can stop unknown threats (URLs and executables) before they reach the endpoint. Sandboxing is the best way to detect new variants of ransomware that are constantly appearing in the wild.
- Configure your firewall/proxy to require user interaction for end users communicating with websites labeled as "uncategorized" (e.g., click a "Proceed" button). Many uncategorized websites are used in targeted phishing campaigns to distribute malware. This two-step process prevents certain types of ransomware from making that external call to the command and control server. If that doesn't happen, your files may not be encrypted.

5. Deploy advanced endpoint protection to protect the endpoint

- Traditional antivirus is not effective against advanced malware, like ransomware, which continuously changes to avoid detection. Ensure that your endpoint protection measures can detect and prevent known and unknown malware, as well as known and unknown exploits, including zero-days.
- Whitelisting may work for some simple, smaller organizations; but, for growing organizations with a lot of applications and complexity, it can quickly require a lot of work to manage the list. Technique-based malware detection is very effective at detecting ransomware.
- Ensure your endpoint protection systems are armed with real-time threat intelligence gained from internal and external sources that cross organizational boundaries, geographies and industries.

LOOKING FOR MORE INFORMATION?

Ransomware: paloaltonetworks.com/solutions/initiatives/ransomware
TRAPS: paloaltonetworks.com/products/secure-the-endpoint/traps
NGFW: paloaltonetworks.com/products/secure-the-network/next-generation-firewall