LEAP SECURITY

Defending Against Ransomware and Zero Days

May 2017

01 Background

Overview

The Information Security industry has recently experienced a surge of ransomware and zero day releases. The latest ransomware to hit the news, "Wannacry" has affected over 200,000[1] systems on a global scale. Combine this with the frequent releases of zero day exploits and we now have a serious threat to both organizations and consumers alike.

Although there are other documents providing guidelines on how to protect against ransomware or zero days we could not find one that did both while providing a good understanding of the associated threats. This document aims to fix that by providing best practices and breaking down each of the associated threats.

What is Ransomware?

Ransomware is a variation of malware with an intent to damage or disable computers. Ransomware specifically, aims to disable computers by encrypting or locking users to prevent their use. If encrypted, a computer generally displays an image and can no longer be used due to the file system being encrypted. The only way to decrypt the content is to pay the "ransom".

The rise of ransomware can be accredited to the success and profits cyber criminals are having from paid ransoms. Leap Security does not advise paying any ransoms or money to cyber criminals.

What are Zero Day Vulnerabilities and Exploits?

Zero day vulnerabilities are vulnerabilities that are unknown to software developers. Similarly, zero day exploits are exploits to the vulnerabilities that are unknown and unpatched by software developers. Zero day exploits are one of the biggest threats in cyber security.

[1] Cnet, *Unprecedented WannaCry attack a nightmarish 'wake-up call'*, https://www.cnet.com/news/wannacry-unprecedented-ransomware-attack-a-nightmarish-wakeup-call/

02 Defending Against the Threats

Best Practices

Make it difficult for attackers to obtain a foothold in your network environments. Create a plan to protect, prevent, and respond. The plan should focus on protecting technological assets, preventing threats and responding to incidents. Although this might sound like common sense, only 52%[2] of organizations agree there is a need to be prepared for a breach.

Overall, the plan and practices applied should cover the deployment of regularly revised and updated firewalls, backups, patch management, network/host based protection, log monitoring, backups, incident response and user security awareness training.

Firewall Configurations

Revise firewall configuration files in an effort to reduce services exposed on the perimeter network. With strict filtering rules, an organization may significantly reduce their attack surface which in turn reduces the chances of being hit with an exploit (including zero days).

Administrative services are services that should never be exposed on the perimeter network. Examples of these are Microsoft's Remote Desktop Protocol ("RDP"), Secure Shell ("SSH"), File Transfer Protocol ("FTP"/"SFTP"), Telnet. Administrative services should only be accessible once users have authenticated through a two factor Virtual Private Network ("VPN") solution. In addition, revise email gateway configurations to ensure the blocking of executables and scripting file extensions (e.g., ps1, bat, vbs).

Patch Management

Create a patch management plan to test patches in a safe network environment prior to applying them on production systems. Test and apply patches frequently especially if they patch a vulnerability with a public exploit. Prioritize the patching of vulnerabilities with publicly available exploits, browser related, and vulnerabilities for services that are exposed on the perimeter.

User Security Awareness Training

In late 2016, 97%[3] of phishing emails sent contained a form of ransomware. Organizations can significantly reduce their chances of infection with a combination of security controls and frequent user security awareness training. User security awareness training should cover the dangers associated with phishing attacks and opening attachments from unknown senders as well as detailing alerting and preventative procedures.

---

[2] Kapersky, *Business Perception Of It Security: In The Face Of An Inevitable Compromise*, https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky%20Lab%20Report_IT%20Security%20Perception_Global_final.pdf

[3] Phishme, *Ransomware Delivered by 97% of Phishing Emails by end of Q3 2016 Supporting Booming Cybercrime Industry,* https://phishme.com/ransomware-delivered-97-phishing-emails-end-q3-2016-supporting-booming-cybercrime-industry/

Network and Host Based Protection

If a threat does manage to affect systems or network environments the next layer of defense would be network and host based protection systems followed by an alerting mechanism (i.e., log monitoring). Ensure your organization has implemented modern network and host based Intrusion Prevention Systems ("IPS") and Antivirus with behavior monitoring. Unlike signature based solutions, modern behavior based protection solutions analyze a threat in real time and prevent it from running even if the solution has no record of it. It helps stops zero day exploits and ransomware.

Logs and Monitoring

The proper implementation and configuration of a log monitoring solution may significantly help in case of an incident. Many times log monitoring can help prevent threats by alerting administrators of network anomalies. Recognizing abnormal behavior can help incident response teams triangulate the threat and perform triage in a timely manner.

Backup and Incident Response Strategies

Ensure your organization is regularly performing backups and storing a copy at an off-site location. With the proper backup plans and procedure an organization would never need to pay a ransom to malware developers. Simply wipe the system affected and restore an earlier backup.

In addition, it is important to have an incident response plan in case of a breach. The plan should detail how to perform triage and control the breach from further spreading on the network. Employees should understand the first step in an incident is to call the Incident Response team as any action on a computer (such as powering a system down) after infection may hamper the digital forensics process.

04 Conclusion

A professor once said "one year in technology is equivalent to ten years in any other profession." Cyber security is an ever changing field and it is important to constantly revise our network configurations to ensure protection against the new emerging threats.

That concludes our article, we hope you learned something new or were reminded of some practices your organization still needs to implement. Feel free to reach out and contact us with any questions or comments at info@leapsecurity.com. We are always available to chat about your projects or answer any questions you may have. Stay secure! Leapsec, over and out.