SIRIUS COMPUTER SOLUTIONS

Ransomware

Alan Salesman, CISSP,CCSP,CBCP,

Agenda

What is Ransomware

Ransomware Statistics

Recent High Profile Ransomware

Ransomware Process

Locky

Security Weaknesses

What is Ransomware

Ransomware is malicious software that criminals use to encrypt files and hold valuable data for ransom

Ransomware is dominating the malware market. Although it is not a new threat, it has evolved to become the most profitable malware type in history. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent.[1]

1 Source Cisco midyear Security Report- 2016

Ransomware statistics by Industry

In 2014-2015, around 27,000 corporate users were attacked.

But in 2015-2016, the figure rose six-fold to more than 158,000.

The root cause is obvious: organizations are more likely to pay higher ransoms, because they are less likely to be able to weather a complete loss of their systems.

Recent high profile Ransomware attacks

Hollywood Presbyterian Hospital – Using phishing to trick an unsuspecting employee, attackers seized the hospital's entire IT system, stalled critical healthcare related communications and extorted $17,000 in ransom. [1]

Plainfield, New Jersey – Using phishing emails targeted at employees researching grants, hackers compromised three servers before city officials were able to pull them offline, effectively locking up the town's files in order to receive a small sum until the officials turned to law enforcement for help.[1]

This year, a South Carolina school district paid USD 10,000 in Bitcoin to regain access to their servers after they were infected with ransomware. Meanwhile, an exemplary school district in New Jersey declined to pay their cyber extortionists after becoming infected with ransomware, as they were able to restore their servers from backups. The two cases illustrate the criticality of maintaining secure, offline backups.[2]

1 phishme.com

2 https://www.controlrisks.com/en/services/security-risk/cyber-security-services/the-ransomware-industrys-rapid-evolution#fn4

Ransomware Attack Phases

1. Exploitation – Malicious file needs to be executed on victims computer (phishing email or exploit kit such as Angler used for CryptoLocker malware

2. Delivery/Execution/Infection – the ransomware executable files are delivered to victims system and if executed, malware and other mechanisms will be put in place

3. Backup spoliation - Immediately the ransomware targets the backups and or folders on the victims system and removes them to prevent restoring from backup including Windows shadow copies

4. File Encryption – Once backups are completely removed, malware will perform a secure key exchange with the criminal orgs C2 server, establishing the encryption keys that will be used on the local system

5. User (Victim) notification and cleanup – With backup files removed and the encryption dirty work done, the demand instructions for extortion and payment are presented.

Source " Log Rhythm How Ransomware Works”

LOCKY Wallpaper

"Locky" sets your wallpaper to make sure you know what to do next

image source: https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

Locky Decrypter

Security Weaknesses

- Updates/patches not regularly implemented in a timely manner
- Poor backup strategy; backups not offline and off-site
- Poor or limited Security Awareness and security training
- Unnecessary elevated access rights – users utilizing admin rights
- Signature based antivirus limited ability to protect against zero day attacks
- Access to network shares
- Poor or non existent BCP/DR and or IR capabilities
- Using security technology and practices that may be years behind current offerings and practices
- SSL/TLS decrypting and inspecting that traffic for security purposes

Backups

The only options for recovering data after a ransomware infection are to restore it from backup files, or to pay the ransom.

However, paying the ransom is no guarantee that the malware will be eradicated, or that it won't return.

Further, it is not possible to decrypt without the keys, and it is extremely unlikely to recover the keys via law enforcement action including the FBI.

Disaster Recovery

Organizations must have effective and tested disaster recovery plans with verified off-line backups.

Our team has seen several new variants in the wild that target and destroy an organization's backup infrastructure – by obtaining weak or default passwords.

Having a Plan

Having a plan to detect, respond and contain an incident saves valuable time during an incident.

Consider investing in endpoint detection and response tools, as well as log correlation to spot ransomware quickly, help you understand where it is coming from, and assist in containment.

Zero-Day Detection Capabilities

Antivirus alone cannot always detect the types of behaviors that signal a ransomware attack, new variants are constantly released, to a point that antivirus teams can't keep up.

Signature based technologies are less effective in detecting a majority of malware today due to the ease in which a given piece of malware can be camouflaged or "packed" to slip past traditional AV.

- Ensure your network and endpoint protection have the ability to detect and defend against obfuscated malware or zero-day attacks.
- Consider implementing network devices that can block by file type and provide application control to the endpoint device.

True-up User Access Permissions

Reduce data attack surface exposed to ransomware by strictly governing what users have access to.

Administrators should never use their admin accounts for day-to-day business such as email, because mapped drives are an easy and fast vector for the malware to encrypt file server data.

Several excellent tools are available to help organizations quickly detect anomalous user file access and change behavior.

Vulnerability and Patch Management:

Regularly conduct internal and external vulnerability scans, then mitigate.

Vulnerability and patch management isn't fun for anyone, but it is the foundation of a good security program for all threats – including ransomware.

Web applications with OWASP top 10 vulnerabilities

IT leadership need to address the balance of regular vulnerability and patch management inconsistencies based on organizational operational tempo

Block Unnecessary File Types and Show Full File Extensions:

- Tune your mail protection to block unnecessary file types. Block all unnecessary file types over email including “.exe” if possible.
- Ransomware often arrives as .pdf.exe. Enabling visibility of full file extensions makes suspicious files easier to spot.

Alert on Anomalous User Behavior:

By setting up notifications to alert you about an abnormal user or system behavior, organizations may detect an outbreak early – when it's easier to contain.

Understanding abnormal system or user behavior – particularly file encryption – can tip you off to ransomware and allow you to thwart the attack.

User behavior analytics is a powerful tool for many threats including ransomware.

Closing Thoughts

Do you know where you are from a security posture?

Where is your critical data is located?

How and where does your data flow in and out of the organization?

What are your patch levels?

Risk Assessment (Vulnerability Scans (Internal/External)

Web Application vulnerability assessment

Validate backup and restore

Network Security Architecture review

Next Gen Security tools

Security Awareness and Security training

THANK YOU

www.siriuscom.com