Solution Brief

Protect health care systems against ransomware

Ransomware is malware that generally employs asymmetric encryption to hold a victim's information hostage. Asymmetric (public-private) encryption is cryptography that uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server. The attacker makes the private key available to the victim only after the ransom is paid, though that is not always the case—as seen in recent ransomware campaigns. Without access to the private key, it is nearly impossible to decrypt files that are being held for ransom.

Ransomware has been at the top of every security professional's mind for the last few years. Unfortunately, ransomware is a simple, effective cyberattack tool used for easy monetary gain. During the past year, we have seen a shift in targets from individuals to businesses because the latter will pay higher ransoms. Recently, hospitals have become a very popular target of ransomware authors. In the *McAfee Labs Threats Report: September 2016*, we analyzed Q1/Q2 2016 ransomware attacks on hospitals and discovered that they were successful, related, and targeted attacks though relatively unsophisticated. We also discussed the hospital-specific challenges concerning ransomware, including legacy systems and medical devices with weak security, plus the life and death need for immediate access to information.

Policies and procedures to protect against ransomware

The most important step to protect systems from ransomware is to be aware of the problem and the ways in which it spreads. Here are a number of policies and procedures hospitals should follow to minimize the success of ransomware attacks:

- Have a plan of action in the event of an attack. Know where critical data is located and understand if there is a method to infiltrate it. Perform business continuity and disaster recovery drills with the hospital emergency management team to validate recovery point and time objectives. These exercises can uncover hidden impacts to hospital operations that otherwise do not surface during normal backup testing. Most hospitals paid the ransom because they had no contingency plans!

intel Security

- Keep system patches up to date. Many vulnerabilities commonly abused by ransomware can be patched. Keep up to date with patches to operating systems, Java, Adobe Reader, Flash, and applications. Have a patching procedure in place and verify if the patches have been applied successfully.
- For legacy hospital systems and medical devices that cannot be patched, mitigate the risk by leveraging application whitelisting, which locks down systems and prevents unapproved program execution. Segment these systems and devices from other parts of the network using a firewall or intrusion prevention system. Disable unnecessary services or ports on these systems to reduce exposure to possible entry points of infection.
- Protect endpoints. Use endpoint protection and its advanced features. In many cases, the client is installed with only default features enabled. By implementing some advanced features—for example, "block executable from being run from Temp folder"—more malware can be detected and blocked.
- If possible, prevent the storage of sensitive data on local disks. Require users to store data on secure network drives. This will limit downtime because infected systems can simply be reimaged.
- Employ antispam. Most ransomware campaigns start with a phishing email that contains a link or a certain type of attachment. In phishing campaigns that pack the ransomware in a .scr file or some other uncommon file format, it is easy to set up a spam rule to block these attachments. If .zip files are allowed to pass, scan at least two levels into the .zip file for possible malicious content.
- Block unwanted or unneeded programs and traffic. If there is no need for Tor, block the application and its traffic on the network. Blocking Tor will often stop the ransomware from getting its public RSA key from the control server, thereby blocking the ransomware encryption process.
- Add network segmentation for critical devices required for patient care.
- "Air gap" backups. Ensure backup systems, storage, and tapes are in a location not generally accessible by systems in production networks. If payloads from ransomware attacks spread laterally they could potentially affect backed-up data.
- Leverage a virtual infrastructure for critical electronic medical records systems that are air gapped from the rest of the production network.
- Perform ongoing user-awareness education. Because most ransomware attacks begin with phishing emails, user awareness is critically important. For every 10 emails sent by attackers, statistics have shown that at least one will be successful. Do not open emails or attachments from unverified or unknown senders.

How Intel Security technology can help protect against ransomware

McAfee VirusScan Enterprise and McAfee Endpoint Security 10

- With McAfee VirusScan Enterprise (VSE) or McAfee Endpoint Security (ENS), implement the following:
  - Use McAfee ePolicy Orchestrator (ePO) daily to deploy updated DATs.
  - Ensure McAfee Global Threat Intelligence (McAfee GTI) is enabled; McAfee GTI contains more than 7 million unique ransomware signatures.
  - Develop Access Protection rules to stop installation and payloads of ransomware; refer to Access Protection Rules Knowledge Base Articles KB81095 and KB54812.
  - Use Dynamic Application Containment to prevent unknown applications from performing malicious activities.

McAfee Threat Intelligence Exchange

- With McAfee Threat Intelligence Exchange (TIE) set up the following policies:
  - Start with observation mode.
  - As endpoints are discovered with suspected processes, use system tags to apply TIE enforcement policies.
  - Clean at Reputation: known malicious.
  - Block at Reputation: most likely malicious (blocking at unknown would provide better protection but may also add to initial administrative workload).
  - Submit files to McAfee Advanced Threat Defense (ATD) at a reputation level of unknown and below.
  - TIE Server policy: Accept ATD reputations for files not yet seen by TIE.
- McAfee Threat Intelligence Exchange Manual Intervention:
  - File reputation enforcement (subject to operation mode).
  - Most likely malicious: Clean/delete.
  - Might be malicious: Block.
  - Enterprise (organizational) reputation can override McAfee GTI. You can choose to block an undesired process, for example, an unsupported or vulnerable application. Mark file as Might be malicious.
  - Feed third-party reputation data into TIE via indicators of compromise.

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense has the following in-box detection capabilities:
  - Signature-based detection: Signatures maintained by McAfee Labs include more than 150 million signatures including CTB-Locker, CryptoWall, and its variants.
  - Reputation-based detection: McAfee GTI.
  - Real-time static analysis and emulation: Used for signatureless detection.
  - Custom YARA rules.
  - Full static-code analysis: Reverse engineers file code to assess attributes and function sets and fully analyze source code without execution.
  - Dynamic sandbox analysis.
- Create analyzer profiles where ransomware is likely to run:
  - Common OS, Windows 7, Windows 8, XP.
  - Install Windows applications (Word, Excel) and enable macros.

- Provide unique Analyzer Profiles for separate operating systems with Internet access:
  - Many samples run a script from a Microsoft Office document that makes an outbound connection and activates the malware. Providing an Analyzer Profile with an Internet connection increases detection rates.

McAfee Application Control

- McAfee Application Control provides protection with application whitelisting. It is ideal to protect all types of devices, especially:
  - Static devices such as medical appliances.
  - Systems with legacy operating systems that are no longer receiving updates.
  - Application servers that provide a limited number of services.
  - Systems that are infrequently changed.
- Initial installation
  - McAfee Application Control will completely scan a system during installation and create the endpoint inventory and applications to whitelist.
- Observation mode
  - Allows administrators to track new apps installed/launched, with an option to merge them into the centralized whitelist if the application is determined to be authorized.
  - Assists the whitelisting procedure by identifying new trusted updaters for applications within the environment.
  - Identifies methods to update the whitelist such as approved processes, certificates, directories, or users.
- Self-approval mode
  - Users will be able to approve nonwhitelisted applications. This allows for flexibility and minimal business impact.
  - Administrators will be able to centrally track user-approved content and accept or revoke the authorization of the application based on reputation and the organization's policies.
- Enforce whitelist
  - The system is completely protected from unknown applications, including malicious applications such as ransomware.
  - Provides an End User Notification for the procedure to approve new executables.

Further reading

Intel Security Expert Center Community

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com