Solution Brief

Defeat Ransomware: Ensure Your Data Is Not Taken Hostage

Ransomware is malware that employs asymmetric encryption to hold a victim's information at ransom. Asymmetric (public-private) encryption is cryptography in which a pair of keys is used 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 next to impossible to decrypt the files that are being held for ransom.

A look into ransomware

For an in-depth technical look into ransomware, please refer to the ***McAfee Labs Threats Report: May 2015***. In the *McAfee Labs Threats Report: November 2014*, we predicted nine major threats that would occur in 2015. Regarding ransomware, McAfee Labs said "Ransomware will evolve its methods of propagation, encryption, and the targets it seeks." Almost immediately there was a huge spike in the prevalence of ransomware, as well as the appearance of new families such as Teslacrypt, and further changes to current families such as CTB-Locker, CryptoWall, and TorrentLocker.

Most ransomware campaigns begin with a phishing attack. Over time, they have become more sophisticated, many now specifically and meticulously crafted to the locale of victims that are being targeted.

New technologies have also been adapted to make ransomware more powerful:

- **Virtual currency:** By using **virtual currency** as the method to pay ransoms, attackers are not exposed to traditional banking and the possibility that money transfers can be traced.
- **Tor network:** By using the **Tor network**, attackers can more easily hide the location of their control servers, which store the victims' private keys. Tor makes it possible to maintain the criminal infrastructure for a long time and to even rent the infrastructure to other attackers so they can run affiliate campaigns.
- **Moving to mobile:** In June 2014, researchers discovered the first ransomware family to encrypt data on Android devices.[1] Pletor uses AES encryption, locks the data on the phone's memory card, and uses Tor, SMS, or HTTP to connect to the attackers.

intel Security

- **Targeting mass-storage devices:** In August 2014, Synolocker began targeting network-attached storage (NAS) disk and rack stations from Synology.[2] The malware exploits a vulnerability in unpatched versions of the NAS servers to remotely encrypt all data on the servers using both RSA 2,048-bit keys or 256-bit keys.

Safeguarding against ransomware

Here are some good practices and policies to better protect yourself and your organization against the threat of ransomware.

- **Perform ongoing user-awareness education:** Because most ransomware attacks begin with phishing emails, user awareness is critically important and necessary. For every ten 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.
- **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 that the patches were applied successfully.
- **Use great caution when opening attachments:** Configure antivirus software to automatically scan all email and instant-message attachments. Make sure email programs do not automatically open attachments or automatically render graphics, and ensure that the preview pane is turned off. Never open unsolicited emails, or unexpected attachments—even from known people.
- **Beware of spam-based phishing schemes:** Do not click on links in emails or instant messages.

How Intel Security can help protect against ransomware

McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in trusted websites are just some of the attack methods used to deliver ransomware. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway anti-malware engine:** Signatureless intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protect against zero-day and targeted attacks. The gateway anti-malware engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee Global Threat Intelligence (McAfee GTI):** Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection solution that combines multiple inspection engines that apply signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing. McAfee Advanced Threat Defense will protect against prevalent ransomware such as CTB-Locker, CryptoWall, and others.

- **Signature-based detection:** Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledge base is created and maintained by McAfee Labs, and currently includes more than 150 million signatures including CTB-Locker, CryptoWall, and its variants.

- **Reputation-based detection:** Looks up the reputation of files using the McAfee GTI service to detect newly emerging threats.
- **Real-time static analysis and emulation:** Provides real-time static analysis and emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.
- **Full static-code analysis:** Reverse-engineers file code to assess all its attributes and instruction sets, and fully analyze source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by the specific malware.
- **Dynamic sandbox analysis:** Executes file code in a virtual runtime environment and observes the resulting behavior. Virtual environments can be configured to match your company's host environments, and supports custom OS images of Windows 7 (32- or 64-bit), Windows XP, Windows Server 2003, Windows Server 2008 (64-bit), and Android.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt to suit your environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks, thanks to its visibility into immediate threats such as unknown files or applications being executed in the environment. Blocking unknown or new executables ensures proactive protection against ransomware.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation:** McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process' actions from installation to the present enables faster response and remediation.
- **Indicators of compromise (IoCs):** Import known bad files hashes and McAfee Threat Intelligence Exchange can immunize your environment against these known bad files through policy enforcement. If any of the IoCs trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the IoC.

McAfee VirusScan Enterprise

Detecting and protecting against ransomware is simple with **McAfee VirusScan® Enterprise**. McAfee VirusScan Enterprise uses the award-winning McAfee scanning engine to protect files from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks:** Integrates anti-malware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in applications.

- **Unbeatable malware detection and cleaning:** Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques including port blocking, filename blocking, folder/directory lockdown, file-share lockdown, and infection tracing and blocking.
- **Real-time security with McAfee GTI integration:** Protects against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in the market.

McAfee Network Security Platform

McAfee Network Security Platform is designed to perform deep inspections of network traffic. McAfee Network Security Platform combines advanced inspection techniques—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent attacks such as ransomware attempting to communicate via network protocols such as Tor, IRC, and others.

- **Comprehensive malware defense:** Combines file reputation from McAfee GTI, deep file analysis with JavaScript inspection, and signatureless, advanced malware analysis to detect and defeat zero-day threats, custom malware, and other stealthy attacks.
- **Leverages advanced inspection techniques:** Includes full protocol analysis, threat reputation, and behavior analysis to detect and prevent both known and zero-day attacks on the network.
- **Integration with McAfee GTI:** Combines real-time file reputation, IP reputation, and geolocation feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.
- **Security Connected:** Actionable integration with McAfee Advanced Threat Defense enables McAfee Network Security Platform to submit suspect files found in monitored traffic to McAfee Advanced Threat Defense, and deny or allow them based on findings from McAfee Advanced Threat Defense.

In addition to these Intel Security products, we recommend one additional class of security technology.

- **Email gateway security:** Most ransomware enters a system through an attachment to an email message, so a robust email gateway security product that scans all attachments for malware should be part of a good defense against this type of attack.

Ensuring your organization's precious data is not ripe for the taking is a daunting task, especially with the steady rise of ransomware as an attack vector. Intel Security technology can help your company proactively protect itself against threats such as ransomware both on the endpoint and network.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

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