DEFENSES AGAINST RANSOMWARE:

EFFECTIVE SOLUTIONS TO PROTECT YOUR CRITICAL DATA

THE GROWING RANSOMWARE THREAT

Ransomware is a common method of cyber extortion for financial gain. It's a type of attack that instantly prevents users from interacting with their files, applications or systems until the victim pays the ransom and the attacker restores access with a decryption key. Ransomware activities targeting large and small organizations have been rising steadily since mid-2015.[1] Attackers often target essential and highly sensitive information from a wide range of data-centric businesses and verticals including health care, law firms and energy organizations. And they tend to focus on small to midsize enterprises because those victims have limited security budgets and expertise.

More and more frequently, ransomware is being delivered by sophisticated persistent cyber attacks. Organizations face increasing challenges and cost to defend against ransomware attacks. Health care entities are now required to apply the HIPAA (Health Insurance Portability and Accountability Act) requirements related to security, privacy and breach notification in responding to ransomware attacks.[2] To defend against these attacks and the ransomware itself, organizations need a combination of technology and robust threat intelligence.

Traditional security solutions, including anti-virus software, next-generation firewalls, secure email and web gateways and intrusion preventions systems rely on static analysis and signatures to detect and block known threats. An attacker can test those defenses and adjust their tactics to bypass them.

Traditional pattern-matching and signature-based defenses cannot:

- Update fast enough to keep pace with evolving attacks
- Optimize and automate operations to detect unknown, never-before-seen threats in real time
- Detect custom and encrypted communication between an external command-and-control server (CnC) and infected host
- Protect against multi-stage web- or email-based ransomware attacks

[1] Hummel, Richard, et al. (May 18, 2016). "Ransomware Activity Spikes in March, Steadily Increasing Throughout 2016."
[2] Samuels, Jocelyn (July 11, 2016). "Your Money or Your PHI: New Guidance on Ransomware."

FireEye

Ransomware via web and email

Web-based ransomware attacks tend to use "drive-by-download" exploit kits that take advantage of browser, application and system vulnerabilities in a multi-stage process:

- **Stage 1** – Infect a legitimate website or hacks an advertising network to insert code.
- **Stage 2** – Profile the user system and redirect them to another web page with an exploit kit that detects vulnerable software such as older versions of Java or Flash on their computer.
- **Stage 3** – Deliver an encrypted, obfuscated or encoded malicious payload to the user's system. Ransomware takes effect once the payload is decrypted.
- **Stage 4** – Establish a connection to a callback server so the attacker can set up the unique keys to encrypt the victim's data.

Traditional sandboxes cannot see through the encryption in Stage 3 and therefore cannot analyze increasingly common, sophisticated multi-flow attacks.

Most reported ransomware infections are introduced via email attachments or embedded links. According to a report by the Cyber Threat Alliance (CTA), CryptoWall 3.0, which caused US $325 million in damage worldwide, was distributed through phishing attacks via email (67.3%) and exploit kits (30.7%).[3] Attackers often target key personnel and high-value computers with spear phishing to maximize their gains. They get the user to execute the file or click on the link through social engineering techniques.

Successful approaches to defend against ransomware

Ransomware often uses web and email vectors to reach victim systems. You should set up and tighten security controls to monitor email, IPS, network and endpoints to detect behavior that can indicate ransomware activity. Many commonsense measures are still recommended as part of a complete security solution. For network security, these include appropriate network segmentation, access controls and regular backups, preferably offsite. For email security, include basic spam and antivirus filters. For endpoint security, implement effective endpoint visibility that can help detect threats, enable analysts to determine the nature of a threat and take action. You should also educate employees about the latest ransomware campaigns and how to avoid them.

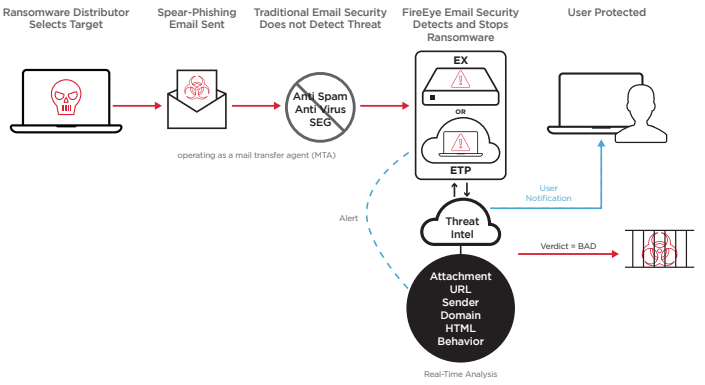
But because cyber criminals are continually improving their tools and tactics, security solutions must provide real-time protection to prevent or interfere with the activation of ransomware. This includes inline protection along with actionable threat intelligence that's updated as quickly as possible and continually looks for threats across all critical attack vectors.

Every component of the FireEye solution, the first to be certified by the U.S. Department of Homeland Security Safety Act, is a step toward stronger cyber security. Combining the following elements contributes to the strongest possible defense against ransomware.

FireEye Email Security

Offline and cloud-based analysis are often too slow to stop ransomware from encrypting your systems and data. FireEye Email Security deployed inline, either on premise (EX) or cloud based (ETP), operates as a mail transfer agent (MTA) and quarantines, analyzes and blocks ransomware emails before they reach the recipient (Fig. 1). Enhanced email security with a store and forward architecture and near-real time speed effectively stops many attacks before they occur with minimal business lag.

FIGURE 1. FIREEYE EMAIL SECURITY DETECTS AND PREVENTS EMAIL-BASED RANSOMWARE ATTACKS.

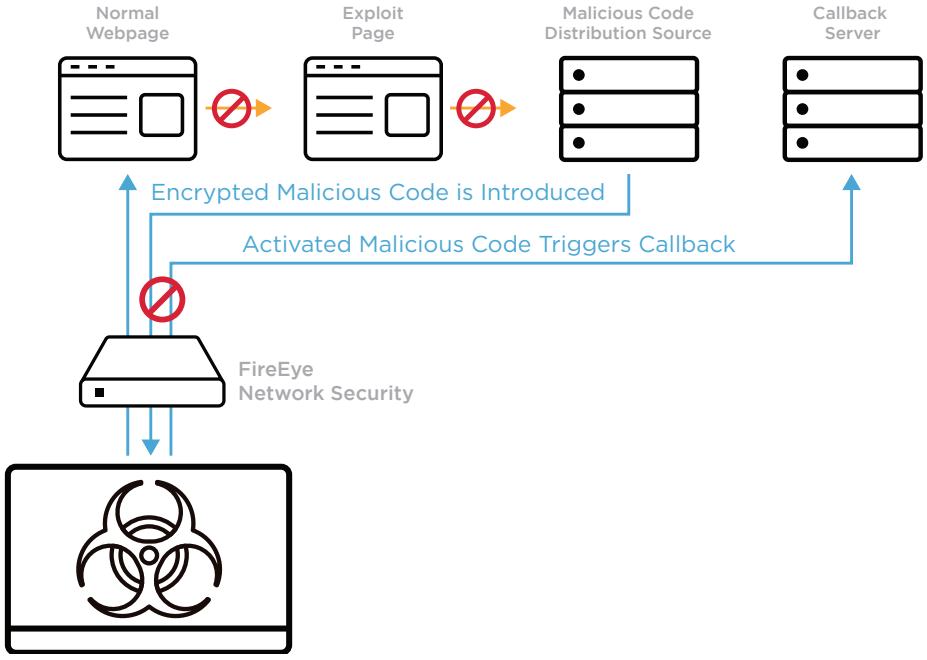


[3] Cyber Threat Alliance (October 2015). Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat.

FireEye Network Security

Ransomware intrusion involves three main stages: initial infection, file encryption and command-and-control (CnC) server access. FireEye Network Security identifies the attack process and detects and blocks communication between the servers that deliver encrypted malicious code to the victim and for callback (Fig. 2).

FIGURE 2. FIREEYE NETWORK SECURITY DETECTS AND PREVENTS WEB-BASED RANSOMWARE ATTACKS.



FireEye Network Security is not a sandbox solution. Sandboxes fail to detect multi-stage attack flows because they only analyze files in isolation. The FireEye Multi-Vector Virtual Execution™ (MVX) engine at the heart of FireEye Network Security can readily analyze traffic and detect attacks that span multiple phases, including those with encrypted malware that evade typical sandbox solutions.

FireEye Endpoint Security

Endpoints and their users are the starting point for ransomware attacks. An attack often uses hard-to-detect discreet processes that exploit a vulnerability in a common application. FireEye Endpoint Security detects and analyzes these processes to determine if an exploit is taking place, giving analysts the information needed to stop an incident. And it provides needed visibility into endpoints so analysts can conduct detailed investigations to curtail damage and adapt the defense against further attack.

FireEye stops Cerber ransomware

FireEye Endpoint Security detected a new Cerber ransomware campaign on Friday, June 10, 2016. The attack campaign was set up to send an email with a malicious Microsoft Word document with a macro. If a target opened the document the malicious macro would contact an external command-and-control (CnC) server and download the dangerous Cerber ransomware. Victims were instructed to pay a ransom of about US $1,400 for a key to decrypt their files. Using Endpoint Security, FireEye was the first to detect, investigate and stop this infection and worked with security agencies such as the United States Computer Emergency Readiness Team (US-CERT) and web hosting providers to shut down the CnC server.

FireEye Threat Intelligence

FireEye continually monitors malware trends and ransomware campaigns. Researchers dissect ransomware families and analyze their behaviors. This knowledge is codified into FireEye Dynamic Threat Intelligence (DTI) and pushed to the MVX engine, enabling customer appliances to detect existing, evolving and new ransomware techniques.

FireEye iSIGHT threat Intelligence provides actionable tactical, operational and strategic intelligence that helps organizations better manage their risk and response to ransomware and other current threats. This threat intelligence is derived from attackers' development environments, from a strong understanding of attacker tools, tactics and procedures (TTPs) and from hundreds of incident response engagements. These continually updated, shared, context-rich sources of insight create an industry-leading intelligence network that helps security teams predict, detect and respond to ransomware attacks.

Conclusion

Advanced detection and prevention supported by actionable threat intelligence is the best defense against ransomware and other advanced attacks. The FireEye solution defends against the growing and ever-changing ransomware threat. It provides real-time, inline protection for multiple attack vectors to prevent or interfere with the activation of ransomware and protect you from financial loss and business disruption.

For more information about how to combat ransomware visit:
https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye