EFFECTIVE RANSOMWARE RESPONSES

UNDERSTANDING RANSOMWARE AND HOW TO SUCCESSFULLY COMBAT IT

WHITE PAPER

FireEye

CONTENTS

PREFACE

The M-Trends 2016 Annual Threat Report[1] indicates that Mandiant investigators responded more often to clients dealing with digital blackmail schemes. Most cases cited impacts to either the confidentiality or availability of data. Targeted organizations were threatened with the public release of sensitive data while targets of opportunity were typically infected with commodity ransomware such as TorrentLocker or CryptoWall. In a particularly high-profile case, the Hollywood Presbyterian Medical Center in Los Angeles was attacked on February 5, 2016.[2] This hospital lost access to electronic patient records and email, and its business operations and administrative functions were significantly affected, causing the hospital to reportedly pay a ransom equivalent to approximately $17,000.

Ransomware operators have infected victims worldwide using their native languages. This type of malware has primarily affected Windows operating systems, but in recent years, ransomware has been developed to affect other operating systems, such as Android (Simplocker)[3] and Mac OS X (KeRanger).[4] Organizations have a pressing reason to exercise caution against ransomware due to its expanding and widespread distribution and popularity[5] among malicious actors.

1 Mandiant, a FireEye company. "M-Trends 2016." February 2016
2 Los Angeles Times. "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." February 18, 2016
3 WeLiveSecurity.com. "ESET Analyzes Simplocker – First Android File-Encrypting, TOR-enabled Ransomware." June 4, 2014.
4 WeLiveSecurity.com. "New Mac ransomware appears: KeRanger, spread via Transmission app." March 7, 2016.
5 PCMag.com. "The Growing Threat of Ransomware." April 13, 2016.

The impact of ransomware is immediate, compared to stealthier malware used in advanced attacks.

About Ransomware

Ransomware is a type of malware that renders the victim's computer or specific files unusable or unreadable, and demands a ransom from the victim in return for a cryptographic key which can be used to restore the computer or decrypt the encrypted files.

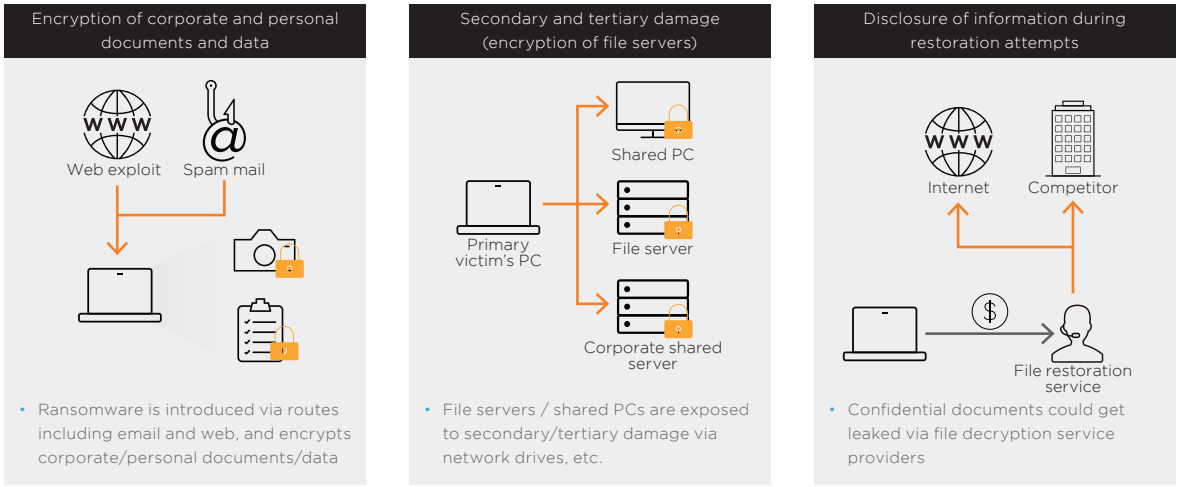
Once it infects a target system, modern ransomware encrypts a targeted group of critical files, making them unavailable to the user. It then displays instructions for payment required to restore access to the files. Online virtual currencies such as PayPal and Bitcoin are preferred methods of payment because they are not easily traceable.

The impact of ransomware is immediate, compared to stealthier malware such as those used in an advanced threat attacks. There is growing concern about the complex effects of ransomware on organizations, which include monetary damage and business downtime.

Damage by Ransomware

There are three main types of damage caused by ransomware.

FIGURE 1. TYPES OF DAMAGE CAUSED BY RANSOMWARE.



Encryption of corporate and personal documents and data

Ransomware encrypts important documents and data on a system to render them inaccessible to an organization or individual. Since the encrypted files cannot be restored with off-the-shelf security solutions, the victim must either pay the ransom to the attacker or use pre-existing backups to restore the files. In limited cases, flaws in ransomware encryption implementation can also be identified and used to recover data. However, many popular ransomware families only encrypt files after receiving a response or public RSA key from the attacker's command and control server. This trend means that blocking control server traffic may prevent encryption.

In many cases, complete recovery is nearly impossible without the attacker's decryption key. Once a computer gets infected with ransomware, damage is almost always instantaneous and unavoidable because data on that computer is, at least temporarily, unusable.

Secondary and tertiary damage

Ransomware can cause secondary or tertiary damage through equipment such as file servers or network share devices. If the initial victim's computer is connected to such devices, the ransomware will often encrypt the entire shared resource.

In ransomware campaigns malicious actors can spread ransomware to new victims within infected organizations. Popular tools used to download ransomware also steal email credentials, and attackers use compromised email accounts to further distribute ransomware.

Through these two proliferation mechanisms, a single infected PC can introduce ransomware to an entire enterprise and cause significant damage.

Disclosure of confidential or proprietary information during restoration attempts

Malicious actors may try to steal data from (or otherwise abuse) systems that have been affected by ransomware. In multiple cases, threat actors have been observed deploying ransomware alongside capabilities that steal data. Infections with fraud-enabling malware often serve as a foothold for the attacker to perform a variety of monetization actions.

Severity of Ransomware

The volume and variety of ransomware is growing and causing more damage. Attackers are also becoming more flagrant, threatening to corrupt confidential files or publish them online if the ransom is not paid by a specified time.

FireEye regularly identifies and announces the discovery of new variations of ransomware. FireEye Threat Intelligence has observed ransomware such as CryptoWall generate illegal gains of $1 million over a six-month period in 2015. FireEye also estimates that the TeslaCrypt hackers took home $76,522 USD between Feb. 7 and Apr. 28, 2015.

Cyber attacks that use ransomware are expected to increase in the next few years. They are fairly easy to deploy even for novice computer users worldwide.

Five examples of ransomware variations FireEye detects

CryptoWall – Appearing a few months after the discovery of CryptoLocker, CryptoWall showed behaviors similar to CryptoLocker. During six months in 2014, the ransomware earned an estimated $1 million.

CTB-Locker - First discovered in 2014, CTB-Locker distinguished itself from peers at that time through features such as a Tor-based control server and auto-generated Bitcoin addresses unique to each victim.. The ransomware continues to be sold to cyber criminals.

TorrentLocker – Emerged in 2014 following the takedown of CryptoLocker and is likely linked to the same actors.

Locky – Began spreading in early 2016 using the same mass distribution channels as the Dridex credential theft malware.

TeslaCrypt – First discovered in Feb. 2015, this ransomware encrypts various types of files, including online games. The malware uses multiple tactics to reduce victims' chances of blocking or easily remediating infections. These include encrypting files regardless of whether a connection to the control server can be established, and deleting local "shadow copies" that can be used for data or system recovery.

Ransomware Response Strategy 1: Identify Attack Mechanisms

There is no single solution to the increasing threat of ransomware. The victim typically either pays the ransom and hopes the problem stops there or risks significant business disruption while they attempt to self-recover.

Paying attackers for decryption is not a real solution. Paying them not only creates a financial burden on the victim organization but also directly rewards attackers with money and motivation for further attacks. Law enforcement agencies make no recommendations when it comes to dealing with a ransomware demand. Instead, their advice emphasizes prevention and contingency planning.[6]

Generally speaking, preventing ransomware infections requires updating the OS and application programs to the latest versions and exercising caution when accessing news, advertisement and other websites with security loopholes. Enhancing email security to block phishing emails can stop many attacks before they occur. In the event of an infection, regular backups can help mitigate damage and accelerate recovery time.

Organizations should intensify efforts to identify the exact intrusion mechanisms of ransomware and implement expert security solutions that could protect critical corporate information from ransomware attacks. A sound security strategy must thoroughly analyze the attack mechanisms of ransomware and assess security measures that could mitigate ransomware damage.

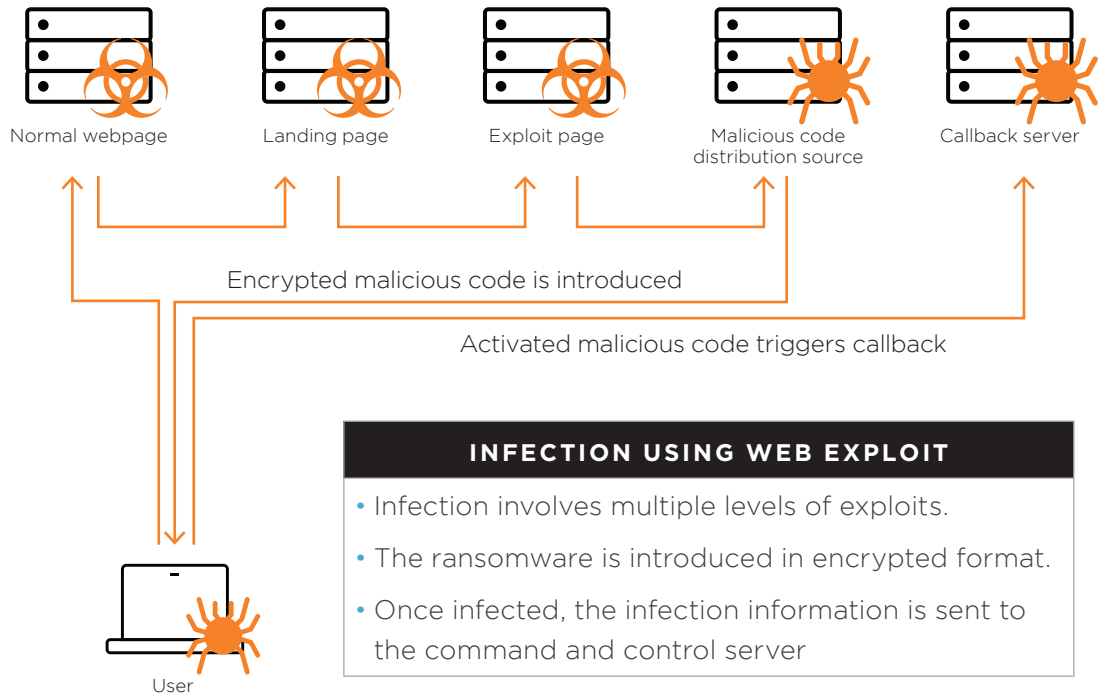
Ransomware is introduced through two main paths: web and email.

Infection via web

Ransomware can attack through websites with exploits. This often occurs with a "drive-by download" exploit kit that takes advantage of vulnerabilities present in major web browsers or applications. The attacker infects a legitimate website or hacks an advertising network to insert code that redirects the victim to another website that hosts an exploit kit. Exploit kits such as Angler and RIG detect vulnerable software such as older versions of Java or Flash on the visitor's computer. They then lure the visitor to download and run the malicious payload. Once the visitor's computer is infected, the ransomware connects to a command and control server that allows the attacker to collect valuable information.

6 Fbi.gov. "Ransomware on the Rise." January 20, 2015.

FIGURE 2. HOW RANSOMWARE INFECTS VICTIMS VIA THE WEB.



In the case of web-based infections, the exact infection path cannot be identified without analyzing the multi-level flow that redirects the user from a normal website to the malicious code distribution source. Malware can go undetected by ordinary security software because it is introduced to the victim's computer in encrypted format.

Behavior-based analysis is needed to identify the encrypted malicious code. To minimize damage, connections to the command and control server must be blocked so additional malicious code is not received and sensitive information is not sent out.

Four activities can help effectively mitigate the damage caused by ransomware introduced via the web:

- A thorough analysis of the entire infection process, from the normal website that the user accessed first, to the redirected page and the site of final infection.
- Disabling execution of scripts running in the browser
- Behavior-based analysis of the malicious code to determine its actual maliciousness and system infection indicators.
- Blocking access to the command and control server.

Ransomware damage can be minimized if any of these four activities are implemented successfully.

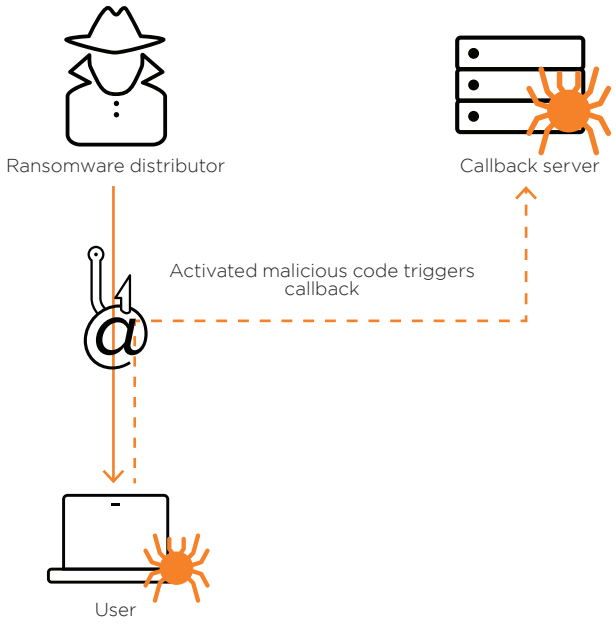
Infection via email

Ransomware can also infect systems via email. In fact, most reported ransomware infections were introduced via email. According to a report by the Cyber Threat Alliance (CTA),[7] CryptoWall 3.0, which caused $325 million damage worldwide, was distributed through phishing attacks via email (67.3%) and exploit kits (30.7%).

When introduced via email, ransomware is delivered through attachments such as compressed files, document files and html files or through links in the email message or a document attachment. Attackers often get the user to execute the file or click on the link through social engineering techniques rather than system vulnerabilities.

Behavior-based analysis is effective against email-delivered ransomware. Behavior analysis makes it possible to proactively block avenues of attack to minimize damage or infection.

FIGURE 3. HOW RANSOMWARE INFECTS VICTIMS VIA EMAIL.



INFECTION USING EMAIL

- Infection attempts using file attachments, malicious links, etc.
- Infection attempts using various file types
- Getting user to activate code using social engineering techniques

7 Cyber Threat Alliance. "Lucrative Ransomware Attacks: Analysis of the Cryptowall Version 3 Threat." October 2015.

Ransomware Response Strategy 2: Implement Advanced Security Solutions

Security firms are quickly launching solutions designed to fight the increasing impact of ransomware. However, many "best of" solutions[8] focus on file backups or detecting specific strains of ransomware. They generally do not provide clear information on how attacks find their way to a target's computer, or how to effectively block the attacks.

FireEye security solutions provide visibility over the ransomware attack process. They present a security strategy for effective response based on the ransomware's intrusion path (web or email).

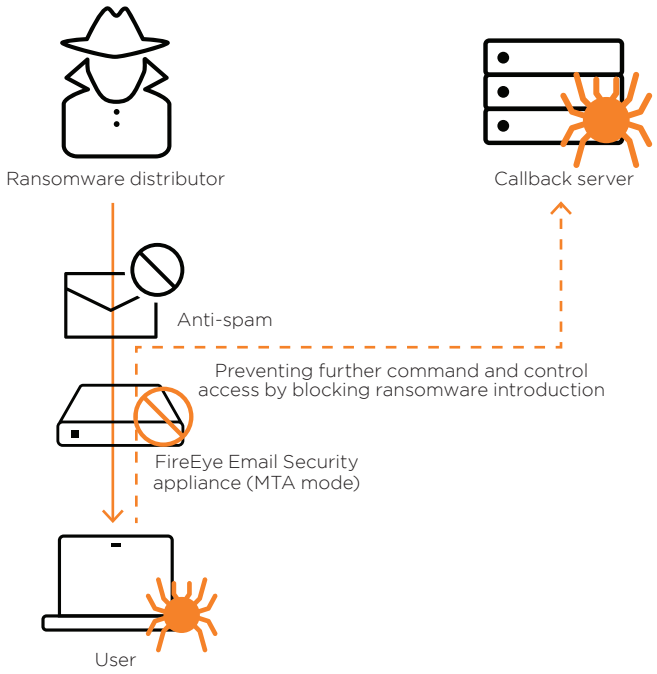
Email security is the first line of defense

An email security solution detects and blocks ransomware that is distributed through email attachments and embedded malicious links.

The majority of ransomware enters an organization using email as a vehicle, usually in the form of spear phishing. Spear phishing is one of the preferred attack strategies because it is difficult to detect. It's reliance on social engineering gives it a high rate of success – it can fool even security professionals and high level technology managers. All it takes is one email to activate ransomware and lock valuable assets.

FireEye email security solutions can block these malicious emails by executing and analyzing suspicious email file attachments and inline URLs. FireEye Email Security can be implemented either on premise with EX Series appliances, or via the cloud with Email Threat Protection Cloud (ETP). When the FireEye email security solutions are deployed inline to SMTP traffic, they can automatically detect and block ransomware before it reaches the end user, preventing malicious data encryption. (Fig. 8)

FIGURE 8. HOW FIREEYE EMAIL SECURITY DETECTS AND BLOCKS EMAIL-BASED RANSOMWARE ATTACKS.

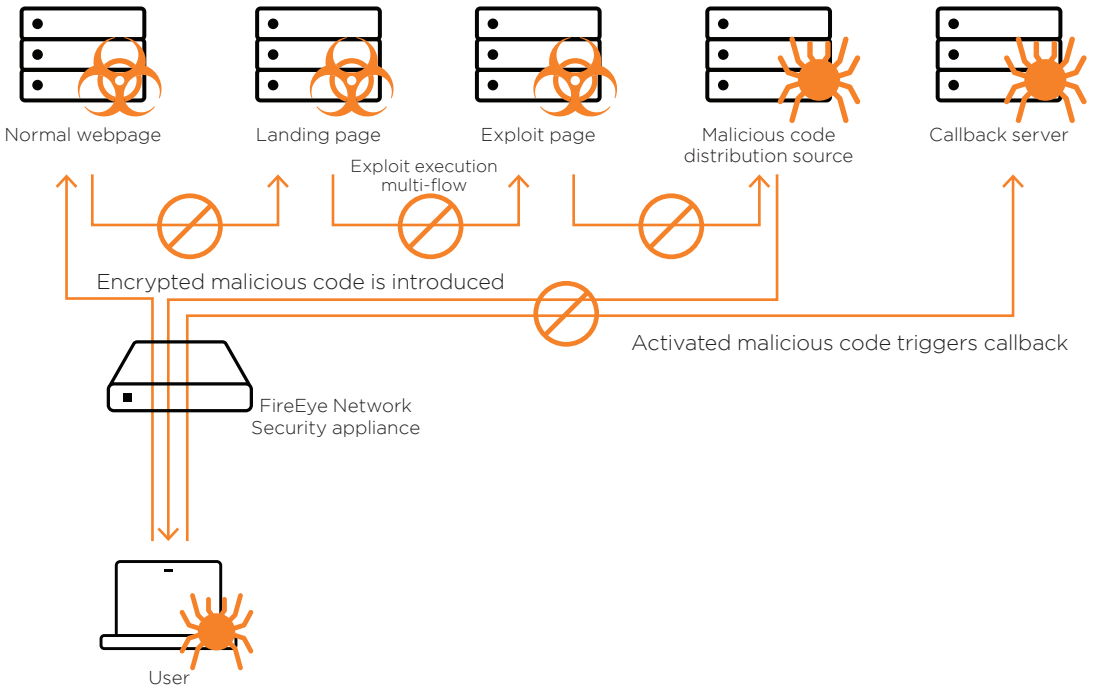


8 Techworld. "The 7 best ransomware removal tools – how to clean up Cryptolocker, CryptoWall and extortion malware." October 8, 2015.

Network security stops the spread

A network security solution identifies the distribution and infection path of ransomware and blocks the ransomware to minimize damage.

FIGURE 4. HOW FIREEYE NETWORK SECURITY DETECTS AND BLOCKS WEB-BASED RANSOMWARE ATTACKS.



Web-based ransomware attacks can be prevented by accurately identifying distribution sites spreading ransomware and blocking them. (Fig. 4)

Ransomware intrusion involves three main stages: initial infection, file encryption and command and control server access.

Initial infection

In this stage, the victim is redirected from a normal webpage to the malicious code distribution site and then the exploit is activated. The overall web flow must be analyzed to identify and block the distribution site.

FireEye network security solutions can identify the attack process attempted over web traffic. This allows organizations to know which websites are used as ransomware distribution sites and apply active blocking policies.

In a recent case, users who searched for the keywords 'Park Byeong-ho posting' and accessed certain online news pages on a Korean portal were redirected to exploit sites, where their computers became infected with ransomware. Customers using FireEye network security solutions had correctly identified initial infection attempts. FireEye followed through with the following recommendations and

actions. First, customers were to block the exploit landing page address and online news site if they were not associated with business. This would prevent additional host compromise by the ransomware. FireEye summarized and shared indicators of compromise (IOCs) for the ransomware with customers to investigate the possibility of additional compromise. Finally, to prevent web-based exploits, targeted companies were to update all their web technologies (Flash, Java, Silverlight and others) to the latest versions.

File encryption

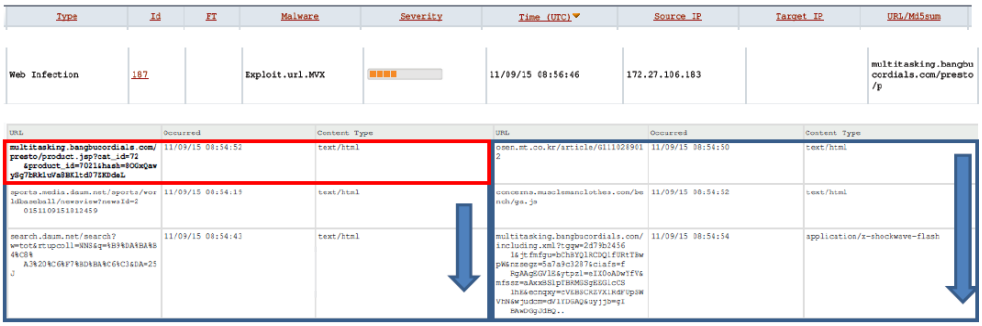
In this stage, ransomware-infected systems may begin to exhibit unusual behavior. If the ransomware managed to avoid detection during initial infection but is detected in this stage, FireEye network security solutions perform a detailed analysis of the malicious code and use indicators of compromise to block the ransomware, establish response measures and identify infected hosts. For example, if ransomware demonstrates the ability to disable the window restoration feature or encrypts files, the FireEye solution analyzes those behaviors and provides detailed trace indicators to the user. This not only helps detect the same attack against other users, but may prevent the spread of ransomware throughout connected systems.

Command and control server access

In this stage, the ransomware sends infection information to command and control servers or receives encryption key values from them. FireEye network security solutions detect and block access to command and control servers. If ransomware cannot communicate with its command and control servers, it cannot encrypt files or cause other types of damage.

FIGURE 5. EXAMPLE: HOW FIREEYE NETWORK SECURITY COMBATS WEB-BASED RANSOMWARE ATTACKS

FIGURE 6. EXPLOIT EXECUTION PROCESS FLOW INFORMATION PROVIDED BY FIREEYE NETWORK SECURITY.



Why FireEye Works

At the core of all FireEye network and email security solutions is the FireEye Multi-Vector Virtual Execution™ (MVX) engine which executes and analyzes files in a virtual environment. It operates far beyond the capabilities of common sandboxing technology. The MVX engine uses a proprietary, custom-built hypervisor for multi-level detection to analyze suspicious code within multiple combinations of operating systems, application programs, web browsers and plug-ins to detect and block cyber threats in real time. The technology provides effective and impactful analysis and detection even for previously unknown patterns, or zero-day threats. In fact, as of June 2016, FireEye had detected 28 of 46 zero-day threats identified by cyber security companies. With real-time visibility over virtually the entire lifecycle of a ransomware attack, from intrusion to infection, the MVX engine allows the user to establish fast, effective responses.

Damage from ransomware attacks is rapidly increasing because it is difficult to identify distribution sites. FireEye combines its technology and decades of security expertise to reliably identify harmful websites and gives customers the information and support needed to deter both web- and email-based attacks that use these sites.

Conclusion

The threat of ransomware attacks is more real than ever. Incidents involving ransomware continue to grow, along with ransomware-caused damage such as direct financial costs and business downtime. Ransomware creators continue to pursue new tactics and develop new variations of their malicious code. And the countless variations of ransomware often go undetected by antivirus software.

Once infected with ransomware, organizations should expect significant damage. Advanced detection and prevention is the best defense. You have an advantage in battle if you know yourself and know your enemy. This is also true for cyber security. To reduce the chance of a ransomware attack, organizations need visibility into their internal system security levels and a strong understanding of the attacker tools, tactics and procedures.

For information about FireEye protection and response solutions used by thousands of government agencies and enterprises of all sizes around the world, visit www.fireeye.com or contact your local sales representative.

For more information on FireEye, visit:
www.FireEye.com

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

www.FireEye.com

FireEye