

White Paper

Four Countermeasures to Protect Against Ransomware

Best Practices for Defense in Depth Against Crimeware

By Doug Cahill, ESG Senior Analyst
August 2016

This ESG White Paper was commissioned by Trend Micro
and is distributed under license from ESG.



Contents

Executive Summary	3
The Rise of Ransomware	3
A Prevalent Strain of Crimeware.....	3
Increasingly Sophisticated Variants Are Emerging.....	3
Indiscriminate Set of Targets Represents a Global Market	3
Attack Vectors and Methods	4
Aligning Countermeasures with the Kill Chain	4
1. Email and Web Controls for End-user Exposure	5
2. Multifaceted Endpoint Controls.....	5
3. Coordinated Network-based Detection	6
4. Server Workload Protection of Critical Data Assets	6
Building a Ransomware Security RFP.....	7
The Bigger Truth	8

Executive Summary

By now, not only security professionals, but also many knowledge workers and consumers are well aware of the insidious nature of ransomware. As its name implies, ransomware is malicious software that holds data files hostage pending the payment of a ransom, typically with untraceable bitcoin as the currency of choice. Ransomware encrypts a series of files preventing access to those files. Absent the victim's ability to restore a backup, the hacker holds the encryption keys required to access the files until the ransom demand is met.

The incident rate of this form of extortion is escalating to epidemic levels. Ransomware is big business. According to the FBI, cyber-criminals collected \$209 million in the first three months of 2016, a run rate that represents a \$1B business.¹ And ransomware is becoming more sophisticated, making it increasingly difficult to detect and prevent.

Organizations must treat mitigating the risks associated with ransomware—data loss, interruption of business operations, and more—as a strategic imperative by implementing a layered security approach that maps to and thus thwarts ransomware attack campaigns. This paper offers a prescriptive approach to do so based on four countermeasures requiring a set of integrated controls for centralized visibility, shared intelligence, and active prevention.

The Rise of Ransomware

A Prevalent Strain of Crimeware

The prevalence of ransomware jumped dramatically in 2015 and has grown more prolific in 2016. According to Verizon's 2016 Data Breach Investigations Report, ransomware incidents saw the largest jump as the malware type employed by cyber-criminals in 2015.² Often coupled with command and control malware to form a one-two attack punch, the rise of ransomware has been enabled in part by a low barrier to entry with ransomware toolkits readily available to bad actors.

Increasingly Sophisticated Variants Are Emerging

Ransomware is evolving using increasingly sophisticated tactics, techniques, and procedures (TTPs) to execute attacks, including:

- **RAA** is javascript masquerading as a Word file with a .DOC file extension to avoid binary detection. Once launched, it seeks to disable the restoration of backups by deleting the Microsoft Volume Shadow Copy Service (VSS). RAA also employs a Trojan horse feature by dropping Pony, a password stealing Trojan, for future hacking.
- Unlike variants with an end-user and endpoint focus, **SamSam** targets servers via a JBoss vulnerability from which it moves laterally to infect and encrypt data on other Windows systems. In the same family of server-side ransomware, **MakTub** is a variant that will compress files to speed the encryption process.
- Hackers are even operationalizing ransomware. **Jigsaw** is a newer variant that includes a chat feature to coordinate the ransom payment between victim and hacker.

Indiscriminate Set of Targets Represents a Global Market

While ransomware attacks on the health care industry have been widely publicized due to their boldness and implications to patient care, large and small education, public, and private sector entities have also regularly been targeted. Ransomware is a horizontal concern with a global addressable market.

¹ <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>

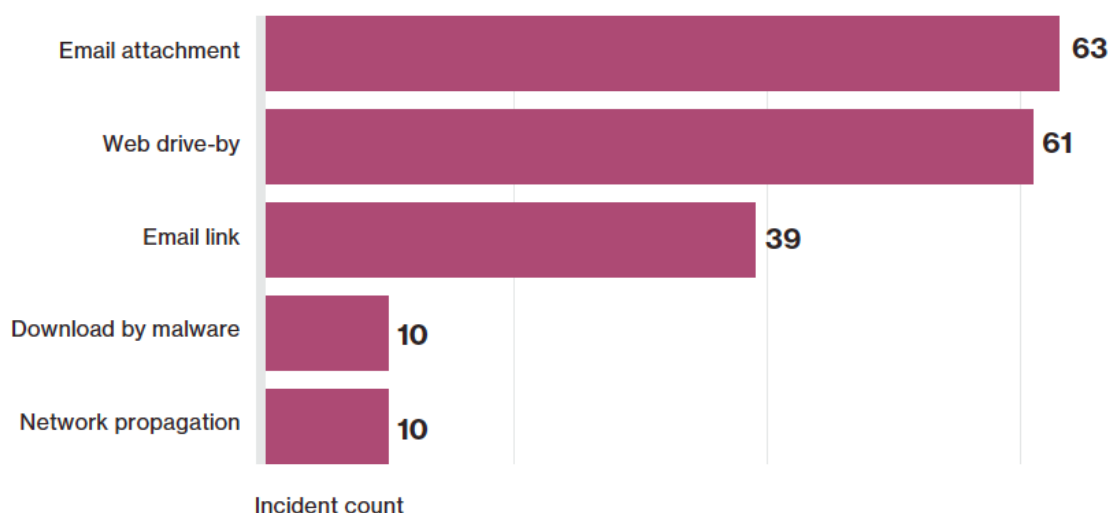
² Source: Verizon Report, [2016 Data Breach Investigations Report](#), 2016.

Ransom amounts are typically measured in the tens of thousands of dollars or less, which is indicative of a business model predicated on a large number of quick and small transactions across a broad set of targets. There have been reports of an increase in the size of ransoms, an effort by hackers to test price elasticity.

Attack Vectors and Methods

While attack methods vary across types of vulnerabilities, the most commonly exploited is human vulnerability via spear phishing. The top entry point vectors to support this method include email attachments and links (see Figure 1).³ Drive-by downloading is also a frequently tapped vector to deliver ransomware payload.

Figure 1. Top Five Malware Vectors within Crimeware



Source: Verizon, 2016

Ransomware is also exploiting application vulnerabilities, as is the case with SamSam, which takes advantage of vulnerabilities in certain web application stacks, and others that exploit vulnerabilities in Adobe Flash and Microsoft Silverlight.

Aligning Countermeasures with the Kill Chain

Ransomware, as is the case with other advanced threats, operates along the cybersecurity kill chain to achieve its objective. Such attack campaigns start with a recon phase to (usually socially) engineer the attack with a vulnerability to exploit (human or code), followed by the delivery, installation, and execution of the malware from which point communication with a remote C&C (command and control) server is established. More advanced ransomware will also move laterally across the network via mapped drives and other vehicles to delete backups and gain access to server-side corporate data assets such as databases, directory services, and more.

In addition to fundamental best practices such as automating full and differential backups, keeping backups offline, conducting regular patching, maintaining strong access controls, and providing ongoing end-user awareness education, more steps for a defense in depth approach are required to combat ransomware. The following four countermeasures map to how ransomware employs the cybersecurity kill chain and offers a proactive prescription for thwarting these attacks, which can protect organizations from the risks they represent.

³ Source: Verizon Report, [2016 Data Breach Investigations Report](#), 2016.

1. Email and Web Controls for End-user Exposure

Human nature is such that our gullibility exposes us to exploitation by the most common ransomware attack methods. This reality is manifested vis-à-vis the applications end-users interact with on a daily basis—email, web browsers, and office productivity applications, including cloud applications such as Microsoft Office 365—which collectively represent a user’s attack surface area. As such, the first level of defense is the implementation of the following controls to protect against these applications being used against end-users as an attack vector to introduce ransomware:

- **Email Controls.** Identifying and blocking fictitious spear phishing emails and scanning for known ransomware malware in emails, both embedded and those sent as an attachment, are essential capabilities, which should be prioritized.
- **Cloud App Coverage.** Given the widespread adoption of cloud applications, the above controls should also support cloud apps, especially Microsoft Office 365. According to research conducted by ESG, 40% of organizations report having already standardized on Microsoft Office 365 as their office productivity application suite with 64% of survey participants citing an intent to do so within 18 to 24 months.⁴
- **Web Controls.** Web controls will employ website reputation to block known bad URLs and scan for malicious downloads and browser exploits on websites being visited by end-users.
- **Advanced Controls.** For new and unknown ransomware, zero-day detection techniques including sandboxing and behavioral monitoring are required. These controls dynamically analyze executables, URLs, and documents to determine if they exhibit behavior consistent with ransomware, such as the rapid encryption of a set of files.

Forty percent of organizations report having already standardized on Microsoft Office 365 as their office productivity application suite with 64% of survey participants citing an intent to do so within 18 to 24 months.

It bears repeating that the most common attack vectors are those associated with how end-users interact with email and the web, making these controls the most critical to implement to reduce the risk of a ransomware incident.

2. Multifaceted Endpoint Controls

In the event that ransomware successfully exploits the exposure layer and arrives on an end-user’s endpoint, a variety of endpoint security controls are required to thwart this stage of the attack:

- **Application Control.** By implementing an application whitelisting and blacklisting approach to binary execution, application control, by definition, will only allow authorized, known-good software to run—thereby preventing executable-based ransomware from gaining a foothold on a targeted device.
- **Behavioral Monitoring.** For other ransomware types, including those delivered as weaponized content, behavioral monitoring along with dynamic analysis via sandboxing will detect the types of behavior consistent with ransomware, including file modifications (i.e., compression and encryption) and attempts to map and connect to network drives.

⁴ Source: ESG Research Report, [Security, Productivity, and Collaboration: Trends in Workforce Mobility](#), May 2016.

- **Host Intrusion Detection and Prevention (HIDS/HIPS).** The detection of how ransomware operates extends to attempts to move laterally via network connections. This requires the use of intrusion detection and prevention rules to detect anomalous netflow activity and then block inbound and outbound connections.
- **Virtual Patching.** The ability to detect the behavior of an exploit will shield endpoints from vulnerabilities in common end-user applications such as Adobe Flash, which is an effective control against both zero-day exploits in systems that have not yet been patched.

3. Coordinated Network-based Detection

While host-based intrusion detection and prevention is the first step in detecting the lateral movement of ransomware, network-based controls can help detect ransomware attacks on the wire and prevent the spread of such attacks to other endpoints and servers. A network-based ransomware countermeasure will provide the following capabilities:

- **Protect Across All Ports and Protocols.** The scale and scope of the network-based solution needs to be able to monitor bi-directional traffic on physical and virtual network segments composed of a wide variety of protocols across all of an organization's network ports.
- **Prevent the Known.** Known ransomware can be detected via a combination of pattern matching, reputation-based assessments, and script emulation to detect, for example, malicious files, exploits, and traffic to and from a command and control server.
- **Detect the Unknown.** Extensive detection methods including custom sandbox analysis should be deployed to protect against new and previously unknown ransomware, including zero-day exploits, using a variety of analysis techniques to detect file modifications and/or other actions and behaviors associated with ransomware.
- **Integrate for Expediency.** Integration with firewalls, web and email gateways, and host-based controls expedites detection and response by sharing contextual threat intelligence between each layer of defense.

4. Server Workload Protection of Critical Data Assets






The data created and accessed via server workloads is often composed of those digital assets that are the most valuable to an organization, making this fourth countermeasure critical for a comprehensive defense in depth implementation. Akin to some of the noted endpoint security controls, but also taking into account the behaviors specific to server-side ransomware such as SamSam and Maktub, server controls should include the following:

- **Malware Scanning and System Integrity Monitoring.** In addition to scanning for known malware, continuously monitoring system activity for the detection of anomalies against a baseline of standard activity can identify new processes, file system modifications, and netflow activity that could indicate the introduction of ransomware.
- **Virtual Patching.** Due to operational impact, many organizations choose to either defer patching or simply deploy updated server configurations in a cutover deployment model. For these reasons, and given the precedence of JBoss vulnerabilities being successfully exploited, virtual patching will detect and prevent attempts by ransomware to exploit vulnerabilities, shielding servers and their associated data assets from compromise.
- **Host Intrusion Detection and Prevention (HIDS/HIPS).** Consistent with the kill chain, server-side ransomware will attempt to move laterally and may set up command and control communications. Detecting such TTPs requires the ability to monitor netflow traffic for nonstandard inbound and outbound communication.

Building a Ransomware Security RFP

The functional capabilities for a ransomware solution should map to these four countermeasures with tight integration points between each for the orchestration of policies and centralized visibility. Such a “platform approach” versus that deployed via a set of disparate point tools will lower operational cost via streamlined workflows, ensure consistency of policies to reduce human error, automate policy assignment for faster time to protection, and coordinate the detection and prevention of ransomware across the spectrum of apps, endpoints, network, and servers.

The structure of a request for proposal for such a solution should include:

	Security Control	Functional Requirements
	EMAIL AND WEB	<ul style="list-style-type: none"> Spear phishing detection Email payload and URL analysis Behavioral monitoring and sandboxing Support for Microsoft Office 365
	ENDPOINT	<ul style="list-style-type: none"> Application control Behavioral monitoring and virtual patching
	NETWORK	<ul style="list-style-type: none"> Monitor all network traffic Custom sandbox analysis
	SERVER WORKLOADS	<ul style="list-style-type: none"> System integrity monitoring Behavioral monitoring and virtual patching
	ADVANCED	<ul style="list-style-type: none"> Integrated, shared, and contextualized threat intelligence Dynamic malware analysis (i.e., sandboxing) Integration with web and email gateways, plus network Centralized Visibility and Control

The Bigger Truth

Transactional repeatability, a low barrier to entry, and a massive target market are central reasons why ransomware is highly attractive to cyber-criminals. This form of cyber-extortion is indicative of the evolving threat landscape and represents another case in point for a defense in depth approach to cybersecurity. Because ransomware takes advantage of a broad attack surface area across applications, users, and devices, cloud-, endpoint-, and server-resident data assets are at risk of being encrypted and held for ransom.

Protecting against ransomware necessitates a proactive security posture enabled by the implementation of email and web controls, multifaceted endpoint controls, coordinated network-based detection of lateral movement, and server workload protection for critical assets. The scope of attack vectors and methods creates a requirement for multiple controls that work together via tight integration to share intelligence and take action. Given ransomware prevalence, a growing number of financially motivated adversaries, the introduction of new ransomware strains, and the potential business impact of an incident, time is of the essence for implementing a comprehensive solution based on these critical four layers of defense.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

© 2016 by The Enterprise Strategy Group, Inc. All Rights Reserved.