INTRODUCTION

Ransomware is one of the biggest security threats facing organizations of all sizes, and Alert Logic® is seeing a rise in more complex ransomware attacks than ever before. These attacks have evolved far beyond the rudimentary versions of “CryptoLocker” from the early 2000s. Over 50 new variants have emerged in the first half of 2016 alone. Most of these have been delivered through infected payloads or malicious links in phishing campaigns, but the proliferation of ransomware isn’t relegated to email campaigns alone. Malicious payloads can be delivered through compromised software and app stores, as well as compromised websites, malvertising, and web exploit kits.

Detecting and mitigating these quickly evolving ransomware attacks must rely heavily on a layered approach to cyber security, one that detects malicious activity at the earliest possible moment. To do so requires the use of endpoint security, vulnerability management, host and network intrusion detection, endpoint policies, and network traffic controls to block malicious activities. In addition, corporate education initiatives that enable users and IT staff to recognize the key indicators of ransomware activity provide an additional layer of protection for businesses.

RANSOMWARE OVERVIEW

Ransomware can be devastating to business operations and data integrity, given its nature of operation. Once a system becomes infected, the aim is to extort a ransom in exchange for restoring access to a system or data (although there is no guarantee that access will be restored). There are two main categories of ransomware: locker and crypto.

- **Locker** denies access to the computer or device that has been infected. Locker variants will normally disable an interface or peripheral access to the device itself and won’t affect the underlying operating system or files.

- **Crypto** prevents access to files or data. Once installed on the host system, files are encrypted and rendered unusable until a decryption key is provided. Often, attackers will seek out specific folders and system files and encrypt with malware, in the hope that either important or sensitive data will be affected, thus making the likelihood of a ransom payment far higher. The latest trends in ransomware often involve high levels of encryption, making it difficult or even impossible to crack keys.

While both versions of ransomware still exist today, crypto is by far the preferred method for attackers, given the reduced ability for users to recover data without making a payment. Ransomware success relies on the often-poor controls around endpoint security, backups, and data segmentation. Attackers understand that many users store personal or key data on their end devices; they will be desperate to recover files, rather than face the prospect of losing them forever. The same is also true of ransomware that targets organizations’ servers. Many businesses will enter a state of panic, preferring to pay a ransom, instead of facing hours, days, or weeks of data recovery and the resulting interruption of business operations.

With the impact of ransomware growing, how do organizations avoid becoming victims of this type of malware?
ALERT LOGIC – A MULTI-LAYERED APPROACH

Alert Logic offers security technology solutions and Security-as-a-Service that performs key functions in detecting ransomware on public cloud, managed/hosted, and on-premises infrastructure.

While Alert Logic does not offer endpoint security products such as malware/antivirus software, our network and data-center focused security services may detect ransomware activity during or after the initial compromise. Our portfolio of threat management solutions provide the following areas of detection, protection and remediation:

ALERT LOGIC® THREAT MANAGER™ WITH ACTIVEWATCH™

Threat Manager provides regular vulnerability scanning and assessments for infrastructure assets—a baseline step in your layered security strategy to protect against ransomware. Additionally, using integrated Intrusion Detection capabilities, Threat Manager may identify outbound command and control communications of ransomware software or related network activity, after it has become active.

In addition to technology-driven detection, Alert Logic ActiveWatch provides an added detection layer via certified security experts who actively monitor, identify, investigate, and escalate incidents to pro-actively identify and protect against ransomware attacks that have propagated into the network.

ActiveWatch services provide visibility and alert coverage for malicious network communications of all sorts, including malware communicating to command and control points. This includes general types of ransomware communications—for those ransomware types that communicate on the network prior to doing damage—and the propagation of malware within an organization via a large-scale incident.

ALERT LOGIC® LOG MANAGER™ WITH LOGREVIEW

Log Manager may expose long-term activity after a successful attack, and may be useful in investigating, remediating, or preventing reinfection. Combined with our LogReview service, organizations receive daily security event log monitoring and ongoing case management via a dedicated global team of security professionals. These tools provide an auditable trail of any suspicious findings and give a historical perspective of your security operation.

ALERT LOGIC® CLOUD INSIGHT

Cloud Insight provides Amazon Web Services (AWS) users with configuration and vulnerability management tools to identify vulnerabilities and misconfigurations that can become points of entry for ransomware attacks. Designed specifically for AWS environments, Cloud Insight detects event-driven changes in AWS infrastructures, providing continuous visibility with prioritized reporting and remediation planning for vulnerabilities that require attention.

Although ransomware automation has not been observed specific to this attack surface, Alert Logic Threat Intelligence continues to monitor and observe changes to ransomware and associated adversary operational activities for emerging threats.
ALERT LOGIC® CLOUD DEFENDER®

Ransomware incidents will, in some cases, need to be exposed by evaluating both network event and log data. Cloud Defender—combining vulnerability scanning, IDS, log management, and web application protection backed by 24x7 expert security monitoring—proactively monitors for ransomware command and control communication from networks to external destinations, as well as internal ransomware infection indicators. Gaining visibility from multiple vantage points at network, system, and application layers, provides high-fidelity detection for Indicators of Compromise (IOCs) of ransomware variants that propagate between clients or within server environments.

ALERT LOGIC: CONTINUAL THREAT INTELLIGENCE AND SECURITY EXPERTISE

The Alert Logic platform is updated on a regular basis with new security content and correlation rules that adapt to the latest ransomware for supported targeted assets within a customer’s data center environment. In addition, when incidents are created, the Alert Logic security analyst team reviews associated events, looking for activity related to ransomware. Through expert knowledge and experience within the Alert Logic Security Operations Center, customers are notified within the shortest timeframe possible and given key remediation advice relevant to their environment and threat surface.

ORGANIZATIONAL RESPONSIBILITIES

Understanding the threat vectors used by ransomware attacks and implementing security controls to mitigate against these vectors is critically important to defending against ransomware attacks. No single security solution can provide complete protection or detection of ransomware threats. As such, a multi-layered approach combining effective endpoint, server, file monitoring, security gateway, and filtering technologies in tandem with better insights, monitoring, and reporting capabilities are all keys to better detection and ultimately better protection.

We strongly encourage all organizations to implement security protection in a layered approach, to prevent or mitigate the impact of malware such as ransomware through:

- **Prevention**: Ensure endpoint computers have anti-malware software that is active and current.
- **Detection**: Deploy and use host and network intrusion detection.
- **Mitigation**: Maintain endpoint policies and network traffic controls to block malicious activities.
- **Response**: Use removal tools for malware, separate or as part of endpoint protection.
- **Recovery**: Verify the availability of data, and use backups to restore any lost or unrecoverable data.

Alert Logic representatives can advise you on appropriate measures to complement our services, and form a layered security strategy against ransomware and other emerging malware.
**ALERT LOGIC SECURITY-AS-A-SERVICE IN ACTION**

The Alert Logic Security Operations Center (SOC) provides 24x7 security monitoring by GIAC-certified security analysts and using state-of-the-art technology. The SOC can identify and analyze threats, and notify customers when action is required. Below are two real-life examples of Alert Logic Security-as-a-Service defending against ransomware threats.

**PROTECTING AGAINST CRYPTOWALL**

An Alert Logic customer was hit with a ransomware attack that bypassed their endpoint security controls, and was delivered directly to a core gateway server for remote and internal access users.

---

**MALWARE ACTIVITY**
- Citrix Gateway Server becomes infected with malware
- Malware C2 Activity to malicious IP
- Analyst Investigates Events Data - Alert Logic Threat Manager & Log Manager

**MALWARE CONTAINED**
- Customer contains infected Citrix Server and removes from network
- Server recovered from backup
- Attack Source Blocked
- User access restored in under 25 minutes of initial incident escalation

---

The Alert Logic SOC identified the suspicious activity via active outbound communication to a command and control network—identified as a malicious source—through Alert Logic security and SOC analytics capabilities. The events were correlated and within 7 minutes an incident was escalated to the customer. Analysis covered over 55 packet captures from triggered event signatures and 82 log entries on the infected server, indicating suspicious activity. All data was correlated into a single incident and the customer was notified directly by a call from the Alert Logic SOC analyst, detailing key remediation guidelines. The customer was able to immediately contain the affected server and prevent further communication to the malicious IP, recovering protected backups to restore user access.
PROTECTING AGAINST CERBER

In another example, Alert Logic identified the infection of a single host of the customer through a phishing email attack, which led to the installation of the “Cerber Trojan” ransomware variant. Events were triggered through the Cloud Defender platform indicating Trojan communication activity (via packet signatures matching the Cerber Trojan) to an external IP.

Customer Type: Manufacturing  
Threat Type: Cerber (Ransomware)  
Alert Logic® Product(s): Cloud Defender®

MALWARE ACTIVITY
- Cloud Defender flags a possibly infected host with Cerber Trojan
- Cerber Trojan is a variation of a known ransomware variant
- Analyst begins immediate review of packet and log data

MALWARE CONTAINED
- Customer disconnects infected host from its network
- Malicious C2 IP blocked
- Infected Host Re-imaged
- Ransomware outbreak contained
- Full AV SCAN of entire organization performed to detect other potentially infected Hosts

INCIDENT ESCALATED (CRITICAL)
- Detailed data analysis discovers host calling out to a previously unknown C&C server IP
- Traffic pattern through signature analysis also confirms analysis of Cerber Ransomware variant
- Analyst immediately calls customer stakeholder informing of critical incident and required remediation steps

The analyst performed detailed data analysis within 4 minutes and immediately informed the customer of the infection and provided remediation advice on containing and cleaning the infected host, in addition to blocking communication to the malicious IP to prevent further ransomware infection. In addition, the customer ran a full antivirus scan across the entire organization to detect other potentially infected hosts, and educated users about the phishing threat vector and best practices for online and email communication.
DISSECTING RANSOMWARE THROUGH THE CYBER KILL CHAIN®

The Cyber Kill Chain (Lockheed Martin Computer Incident Response Team) provides a great platform for understanding how almost all malware applications target and infect organizations. If we apply this methodology to ransomware specifically, we can better understand how we may be targeted, down to the behavior patterns ransomware exhibits when attempting to infect host systems.

IDENTIFY & RECON

To identify a target organization or user, ransomware relies mainly on email addresses to deliver the infected payload. Targets can either be chosen at random from mass email lists (SPAM) acquired through data breaches of other sites or organizations, or they may be specifically targeted through phishing campaigns against a particular organization or individual. Phishing-based ransomware campaigns often rely on data available in open-source professional or personal social media sites. In other examples of ransomware attacks, infected payloads can be delivered through infected websites via web exploit kits, exploiting vulnerabilities in client-side browsers. This type of activity can still be classified as the “recon” stage, given that web exploit kits will still need to identify a browser vulnerability that can be exploited ahead of moving to the next stage, the initial attack.

INITIAL ATTACK

The initial attack is the point at which the infected payload is delivered to the target. As mentioned earlier, the attack tool of choice is often an email with an infected link (to a file or site), or infected attachment (such as a Word document or media file) that requires user interaction (download or open) to ensure successful delivery of the malware application. If we consider another method, such as compromised websites with infected software or applications, the method still relies on file download or installation for successful delivery of the malware application. Less common, however, is delivery of ransomware through infected websites using web exploit kits or the technique known as malvertising. This approach can be very difficult to detect and is often “zero-day” in nature (exploiting browser vulnerabilities that allow download and execution of payloads, often without the user’s knowledge).
COMMAND & CONTROL

Once successfully delivered, the ransomware application will almost always attempt to communicate with its command network (also known as C2 activity), an external IP or domain address through which it attempts to relay data relevant to the infected host system(s), and in some cases retrieve encryption key data. The challenge for most ransomware writers is that embedded public key encryption requires a different key for each infection, so the trend is the download of key data from the C2 infrastructure. This ensures further reliance on malicious IPs and the anonymization of network communication to operate effectively within the targeted environment.

SPREAD

Few ransomware variants today operate on a self-propagation basis once a particular host becomes infected. In fact, the “spread” phase is normally achieved lower down in the chain, through the initial attack vectors used by the malware, such as email, compromised websites, or downloaded applications. However, there are ransomware variants that will attempt to infect system files and spread to other hosts within the infrastructure, and a new era of “CryptoWorms” is expected to surface as malware writers become more sophisticated or existing campaigns become less effective over time.

EXTRACT

The extract phase in ransomware can be viewed from two different angles: 1) the ransom payment itself (Bitcoin), and 2) the ability to find or extract key files for encryption as part of its propagation capabilities on the infected system. In many cases, when the extract phase is reached in the kill chain it is already too late. Without access to the decryption keys, not much can be done to mitigate the infection on the affected hosts. Ransomware will work to target specific files or directories on a host system, specifically searching for data of interest that will help ensure a successful ransom demand and resulting payment. The latest versions of ransomware are becoming more effective at extracting data for encryption from system and user directories.
DEEP DIVE INTO THE ALERT LOGIC APPROACH

Alert Logic provides a great degree of coverage for supporting ransomware detection (including zero-day variants); however, combating ransomware requires a multi-layered approach, combining capabilities across different technologies and services to ensure effective detection at the earliest stage possible. If we consider the Kill Chain when understanding how ransomware proliferates within an organization, then we can be better prepared to assess our current capabilities and understand the efficacy of our existing security framework.

Protecting an organization’s hosts and infrastructure against malware relies on a combination of existing technologies and services, under a coherent framework that delivers the following outcomes:

MONITOR & IDENTIFY

Organizations need to ensure detailed monitoring of industry events from a ransomware campaign perspective in addition to key applications, systems, and networks as part of an effective ransomware protection strategy. This process combines two distinct efforts:

1. **Predictive Analysis:** This step refers to threat intelligence capabilities for discovering the latest ransomware campaigns and variants of existing campaigns. This can include understanding malicious source IPs and domains that can be proactively monitored for communication to the organization’s infrastructure and therefore provide an early warning of a targeted ransomware attack. At the least, telemetry that can identify known ransomware sources combined with other monitoring data (log, packet, and application layer inspection), can help increase detection rates and therefore ensure the right teams within the organization are alerted sooner against potential threats.

2. **Proactive Monitoring:** This step refers to an organization’s ability to capture key data points across the infrastructure and application stack to identify IOCs related to ransomware activity. Put simply, you cannot control what you cannot see. Capturing log data from applications, systems, and network layer devices (or cloud audit trails) combined with deep security analytics will help ensure ransomware threat vectors are identified as early as possible, when key assets may be targeted within the organization. Monitoring at the endpoint, server, and network levels is critical in an overall ransomware protection strategy. Security content and URL filtering are also paramount as part of an effective multi-layered protection strategy.

*The Alert Logic Approach*

As part of a multi-layered approach, Alert Logic provides proactive threat intelligence capabilities, feeding security content into the Cloud Defender platform. Through detailed log, threat, and application monitoring across the existing infrastructure of an organization’s cloud and on-premises environments, Alert Logic security analysts work 24x7 across our global SOC teams, monitoring customer data for the latest trends and IOCs related to ransomware campaigns.

Effective monitoring and identification also combine the implementation of host, server, and security gateway-based tools, providing detection of ransomware threat vectors at the endpoints (AV, HIDS/HIPS and FIM) and gateway entry points (firewalls, content filtering, and file scanning technologies). Alert Logic focuses on key targeted assets within a customer’s data center environment and often provides key notifications where existing security tools may prove ineffective against specific variants of malware.
DETECT & CONTAIN

In the instance where ransomware may have bypassed existing security tools, services, or detection capabilities, it is important that organizations are poised to detect key attributes related to the malware propagation and then immediately contain infected hosts.

1. **Detect:** This step relies heavily on the data points that are being monitored as well as the security content or correlation rules that are deployed across the existing infrastructure to effectively discover IOCs related to ransomware. Organizations need to implement a platform that monitors for ransomware activity 24x7 and is continuously updated and enhanced in terms of security monitoring rules against the latest trends in ransomware activity. This capability is underpinned by the ability to capture log, packet flows (including NetFLOW), and application data using endpoint, server, gateway, and security services. In almost all cases, ransomware will look to change or replace key files or directories and communicate with command and control networks, so these threat vectors can be quickly identified with a multi-layered approach, backed by a 24x7 monitoring operation to detect IOCs for even the most sophisticated or zero-day ransomware threats.

2. **Contain:** This step refers to the immediate quarantine and control of infected devices; particularly, blocking communication to external malicious IPs or domains to limit further risk across the organization. The ability to understand the key attributes of a ransomware attack through incident notification is both a technology and people process. Having expert analysts provide key attack and remediation advice helps organizations quickly and more effectively contain an infected ransomware host. Having access to the attack data (endpoint or server logs, payload scanning results, including packet captures showing propagation attempts or command and control activity) helps organizations better understand the threat at hand, supporting a more informed incident response and mitigation plan.

**The Alert Logic Approach**

Alert Logic provides a platform for monitoring customer log, packet flow, and application data to detect ransomware variants through IOC activity. In cases where ransomware attempts to communicate to command and control infrastructure (including known malicious IPs or domains) or propagate from host to data center assets monitored by Cloud Defender, Alert Logic SOC analysts will review incident data to confirm ransomware activity. In scenarios where the malware may have bypassed existing endpoint and security gateway controls, Cloud Defender customers are given the earliest possible warning of a ransomware infection as a result of key IOC activity detection. Incident data includes contextual information on the threat sources and infected hosts, so that security teams can act quickly to identify risks and contain infection effectively.

RESPOND & MITIGATE

Once ransomware is identified, organizations need to ensure an effective response and mitigation process that enhances security controls, educates internal users (and third-party providers where appropriate) and updates policy to further reduce business risk.
1. **Respond:** The effectiveness of this step is directly related to the organization’s visibility into the ransomware infection (see previous step). Identifying the infected hosts means that full analysis can be done on the extent of the damage from a file encryption perspective. Organizations should also ensure that online backups aren’t affected; this is only achievable through a detailed analysis of log data, including the additional information gathered through packet and application analysis (where appropriate). Once an organization gains a clear understanding of which hosts were infected, the methodology used to propagate the ransomware (e-mail, malicious application, or website), and the damage sustained, they can then implement a response plan to rebuild infected systems and restore data from secure backups (where possible). Oftentimes, multiple systems are required to present data to the key stakeholders, with a clear understanding of the malware application and its attack vectors so that organizations can start to build an effective mitigation strategy against further infection attempts.

2. **Mitigate:** Understanding all the data points gathered through expert analysis of a ransomware attack is paramount in ensuring an effective mitigation plan, which will often involve multiple teams, partners, and users throughout the organization. If there is a deeper understanding of the exposed threat vectors in a particular ransomware attack, then organizations can update systems and infrastructure to further mitigate against future threats, including educating users on safer online practices and improving DevOps and security practices to ensure a better baseline security posture against vulnerabilities that might have been exposed as part of the ransomware infection.

**The Alert Logic Approach**

Alert Logic provides detailed analysis and reporting capability for threats discovered and communicated to customers by our expert SOC analyst teams. This information allows organizations to quickly identify the key data points of a ransomware attack (source, destination host(s), and propagation techniques where appropriate), backed by direct support from the SOC in further understanding the details of the ransomware attack.

**SUMMARY**

Successful detection, response, and mitigation of ransomware attacks rely on many moving parts across an organization, combining security tools, services, and internal teams. Alert Logic provides key detection capabilities for ransomware variants by monitoring and protecting data center assets. When ransomware slips through the existing endpoint security controls, organizations must have visibility into network, log, and application data in order to identify the events triggered by a ransomware attempt. Having a platform in place backed by 24x7 expert SOC analysts monitoring for malicious activity that could signify new zero-day variants is a key piece of the overall multi-layered approach to protecting the organization.

For more information, visit [www.alertlogic.com](http://www.alertlogic.com).