SOLUTION BRIEF

Detecting Ransomware with Unified Security Management®

Reduce Your Risk of Extortion with AlienVault® Unified Security Management® (USM)

Introduction

In a recent ransomware survey, 80% of respondents perceived ransomware as an extreme or moderate threat, and of those organizations that suffered a ransomware attack, 75% experienced up to five attacks over one year[1]. It's no surprise given that ransomware is (at time of publication) a USD $2 billion 'market', and rapidly growing as threat actors, including organized crime and malicious states, try to take their share[2].

Threat detection or threat monitoring tools provide a critical layer of defense against ransomware attacks across all of your environments. Real-time threat detection and incident response is crucial to your ability to contain and the limit the impact of a ransomware outbreak. This extends to everywhere you've deployed assets, whether on-premises, in public cloud environments such as Microsoft Azure or Amazon Web Services, or in cloud applications like Microsoft Office 365 and Google G Suite.

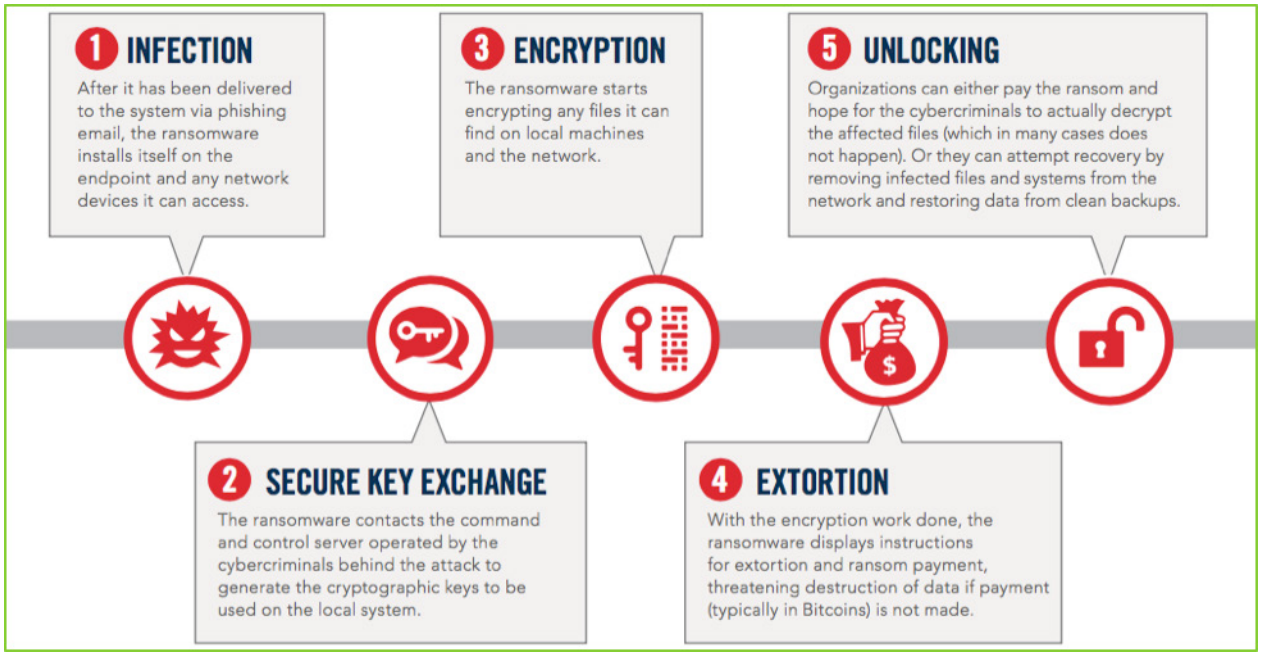
AlienVault® Unified Security Management® (USM) delivers three critical success factors for combating ransomware attacks against all of your critical infrastructure. First, the AlienVault USM platform provides you with the essential security capabilities you need to quickly detect and contain ransomware attacks across your cloud and on-premises environments. Second, continuously updated threat intelligence from the AlienVault Labs Security Research Team and the Open Threat Exchange® (OTX™) ensures the USM platform is always up to date with the knowledge required to detect emerging ransomware tools and techniques and ensures that you have the context needed to understand the threat and how to respond. Third, AlienVault USM delivers integrated security automation and orchestrated response capabilities that enable you to manually or automatically respond to detected threats using other IT security and operations products, such as working with Carbon Black to isolate a system infected by ransomware.

[1] 2017 Ransomware Report, Cybersecurity Insiders, https://www.alienvault.com/resource-center/analyst-reports/2017-ransomware-report

[2] Ransomware Payments to Hit a Record $2 Billion in 2017: Research, LIFARS (Nov 2017), https://lifars.com/2017/11/ransomware-payments-hit-record-2-billion-2017-research

How Ransomware Works

Employees are the weakest link when it comes to ransomware, which often infiltrates organizations through infected email attachments, phishing emails, or by visiting malicious or compromised websites. While these attack methods remain popular, they are not the only distribution method of ransomware. In May 2017, a massive, global ransomware outbreak known as WannaCry propagated by exploiting a vulnerability in the SMB (Server Message Block) service of unpatched Microsoft Windows operating systems. What made it worse is that it was one of the first ransomware variants that was a work type of malware, meaning that the ransomware attempted to self-propagate itself to other vulnerable systems. Since that attack, other ransomware variants have emerged, many of which have leveraged the NSA-developed attack methods leaked by a group of malicious actors known as the Shadow Brokers group.



Anatomy of a Ransomware Attack[3]

Historically, ransomware has primarily targeted Windows operating systems, although Linux and Mac OS X variants are becoming more prevalent. The most well-known type of ransomware is one that encrypts specific files, rendering the system or specific data unusable. This type of encrypting ransomware typically, once the malicious file executes, connects to a Command and Control (C&C, or C2) server to either notify the attacker of its successful infection of a system, gain further instructions, or obtain an encryption key. It then begins to encrypt files on the victim's system as well as any shared drives. The ransomware then displays a ransom note, demanding payment in exchange for a key to decrypt the files. With ransomware using modern encryption algorithms, like AES or RSA, it makes it nearly impossible to guess or crack the key.

In many cases, outbound communication from an infected system is difficult to detect due to ransomware employing techniques such as domain generation algorithms (DGAs). The DGA algorithm enables the ransomware administrator to create thousands of random domains every day that it can use for one or more C&C servers. The same algorithm running on each infected system generates that same list of random domains, and the ransomware tries to connect to each of those domains until it successfully connects to a target C&C server. This approach makes it challenging to use traditional defense tactics like a blacklist to block the connection to a known malicious IP address or domain.

[3] 2017 Ransomware Report, Cybersecurity Insiders, https://www.alienvault.com/resource-center/analyst-reports/2017-ransomware-report

Using AlienVault USM to Detect and Respond to Ransomware

AlienVault Unified Security Management (USM) collects and analyzes security and log data from a wide range of data sources across your on-premises, cloud, and hybrid environments and applications. The platform uses several essential security technologies working in concert to detect and respond to advanced threats like ransomware, including:

Asset Discovery — Monitors your on-premises and cloud environments for new assets, identifying new systems and devices that need to be monitored and assessed for vulnerabilities that ransomware could exploit.

Vulnerability Assessment — Continually scans your environments to detect vulnerabilities that attackers could exploit in a ransomware attack. The USM platform ranks vulnerabilities by severity so that you can prioritize your remediation efforts.

Network Intrusion Detection (IDS) — Analyzes the network traffic to detect signatures of known ransomware, and communications with known malicious servers. Using field-proven IDS technologies, AlienVault USM identifies attacks, malware, policy violations, and port scans that could be indicators of malicious activity on your networks.

Host Intrusion Detection (HIDS) and File Integrity Monitoring (FIM) — Analyzes system behavior and configuration status to identify suspicious activity and potential exposure. This includes the ability to identify changes to critical system and application files, as well as modifications to the Windows Registry, that could be made to initiate the ransomware's encryption engine.

SIEM Event Correlation — Using machine learning and state-based correlation, the USM platform analyzes a large number of seemingly unrelated events across disparate systems to pinpoint the few events that are truly important in that mass of information. The AlienVault Labs Threat Research Team regularly updates the USM platform with ransomware-specific correlation rules that identify a range of behaviors that are indicative of a ransomware infection, including downloading the ransomware file, systems attempting to connect with a C&C server and post data, multiple failed connections from a system attempting to connect to a domain (or multiple domains) within a narrow time window, and more.

SIEM Log Management & Reporting — The USM platform provides the ability to automate the centralized collection and normalization of events and logs from devices, servers, applications and more from across your on-premises and cloud environments, as well as from your cloud applications like Office 365. This data is centrally retained for at least one year, helping support compliance requirements and the ability to perform forensics on attacks that may have only recently been discovered, but that require investigation of more historic data. Centralizing collection also supports the automatic analysis of anomalies and attacks like ransomware, and enables analysts to perform search and forensics on collected data. Analysts can also run any of the built-in and customizable reports, such as to demonstrate compliance with standards like PCI DSS, or for regular review of security events and activities.

AlienVault Threat Intelligence

Cyber criminals and attackers are constantly adapting their methods, making for a constantly evolving threat landscape. Most organizations don't have the time or resources to research the threat environment and continuously update their detection capabilities based on new and emerging threats. The AlienVault Labs Security Research Team handles this task on behalf of AlienVault USM users by delivering continuous threat intelligence updates to the USM platform to keep the threat detection capabilities up to date with the latest threats.

In fact, for many recent threats, the threat detection capabilities were updated the same day, or even before specific vulnerabilities were exploited.

THREAT	DISCOVERED	THREAT DETECTION CAPABILITIES UPDATED IN ALIENVAULT USM
"Petya" / NotPetya	June 27, 2017	Same day
WannaCry	May 12, 2017	Same day
Samba CVE-2017-7494	May 25, 2017	Same day
WordPress Content Injection	February 1, 2017	6 days BEFORE
Adobe 0-day (CVE-2015-0311)	January 22, 2015	3 months BEFORE

Threat intelligence integrated into the USM platform eliminates the need for IT teams to spend time or resources conducting their own research on emerging threats. This threat intelligence is continuously updated in response to new and updated threats, meaning that essential rule sets and threat information are readily available to detect the latest threats, including:

- **Correlation directives** – translates raw events into actionable remediation tasks
- **Network and host IDS signatures** – detects the latest threats in your environment
- **Asset discovery signatures** – identifies the latest OSs, applications and device types
- **Vulnerability assessment signatures** – finds the latest vulnerabilities on all your systems
- **Report templates** – provides new ways of viewing data about your environment and / or meeting compliance requirements
- **Dynamic incident response templates** – delivers customized guidance on how to respond to each alert
- **Support for new data sources** – expands your monitoring footprint

The AlienVault Labs Security Research Team also utilizes the power of the AlienVault® Open Threat Exchange® (OTX™). OTX™ is the world's first truly open threat intelligence community that enables collaborative research. This global community of over 65,000 subscribers, including security researchers and practitioners, contributes over 14 million real-time threat data artifacts to OTX every day. This includes information about ransomware outbreaks as they emerge in the wild, including Indicators of Compromise (IoCs), details about threat actors, targeted industries, and more. OTX enables everyone in the OTX community to share threat data, strengthening their own defenses while helping others do the same.

OTX is fully integrated with AlienVault USM, so you get additional insight into malicious activity targeting your network. This integration with OTX enables AlienVault USM to quickly identify indicators of attacks previously reported by other members of the Open Threat Exchange.

Reduce the Time between Detection and Response with Security Orchestration & Automation

A ransomware attack can spread rapidly across your systems and quickly render them unusable. Time is of the essence. As soon as ransomware is detected in your environment, you must move swiftly to contain the threat and to prevent it from proliferating across your environment. If done manually or done across many disparate systems, or if the attack happens outside of typical working hours, your response effort may be delayed or too slow to contain the attack.

AlienVault USM has advanced security orchestration and automation capabilities that help you respond quickly and efficiently to threats affecting your environments, including response actions that work in alignment with third-party security tools like Cisco Umbrella, Palo Alto Networks, and Carbon Black. For example, if the USM platform detects evidence of ransomware on one of your assets, you can easily orchestrate the isolation of that system from your network through the built-in integration with Carbon Black, helping to prevent further spread of the ransomware.

The security orchestration responses available within AlienVault USM can also be automated, making your response faster and more efficient. For example, if AlienVault USM detects communication with a DGA-generated domain known to be malicious, such as ransomware communicating with its 'Command & Control' server, you can orchestrate a response action that passes the malicious domain details to Cisco Umbrella, which then blocks traffic between that domain and your employees and assets.

Decreasing Your Risk from Ransomware

Ransomware is a prevalent threat and one that the industry expects to see an increased frequency of attack in the coming years. While it remains unknown when the next ransomware attack will hit or what methods it will use, there are several steps you can put into practice to decrease your risk from ransomware:

- **Architect your environment to minimize cross-infection** – This includes implementing network segmentation and a least-privilege model to limit ability for any ransomware to traverse the network.
- **Implement a backup plan** – Even if only part of your data is irretrievably lost due to a ransomware attack, it can still cost your organization in terms of lost productivity and the efforts to try to retrieve that data. Defining and implementing a backup policy is a critical defense, and in particular, using offline backups.
- **Train your organization** – People are often the weak link when it comes to ransomware. Regularly train your employees on how to identify phishing attempts, the risks associated with opening email attachments, and more. Equally important is to ensure they know what to do if they feel that they have been compromised, including who and how to report the incident to ensure the fastest response.
- **Regularly scan for and patch vulnerabilities** – The WannaCry ransomware took advantage of an exploit for which a patch had been available for over one month. The organizations impacted were either unaware of the patch or had failed to deploy the patch in a timely fashion. Knowing what assets exist across your environment, what software and services they run, understanding where vulnerabilities exist and what patches are available are all critical to being able to shore up any gaps before a malicious actor exploits that vulnerability.
- **Ensure your security solutions are up to date** – Any software solution may have flaws, and many software security solutions like vulnerability or malware defense solutions require threat intelligence to be able to know what threats are out there and how to detect them. Ensure that you regularly update your security solutions to address any issues, add new and enhanced capabilities, and ensure that they are running with their latest threat intelligence so that they are optimally protecting your environment.

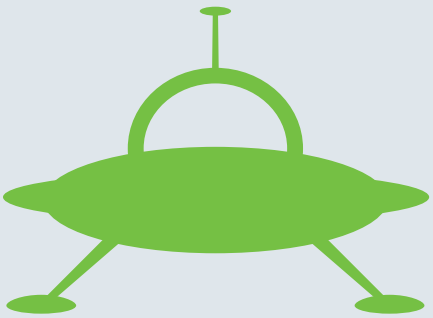
In addition, you should deploy security essentials including asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and SIEM correlation and log management. However, deploying traditional security point products require extensive configuration and tuning during deployment and monitoring after deployment. The lack of integration with other tools means that even with a centralized management console like a SIEM, IT teams must dedicate a significant amount of staff time to managing each security control, and even more time trying to consolidate and correlate all of the alerts being generated by those tools.

This is where AlienVault USM offers an affordable yet comprehensive solution in your battle against ransomware and other threats. It provides built-in essential security capabilities in a unified solution, integrates threat intelligence from AlienVault Labs and OTX, and delivers security orchestration and automation for efficient incident response.

The USM platform provides an effective defense against ransomware and other attacks in a solution that significantly reduces complexity and deployment time, and where you can go from installation to first insight in as little as one hour.

Next Steps:

- Take AlienVault USM for a test drive in our online demo environment
- Start detecting threats in your environment today with a free trial
- View pricing and request a quote



About AlienVault

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault® Unified Security Management™, with the power of AlienVault's Open Threat Exchange®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).