ALIEN VAULT

WHITE PAPER | SPECIAL EDITION

Detecting WannaCry Ransomware

How to Detect & Respond to WannaCry Ransomware with AlienVault USM

A Global Outbreak of WannaCry Ransomware Attacks

On May 12th, 2017, the AlienVault Labs Security Research Team reported seeing a wave of infections related to a new ransomware variant known as "WannaCry." The attacks have been widespread, affecting hospital services, banks, and telecommunications service providers in Europe, and beyond.

At the time of writing, WannaCry ransomware has been linked to over 75,000 attacks in 99 countries[1]. With no apparent target, these attacks could potentially strike any organization vulnerable to such an infection. Therefore, it's important to know the potential risks of the WannaCry Ransomware and how to detect a potential infection early.

How Does WannaCry Ransomware Work?

One of the infection vectors in WannaCry is apparently a module that exploits a vulnerability (MS17-010) in Windows and uses a worm component to spread within a network. It's important to note that the most likely initial attack vector is a phishing attempt that users may fall for to install the ransomware onto their computers. Once there, the virus can spread to other systems more easily.

Once installed, WannaCry locks the files on a computer and asks its victims to pay approximately $300 by Bitcoin within a few hours. It appears the attackers have found people willing to pay.

Using AlienVault USM to Detect WannaCry Ransomware

1. Scan your environment for the MS17-010 vulnerability.

WannaCry Ransomware works by exploiting a Windows vulnerability (MS17-010). This vulnerability was leaked as part of the Shadow Brokers hack of the NSA earlier this year. Microsoft released a patch for MS17-010 on March 14th, however any computers or systems that have not been patched yet are still at high risk.

First and foremost, you need to know whether your critical infrastructure has the MS17-010 vulnerability. To find out, use a trusted vulnerability scanner—such as the built-in vulnerability scanning tool in AlienVault USM—to assess whether your systems and devices are currently at risk. Because USM receives continuous threat intelligence updates, including the latest vulnerability signatures, USM users have the assurance that their vulnerability scans use the latest known vulnerability signatures.

If such vulnerabilities are found in your environment, take swift action to patch your systems, and then re-scan your environment. With USM, you can easily run on-demand vulnerability scans on any part of your environment.

Get started with a free trial of USM Anywhere and start detecting your vulnerabilities within minutes >

2. Monitor your environment for intrusions.

Assessing and remediating vulnerabilities is not the only step you need to take to protect your organization from a

[1] https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today

potential WannaCry ransomware attack. You must also continuously monitor your environments for signs that your vulnerabilities have been exploited, which could indicate that you have been infected by ransomware.

As of April 18th, AlienVault USM users benefited from a threat intelligence update that included an IDS signature to detect a WannaCry ransomware exploit in their environments:

ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response

The built-in intrusion detection tools in USM work to identify threats like ransomware and alert users whenever such threats are detected. And because USM receives continuous threat intelligence updates from the AlienVault Labs Security Research Team (like the example listed above), USM uses the latest global security data in its intrusion detection activities.

The AlienVault Labs Security Research team leverages threat data from the Open Threat Exchange, the world's largest open threat community. During the initial WannaCry attack outbreak, OTX community members shared their threat data related to the ransomware, creating a Pulse of indicators of compromise (IoCs) to the benefit of the global threat intelligence community—and for the direct benefit of USM users.

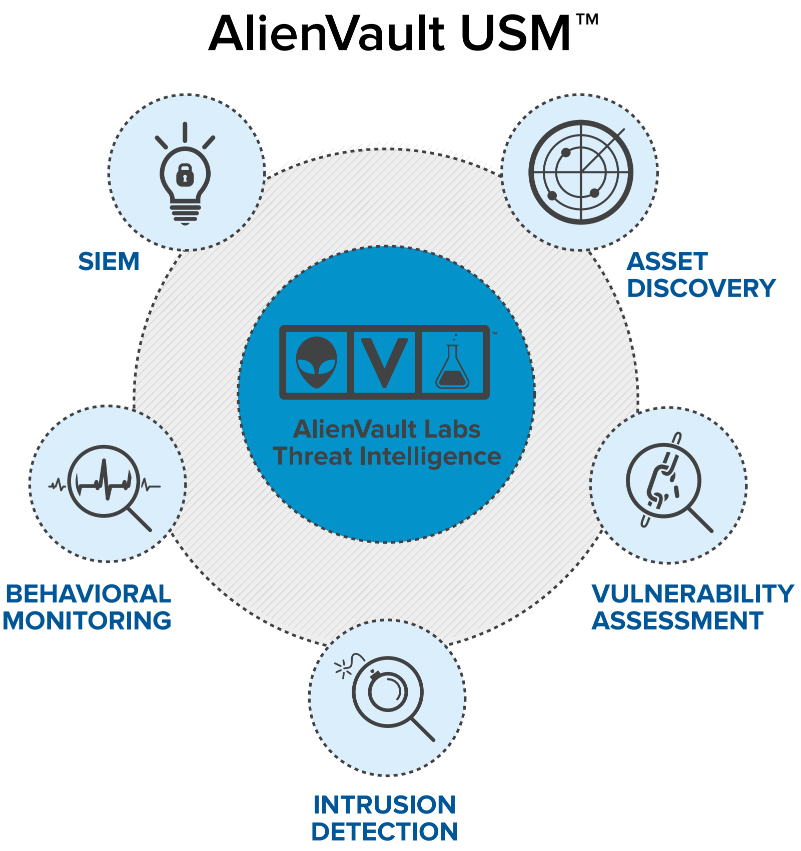
OTX is free to join. You can view all the WannaCry indicators of compromise (IoCs) in OTX here. >

3. Respond quickly to isolate your infected environments.

If you detect WannaCry in your environments, it's imperative that you respond quickly to isolate the threat and prevent it from spreading to other areas of your network. With USM, all asset, vulnerability, and threat data is available to you in a single pane of glass, which helps you to orient yourself to the threat quickly and take action sooner.

Continue reading this white paper to learn more about how AlienVault USM helps you to detect and respond to ransomware more efficiently.

Detecting Ransomware with AlienVault USM



Recent years has seen a marked increase in encrypting ransomware. Ransomware usually propagates as a trojan via email with an attachment or directing users to a malicious website for a drive-by malware download. Historically ransomware has primarily targeted Windows operating systems but Mac OS X variants have also begun to emerge. Typically, once the malicious file executes it connects to a Command and Control (C&C) server where the malware begins to encrypt specific file types on a system as well as shared drives. The ransomware demands payment to provide a password to unlock the encrypted files, or else it will continue to encrypt files until the system is unusable.

Outbound communication from an infected system is often difficult to detect due to ransomware employing techniques such as domain generation algorithms. The algorithm enables the ransomware administrator to create thousands of random domains every day. The same algorithm running on each infected system generates that same list of random domains, and each compromised system tries to connect to each of those domains until it finds the Command and Control (C&C) servers. This approach prevents the use of a blacklist to block the connection to a static IP address or domain.

How AlienVault USM Detects Ransomware

The USM platform uses several built-in technologies working in unison to detect advanced threats like ransomware. A unified approach is the most effective way to detect advanced threats because of its ability to collect log files from a wide range of data sources and correlate them. Event correlation is a technique for taking a large number of seemingly unrelated events across disparate systems and pinpointing the few events that are truly important in that mass of information. AlienVault USM correlation rules identify, isolate, and investigate indicators of exposure (IOEs) and indicators of compromise (IOCs) relating to ransomware.

The USM platform has all of the essential security controls built-in, with its capabilities continually enhanced by AlienVault Labs Threat Intelligence. You can also incorporate log data from virtually any third party security tools via the extensive plugin library, which allows you to preserve the value of previous investments.

The AlienVault USM platform uses a variety of technologies to gather information on a range of threat vectors to provide the 'who, what, where, when and how' of these attacks including:

- **Network Intrusion Detection (IDS)** analyzes the network traffic to detect signatures of known attacks and patterns that indicate malicious activity. Using field-proven IDS technologies, USM identifies attacks, malware, policy violations and port scans by performing signature, anomaly and protocol analysis.
- **Host Intrusion Detection (HIDS) and File Integrity Monitoring (FIM)** analyze system behavior and configuration status to identify suspicious activity and potential exposure. This includes the ability to identify the registry change required to initiate the ransomware's encryption engine.

- **Correlation Directives** – The AlienVault Labs Threat Research Team regularly adds ransomware-specific correlation directives 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

AlienVault Labs Threat Intelligence

Cyber criminals and attackers are constantly evolving their methods, making for a constantly evolving threat landscape. Organizations don't have the time or resources to continuously monitor the threat environment. Instead, they turn to AlienVault Labs to help detect the latest threats. The AlienVault Labs threat research team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape.

The AlienVault Labs team uses this diverse source of information to deliver regular threat intelligence updates to the USM platform. USM's integrated threat intelligence from AlienVault Labs eliminates the need for IT teams to spend precious time conducting their own research on emerging threats, or on alarms triggered by their security tools. The AlienVault Labs team regularly delivers threat intelligence as a coordinated set of updates to the USM platform, which accelerates and simplifies threat detection, prioritization, and response:

- **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
- **Reporting modules** – 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
- **Newly supported data source plug-ins** – expands your monitoring footprint

The AlienVault Labs team also utilizes the power of the Open AlienVault Threat Exchange (OTX). OTX is the world's first truly open threat intelligence community that enables collaborative defense with open access, collaborative research. There are over 1 million threat indicators submitted by the community to OTX every day, from over 26,000 participants in over 140 countries.

OTX is also integrated with the AlienVault USM platform, giving you additional insight into malicious activity targeting your network. The integration with OTX enables the powerful USM correlation engine to quickly identify attackers, their tools, their infrastructure who have previously attacked other members of OTX or engaged in other malicious activity. Using the threat intelligence in combination with behavioral correlation rules provides an accurate way to quickly identify known threats and known malicious actors.

You also have the ability to export indicators of compromise (IoCs) from OTX to almost any security product. OTX enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

Unified Security Management (USM)

The AlienVault USM platform provides a fast and cost-effective way for organizations with limited security staff and budget to address compliance and threat management needs. With all of the essential security controls built-in, the USM platform puts complete security visibility within fast and easy reach of smaller security teams who need to do more with less.

USM combines the following essential security capabilities, including SIEM, for single-pane-of-glass security visibility and management:

› Asset Discovery and Asset Inventory

- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Software Inventory

› Vulnerability Assessment

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning

› Intrusion Detection

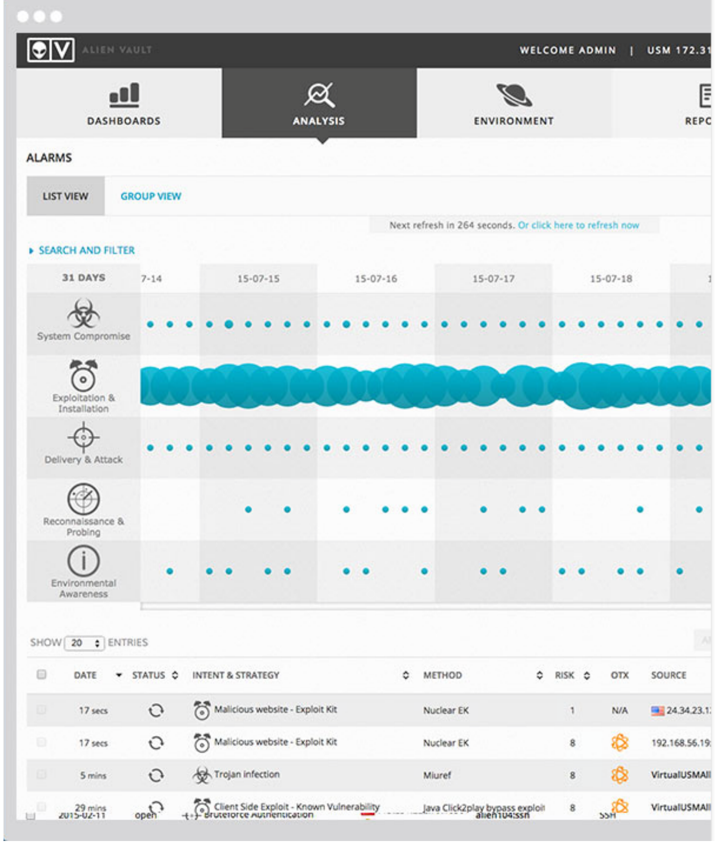
- Network IDS
- Host IDS
- File Integrity Monitoring

› Behavioral Monitoring

- Netflow Analysis
- Service Availability Monitoring

› SIEM

- Log Collection
- OTX Threat Data
- SIEM Event Correlation
- Incident Response



Next refresh in 264 seconds. Or click here to refresh now

DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE
17 secs		Malicious website - Exploit Kit	Nuclear EK	1	N/A	24.34.23.1
17 secs		Malicious website - Exploit Kit	Nuclear EK	8		192.168.56.19
5 mins		Trojan infection	Miuref	8		VirtualUSMAll
29 mins		Client Side Exploit - Known Vulnerability	Java Click2play bypass exploit	8		VirtualUSMAll

USM prioritizes alerts, from highest (System Compromise) to lowest (Environmental Awareness) telling your IT team what are the most important threats facing your network right now

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 SIEM, IT teams have to 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.

By providing built-in essential security capabilities and integrating threat intelligence from AlienVault Labs, the USM platform significantly reduces complexity and deployment time so that you can go from installation to first insight in about an hour.

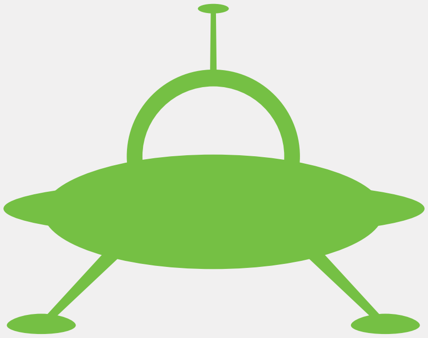
AlienVault USM Architecture

AlienVault USM is composed of three core components, each of which is available as a physical appliance or virtual appliance for maximum deployment flexibility.

1. **AlienVault Sensor:** Sensors perform four of the five essential capabilities of AlienVault: Asset Discovery, Vulnerability Assessment, Threat Detection, and Behavioral Monitoring. Sensor Processes perform initial processing (normalization) on that raw data, then transmit normalized events to the AlienVault Server for correlation and reporting.
2. **AlienVault Server:** The AlienVault Server provides a unified security management and configuration capability for all monitored assets. The Server receives normalized data from one or more Sensors, correlates and prioritizes the security events occurring across all assets, then displays these as alarms and security events in a variety of summary and detailed reports and dashboard views.
3. **AlienVault Logger:** The AlienVault Logger provides the Server with the ability to archive log files for purposes of forensic analysis and to fulfill compliance requirements for log archival and management.

The AlienVault Difference

The AlienVault approach delivers a unique solution to the challenge that under-resourced IT teams face when trying to secure their networks. We start with the USM platform, which is a built-in stack of integrated, essential security technologies. We add to it our experienced team of security experts, whose sole job is to analyze changes in the threat landscape. They then create the threat intelligence updates that are delivered regularly as a coordinated set of enhanced detection capabilities, advanced correlation rules and reports, that help our customers detect, prioritize, and respond to the most critical issues in their networks, such as ransomware.



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 crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures. For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).