BEGINNER'S GUIDE to

Ransomware Detection and Prevention

www.alienvault.com

Ransomware Basics

More than 4,000 ransomware attacks have occurred every day since the beginning of 2016[1].

What is it?

Ransomware is exactly what it sounds like. It's malware that blocks access to a victim's data or threatens to publish or delete their data until a ransom is paid (typically in Bitcoin payments). Because it can be an effective way to steal money (and trivial to do, thanks to Ransomware-as-a-Service offerings on the darknet market), its use is on the rise around the world.

Ransomware can have a huge impact on business operations. In fact, the latest high profile ransomware attack in May 2017—the WannaCry worm—had an enormous impact in a very short period of time. Within a day, WannaCry forced the National Health Service (NHS) in the UK to cancel thousands of operations and medical appointments due to these threats for ransom. Within hours, WannaCry was reported to have infected more than 230,000 computers in over 150 countries.

There are two main types of ransomware:

- **Extortion Attack** – holds the victim's data hostage through encryption
- **Leakware Attack** – threatens to publish the victim's exfiltrated data

In addition to WannaCry, some high-profile examples of Ransomware campaigns include Petya, Locky, TeslaCrypt, CryptoLocker, CryptoWall, and CryptoDefense

---

[1] Source: https://blog.barkly.com/cyber-security-statistics-2017

[2] Source: http://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126

[3] Sources: https://en.wikipedia.org/wiki/Ransomware; https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23

How Does It Work?

It's important to note that not all ransomware exploits work in precisely the same way—especially when it comes to the initial stages of an attack. For example, WannaCry does not rely on phishing its victims as an initial step, but rather executes brute force attacks against open and unprotected services such as RDP and SMB. With every malware attack, however, downloading and installing the malware is the crucial first step.

1. **Malware Delivery:** Somehow the attacker induces the victim user to download malware (or the malware is delivered via vulnerability exploit). A common method is via phishing—the user receives an email and clicks on a link that appears to be to a legitimate website (but it's not; it actually hosts an exploit kit). Or, as in the case of Petya, an infected software update carries the ransomware.

2. **Command-and-Control Server (C2) Connection:** Upon loading the page, the web server hosting the exploit kit begins communicating with the victim machine.

3. **File Execution and System Compromise:** If a vulnerable version is confirmed, the kit attempts to exploit the vulnerability.

4. **File System Encryption:** Once the victim system is compromised, the filesystem is encrypted, and the malware sends the encryption key and host-specific info back to the attacker's C2 server.

5. **User Notification:** The attacker's server then sends a message to the victim alerting them that their data is being held hostage and issuing directions on how to pay. To add urgency, the ransomware will often include a countdown clock ticking down the minutes before the data is destroyed.

Who are the Attackers?

Ransomware, by nature, is a type of financial exploitation, and the attackers behind ransomware campaigns are most often profiteers, rather than nation state or cyber espionage actors. While ransomware campaigns originate from locations all over the globe, ransomware hackers rely on countries with lax cybersecurity laws and accessible bitcoin markets to shield their malicious endeavors. Also, well-known organized cybercrime groups like Janus Cybercrime Solutions have been known to author ransomware campaigns.

Thanks to the recent rise of Ransomware-as-a-Service (RaaS), nearly anyone with criminal intent can get into the ransomware attack business. Advanced malware authors write the ransomware code and then offer it for free or charge a small fee, opting to take a portion of the ransom as a profit. Because the barrier to entry is so low, cyber criminals are incentivized to increase their volume of attacks and ask for higher ransom requests. And because Bitcoin is an anonymous payment service, the risk of getting caught is also very low.

Who Have Been Targeted?

Unlike other types of cyber attacks (e.g. ATM skimmers), ransomware attackers don't seem to have a preference for financial services and retail, but rather, they attack all sizes and types of organizations. Some of the more high profile (and heart-wrenching) ransomware attacks have been against hospitals, notably because their need to restore services (and pay the ransom) is literally a matter of life and death. The WannaCry worm hitting the UK's National Health Service (NHS) is a recent example of this, forcing NHS to cancel operations and appointments at its hospitals across the country.

How Often is it Successful?
How Much Does it Cost the Average Organization?

It's often successful, which is why it's on the rise. According to a June 2016 survey from Osterman Research, nearly one in two participants indicated that their organization suffered at least once ransomware attack in the last year[4]. In the first quarter of 2016, companies paid an estimated $325 million in ransom, and the number of attacks grew from 30 million to over 260 million by the fourth quarter[5].

What Can You Do to Stop It?

There are some best practices you can put into place to avoid being the next victim of a ransomware attack. We've assembled the eleven best practices for detecting ransomware and preventing it from infecting your business.

[4 / 5] Source: http://www.armadacloud.com/roundup-ransomware-statistics-2016/

Ransomware Detection: Top 6 Best Practices

It's important to detect ransomware as quickly as possible—in order to isolate the infected systems and minimize the attack's ability to spread as much as possible. In a recent SANS Institute survey[6], 54% of respondents indicated that it took more than two days from initial compromise to detection, yet a ransomware attack can encrypt a filesystem in minutes. Therefore, real-time ransomware detection is crucial.

1. Perform Asset Discovery and Vulnerability Scans

Knowing what's on your network and in your public and private clouds at all times is essential in order to understand the scope of any security incident. Since the goal of a ransomware attack is to steal your most valuable assets—your data and applications—having an updated and reliable asset inventory to start with provides the security team with the certainty they need in the event of an attack.

Additionally, periodic vulnerability assessments are critical so that as new vulnerabilities and exploits are discovered, vulnerable assets can be patched or reconfigured to address these risks.

AlienVault® USM™ automatically discovers assets across your networks and clouds to build an always updated asset inventory.

Learn More >

[6] Source: https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

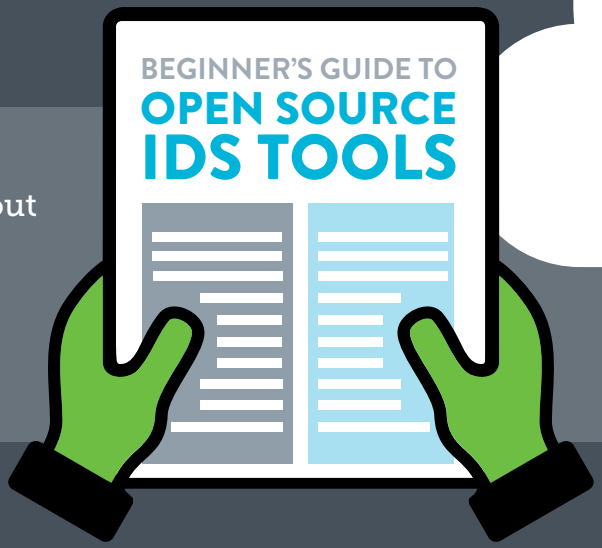
2. Implement Intrusion Detection

While ransomware can be difficult to detect before it's too late, it's not impossible. If you know what to look for, and you have the right intrusion detection technology in place (Cloud-based IDS, Network-based IDS, and Host-based IDS), you can act quickly to contain the damage and quarantine the infected systems. Some examples of ransomware signature behaviors include:

- Communication with an IP or domain with a bad reputation (e.g. Command-and-Control or C2 Server)
- Forcing group policy updates to fail
- Sending data via a covert channel
- Updating an audit policy
- Disabling firewall or antivirus software
- Running unauthorized or unexpected network scans

AlienVault USM includes Cloud-based IDS, Network-based IDS, Host-based IDS technologies to alert on any behavior consistent with ransomware and other malicious activity patterns.
Learn More >

You might also want to check out our Beginner's Guide to Open Source IDS Tools
Read Now >



3. Enable File Integrity Monitoring

Ransomware, like most malware, will kick off system processes and access system files that aren't necessarily part of normal system operations. With File Integrity Monitoring (FIM) technology, you'll be alerted any time a critical system file is accessed, modified, or otherwise messed with. Once the encryption process is kicked off, you may not save that particular system... but once alerted, you can prevent the further spread of the ransomware attack by rapidly isolating and quarantining the compromised system.

AlienVault USM includes File Integrity Monitoring to detect critical changes in real-time. Learn More >

4. Implement Security Automation and Orchestration

Rapid response is a critical success factor in any type of emergency, and a ransomware outbreak is no exception. The faster you can detect and respond to a potential ransomware attack, the more likely you can contain the damage. Unfortunately, cyber security defenses are often a patchwork of controls and consoles, making it difficult to respond quickly and in a coordinated way when attacks happen.

Recent innovations in security automation and orchestration have enhanced incident response by allowing disparate security tools to work together more effectively—all from a single management platform. For example, AlienVault USM Anywhere's architecture makes it possible to readily extend the platform's capabilities through modular software components called AlienApps™. AlienApps interact with other IT security and operations products to help unify your security architecture from a single platform, and centralize your orchestration of incident response activities.

With AlienVault USM Anywhere, you can leverage security automation and orchestration features to disable network access or isolate an endpoint as soon as ransomware activities are detected, like network communication with a known C2 server. Learn More >

5. Conduct Log Monitoring and Analysis (via SIEM)

Hidden inside system logs, application logs, and access and activity logs lie the breadcrumbs of every cyber security attacker. The challenge in detecting that attacker's breadcrumbs is similar to finding a needle inside a haystack. The sheer volume and endless variety of event log data makes it essential to have an automated event correlation solution (e.g. SIEM) to parse through those haystacks and alert you when ransomware attacks happen so you can stop them from propagating.

AlienVault USM collects and aggregates disparate event log data and then applies event correlation rules to find risk "signals" consistent with ransomware (and other attacks) amidst the noise of all of that data. Learn More >

You might also want to check out our Beginner's Guide to SIEM - Read Now >

6. Integrate Security Monitoring with Updated Threat Intelligence

Attackers who conduct ransomware attacks have an entire ecosystem at their disposal, and they're constantly evolving their methods. Security researchers (like those on the AlienVault Labs Security Research Team) have studied their tradecraft and infrastructure in depth, and continue to monitor their attributes, activities, and innovations. These insights translate into tuned security controls (e.g. event correlation rules) to detect the latest ransomware attacks, as well as understand how an attacker's TTPs (tools, techniques and procedures) work for an enhanced response.

Continuous threat intelligence updates can help you stay ahead of emerging threats. Weeks in advance of the global WannaCry outbreak, for example, the AlienVault Labs Security Research Team updated relevant IDS signatures in the Threat Intelligence Subscription so that AlienVault USM customers would be alerted to the vulnerability exploit leveraged by WannaCry.

AlienVault USM includes built-in threat intelligence updated continuously by the AlienVault Labs Security Research Team.
Learn More >

You might also want to check out our Beginner's Guide to Threat Intelligence - Read Now >

PRO TIP: Use a Consolidated, Multi-functional Platform

Each of the above tasks are essential for detecting ransomware quickly enough to protect your data, and for effective security orchestration and fast response, you'll need a unified view. One of the challenges with legacy security technologies is that each of these capabilities is delivered and managed via a single product and UI, which makes getting a complete and unified picture very complicated and time-consuming. And the last thing you have an unlimited supply of, is time. Thankfully, **AlienVault USM** delivers all of the above ransomware detection capabilities from a single management console for unified visibility and rapid response.

Ransomware Prevention: Top 5 Best Practices

1. Conduct End User Security Training

Since most ransomware attacks take advantage of unsuspecting users clicking without thinking[7], educating users is the best first step you can take to combating ransomware. Phishing and spear-phishing techniques that often kickstart ransomware campaigns can't be successful if users are more skeptical of what they see or receive online. The SANS institute has some excellent resources and KnowBe4 even offers a **free ransomware simulation tool**.

2. Set up Reliable Backup and Recovery Procedures (and test them)

In a scenario where you may lose all of your currently accessible data unless you pay, having a reliable backup certainly gives you much more confidence in refusing to pay up[8]. Unfortunately, many organizations either don't do regular system backups, or they do them but never test their recovery procedures. During an emergency (like a ransomware attack) is the worst time to try your recovery procedures for the first time. So now, while it's nice and quiet, schedule regular system backups and test these procedures with system recovery testing. Find out where things break down and continually refine these procedures so you'll be ready if/when there's an emergency.

3. Establish Good Hygiene Practices for Your Endpoints

Ransomware and other malware attacks exploit endpoint vulnerabilities and insecure configurations. Unlike broad-based network attacks (e.g. Distributed Denial of Service or DDoS), ransomware attacks target endpoints because that's where the data lives, and that's what the user uses. Even though it's rather boring, the best fix for ransomware attacks is simply better endpoint security hygiene. Installing application and OS patches as soon as they're available is one of the best ways to prevent ransomware attacks. Another is to disable macros on MS Office applications, as well as remove any and all software that's not necessary.

---

[7] Locky is a good example. It spreads through emails that contain fake invoices as attachments.

[8] Of course, even if you do have a good backup and can recover it, any ransomware attack threat will incur some downtime.

AlienVault USM makes it easy to identify unnecessary or unauthorized software via the automated asset discovery and inventory feature that we covered in the first section of this guide. Learn More >

4. Implement Continuous Vulnerability Assessment

The WannaCry worm—one of the highest profile ransomware attacks—was so successful because it exploited the MS17-010 SMB protocol vulnerability. This vulnerability is very old, very well-known, and affects multiple versions of the Microsoft Windows OS[9]. Regular and continuous vulnerability assessment scanning will identify app, OS, and network vulnerabilities across your assets, so that you can prioritize remediation efforts that can prevent ransomware (and other types of malware) attacks.

[9] For more information on this vulnerability and how to mitigate it, please see: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

AlienVault USM includes its own built-in vulnerability scanning tool to assess whether your systems and devices are currently at risk. Because the USM platform receives continuous threat intelligence updates, including the latest vulnerability signatures, users have the assurance that their vulnerability scans use the latest known vulnerability signatures. Learn More >

5. Block and Filter Outbound Connections (Not Just the Inbound Ones)

As we explained earlier, one of the first stages of a ransomware attack involves the infected endpoint initiating connections outbound to the attacker's C2 server(s). If you block these connections at your gateway, you've effectively disrupted the ransomware attack before it can ever get started. It's also a good idea to set up alerts when these connections are initiated so that you can investigate and correlate these connections with known bad actors.

AlienVault USM—integrated with integrated threat intelligence from the AlienVault Labs Security Research Team, backed by the Open Threat Exchange® (OTX™), flags IP addresses and domains that are known bad actors, alerting you to potentially dangerous network activity.

PRO TIP: Segment Your Network

Nearly every malware attack involves establishing a "beachhead" or compromised system, and then probing the rest of the internal network from this privileged position. Reconnaissance activity like this is not very successful on networks with effective segmentation and isolation. In fact, it doesn't work at all. Explore ways to segment your network to optimize performance as well as improve security.

Unify Your Ransomware Defenses with AlienVault USM

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 the AlienVault Labs Threat Intelligence Subscription. You can also incorporate log data from virtually any third party security tool through the extensive plugin library, which allows you to preserve the value of previous investments.

Essential Security Controls

The AlienVault USM platform provides a fast and cost-effective way for organizations with limited security staff and budget to address emerging risks like ransomware attacks. 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. AlienVault USM combines the following essential security capabilities for single-pane-of-glass security visibility and management across on-premises and cloud environments.

Asset Discovery and Asset Inventory
Get visibility into the assets and user activity in your cloud and on-premises environments.

Vulnerability Assessment
Scan your cloud and on-premises environments to detect assets, assess vulnerabilities, and deliver remediation guidance.

Intrusion Detection
Inspect traffic between devices and protect critical assets and systems in your cloud and on-premises environments.

Behavioral Monitoring
Identify suspicious behavior and potentially compromised systems.

SIEM
Correlate and analyze security event data from across your cloud and on-premises environments.

Integrated, Actionable Threat Intelligence to Combat Ransomware

The secret sauce of the AlienVault USM platform lies in its ability to operationalize dynamic threat intelligence updates, continuously delivered by the AlienVault Labs Security Research Team. The technologies that power the platform come to life with the collaborative content made possible by the AlienVault Labs Team along with the members of the AlienVault OTX community.

This content is comprised of the following:

- **Correlation Directives** – these translate raw events into actionable remediation tasks. The AlienVault Labs Security 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
- **Network and Host IDS Signatures** – these detect the latest threats in your environment including fast moving worms like WannaCry
- **Asset Discovery Signatures** – to identify the latest OSs, applications and device types
- **Vulnerability Assessment Signatures** – to find the latest vulnerabilities on all your systems
- **Reporting Modules** – to provide new ways of viewing data about your environment and / or meeting compliance requirements
- **Dynamic Incident Response Templates** – to deliver customized guidance on how to respond to each alert
- **Newly Supported Data Source Plug-ins** – to expand your monitoring footprint

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. 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.

ALIEN VAULT