**SECTION 0: Company Background**

Pegasus Financial is a leading provider of cloud-based accounting software to help drive our customer’s financial operations forward. Our automated accounting system help companies navigate the shifting challenges and opportunities your accounting team faces every day. Our software handles the basics – like inventory, accounts payable, accounts receivable, general ledger, and purchasing – as well as sophisticated challenges like contract and subscription billing, revenue management, project billing, and other issues facing small businesses.

*Core Financials:*

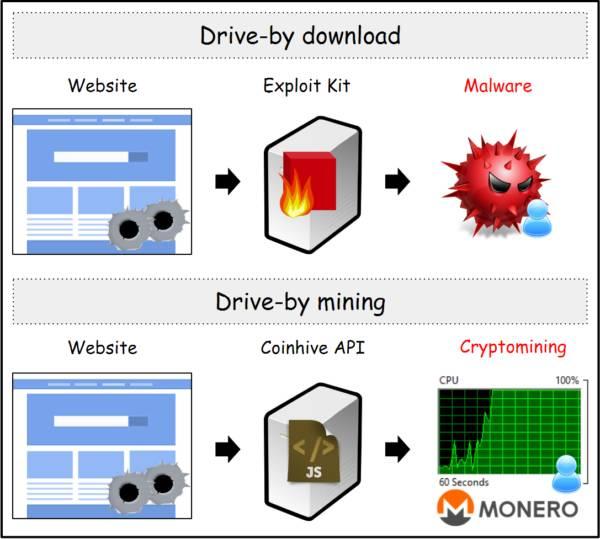
* Accounts Payable
* Accounts Receivable
* Cash Management
* General Ledger
* Order Management
* Purchasing
* Reporting and Dashboards
* Spend Management

Our mission is to provide our customers with a seamless experience their accounting services and financial reporting needs.

**SECTION I: Overview of Malware**

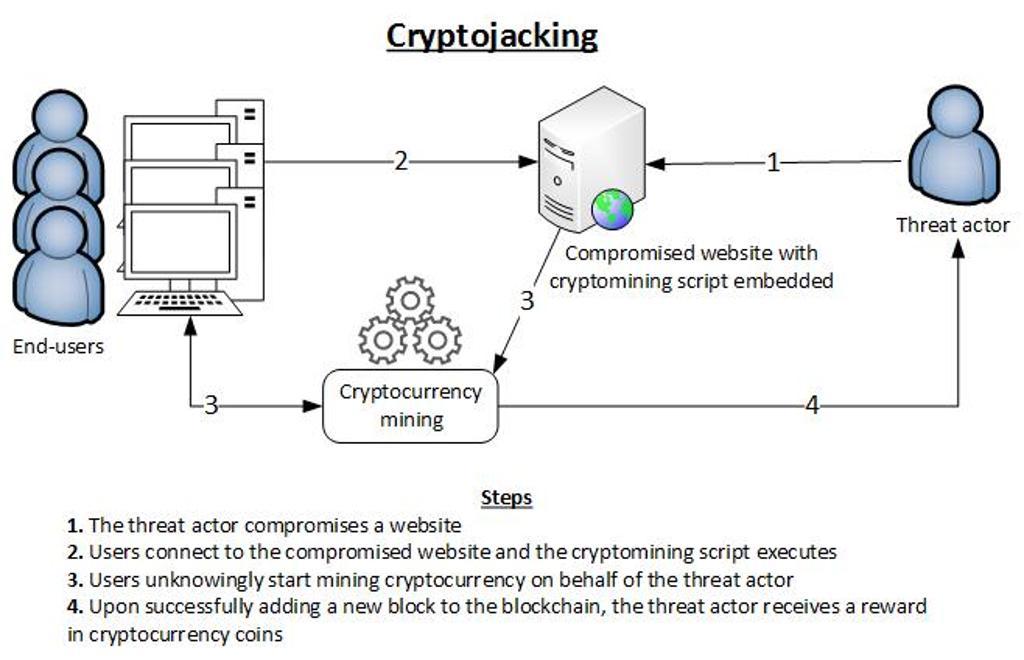
On March 29th, 2019, the Secure Shell Horse (SSH) team discovered a strain of a Linux coinmining malware from the Monero cryptomining malware family on a number of our Linux and Windows machines we are dubbing Pegasus Cryptojacker. The malware was a script in the form of a JavaScript code that exploited a zero day Oracle Weblogic vulnerability (CVE-2017-20171) that allows an unauthenticated attacker with network access to T3 to download cryptojacking malware. We were able to trace the infection back a compromised website <cryptcrisis[dot]com>, which was visited by a number of employees on March 24th. This web-based attack, or Drive-by mining (Figure 1), infected our servers upon visiting the site, gained administrative privileges, and removed our Threat Detection Service agent. Once the agent was disabled, the crytojacking malware was downloaded and installed to begin mining Monero cryptocurrencies.

*Figure 1: Malware vs Cryptomining Comparison*



Based on our analysis, the malware’s ultimate purpose is to mine Monero cryptocurrency using resources that the threat actor is not authorized to access. Once mined, the coins are sent back to the attacker. Monero coin is specifically used because it is the most liquid of cryptocurrencies and user data and ledger are obscured. As noted earlier, the initial infection is web-based, meaning no file is initially downloaded to begin the attack. Rather, the infection begins upon visiting a compromised website, which then opens a backdoor to download the crypto mining malware. In addition, there was code discovered that removed our Cloud Workload Protection (CWPP) products from the compromised Linux servers. Rather than compromising these security products, the malware gained full administrative control over the hosts and then uninstalled these products in the same way a legitimate administrator would. In addition, our research indicated that the malware can also kill any cryptojacking processes that may already be affecting servers, essentially rooting out any competition.

*Figure 2: Cryptomining Malware Diagram*



The malware family is suspected to be developed by the Iron cybercrime group and is also associated with the Xbash malware that was initially report by Palo Alto’s Unit 42 in August of 2018. During our analysis, we discovered that the malware was used by a threat actor that goes by the name the Rocke group. This threat actor engages in distributing and executing crypto mining malware using a variety of threat vectors including, but not limited to: Git repositories, HttpFileServers (HFS), and various payload types (shell scripts, JavaScript backdoors).

The Rocke group initially was reported on by Cisco’s Talos in April 2018 through the use of honeypot systems vulnerable to an Apache Struts vulnerability. In late July, the same group engaged in a similar campaign which allowed Talos to collect more information about the threat actor, including the threat actor’s MinerGate Monero wallet email rocke@live.cn. Talos discovered that Rocke’s command & control (C2) was registered to the address jxci@vip.qq.com. Through a leak that was captured from the Chinese security site Freebuf, a user name “rocke” was associated with this email address. Rocke has been seeking access to cloud storage services, as well as obtaining manuals for programming in the Chinese Easy language. Additionally, Talos discovered a GitHub page with repositories showing this threat actor has become interested in browser-based JavaScript mining through the tool CyrpoNote, as well as browser-based exploitation through the Browser Exploitation Framework.

The malware affected the company in the following manner: (1) employees noted a disruption in productivity was noted because our computing resources were being utilized by the cryptojacking malware; (2) Customer support metrics noted an increase in technical support calls and help desk tickets noting slow service; (3) facilities noted a spike in electricity usage, and (4) the malware successfully gained administrative privileges on the infected devices. The fourth point highlights the skill level of the threat actor and the danger of this strain of malware.

Oracle issued a Critical Patch Update on October 2017 to patch the WLS Security component affected on the Oracle WebLogic Server. Once installed, this patch addressed the exploit and the risk should remain low going forward.

**SECTION II: Technical Exposé**

This document summarizes our analysis of <Pegasus Cryptojacker>, and contains the following:

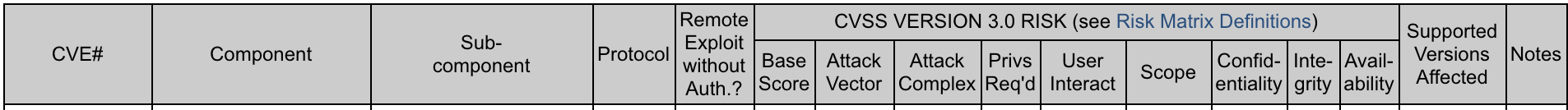
* Static Analysis
* Dynamic Analysis
* Summary of Functionality

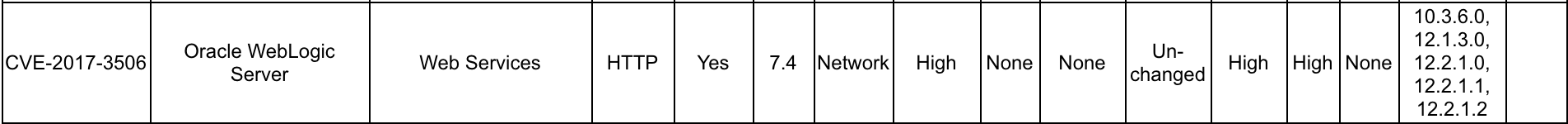
This analysis was performed using the static and dynamic analysis results furnished by Any.Run and VirusTotal.

**Static Analysis**

**Synopsis of Executable**

This section contains a summary of the uploaded executable: Pegasus\_cryptojacker





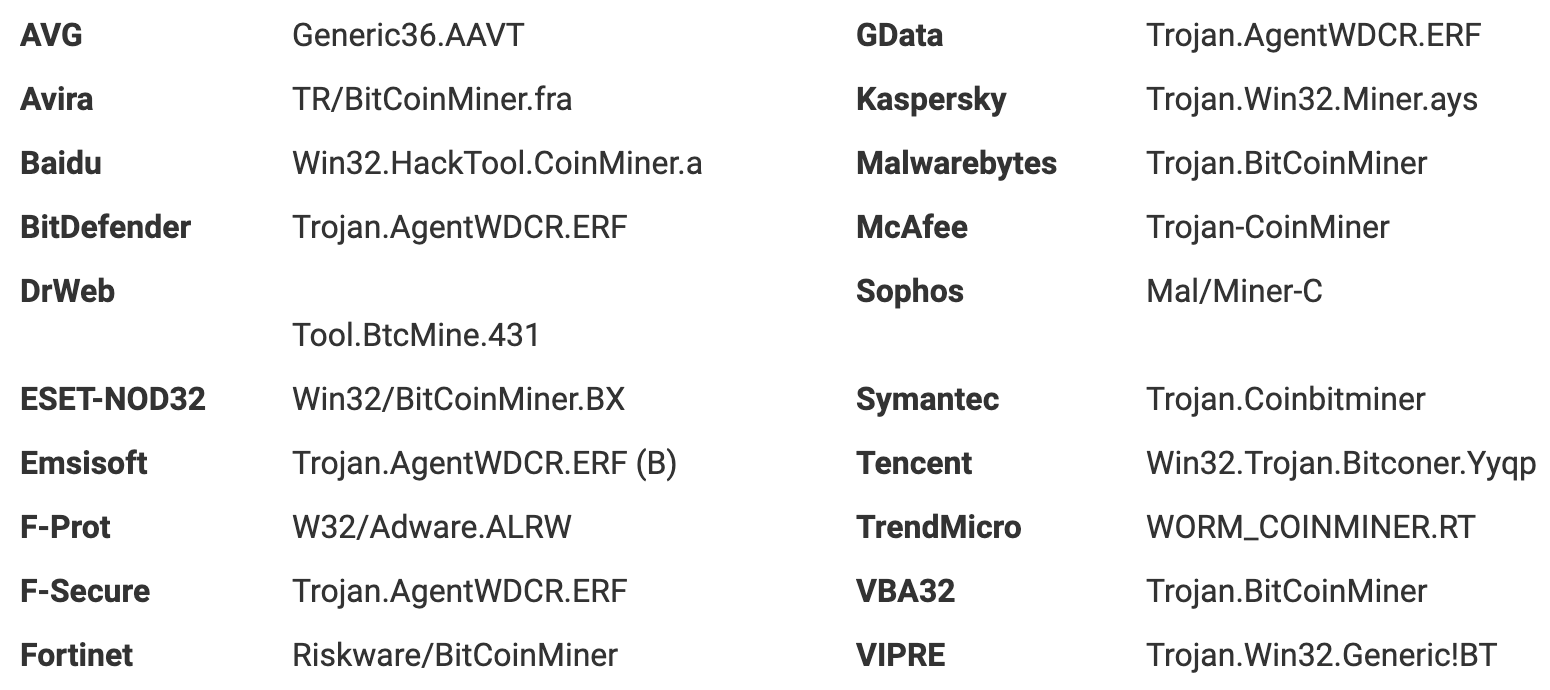
The file type and file size - Initially it is a JavaScript code that determines OS and deactivates cloud security programs. Then downloads cryptominer malware in form of PE32 or Portable Executables for 32 bit machines

Compilation date - 06-Feb-2016 21:24:54

### **Risk**

While many companies may not see cryptominers as a big threat, this is indeed a high priority threat that should be taken seriously. This particular strain of malware can obtain elevated privileges which can ultimately lead to extremely detrimental activity for the company. With admin access the attacker can implement a DDoS attack or affect the integrity of our data as well as confidential client data. For these reasons we rate this 7.5 High risk. Remedial action should be taken immediately.

Most Antivirus software will detect the network trojan for Windows machines. Here is a list of AV’s and their description for this particular malware



**Initial Behavior**

The table below summarizes the initial activity generated by the sample upon upload to Any.Run.

|  |  |
| --- | --- |
| **Activity Type** | **Count** |
| HTTP Requests | **47 Requests** |
| DNS Requests | **84 Requests** |
| Connections | **6609 TCP/UDP connections** |
| Files Changed | **2216** |

Once the C2 connection is established, malware used by the Rocke group downloads shell script named as “a7” to the victim machine. The behaviors of a7 include:

* Achieve persistence through cronjobs
* Kill other crypto mining processes
* Add iptables rules to block other crypto mining malware
* Uninstall agent-based cloud security products
* Download and run UPX packed coin miner from blog[.]sydwzl[.]cn
* Hide process from Linux ps command by using the open source tool “libprocesshider” with LD\_PRELOAD trick
* Adjust malicious file date time

**Dynamic Analysis**

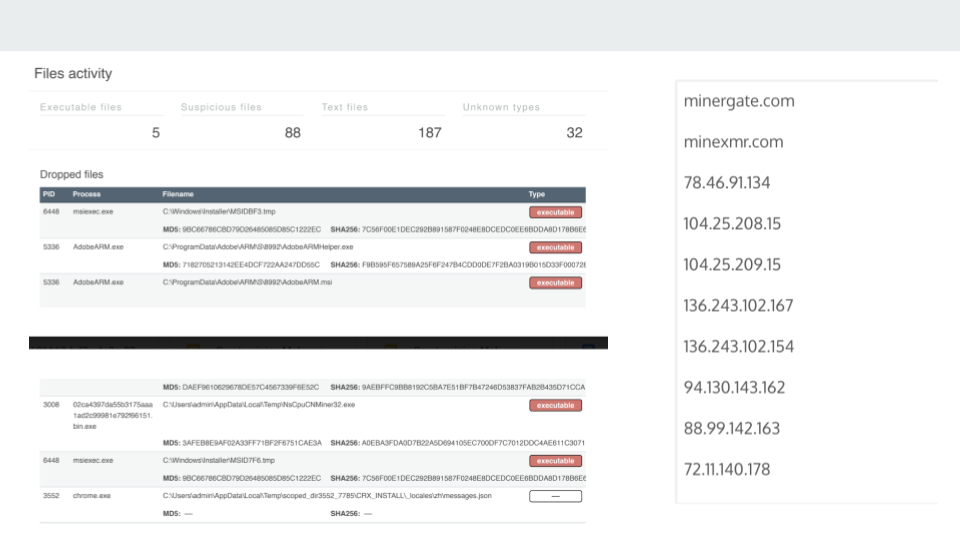
This particular cryptominer that generated Monero affected mainly two types of machines in our company: Linux machine and Windows Machine. We performed our Dynamic Malware analysis using a tool called Any Run and we observed the following facts :

* Process Environment helps to understand how the operating system is affected, which helps to understand what has been done to generate cryptocurrency like Monero.
  + Linux Machines Affected software: WebLogic Server 10.3.6.0.0 , 12.1.3.0.0, 12.2.1.1.0,12.2.1.2.0
  + Window Machine: Total Processes:632,Monitored Processes:570,Malicious Processes: 1 Suspicious Processes:0
* Network Activity can analyse how the malware makes the HTTP Request which block some website or to redirect it or how works with DNS setting to divert it into the particular Mining domain
  + Linux Machine: Affected Domain Names and IP Addresses minergate.com,minexmr.com,78.46.91.134,104.25.208.15,104.25.209.15,136.243.102.167,136.243.102.154,94.130.143.162,88.99.142.163,72.11.140.178

Weblogic vulnerability CVE-2017-10271 in Linux machines.

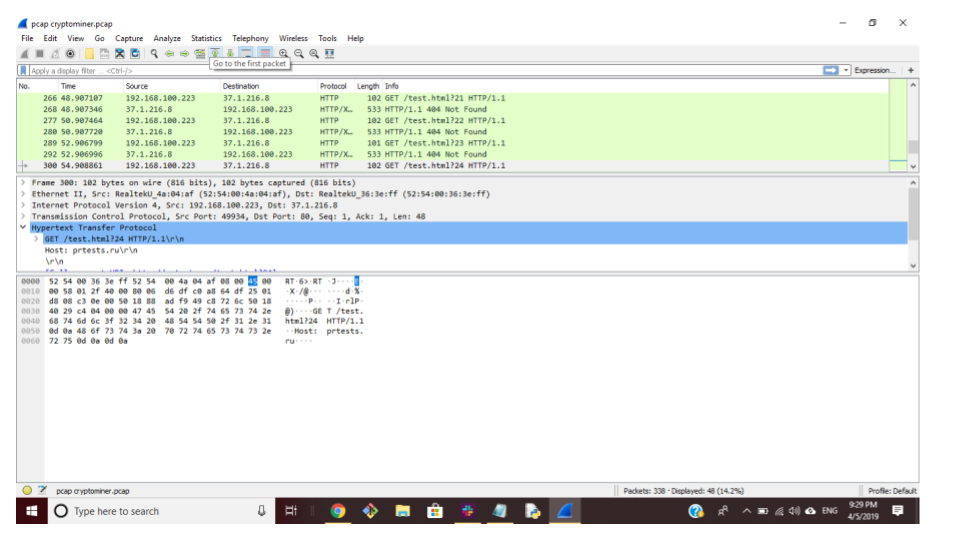
* + Window Machine: Http(s) Requests :47,TCP/UDP connections: 6609,DNS Requests :84, Threats :24
* Filesystem Modifications can change the file system mainly in Root directory for the mining to be done . Malware mainly changes file of root directory as its very difficult to identify it.
  + For a Linux host, first, check the /tmp directory for suspicious files owned by any WebLogic account, such as watch-smartd, Carbon, and default.
  + Window Machine: Executable Files: 5,Suspicious Files 88, Text File 187, Unknown Types 32

*Figure 3: Screenshot of Modified File Activity*



Next, we analysed a PCAP file and found the suspicious files where the malware injected itself.

*Figure 4: Screenshot of PCAP File*



The HTTP Content tab shows where the webcontent modified

**Summary**

Monero is the cryptocurrency built on blockchain technology and cryptography. Cryptomining malware infects the large pool of computers mainly by utilizing the CPU resources without the knowledge of users by some code or script to generate the Monero coin. The Pegasus Cryptojacker malware payload is delivered as a PE32 on Windows machines and on Linux machines it is saved in /tmp file under various names such as watch-smartd, Carbon, and default.

The prominent signs of this malware are that it spikes in CPU usage, which is being utilized for cryptomining. There are network connections being made to Monero mining sites. The machine’s cloud security has been shut off via admin access. Finally there are some unusual redirects in HTTP requests which are typically to other compromised sites.

|  |
| --- |
|  |
|  |

### **Linux vs Windows**

This malware campaign involves two different types of malware which target two different operating systems, Linux and Windows. Despite their similarities, there are some distinct differences between them.

* The Linux Cryptojacker mines Monero , Hijacking user’s computing power,
* The exploit depends on one of two Linux vulnerabilities being open to form an attack vector, which are , CVE-2016-5196, CVE-2017-20171 and CVE -2013-2094 According to the widely referenced exploit tracking website cve.mitre.org,
* Cryptomining malware: refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission

**SECTION III: Containment Strategy**

This section contains counsel as to the scope and severity of infections by Pegasus Cryptojacker, as well as steps to fix infected computers and prevent future attacks.

**Scope**

Cryptominers solve complex cryptographic puzzles and intentionally requires resource-intensive computation. Instead of investing in data-centers, crypto-mining criminals cut that corner by hacking into other people and groups’ machines, and criminally exploiting their CPU power without the user’s consent or knowledge.

The Pegasus Cryptojacker malware targets cloud infrastructure running on Linux servers. Specifically, it targets the Oracle WebLogic servers versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0, 12.2.1.2.0. The malware utilizes the T3 protocol to install a backdoor on the system and use it to download crypojacking malware.

**Severity**

The damage caused by the Pegasus Cryptojacker can be different – from insignificant increase in outgoing traffic to the complete network breakdown or the loss of critical data. The scale of the damage depends on the targets of the malware and sometimes the results of its activity are imperceptible for the users of a compromised machine. In the case of Pegasus Cryptojacker, the following was noted:

* *Slow down in network* - The failure or dramatic slowdown of an individual computer or network can be premeditated or accidental. A virus or a Trojan may delete critical system elements, thus disabling the OS, overload the network with a DDoS attack, or otherwise negatively affect the system’s operability.
* *Caused machines to heat up* - A virus, worm or other type of malware can cause a computer to overheat by causing the processor to max out. By continually maxing out the capacity of the computers CPU, the system can and eventually will overheat and could unexpectedly shut down. Another big culprit of an overheating computer are non-functioning fans.
* *Attacker on the network* - Usually using a Monero client, users can download media via peer-to-peer file sharing. However, these files tend to travel across multiple computers, which probably don’t all have Internet security software, so they are easily infected with malware. Additionally, hackers will set up fake files on these networks that are based on popular downloads that are actually malware in disguise.
* *Back door can lead to more malicious malware* - Access to a computer system or encrypted data that bypasses the system's customary security mechanisms. However, attackers often use backdoors that they detect or install themselves as part of an exploit.

**Level of Difficulty to Remove Malware**

Removing a cryptominer can be difficult without the help of malicious software removal tools. Some computer viruses and other unwanted software reinstall themselves after the viruses and spyware are detected and removed. Fortunately, by updating the computer and by using malicious software removal tools, SSH was successful in permanently removing unwanted software.

Since the Oracle WebLogic Server was not patched, our analysis found that it’s increased activity was caused by cybercriminals engaging in cryptomining. SSH noted a large spike in the number of devices scanning the internet for port 7001/TCP. Additionally, there was a vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (WLS Security). Supported versions that are affected are 10.3.6.0.0 and can be easily exploitable. The vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

**Exposure of Full Root Shell**

The vulnerability affects Bash, a common component known as a shell that appears in many versions of Linux and Unix. Bash acts as a command language interpreter. In other words, it allows the user to type commands into a simple text-based window, which the operating system will then run. Bash can also be used to run commands passed to it by applications and it is this feature that the vulnerability affects. One type of command that can be sent to Bash allows environment variables to be set. Environment variables are dynamic, named values that affect the way processes are run on a computer. The vulnerability lies in the fact that an attacker can tack-on malicious code to the environment variable, which will run once the variable is received.

In other words, this malware gave the attacker elevated privileges to access much more than virtual access to the CPU. A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications. Not every system hack will initially provide an unauthorized user with full access to the targeted system. In those circumstances privilege escalation is required: vertical and horizontal.

Vertical privilege escalation requires the attacker to grant himself higher privileges. This is typically achieved by performing kernel-level operations that allow the attacker to run unauthorized code. Horizontal privilege escalation requires the attacker to use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges

Based on the above, we conclude that this sample is of **High** severity, and should be patched **Immediately**.

**Solution**

The following are activities that should be carried out during the containment stage:

Identify infected systems  
Clearly identifying the infected systems is always the first step in containment. Unfortunately it is also a very complicated process due to the dynamic nature of today's IT environment. The following actions are required:

* Computers that have been infected must be disconnect the computer from the network.
* Bring the computer(s) to the security team for malware removal and virus scanning on all the systems with the latest virus signatures as well as with updated anti-virus detection and repair engines.
* As no single anti-virus software or malicious code detection tool can uncover all types of malicious code, it may be necessary to use more than one anti-virus scanning tool to ensure that all malicious codes are detected.
* Monitor network to verify whether it has spread to other servers review all log files of routers and firewalls.
* Configure IPS or IDS to identify activities associated with infections.
* Perform packet sniffing routines to look for the network traffic matching the characteristics of the malicious code.

Contain the outbreak

Containing the outbreak can be done in various ways;

* By using automated tools: Containing the spread of malicious code can be done with automated tools, such as anti-virus software or malicious code detection tools, IDS and IPS.
* By disabling connectivity: If there is an infected computer, it must disconnect from the internet so the malicious code outbreak can be effectively contained from the overall network infrastructure, which can be accomplished by applying access controls on network devices or physically disconnecting network cables.
* By disabling services and shut down infected servers: Malicious code may propagate through network services, for example network shared drives. Temporarily blocking or even shutting down the network services used by malicious codes helps to contain incidents.
* By eliminating vulnerability and Implement patch: Malicious code may spread by attacking vulnerable network services. By addressing the vulnerabilities that have been exploited by malicious code, such as applying security patches on vulnerable systems, the propagation channels can be eliminated.
* By user participation: By provide users with instructions on how to identify infections, user participation is significant to the containment process in an environment where only a limited number of technical support staff are available to handle an outbreak, for example in small remote branch offices or in a non-managed office environment.

Keep records of all actions taken

It is important to keep a solid record of all actions taken at this stage, because some containment measures may require temporary modifications to the configuration or settings of network infrastructure and systems. These modifications will need to be removed after the incident.

Conclusion

It is also important to understand that stopping further infection by malicious code does not necessarily prevent further damage to infected systems. For instance, the infection can be contained through disabling network connectivity. Yet, the malicious code may be still actively deleting files on the infected system. Therefore, a full eradication process should be carried out as soon as possible or in parallel with the containment process.

**SECTION IV: Awareness Training**

This document explains how end users can

* Identify an infection by Pegasus Cryptojacker
* Protect your data and isolate the infected machine
* Determine which organizational stakeholders to notify in the event of a compromise

**Identification**

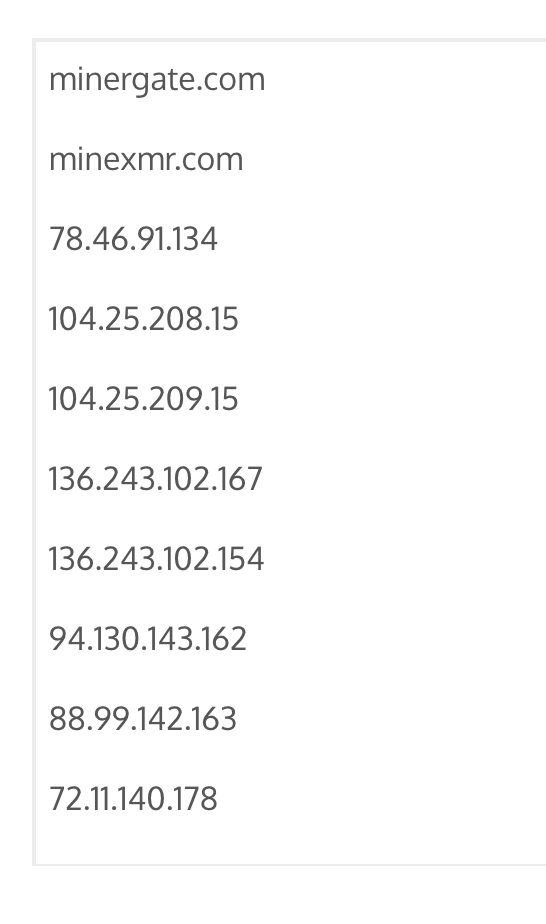
The findings from the analysis of Pegasus Cryptojacker has helped us to create this list of suspicious machine behaviors that may indicate you have been infected. Be on the lookout for the following:

* Machine becomes uncharacteristically hot
* CPU fan becomes louder/faster
* Network speeds seem to slow drastically
* Processes take longer than normal
* When using the process monitor, you notice a spike in CPU usage

All of these may be signs that you have been infected with a cryptojacker. Contact your local security team if you suspect infection.

**Suspicious Network Traffic**

Through the dynamic analysis of this cryptojacker, we have identified the following websites and IP addresses to be specific to this malware. If any of these are detected on the network, take immediate remedial action.

****

**Quarantine and Response**

In the event of an infection, the following are the steps we have identified to quarantine the threat and prevent the spread of the malware:

* Identify all infected machines on the Network
* Disconnect the infected machines from the network
* If the malware has spread to servers, move the uninfected machines to the backup servers to prevent disruption of service
* Update Oracle WebLogic software to latest which has a patch for the vulnerability
* Alternatively you can also search for and delete the malware files: For a Linux host, first, check the **/tmp** directory for suspicious files owned by any WebLogic account, such as **watch-smartd**, **Carbon**, and **default**.

**Escalation**

* If you see anything that makes you even a little bit suspicious, you should contact your security team immediately.
* If you notice spikes in your CPU usage and feel as though your machine has been “slow”, disconnect from the internet.
* Your security preferences should be set so that JavaScript does not automatically run on your machine without a prompt.
* Do not access sites that have been blacklisted on company machines/networks.
* We recommend installing these extensions to block coinminer activity on browsers: Extensions (Nocoin/MinerBlock)
* Always make sure you have all your software updated - this will prevent the likelihood of your machine getting infected.
* Do not hesitate to contact the security team upon any suspicion of threat. The longer you wait the more damage that may be done.

**Resources**

* [Cisco Talos](https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html) - “Rocke: The Champion of Monero Miners,” August, 30 2018
* [CSO Online](https://www.csoonline.com/article/3267572/how-to-detect-and-prevent-crypto-mining-malware.html) = “How to detect and prevent crypto mining malware,” April 4, 2018
* [Malwarebytes](https://www.malwarebytes.com/pdf/white-papers/Drive-By-Cryptocurrency-Mining_Malwarebytes-Labs-Report.pdf) = “A Look into the Global “Drive-By Cryptocurency Mining” Phenomenon,” July 19, 2017
* [NSFocus](https://blog.nsfocusglobal.com/threats/vulnerability-analysis/technical-analysis-and-solution-of-weblogic-server-wls-component-vulnerability/) - “Technical Analysis And Solution Of Weblogic Server Component Vulnerability” Dec. 25, 2017
* [Palo Alto Unit 42](https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/) - “Malware Used by “Rocke” Group Evolves to Evade Detection by Cloud Security Products,” Mar 17, 2017
* [ZDNet](https://www.zdnet.com/article/this-cryptocurrency-mining-malware-now-disables-security-software-to-help-remain-undetected/) - “This cryptocurrency mining malware now disables security software to help remain undetected,” Jan 17, 2017