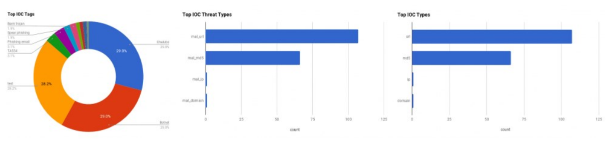
WEEKLY THREAT BRIEFING

# Weekly Threat Briefing: New Security Flaw Impacts Most Linux And BSD Distros

October 30, 2018 | Anomali Threat Research Team



The intelligence in this weekís iteration discuss the following threats: **APT, Data breach, DDoS, NARWHAL SPIDER, Phishing, Ransomware, TA554, Targeted attacks, TRITON,** and **Vulnerabilities**. The IOCs related to these stories are attached to the Community Threat Briefing and can be used to check your logs for potential malicious activity.

## Trending Threats

**New Security Flaw Impacts Most Linux And BSD Distros** (*October 25, 2018*)
The popular "X.Org Server" package for Linux and BSD has a new vulnerability that was recently disclosed. This vulnerability, registered as "CVE-2018-14665," allows for a threat actor to gain elevated privileges and root access via a terminal or SSH session. The X.Org Server package is a core graphics and windowing technology that is the base for KDE and GNOME desktop interfaces, and is found in all major Linux and BSD distributions. This vulnerability was caused by the mishandling of two command-line options "-logfile" and "-modulepath" that can allow a threat actor to insert and execute their own commands. The X.Org Foundation issued a new version to this package (version 1.20.3) to fix this vulnerability. Services like Ubuntu, Fedora, and OpenBSD are among the projects affected.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Exploitation for Privilege Escalation (T1068)

**Misconfigured Container Abused To Deliver Cryptocurrency-mining Malware** (*October 25, 2018*)
There has been an increase of systems containing misconfigured Docker Engine-Community with Docker Application Programme Interface (API) ports, researchers at Trend Micro observed. The misconfigured API ports were seen to be exposed for external access on ports 2375 and 2376 by users with administrative permissions. Threat actors have used those exposed ports to then initiate attacks that ultimately install Monero cryptominers onto the target system. Threat actors create fake users "richard" and "frank" then give them root privileges on the system. Once obtaining those privileges, the threat actors re-configure the Secure Socket Shell (SSH) daemon to allow for password authentication, then install system managing packages and additional files for persistence. Then they scan for open 2375 and 2376 ports and infect systems laterally with Monero miners.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Exploitation for Privilege Escalation (T1068) | [MITRE ATT&CK] Uncommonly Used Port (T1065)

**Cutwail Spam Campaign Uses Steganography To Distribute URLZone** (*October 25, 2018*)
Researchers from CrowdStrike observed a new "Cutwail" botnet campaign from the for-hire threat group, "NARWHAL SPIDER." The targets of this recent spam campaign vary depending on the customer's needs. The threat group uses phishing emails written in Japanese that contain a malicious attachment. The emails are observed to be order forms, payment reports, billing data, among other financial-themes and contain a macro-enabled Microsoft Excel attachment. If the macros are enabled, PowerShell and steganography are employed to distribute "URLZone" malware. The malware initiates by deobfuscating using Visual Basic Application (VBA), and then downloads an image file and executes PowerShell commands that are hidden in the blue and green channels of the image. Once that payload is executed, URLZone connects to a Command and Control (C2) server, though it is unclear at the writing of this article what the final payload delivered is.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Spearphishing Attachment (T1193) | [MITRE ATT&CK] Data Obfuscation (T1001)

**Cathay Pacific Hack: Personal Data Of Up To 9.4 Million Airline Passengers Laid Bare** (*October 25, 2018*)
Airline company, Cathay Pacific, disclosed on October 24, 2018 that they suffered a data breach in which 9.4 million passengers were affected. The data that was accessed by unauthorised threat actors includes: 27 active credit card numbers (without the associated CVV numbers), customer service remarks, dates of birth, email addresses, expired credit card numbers, frequent flyer programme membership numbers, historical travel data, Hong Kong ID card numbers, nationalities, passenger name, passport numbers, phone numbers, and physical addresses. Cathay Pacific employees discovered the compromise following routine IT security processes, according to the company. During a thorough investigation, it is suspected unauthorised access to some data might have occurred in March 2018, though by May 2018 the data was confirmed to have been exposed. The company is in the process of contacting all customers via several communication channels and have reported that, at the time of the article, no passenger data appeared to have been misused. It is not publicly clear what was the cause of the breach.
Click here for Anomali recommendation

**Government Spyware Vendor Left Customer, Victim Data Online For Everyone To See** (*October 24, 2018*)
A German-based spyware organisation, Wolf Intelligence, accidentally leaked over 20 gigabytes of company information such as recordings of customer meetings, scans of the founder's passport, credit card information, and surveillance targets. Researchers from CSIS Security discovered the information on an unprotected Command and Control (C2) server along with a public Google Drive folder. All of the information was able to be publicly accessed by anyone if they knew where to look. The company stated that the cause of the breach was due to a mishandling of the information by a reseller, although the company did not report who that reseller was. Following notice of the data breach, Wolf Intelligence shut down the exposed servers.
Click here for **Anomali** recommendation

**Android/TimpDoor Turns Mobile Devices Into Hidden Proxies** (*October 24, 2018*)
A recent phishing campaign has been observed utilising SMS text messages to trick Android users into downloading a fake voice-messaging application that actually allows threat actors to covertly use the infected devices as network proxies. Researchers at McAfee Mobile Research found that this campaign has been targeting users in the United States since March 2018 and installs a "Socks" proxy that redirects all network traffic through a third-party server via an encrypted shell tunnel connection to bypass security mechanisms. The malware has been dubbed "Android/TimpDoor" and initiates by sending a text message that states something along the lines of "you've received two new voice messages. To hear these, use [URL]." If a user clicks this link, it redirects them to a fake web page that purports to be from a popular advertisement site where the link to download the "voice-messaging" application is located. The application has zero functionality aside from playing the two fake voice messages, though the voice messages length do not correspond with the length the file states it to be. This malware appears to be similar to "MilkyDoor," however, TimpDoor only has one functionality (acting as a proxy) whilst MilkyDoor appears to be a full SDK.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Spearphishing Link (T1192) | [MITRE ATT&CK] Connection Proxy (T1090)

**Malware Targeting Brazil Uses Legitimate Windows Components WMI And CertUtil As Part Of Its Routine** (*October 24, 2018*)
Researchers at Trend Micro have discovered malware that is utilising two legitimate Windows files, "wmic.exe" and "certutil.exe," to install a banking malware payload onto the targeted device. This campaign is conducted through phishing emails purporting to be from Correios, the national postal service of Brazil, that notifies the recipient of an unsuccessful delivery attempt. The email includes a tracking code of the delivery that can be accessed through the link it provides. If the target clicks upon the link, a window pop-up will request a ZIP file to be downloaded and extracted. This will drop a LNK file that will then direct the user to execute "wmic.exe" that connects to the Command and Control (C2) server of the threat actors. The C2 server then sends a script command to make a copy of "certutil.exe" in the "%temp%" folder that is saved as "certis.exe." "Certis.exe" downloads the main payload of the malware that is a Dynamic Link Library (DLL) file. The banking malware apparently only works when the language on the target machine is in Portuguese, meaning that the targets are likely contained to Brazil and possibly Portugal.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Spearphishing Link (T1192)

**sLoad And Ramnit Pairing In Sustained Campaigns Against UK And Italy** (*October 23, 2018*)
A recent phishing email campaign has been observed by researchers at Proofpoint that utilises a new downloader, dubbed "sLoad," to install the Ramnit banking trojan and conduct reconnaissance. The campaign has been ongoing since May 2018 and it is suspected that the threat group "TA554" is behind the attacks that have targeted Canada, Italy, and the UK. The emails are crafted in the target country's language, and personalised to include the intended target's name and email address in parts of the email body so the user may be more inclined to believe the email is legitimate and click on the URL in the email. The URL takes the user to a zipped LNK file that requests macros to be enabled. If they are enabled, it triggers a PowerShell script to run and download sLoad. sLoad is capable of delivering Ramnit, Gootkit, DarkVNC, Ursnif, or PsiXBot as the final payload, although this particular campaign delivers Ramnit as the final payload. This particular campaign employs sophisticated geofencing to restrict access to content depending on the user's IP location.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Spearphishing Link (T1192) | [MITRE ATT&CK] Spearphishing Attachment (T1193)

**Magecart Group Leverages Zero-days In 20 Magento Extensions** (*October 23, 2018*)
Security researcher, William DeGroot, contends that there are approximately 20 Magneto extension zero-day vulnerabilities that would allow threat actors to enter payment skimming malware on online stores' checkout pages. De Groot has only been able to identify two of the 20 extensions that threat actors are targeting, and has requested assistance from the larger information security community to help track the specific extensions that are vulnerable. There are several URL pathways that threat actors have been observed using to exploit these vulnerabilities. The two identified Magneto extensions are "Webcooking_SimpleBundle," which has had a patch released already, and "TBT_Rewards" which was abandoned months ago and no longer receives patches so it should be uninstalled from online stores immediately.
Click here for Anomali recommendation

**Hacker Discloses New Windows Zero-Day Exploit On Twitter** (*October 23, 2018*)
Independent security researcher, "SandboxEscaper," disclosed on Twitter a Proof-of-concept (PoC) for a zero-day exploit in Microsoft Windows that appears to be a privilege escalation flaw in Microsoft Data Sharing (dssvc.dll). The Data Sharing Service allows for data brokering between applications. This particular vulnerability could allow a threat actor with low privileges to elevate their privileges by using "deletebug.exe" and thus gives them the ability to delete critical system files despite not having administrative access. The vulnerability only affects Windows 10 and recent versions of Windows server editions, so Windows 7 and 8.1 are not affected. Even a patched Windows 10 machine that has the latest October 2018 security updates, is still exploitable for this vulnerability.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Exploitation for Privilege Escalation (T1068)

**NSA Tools Used to Attack Nuclear Energy Firms** (*October 23, 2018*)
Unknown threat actors have launched a new campaign that is targeting nuclear energy firms in Egypt, Iran, and Russia, according to Kaspersky Lab researchers. The actors are using National Security Agency (NSA) tools leaked by the group called "Shadow Brokers" in their campaigns. Multiple tools were observed including: "DanderSpritz," which is used to gather data and utilize exploits; "FuzzBunch," which is a framework adaptable for different utilities and work in tangent with various plugins that each have their own malicious purpose; "DarkPulsar," which is a backdoor that is used to connect DanderSpritz and FuzzBunch together. DanderSpritz is used to monitor and steal data, and FuzzBunch to exploit vulnerabilities and gain remote access on an infected system.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Exploitation for Privilege Escalation (T1068)

**TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers** (*October 23, 2018*)
FireEye researchers have published a report in which they claim that the attack framework "TRITON," which specifically targets Industrial Control Systems (ICS), was developed with assistance from the Russian government. Specifically, the malicious activity attributed to TRITON, which first reported on in December 2017, that resulted in the distribution of the malware that "was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM)." CNIIHM is owned by the Russian government and is located in Moscow. Researchers track actors using TRITON as TEMP.Veles and justify their claims with the following evidence: malware development by TEMP.Veles of which some was found during the TRITON intrusion, testing activity was linked to a specific individual with ties CNIIHM, an IP registered to CNIIHM was used by TEMP.Veles in TRITON activity, TEMP.Veles activity aligns with the Moscow time zone, and researchers contend that CNIIHM possesses the skills and knowledge necessary to create TRITON and assist in TEMP.Veles campaigns.
Click here for Anomali recommendation

**Chalubo Botnet Wants To DDoS From Your Server Or IoT Device** (*October 24, 2018*)
A new botnet, dubbed "Chalubo," has been discovered that has been observed targeting insecure Internet-of-Things (IoT) devices and internet-facing SSH servers on Linux systems, according to Sophos researchers. The botnet uses code from the "Xor.DDoS" and "Mirai" botnet malware and other malware techniques such as encryption to make the malware difficult to detect. Chalubo contains a Lua command script and utilises the "Elknot dropper" that has been used in the past by the "Elasticsearch" botnet. The bot was observed to attack a Sophos research honeypot, and the researchers were then able to see that a downloader named "libsdes," creates an empty file to prevent multiple occurrences of the malware from executing. The downloader drops various scheduled task commands to assist in gaining persistence and ensure the malware survives a reboot. The end goal is to commit a Distributed-Denial-of-Service (DDoS) attack from the infected devices. Sophos researchers believe that the bot was going through a testing period after an attack ordered their the honeypot to target a single Chinese IP address. Researchers now believe that the bot will be observed in the future in more wide-spread campaigns.
Click here for Anomali recommendation
**MITRE ATT&CK:** [MITRE ATT&CK] Data Obfuscation (T1001) | [MITRE ATT&CK] Remote Access Tools (T1219) | [MITRE ATT&CK] Brute Force (T1110)

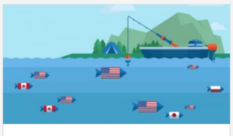
**Gamma Ransomware Compromises Data On 16,000 Patients At California Hernia Institute** (*October 22, 2018*)
The National Ambulatory Hernia Institute (NAHI) in California suffered a data breach following a Gamma ransomware attack on September 13, 2018. Approximately 16,000 patient records containing sensitive data including name, address, date of birth, Social Security Number (SSN), diagnosis, and appointments' data and time. An email address "Glynnaddey@aol[.]com" initiated the attack, though it is unclear how this occurred, which is known to be tied to the Gamma ransomware. The Institute stated that patients in their system prior to July 19, 2018 had their information compromised. NAHI reports that it has moved most of their data to an off-site server and are continuing to investigate the incident.
Click here for Anomali recommendation

*About the Author*
Anomali Threat Research Team

You might also be interested in...

Blog
Wolves Attack When the Herd Is Distracted

Blog
APTs & Threat Actors That May Increase Hostile Activity Due to Elimination of Iranian General Quassem Suleimani


Blog
Phishing Campaign Targets Login Credentials of Multiple US, International Government Procurement

Blog
Malicious Activity Aligning with Gamaredon TTPs Targets Ukraine