FACULTY OF SCIENCE & TECHNOLOGY

Department of Computing & Informatics

Forensic Computing & Security

System Information and Event Management **February 8th 2020**

Word Count: 2985

Paul-David Jarvis

s5115232@bournemouth.ac.uk

System Information and Event Management (SIEM) and APT1 & Log Analysis

Table of Contents

Table of Figures

1.0 SIEM & APT1

1.1 APTs, What are they & Why are they a threat in general?

Advanced persistent threats (APTs) are attacks on a network where an unauthorised threat actor gains unauthorised access to a system or a network and remains within the system or network for an extended amount of time without being detected (Lord, 2018). They are a much larger threat in general compared to other types of malware. Whereas most malware like ransomware has a quick damaging nature with the main goal is to cause as much chaos as possible, advanced persistent threats are more strategic and stealthy and their goal is to secretly move throughout the compromised network or system and to monitor the network activity and steal data. It requires a lot of finesse to successfully carry out an advanced persistent threats attack, retrieve the stolen data and cover your tracks. The finesse needed suggests it requires a lot of skills and resources, those of a script kiddie or student would not possess, rather the skills and resources of a cold intelligence hacker or even nation-states. In the case of APT1, their longest time that they had access to a compromised victim's network was 4 years and 10 months, this suggests that APT1 are extremely skilful and have the resources to carry out a successful attack.

1.2 APT1

APT1, otherwise known as the People's Liberation Army (PLA) unit 61398, is an advanced persistent threat unit that is allegedly the source of several Chinese computer hacking attacks. They are working under the people's liberation army strategic support force (SSF) branch that was formed to be responsible for all space, cyber and electronic warfare for the people's liberation army. All 5 members of APT1 are all featured on the federal bureau of investigation's cyber most wanted list: Gu Chunhui; Huang Zhenyu; Sun Kailiang; Wang Dong and Wen Xinyu and all are wanted for 31 criminal counts of a large variety of cybercrime (Federal Bureau of Investigation, 2014).

Figure 1: From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges. - (Federal Bureau of Investigation, 2014)

Due to a large number of criminal accounts that the 5 members of APT1 were indicted for, their true motives are unclear. One crime that they were indicted for was “Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain” and another was “Theft of Trade Secrets” They uncovered several trade secrets, one for a nuclear plant design which could only be a single one of their motives, they may have also been out for financial gain also.

There has been no recent activity from APT1 that has been released. Mcafee recently released a report on a backdoor that is similar to those used by APT1 but suggested that it was not an APT1 operation. It is very unlikely that they will attempt anything due to them no longer being able to operate with impunity under a shadow or under the flag of China.

The impact of APT1 and all the attacks that they launched were huge. They compromised over a hundred different organisations and different industries nationwide and stole hundreds of terabytes of data from the companies that it has attacked and compromised. The data that they have stolen is broad and includes full system designs including a power plant; proprietary information; business documents such as mergers, contracts and acquisitions; high-ranking personnel meetings briefs and their emails; credentials for users and network information (Fireeye.com, n.d.).

1.3 Tactics and techniques used by APT1 in relation to the cyber kill chain

1.3.1 Reconnaissance

The targets of APT1 are mainly those that speak English or have their headquarters in English speaking countries such as The United States of America. In addition to this, It is clear that APT1 targeted organisations that China identified within its 12th Five Year Plan. Several industries were identified by China’s five year plan but it was mainly Information Technology, Aerospace and Public Administration

1.3.2 Weaponization

APT1 sometimes uses publicly available malware such as Poison Ivy and Gh0st RAT but most times they create their own backdoor. “TROJAN.ECLTYS”, “BACKDOOR.BARKIOFORK”, “BACKDOOR.WAKEMINAP”, “TROJAN.DOWNBOT”, “BACKDOOR.DALBOT”, “BACKDOOR.REVIRD”, “TROJAN.BADNAME” and “BACKDOOR.WUALESS” (FireEye, 2020) are some of the many malware that has been discovered and associated with APT1.

1.3.3 Delivery

APT1 performed spear phishing attacks to send fake emails that at a first glance appeared to be from a person relevant or relevant information to the recipient of the email such as their employer or someone working for the victim's company. The backdoor is delivered by embedding the malicious ZIP file within the email that is being sent. When the PDF is downloaded, at first glance it appears to look like a normal PDF but APT1 embeds hundreds of blank spaces and an executable file extension making it look like an ordinary PDF but actually an executable file. "The_Latest_Syria_Security_Assessment_Report.zip" and "South_China_Sea_Security_Assessment_Report.zip" (Fireeye.com, n.d.) are some examples of the type of names that APT1 have called their ZIP files in order to stay inconspicuous.

1.3.4 Exploitation & Installation

When the employees look at the malicious ZIP file, it will look normal and have a name that is extremely relevant to the target like something relating to their profession or company, APT1 focused on the company and picked a name that includes military, economic and diplomatic themes. When the victim runs the backdoor that APT1 embedded in the email as the malicious ZIP file and that they downloaded, the backdoor will now be run and installed on the victim's computer.

1.3.5 Command and Control

The backdoor that APT1 delivered to their target will initiate an outbound connection to their "command and control" server. This is typically a computer that APT1 can use to send commands to all the systems and networks that have been compromised by them. This allowed APT1 to have continuous access to the computers or networks that they attacked and compromised.

1.3.6 Actions and Objectives

Actions and objectives are the final stage of the kill chain and the stage where APT1 began doing internal reconnaissance on the network using batch scripts that identified the victim's network information, services and processes running as well as the shared sources on the network. APT1 can now connect to the shared resources. APT1 finds files and information that may be interesting to them and archives them before exfiltrating them.

1.4 How a SIEM solution could provide intelligence in the different phases of the kill chain for detection.

1.4.1 Reconnaissance

During the first stage of the cyber kill chain reconnaissance, SIEM software will not be able to provide any intelligence at this kill chain stage as it is mainly just APT1 doing their research and picking their targets such as harvesting emails and other information that they can use to attack their targets.

1.4.2 Weaponization

Within the weaponization phase of the cyber kill chain, SIEM software will not be able to offer any intelligence or help. This is because, during this stage, APT1 is creating custom backdoors or planning on using publicly available backdoors like Poison Ivy, SIEM software will identify threats, however, APT1 has not attacked their targets at this point and is not leaving any logs behind for the SIEM software to identify.

1.4.3 Delivery

During the delivery phase of the cyber kill chain, A SIEM software can monitor a large volume of events and logs from all devices within the network such as servers, hosts and other devices. The SIEM software filters using the correlation rules that are written to spot threats that may have been downloaded or implemented into the system by a malicious threat actor. (Shelley, 2015)

1.4.4 Exploitation & Installation

During the exploitation and installation stage, a SIEM software will be able to help detect and prevent when an unauthorised threat actor has gained access into the victim's network or system. SIEM software will allow the victim's company's incident responders to address the discovered security breach quickly and minimise the damage to the company. (Security Boulevard, 2018) SIEM software will provide an automated response mechanism that will stop attacks that are still in progress and to contain the compromised hosts and devices to contain the attack. (Scarfone, 2018)

1.4.5 Command and Control

During the command and control stage of the cyber kill chain, SIEM software can detect if users are changing or escalating their privileges and can also discover malware by correlating network traffic with threat intelligence to determine whether there is communication with external threat actors. (Exabeam, 2020)

1.4.6 Actions and Objectives

SIEM software can monitor traffic with certain protocols such as FTP which is known for facilitating large data transfers that could be a malicious threat actor transferring files and data with malicious purpose. If the SIEM software notices requests with unusual quantities or file types and if the target and recipient for the file transfer is unknown or malicious that is being transferred then it will alert you. The SIEM software can also monitor emails and mobile devices to detect whether emails are being forwarded and detect any anomalies that might indicate information leaked through a mobile. (Exabeam, 2020)

1.4.7 Relevant Indicators of Compromise (IoC)

Symantec released a report that includes a tone of information regarding the relevant indicators of compromise that has been associated with APT1. These Indicators types are network, file, system and email.

1.4.7.1 Network

The network indicators of compromise that has been associated with APT1 are HTTP requests, domains and IP addresses. Traffic that has a POST request will include “name=GeorgeBush&userid=<4 digit number>&other=” and traffic with GET request leading to other pages include:

- aspnet_client/report.asp
- Resource/device_Tr.asp
- images/device_index.asp
- news/media/info.html
- Backsangho.jpg
- addCats.asp
- SmartNav.jpg
- nblogo2.jpg

Some of the domains that have been discovered and associated with APT1 are:

- GT446.ezua.COM
- Aunewsonline.com
- Avvmail.com
- Cas.ibooks.tk
- Cas.m-e.org.ru
- Colville.com
- Cvba.com
- Deebeedesigns.ca

Some of the many Internet protocol addresses that have been discovered and associated with APT1 are:

- 140.116.70.8
- 143.89.35.7
- 143.89.35.7
- 150.176.164.6
- 218.232.66.12
- 218.233.206.2
- 218.234.17.30
- 24.73.192.154

(Symantec.com, 2013)

1.4.7.2 File

Some of the filenames and their locations on compromised machines that have been discovered and associated with APT1 are:

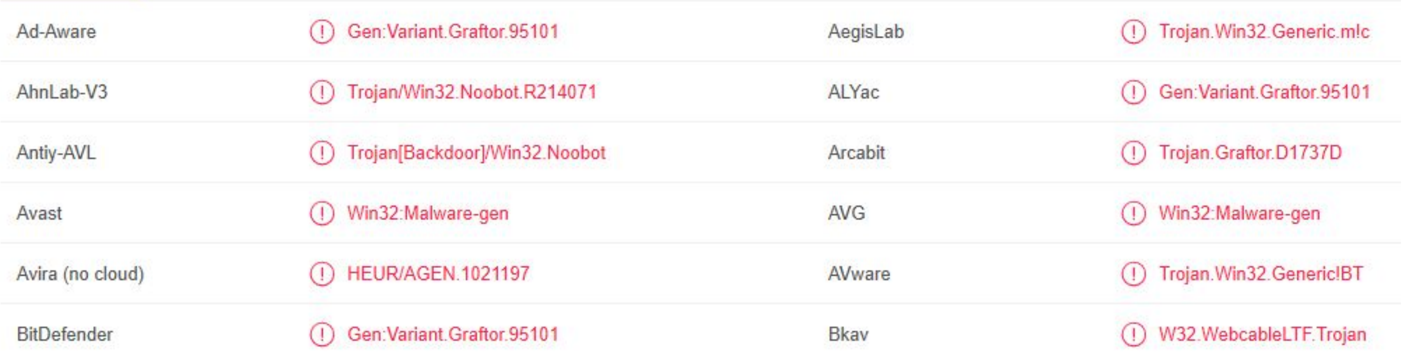
- %TEMP%\AdobeARM.exe
- %TEMP%\iTunesHelper.exe
- %PROGRAMS%\Startup\AdobeRe.exe
- Rouj.exe
- %USERPROFILE%\Local Settings\iexplore.exe
- %USERAPPDATA%\Microsoft\wuauclt.exe

APT1 used many malicious files, some of the file MD5 hashes that were discovered and included are:

- 017c03ad61f89ee6597ead40cc552aef
- 019cb1a6776f0e0d353814711e9e171b
- 02043566d027445374a1f7f0fc35d495
- 025dc68c8e06d6488e338dcc55b295eb

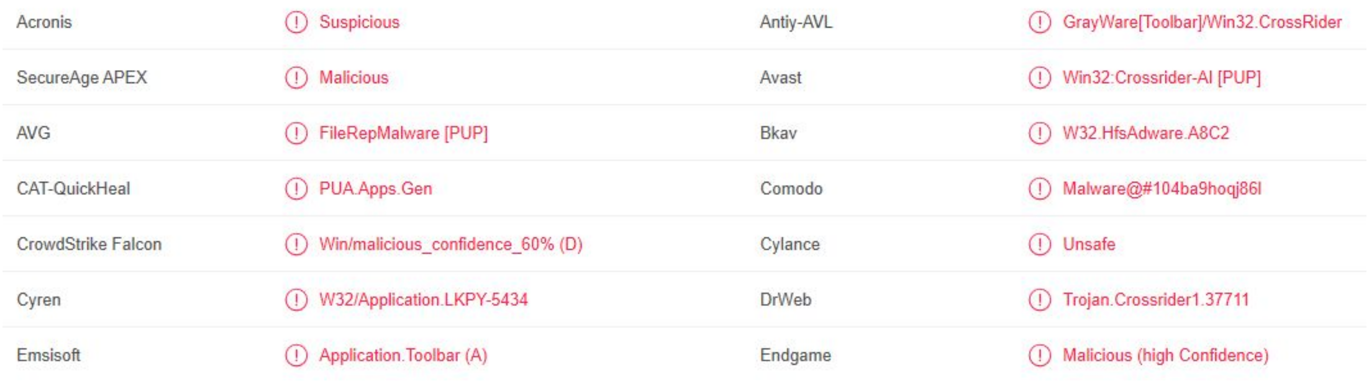
(Symantec.com, 2013)

Below are two hashes that have been scanned using virus total to reveal that the majority of scanners have noted that these are malicious files.



Ad-Aware	ⓘ Gen:Variant.Graftor.95101	AegisLab	ⓘ Trojan.Win32.Generic.m!c
AhnLab-V3	ⓘ Trojan/Win32.Noobot.R214071	ALYac	ⓘ Gen:Variant.Graftor.95101
Antiy-AVL	ⓘ Trojan[Backdoor]/Win32.Noobot	Arcabit	ⓘ Trojan.Graftor.D1737D
Avast	ⓘ Win32:Malware-gen	AVG	ⓘ Win32:Malware-gen
Avira (no cloud)	ⓘ HEUR/AGEN.1021197	AVware	ⓘ Trojan.Win32.Generic!BT
BitDefender	ⓘ Gen:Variant.Graftor.95101	Bkav	ⓘ W32.WebcableLTF.Trojan

Figure 2: Virus total scan of MD5 hash “00b61db083b07a64fb6072b42aa83dc1”. - (Virustotal.com, 2020)



Acronis	ⓘ Suspicious	Antiy-AVL	ⓘ GrayWare[Toolbar]/Win32.CrossRider
SecureAge APEX	ⓘ Malicious	Avast	ⓘ Win32:Crossrider-AI [PUP]
AVG	ⓘ FileRepMalware [PUP]	Bkav	ⓘ W32.HfsAdware.A8C2
CAT-QuickHeal	ⓘ PUA.Apps.Gen	Comodo	ⓘ Malware@#104ba9hoqj86l
CrowdStrike Falcon	ⓘ Win/malicious_confidence_60% (D)	Cylance	ⓘ Unsafe
Cyren	ⓘ W32/Application.LKPY-5434	DrWeb	ⓘ Trojan.Crossrider1.37711
Emsisoft	ⓘ Application.Toolbar (A)	Endgame	ⓘ Malicious (high Confidence)

Figure 3: Virus total scan of MD5 hash “0136ab6d2e507d4e63990b196121d41c” . - (Virustotal.com, 2020)

1.4.7.3 System

Some of the registry entries that have been associated with APT1 are:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Acroread"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Adobe Update"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCheck"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCom"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"IMSCMig"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"McUpdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Register"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"SysTray"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"systemupdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"wininstaller"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"APVSVC"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"AdobeUpdate"

(Symantec.com, 2013)

1.4.7.4 Email

Some of the subject lines of the emails that APT1 sends with the malicious attachments are:

- Capt [REMOVED] update
- Fw: LES Request
- Libya crisis
- Five Simple Questions for Democrats on Spending Cuts
- Behind the Easing of Israeli-Palestinian Tensions
- Business Exec Urges Broad Trade Agenda To Curb China Role In Latin America
- President Chavezs Comments About President Obama and the United States on Sundays "Alo,Presidente"
- FW: New Standdard Operational Procedures (SOPs) between the
- AGENDA
- [REMOVED] Help You Save Enough for Retirement

- Human right of north Afica under war
- Spreading Civil Unrest in the Middle East and North Africa

Some of the email attachment names that are included within the emails that APT1 send to their targets are:

- agenda201005.pdf
- Human right report of noth Afica under the war.scr
- Middle_East_Civil_Unrest.pdf   Protests Spread in Syria.pdf
- Cybersecurity and Cyber War.pdf
- The Meeting intivation of International Atomic Energy Agency 06-05-2011.scr
- meeting invitation of British Council 2011.scr
- Meeting information details of [REMOVED].exe
- Meeting information details of [REMOVED].exe
- Meeting detail information from [REMOVED].scr
- Meeting detail information from [REMOVED].scr

(Symantec.com, 2013)

2.0 Log Analysis Of A Compromised System

When looking over the access log file, I have discovered 3 malicious running WPScan and performing malicious requests in an attempt to gain access to root files. The IPs are 192.168.107.138, 192.168.107.153 and 192.168.107.155. These IPs performed WPScans and Nikto. 192.168.107.138 is the origin from the events linked to Nikto performing a vulnerability scan to check whether SQLi, XSS and other attacks are a potential attack surface, these were not included as they all failed. The attacks included below are returned successful status and thus considered incidents.

2.1 Attack Summary

The first incident was a brute force attacked on the WordPress login page by using WPScan. The attacker hit the webpage with roughly 15,000 attempts which reinforces the idea that this was a brute force rather than a dictionary attack. Taking into consideration that the last incident was a different status code to the rest suggests that this incident was a success and the attacker (192.168.107.138) gained access.

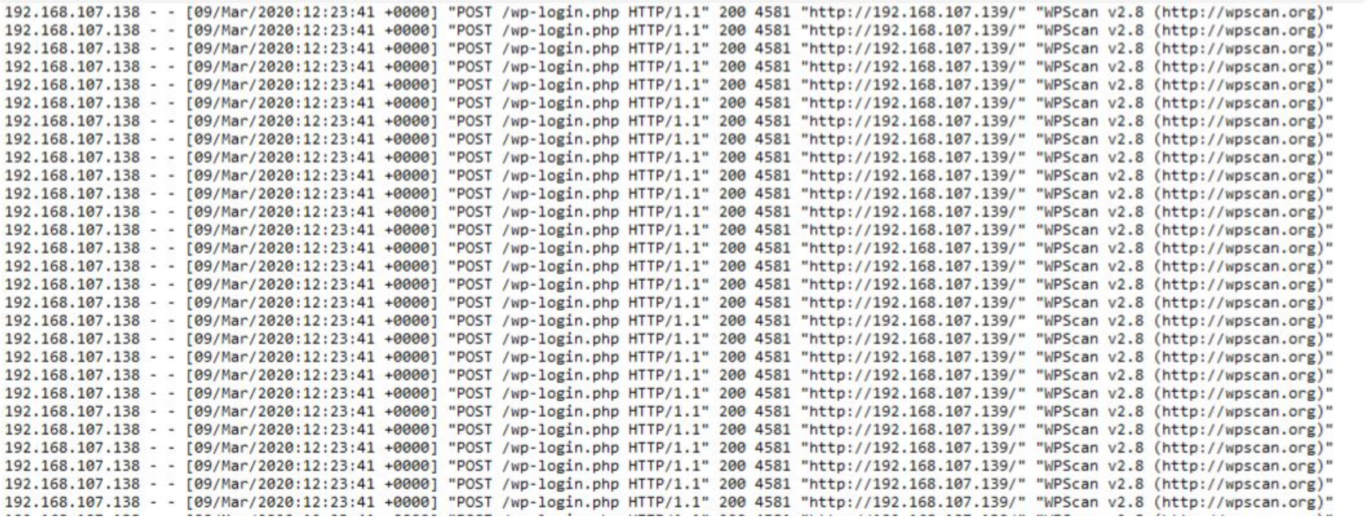
The second incident was a common vulnerability (CVE-2014-8799) in the DukaPress plugin. The attacker (192.168.107.153) exploited a directory traversal vulnerability due to DukaPress not being able to sufficiently sanitise the user's input. The attacker was successful in crafting a specific URL that would grant him access to the wp-config.php file.

A third incident was when an attacker (192.168.107.172) sent over 3,000 events to strange directories to try and flood the servers to cause a DoS attack.

The fourth potential incident was when an attacker (192.168.107.155) ran a WordPress Scan using WPScan and created an account. After a minute, the same IP logged into the WordPress successfully from a Firefox browser and proceeded to access WordPress admin content.

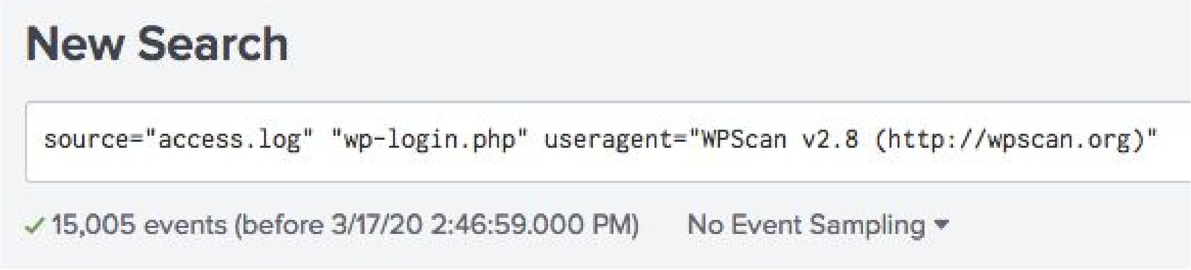
2.2 WPScan Brute Force

The access.log file in figure 4 shows that roughly around 15,000 POST requests were made to the WordPress login page. This suggests a brute force attack and can be seen in figure 4 showing that the user agent is “WPScan v2.8”. The attack started on 9th of March at 12:18 till 12:24 originating all from the same IP address 192.168.107.138 that can be seen in figure 5. All the attacks apart from one had the status 200 apart from one with the status 302 which suggests the attacker's brute force attack was a success and he was redirected. The most effective way to counter this attack is by adding a rule that blocks the user after a specific number of incorrect login attempts. I used Splunk Cloud also to analyse the logs and to filter it using the search feature seen in figure 5 looking for events that have “wp-login” in the event. It showed that roughly 2,000 login attempts were made every minute and the events can be seen in figure 6 and visualised in figure 7 showing the amount made every minute.



```
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
192.168.107.138 - - [09/Mar/2020:12:23:41 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)"
```

Figure 4: Brute Force Login Logs. - (SIEM-May2020, 2020)

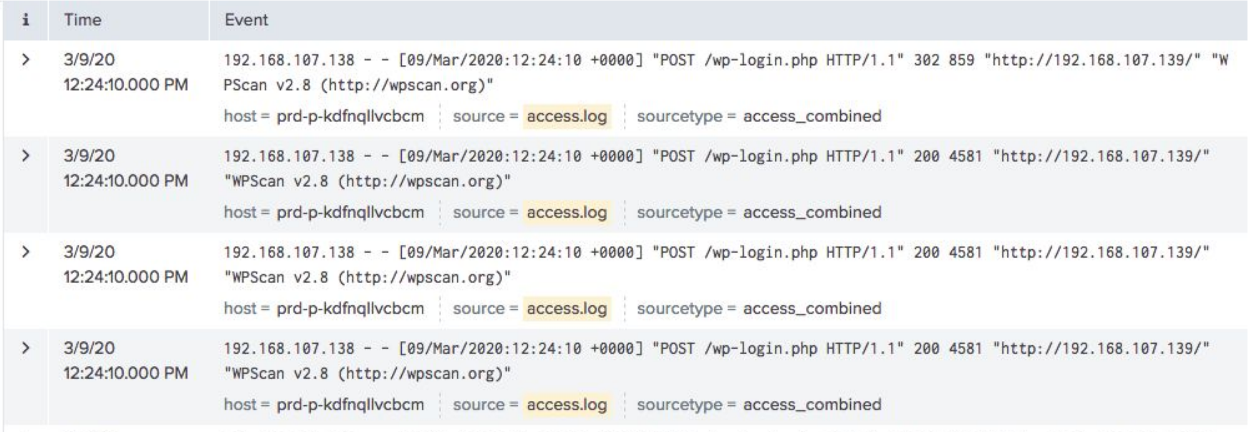


New Search

```
source="access.log" "wp-login.php" useragent="WPScan v2.8 (http://wpscan.org)"
```

✓ 15,005 events (before 3/17/20 2:46:59.000 PM)

Figure 5: Brute Force Login Splunk Search. - (Splunk, 2020)



i	Time	Event
>	3/9/20 12:24:10.000 PM	192.168.107.138 - - [09/Mar/2020:12:24:10 +0000] "POST /wp-login.php HTTP/1.1" 302 859 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)" host = prd-p-kdfnqllvcbcm source = access.log sourcetype = access_combined
>	3/9/20 12:24:10.000 PM	192.168.107.138 - - [09/Mar/2020:12:24:10 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)" host = prd-p-kdfnqllvcbcm source = access.log sourcetype = access_combined
>	3/9/20 12:24:10.000 PM	192.168.107.138 - - [09/Mar/2020:12:24:10 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)" host = prd-p-kdfnqllvcbcm source = access.log sourcetype = access_combined
>	3/9/20 12:24:10.000 PM	192.168.107.138 - - [09/Mar/2020:12:24:10 +0000] "POST /wp-login.php HTTP/1.1" 200 4581 "http://192.168.107.139/" "WPScan v2.8 (http://wpscan.org)" host = prd-p-kdfnqllvcbcm source = access.log sourcetype = access_combined

Figure 6: Brute Force Login Splunk. - (Splunk, 2020)

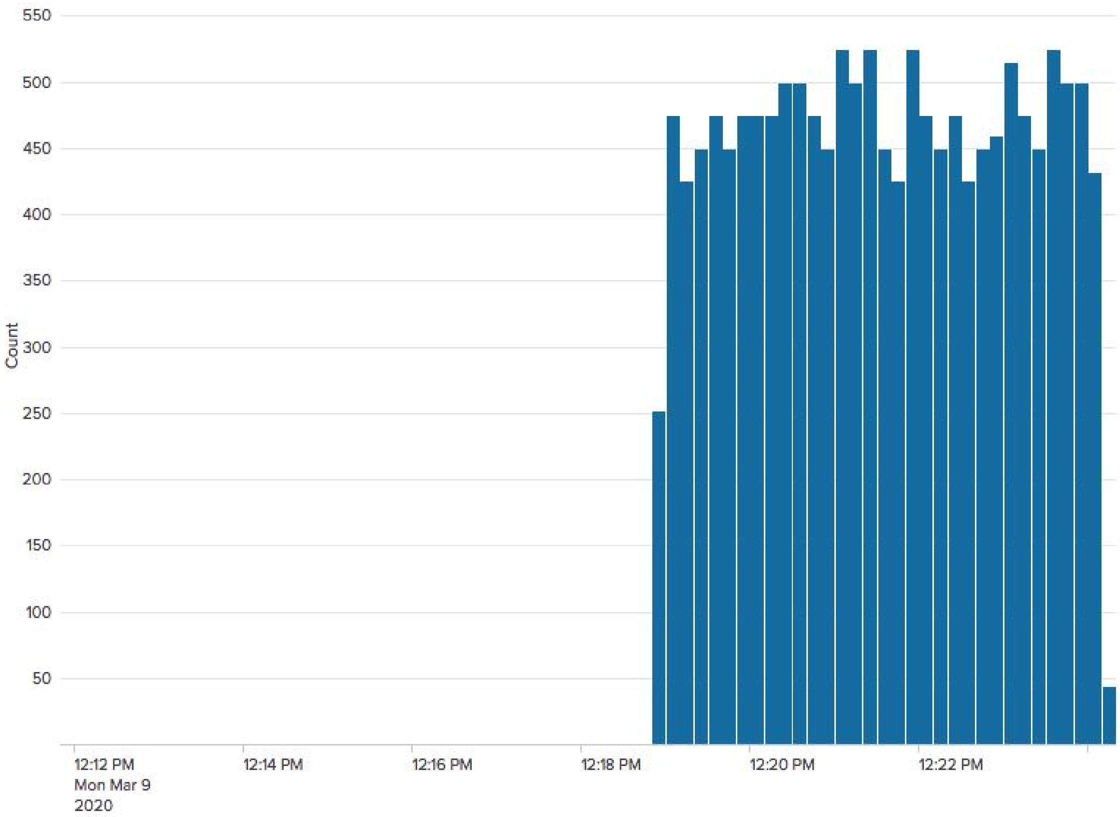
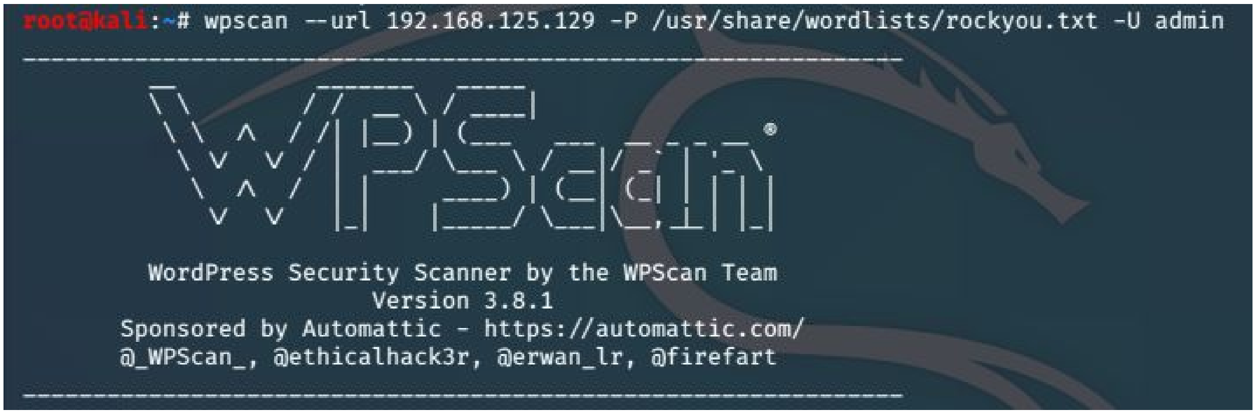


Figure 7: Brute Force Login Bar chart. - (Splunk, 2020)



```
root@kali:~# wpscan --url 192.168.125.129 -P /usr/share/wordlists/rockyou.txt -U admin
_______________________________________________________________

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.1
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

Figure 7a: Wpscan (Personal - Kali)

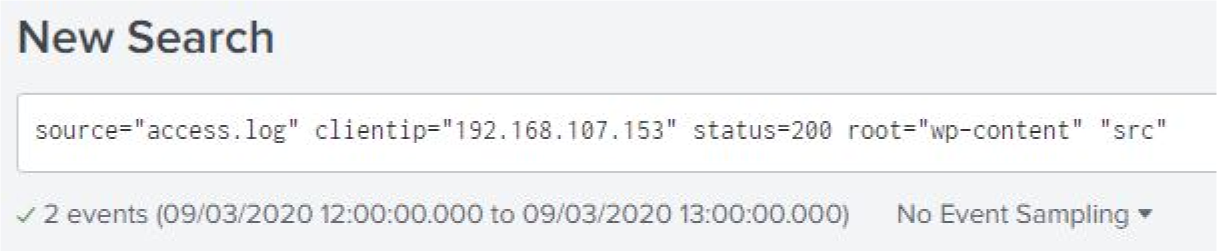
2.3 Dukapress Path Traversal Attack

When looking over the access log file with Splunk and the filters I discovered that the attacker was able to send specially-crafted URL requests to view arbitrary files on the system. I added the filter status 200 to make sure that the request was a success and when looking at the filter “root” I saw something interesting which is the wp-content folder which holds important information relating to the WordPress website, this can be seen in figure 8. I then saw something even more interesting and that was “src=../../../../includes.php” and “src=../../../../wp-config.php”, these events can be seen in figure 9. The first event was at 12:55 and the last was at 12:57, this attack came from the same IP that ran the Nikto scan which was 192.168.107.153.

These requests wouldn’t happen naturally and when researching this string I came across a CVE-2014-8799 that shows these strings as proof of concept and can be seen in figure 10. It appears this DukePress plugin vuilnerabilitiy allows an attacker to send the specially-crafted URL requests to the dp_image.php script containing "dot dot" sequences (/../) in the src parameter to view arbitrary files on the system.

One of the attack URL requests was "GET /wp-content/plugins/dukapress/lib/dp_image.php?src=../../../../wp-config.php HTTP/1.1" This wordpress file contains confident and sensitive credentials used to access the MySQL database such as the name of the database and the username and password to access the database. This type of information is not only crucial to keep private to protect the database and the WordPress website, but the database may contain potential reused credentials such as email addresses, usernames and passwords that could be used to access the employee emails or SSH if the service is running.

The solution to this vulnerability is extremely easy to do and that is to update WordPress to the latest version. It is always recommended to update any software or services to the latest versions to patch vulnerabilities such as this.

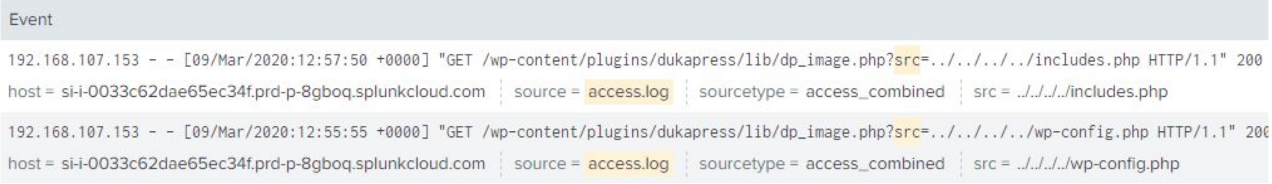


New Search

```
source="access.log" clientip="192.168.107.153" status=200 root="wp-content" "src"
```

✓ 2 events (09/03/2020 12:00:00.000 to 09/03/2020 13:00:00.000)

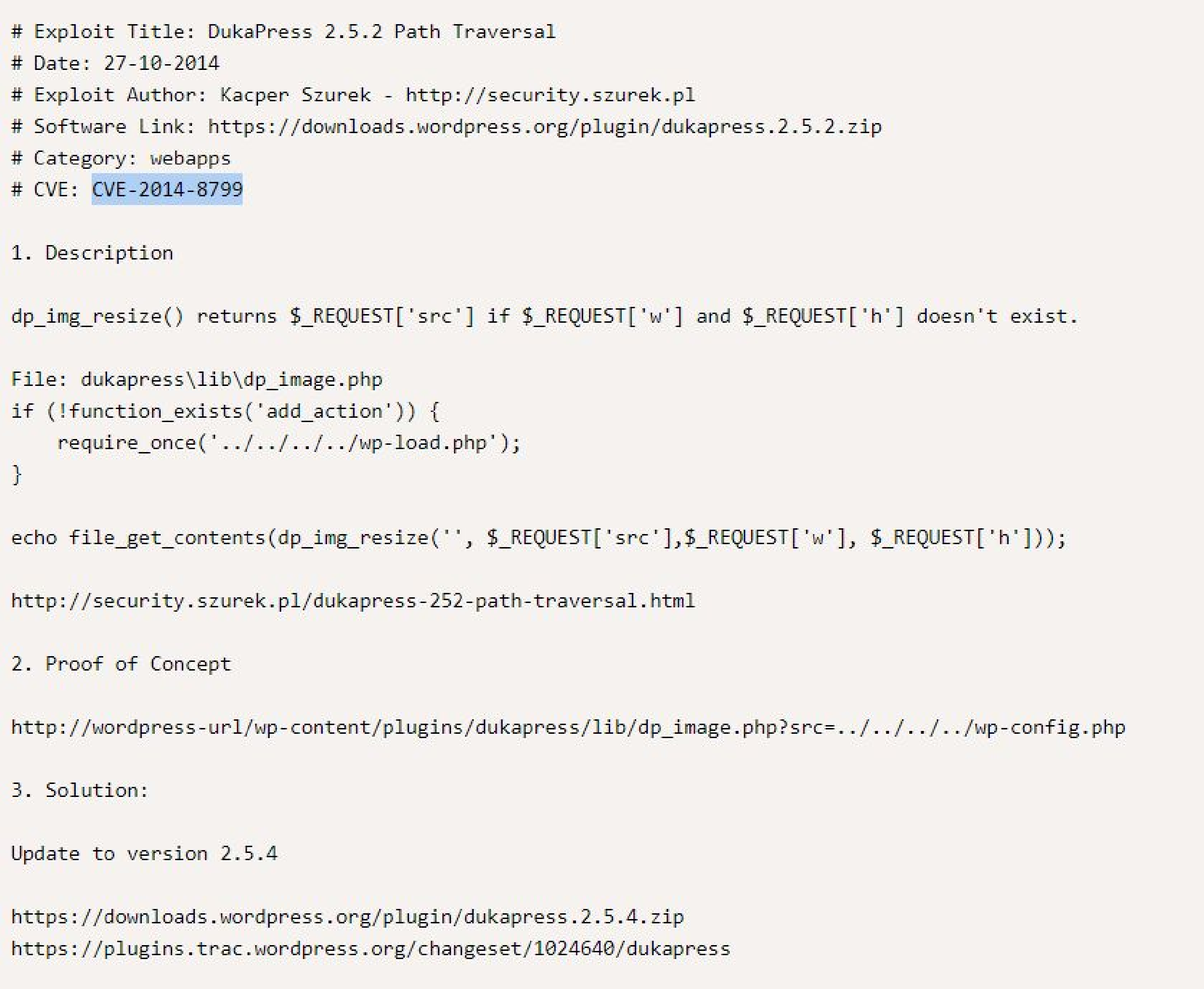
Figure 8: CVE-2014-8799 Query - (SIEM-May2020, 2020)



Event

```
192.168.107.153 - - [09/Mar/2020:12:57:50 +0000] "GET /wp-content/plugins/dukapress/lib/dp_image.php?src=../../../../includes.php HTTP/1.1" 200
host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined | src = ../../../../includes.php
192.168.107.153 - - [09/Mar/2020:12:55:55 +0000] "GET /wp-content/plugins/dukapress/lib/dp_image.php?src=../../../../wp-config.php HTTP/1.1" 20
host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined | src = ../../../../wp-config.php
```

Figure 9: Src=../../../../ Logs - (SIEM-May2020, 2020)

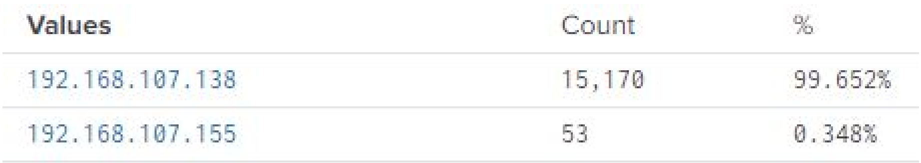


```
# Exploit Title: DukaPress 2.5.2 Path Traversal
# Date: 27-10-2014
# Exploit Author: Kacper Szurek - http://security.szurek.pl
# Software Link: https://downloads.wordpress.org/plugin/dukapress.2.5.2.zip
# Category: webapps
# CVE: CVE-2014-8799

1. Description

dp_img_resize() returns $_REQUEST['src'] if $_REQUEST['w'] and $_REQUEST['h'] doesn't exist.

File: dukapress\lib\dp_image.php
if (!function_exists('add_action')) {
    require_once('../../../../wp-load.php');
}

echo file_get_contents(dp_img_resize('', $_REQUEST['src'],$_REQUEST['w'], $_REQUEST['h']));

http://security.szurek.pl/dukapress-252-path-traversal.html

2. Proof of Concept

http://wordpress-url/wp-content/plugins/dukapress/lib/dp_image.php?src=../../../../wp-config.php

3. Solution:

Update to version 2.5.4

https://downloads.wordpress.org/plugin/dukapress.2.5.4.zip
https://plugins.trac.wordpress.org/changeset/1024640/dukapress
```

Figure 10: DukaPress Path Traversal - (SIEM-May2020, 2020)

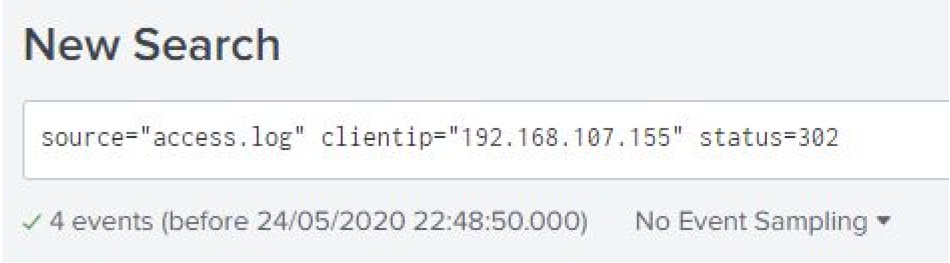
2.4 WPScan Account Creation

While looking through the logs using the search query used to identify the brute force attack in the first incident, I noticed in the client IP field that there was the IP that was the origin for the WPScan brute force attack and another, I showed this in figure 11. Upon further research using Splunk interesting fields options, the search query used can be seen in figure 12. I discovered 4 events coming from the IP 192.168.107.155 and the first event was at 12:20 and the last was at 12.23. It appears that an attacker originating from 192.168.107.155 created an account during their WPScan and can be seen in the first two events shown in figure 13. The first event accessed the signup page in the wordpress website and the second event is sending a request labeled register and then seconds later the events in the log shows the attacker accessing their account they just created from Firefox and was able to edit WordPress admin content. This can all be seen in figure 13.



Values	Count	%
192.168.107.138	15,170	99.652%
192.168.107.155	53	0.348%

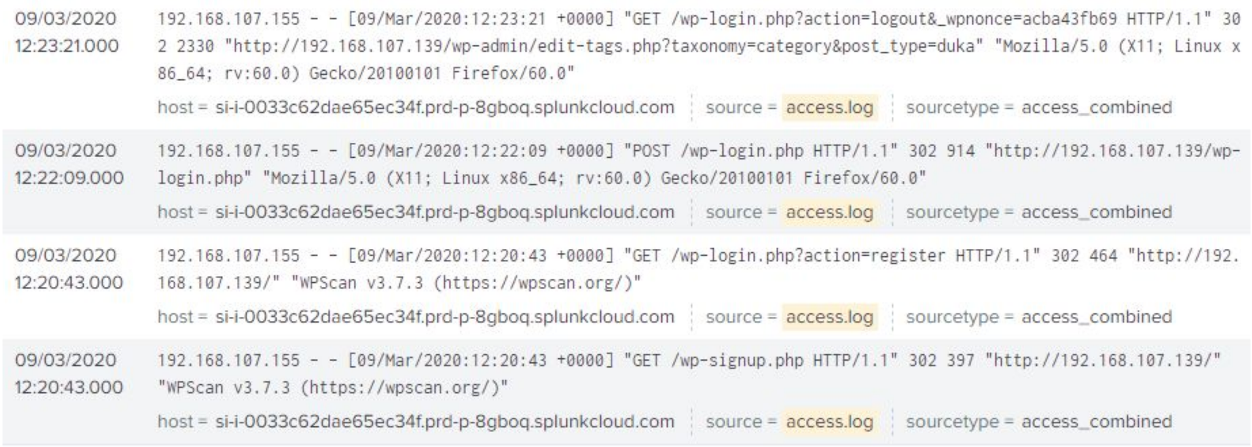
Figure 11: WPScan IPs - (SIEM-May2020, 2020)



```
source="access.log" clientip="192.168.107.155" status=302
```

✓ 4 events (before 24/05/2020 22:48:50.000) No Event Sampling ▾

Figure 12: WPScan Account Creation Query - (SIEM-May2020, 2020)

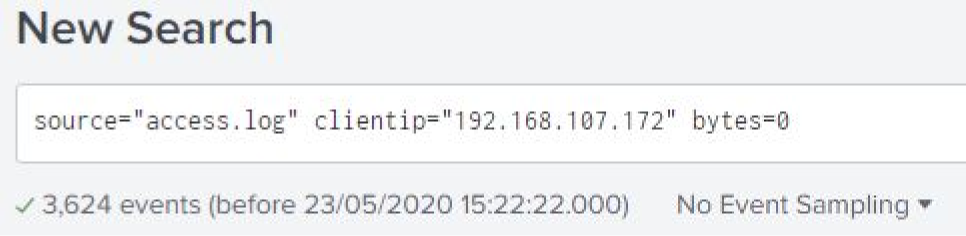


```
09/03/2020    192.168.107.155 - - [09/Mar/2020:12:23:21 +0000] "GET /wp-login.php?action=logout&_wpnonce=acba43fb69 HTTP/1.1" 30
12:23:21.000  2 2330 "http://192.168.107.139/wp-admin/edit-tags.php?taxonomy=category&post_type=duka" "Mozilla/5.0 (X11; Linux x
              86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
              host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined
09/03/2020    192.168.107.155 - - [09/Mar/2020:12:22:09 +0000] "POST /wp-login.php HTTP/1.1" 302 914 "http://192.168.107.139/wp-
12:22:09.000  login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
              host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined
09/03/2020    192.168.107.155 - - [09/Mar/2020:12:20:43 +0000] "GET /wp-login.php?action=register HTTP/1.1" 302 464 "http://192.
12:20:43.000  168.107.139/" "WPScan v3.7.3 (https://wpscan.org/)"
              host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined
09/03/2020    192.168.107.155 - - [09/Mar/2020:12:20:43 +0000] "GET /wp-signup.php HTTP/1.1" 302 397 "http://192.168.107.139/"
12:20:43.000  "WPScan v3.7.3 (https://wpscan.org/)"
              host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com | source = access.log | sourcetype = access_combined
```

Figure 13: WPScan Account Creation Events - (SIEM-May2020, 2020)

2.5 DoS Attack

While looking through the other IPs under the clientip field I saw that there were 3,624 events all originating from the IP 192.168.107.172 and can be seen from figure 14. This attack started at 13:10 and ended at 13:22. These 3,624 events were all GET requests to strange URLs and requesting no or little data. My first thought that considering there is only a single IP then it's not a DDoS attack but could potentially be a DoS attack. I felt like the attacker could have been spam requesting these fake directories in order to divert resources and can be seen in figure 15. Taking into consideration that they are requested little to no bytes meaning this isn't a ping of death type of DoS but a SYN flood DoS. To counter a DoS attack you can implement a IPS or a IDS and to implement firewall rules to block traffic like this.

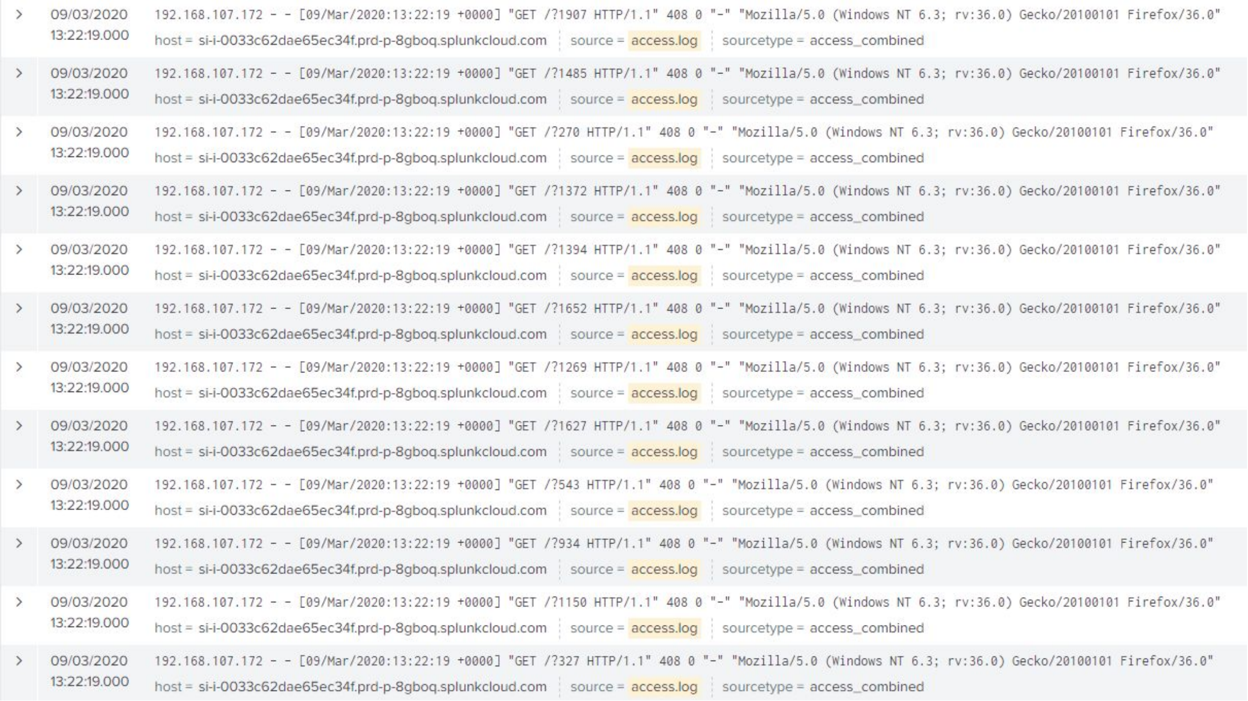


New Search

```
source="access.log" clientip="192.168.107.172" bytes=0
```

✓ 3,624 events (before 23/05/2020 15:22:22.000)   No Event Sampling ▾

Figure 14: DoS Search Query - (Splunk, 2020)



```
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1907 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1485 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?270 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1372 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1394 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1652 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1269 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1627 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?543 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?934 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?1150 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
> 09/03/2020   192.168.107.172 - - [09/Mar/2020:13:22:19 +0000] "GET /?327 HTTP/1.1" 408 0 "-" "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
  13:22:19.000 host = si-i-0033c62dae65ec34f.prd-p-8gboq.splunkcloud.com   source = access.log   sourcetype = access_combined
```

Figure 15: DoS Splunk Logs - (Splunk, 2020)

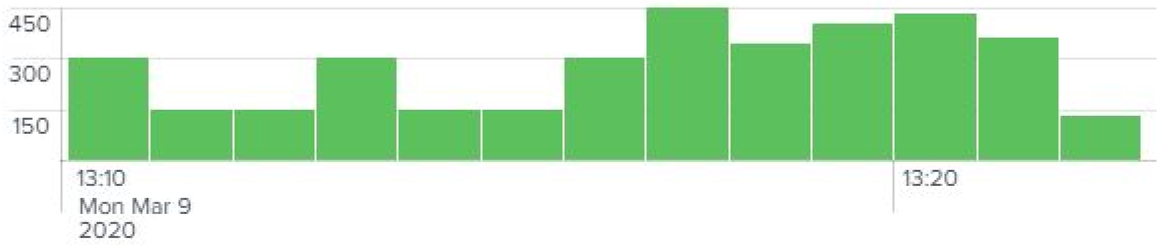


Figure 16: DoS Splunk Events Chart- (Splunk, 2020)

3.0 References

Lord, N. (2018). What is an Advanced Persistent Threat? APT Definition. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition [Accessed 10 Feb. 2020].

Federal Bureau of Investigation. (2014). Five Chinese Military Hackers Charged with Cyber Espionage Against U.S. | Federal Bureau of Investigation. [online] Available at: https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us [Accessed 10 Feb. 2020].

Fireeye.com. (n.d.). APT1: Exposing One of China’s Cyber Espionage Units. [online] Available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [Accessed 10 Feb. 2020].

FireEye. (2020). Advanced Persistent Threat Groups | FireEye. [online] Available at: https://www.fireeye.com/current-threats/apt-groups.html [Accessed 11 Feb. 2020].

Shelley, S. (2015). Introducing the Defensive Framework for Spear Phishing. [online] Info.phishlabs.com. Available at: https://info.phishlabs.com/blog/introducing-the-defensive-framework-for-spear-phishing [Accessed 13 Feb. 2020].

Security Boulevard. (2018). The Top Security Tools to Use Across the Cyber Kill Chain - Security Boulevard. [online] Available at: https://securityboulevard.com/2018/08/the-top-security-tools-to-use-across-the-cyber-kill-chain/ [Accessed 13 Feb. 2020].

Scarfone, K. (2018). SIEM benefits include efficient incident response, compliance. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products [Accessed 13 Feb. 2020].

Exabeam. (2020). 10 SIEM Use Cases in a Modern Threat Landscape | Exabeam. [online] Available at: https://www.exabeam.com/siem-guide/siem-use-cases/ [Accessed 16 Feb. 2020].

Virustotal.com. (2020). VirusTotal. [online] Available at: https://www.virustotal.com/gui/home/upload [Accessed 16 Feb. 2020].

Symantec.com. (2013). Comment Crew: Indicators of Compromise. [online] Available at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/comment_crew_indicators_of_compromise.pdf [Accessed 16 Feb. 2020].

Cve.mitre.org. 2020. CVE -CVE-2014-8799. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8799> [Accessed 24 May 2020].

Exchange.xforce.ibmcloud.com. 2020. Dukapress Plugin For Wordpress Dp_Image.Php Directory Traversal CVE-2014-8799 Vulnerability Report. [online] Available at: <https://exchange.xforce.ibmcloud.com/vulnerabilities/98943> [Accessed 24 May 2020].

Kacper Szurek. 2014. Dukapress 2.5.2 Path Traversal. [online] Available at: <https://security.szurek.pl/en/dukapress-252-path-traversal.html> [Accessed 24 May 2020].

Szurek, K., 2020. Wordpress Plugin Dukapress 2.5.2 - Directory Traversal. [online] Exploit Database. Available at: <https://www.exploit-db.com/exploits/35346?fbclid=IwAR2HYqfbraZoxn6a4uN5V7PQPh9QU8v0vQoyihZ1RhTjVa69ZZiKyFWPVGQ> [Accessed 24 May 2020].