Lab Report

Name: Inor Wang
Title: Microsoft IIS Web Log Analysis
Case: 25-T103
Date: 09/26/2025

Table of Contents

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	09/26/2025	0.1	Draft

Executive Summary

On **September 26, 2025**, Inor Wang submitted a report to **Professor Jacob D. Stauffer** documenting an offline forensic examination of **IIS web server logs** extracted from a zipped evidence set provided by the professor. The objective was to produce an industry-level, reproducible workflow that any examiner could follow to identify adversary activity, answer scoped questions, and preserve evidentiary integrity. The data set comprised **u_ex201109.log, u_ex201110.log, and u_ex201111.log**. Analysis was performed primarily in **Windows PowerShell** (Get-Content, filtering, parsing, counting) with targeted **OSINT** for user-agent and status-code interpretation; **evidence integrity** was maintained and verified with **MD5, SHA1, and SHA256** hashes.

Key findings from the examination are as follows:

- **Attack Timing:** Earliest indicator of compromise observed at **2020-11-10 05:35:44 UTC UTC**.
- **Adversary Source IP: 49.65.220.209** (WHOIS range CHINANET-JS, **CN**). Approximately **475 POST** and **13 GET** requests attributable to this IP. A second IP, **167.179.91.123**, appears frequently but aligns with the site/origin and asset fetches rather than attacker actions.
- **Focused Targets (URI stubs):** /CFT/admin/images/pass.png, /CFT/admin/index.php, /CFT/admin/main.php, /CFT/logos/miansha.php.
- **SQL Injection Attempt: 2020-11-10 05:45:59 UTC**; payload attempted to read ../../../etc/passwd (a Linux path), which would fail on a **Windows/IIS** host.
- **Web Shell Deployment:** User-agent **antSword/v2.1** observed; backdoor file identified as **miansha.php** under /CFT/logos/.
- **Response Codes:** Server returned **200 (OK)** and **302 (Found)** to the attacker; 302 responses included temporary redirects (via the **Location** header).
- **User-Agent Profile: 13 distinct UAs**, including legacy browsers, **Baiduspider** impersonation, and the **antSword** client, consistent with evasion and misdirection tradecraft.

- **Platform Details:** IIS version **10.0** (W3C extended logging enabled). The local destination IP was redacted in the logs as **CLI.ENT.IP.ADD** to protect client infrastructure details.

The examination conclusively identifies the attacker's **start time**, **source**, **methods** (high-volume POSTs, SQLi probing, web shell deployment), **targets**, and **server responses**. Procedures, commands, and outputs were documented to ensure **repeatability** and **verifiability**, with cryptographic hashes recorded to uphold **chain-of-custody**. These methods and results demonstrate a defensible workflow for analyzing IIS logs to derive actionable incident-response findings.

Synopsis

A set of IIS web server log files was provided for offline analysis to answer defined investigative questions about activity on a seized host. IIS logs are a primary source of request and configuration evidence (sites and bindings, client IPs, authentication, methods, URIs, status codes, bytes, user-agents, and timing), enabling reconstruction of access patterns and potential misuse. The professor requested a step-by-step, reproducible workflow with annotated screenshots supporting each finding.

Client Questions:

1. What is the exact date and timestamp the adversary began their attack? (Time must be in UTC)
2. What is the source IP address of the adversary?
3. What is the local IP address the adversary attacked? (Yes, it is not an actual IP address)
4. What country does the IP address reside in?
5. How many POST requests were performed by the attacker?
6. How many GET requests were performed by the attacker?
7. The attacker focused their attacks on four files (URI stubs), name them.
8. What is the exact date and timestamp the SQL injection attack occurred?
9. The SQL injection attack attempted to perform a simple Linux command to view the contents of a file. Obviously, this is a Windows system, so this would have failed. What is the full path of the file the attacker attempted to view? Include the entire path including all punctuation (e.g. '/', ",'.').
10. There are two types of HTTP response codes sent by the server to the attacker. What are the numbers and their explanations using this site https://developer.mozilla.org/en-US/docs/Web?HTTP/Status?
11. User agents are used to determining the client's browser and operating system. In this attack, the adversary used 13 different user agents. Using this site https://developers.whatismybrowser.com/useragents/parse/#parse-useragent, what are the web browser version and operating system of each?
12. Web spiders are applications that "crawl" the Internet and catalog all resources. This operation is performed by legitimate sites like Google, Yahoo, and Baidu. It appears that the adversary attempted to misdirect investigators by changing their user-agent to one that resembles a web spider. What is this user-agent in its entirety?

13. This attacker installed a web shell backdoor on this system. What is the name of the file containing the web shell

14. What is the file name of the IIS log file that contained the attack?

15. What is the version of this IIS server?

Scope of Work:

- Acquisition of the forensic image from Professor Stauffer in the UTSA Canvas website.
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.

Evidence Analyzed

This section provides details of the digital evidence collected

Evidence ID	**E001**
Name	IIS Webserver Logs - November 2020.7z
Type	Zip archive data, at least v2.0 to extract, compression method=deflate
Size	597,520 bytes (0.57MB)
MD5	1518C2899975CEC8DCB66BA4EB07BE84
SHA1	FACE86CDA0F1384A70445D68EA588FEDCBE0AF94
SHA256	466E87B68017F28F2B32C7B2E69EB692048DE8FB69C5565870864207D7254714

Tools Used

Workstation

Hostname	**Operating System**	**Build**	**Physical / Virtual**	**Built**
IS-4523-001-WINDOWS	Windows 11	2021	Virtual	09/06/2025

Software

Name	**Version**	**Release**	**Purpose**
Firefox Developer Edition	144.0	Sep 2025	Used for OSINT
Windows Powershell	7.5.3	Sep 2025	Used for parsing log files with Get-Content

Analysis Findings

Overview of Examination Procedures

The forensic analysis of the provided IIS web server logs was conducted in a structured, repeatable manner to ensure accuracy and evidentiary integrity. The logs (**u_ex201109.log**, **u_ex201110.log**, and **u_ex201111.log**) were examined using Windows PowerShell, more specifically the **Get-Content command**, as the primary tool for filtering, parsing, and counting log entries. Additionally, OSINT was needed for one of the questions provided to the examiner from the client. The evidence collected was provided by Professor Stauffer in an .zip folder. The evidence was verified via **MD5, SHA1, and SHA256 hashes** to maintain integrity.

Additional targeted analysis was performed using:

- **Windows Powershell** → to analyze the IIS web server logs using Get-Content
- **Firefox Developer Edition** → used as primary web browser for the purpose of OSINT

Throughout the process, all findings were documented, and cryptographic hash values were maintained for validation.

Evidence Reviewed

1. **IIS Webserver Log folder (E001)**: Zipped folder containing 3 webserver logs

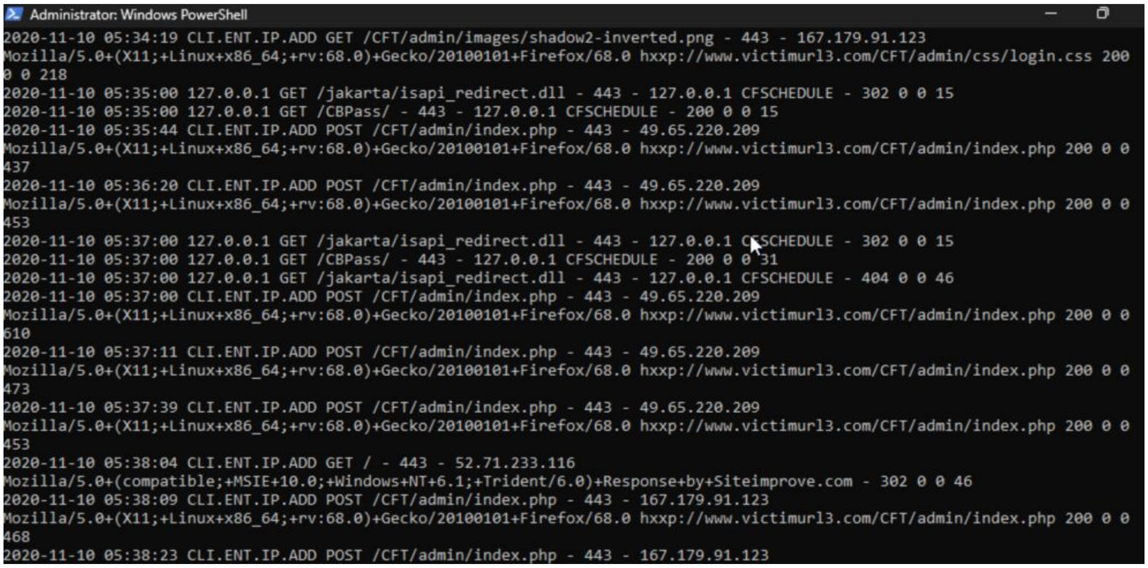
Key Findings

1. What is the exact date and timestamp the adversary began their attack? (Time must be in UTC)

- **Analysis Performed:**
    - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command. However more specifically, the exact date and timestamp the adversary began their attack was within the u_ex201110.log file.
    - Before the examiner was asked to conduct incident response operations, the client extracted and performed basic analysis on the logs regarding the initial compromise of the system. As stated within the client's information and this lab's scope of work, the initial compromise occurred Monday, November 9, 2020, at approximately 11:30:00 PM GMT-06:00.
    - The examiner first converted the timezone of the initial compromise given to the examiner into UTC which is the universal timezone within this report.
    - The examiner also used the command, *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "2020-11-10 05:29" | Select-String "49.65.220.209,* to confirm.

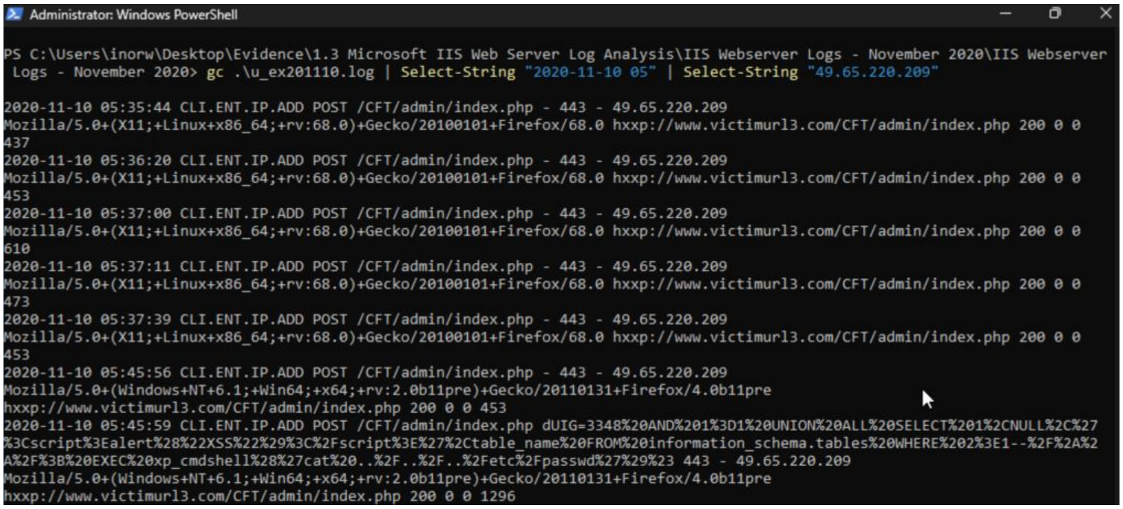
        - The examiner conducted this operation since the client stated that the compromise occurred at approximately 11:30:00PM GMT-06:00 which is an approximate.
    - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String “2020-11-10 05:29*
- **Answer:**
  As shown in Figure 1, suspicious activity began at **2020-11-10 05:35:44 UTC** which indicates IOC (indication of compromise), hence when the adversary began their attack. This is also confirmed with the POST HTTP requests which is what the adversary was trying to accomplish as shown in Figure 2.

- **Supporting Evidence:**



```
2020-11-10 05:34:19 CLI.ENT.IP.ADD GET /CFT/admin/images/shadow2-inverted.png - 443 - 167.179.91.123
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/css/login.css 200
0 0 218
2020-11-10 05:35:00 127.0.0.1 GET /jakarta/isapi_redirect.dll - 443 - 127.0.0.1 CFSCHEDULE - 302 0 0 15
2020-11-10 05:35:00 127.0.0.1 GET /CBPass/ - 443 - 127.0.0.1 CFSCHEDULE - 200 0 0 15
2020-11-10 05:35:44 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
437
2020-11-10 05:36:20 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:37:00 127.0.0.1 GET /jakarta/isapi_redirect.dll - 443 - 127.0.0.1 CFSCHEDULE - 302 0 0 15
2020-11-10 05:37:00 127.0.0.1 GET /CBPass/ - 443 - 127.0.0.1 CFSCHEDULE - 200 0 0 31
2020-11-10 05:37:00 127.0.0.1 GET /jakarta/isapi_redirect.dll - 443 - 127.0.0.1 CFSCHEDULE - 404 0 0 46
2020-11-10 05:37:00 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
610
2020-11-10 05:37:11 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
473
2020-11-10 05:37:39 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:38:04 CLI.ENT.IP.ADD GET / - 443 - 52.71.233.116
Mozilla/5.0+(compatible;+MSIE+10.0;+Windows+NT+6.1;+Trident/6.0)+Response+by+Siteimprove.com - 302 0 0 46
2020-11-10 05:38:09 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 167.179.91.123
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
468
2020-11-10 05:38:23 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 167.179.91.123
```

Figure 1. Shows the output and specifically where the attack began



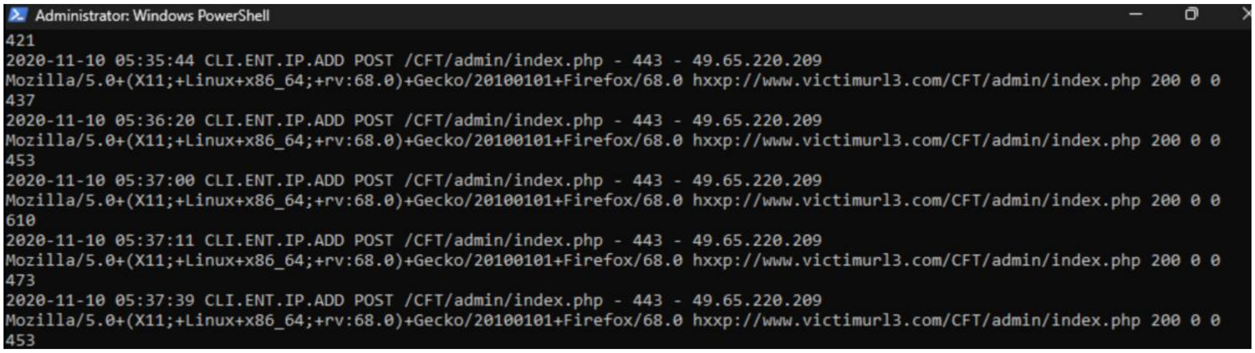
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201110.log | Select-String "2020-11-10 05" | Select-String "49.65.220.209"

2020-11-10 05:35:44 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
437
2020-11-10 05:36:20 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:37:00 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
610
2020-11-10 05:37:11 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
473
2020-11-10 05:37:39 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:45:56 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0 453
2020-11-10 05:45:59 CLI.ENT.IP.ADD POST /CFT/admin/index.php dUIG=3348%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27
%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2
A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 443 - 49.65.220.209
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0 1296
```

Figure 2. Shows the output for specifically the adversary IP address

2. *What is the source IP address of the adversary?*

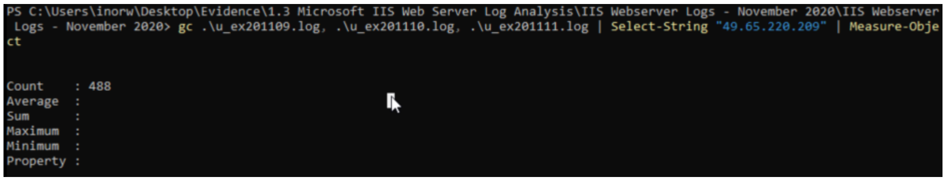
- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - As you can see in Figure 3, the adversary IP address that the examiner believes is, is 49.65.220.209. To verify, the examiner cross referenced what the client already knows about the adversary to ensure the correct IP address is recorded.
    - The client states, "web server recorded approximately 500 entries from the attackers IP address", therefore the examiner checked if the IP address, 49.65.220.209, has approximately 500 entries. As shown in Figure 4, the IP address (49.65.220.209) does.
      - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Measure-Object*
    - However, there is another IP address that has multiple POST requests and at around the same time of compromise, 167.179.91.123. Therefore to ensure that the examiner reports the correct IP address, the same command must be conducted previously to check how many entries the web server recorded and cross-reference it to the fact that the client provided. As shown in Figure 5, the IP address (167.179.91.123) has 399 entries.
      - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "167.179.91.123" | Measure-Object*
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "2020-11-10 05" | Select-String "/CFT/admin/index.php" | Select-String "POST"*
- **Answer:**
  The source IP address of the adversary is **49.65.220.209** as shown in Figure 3.

- **Supporting Evidence:**



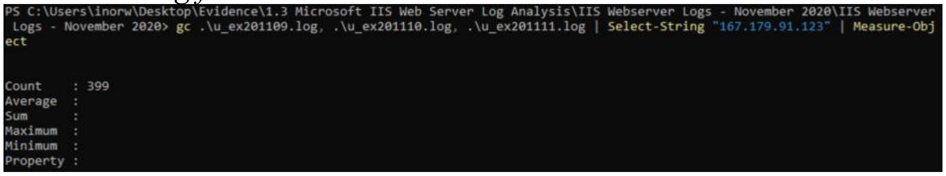
```
421
2020-11-10 05:35:44 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
437
2020-11-10 05:36:20 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:37:00 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
610
2020-11-10 05:37:11 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
473
2020-11-10 05:37:39 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
```

Figure 3. gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "2020-11-10 05" | Select-String "/CFT/admin/index.php" | Select-String "POST"



```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Measure-Obje
ct


Count    : 488
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

Figure 4. Showing the amount of entries the IP address "49.65.220.209" was recorded in the IIS web server log file



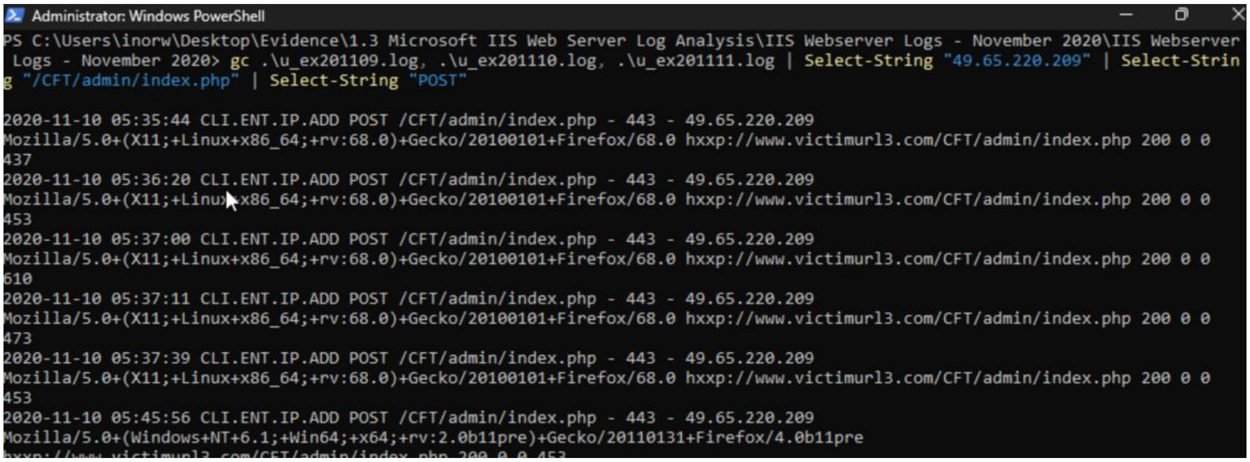
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "167.179.91.123" | Measure-Obj
ect


Count    : 399
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

Figure 5. Showing the amount of entries the IP address "167.179.91.123" was recorded in the IIS web server log file

3. What is the local IP address the adversary attacked? (Yes, it is not an actual IP address)

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "/CFT/admin/index.php" | Select-String "POST"*
- **Answer:**
  Since IIS logs record entries in W3C format and by examining the structure of the entries within the webserver logs, the second entry is the destination/local IP address. Therefore, the local IP address the adversary attacked is **CLI.ENT.IP.ADD** as shown in Figure 6. Which is not an IP address however the professor removed the local IP address for this lab to ensure the client's IP address is not exposed.

- **Supporting Evidence:**



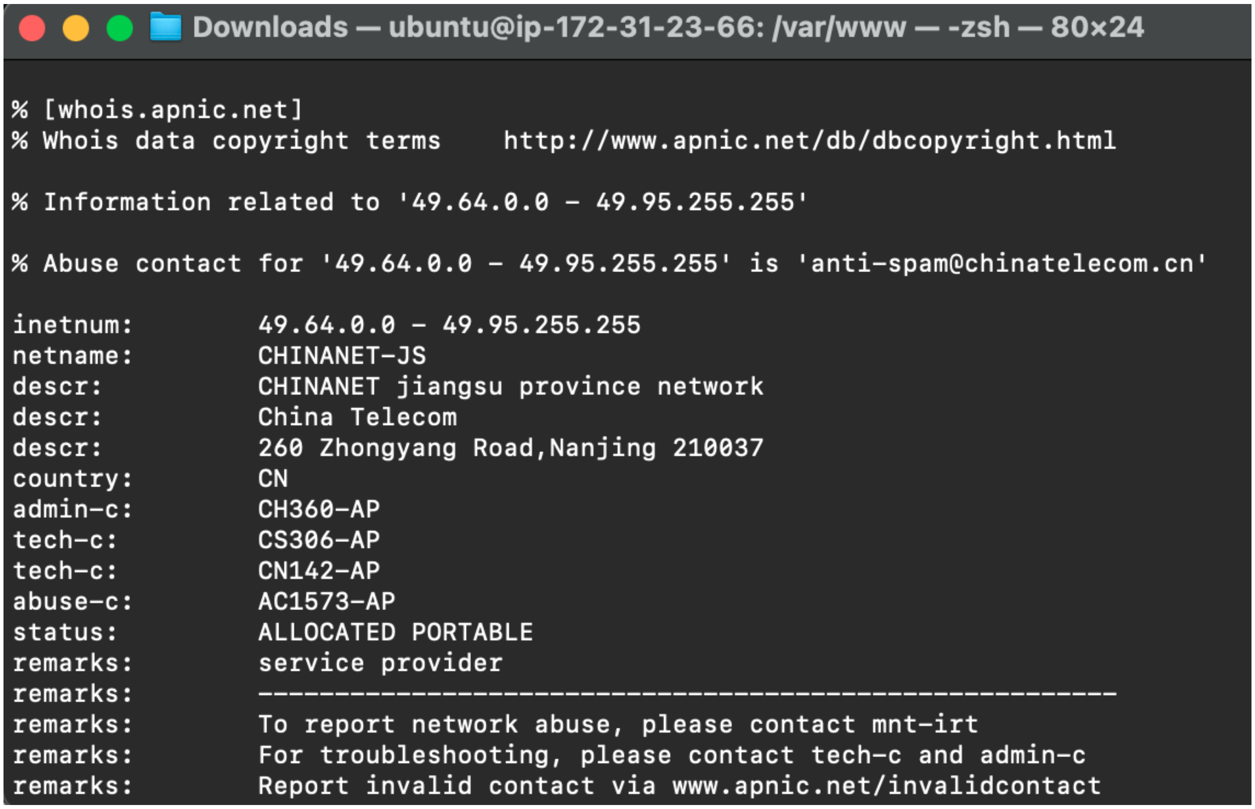
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "/CFT/admin/index.php" | Select-String "POST"

2020-11-10 05:35:44 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
437
2020-11-10 05:36:20 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:37:00 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
610
2020-11-10 05:37:11 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
473
2020-11-10 05:37:39 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0 hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0
453
2020-11-10 05:45:56 CLI.ENT.IP.ADD POST /CFT/admin/index.php - 443 - 49.65.220.209
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0 453
```

Figure 6. Shows the destination/local IP address from the log entries from 49.65.220.209

4. What country does the IP address reside in?

- **Analysis Performed:**
  - The examiner proceeded to use his host computer's terminal to conduct the whois command to find out what country does the adversary IP address reside in.
  - As shown in Figure 7, it shows the inetnum of 49.64.0.0 – 49.95.255.255 which is the IP range and the net name is CHINANET-JS residing in country code CN.
  - Command: *whois 49.65.220.209*
- **Answer:**
  The adversary IP address resides in China as show in Figure 7.

- **Supporting Evidence:**



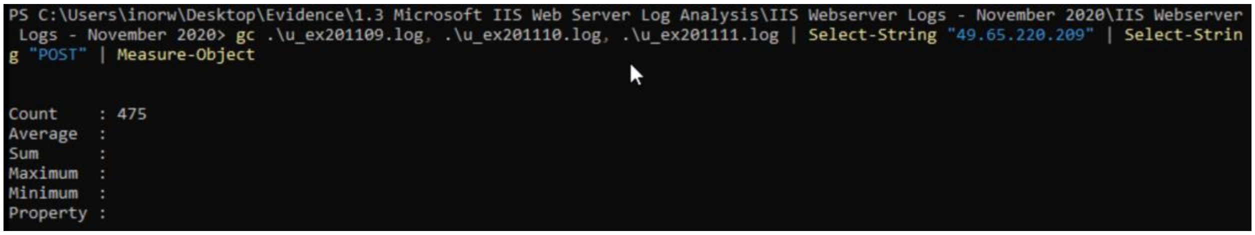
```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '49.64.0.0 - 49.95.255.255'

% Abuse contact for '49.64.0.0 - 49.95.255.255' is 'anti-spam@chinatelecom.cn'

inetnum:        49.64.0.0 - 49.95.255.255
netname:        CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          260 Zhongyang Road,Nanjing 210037
country:        CN
admin-c:        CH360-AP
tech-c:         CS306-AP
tech-c:         CN142-AP
abuse-c:        AC1573-AP
status:         ALLOCATED PORTABLE
remarks:        service provider
remarks:        --------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
```

Figure 7. whois command on the adversary IP address

5. How many POST requests were performed by the attacker?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "POST" | Measure-Object*
- **Answer:**
  After filtering for the strings, "49.65.220.209" and "POST", the count is 475 as shown in Figure 8. Therefore, the adversary performed **475 POST requests**.

- **Supporting Evidence:**



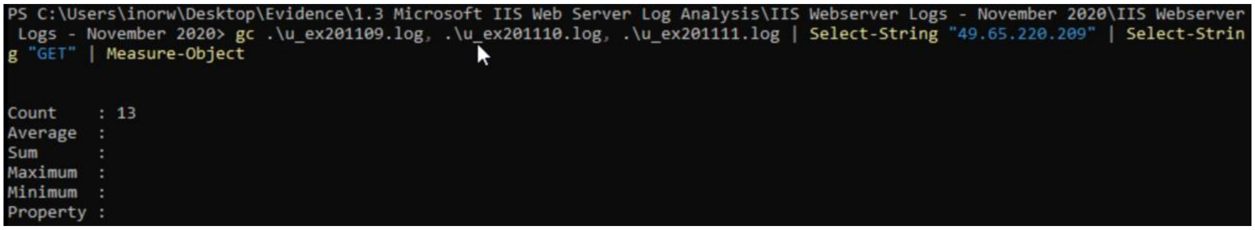
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "POST" | Measure-Object


Count    : 475
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

Figure 8. The count of POST requests that were performed from 49.65.220.209

6. How many GET requests were performed by the attacker?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "GET" | Measure-Object*
- **Answer:**
  After filtering for the strings, "49.65.220.209" and "GET", the count is 13 as shown in Figure 9. Therefore, the adversary performed **13 GET requests**.

- **Supporting Evidence:**

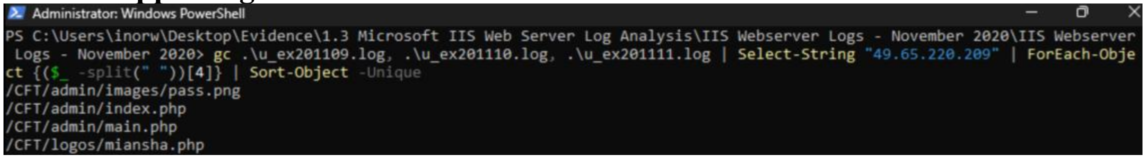


```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "GET" | Measure-Object


Count    : 13
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

Figure 9. The number of GET requests from 49.65.220.209

7. The attacker focused their attacks on four files (URI stubs), name them.

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Object {($_ -split(" "))[4]} | Sort-Object -Unique*
  - The ForEach-Object {($_ -split(" "))[4]} section takes each line of text that was found, splits it into pieces wherever there is a space, and then outputs only the fifth piece (index 4) from that line.
- **Answer:**
  Since IIS logs record entries in W3C format and by examining the structure of the entries within the webserver logs, the fourth entry is the URI stem. The examiner executed a command which shows only the fourth entry which is shown in Figure 10. Therefore, the four files (URI stubs) that the adversary focused their attacks on were: **"/CFT/admin/images/pass.png", "/CFT/admin/index.php", "/CFT/admin/main.php", "/CFT/logos/miansha.php".**
- **Supporting Evidence:**

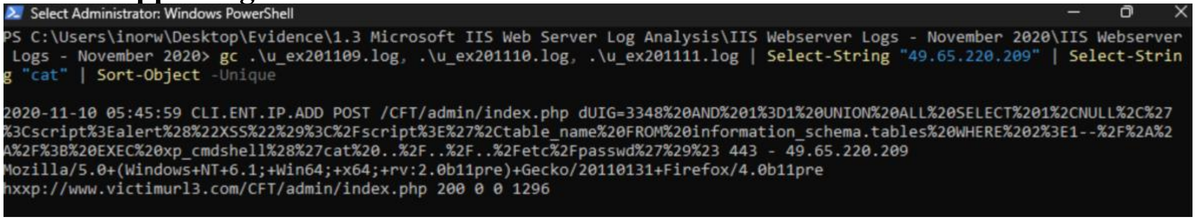


```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[4]} | Sort-Object -Unique
/CFT/admin/images/pass.png
/CFT/admin/index.php
/CFT/admin/main.php
/CFT/logos/miansha.php
```

Figure 10. The URI stubs within the log file

8. What is the exact date and timestamp the SQL injection attack occurred?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - As stated in question 9, the SQL inject attack attempted to perform a simple Linux command to **view the contents of a file**. Therefore, I used the "Select-String "cat" option to filter only for log entries that contain "cat" which is shown in Figure 11.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "cat" | Sort-Object -Unique*
- **Answer:**
  The exact date and timestamp when the SQL injection attacked occurred was **2020-11-10 05:45:59 UTC** which is shown in Figure 11.
- **Supporting Evidence:**



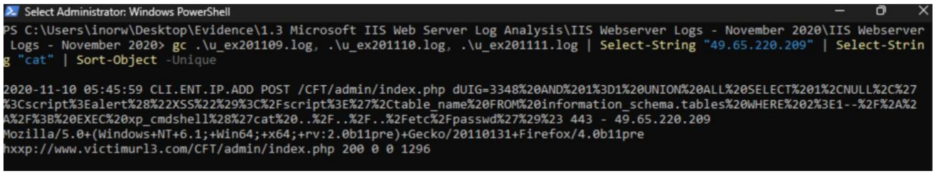
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "cat" | Sort-Object -Unique

2020-11-10 05:45:59 CLI.ENT.IP.ADD POST /CFT/admin/index.php dUIG=3348%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27
%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2
A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 443 - 49.65.220.209
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0 1296
```

Figure 11. Showing the SQL injection from 49.65.220.209 which shows the date and timestamp

9. The SQL injection attack attempted to perform a simple Linux command to view the contents of a file. Obviously, this is a Windows system, so this would have failed. What is the full path of the file the attacker attempted to view? Include the entire path including all punctuation (e.g. '/', ",'.').

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "cat" | Sort-Object -Unique*
- **Answer:**
  The full path of the file the adversary attempted to view was **"../../../etc/passwd"** as shown in Figure 12.

- **Supporting Evidence:**



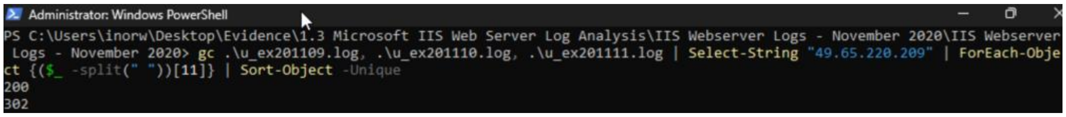
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "cat" | Sort-Object -Unique

2020-11-10 05:45:59 CLI.ENT.IP.ADD POST /CFT/admin/index.php dUIG=3348%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27
%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2
A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 443 - 49.65.220.209
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
hxxp://www.victimurl3.com/CFT/admin/index.php 200 0 0 1296
```

Figure 12. Shows the SQL injection attack attempted from 49.65.220.209

10. There are two types of HTTP response codes sent by the server to the attacker. What are the numbers and their explanations using this site https://developer.mozilla.org/en-US/docs/Web/HTTP/Status?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - The 11th entry in the IIS W3C log is the HTTP response code.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Object {($_ -split(" "))[11]} | Sort-Object -Unique*
- **Answer:**
  The server returned two types of HTTP response codes to the attacker: 200 and 302. A 200 OK indicates the request succeeded (for example GET, POST, PUT, HEAD, etc.). A 302 Found indicates the requested resource is temporarily available at a different URI; the response typically includes a Location header with the temporary URI.

- **Supporting Evidence:**



```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[11]} | Sort-Object -Unique
200
302
```

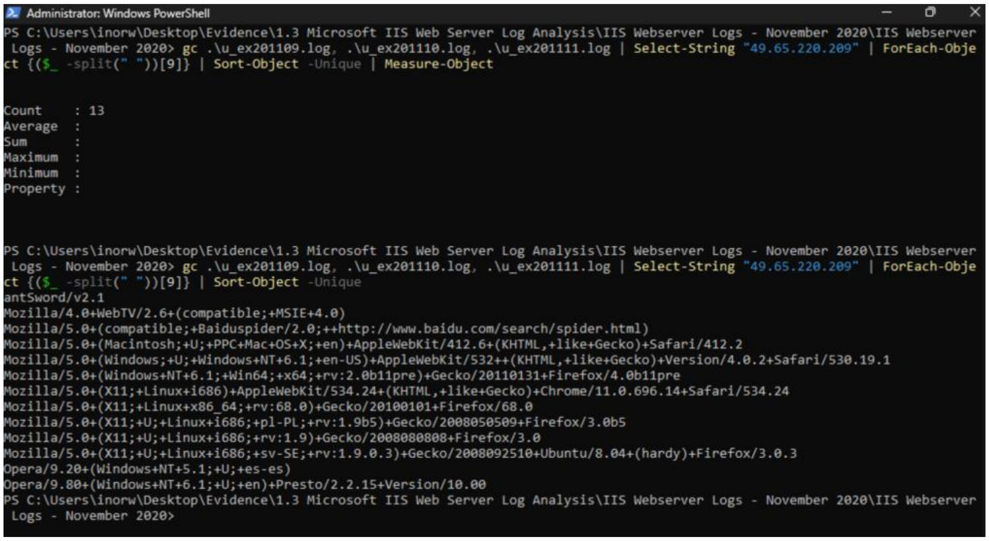
Figure 13. The command output that shows the unique HTTP response codes from 49.65.220.209

11. User agents are used to determining the client’s browser and operating system. In this attack, the adversary used 13 different user agents. Using this site https://developers.whatismybrowser.com/useragents/parse/#parse-useragent, what are the web browser version and operating system of each?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - The 9th entry in the IIS W3C webserver log is the user agent.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String “49.65.220.209” | ForEach-Object {($_ -split(“ “))[9]} | Sort-Object -Unique*
- **Answer:**

  The 13 different user agents, which are used to determine the client’s browser and operating system, are shown in Figure 14. From those user-agent strings: **antSword/v2.1** is the antSword webshell client (v2.1; OS not specified). **Mozilla/4.0 (compatible; MSIE 4.0)** is Internet Explorer **4.0** on Windows (unspecified edition). **Baiduspider/2.0** is the Baidu crawler (bot; no OS). **Safari/412.2** on **Mac OS X (PowerPC)** corresponds to Safari **2.0** (build 412.2). **Safari/530.19.1** with **Version/4.0.2+** on **Windows NT 4.0** is Safari **4.0.2+**. The **Firefox/4.0b1pre** UA indicates Firefox **4.0 beta 1 pre-release** on **Windows 7 (NT 6.1)**. **Chrome/11.0.696.14** is Google Chrome **11.0.696.14** on **Linux x86_64**. **Firefox/68.0** is Firefox **68.0** on **Linux x86_64**. The mixed UA showing **Firefox/3.0b5** (rv:1.9.3a5pre) is Firefox **3.0 beta 5** on **Windows XP (NT 5.1)**. The hybrid UA with **Ubuntu/8.04 (hardy) Firefox/3.0.3** but **Windows NT 6.0** suggests a spoofed string; browser is Firefox **3.0.3** while the OS claims **Windows Vista (NT 6.0)** despite the Ubuntu tag. Finally, the **Opera Version/10.00 (Presto/2.2.15)** string is Opera **10.00** on **Windows 7 (NT 6.1)**.

- **Supporting Evidence:**



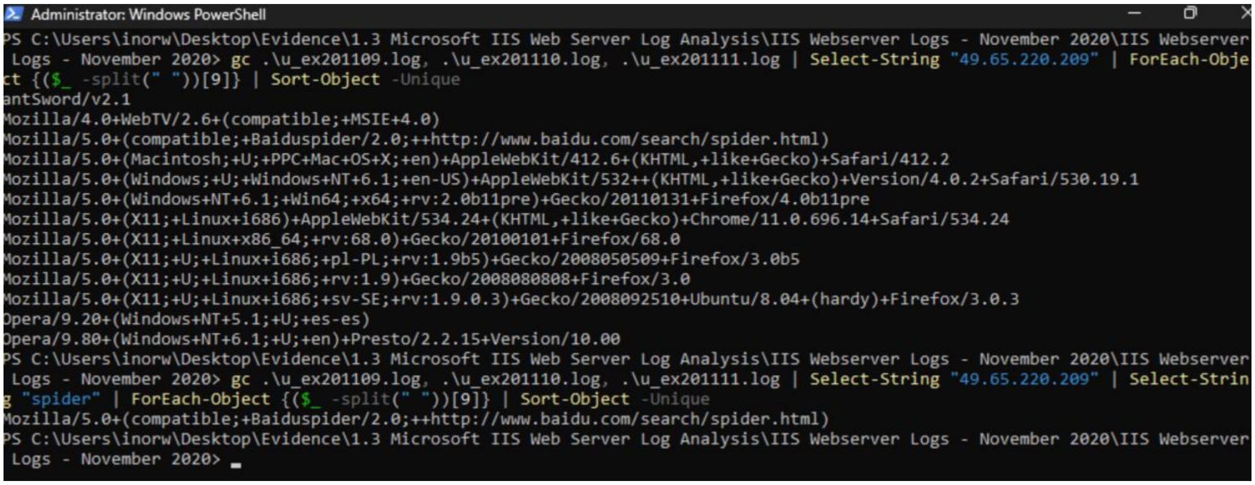
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[9]} | Sort-Object -Unique | Measure-Object


Count    : 13
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[9]} | Sort-Object -Unique
antSword/v2.1
Mozilla/4.0+WebTV/2.6+(compatible;+MSIE+4.0)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
Mozilla/5.0+(Macintosh;+U;+PPC+Mac+OS+X;+en)+AppleWebKit/412.6+(KHTML,+like+Gecko)+Safari/412.2
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+en-US)+AppleWebKit/532++(KHTML,+like+Gecko)+Version/4.0.2+Safari/530.19.1
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
Mozilla/5.0+(X11;+Linux+i686)+AppleWebKit/534.24+(KHTML,+like+Gecko)+Chrome/11.0.696.14+Safari/534.24
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0
Mozilla/5.0+(X11;+U;+Linux+i686;+pl-PL;+rv:1.9b5)+Gecko/2008050509+Firefox/3.0b5
Mozilla/5.0+(X11;+U;+Linux+i686;+rv:1.9)+Gecko/2008080808+Firefox/3.0
Mozilla/5.0+(X11;+U;+Linux+i686;+sv-SE;+rv:1.9.0.3)+Gecko/2008092510+Ubuntu/8.04+(hardy)+Firefox/3.0.3
Opera/9.20+(Windows+NT+5.1;+U;+es-es)
Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.2.15+Version/10.00
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020>
```

Figure 14. Command output showing the adversary's user-agents

12. Web spiders are applications that "crawl" the Internet and catalog all resources. This operation is performed by legitimately sites like Google, Yahoo, and Baidu. It appears that the adversary attempted to misdirect investigators by changing their user-agent to one that resembles a web spider. What is this user-agent in its entirety?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - The examiner sorted for "spider" within the logs as shown in Figure 15.
    - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-String "spider" | ForEach-Object {($_ -split(" "))[9]} | Sort-Object -Unique*
  - Although, the examiner primarily looked through the previous command's output (question 12), in order to find the spider as shown in Figure 14 and 15.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Object {($_ -split(" "))[9]} | Sort-Object -Unique*
- **Answer:**
  The user-agent that is being changed to resemble a web spider by the adversary to misdirect investigators is "**Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html**)" as shown in Figure 15.

- **Supporting Evidence:**



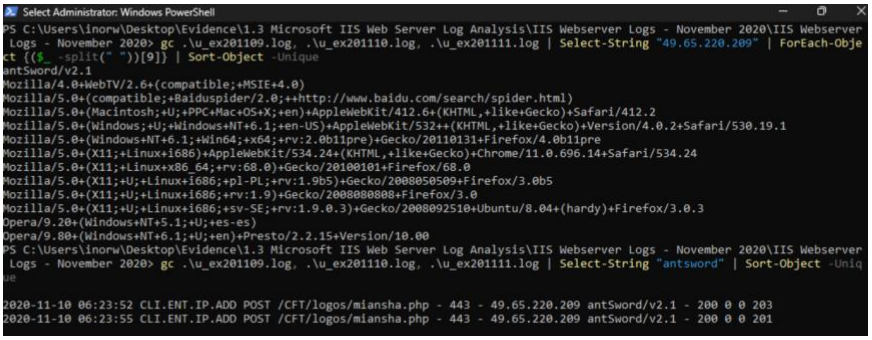
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[9]} | Sort-Object -Unique
antSword/v2.1
Mozilla/4.0+WebTV/2.6+(compatible;+MSIE+4.0)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
Mozilla/5.0+(Macintosh;+U;+PPC+Mac+OS+X;+en)+AppleWebKit/412.6+(KHTML,+like+Gecko)+Safari/412.2
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+en-US)+AppleWebKit/532++(KHTML,+like+Gecko)+Version/4.0.2+Safari/530.19.1
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
Mozilla/5.0+(X11;+Linux+i686)+AppleWebKit/534.24+(KHTML,+like+Gecko)+Chrome/11.0.696.14+Safari/534.24
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0
Mozilla/5.0+(X11;+U;+Linux+i686;+pl-PL;+rv:1.9b5)+Gecko/2008050509+Firefox/3.0b5
Mozilla/5.0+(X11;+U;+Linux+i686;+rv:1.9)+Gecko/2008080808+Firefox/3.0
Mozilla/5.0+(X11;+U;+Linux+i686;+sv-SE;+rv:1.9.0.3)+Gecko/2008092510+Ubuntu/8.04+(hardy)+Firefox/3.0.3
Opera/9.20+(Windows+NT+5.1;+U;+es-es)
Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.2.15+Version/10.00
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | Select-Strin
g "spider" | ForEach-Object {($_ -split(" "))[9]} | Sort-Object -Unique
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> _
```

Figure 15. User-agents output, more specifically showing the webspider.

13. This attacker installed a web shell backdoor on this system. What is the name of the file containing the web shell?

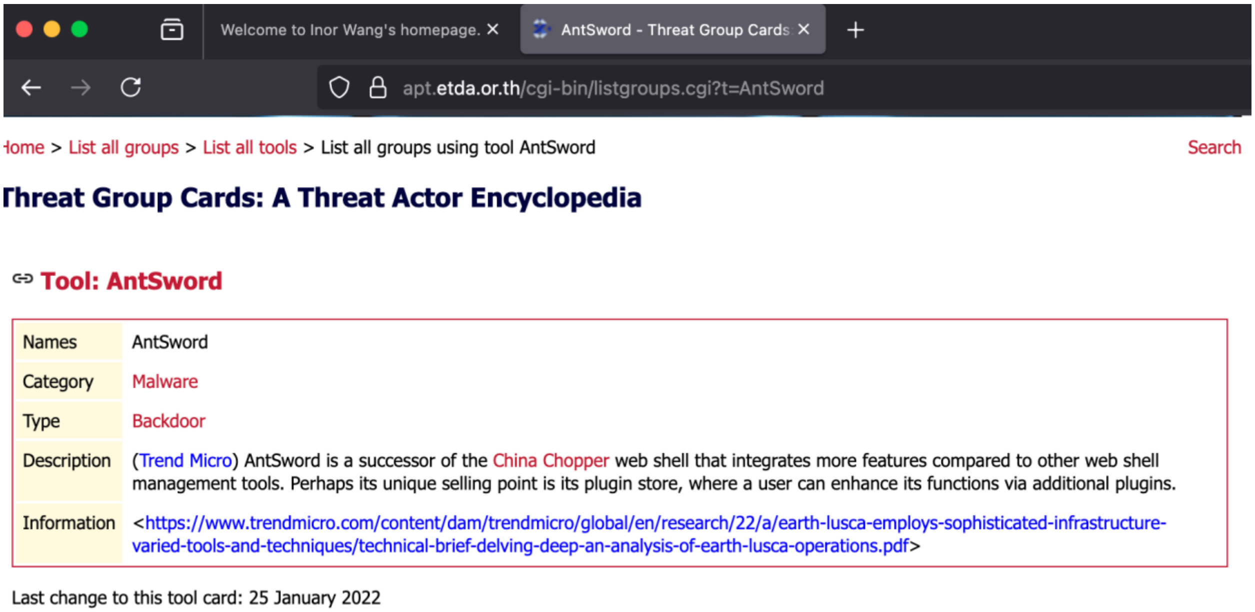
- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - Using OSINT resources as shown in Figures 17 and 18, the examiner discovered that AntSword is a web shell that is often used for backdoors.
  - Command: *gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "antSword" | Sort-Object -Unique*
- **Answer:**
  The adversary installed a web shell backdoor on the system using antSword v2.1 and the name of the file containing the web shell is **miansha.php** as shown in Figure 16.

- **Supporting Evidence:**



```
Select Administrator: Windows PowerShell
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "49.65.220.209" | ForEach-Obje
ct {($_ -split(" "))[9]} | Sort-Object -Unique
antSword/v2.1
Mozilla/4.0+WebTV/2.6+(compatible;+MSIE+4.0)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
Mozilla/5.0+(Macintosh;+U;+PPC+Mac+OS+X;+en)+AppleWebKit/412.6+(KHTML,+like+Gecko)+Safari/412.2
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+en-US)+AppleWebKit/532++(KHTML,+like+Gecko)+Version/4.0.2+Safari/530.19.1
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64;+rv:2.0b11pre)+Gecko/20110131+Firefox/4.0b11pre
Mozilla/5.0+(X11;+Linux+i686)+AppleWebKit/534.24+(KHTML,+like+Gecko)+Chrome/11.0.696.14+Safari/534.24
Mozilla/5.0+(X11;+Linux+x86_64;+rv:68.0)+Gecko/20100101+Firefox/68.0
Mozilla/5.0+(X11;+U;+Linux+i686;+pl-PL;+rv:1.9b5)+Gecko/2008050509+Firefox/3.0b5
Mozilla/5.0+(X11;+U;+Linux+i686;+rv:1.9)+Gecko/2008080808+Firefox/3.0
Mozilla/5.0+(X11;+U;+Linux+i686;+sv-SE;+rv:1.9.0.3)+Gecko/2008092510+Ubuntu/8.04+(hardy)+Firefox/3.0.3
Opera/9.20+(Windows+NT+5.1;+U;+es-es)
Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.2.15+Version/10.00
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log, .\u_ex201110.log, .\u_ex201111.log | Select-String "antsword" | Sort-Object -Uniq
ue

2020-11-10 06:23:52 CLI.ENT.IP.ADD POST /CFT/logos/miansha.php - 443 - 49.65.220.209 antSword/v2.1 - 200 0 0 203
2020-11-10 06:23:55 CLI.ENT.IP.ADD POST /CFT/logos/miansha.php - 443 - 49.65.220.209 antSword/v2.1 - 200 0 0 201
```

Figure 16. Showing user-agents, more specifically the antSword



Welcome to Inor Wang's homepage. ✕
AntSword - Threat Group Cards ✕
+
apt.etda.or.th/cgi-bin/listgroups.cgi?t=AntSword

Home > List all groups > List all tools > List all groups using tool AntSword   Search

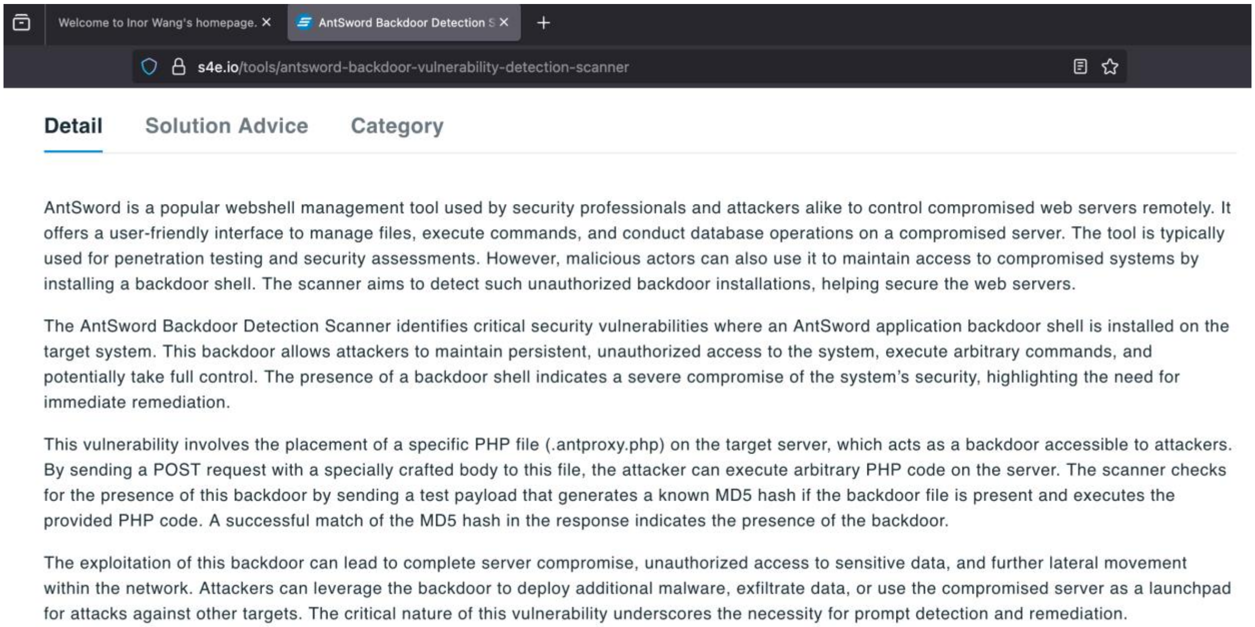
Threat Group Cards: A Threat Actor Encyclopedia

Tool: AntSword

Names	AntSword
Category	Malware
Type	Backdoor
Description	(Trend Micro) AntSword is a successor of the China Chopper web shell that integrates more features compared to other web shell management tools. Perhaps its unique selling point is its plugin store, where a user can enhance its functions via additional plugins.
Information	<https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf>

Last change to this tool card: 25 January 2022

Figure 17. OSINT about AntSword


Welcome to Inor Wang's homepage.
AntSword Backdoor Detection S
s4e.io/tools/antsword-backdoor-vulnerability-detection-scanner
Detail
Solution Advice
Category

AntSword is a popular webshell management tool used by security professionals and attackers alike to control compromised web servers remotely. It offers a user-friendly interface to manage files, execute commands, and conduct database operations on a compromised server. The tool is typically used for penetration testing and security assessments. However, malicious actors can also use it to maintain access to compromised systems by installing a backdoor shell. The scanner aims to detect such unauthorized backdoor installations, helping secure the web servers.

The AntSword Backdoor Detection Scanner identifies critical security vulnerabilities where an AntSword application backdoor shell is installed on the target system. This backdoor allows attackers to maintain persistent, unauthorized access to the system, execute arbitrary commands, and potentially take full control. The presence of a backdoor shell indicates a severe compromise of the system's security, highlighting the need for immediate remediation.

This vulnerability involves the placement of a specific PHP file (.antproxy.php) on the target server, which acts as a backdoor accessible to attackers. By sending a POST request with a specially crafted body to this file, the attacker can execute arbitrary PHP code on the server. The scanner checks for the presence of this backdoor by sending a test payload that generates a known MD5 hash if the backdoor file is present and executes the provided PHP code. A successful match of the MD5 hash in the response indicates the presence of the backdoor.

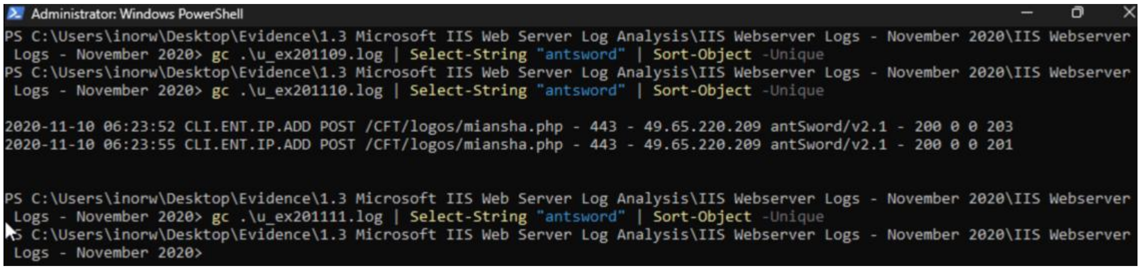
The exploitation of this backdoor can lead to complete server compromise, unauthorized access to sensitive data, and further lateral movement within the network. Attackers can leverage the backdoor to deploy additional malware, exfiltrate data, or use the compromised server as a launchpad for attacks against other targets. The critical nature of this vulnerability underscores the necessity for prompt detection and remediation.

Figure 18. OSINT about AntSword

14. What is the file name of the IIS log file that contained the attack?

- **Analysis Performed:**
  - The u_ex201109.log, u_ex201110.log, u_ex201111.log files were analyzed through the Windows Powershell using the Get-Content (gc) command.
  - The examiner searched for "antSword" within all three log files to find out which IIS log file contained the attack as shown in Figure 19.
  - Command 1: *gc .\u_ex201109.log | Select-String "antSword" | Sort-Object -Unique*
  - Command 2: *gc .\u_ex201110.log | Select-String "antSword" | Sort-Object -Unique*
  - Command 3: *gc .\u_ex201111.log | Select-String "antSword" | Sort-Object -Unique*
- **Answer:**
  The file name of the IIS log file that contained the attack is **u_ex201110.log** as shown in Figure 19.

- **Supporting Evidence:**



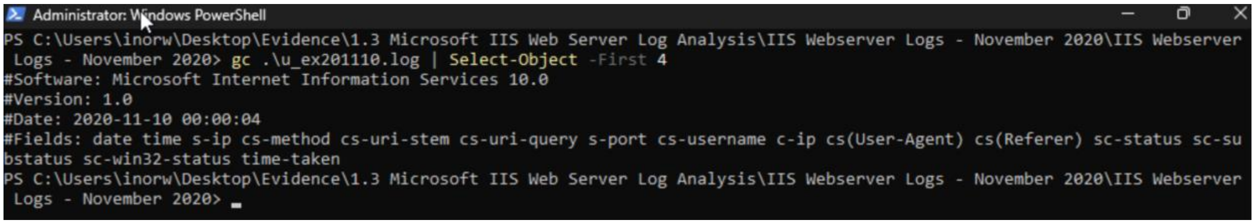
```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201109.log | Select-String "antsword" | Sort-Object -Unique
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201110.log | Select-String "antsword" | Sort-Object -Unique

2020-11-10 06:23:52 CLI.ENT.IP.ADD POST /CFT/logos/miansha.php - 443 - 49.65.220.209 antSword/v2.1 - 200 0 0 203
2020-11-10 06:23:55 CLI.ENT.IP.ADD POST /CFT/logos/miansha.php - 443 - 49.65.220.209 antSword/v2.1 - 200 0 0 201


PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201111.log | Select-String "antsword" | Sort-Object -Unique
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020>
```

Figure 19. Finding the IIS log file that contained the attack

15. What is the version of this IIS server?

- **Analysis Performed:**
    - The u_ex201110.log files was analyzed through the Windows Powershell using the Get-Content (gc) command.
    - The examiner got the contents of the file and sorted to only look at the first 4 lines which contains information about the log file.
    - As shown in Figure 20, it states "#Software: Microsoft Internet Information Services 10.0".
    - Command: *gc .\u_ex201110.log | Select-Object -First 4*
- **Answer:**
  The version of the IIS server is **10.0** as shown in Figure 20.

- **Supporting Evidence:**



```
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> gc .\u_ex201110.log | Select-Object -First 4
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2020-11-10 00:00:04
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-su
bstatus sc-win32-status time-taken
PS C:\Users\inorw\Desktop\Evidence\1.3 Microsoft IIS Web Server Log Analysis\IIS Webserver Logs - November 2020\IIS Webserver
 Logs - November 2020> _
```

Figure 20. Showing the first 4 lines of the IIS webserver log

Conclusion

The examiner, Inor Wang, enjoyed this lab! There is no critique from me.

References

0daybug. (n.d.). AntSword backdoor vulnerability. CNBlogs. https://www.cnblogs.com/0daybug/p/16740163.html.

AntSword. (n.d.). AntSword. Electronic Transactions Development Agency (ETDA). https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=AntSword.

Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.

Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.

Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.

Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.

Reddy, N. (2019). Practical cyber forensics: An incident-based approach to forensic investigations. APress. https://doi.org/10.1007/978-1-4842-4460-9.

S4E. (n.d.). AntSword backdoor vulnerability detection scanner. S4E. https://s4e.io/tools/antsword-backdoor-vulnerability-detection-scanner.