LAB REPORT

Final Exam Part 2 Fall 2023 A

Richard Flores

Northern Virginia Community College

ITN 262 01YA

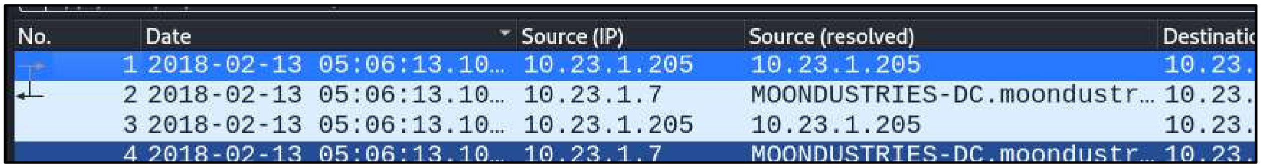
Prof. “Michael” Hon

December 11, 2023

I. Part A

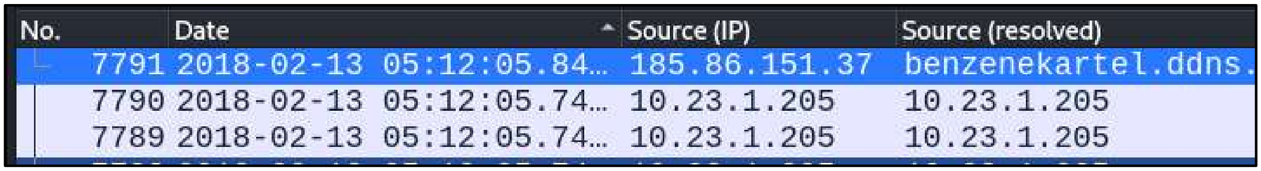
A. Date and time of the malicious activity in UTC (GMT).

1. **February 13, 2018 at 5:06 AM to 5:12 AM**



No.	Date	Source (IP)	Source (resolved)	Destinatic
1	2018-02-13 05:06:13.10…	10.23.1.205	10.23.1.205	10.23.
2	2018-02-13 05:06:13.10…	10.23.1.7	MOONDUSTRIES-DC.moondustr…	10.23.
3	2018-02-13 05:06:13.10…	10.23.1.205	10.23.1.205	10.23.
4	2018-02-13 05:06:13.10…	10.23.1.7	MOONDUSTRIES-DC.moondustr…	10.23.

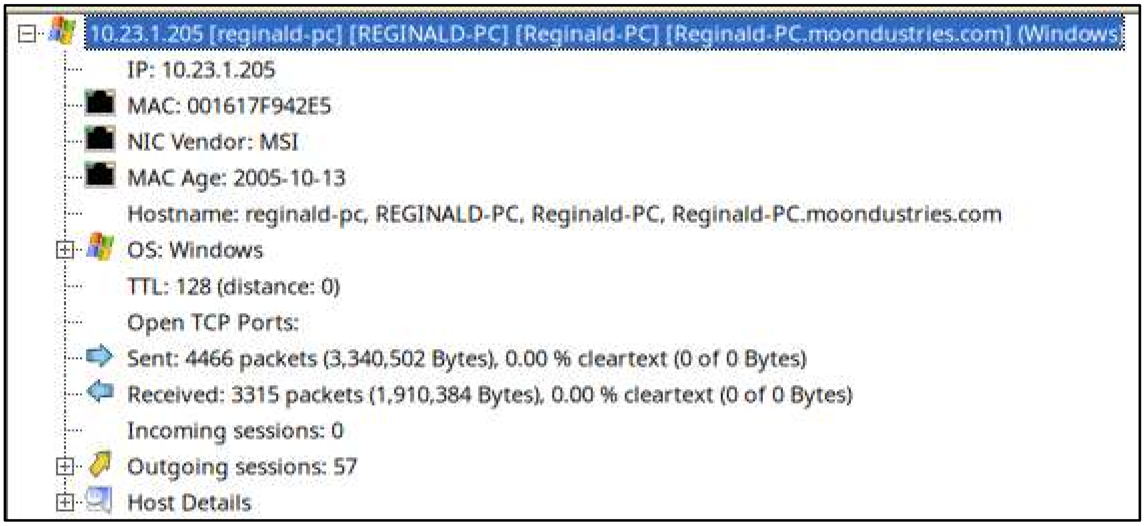
…



No.	Date	Source (IP)	Source (resolved)
7791	2018-02-13 05:12:05.84…	185.86.151.37	benzenekartel.ddns.
7790	2018-02-13 05:12:05.74…	10.23.1.205	10.23.1.205
7789	2018-02-13 05:12:05.74…	10.23.1.205	10.23.1.205

B. IP address of the affected Windows host.

1. **10.23.1.205**



```
10.23.1.205 [reginald-pc] [REGINALD-PC] [Reginald-PC] [Reginald-PC.moondustries.com] (Windows)
    IP: 10.23.1.205
    MAC: 001617F942E5
    NIC Vendor: MSI
    MAC Age: 2005-10-13
    Hostname: reginald-pc, REGINALD-PC, Reginald-PC, Reginald-PC.moondustries.com
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 4466 packets (3,340,502 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 3315 packets (1,910,384 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 57
    Host Details
```

C. Mac address of the affected Windows host.

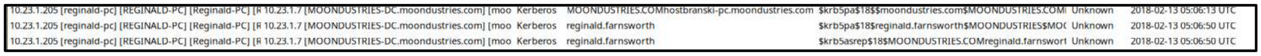
1. **00:16:17:F9:42:E5 (see above)**

D. Host name of the affected Windows host.

1. **reginald-pc (see above)**

E. User account name on the affected Windows host.

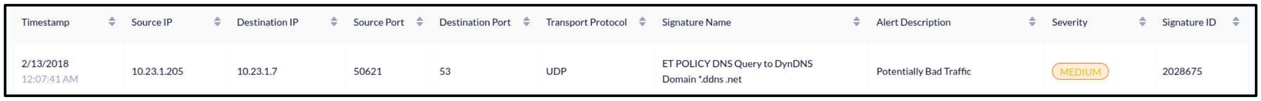
1. **reginald.farnsworth**



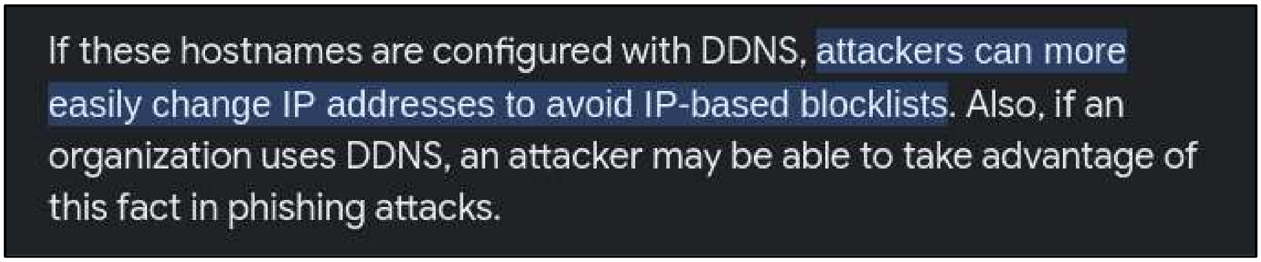
```
10.23.1.205 [reginald-pc] [REGINALD-PC] [Reginald-PC] [R 10.23.1.7 [MOONDUSTRIES-DC.moondustries.com] [moo  Kerberos   MOONDUSTRIES.COMhostbranski-pc.moondustries.com  $krb5pa$18$$moondustries.com$MOONDUSTRIES.COMI  Unknown   2018-02-13 05:06:13 UTC
10.23.1.205 [reginald-pc] [REGINALD-PC] [Reginald-PC] [R 10.23.1.7 [MOONDUSTRIES-DC.moondustries.com] [moo  Kerberos   reginald.farnsworth                              $krb5pa$18$reginald.farnsworth$MOONDUSTRIES$MO(  Unknown   2018-02-13 05:06:50 UTC
10.23.1.205 [reginald-pc] [REGINALD-PC] [Reginald-PC] [R 10.23.1.7 [MOONDUSTRIES-DC.moondustries.com] [moo  Kerberos   reginald.farnsworth                              $krb5asrep$18$MOONDUSTRIES.COMreginald.farnswort  Unknown   2018-02-13 05:06:50 UTC
```

F. **What malware might be involved.**

1. **Suspect DNS poisoning was likely**

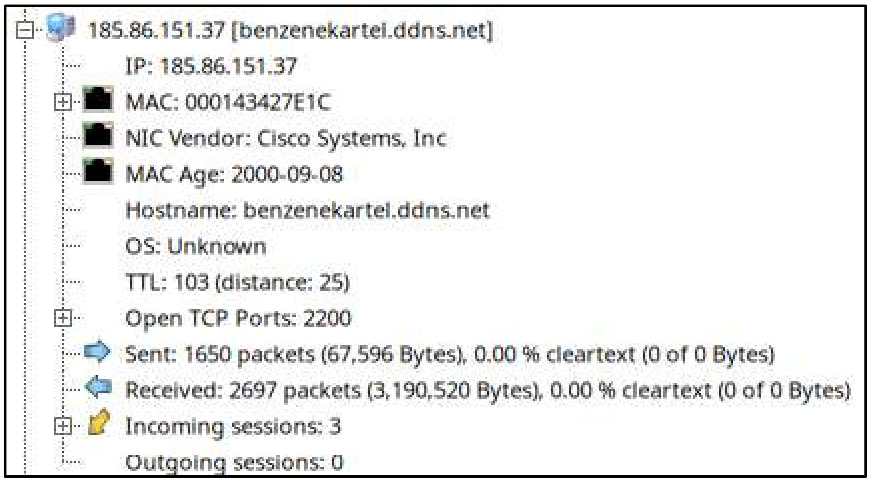


Timestamp	Source IP	Destination IP	Source Port	Destination Port	Transport Protocol	Signature Name	Alert Description	Severity	Signature ID
2/13/2018 12:07:41 AM	10.23.1.205	10.23.1.7	50621	53	UDP	ET POLICY DNS Query to DynDNS Domain *.ddns .net	Potentially Bad Traffic	MEDIUM	2028675



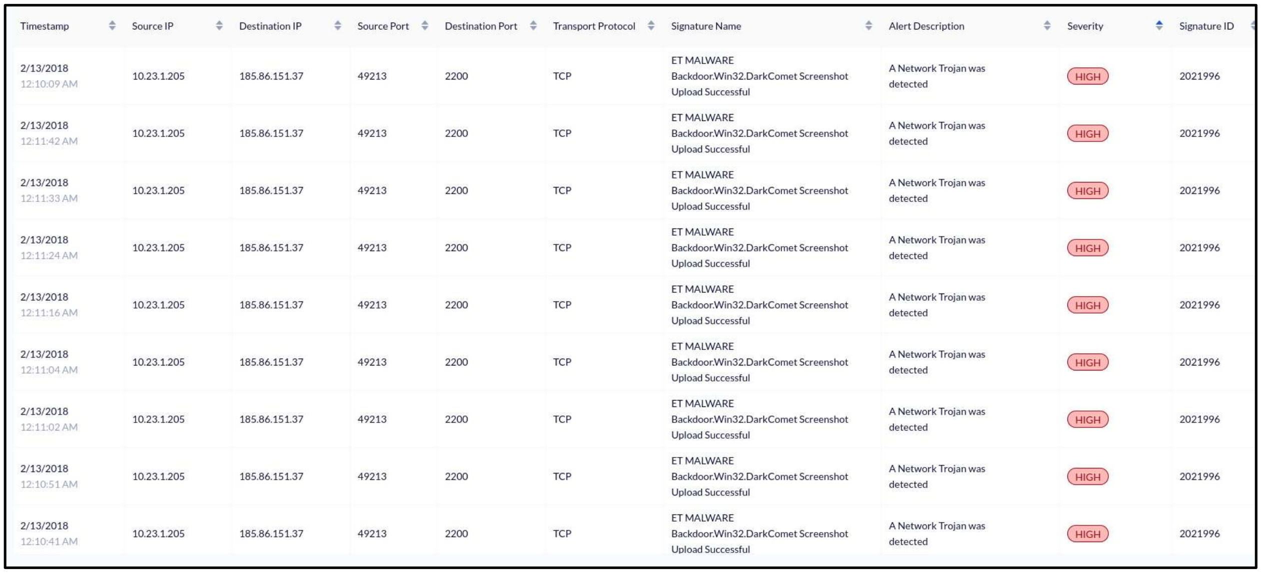
If these hostnames are configured with DDNS, attackers can more easily change IP addresses to avoid IP-based blocklists. Also, if an organization uses DDNS, an attacker may be able to take advantage of this fact in phishing attacks.

2. **Attackers domain name is suspicious. Appears to be attempting to appear as a DNS server, but TLD is .net.**



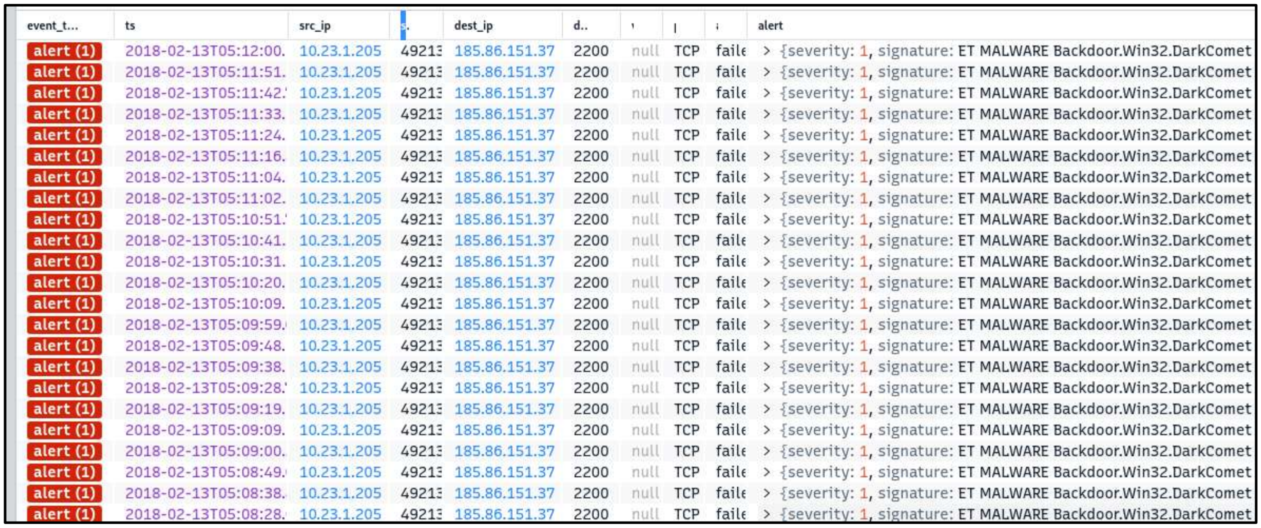
```
185.86.151.37 [benzenekartel.ddns.net]
    IP: 185.86.151.37
    MAC: 000143427E1C
    NIC Vendor: Cisco Systems, Inc
    MAC Age: 2000-09-08
    Hostname: benzenekartel.ddns.net
    OS: Unknown
    TTL: 103 (distance: 25)
    Open TCP Ports: 2200
    Sent: 1650 packets (67,596 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 2697 packets (3,190,520 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 3
    Outgoing sessions: 0
```

3. Network Trojan “Dark Commet” was detected by DynamiteLab.



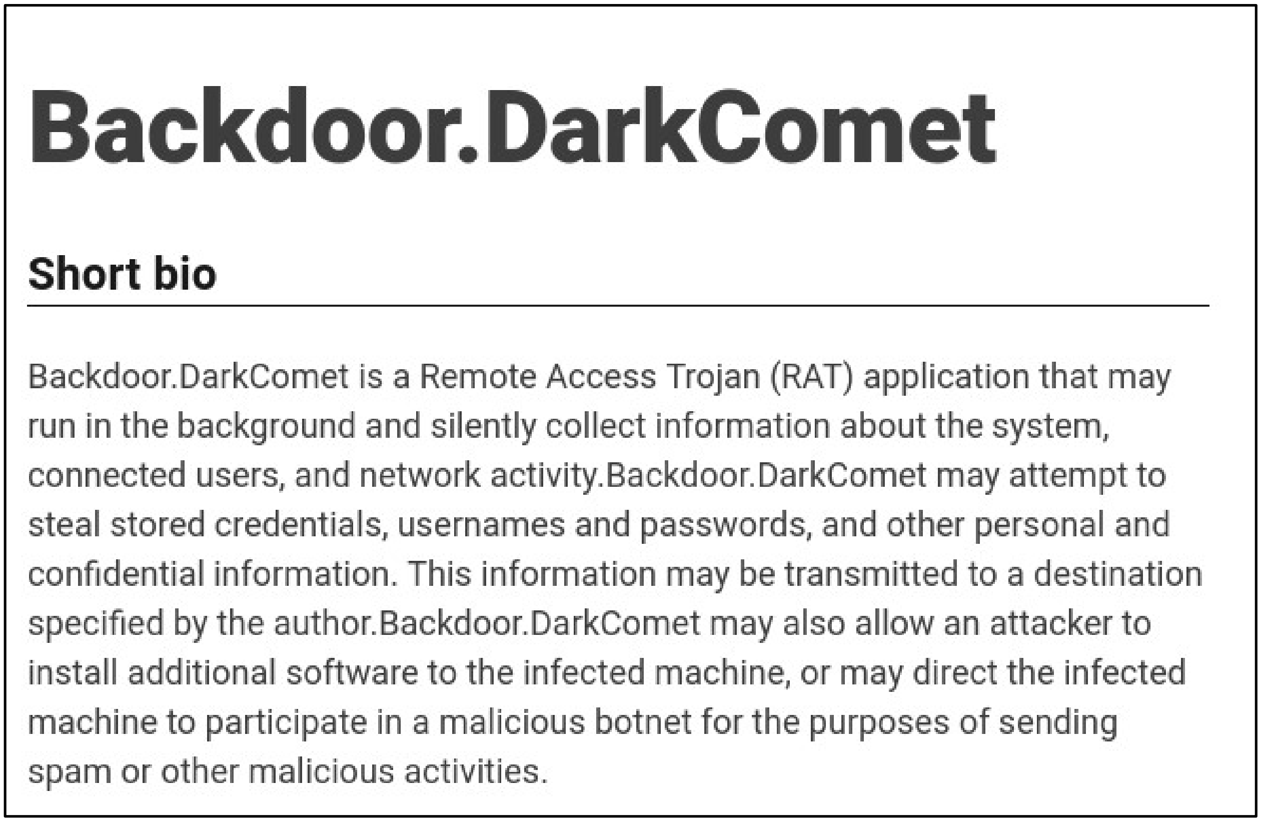
Timestamp	Source IP	Destination IP	Source Port	Destination Port	Transport Protocol	Signature Name	Alert Description	Severity	Signature ID
2/13/2018 12:10:09 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:42 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:33 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:24 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:16 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:04 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:11:02 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:10:51 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996
2/13/2018 12:10:41 AM	10.23.1.205	185.86.151.37	49213	2200	TCP	ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful	A Network Trojan was detected	HIGH	2021996

4. Also detected by Zui.



event_t...	ts	src_ip	s.	dest_ip	d..				alert
alert (1)	2018-02-13T05:12:00.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:51.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:42.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:33.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:24.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:16.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:04.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:11:02.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:10:51.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:10:41.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:10:31.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:10:20.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:10:09.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:59.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:48.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:38.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:28.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:19.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:09.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:09:00.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:08:49.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:08:38.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet
alert (1)	2018-02-13T05:08:28.	10.23.1.205	49213	185.86.151.37	2200	null	TCP	faile	> {severity: 1, signature: ET MALWARE Backdoor.Win32.DarkComet

5. **Remote Access Trojan (RAT) that leaves a backdoor into a system. Description from Malwarebytes:**



Backdoor.DarkComet

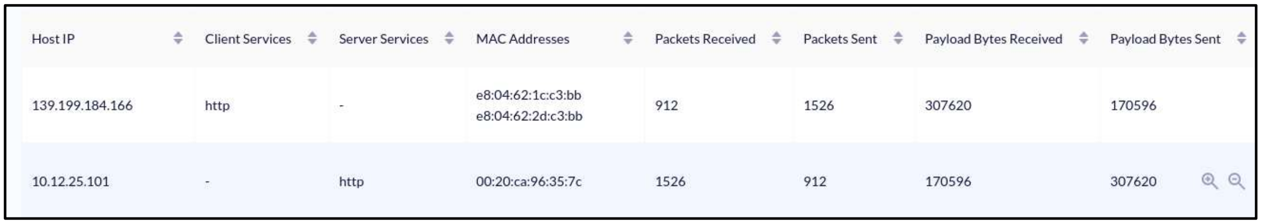
Short bio

Backdoor.DarkComet is a Remote Access Trojan (RAT) application that may run in the background and silently collect information about the system, connected users, and network activity.Backdoor.DarkComet may attempt to steal stored credentials, usernames and passwords, and other personal and confidential information. This information may be transmitted to a destination specified by the author.Backdoor.DarkComet may also allow an attacker to install additional software to the infected machine, or may direct the infected machine to participate in a malicious botnet for the purposes of sending spam or other malicious activities.

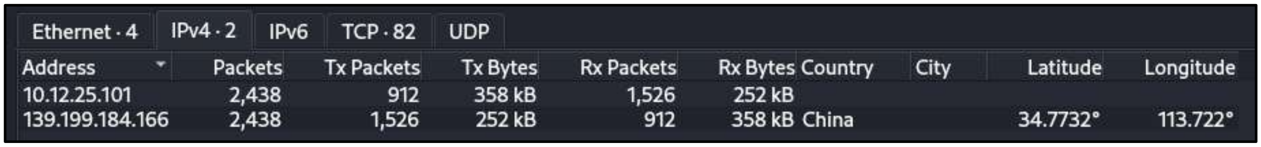
II. Part B

A. Identify the victim IP and what happened to the victim machine

1. Victim: 10.12.25.101



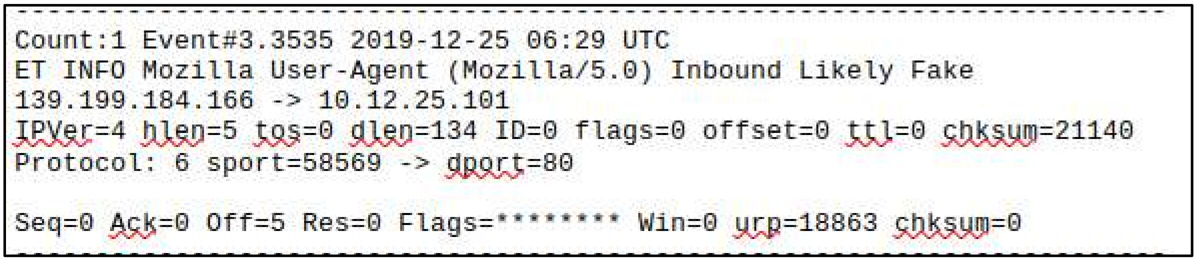
Host IP	Client Services	Server Services	MAC Addresses	Packets Received	Packets Sent	Payload Bytes Received	Payload Bytes Sent
139.199.184.166	http	-	e8:04:62:1c:c3:bb e8:04:62:2d:c3:bb	912	1526	307620	170596
10.12.25.101	-	http	00:20:ca:96:35:7c	1526	912	170596	307620



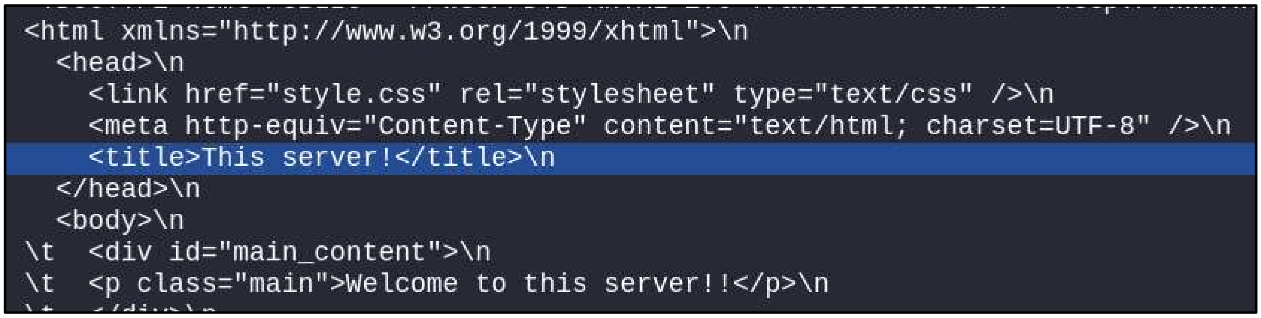
Address	Packets	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude
10.12.25.101	2,438	912	358 kB	1,526	252 kB				
139.199.184.166	2,438	1,526	252 kB	912	358 kB	China		34.7732°	113.722°

2. What happened

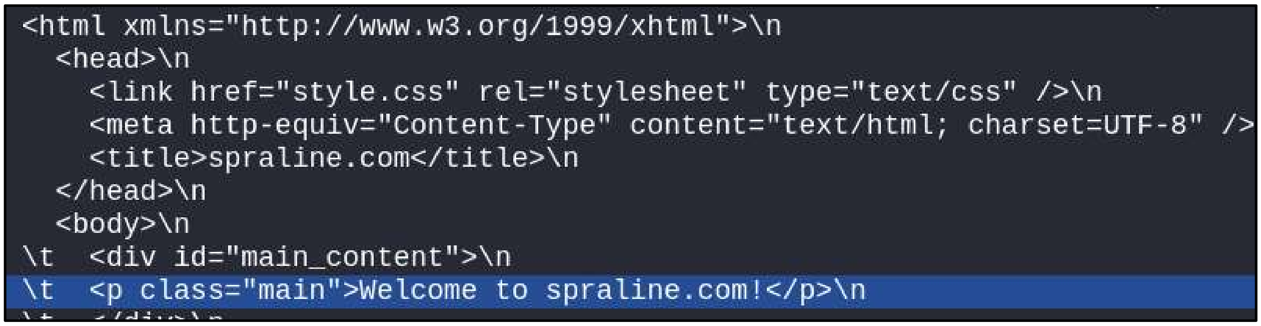
a) 10.12.25.101 connected to suspicious server.



```
Count:1 Event#3.3535 2019-12-25 06:29 UTC
ET INFO Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
139.199.184.166 -> 10.12.25.101
IPVer=4 hlen=5 tos=0 dlen=134 ID=0 flags=0 offset=0 ttl=0 chksum=21140
Protocol: 6 sport=58569 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=18863 chksum=0
```

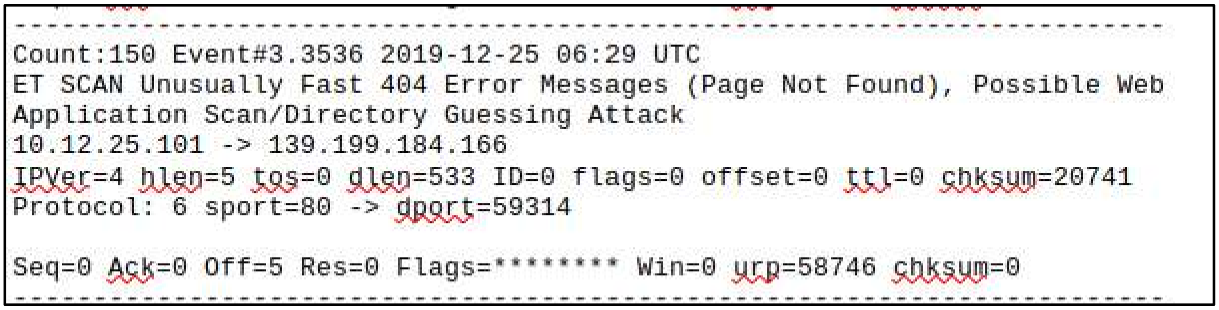


```
<html xmlns="http://www.w3.org/1999/xhtml">\n
  <head>\n
    <link href="style.css" rel="stylesheet" type="text/css" />\n
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />\n
    <title>This server!</title>\n
  </head>\n
  <body>\n
\t  <div id="main_content">\n
\t  <p class="main">Welcome to this server!!</p>\n
```



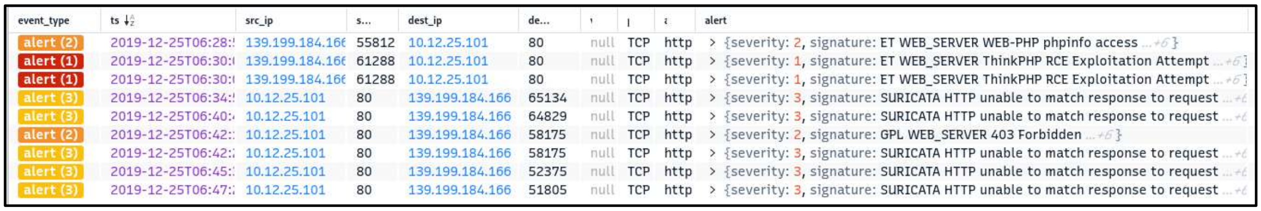
```
<html xmlns="http://www.w3.org/1999/xhtml">\n
  <head>\n
    <link href="style.css" rel="stylesheet" type="text/css" />\n
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>spraline.com</title>\n
  </head>\n
  <body>\n
\t  <div id="main_content">\n
\t  <p class="main">Welcome to spraline.com!</p>\n
```

b) **Suspicious amount and speed of 404 not founds coming that were flagged as a likely attack (brute force/guessing or a scan.**



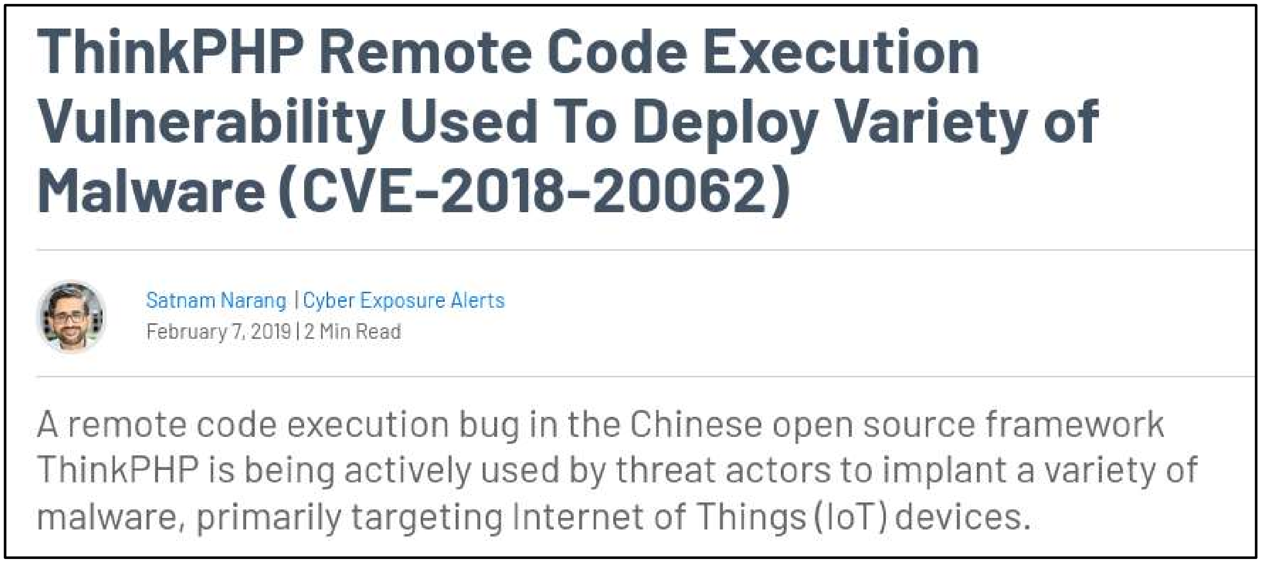
```
---------------------------------------------------------------------------
Count:150 Event#3.3536 2019-12-25 06:29 UTC
ET SCAN Unusually Fast 404 Error Messages (Page Not Found), Possible Web
Application Scan/Directory Guessing Attack
10.12.25.101 -> 139.199.184.166
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20741
Protocol: 6 sport=80 -> dport=59314

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=58746 chksum=0
---------------------------------------------------------------------------
```

c) **ThinkPHP RCE detected.**



event_type	ts	src_ip	s...	dest_ip	de...	'	|	¿	alert
alert (2)	2019-12-25T06:28:	139.199.184.16	55812	10.12.25.101	80	null	TCP	http	> {severity: 2, signature: ET WEB_SERVER WEB-PHP phpinfo access ... +6 }
alert (1)	2019-12-25T06:30:	139.199.184.16	61288	10.12.25.101	80	null	TCP	http	> {severity: 1, signature: ET WEB_SERVER ThinkPHP RCE Exploitation Attempt ... +6]
alert (1)	2019-12-25T06:30:	139.199.184.16	61288	10.12.25.101	80	null	TCP	http	> {severity: 1, signature: ET WEB_SERVER ThinkPHP RCE Exploitation Attempt ... +6]
alert (3)	2019-12-25T06:34:	10.12.25.101	80	139.199.184.166	65134	null	TCP	http	> {severity: 3, signature: SURICATA HTTP unable to match response to request ... +6
alert (3)	2019-12-25T06:40:	10.12.25.101	80	139.199.184.166	64829	null	TCP	http	> {severity: 3, signature: SURICATA HTTP unable to match response to request ... +6
alert (2)	2019-12-25T06:42:	10.12.25.101	80	139.199.184.166	58175	null	TCP	http	> {severity: 2, signature: GPL WEB_SERVER 403 Forbidden ... +6 }
alert (3)	2019-12-25T06:42:	10.12.25.101	80	139.199.184.166	58175	null	TCP	http	> {severity: 3, signature: SURICATA HTTP unable to match response to request ... +6
alert (3)	2019-12-25T06:45:	10.12.25.101	80	139.199.184.166	52375	null	TCP	http	> {severity: 3, signature: SURICATA HTTP unable to match response to request ... +6
alert (3)	2019-12-25T06:47:	10.12.25.101	80	139.199.184.166	51805	null	TCP	http	> {severity: 3, signature: SURICATA HTTP unable to match response to request ... +6

d) Allows other malware to be deployed. (from tenable)

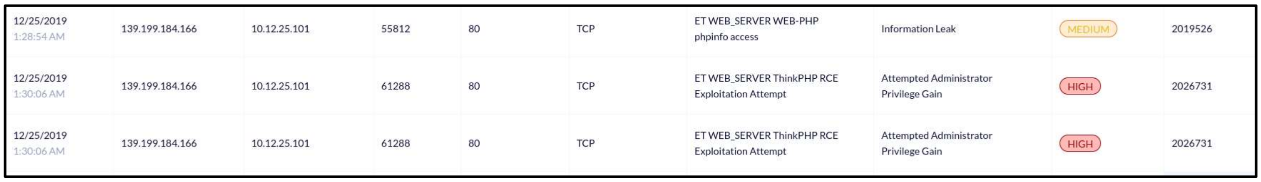


ThinkPHP Remote Code Execution Vulnerability Used To Deploy Variety of Malware (CVE-2018-20062)

Satnam Narang | Cyber Exposure Alerts
February 7, 2019 | 2 Min Read

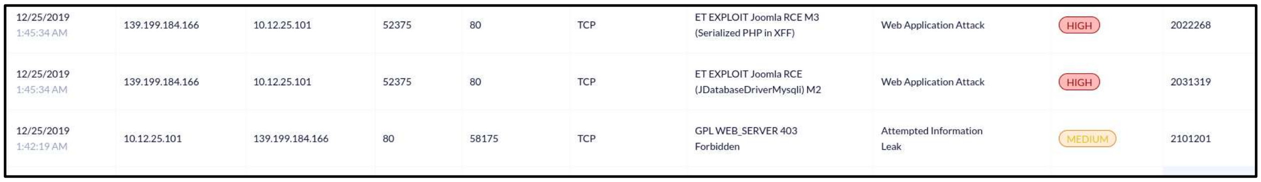
A remote code execution bug in the Chinese open source framework ThinkPHP is being actively used by threat actors to implant a variety of malware, primarily targeting Internet of Things (IoT) devices.

e) Privilege gain was attempted by ThinkPHP.



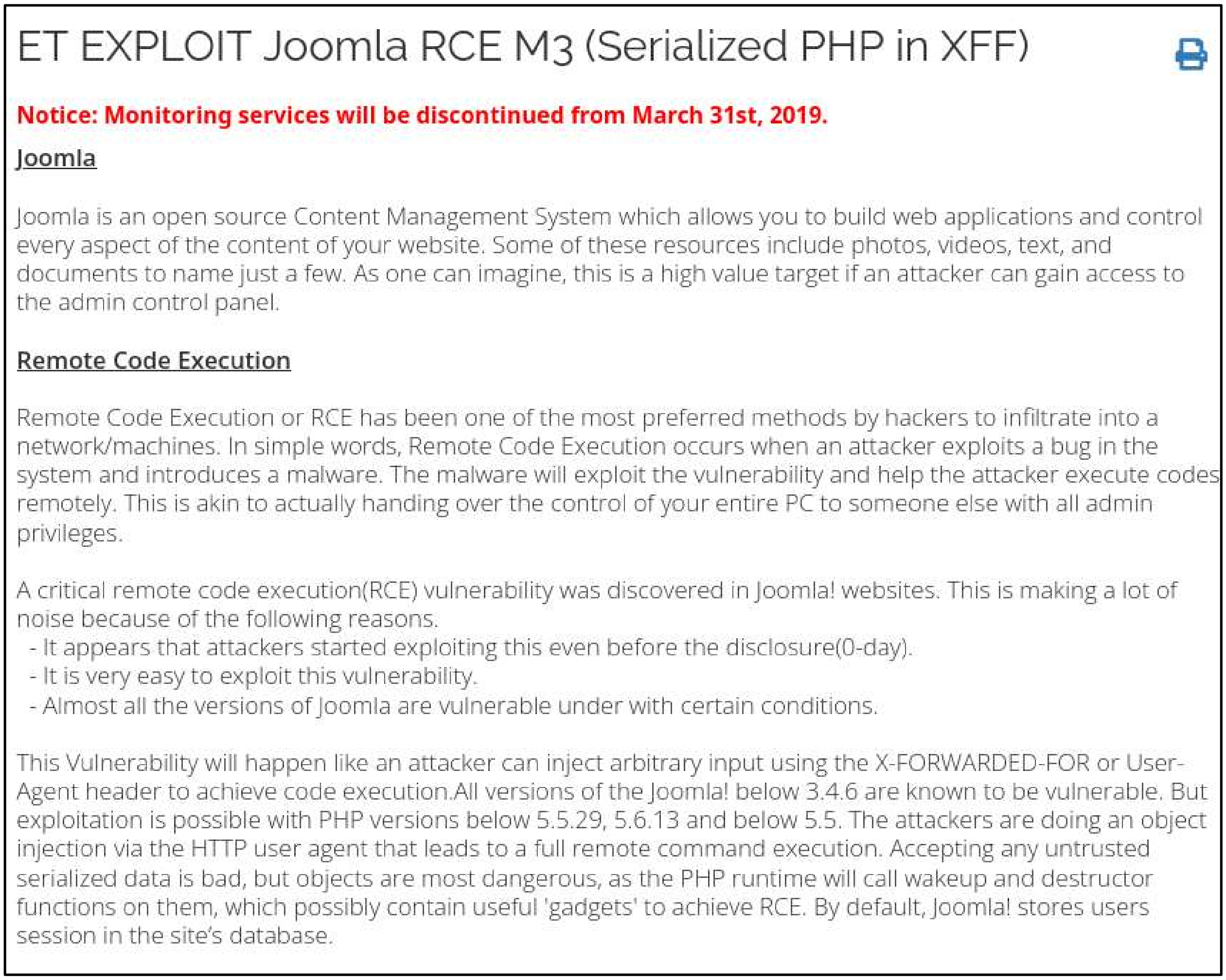
12/25/2019 1:28:54 AM	139.199.184.166	10.12.25.101	55812	80	TCP	ET WEB_SERVER WEB-PHP phpinfo access	Information Leak	MEDIUM	2019526
12/25/2019 1:30:06 AM	139.199.184.166	10.12.25.101	61288	80	TCP	ET WEB_SERVER ThinkPHP RCE Exploitation Attempt	Attempted Administrator Privilege Gain	HIGH	2026731
12/25/2019 1:30:06 AM	139.199.184.166	10.12.25.101	61288	80	TCP	ET WEB_SERVER ThinkPHP RCE Exploitation Attempt	Attempted Administrator Privilege Gain	HIGH	2026731

f) Joomla RCE was also detected



12/25/2019 1:45:34 AM	139.199.184.166	10.12.25.101	52375	80	TCP	ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)	Web Application Attack	HIGH	2022268
12/25/2019 1:45:34 AM	139.199.184.166	10.12.25.101	52375	80	TCP	ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli) M2	Web Application Attack	HIGH	2031319
12/25/2019 1:42:19 AM	10.12.25.101	139.199.184.166	80	58175	TCP	GPL WEB_SERVER 403 Forbidden	Attempted Information Leak	MEDIUM	2101201

g) Vulnerability within Joomla Content Management System that also allows additional malware to be installed. Was 0-day attack. All versions of Joomla vulnerable.



ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)

Notice: Monitoring services will be discontinued from March 31st, 2019.

Joomla

Joomla is an open source Content Management System which allows you to build web applications and control every aspect of the content of your website. Some of these resources include photos, videos, text, and documents to name just a few. As one can imagine, this is a high value target if an attacker can gain access to the admin control panel.

Remote Code Execution

Remote Code Execution or RCE has been one of the most preferred methods by hackers to infiltrate into a network/machines. In simple words, Remote Code Execution occurs when an attacker exploits a bug in the system and introduces a malware. The malware will exploit the vulnerability and help the attacker execute codes remotely. This is akin to actually handing over the control of your entire PC to someone else with all admin privileges.

A critical remote code execution(RCE) vulnerability was discovered in Joomla! websites. This is making a lot of noise because of the following reasons.

- It appears that attackers started exploiting this even before the disclosure(0-day).
- It is very easy to exploit this vulnerability.
- Almost all the versions of Joomla are vulnerable under with certain conditions.

This Vulnerability will happen like an attacker can inject arbitrary input using the X-FORWARDED-FOR or User-Agent header to achieve code execution.All versions of the Joomla! below 3.4.6 are known to be vulnerable. But exploitation is possible with PHP versions below 5.5.29, 5.6.13 and below 5.5. The attackers are doing an object injection via the HTTP user agent that leads to a full remote command execution. Accepting any untrusted serialized data is bad, but objects are most dangerous, as the PHP runtime will call wakeup and destructor functions on them, which possibly contain useful 'gadgets' to achieve RCE. By default, Joomla! stores users session in the site's database.