Executive Summary

This analysis examines a network capture from a virtual machine (VM), that was compromised through a multi-stage exploit kit (EK) attack. The infection began when a user accessed a legitimate-looking website, which contained embedded content designed to redirect the browser to a malicious exploit kit landing page.

The EK then attempted to exploit known vulnerabilities in PDF and Flash components within the browser environment. Upon successful exploitation, a malicious executable (EXE) payload were downloaded and executed on the VM, establishing foothold for further malicious activity.

Post-infection network analysis revealed the payload generated SMTP-based mass-mailing traffic and outbound connections to a command-and-control (C2) server, indicating both propagation and remote-control capabilities.

Note: All URLs in this report have been defanged (e.g., “http” → “hxxp”, “.” → “[.]”) to prevent accidental clicks or automatic execution.

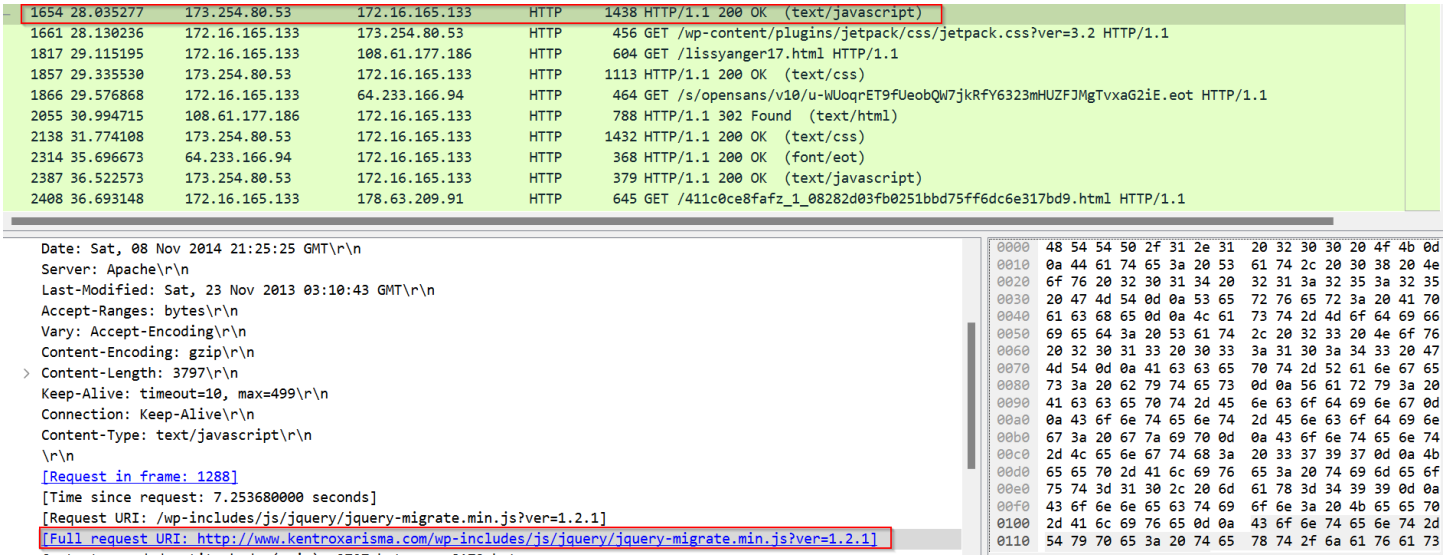
Infected Host Information:
IP Address: 172.16.165.133
Hostname: WIN-C2KE6N4W3N1
Mac Address: 00:0C:29:77:AC:27

Threat Information:
IP Addresses: [173.254.80.53], [173.63.209.91], [108.61.177.186], [111.121.193.238]
SHA-256 hash of 7.exe:
FF29B5ADC5F95F5E33FD4E0B9C21D211388EB5E47F46E768C0E1A8D224E68D7E
Domains: [genfaglobal[.]ga], [seedradrivergy[.]co[.]vu], [kentroxarisma[.]com]

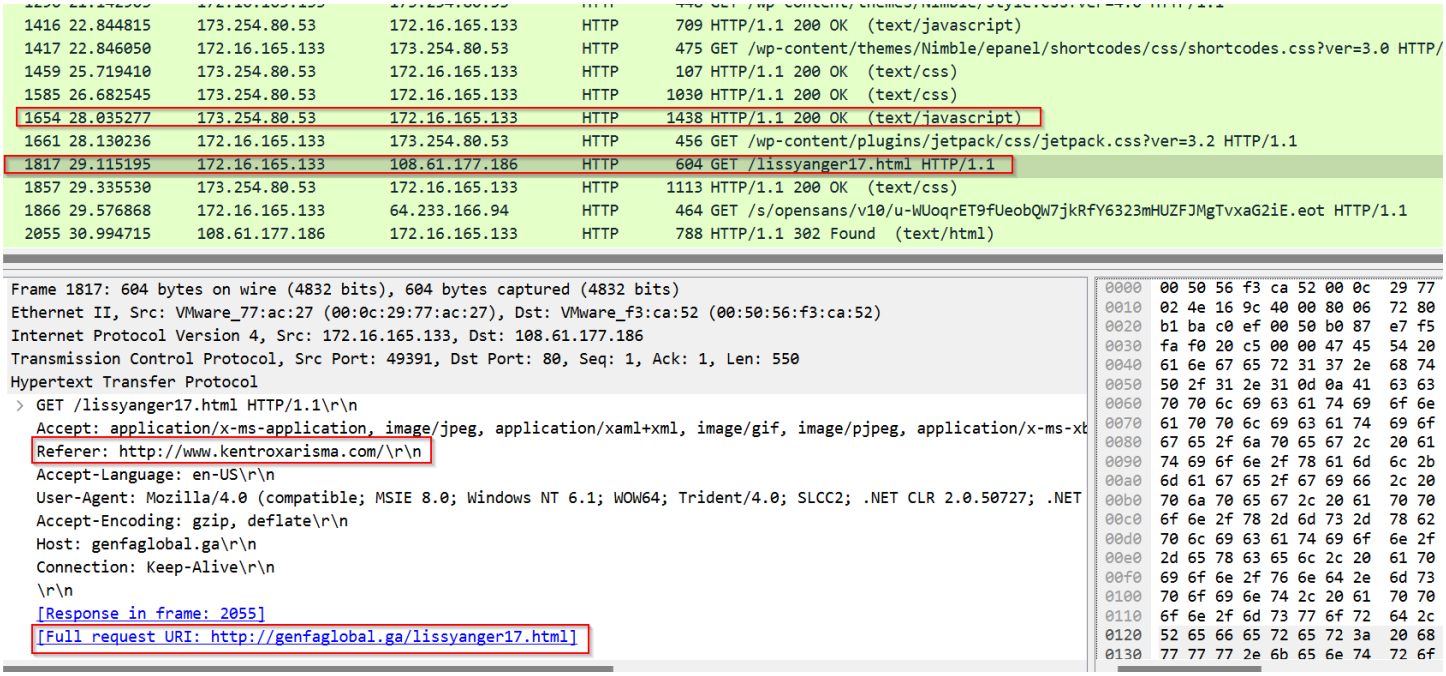
Infection Overview

The infection originated when a user visited the legitimate-looking website hxxp://www[.]kentroxarisma[.]com/ with the IP address: 173.254.80.53. During page load, the browser automatically requested an embedded JavaScript resource:

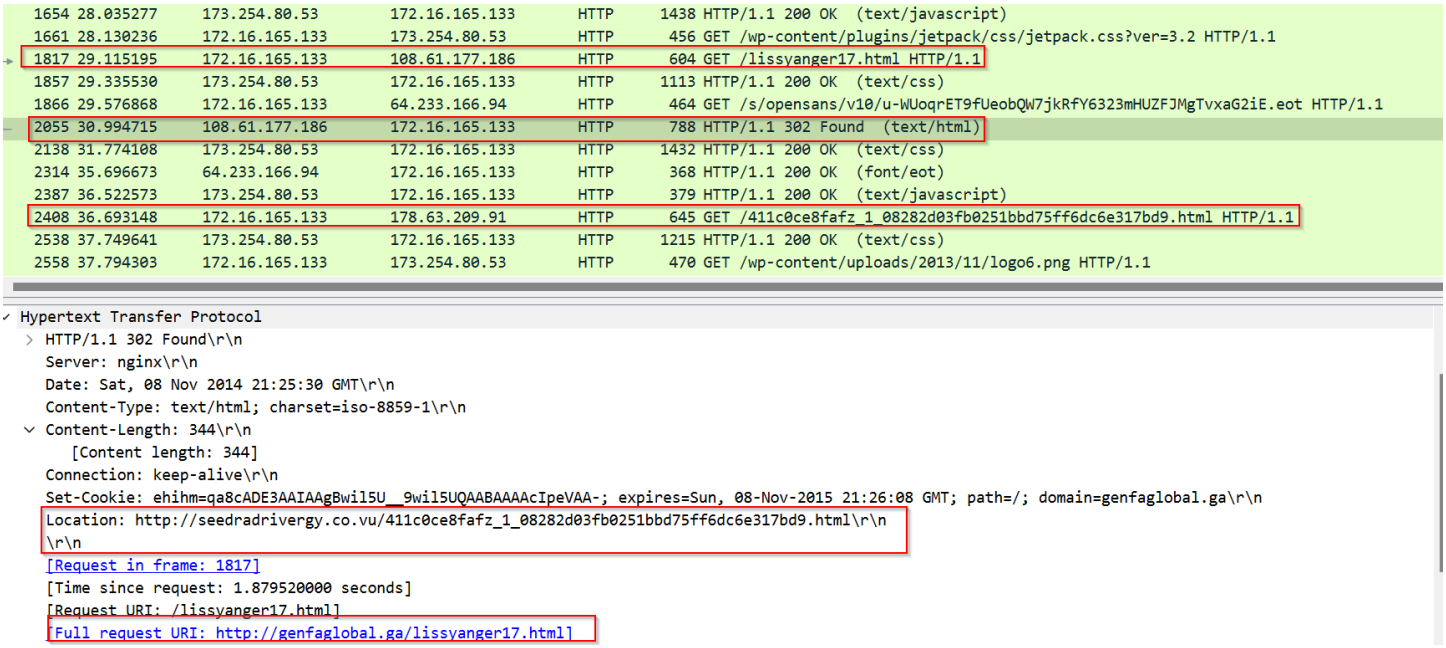
hxxp://www[.]kentroxarisma[.]com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1



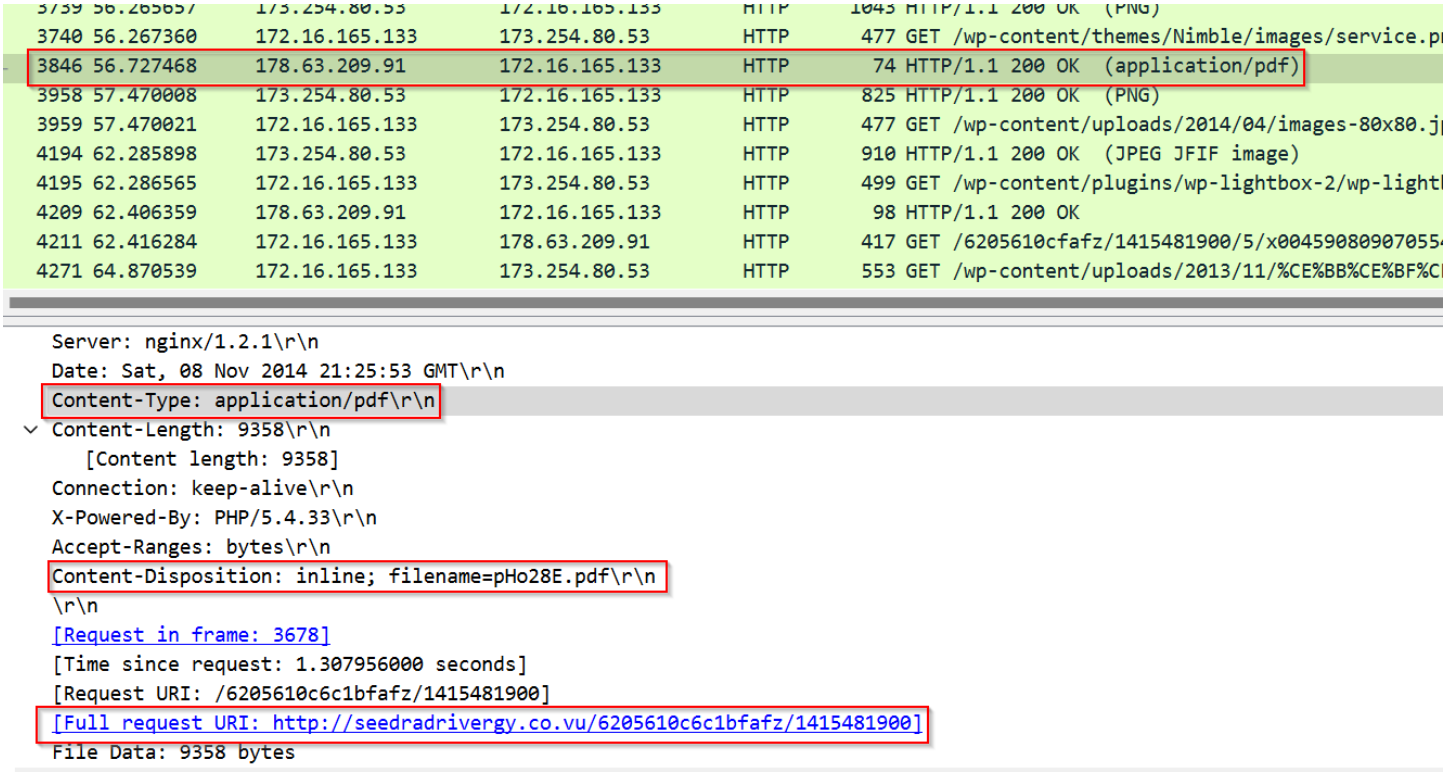
This script acted as the trigger for the exploit kit, causing the browser to request the redirector page: hxxp://genfaglobal[.]ga/lissyanger17.html with the IP address 108.61.177.186 . The request to genfaglobal.ga included a Referer header pointing back to kentroxarisma.com, confirming the browser followed the embedded resource.



In response, the genfaglobal.ga server issued a 302 redirect to the exploit kit landing page hosted at: hxxp://seedradrivergy[.]co[.]vu/6205610cfafz/1415481900/7 with the IP address 173.63.209.91.



This multi-stage redirection led to the delivery of PDF and Flash exploits targeting vulnerabilities in the victim's browser environment.



```
3603 54.978487    172.16.165.133    176.74.176.188    HTTP     409 GET /?f HTTP/1.1
3641 55.176320    178.63.209.91     172.16.165.133    HTTP    1273 HTTP/1.1 200 OK
3654 55.255875    172.16.165.133    178.63.209.91     HTTP     415 GET /6205610cfafz/1415481900/5/x0045908090705
3678 55.419512    172.16.165.133    178.63.209.91     HTTP     671 GET /6205610c6c1bfafz/1415481900 HTTP/1.1
3718 55.809971    176.74.176.188    172.16.165.133    HTTP     207 HTTP/1.1 200 OK  (text/html)
3739 56.265657    173.254.80.53     172.16.165.133    HTTP    1043 HTTP/1.1 200 OK  (PNG)
3740 56.267360    172.16.165.133    173.254.80.53     HTTP     477 GET /wp-content/themes/Nimble/images/service.
3846 56.727468    178.63.209.91     172.16.165.133    HTTP      74 HTTP/1.1 200 OK  (application/pdf)
3958 57.470008    173.254.80.53     172.16.165.133    HTTP     825 HTTP/1.1 200 OK  (PNG)
3959 57.470021    172.16.165.133    173.254.80.53     HTTP     477 GET /wp-content/uploads/2014/04/images-80x80.
4194 62.285898    173.254.80.53     172.16.165.133    HTTP     910 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
Server: nginx/1.2.1\r\n
Date: Sat, 08 Nov 2014 21:25:52 GMT\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 33593\r\n
   [Content length: 33593]
Connection: keep-alive\r\n
X-Powered-By: PHP/5.4.33\r\n
Accept-Ranges: bytes\r\n
Content-Disposition: inline; filename=6205610c.swf\r\n
\r\n
[Request in frame: 3497]
[Time since request: 1.283276000 seconds]
[Request URI: /6205610ca76bfafz/1415481900]
[Full request URI: http://seedradrivergy.co.vu/6205610ca76bfafz/1415481900]
File Data: 33593 bytes
```

Successful exploitation triggered the download and execution of the malicious executable (EXE) payload on the virtual machine, establishing a foothold for post-infection activity.

```
3718 55.809971    176.74.176.188    172.16.165.133    HTTP     207 HTTP/1.1 200 OK  (text/html)
3739 56.265657    173.254.80.53     172.16.165.133    HTTP    1043 HTTP/1.1 200 OK  (PNG)
3740 56.267360    172.16.165.133    173.254.80.53     HTTP     477 GET /wp-content/themes/Nimble/images/service.png H
3846 56.727468    178.63.209.91     172.16.165.133    HTTP      74 HTTP/1.1 200 OK  (application/pdf)
3958 57.470008    173.254.80.53     172.16.165.133    HTTP     825 HTTP/1.1 200 OK  (PNG)
3959 57.470021    172.16.165.133    173.254.80.53     HTTP     477 GET /wp-content/uploads/2014/04/images-80x80.jpg H
4194 62.285898    173.254.80.53     172.16.165.133    HTTP     910 HTTP/1.1 200 OK  (JPEG JFIF image)
4195 62.286565    172.16.165.133    173.254.80.53     HTTP     499 GET /wp-content/plugins/wp-lightbox-2/wp-lightbox-
4209 62.406359    178.63.209.91     172.16.165.133    HTTP      98 HTTP/1.1 200 OK
```

```
HTTP/1.1 200 OK\r\n
Server: nginx/1.2.1\r\n
Date: Sat, 08 Nov 2014 21:25:53 GMT\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 196608\r\n
   [Content length: 196608]
Connection: keep-alive\r\n
X-Powered-By: PHP/5.4.33\r\n
Accept-Ranges: bytes\r\n
Content-Disposition: inline; filename=5.exe\r\n
\r\n
[Request in frame: 3654]
[Time since request: 7.150484000 seconds]
[Request URI: /6205610cfafz/1415481900/5/x004590809070554515d565b010b03510053535c0505;1;6]
[Full request URI: http://seedradrivergy.co.vu/6205610cfafz/1415481900/5/x004590809070554515d565b010b03510053535c0505;1;6]
```

```
4996 74.584267   172.16.165.133   173.254.80.53    HTTP   494 GET /wp-content/themes/Nimble/js/jquery.flexslide
5007 74.608376   172.16.165.133   178.63.209.91    HTTP   366 GET /6205610cfafz/1415481900/7 HTTP/1.1
5765 84.589253   178.63.209.91    172.16.165.133   HTTP  1496 HTTP/1.1 200 OK
5769 84.709501   173.254.80.53    172.16.165.133   HTTP  1052 HTTP/1.1 200 OK  (text/javascript)
5771 84.712343   172.16.165.133   173.254.80.53    HTTP   480 GET /wp-content/themes/Nimble/images/left-qoute.p
```

```
Server: nginx/1.2.1\r\n
Date: Sat, 08 Nov 2014 21:26:15 GMT\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 196608\r\n
   [Content length: 196608]
Connection: keep-alive\r\n
X-Powered-By: PHP/5.4.33\r\n
Accept-Ranges: bytes\r\n
Content-Disposition: inline; filename=7.exe\r\n
\r\n
[Request in frame: 5007]
[Time since request: 9.980877000 seconds]
[Request URI: /6205610cfafz/1415481900/7]
[Full request URI: http://seedradrivergy.co.vu/6205610cfafz/1415481900/7]
```

The malicious executable seems to be acting as a backdoor in order to use the VM as a mass mailer. Post execution of the malicious payload there is a large amount of traffic on port 25 and there are a lot of DNS queries for mail servers.

```
 9224 164.222472   172.16.165.133   94.100.180.150   TCP   66 49418 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
 9239 167.235844   172.16.165.133   94.100.180.150   TCP   66 [TCP Retransmission] 49418 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
 9560 173.242832   172.16.165.133   94.100.180.150   TCP   62 [TCP Retransmission] 49418 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
 9563 175.080727   207.46.163.247   172.16.165.133   TCP   60 25 → 49414 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
10022 199.112105   98.138.112.37    172.16.165.133   TCP   60 25 → 49415 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
10152 213.903414   172.16.165.133   65.55.33.119     TCP   66 49420 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10153 213.903428   172.16.165.133   64.233.166.27    TCP   66 49421 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10154 213.903522   172.16.165.133   152.163.0.67     TCP   66 49422 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10155 213.903737   172.16.165.133   64.233.168.27    TCP   66 49423 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10156 213.903846   172.16.165.133   98.136.217.203   TCP   66 49424 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10157 213.904010   172.16.165.133   74.125.205.27    TCP   66 49425 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10158 213.904243   172.16.165.133   65.54.188.72     TCP   66 49426 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10159 213.904388   172.16.165.133   152.163.0.99     TCP   66 49427 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10160 213.904526   172.16.165.133   74.125.205.27    TCP   66 49428 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
10088 211.465953   172.16.165.133   172.16.165.2   DNS   86 Standard query 0x9333 A gmail-smtp-in.l.google.com
10089 211.474806   172.16.165.133   172.16.165.2   DNS   81 Standard query 0x22d8 A mta5.am0.yahoodns.net
10090 211.475381   172.16.165.133   172.16.165.2   DNS   91 Standard query 0x9df7 A alt1.gmail-smtp-in.l.google.com
10091 211.498771   172.16.165.133   172.16.165.2   DNS   75 Standard query 0xb5e5 A mx4.hotmail.com
10092 211.499995   172.16.165.133   172.16.165.2   DNS   80 Standard query 0x48ae A mailin-03.mx.aol.com
10093 211.500491   172.16.165.133   172.16.165.2   DNS   91 Standard query 0xccfc A alt3.gmail-smtp-in.l.google.com
10094 211.500767   172.16.165.133   172.16.165.2   DNS   91 Standard query 0xfd5b A alt1.gmail-smtp-in.l.google.com
10095 211.501090   172.16.165.133   172.16.165.2   DNS   81 Standard query 0x6b94 A mta6.am0.yahoodns.net
10096 211.501383   172.16.165.133   172.16.165.2   DNS   75 Standard query 0xcdb6 A mx3.hotmail.com
10097 211.501718   172.16.165.133   172.16.165.2   DNS   81 Standard query 0x8e81 A mta5.am0.yahoodns.net
10098 211.502192   172.16.165.133   172.16.165.2   DNS   75 Standard query 0x487c A mx2.hotmail.com
10101 212.415042   172.16.165.133   172.16.165.2   DNS   86 Standard query 0x8216 A gmail-smtp-in.l.google.com
10102 212.446405   172.16.165.133   172.16.165.2   DNS   75 Standard query 0xc91c A mx4.hotmail.com
10103 212.464465   172.16.165.133   172.16.165.2   DNS   91 Standard query 0xec70 A alt3.gmail-smtp-in.l.google.com
10104 212.464512   172.16.165.133   172.16.165.2   DNS   80 Standard query 0xa18c A mailin-04.mx.aol.com
```

There is also evidence of remote access via a command and control server (C2) to the system as there are multiple call backs to the IP address 111.121.193.238 on port 443.

```
6475 93.742912   111.121.193.238   172.16.165.133   SSL   254 Continuation Data
6477 93.757716   172.16.165.133    111.121.193.238  SSL   195 Continuation Data
6757 98.774605   111.121.193.238   172.16.165.133   SSL   759 Continuation Data
5927 88.628332   172.16.165.133    111.121.193.238  TCP    66 49410 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
6134 91.017452   111.121.193.238   172.16.165.133   TCP    60 443 → 49410 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6135 91.017481   172.16.165.133    111.121.193.238  TCP    60 49410 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6478 93.757784   111.121.193.238   172.16.165.133   TCP    60 443 → 49410 [ACK] Seq=201 Ack=142 Win=64240 Len=0
6758 98.775973   172.16.165.133    111.121.193.238  TCP    60 49410 → 443 [ACK] Seq=142 Ack=907 Win=63335 Len=0
6761 98.782973   172.16.165.133    111.121.193.238  TCP    60 49410 → 443 [FIN, ACK] Seq=142 Ack=907 Win=63335 Len=0
6762 98.782980   111.121.193.238   172.16.165.133   TCP    60 443 → 49410 [ACK] Seq=907 Ack=143 Win=64239 Len=0
```

Conclusion

This investigation identified malicious activity originating from an attacker, resulting in the compromise of the victim VM. Analysis revealed the use of malicious JavaScript from a compromised website, which redirected the victim to an attacker-controlled server. From there, the attacker established a foothold and initiated communication with external systems, potentially exfiltrating data and enabling further malicious actions. The findings underscore the importance of continuous network monitoring, timely patching of software vulnerabilities, and user awareness training to prevent similar incidents.