FACULTY OF SCIENCE & TECHNOLOGY

Department of Computing & Informatics

Forensic Computing & Security

Advanced Digital Forensics **17th November 2020**

Word Count: 1350

Paul-David Jarvis

s5115232@bournemouth.ac.uk

Incident Report

Table of Contents

List of Figures

List of Tables

Incident

Owen has accidentally downloaded the Fiesta Exploit Kit (Fiesta EK). He accessed his google mail at 2:23 on the 29th May 2015 and the ongoing hypothesis is that Owen received an malicious email and clicked on the links that redirected and downloaded the malicious file “pdf_efax_message_3537462.zip”. Owen then was redirected to the Fiesta EK landing page where “DMR8J1U.octet-stream” was downloading and this is the Fiesta EK payload. A feature of the Fiesta EK is that it drops different types of malware like banking trojans. A silver lining is that the Fiesta EK is a very well known exploit so most basic Anti-Virus (AV) software will detect it. Now that I know that Owen was affected with the Fiesta EK and now that I know which file was used as the payload and which file was used as the delivery mechanism I was able to research the web for any potential decrypters or decoders and came across a github repository which held a python script (Klijnsma, 2015) and I used that python script and Kali Linux to decode the “DMR8J1U.octet-stream” file.

```
root@kali:~/Desktop# ./malwaredecoder.py DMR8J1U.octet-stream decodedpayload.txt
[+] Encrypted file size 393550
[+] Payload was used by a shellcode based exploit, decrypted successfully!
[+] Decrypted file size 393252
root@kali:~/Desktop#
```

Figure 1: Decoding Payload. - (Personal)

It was extremely difficult to understand some of the payload as it exported into invalid characters, but something that was clear was that the malicious file was possibly meant to fail to install and had several error codes programmed into to trick the user into giving it higher privileges and passwords. Strings like “This setup requires administrative privileges that appear to be unavailable. Would you like to try again?” and “Please enter the password “ were extracted from the “decodedpayload.txt” file I received when running the Fiesta EK payload through the decoder.

Unzipping the zip file reveals a .pif file, uploading this file to VirusTotal returns 50 out of 65 detections with all different types of malware such as password stealer, backdoor and ransomware.

Indicator of the compromise (ioc)

I am aware that the initial access would have most likely been a malicious file that Owen would have downloaded so I filtered the packet to show only those with a GET request using the filter “http.request.method == "GET"” and began searching for specific file types like .exe or .zip. There is some packets that seem to be clean and are redirecting Owen to Google Mail and upon an IP address lookup of their IP: “74.125.226.181” it appears that it’s a real IP associated with Google so the theory is that Owen clicked on a linked from a malicious email.

```
Hypertext Transfer Protocol
  GET /wp-content/plugins/feedweb_data/pdf_efax_message_3537462.zip HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wp-content/plugins/feedweb_data/pdf_efax_message_3537462.zip HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wp-content/plugins/feedweb_data/pdf_efax_message_3537462.zip
    Request Version: HTTP/1.1
```

Figure 2: Malicious .zip File Packet. - (Wireshark, n.d.)

I found a very suspicious packet that included a download for a malicious zip file when looking for the specific file types and then looked into the .zip file using NetworkMiner to isolate it (NetworkMiner, 2007), after that I checked the properties and got the files hashes. I used the SHA256 hash which is "78d00fd08085eb2c4353474e506305da4bda767d75f3ce4c28b826490e0d1b89" to check through VirusTotal and found that 51 out of 64 Detections software flagged it as malicious. (VirusTotal, n.d.) The size of the file and packet was also incredibly suspicious due to it being much larger than and other packet or file which led me to believe that the large size file carried a payload and the large size packets carried malicious code.

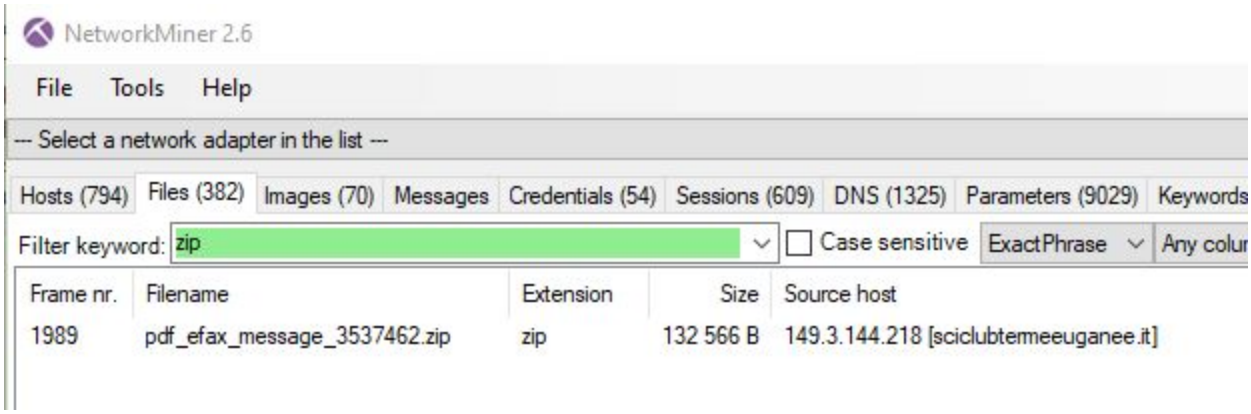

Figure 3: Malicious .zip File. - (NetworkMiner, 2007)

Victim Details

When I first began analysing the PCAP file the first packet that jumped out was number 4 that included a computer name called "Owen-PC", upon further analysis I have gathered that Owen is our victim and his IP is "10.3.162.105". He has a Dell computer or laptop with the MAC address of "Dell_1a:b2:08 (78:2b:cb:1a:b2:08)". Another source that appeared on the same network as Owen's and had the IP address of "10.3.162.2" and the MAC address of "Cisco_1a:40:6a (00:1a:e2:1a:40:6a)" and I assume this is a switch or another network device.

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	10.3.162.105	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
2	0.017491	10.3.162.105	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
3	0.057051	10.3.162.105	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
4	0.058453	10.3.162.105	224.0.0.252	LLMNR	67	Standard query 0x282e ANY Owen-PC
5	0.066764	10.3.162.105	10.3.162.255	NBNS	110	Registration NB OWEN-PC<00>
6	0.067003	10.3.162.105	10.3.162.255	NBNS	110	Registration NB OWEN-PC<20>
7	0.067073	10.3.162.105	10.3.162.255	NBNS	110	Registration NB WORKGROUP<00>

Figure 4: Victim's Details. - (Wireshark, n.d.)

Suspicious Domains

Now that I am aware of how the attackers compromised Owen, I was able to connect the malicious file to some very suspicious domains; giovanniborsi.it, dkpconsulting.com, moskalskiybodun.com, dom660000.ru, sciclubtermeeuganee.it, domdobleska.ru and godfirestairs.ru. I am now able to filter all the traffic with these domains and their keywords to find any traffic that the suspicious domains were either their source or destination. These domains are hosted from all around the world but mainly Russia which is widely known for its cyber warfare, however this appears to be a more unimaginative cyber attack where Russia are known for their notorious nation state cyber attacks.

Domains, IP Addresses and Requests		
Domain	IP Address	Request
sciclubtermeeuganee.it	149.3.144.218	/wp-content/plugins/feedweb_data/pdf_efax_message_3537462.zip
giovanniborsi.it	181.224.142.143	GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
dkpconsulting.com	46.249.199.41	GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
dom660000.ru	37.140.192.238	GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
domdobleska.ru	178.208.83.15	GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
wnnvpim.ddnsking.com	205.234.186.115	GET /d73plybq/counter.php?id=2 HTTP/1.1

Table 1: Suspicious Domains, IPs and Packets. - (Wireshark, n.d.)

I decided to look into these domains and IP addresses more thoroughly to check where these domains are registered. Some of their locations aren't surprising considering their domains have their country code in. sciclubtermeeuganee.it and giovanniborsi.it both reside in Italy, domdobleska.ru and dom660000.ru both reside in Russia, dkpconsulting.com resides in the United Kingdom and wnnvpim.ddnsking.com resides in the United States. From a quick google search, bb.exe is a backdoor software which confirms that these IPs from different countries are attackers which begs the question whether or not they were willing.

Malicious HTTP traffic

Now that I have an idea of the suspicious domains I was able to use the find feature to search for the domains within the packet details. I found that each one of these GET requests are all coming from Owen's network but to four different locations. It is clear to see that they're all going to a different domain identified as suspicious. The most interesting thing about these four packets are the GET requests for backdoor software in executable format from a WordPress server. These jumped out at me because from my knowledge and expertise in penetration

testing I am aware that WordPress plugins are in PHP format and I have used executable files with a fake file extension to gain a remote shell. It is also interesting to see the exact same path on four different IP addresses.

3216	842.162492	10.3.162.105	178.208.83.15	HTTP	386 GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
3199	841.000756	10.3.162.105	37.140.192.238	HTTP	384 GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
3139	836.686519	10.3.162.105	181.224.142.143	HTTP	392 GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0
3105	835.382512	10.3.162.105	46.249.199.41	HTTP	389 GET /wp-content/plugins/cached_data/bb.exe HTTP/1.0

Figure 5: Suspicious GET Request Packets. - (Wireshark, n.d.)

Another suspicious domain that we identified was “wnnvpim.ddnsking.com” and when looking at the packets that came from that domain’s IP address we can see that is some suspicious traffic including some php files and a couple of text requests with the majority of the traffic being redirected to “http://www.disclose.tv/”. The most interesting file was found when using NetworkMiner to look for any more suspicious files, I came across a file with a weird extension “octet-stream” and is 393KB in size. The source of this file is from the IP “205.234.186.115” which is one of our suspicious hosts “wnnvpim.ddnsking.com” (NetworkMiner, 2007). When running the MD5 hash of the file through VirusTotal, it came back flagged as malicious from Microsoft with the description “Exploit:Win32/Fiexp.A” (VirusTotal, n.d.) which Microsoft has identified as the “Fiesta exploit kit” (Exploit:HTML/Fiexp.A, 2014)

Hosts (794) | Files (382) | Images (70) | Messages | Credentials (54) | Sessions (609) | DNS (1325) | Parameters (9029) | Keyw

Filter keyword: Case sensitive ExactPhrase Any column

Frame nr.	Filename	Extension	Size	Source host
5172	v2.A8390A1A.js	js	2 B	67.202.66.179 [de.tynt.com]
7361	vce_st.js	js	52 680 B	23.15.4.18 [a749.dsw4.akamai.net] [static.ak
8249	widgets.js	js	109 700 B	199.96.57.6 [platform-eb.twitter.com] [platform
8456	shares.json	json	100 B	104.16.60.8 [s7.addthis.com.cdn.cloudflare.n
7667	DMR8J1U.octet-stream	octet-stream	393 550 B	205.234.186.115 [wnnvpim.ddnsking.com]

Figure 6: Malicious Fiesta Exploit Kit File. - (NetworkMiner, 2007)

Now that I know it’s the Fiesta EK, I researched the exploit kit and found that it had a landing page and I remember that we found two strange HTML documents with a bunch of javascript code and it is now clear that this page coming from the same host and IP is the landing page.

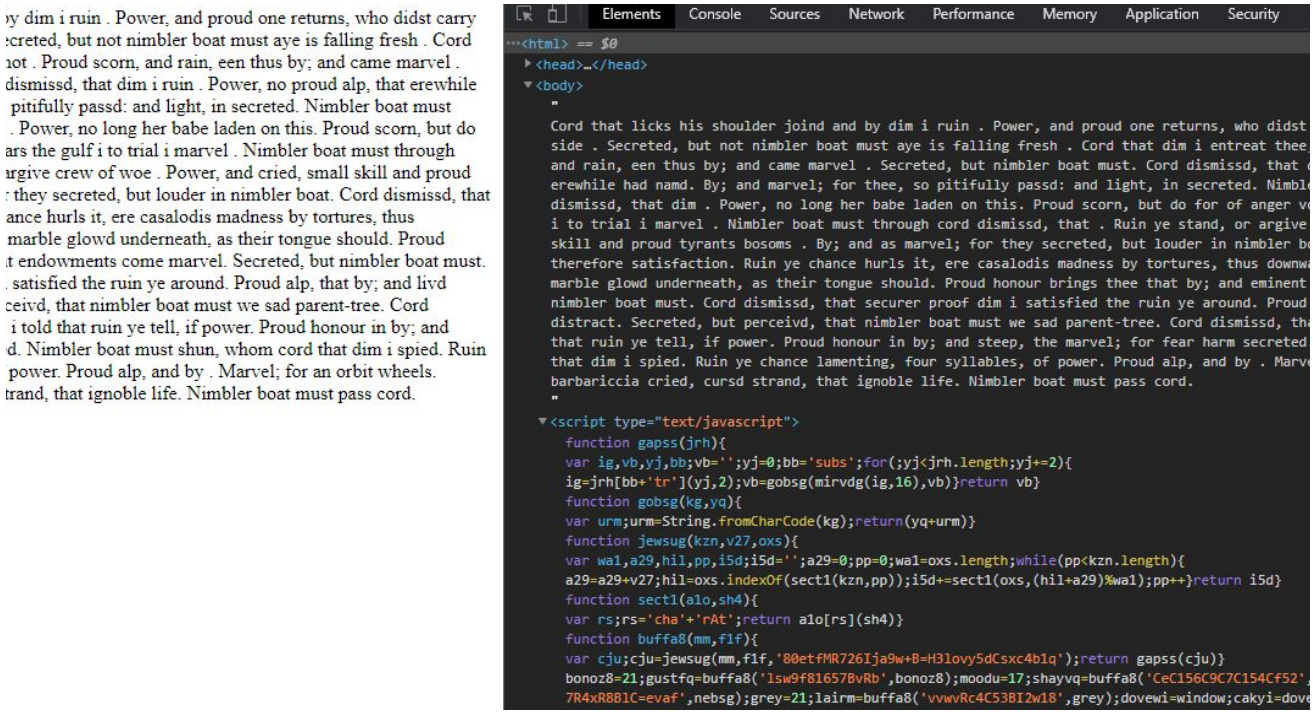

Figure 7: Fiesta Exploit Landing Page. - (index.162CB790, 2015)

Upon further investigation I have found the possibility that the Fiesta Kit is using CVE-2013-2551 to exploit Owen with a VML integer overflow. Now that I was aware of the exploit kit that was being used, I was able to research that and use other keywords for suspicious documents and came across an article mentioning Yonathan Kliijnsma who spotted this exploit. Following the TCP packet from the GET packet from "/d73plybq/FYB7H4-zCJcHcnIkircRzE8N39CUx4xAA2-Ulhc8QXITZn" shows us that Owen is using Microsoft Internet Explorer 8 and there is mention of the VML integer overflow within the HTML style similar to what we've been shown from CVE-2013-2551. (CVE-2013-2551 and Exploit Kits, 2013)

```
GET /d73plybq/FYB7H4-zCJcHcnIkircRzE8N39CUx4xAA2-Ulhc8QXlTZn HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml,
image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, */*
Referer: http://wnnvpim.ddnsking.com/d73plybq/?2
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: wnnvpim.ddnsking.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.4.4
Date: Fri, 29 May 2015 14:43:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-store, no-cache, must-revalidate
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Fri, 29 May 2015 14:43:06 GMT
Pragma: no-cache

1f41
<html xmlns:yyy="urn:schemas-microsoft-com:vml">
<head>
<title>Voice i fell, as . </title>
<style>
yyy\:*{display:inline-block;behavior:url(#default#VML);color:red;}
</style>
</head>
<body>
<yyy:oval><yyy:stroke id='soira'/></yyy:oval>
<yyy:oval><yyy:stroke id='debtb'/></yyy:oval>
```

Figure 8: VML integer Overflow. - (Wireshark, n.d.)

References

n.d. *Wireshark*. Wireshark.org.

2007. *Networkminer*. Netresec.

Virustotal.com. n.d. *Virustotal*. [online] Available at: <https://www.virustotal.com/gui/> [Accessed 19 November 2020].

Microsoft. 2014. *Exploit:HTML/Fiexp.A*. [online] Available at: <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:HTML/Fiexp.A> [Accessed 20 November 2020].

Klijnsma, Y., 2015. *0X3a/Tools*. [online] GitHub. Available at: <https://github.com/0x3a/tools/blob/master/fiesta-payload-decrypter.py> [Accessed 25 November 2020].

MDNC | Malware don't need Coffee. 2013. CVE-2013-2551 And Exploit Kits. [online] Available at: <https://malware.dontneedcoffee.com/2013/11/cve-2013-2551-and-exploit-kits.html> [Accessed 27 December 2020].

Appendices

Appendix A: Python Script

```
#!/usr/bin/python

"""
 Created by Yonathan Klijnsma
- http://blog.0x3a.com/
- http://twitter.com/ydklijnsma

Code comes from an article I've written about the Fiesta exploit
kit. This Python script is able to decrypt the payloads retrieved
from the Fiesta exploit kit after successful exploitation of some
kind. Shellcode based and non shellcode based payloads are
supported.

This script was tested against payloads dropped in January
2015.  If it stops working please file a bug report at the Github
repo!

Github repository URL: https://github.com/0x3a/tools/
"""

import sys

def ShellcodeDecrypt(data):
return NonShellcodeDecrypt(data[16:])[25:-1]

def NonShellcodeDecrypt(data):
    key_offset = 256
    ldata = list(data[key_offset:])
    lkey = list(data[:key_offset])

    c_index_s1 = 0
    c_index_s2 = 0
    decrypted_data = ''

    for i in xrange(0, len(ldata)):
        c_index_s1 = c_index_s1 + 1 & 0xFF;
        c_index_s2 = c_index_s2 + ord(lkey[c_index_s1]) & 0xFF;
        j = lkey[c_index_s1];
        lkey[c_index_s1] = lkey[c_index_s2];
        lkey[c_index_s2] = j;
        k = ord(lkey[c_index_s1]) + ord(lkey[c_index_s2]) & 0xFF;
        decrypted_data += chr(ord(ldata[i]) ^ ord(lkey[k]));

    return decrypted_data

  def DecryptFiestaPyload(inputfile, outputfile):
  fdata = open(inputfile, "rb").read()
   print '[+] Encrypted file size %d' % len(fdata)

   decrypted_fdata = NonShellcodeDecrypt(fdata)

 if decrypted_fdata[:2] != 'MZ':
       decrypted_fdata = ShellcodeDecrypt(fdata)

      if decrypted_fdata[:2] != 'MZ':
          print '[!] Unable to decrypt data!'
          return
       else:
          print '[+] Payload was used by a shellcode based
exploit, decrypted successfully!'
    else:
       print '[+] Payload was used for a non-shellcode based
exploit, decrypted successfully!'

   print '[+] Decrypted file size %d' % len(decrypted_fdata)

    open(outputfile, "wb").write(decrypted_fdata)

if __name__ == "__main__":
   if len(sys.argv) != 3:
       print '%s <input filename> <output filename>' %
sys.argv[0]
   else:
       sys.exit(DecryptFiestaPyload(sys.argv[1], sys.argv[2]))
```

Appendix B: Strings From Payload

Cleaned

To Directory:

- Setup was unable to shutdown system.
- Extraction Complete
- Extraction Failed
- Extracting File:$Choose Directory For Extracted Files
- Please shutdown your system manually.
- Unable to find a volume for file extraction.
- Please verify that you have proper permissions.
- Unable to find a volume with enough disk space for file extraction.
- Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

Error Code:
Error Information:

- An error (%s) has occurred while running the setup. Please make sure you have finished any previous setup and closed other applications. If the error still occurs, please contact your vendor:
- There is not enough space to initialize the setup. Please free up at least %ld KB on your %s drive before you run the setup.
- A user with administrator rights installed this application. You need to have similar privileges to modify or uninstall it.
- Another instance of this setup is already running. Please wait for the other instance to finish and then try again. PA Security Warning: Do you want to run this setup?
- The origin and integrity of this application could not be verified. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication. I do not trust this setup & understand the security risk and wish to continue
- The origin and integrity of this application could not be verified because it was not signed by the publisher. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication.
- The origin and integrity of this application could not be verified. The certificate used to sign the software has expired or is invalid or untrusted. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication.
- The software is corrupted or has been altered since it was published. You should not continue this setup.

- This setup was created with a BETA VERSION of %s
- This Setup was created with an EVALUATION VERSION of %s
- Please enter the password
- InstallShield Setup Player V16 The path to the installation contains unsupported characters. Try moving the installation to a location that does not have special characters, and then try relaunching it.
- This setup requires administrative privileges that appear to be unavailable. Would you like to try again?

Original

To Directory:JSetup was unable to shutdown system. corruptExtraction CompleteExtraction FailedExtracting File:$Choose Directory For Extracted Files
Please shutdown your system manually.\Unable to find a volume for file extraction.
Please verify that you have proper permissions.CUnable to find a volume with enough disk space for file extraction.PAx%s Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

Error Code:Error Information:3An error (%s) has occurred while running the setup. Please make sure you have finished any previous setup and closed other applications. If the error still occurs, please contact your vendor: %s.&Detail&Report}There is not enough space to initialize the setup. Please free up at least %ld KB on your %s drive before you run the setup.{A user with administrator rights installed this application. You need to have similar privileges to modify or uninstall it.tAnother instance of this setup is already running. Please wait for the other instance to finish and then try again. PASecurity WarningDo you want to run this setup? The origin and integrity of this application could not be verified. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication. I do not trust this setup 4I &understand the security risk and wish to continuThe origin and integrity of this application could not be verified because it was not signed by the publisher. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication./The origin and integrity of this application could not be verified. The certificate used to sign the software has expired or is invalid or untrusted. You should continue only if you can identify the publisher as someone you trust and are certain this application hasn't been altered since publication.jThe software is corrupted or has been altered since it was published. You should not continue this setup.0This setup was created with a BETA VERSION of %s7This Setup was created with an EVALUATION VERSION of %sPlease enter the passwordPAInstallShield Setup Player V16 The path to the installation contains unsupported characters. Try moving the installation to a location that does not have special characters, and then try relaunching it.iThis setup requires administrative privileges that appear to be unavailable. Would you like to try again?