SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

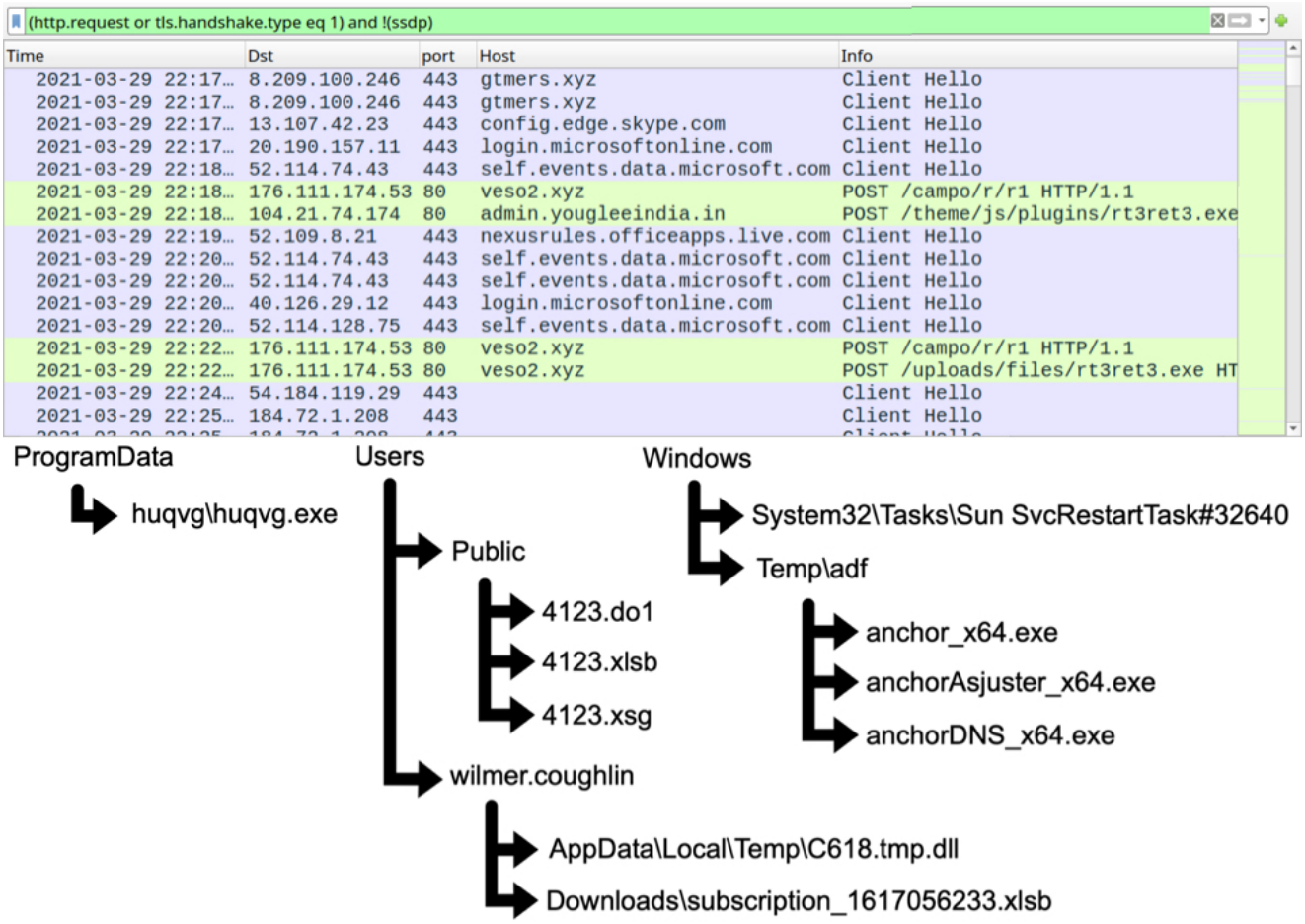
Published: 2021-04-14
Last Updated: 2021-04-14 00:18:26 UTC
by Brad Duncan (Version: 1)

Introduction

Thanks to everyone who participated in our forensic quiz originally posted on April 1st, 2021. We received 22 submissions through our contact page, and two people had all the correct answers. Unfortunately, we can only pick one winner for the contest. In this case, our winner was the first to submit the correct information. Join us in congratulating this month's winner, Alex Rodriguez-Vargas! Alex will receive this month's prize: a Raspberry Pi 4 kit.

Several people came close and almost had everything. This exercise required reviewing both the pcap and malware recovered from the infected Windows host. You can still find the pcap and malware at this Github repository.

The pcap of infection traffic for this quiz was generated from a spreadsheet retrieved when I recorded this Youtube video. The pcap in this month's quiz starts during HTTPS traffic to the "unsubscribe" page seen in the video.



Shown above: Pcap from this quiz filtered in Wireshark, and a list of the malware/artifacts.

Answers

IP address of the infected Windows computer:

> ***192.168.5.125***

Host name of the infected Windows computer:

> ***LAPTOP-X9NAQ2EU***

User account name on the infected Windows computer:

> ***wilmer.coughlin***

Date and time the infection activity began in UTC (the GMT or Zulu timezone):

> ***2021-03-29 at 22:18 UTC***
>
> NOTE: The infection activity could be considered as early as 22:15 UTC which is when the malicious domain gtmers[.]xyz appears. Or it could be considered as late as 22:22 UTC, which is when the spreadsheet macro successfully downloaded a malicious EXE for BazarLoader.

The family or families of malware on the infected computer:

- ***BazaLoader (BazarLoader)***
- ***Cobalt Strike***
- ***Anchor***

To help in your analysis of this activity, please review the ***Prerequisites*** section in our original blog for this quiz.

BazaLoader (BazarLoader) Activity

From the malware archive in the Downloads directory under wilmer.coughlin, there is an Excel spreadsheet named subscription_1617056233.xlsb. This spreadsheet has malicious macros. I submitted it to the Triage Hatching sandbox, and it generated the following traffic:

hxxp://veso2[.]xyz/campo/r/r1

In the pcap, this URL caused a redirect. First it redirected to:

hxxp://admin.youglessindia[.]in/theme/js/plugins/rt3ret3.exe

But that follow-up URL did not return any malware. This happened while I was still recording the Youtube video. At the video's 10 minute mark, I enable macros on the malicious spreadsheet, but nothing apparently happened. So the call center operator had me re-open the spreadsheet and enable macros again. That second time, the campo URL redirected to:

hxxp://veso2[.]xyz/uploads/files/rt3ret3.exe

The above URL returned a Windows executable (EXE) file. This EXE from the pcap has the same SHA256 hash as the file located in our malware archive at:

ProgramData\huqvg\huqvg.exe

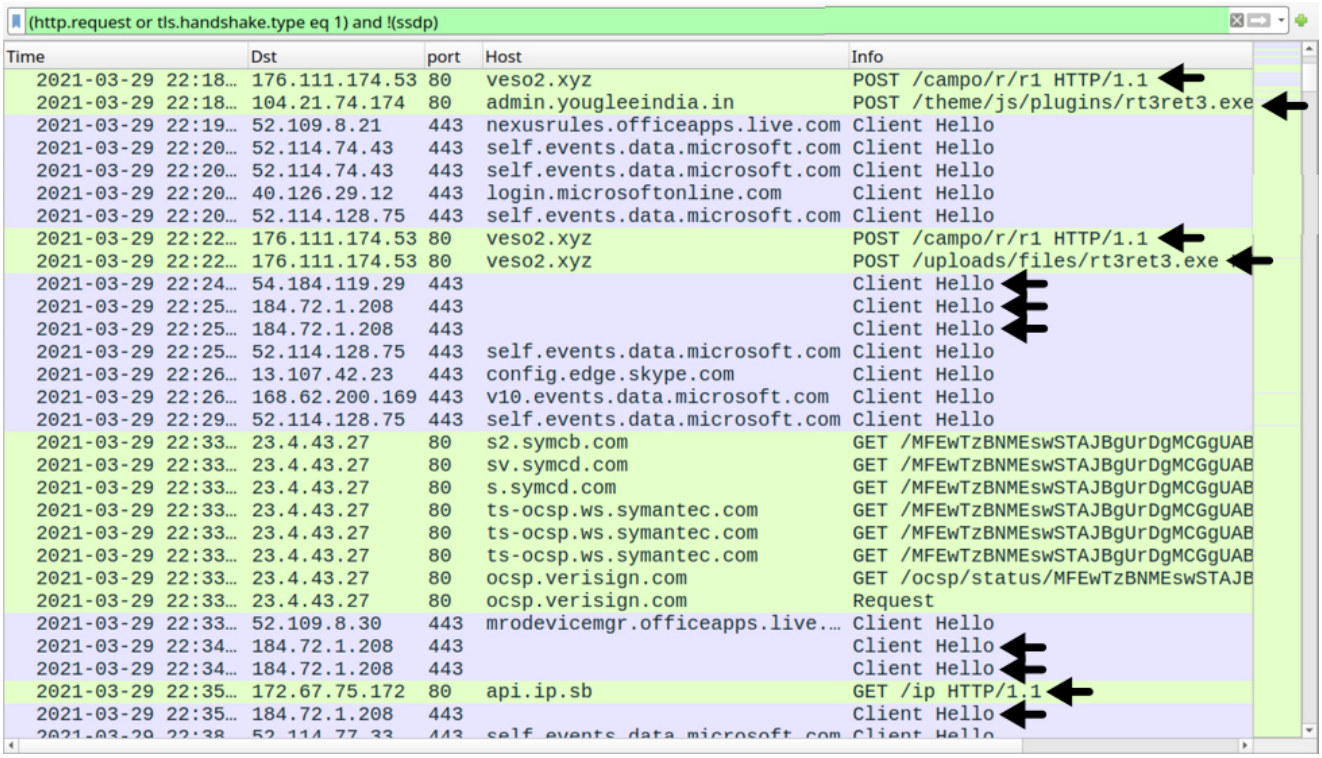
Of note, opening the spreadsheet and enabling macros generated the following artifacts:

- Users\Public\4123.do1
- Users\Public\4123.xlsb
- Users\Public\4123.xsg

Traffic caused by BazaLoader (BazarLoader) in this pcap is:

- 176.111.174[.]53 port 80 - veso2[.]xyz - POST /campo/r/r1
- 104.21.74[.]174 port 80 - admin.youglessindia[.]in - POST /theme/js/plugins/rt3ret3.exe
- 176.111.174[.]53 port 80 - veso2[.]xyz - POST /uploads/files/rt3ret3.exe
- 54.184.119[.]29 port 443 - HTTPS traffic
- 184.72.1.208 port 443 - HTTPS traffic
- port 80 - api.ip[.]sb - GET /ip

Of note, the last entry above is an IP address check by the infected Windows host. I don't normally see that with BazaLoader activity, but I could not positively attibute it to any of the other malware activity in this pcap.



(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2021-03-29 22:18…	176.111.174.53	80	veso2.xyz	POST /campo/r/r1 HTTP/1.1
2021-03-29 22:18…	104.21.74.174	80	admin.yougleeindia.in	POST /theme/js/plugins/rt3ret3.exe
2021-03-29 22:19…	52.109.8.21	443	nexusrules.officeapps.live.com	Client Hello
2021-03-29 22:20…	52.114.74.43	443	self.events.data.microsoft.com	Client Hello
2021-03-29 22:20…	52.114.74.43	443	self.events.data.microsoft.com	Client Hello
2021-03-29 22:20…	40.126.29.12	443	login.microsoftonline.com	Client Hello
2021-03-29 22:20…	52.114.128.75	443	self.events.data.microsoft.com	Client Hello
2021-03-29 22:22…	176.111.174.53	80	veso2.xyz	POST /campo/r/r1 HTTP/1.1
2021-03-29 22:22…	176.111.174.53	80	veso2.xyz	POST /uploads/files/rt3ret3.exe
2021-03-29 22:24…	54.184.119.29	443		Client Hello
2021-03-29 22:25…	184.72.1.208	443		Client Hello
2021-03-29 22:25…	184.72.1.208	443		Client Hello
2021-03-29 22:25…	52.114.128.75	443	self.events.data.microsoft.com	Client Hello
2021-03-29 22:26…	13.107.42.23	443	config.edge.skype.com	Client Hello
2021-03-29 22:26…	168.62.200.169	443	v10.events.data.microsoft.com	Client Hello
2021-03-29 22:29…	52.114.128.75	443	self.events.data.microsoft.com	Client Hello
2021-03-29 22:33…	23.4.43.27	80	s2.symcb.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	sv.symcd.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	s.symcd.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	ts-ocsp.ws.symantec.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	ts-ocsp.ws.symantec.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	ts-ocsp.ws.symantec.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB
2021-03-29 22:33…	23.4.43.27	80	ocsp.verisign.com	GET /ocsp/status/MFEwTzBNMEswSTAJB
2021-03-29 22:33…	23.4.43.27	80	ocsp.verisign.com	Request
2021-03-29 22:33…	52.109.8.30	443	mrodevicemgr.officeapps.live.…	Client Hello
2021-03-29 22:34…	184.72.1.208	443		Client Hello
2021-03-29 22:34…	184.72.1.208	443		Client Hello
2021-03-29 22:35…	172.67.75.172	80	api.ip.sb	GET /ip HTTP/1.1
2021-03-29 22:35…	184.72.1.208	443		Client Hello

Shown above: Some of the BazaLoader traffic from this infection.

Cobalt Strike Activity

Cobalt Strike was sent through encrypted HTTPS traffic generated by BazaLoader. A DLL for Cobalt Strike was saved to the infected host at:

C:\Users\wilmer.coughlin\AppData\Local\Temp\C618.tmp.dll

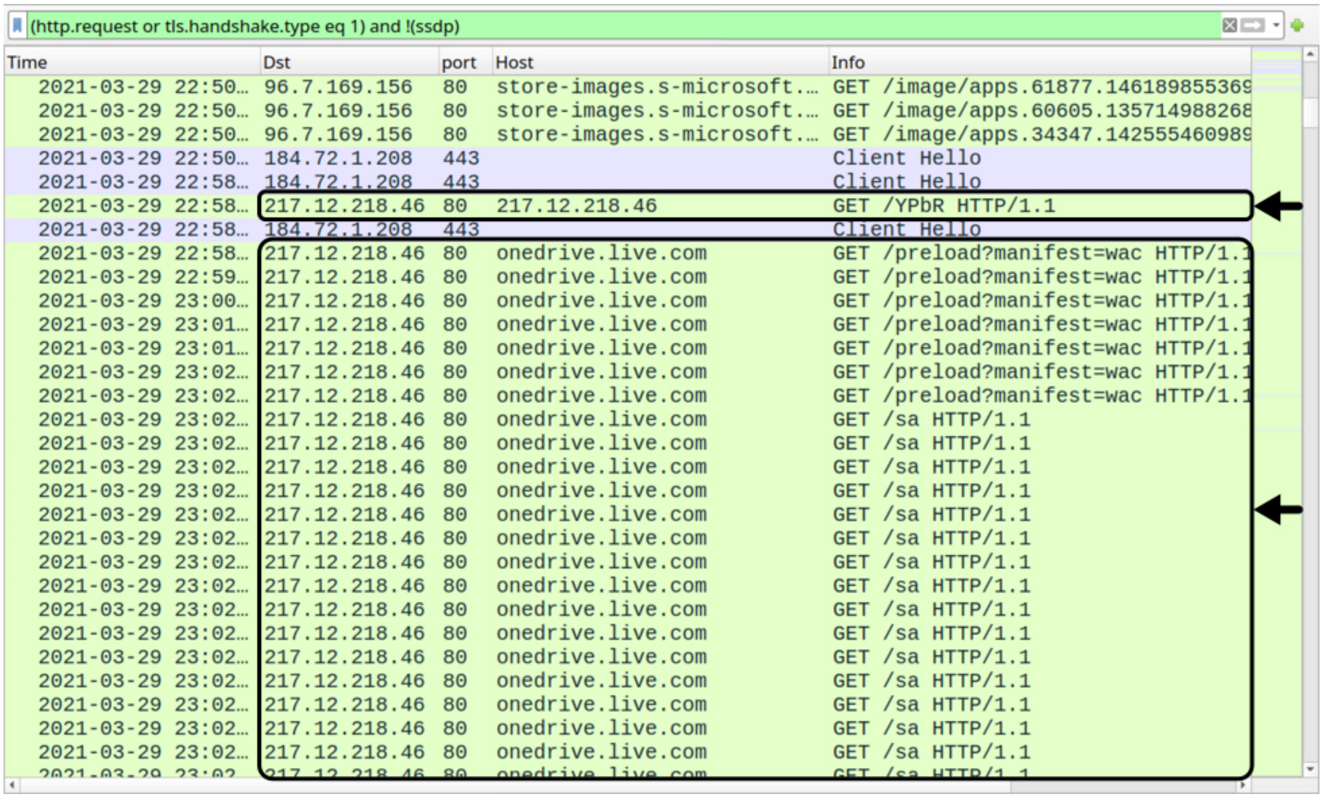
The run method for the above Cobalt Strike DLL is:

rundll32.exe *[filename]*,lowslow

This generated the following Cobalt Strike traffic:

- 217.12.218[.]46 port 80 - 217.12.218[.]46 - GET /YPbR
- 217.12.218[.]46 port 80 - onedrive.live.com - GET /preload?manifest=wac
- 217.12.218[.]46 port 80 - onedrive.live.com - GET /sa

There were a great deal of HTTP requests generated by the Cobalt Strike, about 40 to 60 HTTP requests every minute. Of note, the domain onedrive.live[.]com does not resolve to 217.12.218[.]46, which means this is a deception intentionally generated by the malware. During the Cobalt Strike traffic, seven HTTP requests to checkip.amazonaws[.]com appear as the infected Windows host periodically checks its IP address.



(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2021-03-29 22:50…	96.7.169.156	80	store-images.s-microsoft.…	GET /image/apps.61877.146189855369
2021-03-29 22:50…	96.7.169.156	80	store-images.s-microsoft.…	GET /image/apps.60605.135714988268
2021-03-29 22:50…	96.7.169.156	80	store-images.s-microsoft.…	GET /image/apps.34347.142555460989
2021-03-29 22:50…	184.72.1.208	443		Client Hello
2021-03-29 22:58…	184.72.1.208	443		Client Hello
2021-03-29 22:58…	217.12.218.46	80	217.12.218.46	GET /YPbR HTTP/1.1
2021-03-29 22:58…	184.72.1.208	443		Client Hello
2021-03-29 22:58…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 22:59…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:00…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:01…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:01…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /preload?manifest=wac HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1
2021-03-29 23:02…	217.12.218.46	80	onedrive.live.com	GET /sa HTTP/1.1

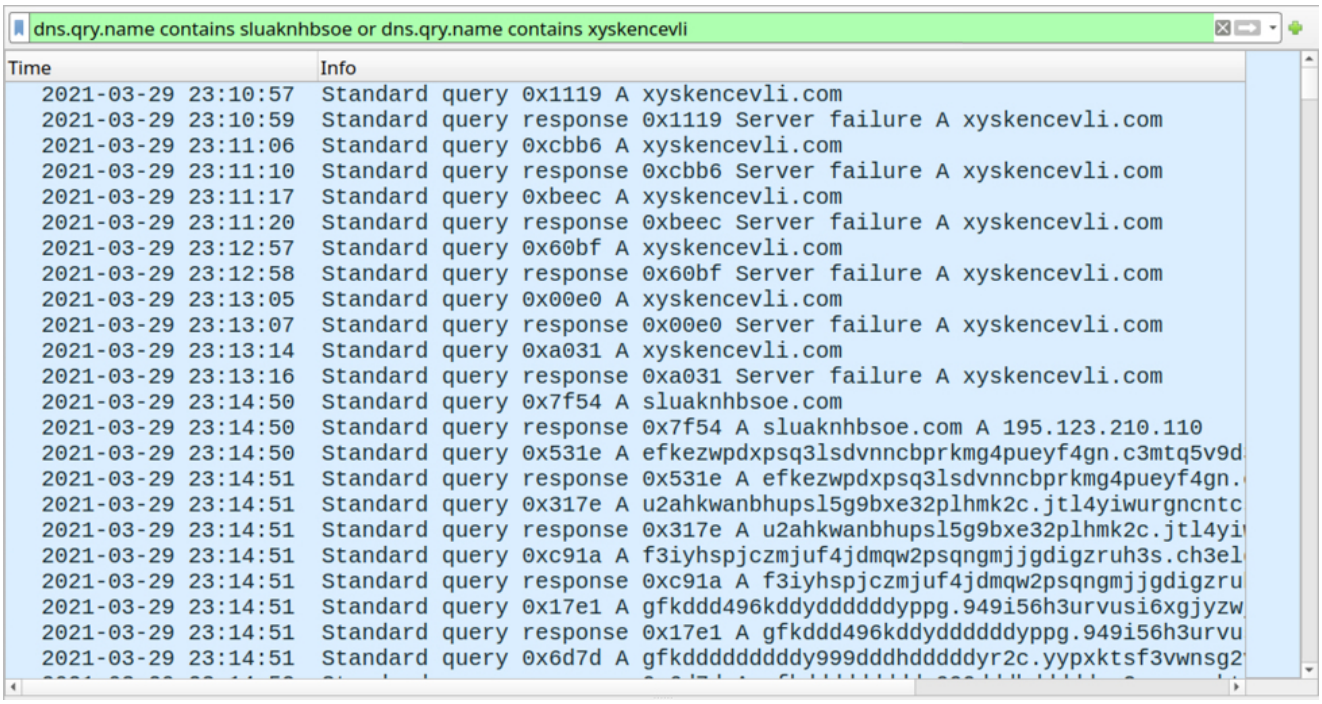
Shown above: Start of Cobalt Strike activity in the pcap.

Anchor Activity

Anchor DNS malware uses DNS queries to stealthily communicate to C2 servers. Our pcap contains DNS activity that follows patterns reported for Anchor. The associated domains are:

- sluaknhbsoe[.]com
- xyskencevli[.]com

The domain xyskencevli[.]com did not resolve, but sluaknhbsoe[.]com did. The pcap contains several DNS queries with long strings for sub-domain of sluaknhbsoe[.]com.



Shown above: DNS traffic caused by Anchor DNS malware.

This type of DNS tunneling does not rely on direct contact with the the C2 domain. Malware families like Anchor use this method to disguise tunneling from an Windows infected host. However, we can easily spot the unusual DNS queries from the pcap.

Of note, the following binaries are included in the malware archive:

- Windows\Temp\adf\anchor_x64.exe
- Windows\Temp\adf\anchorAsjuster_x64.exe
- Windows\Temp\adf\anchorDNS_x64.exe

The malware archive also contains a scheduled task at:

Windows\System32\Tasks\Sun SvcRestartTask#32640

This shows a task to run the following command:

Windows\Temp\adf\anchorDNS_x64.exe -s

The task is designed to keep Anchor DNS malware persistent on the infected Windows host.

Shown above: Scheduled task for Anchor malware.

Indicators of Compromise (IOCs)

SHA256 hash: ae6dbc08e0e21b217352175f916cfd5269c4fd8d5de6bff2d0a93a366f78e8d1

- File size: 181,413 bytes
- File name: subscription_1617056233.xlsb
- File description: Spreadsheet with macros for BazaLoader (BazarLoader)

SHA256 hash: 291c573996c647508544e8e21bd2764e6e4c834d53d6d2c8903a0001c783764b

- File size: 242,176 bytes
- File location: hxxp://veso2[.]xyz/uploads/files/rt3ret3.exe
- File location: C:\ProgramData\huqvg\huqvg.exe
- File description: EXE for BazaLoader (BazarLoader)

SHA256 hash: cc74f7e82eb33a14ffdea343a8975d8a81be151ffcb753cb3f3be10242c8a252

- File size: 299,520 bytes
- File location: C:\Users\wilmer.coughlin\AppData\Local\Temp\C618.tmp.dll
- File description: DLL for Cobalt Strike
- Run method: rundll32.exe *[filename]*,lowslow

SHA256 hash: 3ab8a1ee10bd1b720e1c8a8795e78cdc09fec73a6bb91526c0ccd2dc2cfbc28d

- File size: 251,904 bytes
- File location: C:\Windows\Temp\adf\anchorAsjuster_x64.exe

- File description: Anchor malware EXE (1 of 3)
- Note: This is not inherently malicious on its own, but can be used to run the other two Anchor files.

SHA256 hash: a8a8c66b155fcf9bfdf34ba0aca98991440c3d34b8a597c3fdebc8da251c9634

- File size: 347,648 bytes
- File location: C:\Windows\Temp\adf\anchor_x64.exe
- File description: Anchor malware EXE (2 of 3)

SHA256 hash: 9fdbd76141ec43b6867f091a2dca503edb2a85e4b98a4500611f5fe484109513

- File size: 347,648 bytes
- File location: C:\Windows\Temp\adf\anchorDNS_x64.exe
- File description: Anchor malware EXE (3 of 3)

HTTPS traffic that returned malicious spreadsheet:

8.209.100[.]246 port 443 - gtmers[.]xyz

BazaLoader traffic:

- 176.111.174[.]53 port 80 - veso2[.]xyz - POST /campo/r/r1
- 104.21.74[.]174 port 80 - admin.yougleeindia[.]in - POST /theme/js/plugins/rt3ret3.exe
- 176.111.174[.]53 port 80 - veso2[.]xyz - POST /uploads/files/rt3ret3.exe
- 54.184.119[.]29 port 443 - HTTPS traffic caused by BazaLoader (BazarLoader)
- 184.72.1[.]208 port 443 - HTTPS traffic caused by BazaLoader (BazarLoader)

IP address checks by the infected Windows host:

- port 80 - api.ip[.]sb - GET /ip
- port 80 - checkip.amazonaws[.]com - GET /

Cobalt Strike traffic:

- 217.12.218[.]46 port 80 - 217.12.218[.]46 - GET /YPbR
- 217.12.218[.]46 port 80 - onedrive.live[.]com - GET /preload?manifest=wac
- 217.12.218[.]46 port 80 - onedrive.live[.]com - GET /sa

Domains used by Anchor malware:

- sluaknhbsoe[.]com
- xyskencevli[.]com

Final words

Another case of type of infection, one where BazaLoader leads to Cobalt Strike and Anchor, was reported here last month. It even reports the same domains used by Anchor DNS that we see in this month's quiz.

Thanks to all who participated, and congratulations again to Alex Rodriguez-Vargas for winning this month's contest!

You can still find the pcap and malware at this Github repository.

Brad Duncan
brad [at] malware-traffic-analysis.net