SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center InfoSec Handlers Diary Blog

isc.sans.edu/diary/rss/28664

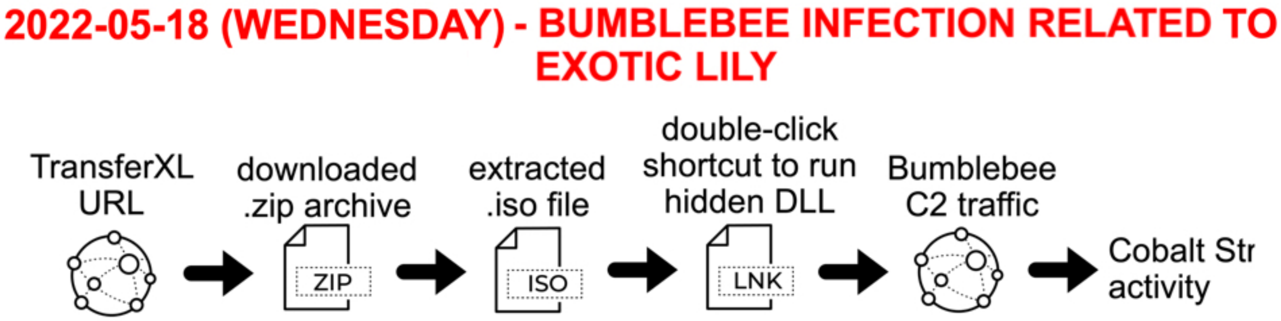
Bumblebee Malware from TransferXL URLs

Published: 2022-05-19
Last Updated: 2022-05-20 04:48:30 UTC
by Brad Duncan (Version: 1)
2 comment(s)

Introduction

Last month, Google's Threat Analysis Group (TAG) reported on EXOTIC LILY using file transfer services like TransferNow, TransferXL, WeTransfer, or OneDrive to distribute malware (link). Threat researchers like @k3dg3 occasionally report malware samples from this activity. Based on @k3dg3's recent tweet, I searched through VirusTotal and found a handful of active TransferXL URLs delivering ISO files for Bumblebee malware.

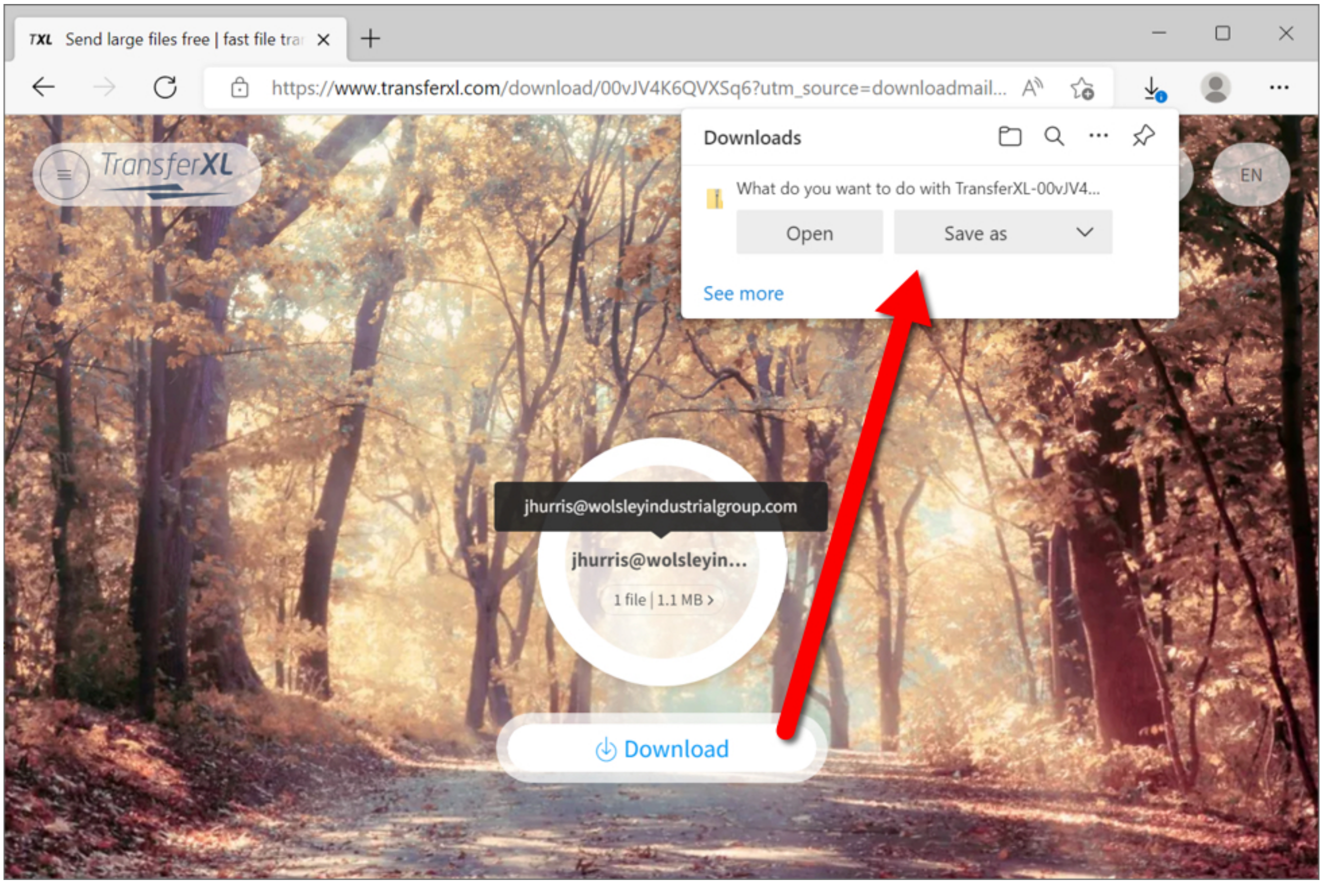
Today's diary reviews an infection generated from this activity on Wednesday 2022-05-18.


2022-05-18 (WEDNESDAY) - BUMBLEBEE INFECTION RELATED TO EXOTIC LILY
TransferXL URL
downloaded .zip archive
ZIP
extracted .iso file
ISO
double-click shortcut to run hidden DLL
LNK
Bumblebee C2 traffic
Cobalt Str activity

Shown above: Flow chart for infection discussed in this diary.

TransferXL URLs

TransferXL is a legitimate file sharing service. However, like other services with a cost-free tier, TransferXL has been abused by criminals as a way to distribute malicious files. However, with TransferXL, we have the benefit of seeing an email address used to share the malicious file. The image below shows a malicious TransferXL URL recently submitted to VirusTotal. Viewed in a web browser, it sends a malicious file. The associated email address is ***jhurris@wolsleyindustrialgroup.com***.



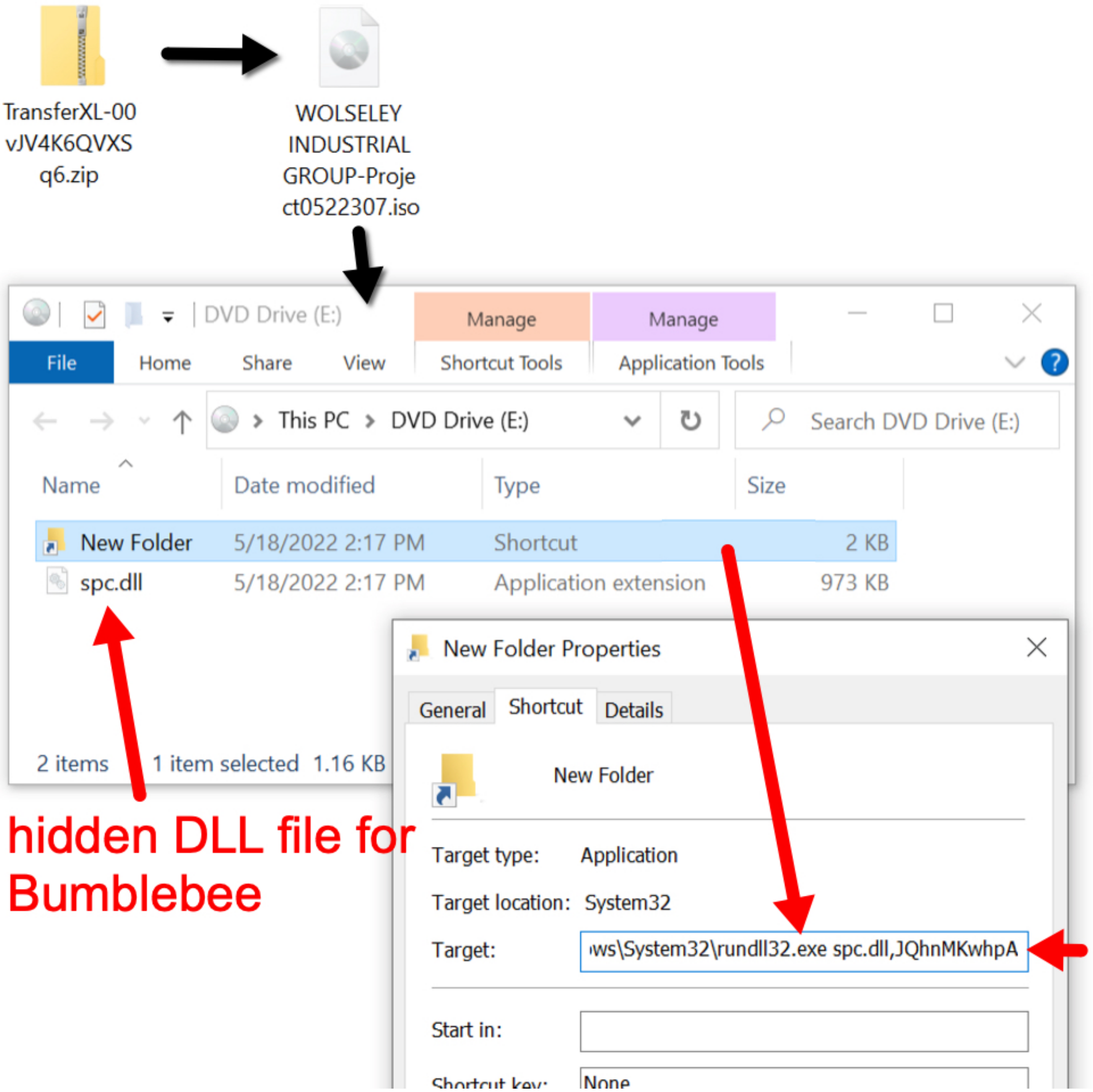
https://www.transferxl.com/download/00vJV4K6QVXSq6?utm_source=downloadmail...

What do you want to do with TransferXL-00vJV4...

jhurris@wolsleyindustrialgroup.com

Shown above: Malicious TransferXL URL delivering malware.

The downloaded zip archive contains an ISO disk image. When double-clicked, this file is mounted as a DVD drive. The ISO file contains a visible Windows shortcut and a hidden malware DLL for Bumblebee. Double-clicking the Windows shortcut will run the hidden malware DLL on a vulnerable Windows host.



Name	Date modified	Type	Size
New Folder	5/18/2022 2:17 PM	Shortcut	2 KB
spc.dll	5/18/2022 2:17 PM	Application extension	973 KB

Target type: Application

Target location: System32

Target: ws\System32\rundll32.exe spc.dll,JQhnMKwhpA

Start in:

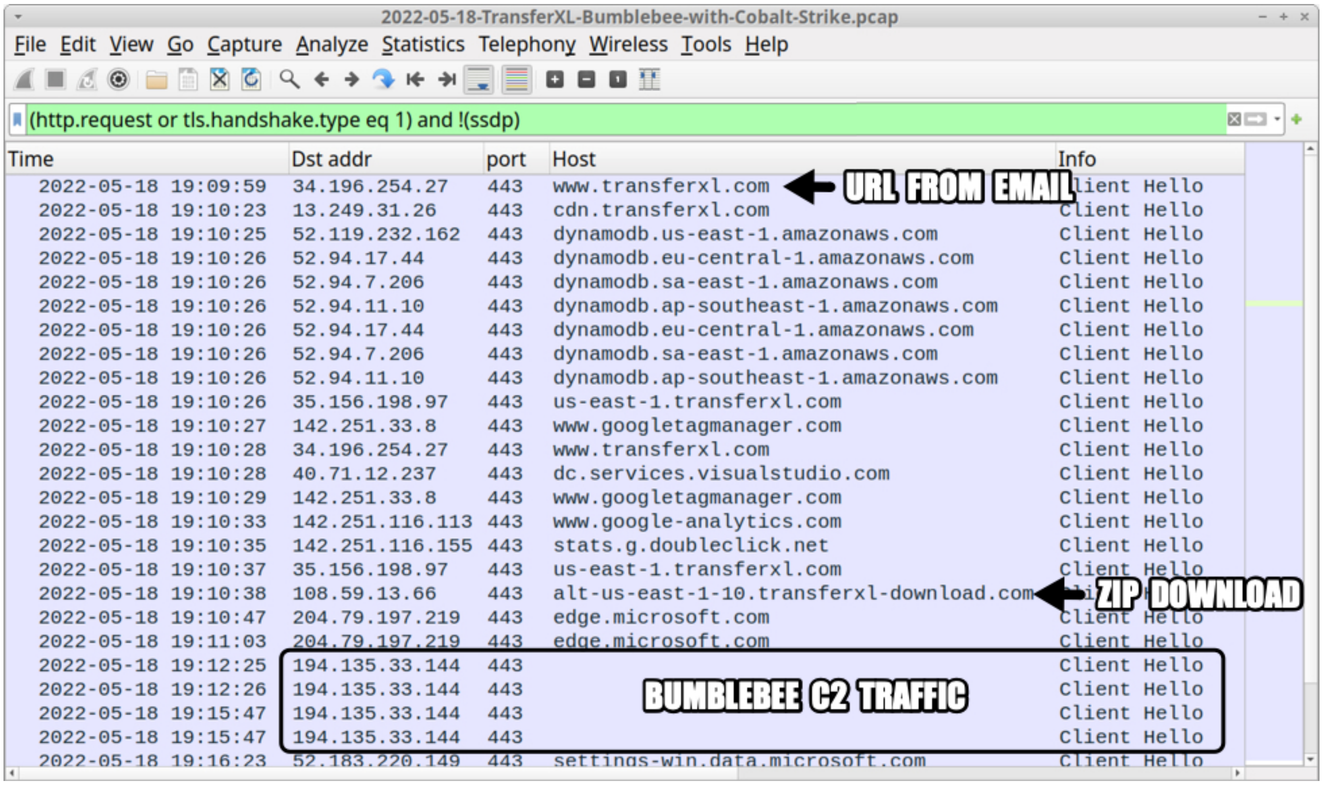
Shortcut key: None

hidden DLL file for Bumblebee

Shown above: Downloaded ISO file mounted as a disk image containing Windows shortcut and hidden malware DLL.

Traffic from an infection

After downloading malware from the malicious TransferXL URL, the infected host generated Bumblebee C2 traffic to ***194.135.33[.]144*** over TCP port 443.

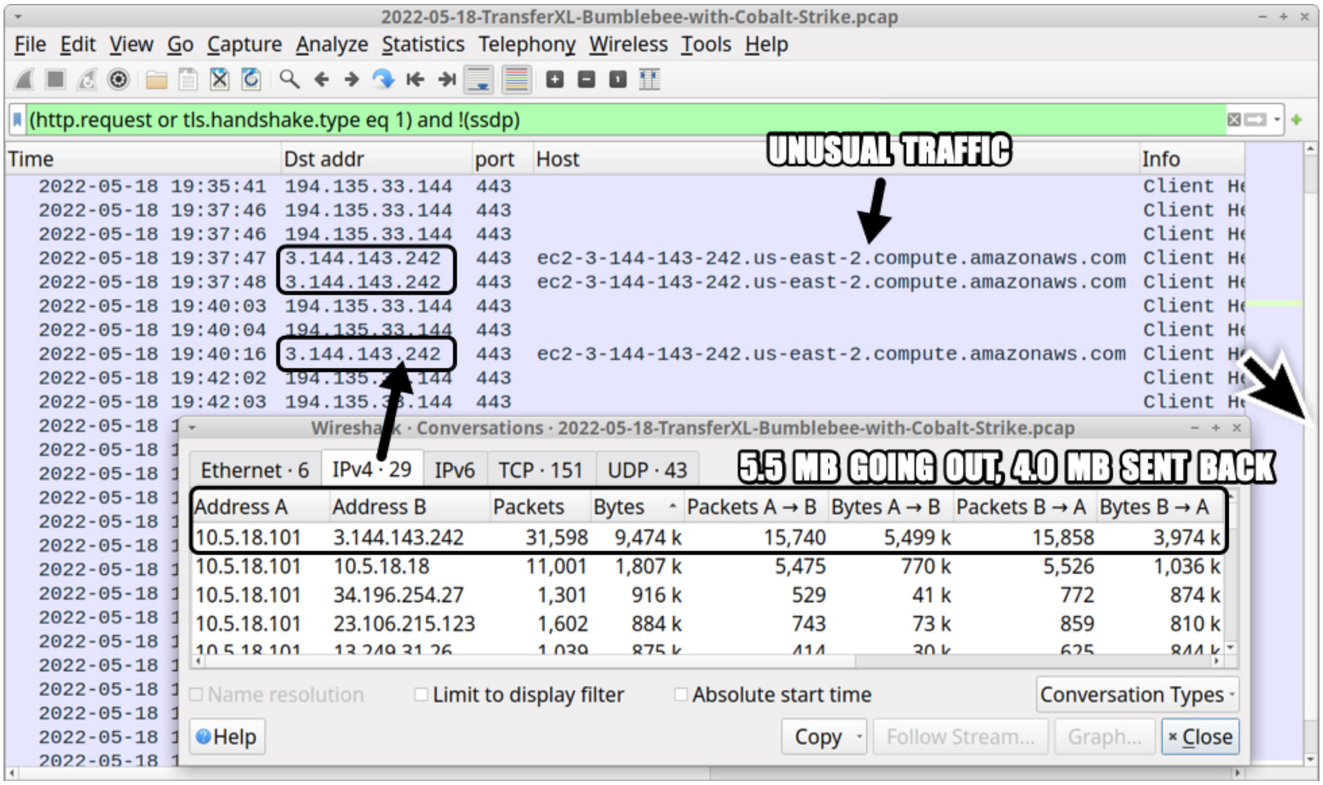

2022-05-18-TransferXL-Bumblebee-with-Cobalt-Strike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
URL FROM EMAIL
ZIP DOWNLOAD
BUMBLEBEE C2 TRAFFIC

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

Time	Dst addr	port	Host	Info
2022-05-18 19:09:59	34.196.254.27	443	www.transferxl.com	Client Hello
2022-05-18 19:10:23	13.249.31.26	443	cdn.transferxl.com	Client Hello
2022-05-18 19:10:25	52.119.232.162	443	dynamodb.us-east-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.17.44	443	dynamodb.eu-central-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.7.206	443	dynamodb.sa-east-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.11.10	443	dynamodb.ap-southeast-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.17.44	443	dynamodb.eu-central-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.7.206	443	dynamodb.sa-east-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	52.94.11.10	443	dynamodb.ap-southeast-1.amazonaws.com	Client Hello
2022-05-18 19:10:26	35.156.198.97	443	us-east-1.transferxl.com	Client Hello
2022-05-18 19:10:27	142.251.33.8	443	www.googletagmanager.com	Client Hello
2022-05-18 19:10:28	34.196.254.27	443	www.transferxl.com	Client Hello
2022-05-18 19:10:28	40.71.12.237	443	dc.services.visualstudio.com	Client Hello
2022-05-18 19:10:29	142.251.33.8	443	www.googletagmanager.com	Client Hello
2022-05-18 19:10:33	142.251.116.113	443	www.google-analytics.com	Client Hello
2022-05-18 19:10:35	142.251.116.155	443	stats.g.doubleclick.net	Client Hello
2022-05-18 19:10:37	35.156.198.97	443	us-east-1.transferxl.com	Client Hello
2022-05-18 19:10:38	108.59.13.66	443	alt-us-east-1-10.transferxl-download.com	Client Hello
2022-05-18 19:10:47	204.79.197.219	443	edge.microsoft.com	Client Hello
2022-05-18 19:11:03	204.79.197.219	443	edge.microsoft.com	Client Hello
2022-05-18 19:12:25	194.135.33.144	443		Client Hello
2022-05-18 19:12:26	194.135.33.144	443		Client Hello
2022-05-18 19:15:47	194.135.33.144	443		Client Hello
2022-05-18 19:15:47	194.135.33.144	443		Client Hello
2022-05-18 19:16:23	52.183.220.149	443	settings-win.data.microsoft.com	Client Hello

Shown above: Initial infection activity with Bumblebee C2 traffic filtered in Wireshark.

Approximately 15 minutes after the Bumblebee C2 traffic first appeared, the infected Windows host generated HTTPS traffic to ***ec2-3-144-143-232-us-east-2.compute.amazonaws[.]com*** on ***3.144.143[.]242*** over TCP port 443. The infected host sent approximately 5.5 MB of data out and received approximately 4.0 MB of data back from that server.


2022-05-18-TransferXL-Bumblebee-with-Cobalt-Strike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · 2022-05-18-TransferXL-Bumblebee-with-Cobalt-Strike.pcap
Ethernet · 6
IPv4 · 29
IPv6
TCP · 151
UDP · 43
☐ Name resolution
☐ Limit to display filter
☐ Absolute start time
Conversation Types
Help
Copy
Follow Stream...
Graph...
Close

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

```
Time                 Dst addr         port  Host                                              Info
  2022-05-18 19:35:41  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:46  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:46  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:47  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:37:48  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:40:03  194.135.33.144  443                                                    Client He
  2022-05-18 19:40:04  194.135.33.144  443                                                    Client He
  2022-05-18 19:40:16  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:42:02  194.135.33.144  443                                                    Client He
  2022-05-18 19:42:03  194.135.33.144  443                                                    Client He
```

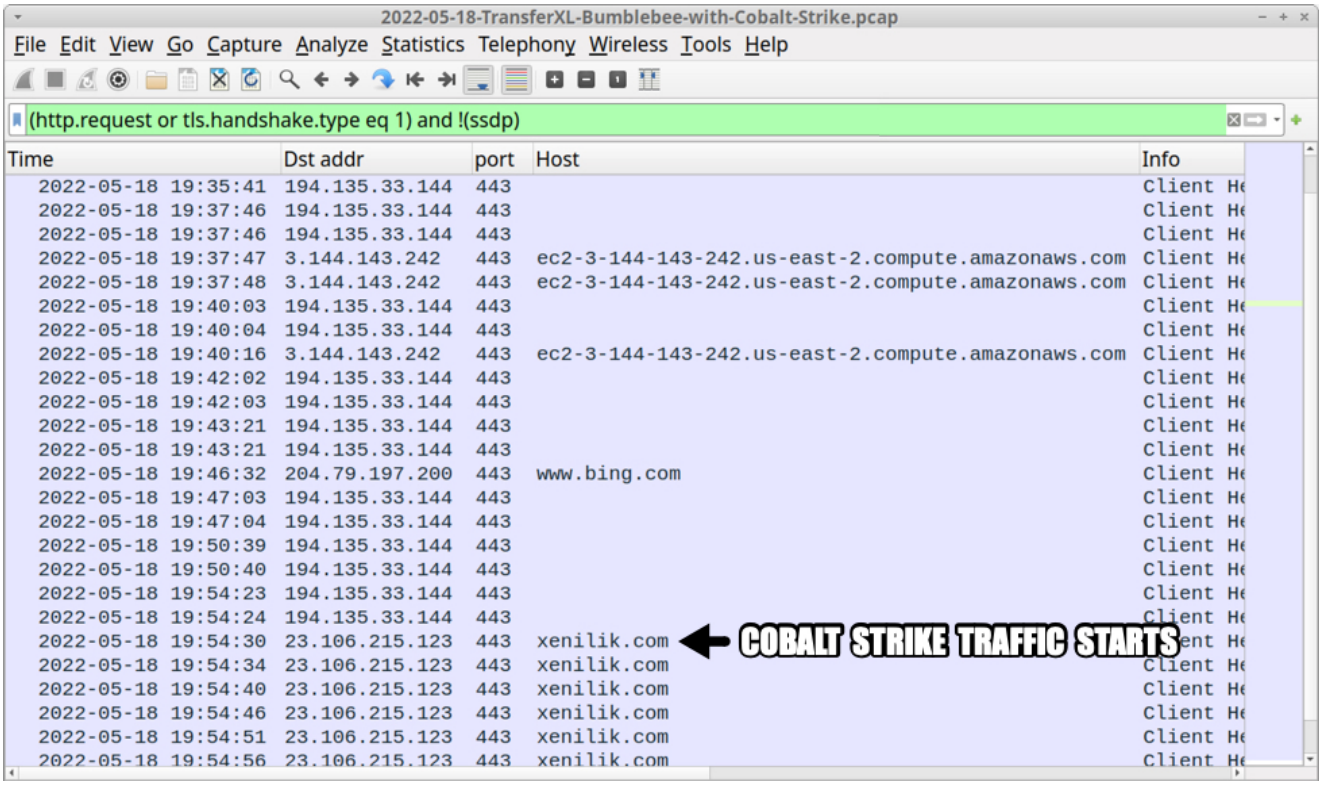
UNUSUAL TRAFFIC

5.5 MB GOING OUT, 4.0 MB SENT BACK

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
10.5.18.101	3.144.143.242	31,598	9,474 k	15,740	5,499 k	15,858	3,974 k
10.5.18.101	10.5.18.18	11,001	1,807 k	5,475	770 k	5,526	1,036 k
10.5.18.101	34.196.254.27	1,301	916 k	529	41 k	772	874 k
10.5.18.101	23.106.215.123	1,602	884 k	743	73 k	859	810 k
10.5.18.101	13.249.31.26	1,039	875 k	414	30 k	625	844 k

Shown above: Encrypted (HTTPS) traffic to an amazonAWS server.

Approximately 14 minutes after HTTPS traffic to the amazonAWS server, HTTPS Cobalt Strike traffic appeared on ***23.106.215[.]123*** over TCP port 443 using ***xenilik[.]com*** as the domain. It lasted approximately 3 minutes.


2022-05-18-TransferXL-Bumblebee-with-Cobalt-Strike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
Time                 Dst addr         port  Host                                              Info
  2022-05-18 19:35:41  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:46  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:46  194.135.33.144  443                                                    Client He
  2022-05-18 19:37:47  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:37:48  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:40:03  194.135.33.144  443                                                    Client He
  2022-05-18 19:40:04  194.135.33.144  443                                                    Client He
  2022-05-18 19:40:16  3.144.143.242   443   ec2-3-144-143-242.us-east-2.compute.amazonaws.com  Client He
  2022-05-18 19:42:02  194.135.33.144  443                                                    Client He
  2022-05-18 19:42:03  194.135.33.144  443                                                    Client He
  2022-05-18 19:43:21  194.135.33.144  443                                                    Client He
  2022-05-18 19:43:21  194.135.33.144  443                                                    Client He
  2022-05-18 19:46:32  204.79.197.200  443   www.bing.com                                     Client He
  2022-05-18 19:47:03  194.135.33.144  443                                                    Client He
  2022-05-18 19:47:04  194.135.33.144  443                                                    Client He
  2022-05-18 19:50:39  194.135.33.144  443                                                    Client He
  2022-05-18 19:50:40  194.135.33.144  443                                                    Client He
  2022-05-18 19:54:23  194.135.33.144  443                                                    Client He
  2022-05-18 19:54:24  194.135.33.144  443                                                    Client He
  2022-05-18 19:54:30  23.106.215.123  443   xenilik.com                                      Client He
  2022-05-18 19:54:34  23.106.215.123  443   xenilik.com                                      Client He
  2022-05-18 19:54:40  23.106.215.123  443   xenilik.com                                      Client He
  2022-05-18 19:54:46  23.106.215.123  443   xenilik.com                                      Client He
  2022-05-18 19:54:51  23.106.215.123  443   xenilik.com                                      Client He
  2022-05-18 19:54:56  23.106.215.123  443   xenilik.com                                      Client He
```

COBALT STRIKE TRAFFIC STARTS

Shown above: Traffic from the infection showing Cobalt Strike activity.

Indicators of Compromise (IOCs)

TransferXL URLs associated with the above email returning zip archives containing malicious ISO files.

- ***hxxps://www.transferxl[.]com/download/00ZNPDZqZwZ9m***
- ***hxxps://www.transferxl[.]com/download/00jwbtRXtsSsZX***
- ***hxxps://www.transferxl[.]com/download/00vJV4K6QVXSq6***
- ***hxxps://www.transferxl[.]com/download/00y12VGg75h7K***
- ***hxxps://www.transferxl[.]com/download/08j8ZRjHFkVxxc***

NOTE: The above URLs usually have ?utm_source=downloadmail&utm_medium=e-mail appended to them.

Email addresses associated with malicious TransferXL URLs:

- ***andresbolivar@southerncompanygas[.]co***
- ***jhurris@wolsleyindustrialgroup[.]com***
- ***m.jones@wolsleyindustrialgroup[.]com***
- ***mjones@wolsleyindustrialgroup[.]co***

Domains from the above emails:

- ***southerncompanygas[.]co*** - registered 2022-04-27
- ***wolsleyindustrialgroup[.]com*** - registered 2022-04-29
- ***wolsleyindustrialgroup[.]co*** - not registered

Malware from an infected Windows host:

SHA256 hash: 1ec8c7e21090fb4c667f40c8720388a89789c569169fe0e41ec81567df499aac

- File size: 669,897 bytes
- File name: ***TransferXL-00jdMwft3vVZ7Q.zip***
- File description: Zip archive retrieved from TransferXL URL

SHA256 hash: 24aa82e1a085412686af5d178810fc0d056c5b8167ae5b88973b33071aa14569

- File size: 1,052,672 bytes
- File name: ***documents-2205210.iso***
- File description: ISO file extracted from downloaded zip archive

SHA256 hash: ade875616534b755f33f6012ea263da808dd7eb50bc903fc97722f37fac7c164

- File size: 1,191 bytes

- File name: ***New Folder.lnk***
- File description: Windows shortcut contained in ISO file
- Shortcut: C:\Windows\System32\rundll32.exe spc.dll,JQhnMKwhpA

SHA256 hash: 88c07354f1d7b0485452d5c39dc1a6d73884e163bc5489c40adc6662602b4d76

- File size: 997,888 bytes
- File name: ***spc.dll***
- File description: 64-bit DLL (hidden flag set) for Bumblebee malware
- Run method: rundll32.exe *[filename]*,JQhnMKwhpA

Traffic from the infected Windows host:

- 194.135.33[.]144 port 443 - Bumblebee C2 HTTPS traffic
- 3.144.143[.]242 port 443 - ***ec2-3-144-143-242.us-east-2.compute.amazonaws[.]com*** - HTTPS traffic
- 23.106.215[.]123 port 443 - ***xenilik[.]com*** - Cobalt Strike HTTPS traffic

Final words

As the Google TAG blog post notes, EXOTIC LILY is using this method to push Bumblebee malware, and Bumblebee leads to further malware like Cobalt Strike. And Cobalt Strike has been documented by different sources as leading to ransomware.

Today's diary reviewed a Bumblebee malware infection associated with EXOTIC LILY that led to Cobalt Strike activity.

Pcap and malware samples associated with this infection are available here.

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

Keywords: Bumblebee malware EXOTIC LILY TransferXL Cobalt Strike

2 comment(s)

DEV522
Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked