

# Internet Storm Center

 [isc.sans.edu/forums/diary/Emotet infection with Cobalt Strike/28824/](https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/)

## Emotet infection with Cobalt Strike

**Published:** 2022-07-07

**Last Updated:** 2022-07-07 22:47:35 UTC

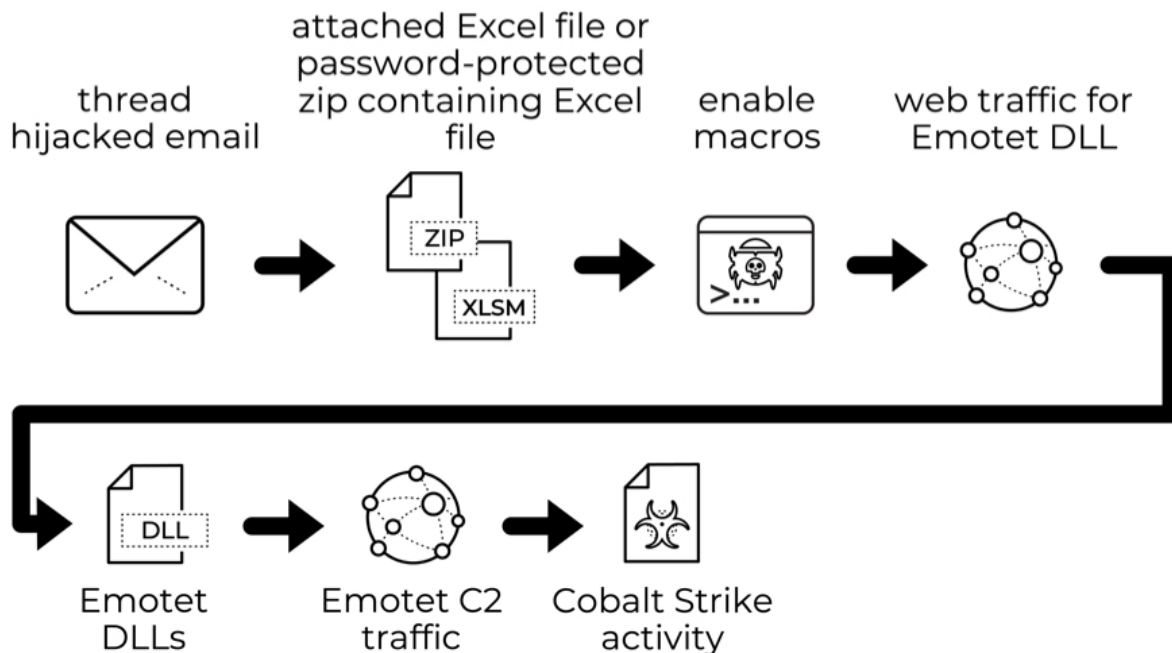
by [Brad Duncan](#) (Version: 1)

[0 comment\(s\)](#)

### **Introduction**

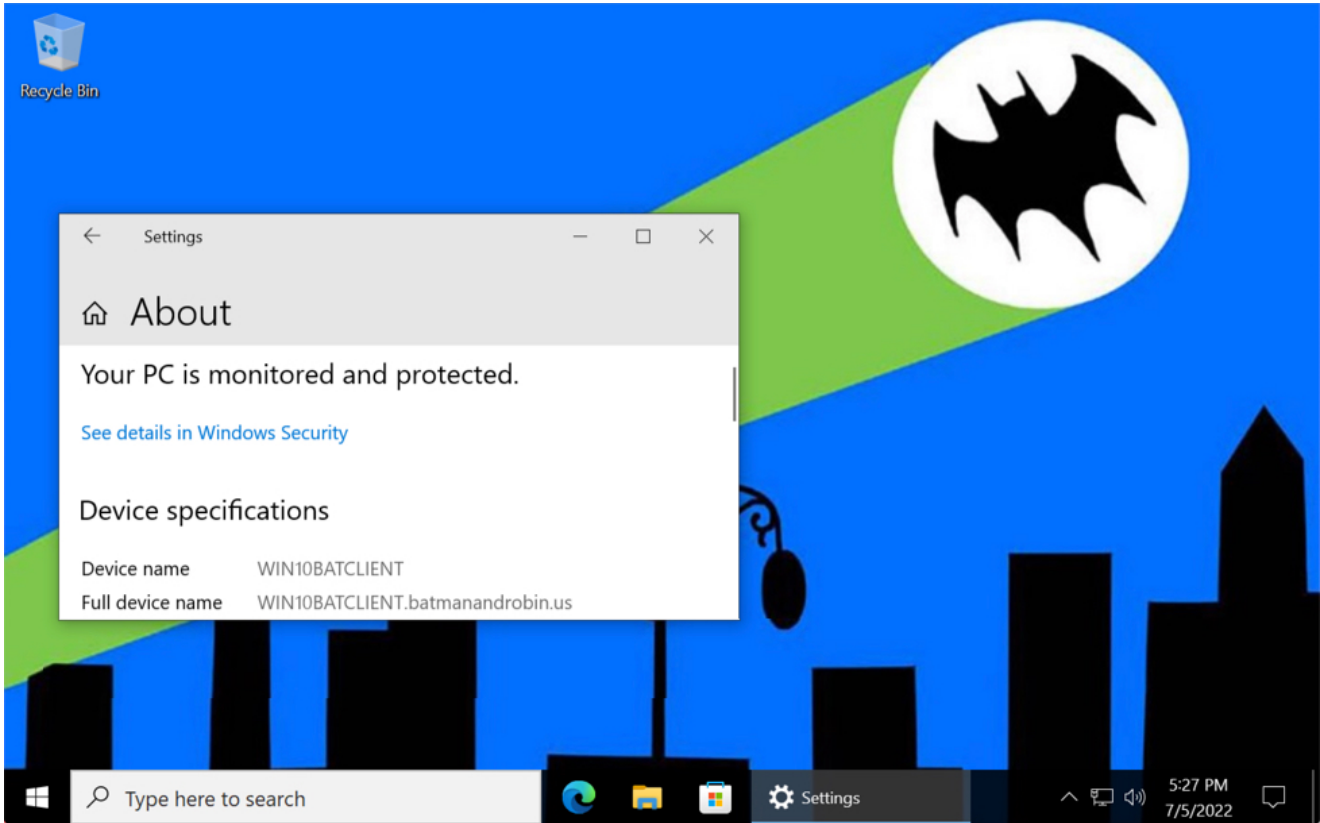
Although I haven't been posting examples lately, Emotet has remained active since I last wrote [an ISC diary about it in February 2022](#). Today on Thursday 2022-07-07, I have a new example of an Emotet infection with Cobalt Strike to share.

### **2022-07-07 (THURSDAY): EMOTET INFECTION WITH COBALT STRIKE**

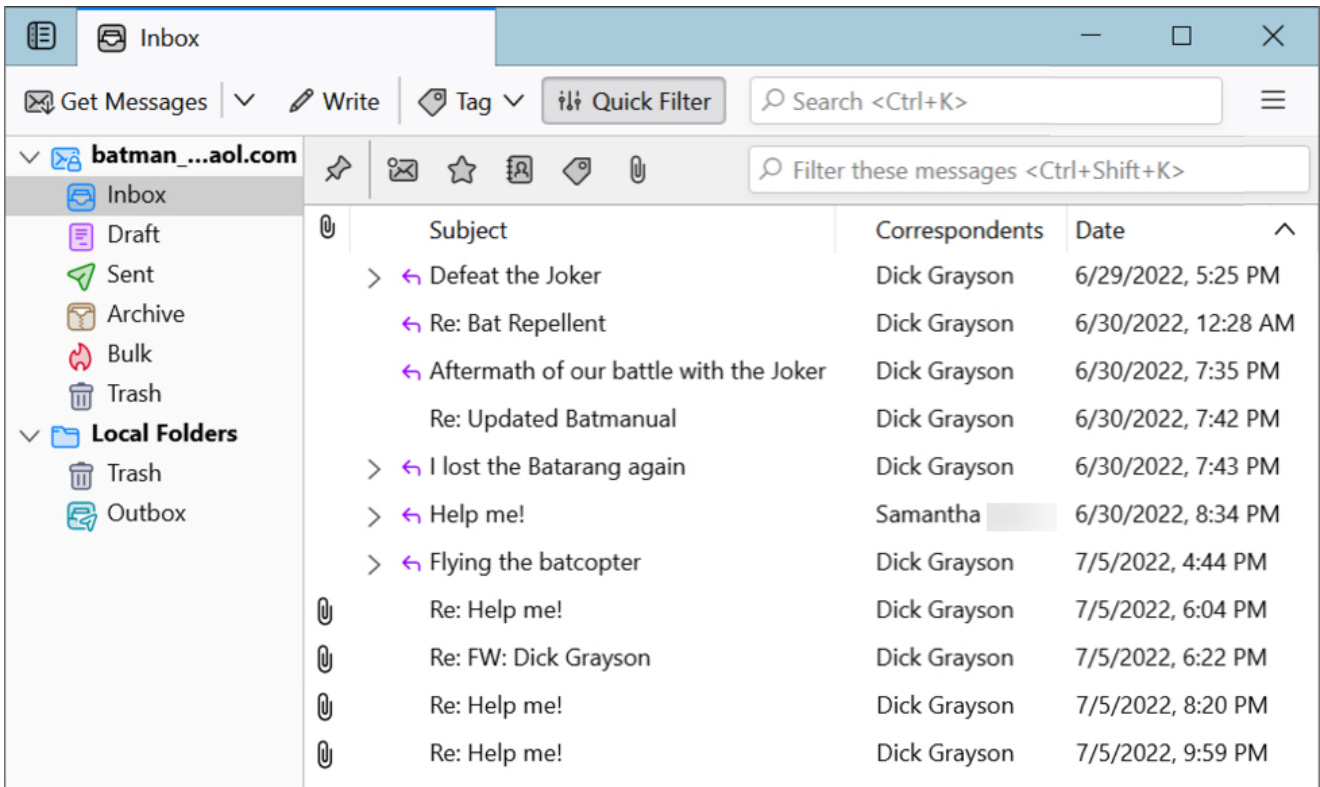


Shown above: Flow chart from today's Emotet activity on Thursday 2022-07-07.

### **Images from the infection**



Shown above: Desktop from the Windows host in my lab used for today's Emotet infection.



Shown above: Email client I had populated with messages before today's infection. The last four messages with attachments are Emotet malspam based on a previous Emotet infection.

Inbox Re: Help me! - Inbox

Get Messages Write Tag Quick Filter Search <Ctrl+K>

From Dick Grayson <ninoty-kou@mj.scn-net.ne.jp>  
To Bruce Wayne <batman\_the\_caped\_crusader@aol.com> 7/5/2022, 9:59 PM  
Subject **Re: Re: Help me!**

Per your request, please find the attached form.

Dick Grayson  
[robin\\_the\\_boy\\_wonder@yahoo.com](mailto:robin_the_boy_wonder@yahoo.com)

This seems like a trap, Batman!

Dick Grayson (a.k.a. Robin)  
robin\_the\_boy\_wonder@yahoo.com

On Thursday, June 30, 2022, 03:35:16 PM CDT, Bruce Wayne <batman\_the\_caped\_crusader@aol.com> wrote:

Where are you at, Samantha?? And what is the nature of your emergency?

Bruce Wayne  
batman\_the\_caped\_crusader@aol.com

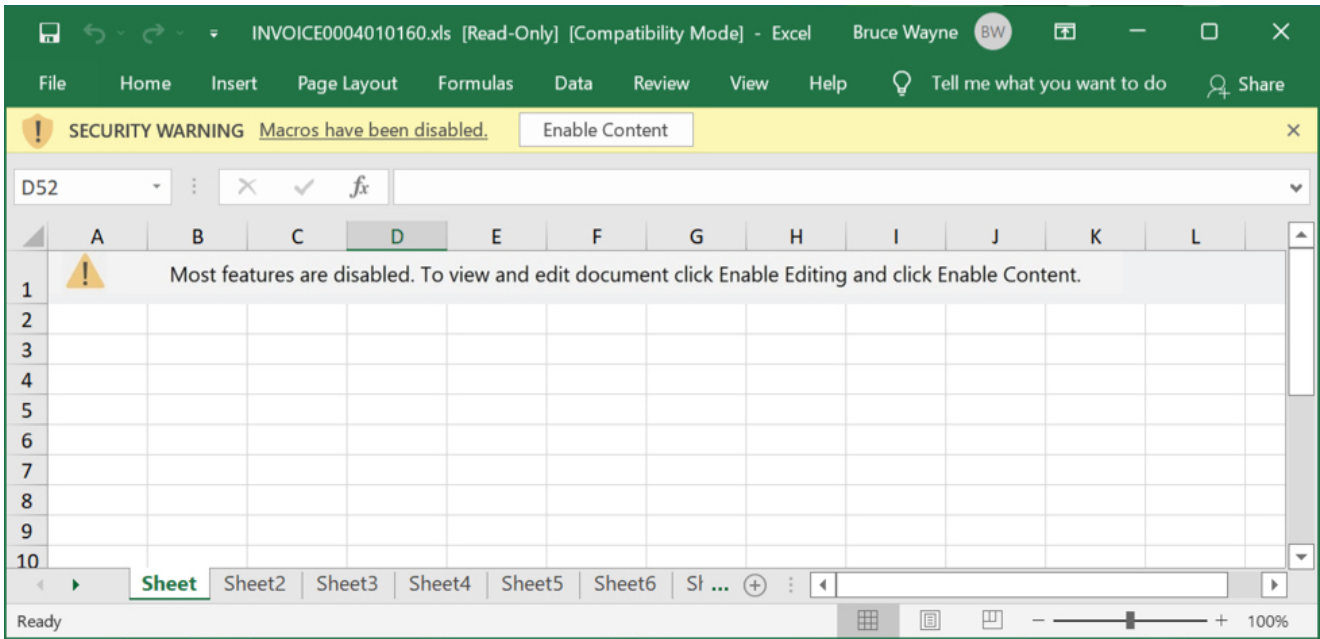
-----Original Message-----  
From: Samantha <samantha @ >  
To: Bruce Wayne (a.k.a. Batman) <batman\_the\_caped\_crusader@aol.com>; Dick Grayson (a.k.a. Robin) <robin\_the\_boy\_wonder@yahoo.com>  
Sent: Thu, Jun 30, 2022 3:34 pm  
Subject: Help me!

Help me, Batman and Robin! ?- Samantha

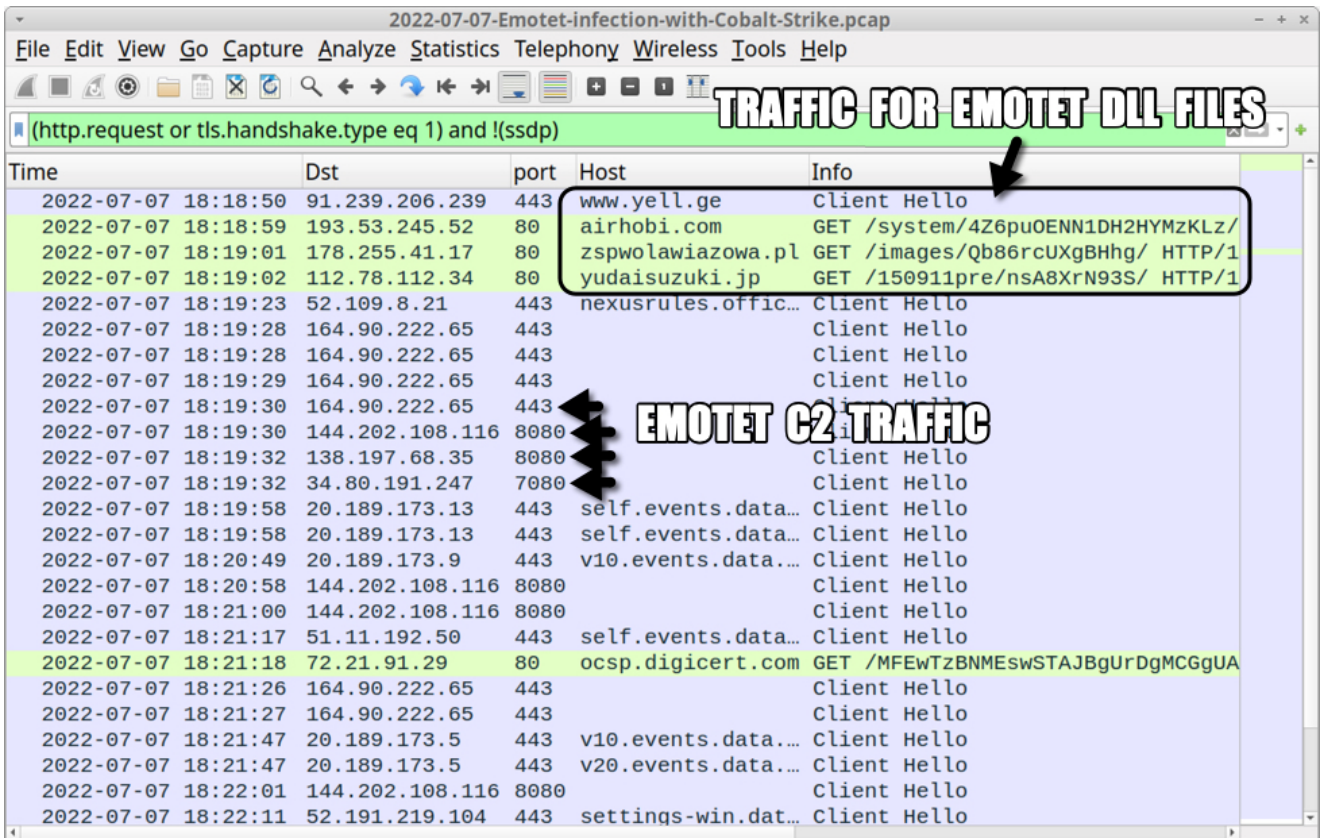
1 attachment: INVOICE0004010160.xls 95.0 KB Save

INVOICE0004010160.xls 95.0 KB

Shown above: *Emotet malspam used for today's infection.*



Shown above: Malicious Excel spreadsheet used for today's infection.



Shown above: Traffic from the infection filtered in Wireshark (1 of 2).

2022-07-07-Emotet-infection-with-Cobalt-Strike.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

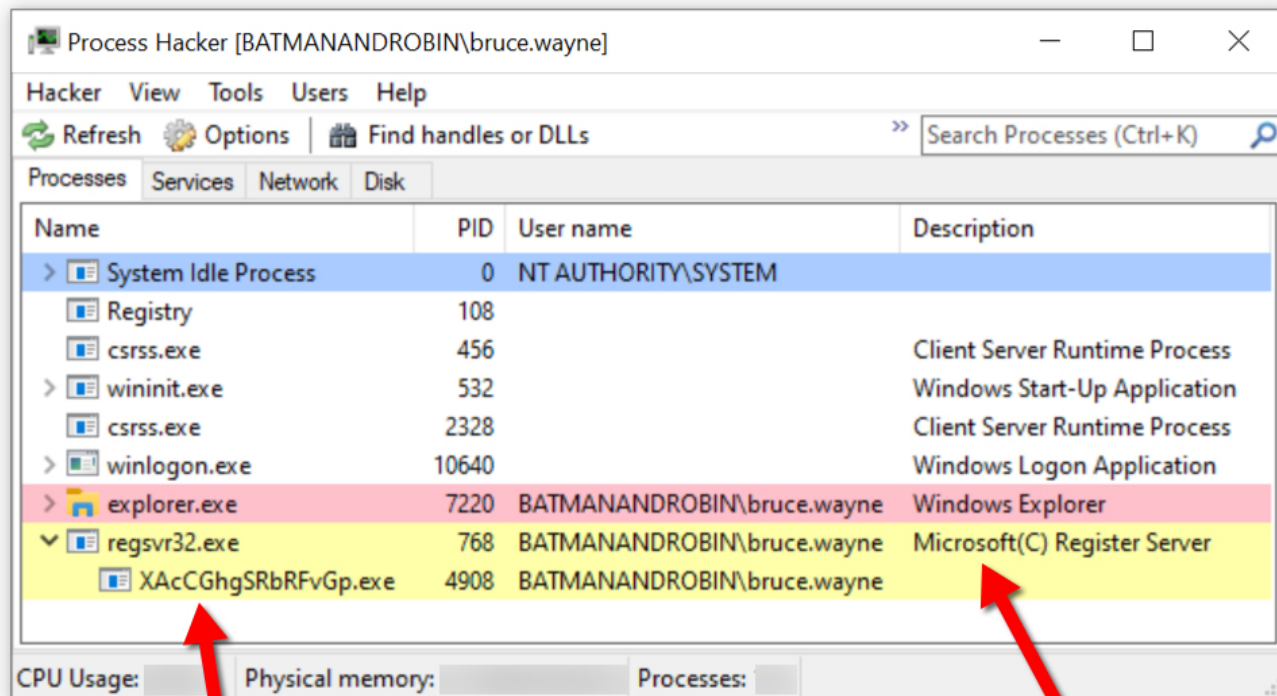
(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2022-07-07 18:31:04	164.90.222.65	443		Clie
2022-07-07 18:32:34	164.90.222.65	443		Clie
2022-07-07 18:32:36	164.90.222.65	443		Clie
2022-07-07 18:32:36	146.59.151.250	443		Clie
2022-07-07 18:33:46	164.90.222.65	443		Clie
2022-07-07 18:33:52	164.90.222.65	443		Clie
2022-07-07 18:34:14	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:35:11	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:35:16	164.90.222.65	443		Clie
2022-07-07 18:35:54	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:36:37	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:37:14	20.189.173.5	443	v10.events.data.microsoft.com	Clie
2022-07-07 18:37:17	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:37:20	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:37:52	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:38:34	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:39:10	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:39:51	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:40:34	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:40:53	40.83.240.146	443	client.wns.windows.com	Clie
2022-07-07 18:41:14	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:41:55	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:42:40	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:43:27	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie
2022-07-07 18:44:21	52.18.235.51	443	distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io	Clie

**COBALT STRIKE TRAFFIC STARTS**

Shown above: Traffic from the infection filtered in Wireshark (2 of 2).





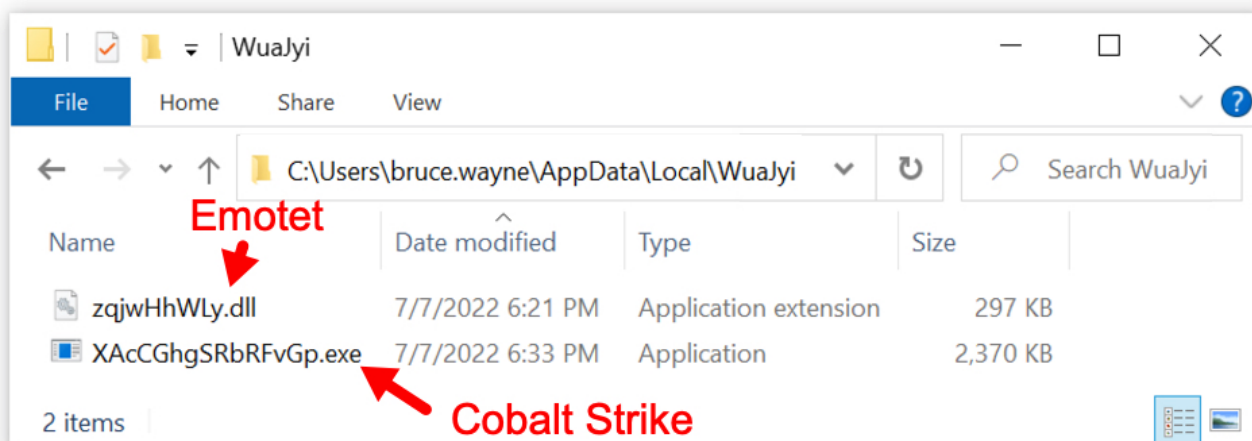
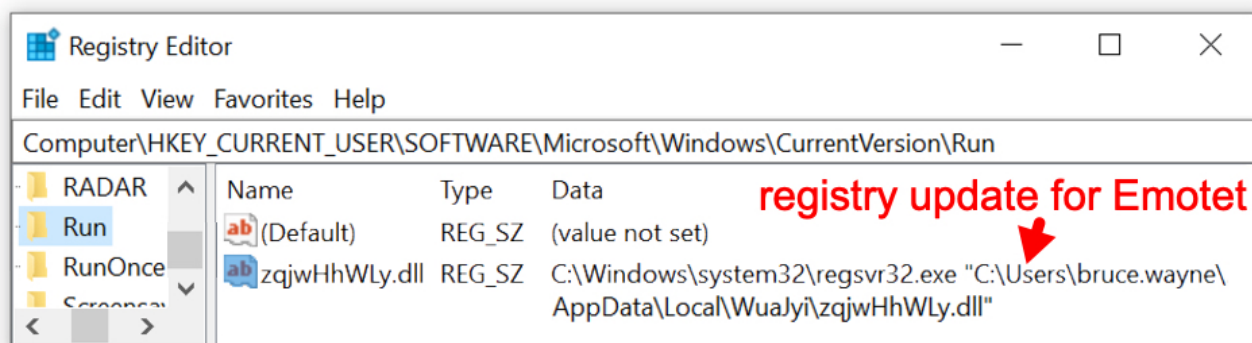
regsvr32.exe "C:\Users\bruce.wayne\AppData\Local\WuaJyi\zqjwHhWLy.dll"  
 File:  
 C:\Windows\System32\regsvr32.exe  
 Microsoft(C) Register Server 10.0.19041.1  
 Microsoft Corporation  
 Notes:  
 Signer: Microsoft Windows  
 Console host: Non-existent process (9180)

**process for Emotet**

"C:\Users\bruce.wayne\AppData\Local\WuaJyi\XAcCGhgSRbRFvGp.exe"  
 File:  
 C:\Users\bruce.wayne\AppData\Local\WuaJyi\XAcCGhgSRbRFvGp.exe  
 Notes:  
 Console host: regsvr32.exe (768)

**process for Cobalt Strike**

Shown above: Process Hacker showing processes for both Emotet and Cobalt Strike.



Shown above: Registry update and location of persistent Emotet directory with Cobalt Strike.

### Indicators of Compromise (IOCs)

Malware from an infected Windows host:

SHA256 hash:

25d4b42c98e6fb6ea5f91393252a446e0141074765e955b3e561d8b56454a73a

- File size: 97,280 bytes
- File name: INVOICE0004010160.xls
- File description: Excel spreadsheet with macros for Emotet

SHA256 hash: 1e8d9f532c2c5909ba3a8ec8d05fc8bed667dcc0c2592224827b614af7fa3ce1

- File size: 346,112 bytes
- File location: hxxps://www.yell[.]ge/nav\_logo/cvLMav68/
- File location: C:\Users\[username]\soci1.ocx
- File location: C:\Users\[username]\AppData\Local\QjPIBTdyAjEJA\AMtPK.dll
- File description: 64-bit DLL for Emotet
- Run method: regsvr32.exe [filename]

SHA256 hash: aa4b22bf31692e70b63dfa0c93888e1795c2d861550f6926c720c3609df4c39a

- File size: 346,112 bytes
- File location: [http://airhobi\[.\]com/system/4Z6puOENN1DH2HYMzKLz/](http://airhobi[.]com/system/4Z6puOENN1DH2HYMzKLz/)
- File location: C:\Users\[username]\soci2.ocx
- File location: C:\Users\[username]\AppData\Local\WuaJyi\NPpaqh.dll
- File description: 64-bit DLL for Emotet
- Run method: regsvr32.exe [filename]

SHA256 hash: 2c7e18f64c2f229d03afc9b6231f950c0489b684ec0792e75baceb4a03833ff3

- File size: 304,128 bytes
- File location: C:\Users\[username]\AppData\Local\WuaJyi\zqjwHhWLy.dll
- File description: Updated 64-bit Emotet DLL persistent on the infected Windows host
- Run method: regsvr32.exe [filename]

SHA256 hash:

6b4808050c2a6b80fc9945acdecec07a843436ea707f63555f6557057834333e

- File size: 2,426,368 bytes
- File location: C:\Users\[username]\AppData\Local\WuaJyi\XAcCGhgSRbRFvGp.exe
- File description: 64-bit EXE for Cobalt Strike sent to Emotet-infected host

Infection traffic:

URLs generated by Excel macros for Emotet DLL files:

- 91.239.206[.]239 port 443 - [http://www.yell\[.\]jge/nav\\_logo/cvLMav68/](http://www.yell[.]jge/nav_logo/cvLMav68/)
- 193.53.245[.]52 port 80 - [airhobi\[.\]com](http://airhobi[.]com/system/4Z6puOENN1DH2HYMzKLz/) - GET /system/4Z6puOENN1DH2HYMzKLz/
- 178.255.41[.]17 port 80 - [zspwolawiazowa\[.\]pl](http://zspwolawiazowa[.]pl/images/Qb86rcUXgBHhg/) - GET /images/Qb86rcUXgBHhg/
- 112.78.112[.]34 port 80 - [yudaisuzuki\[.\]jpp](http://yudaisuzuki[.]jpp) - GET /150911pre/nsA8XrN93S/

Note: The first two returned DLL files, but the second two did not

Emotet C2 traffic:

- 164.90.222[.]65 port 443 - HTTPS traffic
- 144.202.108[.]116 port 8080 - HTTPS traffic
- 138.197.68[.]35 port 8080 - HTTPS traffic
- 34.80.191[.]247 port 7080 - HTTPS traffic
- 201.73.143[.]120 port 8080 - HTTPS traffic
- 146.59.151[.]250 port 443 - HTTPS traffic
- 162.243.103[.]246 port 8080 - HTTPS traffic

Cobalt Strike traffic:



52.18.235[.]51 port 443 - ***distinctive-obi-mgw.aws-euw1.cloud-ara.tyk[.]jio*** - HTTPS traffic

Cobalt Strike URLs:

- ***distinctive-obi-mgw.aws-euw1.cloud-ara.tyk[.]jio*** - GET /api/v2/login
- ***distinctive-obi-mgw.aws-euw1.cloud-ara.tyk[.]jio*** - POST /api/v2/status?\_\_cfduid=[19 characters, base64 string]

### ***Final words***

While Emotet might not get much high-profile press lately, it remains a continuing presence in our threat landscape. A packet capture (pcap) of today's infection traffic with the email and associated malware samples can be found [here](#).

Brad Duncan

brad [at] malware-traffic-analysis.net

Keywords: [Cobalt Strike](#) [DLL](#) [Emotet](#) [Excel](#) [EXE](#) [malspam](#)

[0 comment\(s\)](#)

Join us at SANS! [Attend with Brad Duncan in starting](#)

**DEV522** Defending Web Application Security Essentials [LEARN MORE](#)  
**Learn** to defend your apps **before** they're hacked 

[Top of page](#)

×

[Diary Archives](#)