Hancitor activity resumes after a hoilday break - SANS ISC

By SANS Internet Storm Center

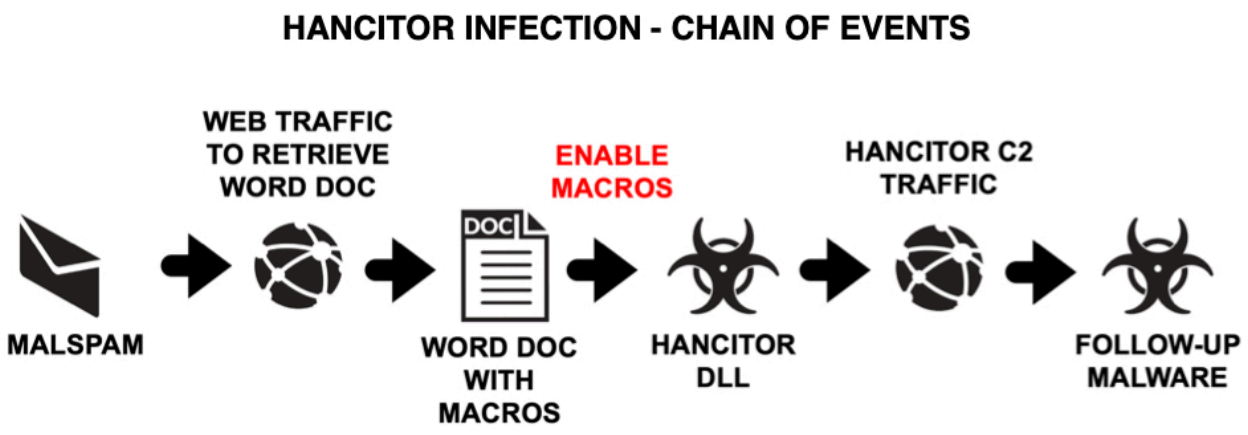
Archived: 2026-04-05 21:08:54 UTC

Introduction

Campaigns spreading Hancitor malware were active from October through December 2020, but Hancitor went quiet after 2020-12-17. On Tuesday 2021-01-12, criminals started sending malicious spam (malspam) pushing Hancitor again. Some people have already tweeted about this year's first wave of Hancitor. See the links below.

- https://twitter.com/James_inthe_box/status/1349015970220748809
- https://twitter.com/ffforward/status/1349018081486659587
- https://twitter.com/r_jordan3/status/1349058833964961794
- https://twitter.com/executemalware/status/1349106968569536518

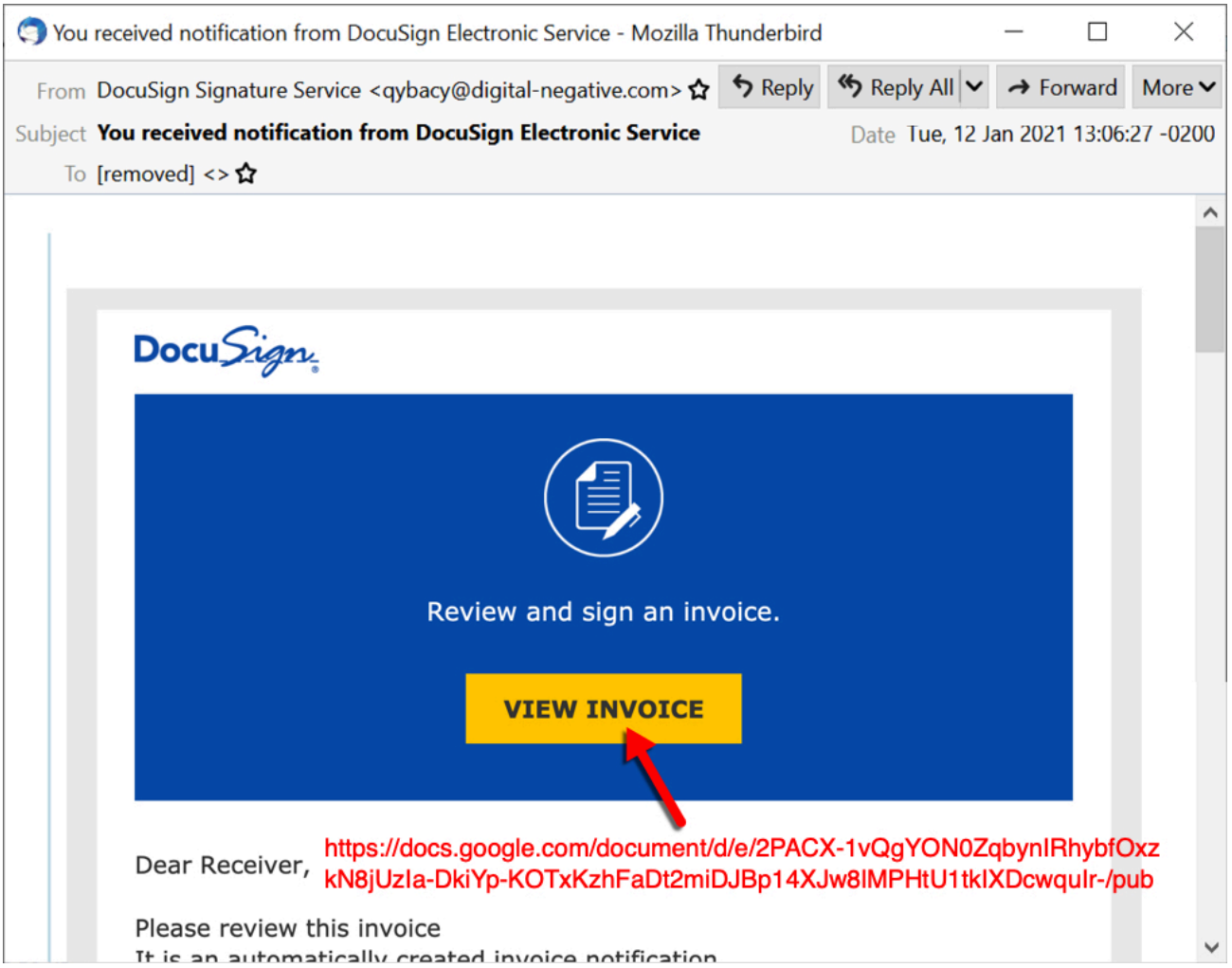
Today's diary reviews recent Hancitor activity from Tuesday 2021-01-12, where we also saw Cobalt Strike after the initial infection.



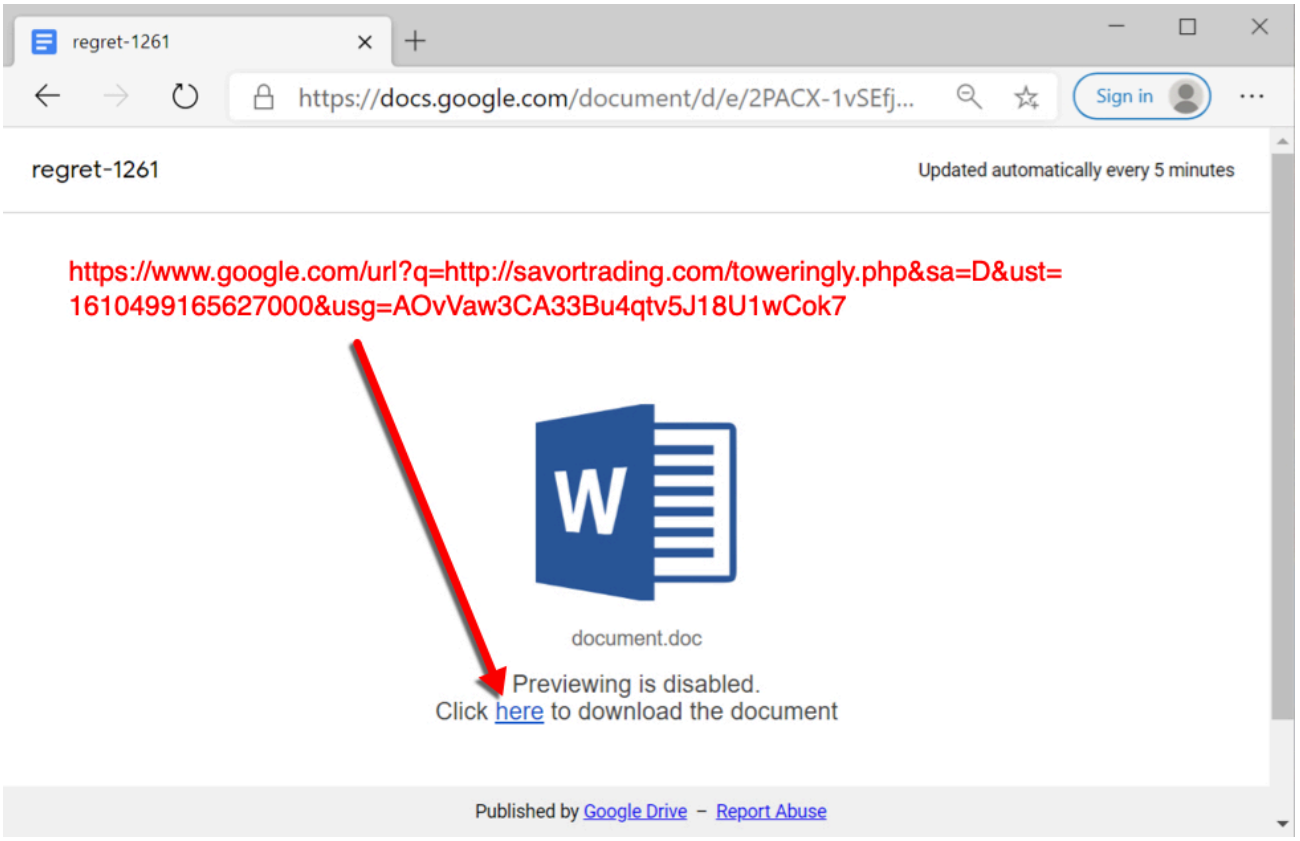
Shown above: Flow chart for recent Hancitor infection activity.

The malspam

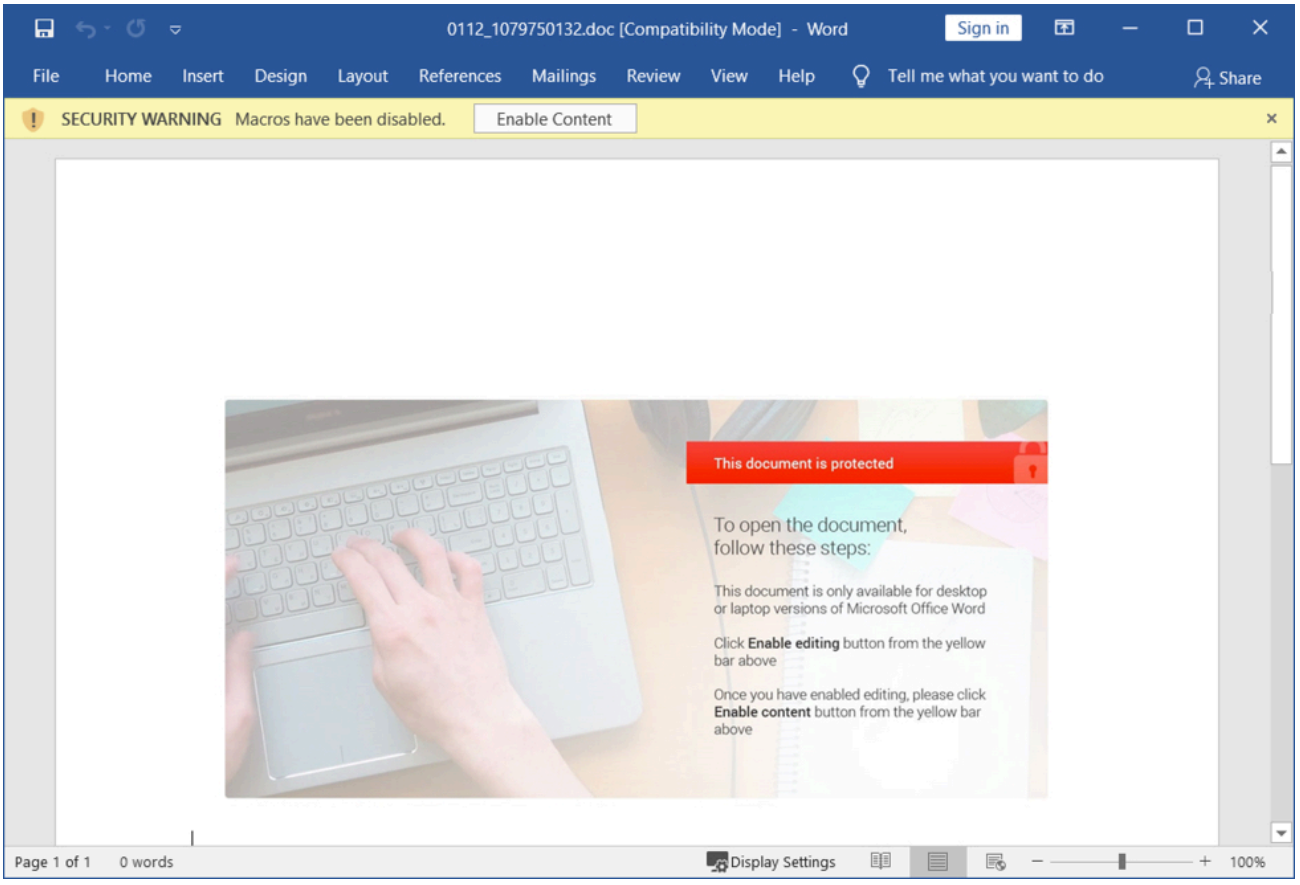
On Tuesday 2021-01-12, malspam spreading used the same fake DocuSign template we saw several times last year. These emails have a link to a Google Docs page.



Shown above: Screenshot from one of the emails distributing Hancitor on Tuesday 2021-01-12.



Shown above: Link from the email redirects to a page that can generate a Word document for Hancitor.



Shown above: Word document with macros for Hancitor.

Infection traffic

As you might expect, traffic to the Google Docs page and clicking on the link generates a great deal of related web activity, mostly HTTPS traffic. Shortly after the Word document is sent, we find indicators of Hancitor and Cobalt Strike malware. I've always seen Cobalt Strike when I test Hancitor in an Active Directory (AD) environment. if you're investigating an actual Hancitor infection, be aware that it will likely send Cobalt Strike if the victim host is signed into an work environment that uses AD.

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

Time	Dst	port	Host	Info
2021-01-12 16:21:26	142.250.68.78	443	docs.google.com	Client Hello
2021-01-12 16:21:26	142.250.68.78	443	docs.google.com	Client Hello
2021-01-12 16:21:27	172.217.5.193	443	lh6.googleuserconten…	Client Hello
2021-01-12 16:21:27	172.217.5.193	443	lh6.googleuserconten…	Client Hello
2021-01-12 16:21:27	142.250.68.42	443	fonts.googleapis.com	Client Hello
2021-01-12 16:21:28	13.107.42.23	443	config.edge.skype.com	Client Hello
2021-01-12 16:21:28	13.107.42.23	443	config.edge.skype.com	Client Hello
2021-01-12 16:21:31	104.31.80.93	80	savortrading.com	GET /sacrifice.php HTTP/1.1
2021-01-12 16:21:31	172.217.14.99	443	ssl.gstatic.com	Client Hello
2021-01-12 16:21:32	104.31.80.93	80	savortrading.com	GET /sacrifice.php HTTP/1.1
2021-01-12 16:21:32	172.217.14.99	443	ssl.gstatic.com	Client Hello
2021-01-12 16:21:35	104.31.80.93	80	savortrading.com	GET /favicon.ico HTTP/1.1
2021-01-12 16:21:35	151.101.2.133	443	www.docusign.com	Client Hello
2021-01-12 16:21:36	23.35.176.251	443	cdn.optimizely.com	Client Hello
2021-01-12 16:21:36	23.3.85.89	443	players.brightcove.n…	Client Hello
2021-01-12 16:21:37	131.253.33.200	443	www.bing.com	Client Hello
2021-01-12 16:21:37	104.127.11.24	443	cdn3.optimizely.com	Client Hello
2021-01-12 16:21:37	151.101.2.110	443	fast.wistia.com	Client Hello
2021-01-12 16:21:37	216.58.193.200	443	www.googletagmanager…	Client Hello
2021-01-12 16:21:37	104.127.11.134	443	a275532918.cdn.optim…	Client Hello
2021-01-12 16:21:37	13.33.68.33	443	sdk.inbenta.io	Client Hello
2021-01-12 16:21:37	172.64.196.24	443	siteimproveanalytics…	Client Hello
2021-01-12 16:21:38	52.202.216.245	443	logx.optimizely.com	Client Hello
2021-01-12 16:21:38	35.244.232.184	443	metrics.brightcove.c…	Client Hello

Shown above: Traffic caused by the Google Docs page before the infection filtered in Wireshark.

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

Time	Dst	port	Host	Info
2021-01-12 16:22:11	23.21.252.4	80	api.ipify.org	GET / HTTP/1.1
2021-01-12 16:22:12	185.87.194.148	80	fruciand.com	POST /8/forum.php HTTP/1.1
2021-01-12 16:22:13	47.254.175.0	80	steroidi.pro	GET /2112.bin HTTP/1.1
2021-01-12 16:22:13	47.254.175.0	80	steroidi.pro	GET /2112s.bin HTTP/1.1
2021-01-12 16:22:13	162.223.31.160	10…	162.223.31.160:1080	GET /GvSL HTTP/1.1
2021-01-12 16:22:13	52.114.132.11	443	self.events.data.m…	Client Hello
2021-01-12 16:22:13	162.223.31.160	443		Client Hello
2021-01-12 16:22:14	162.223.31.160	10…	162.223.31.160:1080	GET /visit.js HTTP/1.1
2021-01-12 16:22:14	8.251.25.254	80	ctldl.windowsupdat…	GET /msdownload/update/v3/s
2021-01-12 16:22:16	162.223.31.160	443		Client Hello
2021-01-12 16:23:03	52.114.132.22	443	v10.events.data.mi…	Client Hello
2021-01-12 16:23:04	52.114.132.22	443	v20.events.data.mi…	Client Hello
2021-01-12 16:23:14	162.223.31.160	10…	162.223.31.160:1080	GET /visit.js HTTP/1.1
2021-01-12 16:23:17	162.223.31.160	443		Client Hello
2021-01-12 16:24:13	185.87.194.148	80	fruciand.com	POST /8/forum.php HTTP/1.1
2021-01-12 16:24:14	162.223.31.160	10…	162.223.31.160:1080	GET /visit.js HTTP/1.1
2021-01-12 16:24:18	162.223.31.160	443		Client Hello
2021-01-12 16:24:47	13.107.246.13	443	pti.store.microsof…	Client Hello
2021-01-12 16:24:47	52.230.222.68	443	client.wns.windows…	Client Hello
2021-01-12 16:25:14	162.223.31.160	10…	162.223.31.160:1080	GET /visit.js HTTP/1.1
2021-01-12 16:25:18	162.223.31.160	443		Client Hello
2021-01-12 16:25:47	52.230.222.68	443	client.wns.windows…	Client Hello
2021-01-12 16:26:14	23.21.252.4	80	api.ipify.org	GET / HTTP/1.1
2021-01-12 16:26:14	185.87.194.148	80	fruciand.com	POST /8/forum.php HTTP/1.1
2021-01-12 16:26:15	162.223.31.160	10…	162.223.31.160:1080	GET /visit.js HTTP/1.1
2021-01-12 16:26:18	40.78.128.150	443	self.events.data.m…	Client Hello

Shown above: Hancitor and Cobalt Strike traffic within an AD environment.

Indicators of Compromise (IOCs)

The following are indicators associated with Hancitor infections from Tuesday 2021-01-12.

Date/time of the six messages:

- Tue, 12 Jan 2021 15:06:25 +0000 (UTC)
- Tue, 12 Jan 2021 16:06:06 +0000 (UTC)
- Tue, 12 Jan 2021 16:41:01 +0000 (UTC)
- Tue, 12 Jan 2021 16:48:35 +0000 (UTC)
- Tue, 12 Jan 2021 17:09:10 +0000 (UTC)
- Tue, 12 Jan 2021 18:06:56 +0000 (UTC)

IP addresses the malspam was received from:

- Received: from digital-negative.com ([179.154.63.198])
- Received: from digital-negative.com ([74.85.247.234])
- Received: from digital-negative.com ([181.137.227.228])
- Received: from digital-negative.com ([104.161.24.86])
- Received: from digital-negative.com ([23.236.75.32])
- Received: from digital-negative.com ([112.15.74.137])

Spoofed sending addresses:

- From: "DocuSign Signature Service" <qybacy@digital-negative.com>
- From: "DocuSign Signature and Invoice" <iqinica@digital-negative.com>
- From: "DocuSign Electronic Signature and Invoice Service" <eupanic@digital-negative.com>
- From: "DocuSign Electronic Signature " <uvizao@digital-negative.com>
- From: "DocuSign Signature Service" <nuxzoj@digital-negative.com>
- From: "DocuSign Electronic Signature Service" <zwtmicy@digital-negative.com>

Subject lines:

- Subject: You received notification from DocuSign Electronic Service
- Subject: You received notification from DocuSign Service
- Subject: You got notification from DocuSign Electronic Signature Service
- Subject: You got invoice from DocuSign Electronic Signature Service
- Subject: You got notification from DocuSign Service
- Subject: You received notification from DocuSign Electronic Signature Service

Links from the malspam:

- hxxps://docs.google[.]com/document/d/e/2PACX-1vSEfjWipv61XyrbNDn1neBUGeHzEPM35pYN5QRYrpUy4X-sbHybYEZ7-b6Zf8yGyA_1e4wNj452FD_O/pub
- hxxps://docs.google[.]com/document/d/e/2PACX-1vTiMxxKYdtOy98JFAiBaNe1W-VVdRGcZOZurDYA1jhcat-mcbcA8Uw7m_v4BvJ-H3o9m7ML_TtRNPQP/pub

- hxxps://docs.google[.]com/document/d/e/2PACX-1vShuUk4DvIVthVxqc8UIUgZ7hOQzBQ1Dop8sXP73qBfS-JrlSrdIaZslExSyrr459kvaMmWbOAUkYii/pub
- hxxps://docs.google[.]com/document/d/e/2PACX-1vRQ8skYzE8fzy9FnmU06fNCSEBTGwdYCxE1_NyLjxTCG7uEhpFtmI_IWAtk1FFmuQyAReDSuUCdyCFs/pub
- hxxps://docs.google[.]com/document/d/e/2PACX-1vT_UMMUFR8J8IbN7rthTdttvciBU-17slZ2anuIq4A-8zT4xtF9ngzzyiEjlE8HSDZQ5tWu_w6HBFMf/pub
- hxxps://docs.google[.]com/document/d/e/2PACX-1vQgYON0ZqbynIRhybfOxzkN8jUzIa-DkiYp-KOTxKzhFaDt2miDJBp14XJw8lMPHtU1tkIXDcwquIr-/pub

URLs that returned script to create the Word docs:

- hxxp://savortrading[.]com/toweringly.php
- hxxps://libifield.co[.]za/figs.php
- hxxps://expertcircles[.]co[.]uk/assotiation.php
- hxxps://libifield[.]co[.]za/oilcan.php
- hxxp://3.133.244[.]105/irs.php

8 examples of downloaded Word docs (read: SHA256 hash - file name):

- 080bade36015dd79925bab0975ac0f30f18424bdd1e7836d63c2dee350bdbd69 - 0112_528419802.doc
- 2ac3b573d70c40c5c0fafe4e5914c723f2322a1c9cd76d232447654604ff8b76 - 0112_929792452.doc
- 385425e94ed8ac21d7888550743b7a2b89afbeb51341713adb6da89cd63b5aff - 0112_203089882.doc
- 7b013a271432cc9dea449ea9fcf727ed3caf7ce4cc6a9ba014b3dd880b5668dd - 0112_1079750132.doc
- 8bcf45c2de07f322b8efb959e3cef38fb9983fdb8b932c527321fd3db5e444c8 - 0112_1005636132.doc
- cab2a47456a2c51504a79ff24116a4db3800b099ec50d0ebea20c2c77739276d - 0112_722674781.doc
- d6755718c70e20345c85d18c5411b67c99da5b2f8740d63221038c1d35ccc0b8 - 0112_153569242.doc
- ed3fa9e193f75e97c02c48f5c7377ff7a76b827082fdbfb9d6803e1f7bd633ca - 0112_114086062.doc
- Note: Each of the above files is 753,152 bytes in size.

SHA256 for 8 examples of DLL files dropped by the Word docs:

- 00b2312dd63960434d09962ad3e3e7203374421b687658bd3c02f194b172bfe3
- 0941090d3eb785dbf88fbfafffad34c4ab42877b279129616a455347883e5738
- 43690eaf47245d69f4bda877c562852e4a9715955c2160345cb6cc84b18ca907
- 82c9bc479ea92c1900422666792877e00256996ce2f931984115598ed2c26f23
- 878319795a84ebfe5122d6fc21d27b4b94b3c28ad66679f841dec28ccc05e801
- c3e06473c4c3d801c962e6c90ccbcab3d532fb5a6649077ea09cd989edf45eaf
- cdcd5ee8b80d3a3863e0c55d4af5384522144011b071d00c9c71ae009305f130
- edabef17fce2aaca61dbd17a57baf780cd82a2b0189b0cf3c5a7a3ca07e94a44
- Note 1: Each of the above file is 570,368 bytes in size.
- Note 2: Each file was saved at C:\Users*[username]*\AppData\Roaming\Microsoft\Templates\W0rd.dll

Traffic to retrieve the Word doc:

- port 443 - ***docs.google.com*** - HTTPS traffic
- 104.31.80[.]93 port 80 - ***savortrading[.]com*** - GET /sacrifice.php

Hancitor post-infection traffic:

- port 80 - ***api.ipify.org*** - GET /
- 185.87.194[.]148 port 80 - ***fruciand[.]com*** - POST /8/forum.php

Binaries used to infect host with Cobalt Strike:

- 47.254.175[.]0 port 80 - ***steroidi[.]pro*** - GET /2112.bin
- 47.254.175[.]0 port 80 - ***steroidi[.]pro*** - GET /2112s.bin

Cobalt Strike Post-infection traffic:

- 162.223.31[.]160 port 1080 - ***162.223.31[.]160:1080*** - GET /GvSL
- 162.223.31[.]160 port 1080 - ***162.223.31[.]160:1080*** - GET /visit.js
- 162.223.31[.]160 port 443 - HTTPS traffic

Final words

Hancitor has been active and evolving for years now, and it remains a notable presence in our current threat landscape. This diary reviewed a recent infection on a vulnerable Windows host from malspam sent on Tuesday 2021-01-12.

Decent spam filters and best security practices should help most people avoid Hancitor infections. Default security settings in Windows 10 and Microsoft Office 2019 should prevent these these infections from happening. However, it's a "cat-and-mouse" game, with malware developers developing new ways to circumvent security measures, while vendors update their software/applications/endpoint protection to address these new developments. And malware distribution through email is apparently cheap enough to remain profitable for the criminals who use it.

A pcap of the infection traffic, some emails, and malware associated with today's diary can be found here.

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