Wireshark Tutorial: Examining Traffic from Hancitor Infections

unit42.paloaltonetworks.com/wireshark-tutorial-hancitor-followup-malware/

Brad Duncan

April 7, 2021

By Brad Duncan

April 7, 2021 at 6:00 AM

Category: Tutorial, Unit 42

Tags: <u>Cobalt Strike</u>, <u>Ficker Stealer</u>, <u>hancitor</u>, <u>NetSupportManager</u>, <u>pcap</u>, <u>Send-Safe</u>, <u>Wireshark</u>, <u>Wireshark Tutorial</u>

traffic-for-wireshark-column-setu	up.pcap				
File Edit View Go Captu	ire Analyze Stat	tistics Telephony Wireles	ss Tools Help		
	۹ 👄 🔿 🧃	F 🕹 📃 🗏 Q, Q, Q			
http.request or ssl.handshake.type	e == 1			Expression	+
Time Dst	t Port	Host	Server Name	Info	^
2018-08-03 19:06:20 19	2.0.79.32 80	college.usatoday.com		GET /2017/03/01/	
2018-08-03 19:06:20 19:	2.0.78.19 443		r-login.wordpress.com	Client Hello	
2018-08-03 19:06:20 19	2.0.78.19 443		r-login.wordpress.com	Client Hello	
2018-08-03 19:06:20 19	2.0.77.32 443		s2.wp.com	Client Hello	
2018-08-03 19:06:20 1	2.0.77 32 443	гор.	s2. p.com	Client Hello	
2018-08-03 19:06:20 1	2.0.77 31 443	I U N	s2 p.com	Client Hello	
2018-08-03 19:06:20 19	2.0.77.32 443		s2.wp.com	Client Hello	
2018-08-03 19:06:20 19	2.0.77.32 443		s1.wp.com	Client Hello	
2018-08-03 19:06:20 19	2.0.77.32 443		s1.wp.com	Client Hello	
2018-08-03 19:06:20 19	2.0.77.32 443		s1.wp.com	Client Hello	
2018-08-03 19:06:20 21	6.58.218 443		fonts.googleapis.com	Client Hello	
2018-08-03 19:06:20 21	6.58.218 443		<pre>fonts.googleapis.com</pre>	Client Hello	
2018-08-03 19:06:20 52	.84.125 80	d15krst4gi8g86.clou		GET /css/usatoda	
2018-08-03 19:06:20 52	.84.125 80	d15krst4gi8g86.clou		GET /js/script.j	
2018-08-03 10.06.70 57	8/ 175 80	d15knet/ai8a86 clou		GET /ccc/ucatoda	Ť
🔵 🌌 traffic-for-wireshark-colum	nn-setup.pcap		Packets: 4448 · Displayed: 1	23 (2.8%) Profile: Defa	ult

This post is also available in: <u>日本語 (Japanese)</u>

Executive Summary

Also known as Chanitor, <u>Hancitor</u> is malware used by a threat actor designated as MAN1, Moskalvzapoe or TA511. Hancitor establishes initial access on a vulnerable Windows host and sends additional malware. This Wireshark tutorial reviews activity from recent Hancitor infections. It provides tips on identifying Hancitor and its followup malware. In this tutorial, we cover examples of Hancitor with <u>Cobalt Strike</u>, <u>Ficker Stealer</u>, <u>NetSupport Manager RAT</u>, a <u>network ping tool</u> and <u>Send-Safe</u> spambot malware.

This tutorial is designed for security professionals who investigate suspicious network activity and review packet captures (pcaps). Familiarity with <u>Wireshark</u> is necessary to understand this tutorial, which focuses on Wireshark version 3.x.

Note: These instructions assume you have customized Wireshark as described in <u>our</u> <u>previous Wireshark tutorial about customizing the column display</u>.

You will need to access a GitHub repository with ZIP archives containing the pcaps used for this tutorial.

Warning: The pcaps for this tutorial contain Windows-based malware. There is a risk of infection if using a Windows computer. If possible, we recommend you review these pcaps in a non-Windows environment such as BSD, Linux or macOS.

Chain of Events for a Hancitor Infection

Hancitor is distributed through email. These emails each contain an HTTPS link for a Google Drive URL through docs.google.com. These Google Drive pages link to a different domain that returns a malicious Word document. Enabling macros on the Word document starts the infection by dropping a DLL.

The infected host first generates Hancitor command and control (C2) traffic. Then we see URLs for followup malware such as Ficker Stealer. If the infected host is part of an Active Directory (AD) environment, Hancitor will also send Cobalt Strike. Cobalt Strike provides another access channel for further malicious files such as a network ping tool or NetSupport Manager RAT-based malware. In some cases, we also see Send-Safe spambot malware, which turns the infected Windows host into a spambot pushing more Hancitor emails.



Figure 1. Chain of events for recent Hancitor infections.

Knowing this chain of events will better help you understand traffic generated during a Hancitor infection. More details can be found in our blog about <u>recent Hancitor infections</u>.

Pcaps of Hancitor Infection Activity

Four password-protected ZIP archives containing five pcaps of recent Hancitor activity are available at <u>this GitHub repository</u>. From the GitHub page, click on each of the ZIP archive entries and download them, as shown in Figures 2 and 3.

	tHub - pan-unit42/ × +			
Why GitHub? Yeam Enterprise Explore Marketplace Pricing Y pan-unit42 / wireshark-tutorial-Hancitor-traffic pan-unit42 / wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02.17-Hancitor-infection.pcap.zip main pan-unit42 / wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02.17-Hancitor-infection.pcap.zip main pandedmaan Add lifes via upload is tample-2.3021 02:17-teacoust.eff is tample-1.3021	→ C ² ¹ / ₀ → C ² ¹ / ₂ ¹ / ₂	github.com/pan-unit42/wireshark-tutorial-H	ancitor 🚥 🗵 😭 🧟 Search	
pan-unik2/ wireshark-tutorial-Hancitor-traffic code bases 1 Pul requests Actions Projects Security Kingins Pinal P 1 tranch © tags Code 1 Security Kingins Pinal P 1 tranch © tags Code 1 2021 02 17 Hancitor-Lead 100 4 days app Example - 2021 02 17 Hancitor-Lead 4 days app Example - 2021 02 17 Hancitor-Lead 4 days app Example - 2021 02 17 Hancitor-Lead 4 days app Example - 2021 02 02 Hancitor-Lead 4 days app Example - 2021 02 17 Hancitor-Lead 4 days app Example - 2021 02 1-02 Hancitor-Lead 4 days app Example - 2021 02 Hanc) Why GitHub?	e Explore \vee Marketplace Pricing \vee	Search	✓ Sign in Sign
Code Issue I Put requests Actions Projects Security Insights P main P1 branch 0 tags Code About Notadiuncan Add Hes via upload 4 days ago 4 days ago Code Code Code Add Hes via upload 4 days ago Code Code Code Code Code ReADME_md Update: Update: Code Code Code Issues I Put requests Actions Projects Security I Instruction: Instruction: Add Hes via upload 4 days ago Code Code Security Viation: Code Security Viation: Code I Security Viation: Code Security Viation: Viation: Code Security Viation: Code Security Viation: Viation: Code Security Viation: Security Viation: Viation: Viation: Code Security Viation: <	pan-unit42/ wireshark-tutoria	al-Hancitor-traffic	Ŭ.	Notifications 🖧 Star 0
Imain Imain	<> Code () Issues % Pull reque	ests () Actions (1) Projects () Security	l∼ Insights	
brad-duncan Add files via upload 4746992 brad-duncan Add files via upload 4 days ago c sample-1:2021-02-17-Hancitor-infe Add files via upload 4 days ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 4 days ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 4 days ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 17 minutes ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 17 minutes ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 17 minutes ago c sample-2 2021-02-10-E5-Hancitor-infe Add files via upload 17 minutes ago c sample-2 2021-02-10-E5-Hancitor-infection.pcap.zip No releases published ReADME.md Vigitub.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip Iter 2. GitHub repository with links to ZIP archives used for this tutorial. eshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip Iter 2. GitHub repository with links to ZIP archives used for this tutorial. eshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip Iter 2 Iter	🐉 main 👻 💱 1 branch 🔿 0 tags		Go to file	About
	brad-duncan Add files via upload	47465	17 minutes ago 🔞 4 commits	No description, website, or topics provided.
	Example-1-2021-02-17-Hancitor-inte	Add files via upload	4 days ago	Readme
Example -3-2021-01-25-Handtor-infe Add files via upload 4 days ag Example -4-2021-02-02-Handtor-infe Add files via upload 17 minutes agg README.md 4 days agg README.md Update README.md 4 days agg No packages published Vigitublo.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip Inte 2. GitHub repository with links to ZIP archives used for this tutorial. eshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main - pan-unit42/wireshark-tutorial-Hancitor-reshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main - pan-unit42/wireshark-tutorial-Hancitor-reshark-tutorial-Hancitor-infection.pcap.zip at main - pan-unit42/wireshark-tutorial-Hancitor-infection.pcap.zip at main - pan-unit42/wireshark-tutorial-Hancitor-traffic Why GitHub? < Team Enterprise Explore < Marketplace Pricing < Search S	Example-2-2021-02-10-Hancitor-infe	Add files via upload	4 days ago	
brandped-42021-02-02-Hancitor-infe Add files via upload	Example-3-2021-01-25-Hancitor-infe	Add files via upload	4 days ago	Releases
README.md Update README.md Packages ReADME.md //github.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip rre 2. GitHub repository with links to ZIP archives used for this tutorial. eshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-reshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-reshark-tutorial-Hancitor · m Why GitHub? Team Enterprise Explore Marketplace Pricing Search Search Im C Packages pan-unit42/wireshark-tutorial-Hancitor-traffic Star Sign in S pan-unit42/wireshark-tutorial-Hancitor-traffic Search Im C pan-unit42/wireshark-tutorial-Hancitor-traffic Socode Issues I1 Pull requests Actions Projects Security Insights Intertorial toestee 35 minutes apo Other Intertorial toestee 35 minutes apo Other Intertorial toestee 35 minutes apo Other Intertorial toestee 35 minutes apo	Example-4-2021-02-02-Hancitor-infe	Add files via upload	17 minutes ago	No releases published
README.md No packages published //github.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip ITE 2. GitHub repository with links to ZIP archives used for this tutorial. teshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-traffic Why GitHub? V Team Enterprise Explore V Marketplace Pricing V Search V Search V Sign in Search V Sign in Search V Sear	README.md	Update README.md	4 days ago	Packanes
//github.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip tre 2. GitHub repository with links to ZIP archives used for this tutorial. teshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-treshark-tutorial-Hancitor-infection.pcap.zip at main · pan-unit42/wireshark-tutorial-Hancitor-treshark-tutorial-Hancitor why GitHub? Team Enterprise Explore Marketplace Pricing Search Pan-unit42 / wireshark-tutorial-Hancitor-traffic > Code Issues 1 Pull requests Actions Projects Security wireshark-tutorial-Hancitor-traffic / Example-1-2021-02-17-Hancitor-infection.pcap.zip Co to file train train train	DEADME and			No packages published
//github.com/pan-unit42/wireshark-tutorial-Hancitor-traffic/blob/main/Example-1-2021-02-17-Hancitor-infection.pcap.zip Ire 2. GitHub repository with links to ZIP archives used for this tutorial. reshark-tutorial-Hancitor-traffic/Example-1-2021-02-17-Hancitor-infection.pcap.zip at main - pan-unit42/wireshark-tutorial-Hancitor-reshark-tutorial-Hancitor - m S A Search IN C Image: Search of the state of t	README.MO			no puonagoo puononou
C Image: Antipost//github.com/pan-unit42/wireshark-tutorial-Hancitor Why GitHub? Team Enterprise Explore Marketplace Pricing Search Image: Search Image: Price Pricing Search Image: Price Price Pricing Search Image: Price Pr	//github.com/pan-unit42/wiresha	rk-tutorial-Hancitor-traffic/blob/main/Exampl tory with links to ZIP archiv	e-1-2021-02-17-Hancitor-infect	ion.pcap.zip torial.
Why GitHub? < Team Enterprise Explore < Marketplace Pricing Search pan-unit42 / wireshark-tutorial-Hancitor-traffic Projects Security Projects Projects Projects Projects Projects Projects Projects Projects Projects <	i//github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-H × +	rk-tutorial-Hancitor-traffic/blob/main/Exampl tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection.	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main - pan-unit42	ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tra
pan-unit42 / wireshark-tutorial-Hancitor-traffic	In EADWIELING I//github.com/pan-unit42/wiresha Ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-H × + → C ^a ŵ ♥ ▲ Nttps://g	rk-tutorial-Hancitor-traffic/blob/main/Exampl tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main · pan-unit42 ancitor ··· ♡ ☆ (♀ Search	ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tr;
(x) Code ① Issues ① Pull requests ④ Actions Projects ① Security M Insights P' main ~ wireshark-tutorial-Hancitor-traffic / Example-1-2021-02-17-Hancitor-infection.pcap.zip Go to file (a) brad-duncan Add files via upload Latest commit be854ee 35 minutes ago (a) Inference Download Upper rew	reading ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-H × + → C ŵ ♡ ● https://g Why GitHub?∨ Team Enterprise	e Explore ~ Marketplace Pricing ~	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main · pan-unit42 ancitor ···· $\varsimes rightarrow right$	ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tra III\ III (Sign in Sigr
	ILEADMELING ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-H × + → C ŵ © â https://g Why GitHub? ✓ Team Enterprise pan-unit42 / wireshark-tutoria	ark-tutorial-Hancitor-traffic/blob/main/Exampl tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing al-Hancitor-traffic	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main - pan-unit42 ancitor 영 쇼) (역 Search Search	ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tr; III\ □ (Sign in Sign kotifications ☆ Star 0 ♀ Fork (
brad-duncan Add files via upload Latest commit be854ee 35 minutes ago Three Add files via upload Latest commit be854ee 35 minutes ago Three Add files via upload Latest commit be854ee 35 minutes ago Devended Dev	HEADWELTER ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-H × + → C û ① î https://g Why GitHub? ✓ Team Enterprise pan-unit42 / wireshark-tutoria <> Code ① Issues î Pull reque	ark-tutorial-Hancitor-traffic/blob/main/Example tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing ~ al-Hancitor-traffic ests O Actions Projects O Security	e-1-2021-02-17-Hancitor-infect res used for this tu pcap.zip at main · pan-unit42 ancitor ···· © 🏠 (Search Search	Ion.pcap.zip torial. //wireshark-tutorial-Hancitor-tr; III\ Sign in Sign Iotifications
At 1 contributor Upper raw	HEADWEIND ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic ireshark-tutorial-Hancitor-traffic ireshark-tutorial-Hancitor-traffic > C	ark-tutorial-Hancitor-traffic/blob/main/Exampl tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing ~ al-Hancitor-traffic ests O Actions Projects O Security actior-traffic / Example-1-2021-02-17-Hancitor-infe	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main · pan-unit42 ancitor ···· © ☆) (Search Search	Ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tr; II\ □ (Sign in Sign kolifications ☆ Star 0 ♀ Fork (Go to file ····
5.31 MB Download	HEADWEIND ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffic reshark-tutorial-H × + → C* ① ① ● https://g Why GitHub? ∨ Team Enterpris pan-unit42 / wireshark-tutorial (> Code ① Issues ① Pull reque * main → wireshark-tutorial-Han (> brad-duncan Add files via upload)	ark-tutorial-Hancitor-traffic/blob/main/Exampletory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing al-Hancitor-traffic ests O Actions Projects O Security	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main - pan-unit42 ancitor ত 🏠 (Search Search Latest	ion.pcap.zip torial. //wireshark-tutorial-Hancitor-tr; III\
Vipur raw	HEADWEIND ://github.com/pan-unit42/wiresha ure 2. GitHub reposi reshark-tutorial-Hancitor-traffin ireshark-tutorial-H × + → C ⁴	ark-tutorial-Hancitor-traffic/blob/main/Exampletory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing al-Hancitor-traffic asts O Actions Projects O Security acitor-traffic / Example-1-2021-02-17-Hancitor-infe	e-1-2021-02-17-Hancitor-infect es used for this tu pcap.zip at main · pan-unit42 ancitor ···· 🖾 🏠 (Search Search	ion.pcap.zip torial. //wireshark-tutorial-Hancitor-tr: III\ □ □ Sign in Sign Iotifications ☆ Star 0 ♀ Fork □ Go to file ····
(Sorry about that, but we can't show files that are this big right now.)	HEADMELTING ://github.com/pan-unit42/wiresha JITE 2. GitHub reposi reshark-tutorial-Hancitor-traffilireshark-tutorial-H × + → C	ark-tutorial-Hancitor-traffic/blob/main/Exampletory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing al-Hancitor-traffic asts O Actions Projects O Security acitor-traffic / Example-1-2021-02-17-Hancitor-infe	e-1-2021-02-17-Hancitor-infect res used for this tu pcap.zip at main · pan-unit42 ancitor ···· © 🏠 (Search Search	ion.pcap.zip torial. //wireshark-tutorial-Hancitor-tr: III\ □ □ Sign in Sign Notifications ☆ Star 0 ♀ Fork Go to file ···· commit be854ee 35 minutes ago ♥ Hirtory
	ITEADME.ma ://github.com/pan-unit42/wiresha Jre 2. GitHub reposi reshark-tutorial-Hancitor-traffi reshark-tutorial-H × + → C	Ark-tutorial-Hancitor-traffic/blob/main/Example tory with links to ZIP archiv c/Example-1-2021-02-17-Hancitor-infection. github.com/pan-unit42/wireshark-tutorial-H e Explore Marketplace Pricing al-Hancitor-traffic asts O Actions Projects O Security acitor-traffic / Example-1-2021-02-17-Hancitor-infection- security converses New raw (Sorry about that, but we can't show files the security of the security show files the secur	e-1-2021-02-17-Hancitor-infect res used for this tu pcap.zip at main · pan-unit42 ancitor ···· © A @ Search Search (! !nsights ction.pcap.zip Latest a at are this big right now.)	ion.pcap.zip torial. /wireshark-tutorial-Hancitor-tr: III\ □ □ Sign in Sign Notifications ☆ Star 0 ♀ Fork Go to file ···· commit b0854ee 35 minutes ago ♥ Hirtory Download ℃

Figure 3. Downloading the first ZIP archive for this tutorial.

Use *infected* as the password to extract pcaps from these four ZIP archives. This should give you the following five pcap files:

- Example-1-2021-02-17-Hancitor-infection.pcap
- Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap
- Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap
- Example-3-2021-01-25-Hancitor-infection.pcap

• Example-4-2021-02-02-Hancitor-infection.pcap

Example 1: Hancitor with Ficker Stealer and Cobalt Strike

Open *Example-1-2021-02-17-Hancitor-infection.pcap* in Wireshark and use a basic web filter as described in our previous <u>tutorial about Wireshark filters</u>. The basic filter for Wireshark 3.x is:

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

If you've set up Wireshark according to our initial <u>tutorial about customizing Wireshark</u> <u>displays</u>, your display should look similar to Figure 4.

-	Example-1-2021-02-17-Hancitor-infection.pcap										
File	e <u>E</u> dit <u>V</u>	/iew <u>G</u>	o <u>C</u> apture	e <u>A</u> nalyze	Statistics	Telepho	ony <u>W</u> ireless <u>T</u> ools <u>H</u> elp				
1	/ / ()										
. (http.requ	lest or t	tls.handsha	ake.type eq	1) and !(ssd	p)			×		•
Tim	e		-	Dst		port	Host	Info			^
	2021-0	2-17	16:14	20.54.2	24.231	443	<pre>geo.prod.do.dsp.mp.microsoft.com</pre>	Client	Hello		
	2021-0	2-17	16:14	104.95.	91.76	443	kv601.prod.do.dsp.mp.microsoft.com	Client	Hello		
	2021-0	2-17	16:14	104.95.	91.76	443	cp601.prod.do.dsp.mp.microsoft.com	Client	Hello		
	2021-0	2-17	16:14	52.114.	77.34	443	<pre>self.events.data.microsoft.com</pre>	Client	Hello		
	2021-0	2-17	16:14	52.242.	211.89	443	client.wns.windows.com	Client	Hello		
	2021-0	2-17	16:14	52.114.	132.22	443	v20.events.data.microsoft.com	Client	Hello		
	2021-0	2-17	16:15	204.79.	197.200	443	www.bing.com	Client	Hello		
	2021-0	2-17	16:15	204.79.	197.200	443	www.bing.com	Client	Hello		
	2021-0	2-17	16:15	104.95.	32.115	443	cdn.onenote.net	Client	Hello		
	2021-0	2-17	16:15	204.79.	197.219	443	edge.microsoft.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.12.78	443	docs.google.com	Client	Hello		
	2021-0	2-17	16:15	20.190.	154.137	443	login.live.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.12.78	443	docs.google.com	Client	Hello		
	2021-0	2-17	16:15	204.79.	197.219	443	edge.microsoft.com	Client	Hello		
	2021-0	2-17	16:15	52.232.	226.150	443	edge.activity.windows.com	Client	Hello		
	2021-0	2-17	16:15	52.232.	226.150	443	edge.activity.windows.com	Client	Hello		
	2021-0	2-17	16:15	13.107.	42.23	443	config.edge.skype.com	Client	Hello		
	2021-0	2-17	16:15	13.107.	42.23	443	config.edge.skype.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.6.138	443	fonts.googleapis.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.6.138	443	fonts.googleapis.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.6.138	443	fonts.googleapis.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.1.225	443	lh6.googleusercontent.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.1.225	443	lh6.googleusercontent.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.9.163	443	fonts.gstatic.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.9.163	443	fonts.gstatic.com	Client	Hello		
	2021-0	2-17	16:15	172.217	7.9.163	443	fonts.gstatic.com	Client	Hello		
	2021-0	2-17	16:15	204.79.	197.200	443	www.bing.com	Client	Hello		Ŧ
4)	•	

Figure 4. Our first pcap in this tutorial filtered in Wireshark.

The pcap comes from an AD environment with the following characteristics:

- LAN segment range: 10.2.17.0/24
- Domain: bean-genie.com
- Domain controller: 10.2.17.2 Bean-Genie-DC
- LAN segment gateway: 10.2.17.1
- LAN segment broadcast address: 10.2.17.255
- IP address of the infected Windows host: 10.2.17.101
- Host name of the infected Windows host: DESKTOP-GBW8K4N

• User account name on the infected Windows host: frankie.muntz

Emails pushing Hancitor use HTTPS links to docs.google.com. In our first pcap, the 13th frame listed in the column display uses this domain name. Below, Figure 5 highlights docs.google.com in our Wireshark column display.

-	 Example-1-2021-02-17-Hancitor-infection.pcap + × 									
Fil	e <u>E</u> dit <u>V</u> iew	<u>Go</u> <u>C</u> aptur	e <u>A</u> nalyze <u>S</u> tatistics	Telepho	ony <u>W</u> ireless <u>T</u> ools <u>H</u> elp					
		 _								
	http.request o	r tls.handsha	ake.type eq 1) and !(ssd	p)			E		•	
Tim	ie	*	Dst	port	Host	Info			^	
	2021-02-17	7 16:14	20.54.24.231	443	<pre>geo.prod.do.dsp.mp.microsoft.com</pre>	Client	Hello			
	2021-02-17	16:14	104.95.91.76	443	kv601.prod.do.dsp.mp.microsoft.com	Client	Hello			
1	2021-02-17	/ 16:14	104.95.91.76	443	cp601.prod.do.dsp.mp.microsoft.com	Client	Hello			
	2021-02-17	16:14	52.114.77.34	443	self.events.data.microsoft.com	Client	Hello			
	2021-02-17	16:14	52.242.211.89	443	client.wns.windows.com	Client	Hello			
	2021-02-17	16:14	52.114.132.22	443	v20.events.data.microsoft.com	Client	Hello			
	2021-02-17	16:15	204.79.197.200	443	www.bing.com	Client	Hello			
	2021-02-17	/ 16:15	204.79.197.200	443	www.bing.com	Client	Hello			
	2021-02-17	/ 16:15	104.95.32.115	443	cdn.onenote.net	Client	Hello			
	2021-02-17	16:15	204.79.197.219	443	edge.microsoft.com	Client	Hello			
	2021-02-17	16:15	172.217.12.78	443	docs.google.com	Client	Hello			
	2021-02-17	16:15	20,190,154,137	443	login.live.com	Client	Hello			
	2021-02-17	/ 16:15	172.217.12.78	443	docs.google.com	Client	Hello			
	2021-02-17	16:15	204.79.197.219	443	edge.microsoft.com	Client	Hello			
	2021-02-17	16:15	52.232.226.150	443	edge.activity.windows.com	Client	Hello			
	2021-02-17	16:15	52.232.226.150	443	edge.activity.windows.com	Client	Hello			
	2021-02-17	16:15	13.107.42.23	443	config.edge.skype.com	Client	Hello			
	2021-02-17	16:15	13.107.42.23	443	config.edge.skype.com	Client	Hello			
	2021-02-17	16:15	172.217.6.138	443	fonts.googleapis.com	Client	Hello			
	2021-02-17	16:15	172.217.6.138	443	fonts.googleapis.com	Client	Hello			
	2021-02-17	16:15	172.217.6.138	443	fonts.googleapis.com	Client	Hello			
	2021-02-17	16:15	172.217.1.225	443	lh6.googleusercontent.com	Client	Hello			
	2021-02-17	16:15	172.217.1.225	443	lh6.googleusercontent.com	Client	Hello			
	2021-02-17	16:15	172.217.9.163	443	fonts.gstatic.com	Client	Hello			
	2021-02-17	/ 16:15	172.217.9.163	443	fonts.gstatic.com	Client	Hello			
	2021-02-17	/ 16:15	172.217.9.163	443	fonts.gstatic.com	Client	Hello			
	2021-02-17	/ 16:15	204.79.197.200	443	www.bing.com	Client	Hello		Ŧ	
4								•		

Figure 5. HTTPS traffic to docs.google.com from our first pcap.

Of note, docs.google.com is a legitimate domain, and it is not inherently malicious. However, Google Drive is frequently abused by the criminals behind Hancitor. Below, Figure 6 shows a web page from one of these URLs created by MAN1/Moskalvzapoe/TA511 for Hancitor.



Figure 6. Example of Google Drive URL hosting a page for Hancitor.

Above in Figure 6, the link in "Click here to download the document" leads to a page that provides the malicious Word document. URLs for these pages end with .php. In many cases, these URLs also use HTTPS. Fortunately, in this tutorial, all four examples have unencrypted HTTP as the URL for the Word document. That makes them easy to find in our pcaps.

Still using your basic web filter, scroll down until you see two HTTP GET requests to the same domain that end with .php. Below, Figure 7 shows these two HTTP GET requests in the Wireshark column display. They are both for:

somdeeppalace[.]com - GET /slickness.php

Example-1-2021-02-17-Hancitor-infection.pcap - + ×								
<u>File Edit View Go Capture</u>	<u>Analyze</u> <u>S</u> tatistics	Teleph	ony <u>W</u> ireless <u>T</u> ools <u>H</u> elp					
$ \blacksquare \ \boxtimes \ \boxdot \ \blacksquare \ \boxtimes \ \boxtimes$								
(http.request or tls.handshake.type eq 1) and !(ssdp)								
Time	Dst	port	Host	Info				
2021-02-17 16:15	52.109.8.21	443	nexusrules.officeapps	Client Hello				
2021-02-17 16:15	23.38.181.191	443	<pre>storeedgefd.dsx.mp.mic</pre>	Client Hello				
2021-02-17 16:15	23.38.181.191	443	<pre>storeedgefd.dsx.mp.mic</pre>	Client Hello				
2021-02-17 16:	159.89.165.126	80	somdeeppalace.com	GET /slickness.php H				
2021-02-17 16:15	23.38.181.191	443	<pre>storeedgefd.dsx.mp.mic</pre>	Client Hello				
2021-02-17 16:	159.89.165.126	80	somdeeppalace.com	GET /slickness.php H				
2021-02-17 16:15	23.38.181.191	443	<pre>storeedgefd.dsx.mp.mic</pre>	Client Hello				
2021-02-17 16:15	51.143.53.152	443	continuum.dds.microsof	Client Hello				
2021-02-17 16:15	34.238.227.240	443	notify.adobe.io	Client Hello				
2021-02-17 16:15	52.167.253.237	443	activity.windows.com	Client Hello				
2021-02-17 16:15	204.79.197.200	443	www.bing.com	Client Hello				
2021-02-17 16:15	52.242.211.89	443	client.wns.windows.com	Client Hello				
2021-02-17 16:16	204.79.197.219	443	edge.microsoft.com	Client Hello				
2021-02-17 16:16	204.79.197.219	443	edge.microsoft.com	Client Hello				
2021-02-17 16:16	159.89.165.126	80	somdeeppalace.com	GET /favicon.ico HT				
2021-02-17 16:16	162.241.124.88	443	webinfoplus.xnmndtbn	Client Hello				
2021-02-17 16:16	162.241.124.88	443	webinfoplus.xnmndtbn	Client Hello				
<u>2021_02_17_16+16</u> ∢	160 0/1 10/ 88	113	Webinfonlus ynmodthn	Client Hello				

Figure 7. Two URLs ending in .php that deliver a malicious Word document for Hancitor. You could also use the following Wireshark filter to more quickly find these two URLs:

http.request.method eq GET and http.request.uri contains .php

Below, Figure 8 shows the results of this filter.

Example-1-2021-02-17-Hancitor-infection.pcap- + ×									
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>									
a 🔳 a 💿 🚞 🖺 🖄 💁 🗢 🌩 🔷 ⊨ 🚔 🧮 🚍 🚍 🖻 🗉 🤉 🏦									
http.request.method eq GE	T and http.request.uri c	ontain	is .php			× 🗆 🔹			
Time	Dst	port	Host	Info					
2021-02-17 16:15	159.89.165.126	80	somdeeppalace.com	GET	/slickness.php	HTTP/1.1			
2021-02-17 16:15	159.89.165.126	80	somdeeppalace.com	GET	/slickness.php	HTTP/1.1			
4						► I			

Figure 8. Filtering specifically for the two URLs.

Right-click on either HTTP GET request for slickness.php in your column display and follow the HTTP stream, as shown below in Figure 9.

-	• Example-1-2021-02-17-Hancitor-infection.pcap - + ×									
File	Edit View Go Capture Analy	ze <u>S</u> tatistics	Teleph	non <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp					
ht	http.request.method eq GET and http.request.uri contains .php									
Time	Dst		port	Host		Info				
+ 2	Mark/Unmark Packet	Ctrl+M	80 80	somdeeppal	ace.com	GET	/slickness.php	HTTP/1.1		
	Ignore/Unignore Packet	Ctrl+D		oomdooppui		0L1	, orrest the solution of the			
	Set/Unset Time Reference	Ctrl+T								
	Time Shift	Ctrl+Shift+T								
	Packet Comment	Ctrl+Alt+C								
	Edit Resolved Name									
	Apply as Filter)								
	Prepare as Filter)								
	Conversation Filter	1								
	Colorize Conversation	,								
	SCTP									
	Follow		L I	CP Stream	′_rl≁ Shi	ft+T				
•	Сору		- L	JDP Stream	4t+Shi	ft+U		•		
	Protocol Preferences	,		LS Stream	Alt+Shi	ft+S				
	Decode As		ŀ	HTTP Stream	Ctrl+Alt+Shi	ft+H				
	Show Packet in New <u>W</u> indow		- F	HTTP/2 Stream						
			(QUIC Stream						

Figure 9. Following HTTP stream for traffic to somdeeppalace[.]com.In the HTTP stream window, scroll down past the second set of HTTP request and response headers, then examine the HTML script after the initial <body> tag. You should find a large amount of base64 text shortly after a script function for saveAs. The beginning of this text is shown below in Figure 10.



Figure 10. HTTP stream showing saveAs function followed by base64 text.

Scroll down to the end of the HTTP stream. You should find a script that offers to save a file named 0217_2857682888090.doc created from the base64 text. This is the malicious Word document. After the closing </body> tag, additional script refreshes the web page to a different URL. See Figure 11 below for details.



Figure 11. Script showing file name for the malicious Word document and refreshing the browser to a different URL.

We can obtain a copy of this malicious Word document by exporting the web page from the pcap and opening it in a web browser. Since this is malware, we recommend you do this in a non-Windows environment or a controlled lab setting.

First, export the web page by using the following menu path, as shown below in Figure 12:

File --> Export Objects --> HTTP

•	Example-1-2021-02-17-Hancitor-infection.pcap - + ×								
<u>File</u> <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>Analyze</u> <u>Statistics</u>	Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp						
<u>O</u> pen	Ctrl+O			E					
Open <u>R</u> ecent	•					C • 4			
<u>M</u> erge		port	Dst	port	Info				
Import from Hex Dump		49756	23.38.181.191	443	49756 → 443	[ACK] S			
Close	Ctrl+W	443	10.2.17.101	49760	Application	Data			
Save	Ctrl+S	49760	34.238.227.240	443	49760 → 443	[ACK] S			
Save As		49760	34.230.227.240	443	$49700 \rightarrow 443$				
Save <u>A</u> s	Ctri+Sniit+S	443	10.2.17.101	49760	443 → 49760	[ACK] S			
File Set	•	49760	34.238.227.240	443	Application	Data			
Export Specified Packets		443	10.2.17.101	49760	443 → 49760	[ACK] S			
Export Packet Dissections	+	443	10.2.17.101	49760	443 → 49760	[ACK] s			
Export Dacket Puter	Ctrl+Chift+V	443	10.2.17.101	49768	New Session	Ticket,			
Export Packet <u>B</u> ytes	CULTERING	49769	204.79.197.219	443	$49769 \rightarrow 443$				
Export PDUs to File		80	10 101	49754	$80 \rightarrow 49754$				
Export TLS Session Keys		80	10 101	49754	80 → 49754	ACK1 Se			
Export Objects	۲.	DICOM	101	49754	80 → 49754	ACK Se			
Print	Ctrl+P	HTTP	2.17.101	49754	80 → 49754	[ACK] Se			
	Calif	IME	2.17.101	49754	80 → 49754				
Quit	Ctrl+Q	1111		10/5/		•			
		SMB							
		TFTP							

Figure 12. Using Wireshark to export HTTP objects from the pcap.

Find the second entry for slickness.php from somdeeppalace[.]com that is 534 kB, as shown below in Figure 13. Then save it as a web page using a file name ending with .htm or .html.

•	Wire	shark · Export · HTTP object list		- + ×
Packet	Hostname	Content Type	Size	Filename
2083	somdeeppalace.com	text/html	937 bytes	slickness.php
2856	somdeeppalace.com	text/html	534 kB	slickness.php
2887	somdeeppalace.com	text/html	279 bytes	favicon.ico
3766	api.ipify.org	text/plain	15 bytes	1
3935	thavelede.ru	application/x-www-form-ur	161 bytes	forum.php
3954	thavelede.ru	text/html	164 bytes	forum.php
4322	belcineloweek.ru	application/octet-stream	273 kB	6sufiuerfdvc.ex
4336	belcineloweek.ru	application/octet-stream	682 bytes	1602s.bin
4341	api.ipify.org	text/plain	15 bytes	?format=xml
4344	belcineloweek.ru	application/octet-stream	682 bytes	rs.r n
4476			5 bytes	
•				
Text Filter:				
Help		S	ave All ×	<u>Close</u> <u>Save</u>

Figure 13. Saving the second entry for sickness.php from the HTTP object list.

Open your saved HTML page in a web browser. You should see a pop-up menu including the option to save the malicious Word document. You should also see that your web browser has been refreshed to a URL ending with the string cashplus. See Figure 14 below for details.



Figure 14. Viewing your saved HTML page in a web browser.

This malicious Word document caused Hancitor C2 traffic that starts less than two minutes later in the pcap.

What does Hancitor C2 traffic look like?

Hancitor first causes an IP address check to api.ipify.org by the infected Windows host. Then it causes the C2 traffic. Hancitor C2 traffic consists of HTTP POST URLs that end with /8/forum.php.

Of note, traffic to api.ipify.org is an indicator, but it's not inherently malicious by itself.

Using your basic web filter, scroll down to find an IP address check to api.ipify.org followed by the first HTTP POST request for Hancitor C2 traffic to thavelede[.]ru. Below, Figure 15 shows where you can find these two items.

✓ Example-1-2021-02-17-Hancitor-infection.pcap - + ×									
<u>File Edit View Go Capture Analy</u>	ze <u>Statistics</u> Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp							
	X 🔶 🌩 🥱 🖗 🏓 📃								
(http.request or tls.handshake.type	eq 1) and !(ssdp)		X 🗆 🔹 🕈						
Time Dst	port	Host	Info						
2021-02-17 16:17:19 52.	.152.110.14 443	slscr.update.microsoft.com	Client Hello						
2021-02-17 16:17:19 52.	.114.75.78 443	v20.events.data.microsoft.com	Client Hello						
2021-02-17 16:17:20 54.	.225.129.141 80	api.ipify.org	GET / HTTP/1.1 IP address						
2021-02-17 16:17:24 52.	.185.211.133 443	settings-win.data.microsoft.com	Client Hello						
2021-02-17 16:17:25 20.	.190.154.136 443	login.live.com	Client Hello						
2021-02-17 16:17:29 52.	.185.211.133 443	settings-win.data.microsoft.com	Client Hello						
2021-02-17 16:17:31 13.	.107.246.19 443	pti.store.microsoft.com	Client Hello						
2021-02-17 16:17:32 192	2.36.41.14 80	thavelede.ru	POST /8/forum.php HTTP/1.1 (ap						
2021-02-17 16:17:34 47.	.254.174.221 80	belcineloweek.ru	GET /6sufluertdvc.exe HTTP/1.1						
2021-02-17 16:17:42 52.	.185.211.133 443	settings-win.data.microsoft.com	Client Hello						
2021-02-17 16:17:51 47.	.254.174.221 80	belcineloweek.ru	GET /1602s.bin HTTP/1.1						
2021-02-17 16:17:51 54.	.225.129.141 80	api.ipify.org	GET /?format=xml HTTP/1.1						
2021-02-17 16:17:51 47.	.254.174.221 80	belcineloweek.ru	GET /1602s.bin HTTP/1.1						
2021-02-17 16:17:52 192	2.99.250.2 443		Client Hello						
2021-02-17 16:17:54 192	2.99.250.2 443		Client Hello						
2021-02-17 16:18:07 192	2.99.250.2 443		Client Hello Hancitor C2						
2021-02-17 16:18:09 192	2.99.250.2 443		Client Hello						
2021-02-17 16:18:29 52.	.185.211.133 443	settings-win.data.microsoft.com	Client Hello						
2021-02-17 16:19:10 192	2.99.250.2 443		Client Hello						
2021-02-17 16:19:11 192	2.99.250.2 443		Client Hello						
4									

Figure 15. IP address check followed by Hancitor C2 noted in the Wireshark column display. Since November 2020, URLs for Hancitor C2 traffic have always ended with /8/forum.php. The easiest way to check for Hancitor-specific traffic in Wireshark is using the following filter:

http.request.uri contains "/8/forum.php" or http.host contains api.ipify.org

The above Wireshark filter should show you Hancitor's IP address check followed by HTTP POST requests for Hancitor C2 traffic, as shown below in Figure 16.

•	• Example-1-2021-02-17-Hancitor-infection.pcap - + ×								
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> tatistics Tele	phony	<u>Wireless</u> <u>T</u> ools <u>H</u> elp	0					
$\blacksquare \blacksquare \boxtimes \textcircled{0} \models \textcircled{1} \boxtimes \textcircled{0} \land \blacklozenge \blacklozenge \clubsuit \clubsuit \clubsuit \clubsuit \clubsuit \blacksquare \blacksquare \blacksquare \blacksquare$									
http.request.uri contains "/8/for http.request.uri contains "/8/for http://doi.org/10.00000000000000000000000000000000000	orum.php" or http.host	contair	is api.ipify.org	X 🗔 🗸 🔶					
Time	Dst	port	Host	Info					
2021-02-17 16:17:20	54.225.129.141	80	api.ipify.org	GET / HTTP/1.1					
2021-02-17 16:17:32	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:17:51	54.225.129.141	80	api.ipify.org	GET /?format=xml HTTP/1.1					
2021-02-17 16:19:52	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:21:53	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:23:55	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:25:57	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:27:58	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:30:20	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:32:22	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:34:43	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:36:44	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (
2021-02-17 16:38:44	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (
•				▶					

Figure 16. Filtering for Hancitor-specific traffic in Wireshark.

- api.ipify.org GET /
- thavelde[.]ru POST /8/forum.php
- zinsubtal[.]ru POST /8/forum.php

The results also include the following HTTP GET request generated by Ficker Stealer malware:

api.ipify.org - GET /?format=xml

We will cover Ficker Stealer traffic later. First, let us examine how Hancitor sends its followup malware.

Hancitor uses a specific domain to send Ficker Stealer and Cobalt Strike as followup malware. This domain changes each day Hancitor is active, but you should see three HTTP GET requests to the same domain for followup malware. One of the URLs ends with .exe, which is for Ficker Stealer. Two of the URLs end with .bin, which are for Cobalt Strike.

Use the following Wireshark filter to find URLs for Ficker Stealer and Cobalt Strike:

http.request.uri contains .exe or http.request.uri contains .bin

The results are shown below in Figure 17.

Example-1-2021-02-17-Hancitor-infection.pcap - + ×								
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp								
/ • • • • • • • • • • • • • • • • • • •								
http.request.uri contains .exe o	🖡 http.request.uri contains .exe or http.request.uri contains .bin							
Time	Dst	port	Host	Info				
2021-02-17 16:17:34	47.254.174.221	80	belcineloweek.ru	GET	/6sufiuerfdvc.exe	HTTP/1.1		
2021-02-17 16:17:51	47.254.174.221	80	belcineloweek.ru	GET	/1602s.bin HTTP/1	.1		
2021-02-17 16:17:51	47.254.174.221	80	belcineloweek.ru	GET	/1602s.bin HTTP/1	.1		
•						۱.		

Figure 17. Filtering for Hancitor sending Cobalt Strike and Ficker Stealer.

As shown above in Figure 17, filtering for followup malware from Hancitor should reveal the following traffic in our first pcap:

- belcineloweek[.]ru GET /6sufiuerfdvc.exe
- belcineloweek[.]ru GET /1602s.bin
- belcineloweek[.]ru GET /1602s.bin

The first HTTP GET request returned an EXE file for Ficker Stealer. The next two HTTP GET requests returned encoded data used to infect the victim with Cobalt Strike.

What does Ficker Stealer infection traffic look like?

Ficker Stealer is the same EXE file for several weeks at a time. Since 2021-01-20 until as recently as 2021-03-04, the SHA256 hash for Ficker Stealer has been:

94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1

The above EXE for Ficker Stealer causes an IP address check to api.ipifiy.org/?format=xml, which is not inherently malicious on its own. Ficker Stealer then generates a DNS query for sweyblidian[.]com and sends non-HTTP traffic over TCP port 80 to that domain. This traffic consists of data stolen from the infected Windows host.

To find the IP address used for sweyblidian[.]com, search for the associated DNS query using the following Wireshark filter:

dns.qry.name contains sweyblidian

The answer to this query is the IPv4 address 185.100.65[.]29, as shown below in Figure 18.



Figure 18. Finding the IP address used for sweyblidian[.]com.Find any TCP streams to that IP address using the following Wireshark filter:

ip.addr eq 185.100.65.29 and tcp.flags eq 0x0002

The results should reveal three TCP SYN segments for two TCP streams (one of the TCP SYN segments is a retransmission), as shown below in Figure 19.

-	Example-1-2021-02-17-Hancitor-infection.pcap							
<u>F</u> ile <u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture <u>A</u>	Analyze <u>S</u> tatistics	Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> el	р			
/ = / © = ^ \ < < + + < + = = = 0 = 1								
lip.addr eq 185.1	00.65.29 and to	cp.flags eq 0x0002					XE	•
Time		Src	port	Dst	port	Info		
2021-02-17	16:17:53	10.2.17.101	49807	185.100.65.29	80	49807 → 80	9 [SYN]	Seq=
2021-02-17	16:17:54	10.2.17.101	49807	185.100.65.29	80	[TCP Retra	ansmiss:	ion]
2021-02-17	16:20:24	10.2.17.101	49857	185.100.65.29	80	49857 → 80	9 [SYN]	Seq=
4								

Figure 19. TCP SYN segments for two TCP streams to the IP address for sweyblidian[.]com.Follow the TCP stream with port 49807 as the TCP source port. This should show approximately 1.16 MB of data. The majority of it appears encoded or otherwise obfuscated, as shown below in Figure 20.

Wireshark · Follow TCP Stream (tcp.stream eq 130) · Example-1-2021-02-17-Hancitor-infection.pcap	- + ×
<pre>.'%userprofile%\Desktop*.txt</pre>	·
.y}oshfcnckd\$ieg02:	
.;=>\$8><\$8:;\$883(.	
.183<ᢤn2'<9k9':8ko'9<12';829hh;li=80	
8UGepcffkULcxolerUZxelcfoyU;~o?{mis\$nolk.f~'xofokyo	
•	
.\$lkioheea\$ieg.	
.nk~x	
.%.	•
813 client pkts, 1 server pkt, 1 turn.	
Entire conversation (1,161 kB) Show and save data as ASCII Street	am 130 ⊊
Find:	Find <u>N</u> ext
Weights Filter Out This Stream Print Save as	× <u>C</u> lose

Figure 20. TCP stream showing the start of data exfiltrated by Ficker Stealer.

After exfiltrating its data, Ficker Stealer goes quiet and we don't see anything more from it. At this point, if the infected computer is a standalone Windows host, we will only see Hancitor C2 traffic. But if the infected computer is part of an AD environment, we should also see Cobalt Strike.

Let's look at the initial requests for Cobalt Strike by Hancitor using the following Wireshark filter:

http.request.uri contains .bin

This should return the following lines:

- belcineloweek[.]ru GET /1602s.bin
- belcineloweek[.]ru GET /1602s.bin

Follow the TCP stream for either of those HTTP GET requests. This TCP stream contains all three HTTP GET requests and responses to and from belcineloweek[.]ru, so you must scroll past a large amount of data representing the Ficker Stealer EXE. Near the end of the TCP stream, you should find two identical HTTP GET requests for 1602s.bin. Both requests return the same 682 bytes of data as shown below in Figure 21. This data is used to infect the victim with Cobalt Strike.

Wireshark · Follow TCP Stream (tcp.stream eq 12	25) · Example-1-2021-02-17-Hancitor-infection.pcap – + ×
	eh_frame. <mark>GET /1602s.bin HTTP/1.1</mark>
Accept: */*	line4: ve4: Trident/7 0: rv:11 0) like Cocke
Host: belcineloweek.ru	1104, X04, 111den(7.0, 1V.11.0) 11Ke Gecko
Cache-Control: no-cache	
HTTP/1.1 200 OK Server: nginy	
Date: Wed, 17 Feb 2021 16:17:51 GMT	
Content-Type: application/octet-stream	
Content-Length: 682	
Last-Modified: Tue 16 Feb 2021 13:56:28	SMT
ETag: "602bcfoc-2aa"	
Accept-Ranges: bytes	
7	.\$1XV1V0B#GDU.D.P
u.d.S#.Pus	
1T	Ta.I
.}E.r.d(}T.rT.g.<.KE<.2K	!.>(}!.,n .}J}yU
xm9AnMA3;WC7	0#L <t;1;f< td=""></t;1;f<>
6Qyx\UF14p0T	rTz zxx\$x.po+
5mC :[VZTLg=	t:BQj~Zu
S C + X T X M m XV	
{.n.S.q@=ZcmAaJ;GET /1	602s.bin HTTP/1.1
Accent */*	¥
3 <mark>client</mark> pkts, 201 server pkts, 5 turns.	
Entire conversation (276 kB) S	how and save data as ASCII T Stream 125 ‡
Find: .bin	Find <u>N</u> ext
⊘ Help	Filter Out This Stream Print Save as Back × Close

Figure 21. TCP stream showing 682 bytes of data returned from belcineloweek[.]ru for Cobalt Strike.

What does Cobalt Strike traffic look like?

It can be HTTP or HTTPS. In this pcap, HTTP GET requests by Hancitor for Cobalt Strike use the letter s in the URLs. The request for 1602s.bin indicates Cobalt Strike for this infection uses HTTPS traffic.

That is indeed what happened. Use your basic web traffic filter, then scroll down, and you should see several frames in the column display to 192.99.250[.]2 over TCP port 443 as shown below in Figure 22. This is Cobalt Strike traffic. Cobalt Strike traffic to this IP address does not have an associated domain, so the host name is blank in the column display.

-						Exa	mple	e-1-2021	-02-17-Hancitor-infection.pcap		- + ×
Ei	le <u>E</u> di	t <u>V</u> iew	<u>G</u> o <u>C</u> a	pture	<u>A</u> nalyze	Statistics	Tele	ephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp		
				×	<u>م</u>	🔶 🌩 🤇) 🍋	•	0 0 1		
	(http.request or tls.handshake.type eq 1) and !(ssdp)										
Tin	ne				Dst			port	Host	Info	^
	2021	-02-17	16:1	L7:24	52.1	85.211.	133	443	settings-win.data.micr	Client Hello	
	2021	-02-17	16:1	L7:25	20.19	90.154.	136	443	login.live.com	Client Hello	
	2021	-02-17	16:1	L7:29	52.18	85.211.	133	443	settings-win.data.micr	Client Hello	
	2021	-02-17	16:1	L7:31	13.1	07.246.	19	443	pti.store.microsoft.com	Client Hello	
	2021	-02-17	' 16:1	L7:32	192.3	36.41.1	4	80	thavelede.ru	POST /8/forum.php HTTP/1	.1
	2021	-02-17	16:1	L7:34	47.2	54.174.	221	80	belcineloweek.ru	GET /6sufiuerfdvc.exe HT	TP/
	2021	-02-17	16:1	L7:42	52.18	85.211.	133	443	settings-win.data.micr	Client Hello	
	2021	-02-17	16:1	L7:51	47.2	54.174.	221	80	belcineloweek.ru	GET /1602s.bin HTTP/1.1	
	2021	-02-17	16:1	L7:51	54.22	25.129.	141	80	api.ipify.org	GET /?format=xml HTTP/1.:	1
	2021	-02-17	16:1	L7:51	47.2	54.174.	221	80	belcineloweek.ru	GET /1602s.bin HTTP/1.1	
	2021	-02-17	16:1	L7:52	192.9	99.250.	2	443	Oakalt Otrilea	Client Hello	
	2021	-02-17	16:1	L7:54	192.9	99.250.	2	443	Cobait Strike	Client Hello	
	2021	-02-17	16:1	L8:07	192.9	99.250.	2	443	traffic	Client Hello	
	2021	-02-17	16:1	L8:09	192.9	99.250.	2	443	uanio	Client Hello	
	2021	-02-17	16:1	18:29	52.1	85.211.	133	443	settings-win.data.micr	Client Hello	
	2021	-02-17	16:1	19:10	192.9	99.250.	2	443		Client Hello	
	2021	-02-17	16:1	19:11	192.9	99.250.	2	443		Client Hello	
	2021	-02-17	16:1	19:12	192.9	99.250.	2	443		Client Hello	
	2021	-02-17	16:1	19:13	192.9	99.250.	2	443	Cobalt Strike	Client Hello	
	2021	-02-17	16:1	19:13	192.9	99.250.	2	443	troffic	Client Hello	
	2021	-02-17	16:1	19:15	192.9	99.250.	2	443	uanic	Client Hello	
	2021	-02-17	16:1	19:16	192.9	99.250.	2	443		Client Hello	
	2021	-02-17	16:1	19:17	192.9	99.250.	2	443		Client Hello	
	2021	-02-17	16:1	19:18	192.9	99,250,	2	443		Client Hello	¥

Figure 22. Traffic from the infected Windows host caused by Cobalt Strike. Certificate issuer data for HTTPS traffic caused by Cobalt Strike HTTPS is unusual. Why? Because all of the identification fields for items like country, locality and organization are blank. We can filter for certificate data in Cobalt Strike's HTTPS traffic and expand the frame details to see this.

First, find certificate data from the IP address for Cobalt Strike traffic by using the following Wireshark filter:

tls.handshake.type eq 11 and ip.addr eq 192.99.250.2

This should reveal two frames in your column display. Expand frame details for either of these frames until you find fields for certificate issuer data. These fields should be blank. Below, Figure 23 shows an example.

▼	 Example-1-2021-02-17-Hancitor-infection.pcap 						
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H</u> elp							
🖉 🔲 🖉 🎯 🚞 🛅 🕅 🔍 🔶	🔶 🥱 🍋 🏓		1				
Its.handshake.type eq 11 and ip.addr eq 1	92.99.250.2					× -	
Time Src	port	Dst	port	Info			
2021-02-17 16:17:53 192.99	.250.2 443	10.2.17.101	49805	Certificat	e, Server	Key Exchange,	Serv
2021-02-17 16:17:55 192.99	.250.2 443	10.2.17.101	49806	Certificat	e, Server	Key Exchange,	Serv
4							Þ
▶ Frame 4357: 1190 bytes on wi	re (9520 bit	s), 1190 byte	es captur	ed (9520 b	its)		*
> Ethernet II, Src: Netgear_b6	6:93:f1 (20:e	5:2a:b6:93:f1	L), Dst:	HewlettP_1	c:47:ae (0	0:08:02:1c:47	:ae
Internet Protocol Version 4,	Src: 192.99	.250.2, Dst:	10.2.17.	101			
Transmission Control Protoco	ol, Src Port:	443, Dst Por	rt: 49805	, Seq: 91,	Ack: 150,	Len: 1136	
 Transport Layer Security 							
- TLSv1.2 Record Layer: Hand	shake Protoc	ol: Certifica	ite				
Version, TLS 1 2 (ovo202	(22)						
Version: 1LS 1.2 (0x0303)						
- Handshake Protocol: Cert	ificate						
Handshake Type: Certifi	icate (11)						
Length: 813	10410 (11)						
Certificates Length: 81	10						
 Certificates (810 bytes 	S)						
Certificate Length: 8	307						
- Certificate: 30820323	3082020ba003	020102020408	b00ee300	d06092a (id-at-comm	onName=,id-at	-or(
 signedCertificate 							
version: v3 (2)	170100						
serialNumber: 146	4/3198 WithDCAEnery	ation)					
	WILLIRSAEHCTY	brion)					
rdnSequence: 6	items (id-at-	commonName=	id-at-org	anizationa	lunitName=	id-at-organi	izat
RDNSequence it	em: 1 item (id-at-country	(Name=)	anizaciona		, id at organi	-zuc
> RDNSequence it	em: 1 item (id-at-state0	Province	Name=)	certit	icate issue	
→ RDNSequence it	em: 1 item (id-at-localit	yName=)	,	data	for Cobalt	
→ RDNSequence it	:em: 1 item (id-at-organiz	zationNam	ie=)			
→ RDNSequence it	em: 1 item (id-at-organiz	zationalU	nitName=)	Strike	ениръ	
→ RDNSequence it	em: 1 item (id-at-commonN	lame=)		traffic		
, Malidity					a carrie	•	Ψ

Figure 23. Certificate issuer data for Cobalt Strike traffic.

For the rest of this pcap, we see HTTP GET requests for Hancitor C2 and HTTPS traffic for Cobalt Strike. Hancitor C2 traffic happens approximately every 2 minutes. HTTPS traffic for Cobalt Strike happens nearly every second.

Example 2, Part 1: Hancitor with Ficker Stealer and Cobalt Strike

Open *Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap* in Wireshark and use a basic web filter, as shown in Figure 24.

•	Example-2-2021	-02-10	-Hancitor-infection-part-1-of-2.pcap		- + ×		
<u>File Edit View Go</u> Capture	<u>A</u> nalyze <u>S</u> tatistics Teler	ohony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp				
/ • • • • • • • • • • • • • • • • • • •							
k (http.request or tls.handshake.type eq 1) and !(ssdp)							
Time	Dst	port	Host	Info			
2021-02-10 16:42:39	52.184.216.246	443	<pre>geo.prod.do.dsp.mp.micros</pre>	Client Hello			
2021-02-10 16:42:40	104.95.91.76	443	kv601.prod.do.dsp.mp.micr	Client Hello			
2021-02-10 16:42:40	104.95.91.76	443	cp601.prod.do.dsp.mp.micr	Client Hello			
2021-02-10 16:42:41	52.114.132.73	443	self.events.data.microsof	Client Hello			
2021-02-10 16:42:41	52.114.75.79	443	v20.events.data.microsoft	Client Hello			
2021-02-10 16:42:45	204.79.197.200	443	www.bing.com	Client Hello			
2021-02-10 16:42:52	40.126.0.69	443	login.microsoftonline.com	Client Hello			
2021-02-10 16:42:54	13.107.42.23	443	config.edge.skype.com	Client Hello			
2021-02-10 16:42:54	142.250.68.142	443	docs.google.com	Client Hello			
2021-02-10 16:42:54	142.250.68.142	443	docs.google.com	Client Hello			
2021-02-10 16:42:55	142.250.114.95	443	fonts.googleapis.com	Client Hello			
2021-02-10 16:42:55	142.250.68.129	443	lh5.googleusercontent.com	Client Hello			
2021-02-10 16:42:55	142.250.114.95	443	fonts.googleapis.com	Client Hello			
2021-02-10 16:42:55	142.250.114.94	443	fonts.gstatic.com	Client Hello			
2021-02-10 16:42:55	142.250.114.94	443	ssl.gstatic.com	Client Hello			
2021-02-10 16:42:55	204.79.197.219	443	edge.microsoft.com	Client Hello			
2021-02-10 16:42:59	85.13.154.57	80	b2b.ebike-your-life.com	GET /commemorative.ph	пр Н		
2021-02-10 16:43:00	85.13.154.57	80	b2b.ebike-your-life.com	GET /commemorative.ph	пр Н		
2021-02-10 16:43:03	85.13.154.57	80	b2b.ebike-your-life.com	GET /favicon.ico HTTF	·/1.		
1 0001 00 10 10 10 000	100 044 140 105	440	un kounuinstarkau unon a	Olient Helle			
→ Frame 1236: 571 byte	s on wire (4568 k	oits)	, 571 bytes captured (4568 b	pits)			
> Ethernet II, Src: He	wlettP_1c:47:ae	00:08	B:02:1c:47:ae), Dst: Netgeau	r_b6:93:f1 (20:e5:2a:k	06:93:f1)		
> Internet Protocol Ve	rsion 4, Src: 10.	2.10	.101, Dst: 142.250.68.142	-			
Transmission Control	Protocol, Src Po	ort: 4	49726, Dst Port: 443, Seq: :	1, Ack: 1, Len: 517			
Transport Layer Secu	rity						

Figure 24. Traffic from part one of our second example filtered in Wireshark using a basic web filter.

The pcap comes from an AD environment with the following characteristics:

- LAN segment range: 10.2.10.0/24
- Domain: pizzawithapples.food
- Domain controller: 10.2.10.10 Apples-DC
- LAN segment gateway: 10.2.10.1
- LAN segment broadcast address: 10.2.10.255
- IP address of the infected Windows host: 10.2.10.101
- Host name of the infected Windows host: DESKTOP-TRH50EJ
- User account name on the infected Windows host: dave.thomas

Above in Figure 24, we see a link to docs.google.com followed by HTTP GET requests to b2b.ebike-your-life[.]com/commemorative.php. As we did in our first example, we can export the HTML page from b2b.ebike-your-life[.]com from our second example and open it in a web browser to get the malicious Word document.

The SHA256 hash for your Word document should be

793d134cdb4bcba47e1f678d052c4d7747b93ea4199714efb8b614321b58dca7, and its name should be 0210_1723194332604.doc.

Also as we did for our first example, find Hancitor C2 activity using the following Wireshark filter:

http.request.uri contains "/8/forum.php" or http.host contains api.ipify.org

This returns IP address checks by Hancitor and Ficker Stealer, along with Hancitor C2 traffic, as listed below and shown in Figure 25.

- api.ipify.org GET /
- anumessensan[.]ru POST /8/forum.php
- api.ipify.org GET /?format=xml

Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap - + ×							
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp							
/ = 2 💿 🚞 🖹 🖄 🗳 🔍 🝁 🔷 🖊 🖨 🗐 🖆 🖃 🗉 🏛							
http.request.uri contains "/8/fo	orum.php" or http.host co	ntains	api.ipify.org	× 🗆 🔹			
Time	Dst	port	Host	Info			
2021-02-10 16:43:38	54.225.129.141	80	api.ipify.org	GET / HTTP/1.1			
2021-02-10 16:43:48	45.9.191.107	80	anumessensan.ru	POST /8/forum.php HTTP/1.1 (
2021-02-10 16:43:58	54.225.129.141	80	api.ipify.org	GET /?format=xml HTTP/1.1			
2021-02-10 16:45:58	45.9.191.107	80	anumessensan.ru	POST /8/forum.php HTTP/1.1 (
4				→			

Figure 25. IP address checks and Hancitor C2 traffic.

Filter for followup malware sent by Hancitor using the following Wireshark filter:

http.request.uri contains .exe or http.request.uri contains .bin

This should reveal Hancitor sending followup malware for Cobalt Strike and Ficker Stealer, as listed below and shown in Figure 26:

- backupez[.]com GET /0902.bin
- backupez[.]com GET /0902s.bin
- backupez[.]com GET /6yudfgh.exe

• Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap - + ×							
<u>File Edit View Go</u> Capture Analyze Statistics Telephony Wireless Tools Help							
/ I () () () () () () () () () (
🖡 http.request.uri contains .exe or http.request.uri contains .bin							
Time	Dst	port	Host	Info			
2021-02-10 16:43:56	8.208.10.147	80	backupez.com	GET	/0902.bin HTTP/1.1		
2021-02-10 16:43:57	8.208.10.147	80	backupez.com	GET	/0902s.bin HTTP/1.1		
2021-02-10 16:43:57	8.208.10.147	80	backupez.com	GET	/6yudfgh.exe HTTP/1.1		
•					•		

Figure 26. Hancitor sends follow-up malware for Cobalt Strike and Ficker Stealer. In this case, one of the GET requests for Cobalt Strike has an s in the URL, but the other does not, so we should see both HTTP and HTTPS traffic caused by the Cobalt Strike.

Return to your basic web filter, then scroll down to see what type of HTTP requests happen after the traffic to backupez[.]com. The results should show HTTP traffic over TCP port 1080 and HTTPS traffic over TCP port 4443.

Your Wireshark setup might not display any HTTP traffic over TCP port 1080, so you might have to set up Wireshark to show it. First, use the menu path *Analyze --> Decode As* shown below in Figure 27 to bring up the *Decode As* window.

-	Example-2-2021-02-10-Hancitor-infection-p	art-1-of-2.pcap – + ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>Analyze</u> <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ool	ls <u>H</u> elp
	Display <u>F</u> ilters	
Apply a display filter <ctrl- :<="" th=""><th>Display Filter <u>M</u>acros</th><th>🗖 - 🕈</th></ctrl->	Display Filter <u>M</u> acros	🗖 - 🕈
Time	Display Filter <u>E</u> xpression	Info
2021-02-10 16:42:29	Apply as Column Ctrl+Shift+I	DHCP Request - Transact
2021-02-10 16:42:29	Apply as Filter	DHCP ACK - Transact
2021-02-10 16:42:29	Prepare a Filter	Membership Report / Join
2021-02-10 16:42:29	Conversation Filter	Membership Report / Leav
2021-02-10 16:42:29 2021-02-10 16:42:29	Enabled Protocols Ctrl+Shift+E	Membership Report / Join
2021-02-10 16:42:29	Decode As	Standard query response
2021-02-10 16:42:29	Reload Lua Plugins Ctrl+Shift+L	Standard query 0x3223 AN
2021-02-10 16:42:29	SCTP +	10.2.10.1 is at 20:e5:2a
2021-02-10 16:42:29	Follow	Who has 10.2.10.10? Tell
2021-02-10 16:42:29	Show Dacket Dutes Ctrl+Shift+O	10.2.10.10 is at a4:1f:7
2021-02-10 16:42:29	Show Packet Bytes Cthronitro	Standard query 0x0052 SR
2021-02-10 16:42:29	Expert Information	Standard query response
2021-02-10 16:42:29	10.2.10.10 53	Standard query 0x8202 A
2021-02-10 16:42:29	10.2.10.101 494	scarchDoguest(1) " <poots< th=""></poots<>
		searchPosEntry(1) = R0012
2021-02-10 16:42:29	ff:ff:ff:ff:ff	Who has 10.2.10.101? (AR
•		>

Figure 27. Menu path for the Decode As window.

Once you have the Decode As window, create a new entry to decode TCP port 1080 as HTTP, as shown below in Figure 28.

•	Wireshark · Decode As ×						
Field	Value	Туре	Default	Current			
TCP port	1080	Integer, base 10	(none)	НТТР			
		/homo/vubu					
<pre>@Help</pre>	<u> </u>	momerxubu	inta-usen	$\boxed{\bullet Save} \times \underline{C}ancel \boxed{\checkmark \underline{O}K}$			

Figure 28. Creating a new entry in the Decode As window to decode TCP port 1080 as HTTP.

When you've created the new entry, either click the OK button or click the Save button. The Save button literally saves the entry, so it will work after you close and open Wireshark again. The OK button applies the decoding only as long as your current Wireshark session stays open.

In this case, we should click the Save button.

After saving the entry, go back to your Wireshark column display and use the basic web filter. Scroll down, and you should see both HTTP and HTTPS traffic for Cobalt Strike, as highlighted below in Figure 29.

Example-2-2021-02-10-Hancitor-infection-part-1-of-2.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	^			
2021-02-10 16:43:38	54.225.129.141	80	api.ipify.org	GET / HTTP/1.1				
2021-02-10 16:43:43	52.114.128.74	443	self.events.data.micr	Client Hello				
2021-02-10 16:43:48	45.9.191.107	80	anumessensan.ru	POST /8/forum.php	H			
2021-02-10 16:43:56	8.208.10.147	80	backupez.com	GET /0902.bin HTT	P/			
2021-02-10 16:43:57	8.208.10.147	80	backupez.com	GET /0902s.bin HT	TP			
2021-02-10 16:43:57	104.160.190.114	1080	104.160.190.114:1080	GET /WWFh HTTP/1.	1			
2021-02-10 16:43:57	8.208.10.147	80	backupez.com	GET /6yudfgh.exe	НТ			
2021-02-10 16:43:57	104.160.190.114	4443		Client Hello 🔶				
2021-02-10 16:43:57	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1.			
2021-02-10 16:43:58	54.225.129.141	80	api.ipify.org	GET /?format=xml	HT			
2021-02-10 16:43:58	104.160.190.114	4443		Client Hello 🔶				
2021-02-10 16:44:09	204.79.197.200	443	www.bing.com	Client Hello				
2021-02-10 16:44:36	52.114.128.10	443	v10.events.data.micro	Client Hello				
2021-02-10 16:44:36	52.114.128.10	443	v20.events.data.micro	Client Hello				
2021-02-10 16:44:39	52.109.8.21	443	nexusrules.officeapps	Client Hello				
2021-02-10 16:44:58	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1.			
2021-02-10 16:44:58	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1.			
2021-02-10 16:44:58	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1.			
2021-02-10 16:44:58	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1.			
2021-02-10 16:44:58	104.160.190.114	1080	104.160.190.114:1080	GET /fwlink HTTP/	1			
4					•			

Figure 29. Traffic caused by Cobalt Strike in our second example. Shown above in Figure 29, traffic caused by Cobalt Strike is:

- 104.160.190[.]114:8080 GET /WWFh
- 104.160.190[.]114:8080 GET /fwlink
- 104.160.190[.]114 port 4443 HTTPS traffic

The first HTTP GET request, ending with WWFh, returned 208,473 bytes of an encoded binary that most likely decodes to a Windows binary used for Cobalt Strike. Follow the TCP stream for this HTTP request, and you should see information shown below in Figure 30.

```
Wireshark · Follow TCP Stream (tcp.stream eq 88) · Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap
GET /WWFh HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
Host: 104.160.190.114:1080
Connection: Keep-Alive
Cache-Control: no-cache
HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 16:42:09 GMT
Content-Type: application/octet-stream
Content-Length: 208473
.....+..a....).{.S...N.A...$..sR~.'X.0....81....P..
6....)/..-/..z.I.z.I.z.I.z.I.z.I.z.I.z.I.z.I^z.IPejGP.c.qib..H6..;...Tq..9Q..W?..w]...
(...1F...#...Lq..A|..A|..A|.Q.n.. ..Q.n.. ...T...o....|.>=...T..
].4
].4
]..
_V..VV.BTV..UV..UV.CTV.STV.3VV.3VF.#VF.!VF.!VF.!VF.!VF.!
s?..s?..q?..q?..s?..s?..s?..s?..s?..s_...>;/.>;0.>;..>;..>;..>;..>;..>{..~U.v
4.v
.Ev
.Eu
.qu
..W
1 client pkt, 159 server pkts, 1 turn.
Entire conversation (208 kB)
                               -
                                   Show and save data as ASCII
                                                       *
                                                                Stream 88
Find:
                                                                   Find Next
Help
                                  Filter Out This Stream
                                                 Print
                                                      Save as...
                                                              Back
                                                                   × Close
```

Figure 30. TCP stream of the initial HTTP GET request to 104.160.190[.]114:8080.Further HTTP traffic to 104.160.190[.]114:8080 for fwlink is Cobalt Strike C2 traffic. This traffic also returns encoded data, if it returns any data at all. In most cases, zero bytes of content are returned. The first HTTP request to 104.160.190[.]114:8080 for fwlink returned 48 bytes of encoded data, as shown below in Figure 31.

 Wireshark · Follow TCP Stream (tcp.stream eq 100) · Example-2-2021-02-10-Hancitor-infection-part-1-of-2.pcap - + ×
<pre>GET /fwlink HTTP/1.1 Accept: */* Cookie: Wa7eqYnNWHNgmEvMy64QCwLraL2yf6KSu3Ga842ubRvUNMMNTiGYS2Xir8jtX12gyuuKXAoBz2Ykk92KMT1ajmS XEHGAW2SL2kpcf/J8PHU0fcpCQguRRSRrhvWfBGqDNLHMbvsyE8/YCtUof0L0I2+j63+j0QwePQ+NX+BU0pE= User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2) Host: 104.160.190.114:1080 Connection: Keep-Alive Cache-Control: no-cache</pre>
HTTP/1.1 200 OK Date: Wed, 10 Feb 2021 16:43:09 GMT Content-Type: application/octet-stream Content-Length: 48
.N.&.M7.K.;)Z).@IbO#.:?.
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (549 bytes) • Show and save data as ASCII • Stream 100 +
Find: Find Next
Help Filter Out This Stream Print Save as Back × Close

Figure 31. First HTTP request for Cobalt Strike C2 traffic returned 48 bytes of data. These HTTP requests for Cobalt Strike C2 happen approximately once every second. HTTPS traffic for Cobalt Strike C2 is similarly busy, with traffic to 104.160.190[.]114 over TCP port 4443 appearing approximately once every second.

Our next pcap for our second example is from later during the same infection, when we see indicators of Send-Safe spambot malware.

Example 2, Part 2: Hancitor C2, Cobalt Strike C2 and Send-Safe Spambot Malware

Open *Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap* in Wireshark and use a basic web filter, as shown in Figure 32.

Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap - + ×								
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>								
/ • • • • • • • • • • • • • • • • • • •								
(http.request or tls.handshake.type eq 1) and !(ssdp)								
Time	Dst	port Host		Info	^			
2021-02-10 18:28:48	104.160.190.114	4443		Client Hello				
2021-02-10 18:28:48	104.160.190.114	4443		Client Hello				
2021-02-10 18:28:49	104.160.190.114	4443		Client Hello				
2021-02-10 18:28:52	104.160.190.114	1080 104.16	0.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:52	104.160.190.114	1080 104.16	0.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:52	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:53	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/	-			
2021-02-10 18:28:53	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:53	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:53	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/:				
2021-02-10 18:28:54	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:54	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/:				
2021-02-10 18:28:54	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:55	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/:				
2021-02-10 18:28:55	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:55	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:55	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:55	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:56	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:56	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:56	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:56	104.160.190.114	1080 104.16	0.190.114:1080	GET /fwlink HTTP/				
2021-02-10 18:28:57	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/:				
2021-02-10 18:28:57	104.160.190.114	1080 104.16	60.190.114:1080	GET /fwlink HTTP/				
1				•				

Figure 32. Traffic from part two of our second example filtered in Wireshark using a basic web filter.

This pcap happens later during the same infection as our previous pcap. At times, we see up to three or four HTTP GET requests for Cobalt Strike C2 traffic during the same second.

However, this pcap reveals that Hancitor sent another Windows executable file, and that executable is Send-Safe-based spambot malware.

To find this Windows executable file, use the following Wireshark filter:

http.request.uri contains .exe

The result is another HTTP GET request to backupez[.]com, which is the domain used by Hancitor to push followup malware in part one of this example. The URL ends with 47.exe. See the result below in Figure 33.

• Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap - + ×						
<u>File E</u> dit <u>View Go</u> Capture <u>Analyze</u> <u>Statistics</u> Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp						
/ • • • • • • • • • • • • • • • • • • •						
🖡 http.request.uri contains .exe 🛛 💌 👻						
Time	Dst	port	Host	Info		
2021-02-10 18:30:24	8.208.10.147	80	backupez.com	GET	/47.exe	HTTP/1.1
•						•

Figure 33. Hancitor retrieves Windows executable for Send-Safe spambot malware.

You can export this file from the pcap using the menu path *File --> Export Objects --> HTTP.* Select the entry for 47.exe from backupez[.]com, as shown below in Figure 34.

Examp	le-2-2021-02-10-Ha	ncitor-in	fection-pa	rt-2-of-2.pcap		- + ×			
File Edit View Go Capture	Analyze Statistics	Telephor	ny <u>W</u> ireles	s <u>T</u> ools <u>H</u> elp					
<u>O</u> pen	Ctrl+O			4 - 1					
Open <u>R</u> ecent	÷					X 🗆 🗸 🍦			
. <u>M</u> erge		port	Host	Info	,				
Import from Hex Dump		7 80	backup	ez.com GE	/47.exe H	TP/1.1			
Close	Ctrl+W		-	Wi	reshark · Expor	t · HTTP objec	t list		- + ×
Save	Ctrl+S		Packet *	Hostname	Content Type			Size	Filename
Save <u>A</u> s	Ctrl+Shift+S		3132 3134	anumessensar anumessensar	.ru application/x .ru text/html	-www-form-ur	lencoded	175 bytes 44 bytes	forum.php forum.php
File Set	+		5226	backupez.com	application/c	ctet-stream		1,878 kB	47.exe
Export Specified Packets			4						•
Export Packet Dissections	*		Text Filter	:					
Export Packet <u>Bytes</u>	Ctrl+Shift+X		Help				Save All	× <u>C</u> lose	e <u>S</u> ave
Export PDUs to File									
Export TLS Session Keys									
Export Objects	•	DICO	м						
Print	Ctrl+P	HTTP							
Quit	Ctrl+Q	IMF							
		SMB.							
		TFTP.							
•						Þ			

Figure 34. Exporting the Send-Safe spambot EXE from the pcap. The SHA256 hash of 47.exe is:

51ca66a8ac7f4e072b39ef886d7d414d6c6868d0d67a46150835297e65493dc6

Send-Safe was a commercially available program sold through a now-defunct website named send-safe[.]com. It was advertised as "...a bulk-emailing program that allows you to send email from your own computer, or a remote computer with or without the use of proxies."

This program has been used by various threat actors as malware to turn infected Windows computers into spambot hosts.

What does Send-Safe spambot traffic look like? Our infected Windows host generated the following traffic:

- HTTPS traffic to 31.44.184[.]47 over TCP port 50025
- Traffic to 31.44.184[.]47 over UDP port 50026
- SMTP traffic sending out malicious spam pushing Hancitor.

To find Send-Safe UDP traffic, use udp.port eq 50026 for your Wireshark filter. The results should look like Figure 35 below.

File Édit View Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Control I
Image: Content of the term of the term of the term of t
Image: Normal State Dest port Info 2021-02-10 18:30:27 10.2.10.101 50815 31.44.184.47 50026 50815 → 50026 Len=72 2021-02-10 18:30:28 31.44.184.47 50026 10.2.10.101 50815 50026 → 50815 Len=8 2021-02-10 18:30:29 10.2.10.101 50816 31.44.184.47 50026 50816 → 50026 Len=72 2021-02-10 18:30:29 10.2.10.101 50816 31.44.184.47 50026 50816 -50026 Len=72 2021-02-10 18:30:30 10.2.10.101 50817 50026 50817 -50026 Len=72 2021-02-10 18:30:30 31.44.184.47 50026 10.2.10.101 50817 -50026 Len=72 2021-02-10 18:30:31 10.2.10.101 50818 31.44.184.47 50026 50817 -50026 Len=72 2021-02-10 18:30:31 10.2.10.101 50818 31.44.184.47 50026 50817 Len=24 2021-02-10 18:30:
$\begin{array}{ c c c c c c c c c c c c c c c c c c c$
$\begin{array}{cccccccccccccccccccccccccccccccccccc$
2021-02-10 18:30:31 31.44.184.47 50026 10.2.10.101 50818 50026 → 50818 Len=24 2021-02-10 18:30:32 10.2.10.101 50819 31.44.184.47 50026 50819 → 50026 Len=72 2021-02-10 18:30:33 31.44.184.47 50026 10.2.10.101 50819 50026 → 50819 Len=72 2021-02-10 18:30:34 10.2.10.101 50820 31.44.184.47 50026 50820 → 50026 Len=72
2021-02-10 18:30:32 10.2.10.101 50819 31.44.184.47 50026 50819 → 50026 Len=72 2021-02-10 18:30:33 31.44.184.47 50026 10.2.10.101 50819 50026 → 50819 Len=24 2021-02-10 18:30:34 10.2.10.101 50820 31.44.184.47 50026 50820 → 50026 Len=72
2021-02-1018:30:3331.44.184.475002610.2.10.1015081950026 → 50819Len=242021-02-1018:30:3410.2.10.1015082031.44.184.475002650820 → 50026Len=72
2021-02-10 18:30:34 10.2.10.101 50820 31.44.184.47 50026 50820 → 50026 Len=72
2021-02-10 18:30:34 31.44.184.47 50026 10.2.10.101 50820 50026 → 50820 Len=24
2021-02-10 18:30:35 10.2.10.101 50821 31.44.184.47 50026 50821 → 50026 Len=72
2021-02-10 18:30:35 31.44.184.47 50026 10.2.10.101 50821 50026 → 50821 Len=24
2021-02-10 18:30:36 10.2.10.101 50822 31.44.184.47 50026 50822 → 50026 Len=72
2021-02-10 18:30:36 31.44.184.47 50026 10.2.10.101 50822 50026 → 50822 Len=24
2021-02-10 18:30:37 10.2.10.101 50823 31.44.184.47 50026 50823 → 50026 Len=72
2021-02-10 18:30:37 31.44.184.47 50026 10.2.10.101 50823 50026 → 50823 Len=24
2021-02-10 18:30:38 10.2.10.101 50824 31.44.184.47 50026 50824 → 50026 Len=72
2021-02-10 18:30:39 31.44.184.47 50026 10.2.10.101 50824 50026 → 50824 Len=24
2021-02-10 18:30:40 10.2.10.101 50825 31.44.184.47 50026 50825 → 50026 Len=72
2021-02-10 18:30:40 31.44.184.47 50026 10.2.10.101 50825 50026 → 50825 Len=24
2021-02-10 18:30:41 10.2.10.101 50826 31.44.184.47 50026 50826 → 50026 Len=72
2021-02-10 18:30:41 31.44.184.47 50026 10.2.10.101 50826 50026 → 50826 Len=24
2021-02-10 18:30:42 10.2.10.101 50827 31.44.184.47 50026 50827 → 50026 Len=72
2021-02-10 18:30:42 31.44.184.47 50026 10.2.10.101 50827 50026 → 50827 Len=24

Figure 35. UDP traffic caused by Send-Safe-based spambot malware. To view Send-Safe SMTP traffic and HTTPS traffic, use the following Wireshark filter:

(tcp.port eq 50025 and tls.handshake.type eq 1) or smtp.data.fragment

Your results should look similar to Figure 36.

Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap - + ×							- + ×
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
(tcp.port eq 50025 and tls.hand	lshake.type eq 1) or smtp.	data.fragme	ent			×	
Time	Dst	port	Info				^
2021-02-10 18:30:38	31.44.184.47	50025	Client Hello				
2021-02-10 18:30:38	31.44.184.47	50025	Client Hello				
2021-02-10 18:30:48	31.44.184.47	50025	Client Hello				
2021-02-10 18:30:48	31.44.184.47	50025	Client Hello				
2021-02-10 18:30:59	31.44.184.47	50025	Client Hello				
2021-02-10 18:30:59	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:08	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:09	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:11	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:11	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:12	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:13	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:17	216.200.145.235	25	from: "KeyCorp	Fraud	Protection	Team" <ycl< td=""><td></td></ycl<>	
2021-02-10 18:31:17	72.52.178.67	25	from: "KeyCorp	Theft	Protection	Squad" <1	
2021-02-10 18:31:17	172.217.195.26	25	from: "KeyBank	Theft	Protection	Group" <e< td=""><td></td></e<>	
2021-02-10 18:31:18	172.217.195.26	25	from: "KeyCorp	Fraud	Avoidance T	eam" <oto< td=""><td></td></oto<>	
2021-02-10 18:31:18	172.217.195.26	25	from: "KeyCorp	Fraud	Protection	Squad" <1	
2021-02-10 18:31:18	192.96.216.82	25	from: "KeyCorp	Theft	Prevention	Team" <rv< td=""><td></td></rv<>	
2021-02-10 18:31:18	216.8.138.86	25	from: "KeyBank	Fraud	Prevention	Squad" <u< td=""><td></td></u<>	
2021-02-10 18:31:18	67.192.26.184	25	from: "KeyCorp	Theft	Protection	Crew" <tp< td=""><td></td></tp<>	
2021-02-10 18:31:18	216.163.188.54	25	from: "KeyBank	Theft	Protection	Group" <e< td=""><td></td></e<>	
2021-02-10 18:31:18	148.163.146.64	25	from: "KeyBank	Theft	Protection	Team" <ta< td=""><td></td></ta<>	
2021-02-10 18:31:18	64.233.177.26	25	from: "KeyCorp	Fraud	Prevention	Crew" <ze< td=""><td></td></ze<>	
2021-02-10 18:31:18	31.44.184.47	50025	Client Hello				
2021-02-10 18:31:18	217.74.103.251	25	from: "KeyCorp	Theft	Prevention	Crew" <xo< td=""><td></td></xo<>	
2021-02-10 18:31:18	8.31.233.172	25	from: "KevBank	Theft	Protection	Groun" <h< td=""><td>Ŧ</td></h<>	Ŧ

Figure 36. HTTPS and spambot traffic caused by Send-Safe-based malware. HTTPS traffic over TCP port 50025 caused by Send-Safe has certificate issuer data that uses Send-Safe as the organizationName and commonName, as shown below in Figure 37.

Example-2-2021-02-10-Hancitor-infection-part-2-of-2.pcap								
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>								
Itls.handshake.type eq 11 and ip.ad	ddr eq 31.44.184.47	7				× 🖘 🔹		
Time Sr	rc	port D	Ost	port	Info			
2021-02-10 18:30:38 3	1.44.184.47	50025 1	10.2.10.101	62359	Server Hello,	Certifica		
2021-02-10 18:30:39 3 2021-02-10 18:30:48 3	1.44.184.47 1 <i>44</i> 184 47	50025 1 50025 1	L0.2.10.101	62360 62372	Server Hello,	Certifica		
<pre>> Frame 5270: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) > Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:4 > Internet Protocol Version 4, Src: 31.44.184.47, Dst: 10.2.10.101 > Transmission Control Protocol, Src Port: 50025, Dst Port: 62359, Seq: 1, Ack: 150, Len: 708</pre>								
<pre>> Transport Layer Security > TLSv1 Record Layer: Handshake Protocol: Server Hello > TLSv1 Record Layer: Handshake Protocol: Certificate Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 615 > Handshake Protocol: Certificate Handshake Type: Certificate (11) Length: 611 Certificates Length: 608 > Certificates (608 bytes) Certificate Length: 605 < Certificate: 30820259308201c2a00302010202045077ae78300d06092a (id-at-commonName=Send- < signedCertificate</pre>								
version: v3 serialNumber	(2) : 1350020728							
 signature (sł sisuer: rdnSe rdnSequence RDNSequen 	halWithRSAEnce equence (0) e: 6 items (i ice item: 1 i ice item: 1 i	cryption) d-at-comm tem (id-a tem (id-a tem (id-a tem (id-a tem (id-a tem (id-a	nonName=Send-S tt-countryName tt-stateOrProv tt-localityNam tt-organizatio tt-organizatio tt-commonName=	afe,id-at =Unknown) inceName= e=Unknown nName=Sen nalUnitNa Send-Safe	-organizationa Unknown)) d-Safe) me=Unknown))	alUnitName=Unk		

Figure 37. Send-Safe-specific certificate issuer data in HTTPS traffic caused by Send-Safe malware.

Since the SMTP traffic in this pcap is unencrypted, you can extract the emails using Wireshark. The menu path is *File --> Export Objects --> IMF* as shown below in Figure 38.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Open Ctrl+O Import Content View Size Filename Merge Import from Hex Dump Filename Constantinlupescu.com EML file 10 kB KeyCorp Platform Close Ctrl+W .114 State Opaeb@constantinlupescu.com EML file 10 kB KeyBank System	• + ×
Open Ctrl+O Wireshark · Export · IMF object list Open Recent Packet * Hostname Content Type Size Filename Merge Packet * Hostname Content Type Size Filename Import from Hex Dump Close Ctrl+W .114 Yester Mireshark · Export · IMF object list	+ ×
Open Recent Packet * Hostname Content Type Size Filename Merge 7911 ychoned@constantinlupescu.com EML file 10 kB KeyCorp Platform Import from Hex Dump 7938 Irwragq@constantinlupescu.com EML file 10 kB KeyBank Platform Close Ctrl+W .114 111 otopaeb@constantinlupescu.com EML file 10 kB KeyBank System	^
Merge 7911 ychoned@constantinlupescu.com EML file 10 kB KeyCorp Platforn Import from Hex Dump 7938 Irwragq@constantinlupescu.com EML file 10 kB KeyBank Platforn Close Ctrl+W .114 8111 otopaeb@constantinlupescu.com EML file 10 kB KeyBank Platforn	-
Import from Hex Dump 7938 Irwragq@constantinlupescu.com EML file 10 kB KeyBank Platford Import from Hex Dump 7948 egeoqi@constantinlupescu.com EML file 10 kB KeyBank Platford Close Ctrl+W .114 8111 otopaeb@constantinlupescu.com EML file 10 kB KeyBank System	1 Em
Import from Hex Dump 7948 egeoqi@constantinlupescu.com EML file 10 kB KeyCorp System Close Ctrl+W .114 8111 otopaeb@constantinlupescu.com EML file 10 kB KeyBank System	n Nc
Close Ctrl+W +114 8111 otopaeb@constantinlupescu.com EML file 10 kB KeyBank System	Noti
	Not
Save Ctrl+S 8162 l@constantinlupescu.com EML file 10 kB KeyCorp Platform	n Nc
Save As Ctrl+Shift+S 114 8287 ryvywol@constantinlupescu.com EML file 10 kB KeyBank System	Ema
114 8397 umnap@constantinlupescu.com EML file 10 kB KeyBank System	Mes
File Set , 8436 tpduxo@constantinlupescu.com EML file 10 kB KeyBank Platfor	n Nc
Export Specified Packets	Noti
Export Packet Dispertions	1 Em 👻
Tayl Filter	
Export Packet Bytes Ctrl+Shift+X .114	
Export PDUs to File	ave
Export TLS Session Keys 114 114 2 10 101 62074	
Export Objects DICOM 104.160.190.114 4443	
10.2.10.101 62074	
Print Ctrl+P HITP 104.160.190.114 4443	
Quit Ctrl+Q IMF 104.160.190.114 4443	
2021-02-10 18:28:48 104.160.190 _{SMB} 10.2.10.101 62075	
2021-02-10 18:28:48 10.2.10.101 104.160.190.114 4443	
2021-02-10 18:28:48 10.2.10.101 IFP 104.160.190.114 4443	
2021-02-10 18:28:48 104.160.190.114 4443 10.2.10.101 62075	
2021-02-10 18:28:48 104.160.190.114 4443 10.2.10.101 62075	
2021-02-10 18:28:48 10.2.10.101 62075 104.160.190.114 4443	
2021-02-10 18:28:48 104.160.190.114 4443 10.2.10.101 62075	
2021-02-10 18:28:48 10.2.10.101 62075 104.160.190.114 4443	
2021-02-10 18:28:48 10.2.10.101 62075 104.160.190.114 4443	

Figure 38. Exporting emails caused by the Send-Safe spambot malware.

This pcap contains 167 emails you can export. On average, several messages were pushed out each second from this Send-Safe-infected Windows host.

Below, Figure 39 shows what one of the exported items of Hancitor spam looks like in a Thunderbird email client. The template for this specific wave of Hancitor spam spoofed a well-known bank.



Figure 39. An example of a Hancitor email exported from the pcap.

Example 3: Hancitor with Ficker Stealer, Cobalt Strike and a Network Ping Tool

Open *Example-3-2021-01-25-Hancitor-infection.pcap* in Wireshark and use a basic web filter, as shown in Figure 40.

Example-3-2021-01-25-Hancitor-infection.pcap - +						- + ×					
F	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help										
$\measuredangle \blacksquare \oslash \otimes \models \blacksquare \blacksquare X \oslash 4 \Rightarrow \Rightarrow 4 \Rightarrow \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare$											
(http.request or tls.handshake.type eq 1) and !(ssdp)											
Ti	me			Dst		port	Host	Info			^
	2021-	01-25	16:29	13.88.28	.53	443	self.events.data.micr	Client	Hello		
	2021-	01-25	16:29	168.62.5	7.154	443	v20.events.data.micro…	Client	Hello		
	2021-	01-25	16:29	204.79.1	97.200	443	www.bing.com	Client	Hello		
	2021-	01-25	16:30	40.126.0	.71	443	login.microsoftonline	Client	Hello		
	2021-	01-25	16:30	172.217.	9.14	443	docs.google.com	Client	Hello		
	2021-	01-25	16:30	13.107.4	2.23	443	config.edge.skype.com	Client	Hello		
	2021-	01-25	16:30	216.58.1	93.138	443	fonts.googleapis.com	Client	Hello		
	2021-	01-25	16:30	216.58.1	94.65	443	lh6.googleusercontent	Client	Hello		
	2021-	01-25	16:30	216.58.1	93.138	443	fonts.googleapis.com	Client	Hello		
	2021-	01-25	16:30	172.217.	14.163	443	fonts.gstatic.com	Client	Hello		
	2021-	01-25	16:30	172.217.	12.35	443	ssl.gstatic.com	Client	Hello		
	2021-	01-25	16:30	198.38.8	2.169	80	www.nucala.inspia.net	GET /ma	rs.php	HTTP,	
	2021-	01-25	16:30	198.38.8	2.169	80	www.nucala.inspia.net	GET /ma	rs.php	HTTP.	
	2021-	01-25	16:30	198.38.8	2.169	80	www.nucala.inspia.net	GET /fa	vicon.i	CO H	
	2021-	01-25	16:30	151.101.	2.133	443	www.docusign.com	Client	Hello		
	2021-	01-25	16:30	72.21.91	.29	80	ocsp.digicert.com	GET /MF	EwTzBNM	EswS ⁻	
	2021-	01-25	16:30	173.223.	156.159	443	cdn.optimizely.com	Client	Hello		
	2021-	01-25	16:30	173.223.	109.53	443	players.brightcove.net	Client	Hello		
	2021-	01-25	16:30	23.2.243	.88	443	a275532918.cdn.optimi	Client	Hello		
4	0001	01 05	10.00	1 - 1 - 1 - 1	0 110	440	foot victic com	Oliont	ualla	•	Y

Figure 40. Traffic from the fourth pcap filtered in Wireshark using our basic web filter. The pcap comes from an AD environment with the following characteristics:

- LAN segment range: 10.1.25.0/24
- Domain: permafrostie.com
- Domain controller: 10.1.25.2 Permafrostie-DC
- LAN segment gateway: 10.1.25.1
- LAN segment broadcast address: 10.1.25.255
- IP address of the infected Windows host: 10.1.25.101
- Host name of the infected Windows host: DESKTOP-GAL3OV5
- User account name on the infected Windows host: barry.paulsen

The page that delivered the initial Word document was www.nuicala.inspia[.]net/mars.php. As we did in our two previous examples, we can export the web page, open it in a browser and get the malicious Word document used to kick off this Hancitor infection.

The SHA256 hash and name for the extracted malicious Word document is:

8922dbb1e7f157c62fe64d03278757d78d136eb94d00ac2df101789d602f1224 0125_206410993.doc

Based on techniques from our first two examples, you can find the following information from this Hancitor infection:

Hancitor traffic:

• port 80 - api.ipify.org - GET /

• 83.220.169[.]45 port 80 - wasintodese[.]ru - POST /8/forum.php

Followup malware for Cobalt Strike:

- 8.209.78[.]68 port 80 drivewaysnowservice[.]com GET /2101.bin
- 8.209.78[.]68 port 80 drivewaysnowservice[.]com GET /2101s.bin

Followup malware for Ficker Stealer

8.209.78[.]68 port 80 - drivewaysnowservice[.]com - GET /6gfbd5ws.exe

Cobalt Strike traffic:

- 23.106.80[.]14 port 1080 23.106.80[.]14:1080 GET /JdHf
- 23.106.80[.]14 port 1080 23.106.80[.]14:1080 GET /match
- 23.106.80[.]14 port 1080 23.106.80[.]14:1080 POST /submit.php?id=2612103345
- 23.106.80[.]14 port 4443 HTTPS traffic

Ficker Stealer traffic:

- port 80 api.ipify.org GET /?format=xml
- 185.100.65[.]29 port 80 sweyblidian[.]com TCP traffic

Of note, Ficker Stealer is the same binary for all examples in this tutorial, so we should see the same post-infection traffic by this malware. For Cobalt Strike, any HTTP POST request containing /submit.php?id= has an identification number that's unique for each infected Windows host.

If you see these HTTP POST requests with /submit.php?id= from Cobalt Strike, be alert for indicators of additional malware.

Malware sent through Cobalt Strike appears as an encoded binary that is decoded on the victim host. Because of this, we will not find the actual malware binary in the pcap. Instead, followup malware sent through Cobalt Strike is identified by its post-infection traffic.

In this case, we see ICMP scanning that indicates a <u>network ping tool</u> was sent through Cobalt Strike. Use the Wireshark filter icmp in the pcap, and your column display should look similar to Figure 41 below.

Example-3-2021-01-25-Hancitor-infection.pcap - + ×							
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
	२ 🔶 🌩 🥱		- 1				
📕 icmp					× 🗆 🔹		
Time	Src	Dst	Info		^		
2021-01-25 16:35:42	10.1.25.101	10.1.25.1	Echo (ping) r	equest id:	=0x000		
2021-01-25 16:35:42	10.1.25.1	10.1.25.101	Echo (ping) r	eply id:	=0×000		
2021-01-25 16:35:42	10.1.25.101	10.1.25.2	Echo (ping) r	equest id	=0×000		
2021-01-25 16:35:42	10.1.25.2	10.1.25.101	Echo (ping) r	eply id:	=0×000		
2021-01-25 16:38:20	10.1.25.101	192.168.0.0	Echo (ping) r	equest id:	=0×070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.1	Echo (ping) r	equest id	=0×070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.2	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.3	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.4	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.5	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.6	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.7	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.8	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.9	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.10	Echo (ping) r	equest id=	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.11	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.12	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.13	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.14	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.15	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.16	Echo (ping) r	equest id:	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.17	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.18	Echo (ping) r	equest id	=0x070		
2021-01-25 16:38:20	10.1.25.101	192.168.0.19	Echo (ping) r	equest id:	=0x070 -		

Figure 41. ICMP traffic from a network ping tool sent through Cobalt Strike.

As described in our recent blog about <u>Hancitor</u>, samples of the network ping tool recovered from infected Windows hosts generate approximately 1.5 GB of ICMP traffic, as they ping more than 17 million IP addresses targeting internal, non-routable IPv4 address space.

Based on our tests, these network ping tools hit the following address space:

- 192.168.0.0 through 192.168.254.254
- 172.16.0.0 through 172.31.254.254
- 10.0.0.0 through 10.254.254.254

This much ping traffic is prohibitively slow to display in Wireshark. The pcap for our third example of Hancitor has ping traffic to 192.168.0.0/16 and some of the ping traffic hitting the 172.16.0.0/12 address space before the recording was stopped.

Example 4: Hancitor with Ficker Stealer, Cobalt Strike and NetSupport Manager RAT

Open *Example-4-2021-02-02-Hancitor-infection.pcap* in Wireshark and use a basic web filter, as shown in Figure 42.

Example-4-2021-02-02-Hancitor-infection.pcap - +							
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>							
$ \blacksquare \blacksquare \boxtimes \odot \models \blacksquare \boxtimes \boxtimes 4 \Leftrightarrow \phi \Rightarrow \Rightarrow \Rightarrow \Rightarrow \models \Rightarrow \blacksquare \blacksquare$							
(http.request or tls.handshake.type eq 1) a	ind !(ssdp)		×				
Time Dst	port	Host	Info	^			
2021-02-02 16:22:58 52.114.	132.73 443	self.events.data.mi	Client Hello	1 🗋			
2021-02-02 16:22:58 40.122.	160.14 443	v20.events.data.mic	Client Hello				
2021-02-02 16:23:00 204.79.	197.200 443	www.bing.com	Client Hello				
2021-02-02 16:23:00 13.107.	42.14 443	rum14.perf.linkedin	Client Hello				
2021-02-02 16:23:00 20.140.	56.70 443	fp-afd.azureedge.us	Client Hello				
2021-02-02 16:23:00 13.107.	253.254 443	t-ring.msedge.net	Client Hello				
2021-02-02 16:23:00 13.107.	246.13 443	fp-afd.azureedge.net	Client Hello				
2021-02-02 16:23:00 13.107.	4.254 443	c-ring.msedge.net	Client Hello				
2021-02-02 16:23:00 131.253	.33.254 443	a-ring-fallback.mse…	Client Hello				
2021-02-02 16:23:10 40.126.	0.68 443	login.live.com	Client Hello				
2021-02-02 16:23:11 104.214	.58.194 443	checkappexec.micros	Client Hello				
2021-02-02 16:23:12 104.214	.58.194 443	smartscreen-prod.mi	Client Hello				
2021-02-02 16:23:21 52.114.	128.10 443	v10.events.data.mic	Client Hello				
2021-02-02 16:23:23 52.114.	128.10 443	v20.events.data.mic	Client Hello				
2021-02-02 16:23:25 40.126.	0.74 443	login.microsoftonli…	Client Hello				
2021-02-02 16:23:27 13.107.	42.23 443	config.edge.skype.c	Client Hello				
2021-02-02 16:23:27 216.58.	194.78 443	docs.google.com	Client Hello				
2021-02-02 16:23:27 216.58.	194.78 443	docs.google.com	Client Hello				
2021-02-02 16:23:28 172.217	.12.65 443	lh4.googleuserconte	Client Hello				
2021-02-02 16:23:29 172.217	.9.3 443	ssl.gstatic.com	Client Hello				
2021-02-02 16:23:31 77.72.4	.98 80	premierpt.co.uk	GET /footage.php	ł			
2021-02-02 16:23:32 77.72.4	.98 80	premierpt.co.uk	GET /footage.php	ł			
2021-02-02 16:23:41 77.72.4	.98 80	premierpt.co.uk	GET /favicon.ico	ł			
2021-02-02 16:23:41 151.101	.2.133 443	www.docusign.com	Client Hello	v			

Figure 42. Traffic from the fifth pcap filtered in Wireshark using our basic web filter. The pcap comes from an AD environment with the following characteristics:

- LAN segment range: 10.2.2.0/24
- Domain: sillybobcat.com
- Domain controller: 10.2.2.2 Cats-DC
- LAN segment gateway: 10.2.2.1
- LAN segment broadcast address: 10.2.2.255
- IP address of the infected Windows host: 10.2.2.101
- Host name of the infected Windows host: DESKTOP-NDGEE4D
- User account name on the infected Windows host: baxter.murdoch

The page that delivered the initial Word document was premierpt.co[.]uk/footage.php. As we did for our previous examples, we can export the web page, open it in a browser and get the malicious Word document used to kick off this Hancitor infection.

The SHA256 hash and name for the extracted malicious Word document is:

b60431e0fe5bf2b5c7cd5e01add62d24cd6ad2c99eb6a23fb5a2967d812cbf08 0202_10846666250132.doc

Based on techniques from our previous examples, you can find the following information from this Hancitor infection:

Hancitor traffic:

- port 80 api.ipify.org GET /
- 45.9.191[.]107 port 80 knorshand[.]ru POST /8/forum.php

Followup malware for Cobalt Strike:

- 8.209.78[.]68 port 80 bobcatofredding[.]com GET /0102.bin
- 8.209.78[.]68 port 80 bobcatofredding[.]com GET /0102s.bin

Followup malware for Ficker Stealer

8.209.78[.]68 port 80 - bobcatofredding[.]com - GET /6lavfdk.exe

Cobalt Strike traffic:

- 192.254.79[.]71 port 8080 23.106.80[.]14:1080 GET /EbHm
- 192.254.79[.]71 port 8080 23.106.80[.]14:1080 GET /ptj
- 192.254.79[.]71 port 8080 23.106.80[.]14:1080 POST /submit.php?id=242569267
- 192.254.79[.]71 port 443 HTTPS traffic

Ficker Stealer traffic:

- port 80 api.ipify.org GET /?format=xml
- 185.100.65[.]29 port 80 sweyblidian[.]com TCP traffic

As we discussed in our previous example, if you see HTTP POST requests with /submit.php?id= from Cobalt Strike, be alert for indicators of additional malware. Also like our previous example, we cannot find the malware binary in the pcap, so we must identify followup malware by its post-infection traffic.

In this case, we find indicators for NetSupport Manager RAT malware.

This RAT first does an IP address check to the domain geo.netsupportsoftware[.]com . Then it generates traffic with NetSupport Manager as part of the User-Agent string in its HTTP request headers.

Search for this traffic by using the following Wireshark display filter:

http.user_agent contains "NetSupport Manager" or http.host contains netsupport

The results should look similar to Figure 43 below:

-	Example-4-2021-02-02-Hancitor-infection.pcap	- + x					
File Edit View Go Capture Analyze Statistics	Telephony Wireless Tools Help						
🛚 http.user_agent contains "NetSupport Manager" or http.host contains netsupport							
Time Dst	port Host	Info					
2021-02-02 16:34 62.172.138.35	80 geo.netsupportsoftware.com	GET /location/loca.asp HTTP/1.1					
2021-02-02 16:34 46.17.106.230	3543 46.17.106.230	POST http://46.17.106.230/fakeurl.htm H					
2021-02-02 16:34 46.17.106.230	3543 46.17.106.230	POST http://46.17.106.230/fakeurl.htm H					
2021-02-02 16:34 46.17.106.230	3543 46.17.106.230	POST http://46.17.106.230/fakeurl.htm H					
2021-02-02 16:34 46.17.106.230	3543 46.17.106.230	POST http://46.17.106.230/fakeurl.htm H					
2021-02-02 16:35 46.17.106.230	3543 46.17.106.230	POST http://46.17.106.230/fakeurl.htm H					
•		•					

Figure 43. Traffic generated by NetSupport Manager RAT.

Traffic seen above in Figure 43 is:

- 62.172.138[.]35 port 80 geo.netsupportsoftware[.]com GET /location/loca.asp
- 46.17.106[.]230 port 3543 46.17.106[.]230 POST hxxp://46.17.106[.]230/fakeurl.htm

Follow the TCP stream for any of the HTTP POST requests to see what NetSupport Manager C2 traffic looks like. The results should look similar to Figure 44 below.

Þ

```
Wireshark · Follow TCP Stream (tcp.stream eq 286) · Example-4-2021-02-02-Hancitor-infection.pcap
                                                                                     - +
                                                                                        X
POST http://46.17.106.230/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:
                     22
Host: 46.17.106.230
Connection: Keep-Alive
CMD=POLL
INFO=1
ACK=1
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.7 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:
                     61
Connection: Keep-Alive
CMD=ENCD
ES=1
DATA=.g+$.{.. \....W.=M..;.p...w}..o.....
POST http://46.17.106.230/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:
                    240
Host: 46.17.106.230
Connection: Keep-Alive
CMD=ENCD
ES=1
DATA=u.2h.r..4.]..%y-....=I...D3.W.i.7?....=@....F.f....&t.[..
6ra..L.....@..B.....SB...9=M5T.m.<..z.v..$<...'...a....MQ..Y.....z.
8Up."..|..d..oA*.R.!...e.M......[.../~...v..P=n.k....}.M.....U.m..%...
5.?...T"...+..,.2
HTTP/1.1 200 OK
Server: NetSupport Gateway/1 7 (Windows NT)
900 client pkts, 253 server pkts, 492 turns.
Entire conversation (806 kB)
                                          Show and save data as ASCII
                                                                             Stream 286
Find:
                                                                                  Find Next
Help
                                       Filter Out This Stream
                                                          Print
                                                                  Save as...
                                                                            Back
                                                                                   × Close
```

Figure 44. TCP stream of NetSupport Manager RAT C2 traffic.

Of note, this tutorial only contains two examples of followup traffic from Cobalt Strike after a Hancitor infection. Cobalt Strike can be used to send other types of malware, not just a network ping tool or NetSupport Manager RAT.

So if you examine activity from a Hancitor infection with Cobalt Strike, we recommend you search for indicators from any other type of malware.

Conclusion

This tutorial reviewed how to identify Hancitor activity and its followup malware from pcaps of infection traffic. We reviewed five pcaps from four recent examples and found consistent patterns from the network traffic. These patterns are fairly unique and can be used to identify Hancitor activity and its associated malware within your network.

This knowledge can help security professionals better detect and catch Hancitor when reviewing suspicious network activity.

For more help with Wireshark, see our previous tutorials:

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our <u>Terms of Use</u> and acknowledge our <u>Privacy</u> <u>Statement</u>.