standalone quiz.

Cold as Ice: Answers to Unit 42 Wireshark Quiz for IcedID

unit42.paloaltonetworks.com/wireshark-quiz-icedid-answers/

Brad Duncan

May 30, 2023

By Brad Duncan

May 30, 2023 at 6:00 AM

Category: Tutorial

Tags: Advanced Threat Prevention, Advanced URL Filtering, banking trojans, BokBot, Cloud-Delivered Security Services, Cortex XDR, IcedID, next-generation firewall, pcap, WildFire, Wireshark, Wireshark Tutorial

Executive Summary Our introductory blog Cold as Ice: Unit 42 Wireshark Quiz for IcedID provides a packet capture (pcap) from an IcedID infection in April 2023. This blog provides the answers. Also known as Bokbot, IcedID is well-established Windows-based malware that can lead to ransomware.



If you would like to view this quiz without answers, please see our previous blog introducing the



Palo Alto Networks customers are protected from IcedID and other malware through <u>Cortex XDR</u> and our <u>Next-Generation Firewall</u> with <u>Cloud-Delivered Security Services</u> that include <u>WildFire</u>, <u>Advanced Threat Prevention</u> and <u>Advanced URL Filtering</u>.

Related Unit 42 Topics pcap, Wireshark, Wireshark Tutorial, IcedID, BokBot

Table of Contents

Scenario, Requirements and Quiz Material Quiz Questions Quiz Answers Pcap Analysis: IcedID Chain of Events Pcap Analysis: Infection Vector Pcap Analysis: IcedID Traffic Pcap Analysis: BackConnect Traffic Pcap Analysis: Victim Details Conclusion Indicators of Compromise Additional Resources

Scenario, Requirements and Quiz Material

Traffic for this quiz occurred in an Active Directory (AD) environment during April 2023. The infection is similar to previous IcedID activity <u>tweeted by Unit 42 in March 2023</u>. Details of the Local Area Network (LAN) environment for the pcap follow.

- LAN segment range: 10.4.19[.]0/24 (10.4.19[.]1 through 10.4.19[.]255)
- Domain: boogienights[.]live
- Domain controller IP address: 10.4.19[.]19
- Domain controller hostname: WIN-GP4JHCK2JMV
- LAN segment gateway: 10.4.19[.]1
- LAN segment broadcast address: 10.4.19[.]255

This quiz requires Wireshark, and we recommend using the <u>latest version of Wireshark</u>, since it has more features, capabilities and bug fixes over previous versions.

We also recommend readers customize their Wireshark display to better analyze web traffic. <u>A</u> <u>list of tutorials and videos is available</u>. As always, we recommend using Wireshark in a non-Windows environment like BSD, Linux or macOS when analyzing malicious Windows-based traffic.

To obtain the pcap, <u>visit our GitHub repository</u>, download the April 2023 ZIP archive and extract the pcap. Use *infected* as the password to unlock the ZIP archive.

Quiz Questions

For this IcedID infection, we ask participants to answer the following questions previously described in our <u>standalone quiz post</u>:

- What is the date and time in UTC the infection started?
- What is the IP address of the infected Windows client?
- What is the MAC address of the infected Windows client?
- What is the hostname of the infected Windows client?
- What is the user account name from the infected Windows host?
- Is there any follow-up activity from other malware?

Quiz Answers

The AD environment for this pcap contains three Windows clients, but only one was infected with IcedID.

Answers for this Wireshark quiz follow.

- Malicious traffic for this infection started on April 19, 2023, at 15:31 UTC.
- Infected Windows client IP address: 10.4.19[.]136
- Infected Windows client MAC address: 14:58:d0:2e:c5:ae
- Infected Windows client hostname: DESKTOP-SFF9LJF
- Infected Windows client user account name: csilva
- Follow-up activity: BackConnect traffic

Pcap Analysis: IcedID Chain of Events

To understand IcedID network traffic, you should understand the chain of events for an IcedID infection. A flow chart illustrating this chain of events is shown in Figure 1.



Most IcedID infections use a <u>standard variant</u> of IcedID. These infections typically use an EXE or DLL that acts as an installer. This installer generates an unencrypted HTTP GET request that retrieves a gzip-compressed binary. The installer then converts this binary into malware used for a persistent IcedID infection.

The newly created, persistent IcedID generates HTTPS traffic to communicate with command and control (C2) servers. The C2 activity can lead to <u>BackConnect</u> traffic, <u>Cobalt Strike</u> and <u>Virtual Network Computing (VNC)</u> activity.

If the infected host is part of a high-value environment, an IcedID infection would likely <u>lead to</u> <u>ransomware</u>.

Pcap Analysis: Infection Vector

Using Wireshark <u>customized from our tutorials</u>, apply a basic web filter to see if anything stands out. Review the results in your column display. Look for unencrypted HTTP traffic over TCP port 80 directly to an IP address without an associated domain. This is a common characteristic in the chain of events for various malware infections.

At 15:31:08 UTC, the host at 10.4.19[.]136 generated an HTTP GET request to hxxp://80.77.25[.]175/main.php as shown below in Figure 2.

•			2	023-04-Unit42-Wiresharl	k-quiz.pca	ар		- + ×
<u>File</u> <u>Edit</u> <u>Vie</u>	w <u>G</u> o <u>C</u> apture	Analyze Statistics	s Telephony <u>W</u> ir	eless <u>T</u> ools <u>H</u> elp				
	🗎 🗎 🛣 🎑	Q € ≯ 3 	→ 📃 🖿 🖬	8 0 11				
(http.reque	st or tls.handshal	(e.type eq 1) and !(ssdp)				🛛 🗖 🔸 basic	basic+ basic+dns
Time		Src	port	Dst	port	Host	Info	-
2023-04	4-19 15:26:	28 10.4.19	136 51089	51.104.162.168	443	array604.prod.d	Client Hello	
2023-04	4-19 15:26:	29 10.4.19	136 51090	13.107.42.16	443	config.edge.sky	Client Hello	
2023-04	4-19 15:26:	29 10.4.19	136 51091	13.107.42.16	443	config.edge.sky	Client Hello	
2023-04	4-19 15:27:	09 10.4.19	136 51092	20.42.65.85	443	v10.events.data	Client Hello	
2023-04	4-19 15:27:	29 10.4.19	.136 51093	51.104.167.186	443	array607.prod.d	Client Hello	
2023-04	4-19 15:27:	55 10.4.19	136 51094	204.79.197.203	443	windows.msn.com	Client Hello	
2023-04	4-19 15:28:	34 10.4.19	136 51095	40.126.24.84	443	login.live.com	Client Hello	
2023-04	4-19 15:28:	35 10.4.19	136 51096	52.137.106.217	443	settings-win.da	Client Hello	
2023-04	4-19 15:28:	35 10.4.19	136 51097	23.47.50.132	80	adl.windows.com	GET /appraise	rad1/2023
2023-04	4-19 15:28:	38 10.4.19	.136 51098	52.254.114.65	443	fe2cr.update.mi	Client Hello	
2023-04	4-19 15:28:	40 10.4.19	.136 51099	20.242.39.171	443	fe3cr.delivery	Client Hello	
2023-04	4-19 15:28:	41 10.4.19	136 51100	104.208.16.89	443	v10.events.data	Client Hello	
2023-04	4-19 15:28:	43 10.4.19	136 51101	104.208.16.89	443	v10.events.data	Client Hello	
2023-04	4-19 15:30:	41 10.4.19	.136 51108	40.126.28.23	443	login.microsoft	Client Hello	
2023-04	4-19 15:30:	43 10.4.19	.136 51109	142.251.46.131	443	update.googleap	Client Hello	
2023-04	4-19 15:30:	43 10.4.19	136 51110	204.79.197.200	443	edgeservices.bi	Client Hello	
2023-04	4-19 15:31:	07 10.4.19	136 51111	204.79.197.203	443	www.msn.com	Client Hello	
2023-04	4-19 15:31:	08 10.4.19	.136 51112	80.77.25.175	80	80.77.25.175	GET /main.php	HTTP/1.1
2023-04	4-19 15:31:	08 10.4.19	.136 51113	23.221.22.200	443	assets.msn.com	Client Hello	
2023-04	4-19 15:31:	09 10.4.19	.136 51114	204.79.197.239	443	edge.microsoft	Client Hello	
2023-04	4-19 15:31:	09 10.4.19	.136 51115	204.79.197.203	443	www.msn.com	Client Hello	
2022 0	1 10 15.21.	00 10 1 10	106 E1116	22 221 22 21E	112	accete men com	Client Helle	

Figure 2. Suspicious HTTP traffic directly to an IP address shown in Wireshark. Follow the TCP stream for this HTTP GET request, as shown in Figure 3. This should generate a window for TCP stream 32, as shown in Figure 4.

•			20	23-04-Unit4	2-Wireshark-	quiz.pc	ар				- + ×
<u>File Edit Vie</u>	w <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tati	stics Telepho	ny <u>W</u> ire	less <u>T</u> ools	Help						
	📄 🛅 🖹 🙆 🔍 🗧 🗦 🔇	₩ ₩ 💻	0 6								
(http.requ	Mark/Unmark Packet	Ctrl+M						\times	• • basic	basic+ bas	sic+dns
Time	Ignore/Unignore Packet	Ctrl+D	rt	Dst		port	Host	Info			-
2023-	Set/Unset Time Reference	Ctrl+T	L089	51.104.	162.168	443	array604.prod.d	Client	Hello		
2023-	Time Shift	Ctrl+Shift+T	L090	13.107.	42.16	443	config.edge.sky	Client	Hello		
2023-	Packet Comments	,	L091	13.107.	42.16	443	config.edge.sky…	Client	Hello		
2023-			L092	20.42.6	55.85	443	v10.events.data	Client	Hello		
2023-	Edit Resolved Name		L093	51.104.	167.186	443	array607.prod.d	Client	Hello		
2023-	Apply as Filter	,	L094	204.79.	197.203	443	windows.msn.com	Client	Hello		
2023-	Prepare as Filter	,	L095	40.126.	24.84	443	login.live.com	Client	Hello		
2023-	Conversation Filter	,	1096	52.137.	106.217	443	settings-win.da	Client	Hello		
2023-	Colorize Conversation		1097	23.47.5	114 65	80	adl.windows.com	GEI /a	ppraiser	ad 1/2023	5
2023-	colorize conversation		1098	52.254.	20 171	443	felor delivery	Client	Hello		
2023-	SCIP	,	1099	20.242.	.39.171	443	v10 ovents data	Client	Hello		
2023-	Follow		TCP	Stream	Ctrl+Alt+Sh	ift+T	v10.events.data	Client	Hello		
2023-	Сору		UDP	Stream	trl+Alt+Sh	ift+U	login microsoft	Client	Hello		
2023-	Protocol Preferences	,	DCC	P Stream	Ctrl+Alt+Sh	ift+E	undate.googlean	Client	Hello		
2023-	Decede As		TIS	Stream	Ctrl+Alt+Sh	ift+S	edgeservices.bi	Client	Hello		
2023-	Decode As			Dicture	Ctul: Alt: Ch		www.msn.com	Client	Hello		
→ 2023-	Show Packet in New Window	10.100 0	нп	P Stream	Ctri+Alt+Sh	ITT+H	80.77.25.175	GET /ma	ain.php	HTTP/1.1	
2023-04	19 15:31:08 10.4.	19.136 5	HTT	P/2 Stream			assets.msn.com	Client	Hello		
2023-04	19 15:31:09 10.4.	19.136 5	QUI	C Stream			edge.microsoft	Client	Hello		
2023-04	4-19 15:31:09 10.4.	19.136 5	SIP	Call			www.msn.com	Client	Hello		
2022 0	1 10 15:21:00 10 1	10 106 5	1116	11 114	11 115	110	accete men com	Client	110110		v

Figure 3. Following TCP stream for suspicious HTTP GET request.

 Wireshark · Follow TCP Stream (tcp.stream eq 32) · 2 	2023-04-Unit42-Wireshark-quiz.pcap – + ×
GET /main.php HTTP/1.1 Host: 80.77.25.175 Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win (KHTML, like Gecko) Chrome/112.0.0.0 Safari/3 Accept: text/html,application/xhtml+xml,appl apng,*/*;q=0.8,application/signed-exchange;v Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: _subid=17dk1e9d14f; 34ab8=eyJ0eXAi0iJKV1QiLCJhbGci0iJIUzI1NiJ9.ey OFwi0jE20DE5MTc2NDF9LFwiY2FtcGFpZ25zXCI6e1win xNjgxOTE3NjQxfSJ9.9LQV07Pp3-oH0HEmBnzaa7p8B8	<pre>n64; x64) AppleWebKit/537.36 537.36 Edg/112.0.1722.48 ication/xml;q=0.9,image/webp,image/ =b3;q=0.7 yJkYXRhIjoie1wic3RyZWFtc1wiOntcIjIz NTBcIjoxNjgxOTE3NjQxfSxcInRpbWVcIjo jot16pqisEvgs-bII</pre>
HTTP/1.1 302 Moved Temporarily Server: nginx Date: Wed, 19 Apr 2023 15:31:10 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive Set-Cookie: PHPSESSID=ocno7kgfbvjnu3lho0d6pf Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-reva Pragma: no-cache	tkge; path=/ lidate
<pre>Set-Cookie: 34ab8=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey 0FwiOjE20DE5MTc2NDEsXCIyNDJcIjoxNjgxOTE4MjY5 4MTkxNzY0MSxcIjUxXCI6MTY4MTkxODI2OX0sXCJ0aW1 G57F6kgyLIVMTXRyC6IxVuv5x1u7t8L8; expires=Th Age=86400; path=/ Set-Cookie: _subid=17dk1e9d14g; expires=Thu, Age=86400; path=/ Location: https://firebasestorage.googleapis</pre>	yJkYXRhIjoie1wic3RyZWFtc1wiOntcIjIz fSxcImNhbXBhaWduc1wiOntcIjUwXCI6MTY lXCI6MTY4MTkxNzY0MX0ifQ.ebZVp9IxEPe u, 20-Apr-2023 15:31:10 GMT; Max- 20-Apr-2023 15:31:10 GMT; Max-
cathode-377701.appspot.com/o/XSjwp600pq%2FScalt=media&token=a716bdce-1373-44ed-ae89-fdab	an_Inv.zip? afa31c61
Entire conversation (1,637 bytes) Show data as	ASCII - Stream 32
Find:	Find <u>N</u> ext
Help Filter	Out This Stream Print Save as Back × Close

Figure 4. TCP stream for the suspicious HTTP GET request and response.

Figure 4 reveals HTTP request headers that contain a User-Agent string ending with Edg/112.0.1722.48. This string indicates the traffic was likely generated by the Microsoft Edge browser. However, web traffic generated by malware can spoof different User-Agent strings, and some browser extensions also have this ability, so we cannot be certain this was actually Microsoft Edge.

The HTTP response headers in Figure 4 show a 302 code, redirecting traffic to the following URL:

hxxps://firebasestorage.googleapis[.]com/v0/b/serene-cathode-377701.appspot.com/o/XSjwp6O0pq%2FScan_Inv.zip?alt=media&token=a716bdce-1373-44edae89-fdabafa31c61

This Firebase Storage URL has been reported as malicious by at least seven security vendors <u>on</u> <u>VirusTotal</u>, and it <u>appears in URLhaus</u> tagged as IcedID. Fortunately, Google has taken the URL offline, and it is no longer active.

To further refine our search, add the client's IP address 10.4.19[.]136 to the basic web filter as shown below in Figure 5. This reveals HTTPS traffic to firebasestorage.googleapis[.]com shortly after traffic to the initial URL at hxxp://80.77.25[.]175/main.php.

<	2023-04-Unit4	I2-Wireshark-quiz.pcap		- + ×
<u>File Edit View Go Capture Analyze Statis</u>	stics Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp		
	**			
(http.request or tls.handsh	ake.type eq 1) a	nd !(ssdp) and ip.addr eq 10.4.19.1	36 Jasic bas	sic+ basic+dns
Time Dst	port	Host	Info	·
2023-04-19 15:28:34 40.126	6.24.84 443	login.live.com	Client He	llo
2023-04-19 15:28:35 52.137	7.106.217 443	settings-win.data.microsoft.com	Client He	llo
2023-04-19 15:28:35 23.47	.50.132 80	adl.windows.com	GET /appr	aisera
2023-04-19 15:28:38 52.254	4.114.65 443	fe2cr.update.microsoft.com	Client He	llo
2023-04-19 15:28:40 20.242	2.39.171 443	fe3cr.delivery.mp.microsoft.com	Client He	llo
2023-04-19 15:28:41 104.20	98.16.89 443	v10.events.data.microsoft.com	Client He	llo
2023-04-19 15:28:43 104.20	98.16.89 443	v10.events.data.microsoft.com	Client He	llo
2023-04-19 15:30:41 40.126	5.28.23 443	login.microsoftonline.com	Client He	llo
2023-04-19 15:30:43 142.25	51.46.131 443	update.googleapis.com	Client He	llo
2023-04-19 15:30:43 204.79	9.197.200 443	edgeservices.bing.com	Client He	llo
2023-04-19 15:31:07 204.79	9.197.203 443	www.msn.com	Client He	llo
2023-04-19 15:31:08 80.77	.25.175 80	80.77.25.175	GET /main	.php 🦛 🗩 🗩
2023-04-19 15:31:08 23.221	1.22.200 443	assets.msn.com	Client He	llo
2023-04-19 15:31:09 204.79	9.197.239 443	edge.microsoft.com	Client He	llo
2023-04-19 15:31:09 204.79	9.197.203 443	www.msn.com	Client He	llo
2023-04-19 15:31:09 23.221	1.22.215 443	assets.msn.com	Client He	llo
2023-04-19 15:31:09 104.95	5.45.223 443	ecn.dev.virtualearth.net	Client He	llo
2023-04-19 15:31:13 209.19	97.3.8 80	<pre>msedge.b.tlu.dl.delivery.mp.micr</pre>	HEAD /fil	estrea
2023-04-19 15:31:13 209.19	97.3.8 80	<pre>msedge.b.tlu.dl.delivery.mp.micr</pre>	GET /file	stream
2023-04-19 15:31:14 142.25	51.32.234 443	firebasestorage.googleapis.com	Client He	llo
2023-04-19 15:31:14 142.25	51.32.234 443	firebasestorage.googleapis.com	Client He	llo
2023-04-19 15:31:16 209.19	97.3.8 80	msedge.b.tlu.dl.delivery.mp.micr	GET /file	stream -

Figure 5. HTTPS traffic to firebasestorage.googleapis[.]com after the initial suspicious URL.Follow the TCP stream for the initial frame showing fire in the Wireshark column display. The TCP stream reveals 273 KB of data sent from the server to the Windows host, as shown below in Figure 6. This indicates a file might have been sent to the Windows host.



Figure 6. TCP stream showing 275 KB of data sent from firebasestorage.googleapis[.]com to the Windows host.While the Firebase Storage URL is <u>tagged as IcedID on URLhaus</u>, this only indicates a distribution method for the IcedID installer. Based on this pcap, the victim opened a link that led to the Firebase Storage URL, and that URL delivered a file for an IcedID installer. The <u>URLhaus entry for this Firebase Storage URL</u> reveals the ZIP archive it previously hosted, as shown in Figure 7.

(O A	a https://urinaus.abuse.cn/uri/2614322/		ω	
	US ₇ abuse th		Browse AF	PI Feeds	Statistic	s About
- Reporter:	@1	malware_tra	ffic			
Abuse comp sent (?):	laint 🔁	Yes (2023-04	I-20 02:43:04 UTC to network-abuse{at}google[dot]com)			
Tags:	bo	okbot exe I	cedID 🗷 zip			
Tags: Dayloac	d deliv	exe (CETY nts all paylo	ads that URLhaus retrieved from this particular URL.			3
Tags: Dayload The table belo	d deliv w documer Filename	exe (CTY nts all paylo File Type	ads that URLhaus retrieved from this particular URL.	VT	Bazaar	Signature

Figure 7. URLhaus entry for our firebasestorage URL shows it delivered a zip archive.

The ZIP archive was <u>submitted to Malware Bazaar</u>. The archive is password-protected with the ASCII string *1235*, and it contains a file named Scan_Inv.exe. This Windows executable file is an IcedID installer.

Pcap Analysis: IcedID Traffic

An IcedID loader first generates an unencrypted HTTP GET request over TCP port 80 to a domain using GET / without any further URL. This returns a gzip binary used by the installer to create the persistent malware on the victim's host.

To find the gzip binary, use the same basic web filter with the victim's IP address noted earlier in Figure 5. Scroll down to an HTTP GET request to skigimeetroc[.]com at 15:35:39 UTC and follow the TCP stream as shown below, in Figure 8.

File Edit View Go Capture Analyze Statistics Telephon Image: Statistic Statistic Image: Statistic Statistic Image: Statistic Statistic Image: Statistic Statistic Image: Statistic Statistic	23-04-Ui iy <u>W</u> irel	nit42-Wireshark-quiz.pcap less Tools Help		Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference	Ctrl+M Ctrl+D Ctrl+T Ctrl+Shift+T		
Inttp.request or tis.nandsnake.type	eq 1)	and !(ssop) and ip	.addr eq 10.4.19	Packet Comments	,		
Time Dst	port	Host	Info	Edit Resolved Name			
2023-04-19 15:32:19 23.36.63.240	80	go.microsoft.com	POST /fwlink/?				
2023-04-19 15:32:19 20.231.121.79	80	dmd.metaservices	POST /metadata	Apply as Filter	•		
2023-04-19 15:32:19 23.36.63.240	80	go.microsoft.com	POST /fwlink/?	Prepare as Filter	5.		
2023-04-19 15:32:19 20.231.121.79	80	dmd.metaservices	POST /metadata	Conversation Filter			
2023-04-19 15:32:19 13.71.55.58	443	settings-win.dat	Client Hello	Colorize Conversation			
2023-04-19 15:32:20 23:30:03:240	80	dmd motocorvicos	POST / TWLINK/ ?	SCTR			
	80	uniu metaservices	CET (ropositor	SCIF			
2023-04-19 15:35:30 192 153 57 233	80	skigimeetroc.com	GET / HTTP/1 1	Follow		ICP Stream	Ctri+Alt+Shift+1
2023-04-19 15:36:41 104 168 53 18	443	askamoshonsi com	Client Hello	Сору	×	UDP Stream	Ctrl+Alt+Shift+U
2023-04-19 15:36:43 104 168 53 18	443	askamoshopsi.com	Client Hello	Protocol Preferences	*	DCCP Stream	Ctrl+Alt+Shift+E
2023-04-19 15:36:43 104.168.53.18	443	askamoshopsi.com	Client Hello	Decode As		TLS Stream	Ctrl+Alt+Shift+S
2023-04-19 15:36:44 217.199.121.56	443	skansneksskv.com	Client Hello	Chow Dasket in New Window		HTTP Stream	Ctrl+Alt+Shift+H
2023-04-19 15:38:45 20.189.173.13	443	self.events.data	Client Hello	Show Packet in New window	-		curracioniterri
2023-04-19 15:39:14 40.126.24.83	443	login.live.com	Client Hello			HTTP/2 Stream	
2023-04-19 15:39:16 40.126.24.83	443	login.live.com	Client Hello			QUIC Stream	
2023-04-19 15:39:16 40.119.249.228	443	settings-win.dat	Client Hello			SIP Call	
2023-04-19 15:41:27 13.89.179.8	443	v10.events.data	Client Hello				
2023-04-19 15:41:28 13.89.179.8	443	v20.events.data	Client Hello				
2023-04-19 15:41:43 217.199.121.56	443	skansnekssky.com	Client Hello				
2023-04-19 15:42:59 204.79.197.203	443	windows.msn.com	Client Hello				
2023-04-19 15:42:59 20.54.24.69	443	array610.prod.do	Client Hello		w		

Figure 8. Following the TCP stream for IcedID installer's initial HTTP GET request.

This is TCP stream 53 from the pcap, as shown below in Figure 9. The HTTP request headers for traffic generated by the IcedID installer have no User-Agent string. Note the cookie sent in the request headers in Figure 9.



Figure 9. HTTP GET request generated by the IcedID installer.

The cookie line follows:

Cookie: __gads=422998217:1:1808:131; _gid=A0CA96894E9D;

_u=4445534B544F502D534646394C4A46:6373696C7661:46353431423635424230383346354633; __io=21_1181811818_1193560798_2439418475; _ga=1.591597.1635208534.1022; _gat=10.0.22621.64

<u>Cookie parameters</u> for the HTTP GET request caused by this IcedID installer follow:

- ___gads= IcedID campaign identifier and information from the infected host.
- _gid= Value calculated using MAC address of the infected host.
- _u= ASCII text representing hex values of the victim's hostname, Windows user account name and another undetermined value.
- ____io= Domain identifier from the infected host's security identifier (SID).
- _ga= Information based on the infected host's CPU.
- _gat= Windows version. For example, 10.0.22621.64 is an identifier for 64-bit Windows 11 version 22H2 and 10.0.19045.64 is an identifier for 64-bit Windows 10 version 22H2.

These cookie parameters are unique to IcedID infections. You can identify this traffic as IcedID without understanding the values. However, the _u= parameter reveals the victim's hostname and Windows user account name. This information is very useful for our investigation. These hex values translate to a hostname of DESKTOP-SFF9LJF and a Windows user account name of csilva, as shown below in Figure 10.



Using the _u= cookie parameter to determine the victim's hostname and Windows user account name.

After retrieving the gzip binary, an IcedID installer creates persistent IcedID malware that takes over the infection. The infected Windows host then starts generating HTTPS traffic to IcedID C2 servers.

These C2 servers use different domain names and IP addresses than the initial domain contacted by the IcedID installer. IcedID's HTTPS C2 traffic starts within a minute or two after the installer retrieves the gzip binary, and this activity uses at least two domains with random alphabetic names.

Our pcap reveals HTTPS traffic from the infected host to two domains after skigimeetroc[.]com at 15:35:39 UTC. These HTTPS C2 servers are askamoshopsi[.]com on 104.168.53[.]18 and skansnekssky[.]com on 217.199.121[.]56.

To find these servers, use the same basic web filter with the victim's IP address noted earlier in Figure 5. HTTPS traffic starting at 15:36:41 UTC reveals these domains, as shown below in Figure 11.

	202	3-04-Ur	hit42-Wireshark-quiz.pcap	-	+ ×
<u>File Edit View Go</u> Capture Ana	lyze Statistics Telephony	<u>Wirel</u>	ess Tools Help	dID installer retrieves azin hin	oni
	+ > < + >	• •		and installer retrieves gzip bin	ary
(http.request or tls.h	andshake.type e	eq 1)	and !(ssdp) and ip.	addr eq 10.4.19.136 asic basic basic	+dns
Time	Dst	port	Host	Info	^
2023-04-19 15:32:19	20.231.121.79	80	dmd.metaservices	POST /metadata.svc HTTP 1.1	
2023-04-19 15:32:19	23.36.63.240	80	go.microsoft.com	POST /fwlink/?LinkID=7/2669&clc.	
2023-04-19 15:32:19	20.231.121.79	80	dmd.metaservices	POST /metadata.svc H /P/1.1	M
2023-04-19 15:32:19	13.71.55.58	443	settings-win.dat	Client Hello	
2023-04-19 15:32:20	23.36.63.240	80	go.microsoft.com	POST /fwlink/?Lin [/] 1D=252669&clc.	
2023-04-19 15:32:20	20.231.121.79	80	dmd.metaservices	POST /metadata c HTTP/1.1	
2023-04-19 15:34:33	54.145.90.68	80	www.ssl.com	GET /repositor SSLcom-RootCA-E	
2023-04-19 15:35:39	192.153.57.233	80	skigimeetroc.com	GET / HTTP/1.1	
2023-04-19 15:36:41	104.168.53.18	443	askamoshopsi.com	Client Hello	
2023-04-19 15:36:43	104.168.53.18	443	askamoshopsi.com	Client Hello	
2023-04-19 15:36:43	104.168.53.18	443	askamoshopsi.com	Client Hello	
2023-04-19 15:36:44	217.199.121.56	443	skansnekssky.com	Client Hello	
2023-04-19 15:38:45	20.189.173.13	443	self.events.data	Client Hello Servers	
2023-04-19 15:39:14	40.126.24.83	443	login.live.com	Client Hello	
2023-04-19 15:39:16	40.126.24.83	443	login.live.com	Client Hello	
2023-04-19 15:39:16	40.119.249.228	443	settings-win.dat…	Client Hello	
2023-04-19 15:41:27	13.89.179.8	443	v10.events.data	Client Hello	
2023-04-19 15:41:28	13.89.179.8	443	v20.events.data	Client Hello	
2023-04-19 15:41:43	217.199.121.56	443	skansnekssky.com	Client Hello	
2023-04-19 15:42:59	204.79.197.203	443	windows.msn.com	Client Hello	
2023-04-19 15:42:59	20.54.24.69	443	array610.prod.do	Client Hello	
2023-04-19 15:44:21	20.54.25.4	443	array616.prod.do	Client Hello	
2023-04-19 15:46:45	217.199.121.56	443	skansnekssky.com	Client Hello	
2023-04-19 15:51:47	217.199.121.56	443	skansnekssky.com	Client Hello	
2023-04-19 15:54:07	40.119.249.228	443	settings-win.dat	Client Hello	
2023-04-19 15:56:49	217.199.121.56	443	skansnekssky.com	Client Hello	-

Figure 11. HTTPS C2 traffic after HTTP request by the IcedID installer.

Both C2 servers at askamoshopsi[.]com and skansnekssky[.]com use self-signed certificates for their HTTPS traffic. Self-signed certificates for HTTPS traffic will generate warnings about potential security risks when the site is viewed in any modern web browser.

Why do web browsers display warnings about websites that use self signed certificates? Because these are not validated by a <u>Certificate Authority</u>. Criminals can generate self-signed certificates that impersonate an existing company, or they can use generic values for the certificate issuer. Without a validated certificate, web browsers cannot be sure a website is what it says it is.

Figure 12 shows what the server at askamoshopsi[.]com looked like when we attempted to view it with the Firefox web browser. This warning allows users to view the server's self-signed certificate.

$\leftarrow \ \rightarrow \ G$	A Not Secure https://askamoshopsi.co	m		☆	\bigtriangledown	එ ≡			
	Warning: Potential Security Risk A Firefox detected a potential security threat and did visit this site. attackers could try to steal informatio	head not continue n like your p	e to askam o asswords, e	oshopsi.com . If yo emails, or credit ca	u rd				
	details.	-		Cer	ificate for	ocalhost	— Mozilla Firefox	-	÷
	Learn more	e Ce	ertificate fo	r localho × +					
		c ← →	C	Sirefox abo	out:certifica	te?cert=N	MIIDgzCCAmugAwIBAgIEZnED ☆	٢	
-	askamoshopsi.com uses an invalid security certificate The certificate is not trusted because it is self-signed	e.	Certific	ate		localho	ost		
	Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CEF	me		Subject Name Common Name Country State/Province Organization	localhost AU Some-State Internet Wig	lgits Pty Ltd			
avascript:void	(0)	1		Issuer Name Common Name Country State/Province Organization	localhost AU Some-State Internet Wig	laits Ptv Ltd			

Figure 12. Attempting to view the web server at askamoshopsi[.]com using Firefox.As shown above in Figure 12, the certificate uses values like Internet Widgits Pty Ltd for the issuer's Organization name and Some-State for the State/Province name. Values for self-signed certificates used by IcedID C2 servers are the same default values seen when <u>using OpenSSL to create a certificate</u> in Xubuntu as shown below in Figures 13 and 14.

-			Termina	al - xubuntu-user@xubuntu-vm: ~/Desktop	- + ×
File	Edit	View	Terminal	Tabs Help	
xubu	ntu-	user(g <mark>xubuntu</mark>	<pre>-vm:~/Desktop\$ openssl req -x509 -nodes</pre>	-days
365	-ne	wkey	rsa:204	8 -keyout server.key -out server.crt	U
• • • •	• • • •	••••	.++	+.+++++.+.+.++.	+.
+.	••••	+	+++++	+++++++++++++++++++++++++++++++++++++++	++++
++++	++++	++++	++++*.+.	+++	• • • • •
.+	••••	••••	•• •	+++++++++++++++++++++++++++++++++++++++	+++++
++++	++++	****	++*+	++++++++	+

Figure 13. Creating an x509 certificate for a web server using OpenSSL in Xubuntu.



Figure 14. Default values when creating an x509 certificate for a web server using OpenSSL in Xubuntu.

Since Internet Widgits Pty Ltd is a default value for a self-signed certificate in HTTPS traffic, and this value is sometimes seen in C2 traffic for malware. This should be more closely examined if it's found when investigating a suspected malware infection. We can easily check any pcap for this value using the following Wireshark filter:

x509sat.uTF8String eq "Internet Widgits Pty Ltd"

The results from our pcap reveal the same IP addresses used by IcedID C2 servers for askamoshopsi[.]com at 104.168.53[.]18 and skansnekssky[.]com at 217.199.121[.]56. Expand the frame details for any of the results to find the same certificate issuer data, as shown in Figure 15.





Organization name shown in Wireshark.

This certificate data is not unique to IcedID. The same values for self-signed certificates are also seen in HTTPS C2 traffic by other malware families like <u>Bumblebee</u>.

Pcap Analysis: BackConnect Traffic

Undetected IcedID infections lead to follow-up activity like <u>BackConnect</u> traffic.

For the past several months, BackConnect traffic caused by IcedID was easy to detect because it occurred over TCP port 8080. However, as early as April 11, 2023, BackConnect activity for IcedID changed to TCP port 443, making it harder to find.

This BackConnect activity from IcedID <u>Unit 42 tweeted on April 11, 2023</u> used an IP address of 193.149.176[.]100 over TCP port 443. Filter for that IP address in Wireshark and combine it with tcp.flags eq 0x0002 as shown below, in Figure 16. This reveals the beginning of three streams.

·	2023	-04-Unit42-	Wireshark-quiz.pcap			-	+ ×
<u>File Edit View Go Capture Ana</u>	lyze <u>Statistics</u> Telep	hony Wire	eless <u>T</u> ools <u>H</u> elp				
ip.addr eq 193.149.1	76.100 and to	p.flags	eq 0x0002	×	💶 🔸 basic basi	c+ basic+	-dns
Time	Src	port	Dst	port	Info		
2023-04-19 20:48:00	10.4.19.136	51534	193.149.176.100	443	51534 → 443	[SYN]	Seq
2023-04-19 20:49:11	10.4.19.136	51535	193.149.176.100	443	51535 → 443	[SYN]	Seq
2023-04-19 20:49:33	10.4.19.136	51537	193.149.176.100	443	51537 → 443	[SYN]	Seq
4							•

Figure 16. Filtering in Wireshark for BackConnect traffic in our pcap.

Follow the TCP stream for the first result, which is TCP stream 950. This stream reveals encoded or otherwise encrypted TCP traffic, as shown in Figure 17.



Figure 17. The first TCP stream for BackConnect activity.

Go back to the Wireshark filter used to reveal the TCP streams to 193.149.176[.]100. Follow the TCP stream for the second frame in the results, which is TCP stream 951. This reveals encoded or encrypted data followed by a command to reveal all hosts under the domain controller for boogienights[.]live as shown below, in Figure 18.

Wireshark · Follow TCP Stream (tcp.stream eq 951) · 2023-04-Unit42-Wireshark-quiz.pcap - + ×
<pre></pre>
<pre>c:\>net group "Domain Computers" /domain</pre>
net group "Domain Computers" /domain The request will be processed at a domain controller for domain boogienights.live.
Group name Domain Computers Comment All workstations and servers joined to the domain
Members
DESKTOP-JAL4D68\$ DESKTOP-RETP4BU\$ DESKTOP-SFF9LJF\$ The command completed successfully.
c: \> c: \>
15 client pkts, 3 server pkts, 6 turns.
Entire conversation (768 bytes) Show data as ASCII Stream 951
Find: Find Next
Save as Back * Close

Figure 18. BackConnect traffic with a command to and results enumerating the victim's AD environment.

The response to this command enumerates the victim's AD environment, showing three clients logged in to the domain:

- DESKTOP-JAL4D68
- DESKTOP-RETP4BU
- DESKTOP-SFF9LJF

Go back to the Wireshark filter used to reveal the TCP streams to 193.149.176[.]100. Follow the TCP stream for the last frame in the results, which is TCP stream 953. This lists disk drives on the victim client, and it provides a directory listing for each of these drives, as shown below in Figure 19.

The C:\ drive is the victim's system drive. Z:\ is likely a mapped drive from a server's shared directory that does not contain any files.



Figure 19. BackConnect traffic showing contents of the victim's system drive and mapped drive. Previous IcedID infections reveal this threat can use BackConnect traffic to load and run Cobalt Strike. We tweeted about <u>one such case from March 24, 2023</u>. However, this pcap does not contain any indicators of Cobalt Strike.

Previous IcedID infections also reveal this threat can generate VNC traffic over the same IP address used by BackConnect traffic. This happened during the <u>same IcedID infection from</u> <u>March 24, 2023</u>.

Pcap Analysis: Victim Details

The common internal IP address for the malicious traffic we have reviewed is 10.4.19[.]136. This is our victim's IP address. To find the Windows user account name, filter on that IP address and kerberos.CNameString as shown in Figure 20.

2025-04-0111042-001103110110-90	iiz.pcap		- + ×
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>	0		
<u> </u>			
ip.addr eq 10.4.19.136 and kerberos.CNameString		🛛 🗖 🔹 ba	asic basic+ basic+dns
Time Src port Dst	port	CNameString	Info
2023-04-19 19:30:50 10.4.19.136 51424 10.4.19.	19 88	csilva	AS-REQ
2023-04-19 19:30:50 10.4.19.136 51425 10.4.19.	19 88	csilva	AS-REQ
2023-04-19 19:30:56 10.4.19.136 51426 10.4.19.	19 88	csilva	AS-REQ
2023-04-19 19:30:56 10.4.19.136 51427 10.4.19.	19 88	csilva	AS-REQ
2023-04-19 19:30:56 10.4.19.19 88 10.4.19.	136 51427	csilva	AS-REP
2023-04-10 10·30·56 10 4 10 10 88 10 4 10	136 51428	csilva	TGS-REP
• Frame 36053: 284 bytes on wire (2272 bits), 284 byt	es captured (2	2272 b ts)	A
Ethernet II, Src: HewlettP_2e:c5:ae (14:58:d0:2e:c5) Internet Protocol Version 4 Src: 10 4 10 126 Det.	5:ae), Dst: Hew	wlettP 86:39	:8f (00:21:5a:8
Transmission Control Protocol Src Port: 51424 Dst	10.4.19.19 Port: 88 Se	$r \cdot 1$ lock $\cdot 1$	len: 230
- Kerberos 🔶		1. I, IOK. I	, 200
Record Mark: 226 bytes			
- as-req 🔶			
pvno: 5			
msg-type: krb-as-req (10)			
padata: 1 item			
Padding: 0			
kdc options: 40810010			
chame			
name-type: kRB5-NT-PRINCIPAL (1)			
- cname-string: 1 item			
CNameString: csilva	Expand Subtract		
realm: BOOGIENIGHTS	Expand Subtrees		
- Sname	Collapse Subtrees		
	Expand All		
	Collapse All		
	Apply as Column	100 C 100	
	rippiy us column		Ctrl+Shift+I
	Apply as Filter	д	Ctrl+Shift+I
	Apply as Filter Prepare as Filter	3	Ctrl+Shift+I ,
	Apply as Filter Prepare as Filter Conversation Filter	4	Ctrl+Shift+I , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter	4	Ctrl+Shift+I , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow	3	Ctrl+Shift+I , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy	9	Ctrl+Shift+I
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes		Ctrl+Shift+I , , , , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes		Ctrl+Shift+I
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Wiki Protocol Page	(Ctrl+Shift+I , , , , , , , , , , , , , , , , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Wiki Protocol Page Filter Field Beferen		Ctrl+Shift+I , , , , , , , , , , , , , , , , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Export Packet Byte Wiki Protocol Page Filter Field Referen Protocol Preference	(s (ce es	Ctrl+Shift+I , , , , , , , , , , , , , , , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Export Packet Bytes Wiki Protocol Page Filter Field Referen Protocol Preference Decode As	() s () ce es	Ctrl+Shift+I
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Export Packet Bytes Wiki Protocol Page Filter Field Referen Protocol Preference Decode <u>A</u> s		Ctrl+Shift+I , , , , , , , , , , , , , , , , , , ,
	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow Copy Show Packet Bytes Export Packet Bytes Export Packet Bytes Wiki Protocol Page Filter Field Referen Protocol Preference Decode <u>A</u> s Go to Linked Packet	() s () ce es	Ctrl+Shift+I , , , , , , , , , , , , , , , , , , ,

Figure 20. Finding the Windows user account name for our infected Windows host.

In some cases, lightweight directory access protocol (LDAP) might also provide the full name of the user. Use the following Wireshark filter:

Idap.AttributeDescription == "givenName"

This should provide four frames in our column display. Select any of them and expand the frame details until you find the user's full name, Cornelius Silva, as shown below in Figure 21.

 2023-04-Unit42-Wireshark-quiz.pcap 										
<u>File Edit View Go</u> Capture A	nalyze <u>S</u> tatistics Tele	phony <u>W</u> irel	ess <u>T</u> ools <u>H</u> elp							
	२ 🗲 🔶 🗲 🗡 📃									
Idap.AttributeDesc	ription == "giv	enName	•"			basic basic+	basic+dns			
Time	Src	port	Dst	port	Info		^			
2023-04-19 19:34:4	8 10.4.19.136	51453	10.4.19.19	389	SASL GSS-API	Integrity:	sea			
2023-04-19 19:34:4	8 10.4.19.136	51455	10.4.19.19	389	SASL GSS-API	Integrity:	sea			
2023-04-19 19:35:5	9 10.4.19.136	51459	10.4.19.19	389	SASL GSS-API	Integrity:	sea			
2023-04-19 19:35:5	9 10.4.19.136	51460	10.4.19.19	389	SASL GSS-API	Integrity:	sea -			
Frame 26707: 215 by	tos on wire (1	720 bite) 215 bytoc	oontu	rod (1720 bitc)		•			
Frame 30707. 215 Dy	levlettp 201051	720 DILS), ZIS Dyles		teu (1720 DILS)	20, of (00)	21.50.9			
Detremet 11, STC: HewlettP_2e:C5:ae (14:58:d0:2e:C5:ae), DST: HewlettP_86:39:8T (00:21:5a:8)										
Thermet Protocol Version 4, Src: 10.4.19.130, Dst: 10.4.19.19										
b Transmission Control Protocol, Src Port: 51453, DSt Port: 389, Seq: 2356, ACK: 3038, Len: 1										
CACL Duffer Longth: 157										
SASL BUTTER LENGTH: 157										
- SASL BUTTER										
SSS-API Generic Security Service Application Program Interface										
- GSS-API payload (129 bytes)										
The state of the s										
messaget): 4										
- protocolup: searchkequest (3)										
- searchkequest										
baseubject: CN=Cornellus Silva, CN=Users, DC=booglenights, DC=live										
scope: paseupject (0)										
deretAllases: neverDeretAllases (0)										

Figure 21. Finding the victim's full name from LDAP traffic.

Perhaps the easiest way to find a victim's hostname in Wireshark is to combine the victim's IP address with a search for ip contains "DESKTOP-" as shown below, in Figure 22. Several results in the info column show Host Announcement DESKTOP-SFF9LJF sent by our infected Windows host at 10.4.19[.]136.

- + × 2023-04-Unit42-Wireshark-quiz.pcap										
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>										
ip.addr eq 10.4.19.13	36 and ip cont	tains "D		🛛 🗖 🔸 basic basic+ basic+dns						
Time	Src	port	Dst	port	Info					
2023-04-19 15:28:43	10.4.19.136	51103	10.4.19.19	49669	Bind: call_id: 2, Fragment: Single					
2023-04-19 15:28:43	10.4.19.136	51103	10.4.19.19	49669	Alter_context: call_id: 3, Fragment					
2023-04-19 15:31:13	10.4.19.136	51122	10.4.19.19	49669	Bind: call_id: 2, Fragment: Single,					
2023-04-19 15:31:13	10.4.19.136	51122	10.4.19.19	49669	Alter_context: call_id: 3, Fragment					
2023-04-19 15:33:47	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 15:36:45	10.4.19.136	51143	10.4.19.19	49669	Bind: call_id: 2, Fragment: Single					
2023-04-19 15:36:45	10.4.19.136	51143	10.4.19.19	49669	Alter_context: call_id: 3, Fragment					
2023-04-19 15:36:46	10.4.19.136	51144	10.4.19.19	49684	Bind: call_id: 2, Fragment: Single,					
2023-04-19 15:45:45	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 15:57:43	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 16:01:20	10.4.19.136	58746	10.4.19.19	389	searchRequest(21) " <root>" baseObj</root>					
2023-04-19 16:01:20	10.4.19.136	58748	10.4.19.19	389	<pre>searchRequest(22) "<root>" baseObj</root></pre>					
2023-04-19 16:09:40	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 16:21:39	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 16:31:23	10.4.19.136	56323	10.4.19.19	389	<pre>searchRequest(23) "<root>" baseObj</root></pre>					
2023-04-19 16:31:23	10.4.19.136	51187	10.4.19.19	49669	Alter_context: call_id: 6, Fragment					
2023-04-19 16:31:23	10.4.19.136	51187	10.4.19.19	49669	Alter_context: call_id: 7, Fragmen					
2023-04-19 16:33:37	10.4.19.136	138	10.4.19.255	138	Host Announcement DESKTOP-SFF9LJF,					
2023-04-19 16:38:40	10.4.19.136	52275	10.4.19.19	389	<pre>searchRequest(24) "<root>" baseObje</root></pre>					
2023-04-19 16:38:40	10.4.19.136	52275	10.4.19.19	389	<pre>searchRequest(25) "<root>" baseObje</root></pre>					
+	10 1 10 100	50075	10 1 10 10	~~~						

Figure 22. Finding the Windows hostname in Wireshark.

To find the victim's MAC address, just correlate the IP address to the host's MAC address in any of the frame details windows, as shown below in Figure 23.

```
> Frame 6223: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits)
> Ethernet II, Src: HewlettP_2e:c5:ae (14:58:d0:2e:c5:ae), : HewlettP_86:
> Internet Protocol Version 4, Src: 10.4.19.136, : 10.4.19.19
> Transmission Control Protocol, Src Port: 51143, Dst Port: 49669, Seq: 490,
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Alter_
Version: 5
Version (minor): 0
Packet type: Alter_context (14)
> Packet Flags: 0x03
> Data Representation: 10000000 (Order: Little-endian, Char: ASCIT, Float;
```

Figure 23. Correlating the victim's MAC address with its associate IP address.

Conclusion

This blog provides answers and analysis for our Unit 42 Wireshark quiz featuring an IcedID infection from April 2023. IcedID is important to identify and stop, because it is a <u>known vector for</u> <u>ransomware infections</u>.

Many organizations lack access to full packet capture in their IT environment. As a result, security professionals might lack experience reviewing IcedID and other malware traffic. Training material like this Wireshark quiz can help. Pcap analysis is a useful skill that helps us better understand malicious activity.

You can also read the original post, without answers, from our standalone quiz post.

Palo Alto Networks customers are protected from IcedID and other malware through <u>Cortex XDR</u> and our <u>Next-Generation Firewall</u> with <u>Cloud-Delivered Security Services</u> that include <u>WildFire</u>, <u>Advanced Threat Prevention</u> and <u>Advanced URL Filtering</u>.

If you think you might have been compromised or have an urgent matter, get in touch with the <u>Unit 42 Incident Response team</u> or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the <u>Cyber Threat Alliance</u>.

Indicators of Compromise

Traffic from the pcap related to the IcedID infection:

• hxxp://80.77.24[.]175/main.php

- hxxps://firebasestorage.googleapis[.]com/v0/b/serene-cathode-377701.appspot.com/o/XSjwp6O0pq%2FScan_Inv.zip?alt=media&token=a716bdce-1373-44ed-ae89-fdabafa31c61
- 192.153.57[.]223:80 hxxp://skigimeetroc[.]com/
- 104.168.53[.]18:443 askamoshopsi[.]com HTTPS traffic
- 217.199.121[.]56:443 skansnekssky[.]com HTTPS traffic
- 193.149.176[.]100:443 BackConnect traffic

Files associated with traffic from this IcedID infection:

Additional Resources

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 Terms of Use and acknowledge our Privacy Statement.