

Turkey and Defense Post-Incident Report

Date of investigation	2019/09/23
Date of incident	2018-11-07 at 20:47 UTC
Outcome	True Positive - Ursnif or Gozi/IFSB found
Action taken	Identified malware and infected host. Advise firewall rules to block traffic from source. Advise reformatting infected computer or restoring to a backup prior to time of incident.
Reporting tool	Wireshark
Attack vector	Windows malware download from shumbildac[.]com/WES/fatog.php?l=ngul5.xap
Source IP/email	10.22.15.119
Source port	68
Destination IP/email	10.22.15.255
Destination port	67

Narrative

- Date/Time malicious activity started: 2018-11-07 at 20:47 UTC
- MAC address of the infected Windows: 00:11:2f:d1:6e:52
- Host name of the infected Windows host: Danger-Win-PC
- User account name on the infected Windows host: carlos.danger
- URL that returned an EXE:
shumbildac[.]com/WES/fatog.php?l=ngul5.xap
- Size of the EXE: 439,808 bytes
- SHA256 hash of the EXE:
97f149f146b0ec63c32abff204ae27638f0310536172

b0f718f1a91a5672fe71

- Type of malware: Ursnif or Gozi/IFSB

Cyber-Security-Ubuntu [Running] - Oracle VM VirtualBox

Activities Wireshark Mon 16:21

2018-11-13-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
404	2018-11-07 20:40:49.964576	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xd908fcbe
405	2018-11-07 20:40:49.964889	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0xd908fcbe
1702	2018-11-07 20:48:19.459685	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6cde92b
1703	2018-11-07 20:48:19.460248	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0x6cde92b
2250	2018-11-07 20:49:57.537766	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x115aaafe
2251	2018-11-07 20:49:57.538877	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0x115aaafe

Frame 404: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: AsustekC_d1:6e:52 (00:11:2f:d1:6e:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.22.15.119, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Inform)

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 63 82 53 63 35 01 08 3d 07 01 c Sc5...=
0120 00 11 2f d1 6e 52 0c 0d 44 61 6e 67 65 72 2d 57 .../..nr Danger-W
0130 69 6e 2d 50 43 3c 08 4d 53 46 54 20 35 2e 30 37 in-PC< M SFT 5.07

2018-11-13-traffic-analysis-exercise.pcap Packets: 10231 - Displayed: 10231 (100.0%) Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

nbns Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	2018-11-07 20:40:47.036005	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<00>
253	2018-11-07 20:40:47.785146	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<00>
306	2018-11-07 20:40:48.540123	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<00>
399	2018-11-07 20:40:49.291061	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<00>
221	2018-11-07 20:40:47.614882	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<20>
276	2018-11-07 20:40:48.360882	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<20>

Frame 400: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: AsustekC_d1:6e:52 (00:11:2f:d1:6e:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.22.15.119, Dst: 10.22.15.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

0000 ff ff ff ff ff ff 00 11 2f d1 6e 52 08 00 45 00 /..nr..E..
0010 00 60 00 e0 00 00 80 11 06 0c 0a 16 0f 77 0a 16w..
0020 0f ff 00 89 00 89 00 4c d6 18 ce 63 28 10 00 01L...c(..
0030 00 00 00 00 00 01 20 45 45 45 42 45 4f 45 48 45 E EEBEOEHE
0040 46 46 43 43 4e 46 48 45 4a 45 4f 43 4e 46 41 45 FFCCNFHE JECCNFHE
0050 44 43 41 43 41 43 41 00 00 20 00 01 c0 0c 00 20 DCACACA:
0060 00 01 00 04 93 e0 00 06 00 00 0a 16 0f 77w

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
1936	dhsiwyqdlkwsqo.com	text/html	213 kB	QGJ.a
1947	dhsiwyqdlkwsqo.com	image/vnd.microsoft.icon	5,430 bytes	favico
2224	dhsiwyqdlkwsqo.com	text/html	271 kB	6Kwyi
2229	dhsiwyqdlkwsqo.com	text/html	2,320 bytes	8lw2H
2557	ferranorga.net	text/html	248 bytes	client.
1690	shumbildac.com	application/octet-stream	439 kB	fatog.
2325	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	55 kB	authre
2566	www.ferranorga.net	application/x-rar-compressed	773 bytes	client.
5363	www.google-analytics.com	text/javascript	46 kB	ga.js
5690	www.google-analytics.com	text/html	368 bytes	__utm
8061	www.google-analytics.com	image/gif	35 bytes	__utm
8109	www.google-analytics.com	image/gif	35 bytes	__utm
8678	www.google-analytics.com	image/gif	35 bytes	__utm
430	www.msftncsi.com	text/plain	14 bytes	ncsi.tx
4614	www.ucdenver.edu	text/css	19 kB	bootst
4634	www.ucdenver.edu	text/html	100 kB	ucdwe
4666	www.ucdenver.edu	text/css	42 kB	respoi
4674	www.ucdenver.edu	text/css	30 kB	jquery
4708	www.ucdenver.edu	text/css	8,091 bytes	degre
4746	www.ucdenver.edu	text/css	191 kB	corev
4756	www.ucdenver.edu	text/css	117 kB	bootst

.com\Policies\{31B2F340-

115aaafe

6cdde92b

d908fcbe

115aaafe

6cdde92b

d908fcbe