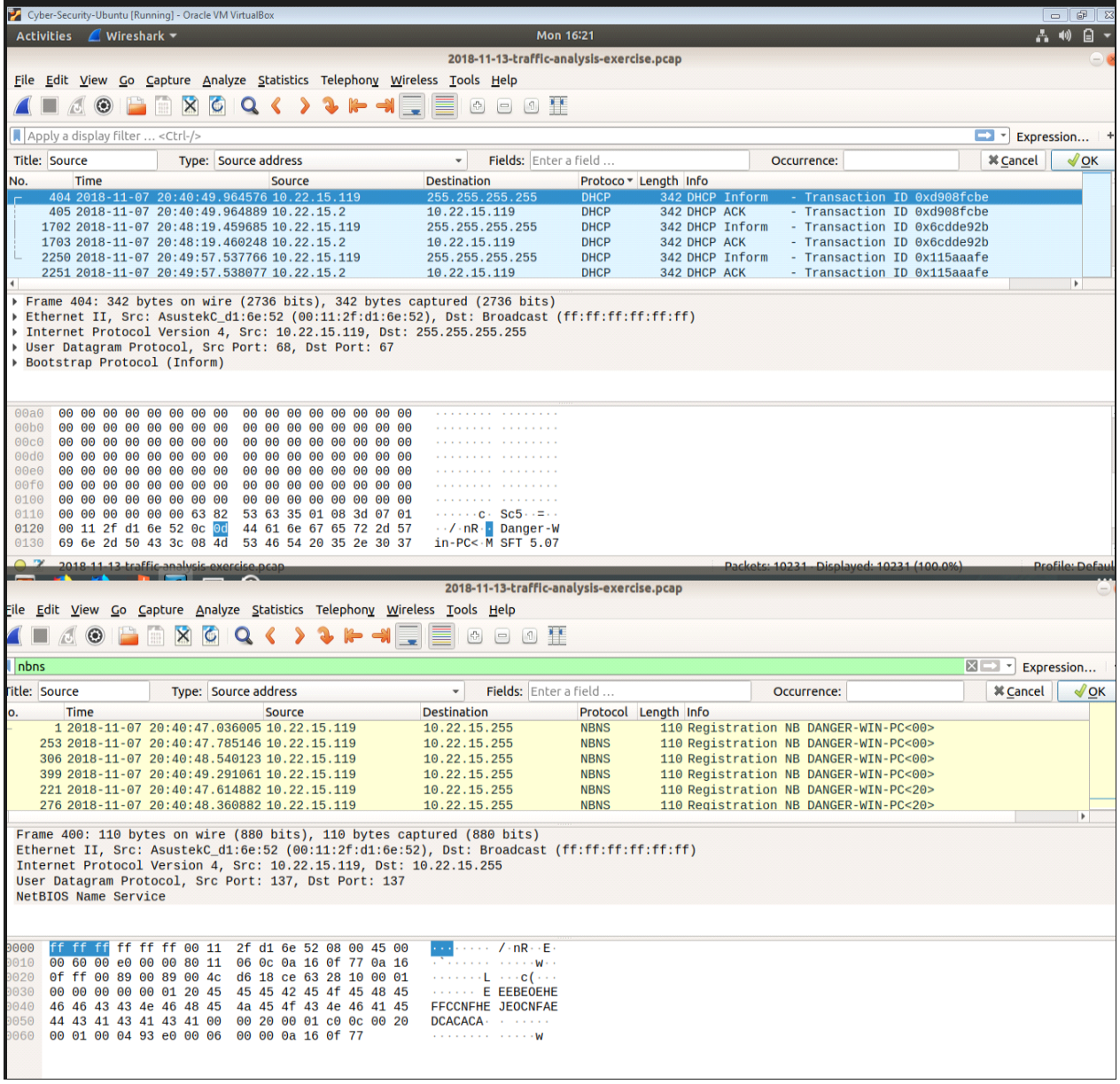
Turkey and Defense Post-Incident Report	
Date of investigation	2019/09/23
Date of incident	2018-11-07 at 20:47 UTC
Outcome	True Positive - Ursnif or Gozi/IFSB found
Action taken	Identified malware and infected host. Advise firewall rules to block traffic from source. Advise reformatting infected computer or restoring to a backup prior to time of incident.
Reporting took	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

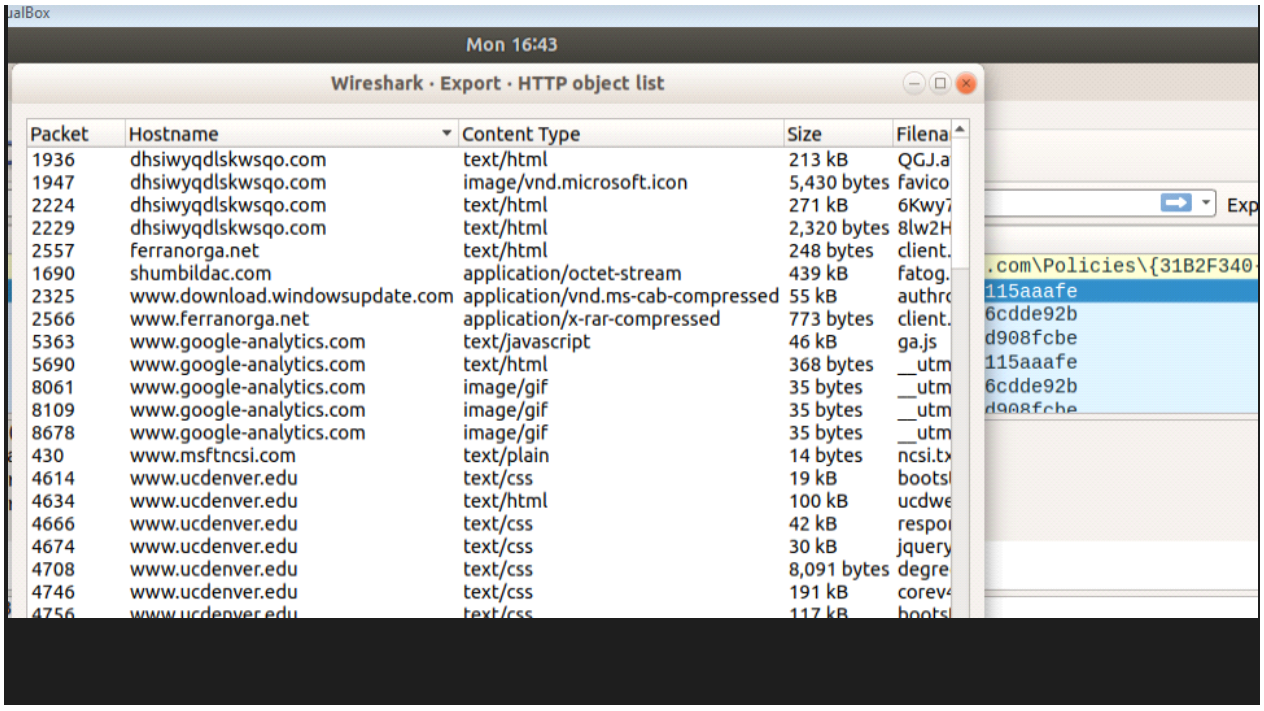
Narrative

- 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




Mon 16:43
Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filena
1936 dhsiwyqdlskwsqo.com text/html 213 kB QGJ.a
1947 dhsiwyqdlskwsqo.com image/vnd.microsoft.icon 5,430 bytes favico
2224 dhsiwyqdlskwsqo.com text/html 271 kB 6Kwy7
2229 dhsiwyqdlskwsqo.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 authro
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 respor
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
.com\Policies\{31B2F340
115aaafe
6cdde92b
d908fcbe
115aaafe
6cdde92b