2020-02-21 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2020/02/21/index.html

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark - Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark - Display Filter Expressions
- Using Wireshark: Exporting Objects from a Pcap

ENVIRONMENT:

- LAN segment range: 172.17.8.0/24 (172.17.8.0 through 172.17.8.255)
- Domain: one-hot-mess.com
- Domain controller: 172.17.8.8 - One-Hot-Mess-DC
- LAN segment gateway: 172.17.8.1
- LAN segment broadcast address: 172.17.8.255

TASK:

Write an incident report based on the pcap, associated alerts, and malware/artifacts from the infected Windows host.

ANSWER:

EXECUTIVE SUMMARY:

On Thursday 2020-02-21 at 00:55 UTC, a Windows 10 client used by Gabriella Ventura was infected with Dridex malware.

DETAILS OF OUR INFECTED HOST:

Host name: DESKTOP-TZMKHKC
Host MAC address: 00:11:75:8c:fd:47 (Intel_8c:fd:47)
Host IP address: 172.17.8.174
User account name: gabriella.ventura

2020-02-21 - TRAFFIC ANALYSIS EXERCISE ANSWERS

INDICATORS OF COMPROMISE (IOCs):

Infection traffic (TCP):

49.51.172.56 port 80 - blueflag.xyz - GET /nCvQOQHCBjZFfiJvyVGA/yrkbdmt.bin

91.211.88.122 port 443 - HTTPS/SSL/TLS traffic caused by Dridex

Alerts associated with this infection traffic:

49.51.172.56 port 80

- ET POLICY Binary Download Smaller than 1 MB Likely Hostile
- ET POLICY PE EXE or DLL Windows file download HTTP
- ET CURRENT_EVENTS WinHttpRequest Downloading EXE
- ET CURRENT_EVENTS Likely Evil EXE download from WinHttpRequest non-exe extension
- ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile

91.211.88.122 port 443

- ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)

Malware/artifacts from the infected Windows host:

SHA256 hash: 01ea3845eac489a2518962e6a9f968cde0811e1531f5a58718fb02cf62541edc
File name: inv_261804.doc
File description: malicious Word doc with macro for Dridex
Reference: https://app.any.run/tasks/1d1dec0f-2f96-4e6f-b1fd-85de837f6cbd/

SHA256 hash: 03c962ebb541a709b92957e301ea03f1790b6a57d4d0605f618fb0be392c8066
File location: http://blueflag.xyz/nCvQOQHCBjZFfiJvyVGA/yrkbdmt.bin
File location: C:\DecemberLogs\Caff54e1.exe
File description: Dridex installer EXE retrieved by Word doc macro
Reference: https://app.any.run/tasks/e35311cc-7cb0-4030-be20-9811c6bf3d9a

SHA256 hash: 943c93039215a85645dc4fa894468e261c997f0f1eeca043d6b5dc10c47108d0
File size: 75,264 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Spelling\qHD3ZbNtI2b\sigverif.exe
File description: Legitimate Windows file copied to new location and used to load Dridex DLL

SHA256 hash: 9ef1deab06b2c809de80fa48ede4a7a9925fde17823d383c2132f43ca1afb92c
File size: 802,816 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Spelling\qHD3ZbNtI2b\VERSION.dll
File description: Dridex DLL loaded by sigverif.exe

SHA256 hash: e9fac70a8201ad2cda3b66dd2931bbc9275109c6e6e955f352fbec08e33d9d24
File size: 166,400 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Templates\LiveContent\16\Ps8EYw7cb1E\iexpress.exe
File description: Legitimate Windows file copied to new location and used to load Dridex DLL

SHA256 hash: bd52a6b3cde81da12d27b316b8791f0b73c6e84e8feafb1994afc4461f0339a2
File size: 802,816 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Templates\LiveContent\16\Ps8EYw7cb1E\VERSION.dll
File description: Dridex DLL loaded by iexpress.exe

SHA256 hash: face2b514ced20add3f8e467dce3769eaaa13398589bc61cf75c7969a641a62d
File size: 60,928 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Vault\wRCV5\WindowsActionDialog.exe
File description: Legitimate Windows file copied to new location and used to load Dridex DLL

SHA256 hash: 16a72e9e46f64a1af57839929d1477f2f20382ecd10b925b5a66538c20c3b11f
File size: 1,089,536 bytes
File location: C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Vault\wRCV5\DUI70.dll
File description: Dridex DLL loaded by WindowsActionDialog.exe

Methods used to keep Dridex persistent on the infected Windows host:

Scheduled task Jqssmf to run:

- C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Vault\wRCV5\WindowsActionDialog.exe

Registry key update:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Kxbpbnmslyha to run:
- C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Templates\LiveContent\16\Ps8EYw7cb1E\iexpress.exe

Windows shortcut Wiqzbgfwkifvvu.lnk in the Start Up menu to run:

- C:\Users\gabriella.ventura\AppData\Roaming\Microsoft\Spelling\qHD3ZbNtI2b\sigverif.exe