

Lab - Investigating an Attack on a Windows Host

Objectives

In this lab you will:

Investigate the Attack with Sguil

This lab is based on an exercise from the website malware-traffic-analysis.net which is an excellent resource for learning how to analyze network and host attacks. Thanks to brad@malware-traffic-analysis.net for permission to use materials from his site.

Background / Scenario

In March 2019, network security monitoring tools alerted that a Windows computer on the network was infected with malware. In this task, you are to investigate the alerts and answer the following questions:

- What was the specific time of the attack on 2019-03-19?
- Which Windows host computer was infected? Who was the user?
- What was the computer infected with?

Required Resources

- Security Onion virtual machine
- Internet access

Instructions

Investigate the Attack with Sguil

In Part 1, you will use Sguil to check the IDS alerts and gather more information about the series of events related to an attack on 3-19-2019.

Note: The alert IDs used in this lab are for example only. The alert IDs on your VM may be different.

Step 1: Open Sguil and locate the alerts on 3-19-2019.

- a. Login to Security Onion VM with the **analyst** username and **cyberops** password.
- b. Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**. Click **Select All** and **Start Sguil** to view all the alerts generated by the network sensors.
- c. Locate the group of alerts from 19 March 2019.

According to Sguil, what are the timestamps for the first and last of the alerts that occurred on 3-19-2019? What is interesting about the timestamps of all the alerts on 3-19-2019?

01:45:03 to 04:54:34. The alerts show suspicious activity for a little over 3 hours but the majority of the alerts took place for a little over 3 minutes and 43 seconds.

Step 2: Review the alerts in detail.

- a. In Sguil, click the first of the alerts on 3-19-2019 (Alert ID 5.439). Make sure to check the **Show Packet Data** and **Show Rule** checkboxes to examine the packet header information and the IDS signature rule

Lab - Investigating an Attack on a Windows Host

related to the alert. Right on the **Alert ID** and pivot to Wireshark. Based on the information derived from this initial alert answer the following questions:

What was the source IP address and port number and destination IP address and port number?

Source: 10.0.90.215:52609, Destination: 10.0.90.9:53

What type of protocol and request or response was involved?

UDP, Dynamic DNS, update and response

What is the IDS alert and message?

Alert udp \$EXTERNAL_NET any -> \$HOME_NET 53, msg: "ET POLICY DNS Update from External net"

Do you think this alert was the result of an IDS misconfiguration or a legitimate suspicious communication?

This alert may be the result of a misconfiguration in the IDS because the DNS request was a Dynamic DNS update from an internal host to a DNS server on the internal network and not from an external network to the internal network.

What is the hostname, domain name, and IP address of the source host in the DNS update?

Bobby-Tiger-PC, littletigers.info, 10.0.90.215

- b. In Sguil, select the second of the alerts on 3-19-2019. Right click the Alert ID 5.440 and select **Transcript**.

seconion-import-1_411

File

Sensor Name: seconion-import-1
Timestamp: 2019-03-19 01:47:04
Connection ID: seconion-import-1_411
Src IP: 10.0.90.215
Dst IP: 209.141.34.8
Src Port: 49204
Dst Port: 80
OS Fingerprint: 10.0.90.215:49204 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460.N.W8.N.N.S.:Windows:?]
OS Fingerprint: -> 209.141.34.8:80 (distance 0, link: ethernet/modem)

SRC: GET /test1.exe HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
SRC: Host: 209.141.34.8
SRC: Connection: Keep-Alive
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 19 Mar 2019 01:45:55 GMT
DST: Server: Apache/2.4.6 (CentOS)
DST: Last-Modified: Mon, 18 Mar 2019 22:00:46 GMT
DST: ETag: "c6200-584658544df80"
DST: Accept-Ranges: bytes
DST: Content-Length: 811520
DST: Connection: timeout=5, max=100
DST: Connection: Keep-Alive

Debug Messages

DST: Connection: Keep-Alive
DST: Content-Type: application/octet-stream
DST:
DST: MZ.....@.....!L!This program cannot be run in DOS mode.
DST:
DST:
DST:g.F.4.F.4.F.4...5.F.4...5.F.4...5.F.4.F.43F.4...5.F.4./4.F.4...5.F.4Rich.F.4.....
DST:PE.....IZ.....f.....k.....@.....
DST:
DST:
DST:0.....8.....@.....
DST:text....e....f.....
DST:data...H.....j.....@....idata_n.....l.....@...@.rsrc.....~.....@...@.relo
c.....
DST:
DST:X.....@..B.....
DST:@.P.@.....
DST:@.0.@.....@.....5.....k@.....j@..p@.....1..@1..2...4..
5..B..J..J..pK..L..pL..M..M..M..PP..@d...d..Ph..j..k...k..
n..@p..p..pq..t..Ot.....advapi32.dll...CheckTokenMembership..."
...INF...[...].Reboot..AdvancedINF.Version.setupx.dll..setupapi.dll....BAT....SeShutdownPrivilege.a
dypack.dll.DelNodeRunDLL32.*.....wininit.ini.%lu.Software\Microsoft\Windows\CurrentVersion\App
Paths\...K.e.r.n.e.i.3.2...d.I.L...HeapSetInformation..TITLE...EXTRACTOPT..INSTANCECHECK...VE
RCHECK....DecryptFileA...LICENSE.<None>..REBOOT..SHOWWINDOW..ADMQCMD.USRQCMD.R
UNPROGRAM..POSTRUNPROGRAM..FINISHMSG...LoadString() Error. Could not load string
resource.....CABINET.FILESIZES...PACKINSTSPACE...UPROMPT.IXP%03d.TMP.IXP.i386.....mips..

From the transcript answer the following questions:

Lab - Investigating an Attack on a Windows Host

What is the source and destination IP address and port numbers?

Source 10.0.90.215:49204 and Destination 209.141.34.8:80

Looking at the request (blue) what was the request for?

GET /test1.exe

Looking at the reply (red) many files will reveal their file signature in the initial few characters of the file when viewed as text. File signatures help identify the type of file that is represented. Use a web browser to search for a list of common file signatures.

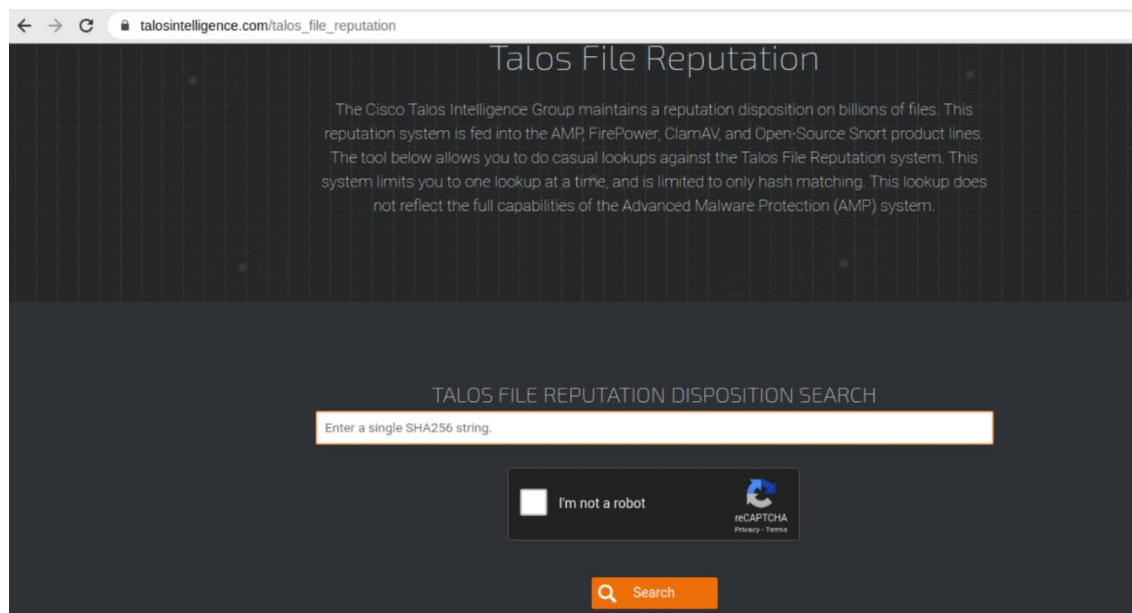
What is the initial few characters of the file file. Search for this file signature to find out what type of file was downloaded in the data?

The initial characters of this file is MZ, a Windows executable .exe or .dll file

- c. Close the transcript. Use Wireshark to export the executable file for malware analysis (**File > Export Objects > HTTP...**). Save the file to the analyst's home folder.
- d. Open a terminal in Security Onion VM and create a SHA256 hash from the exported file. Use the following command:

```
analyst@SecOnion:~$ sha256sum test1.exe
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85  test1.exe
```

- e. Copy the file hash and submit it to the Cisco Talos file reputation center at https://talosintelligence.com/talos_file_reputation.



Did Talos recognize the file hash and identify it as malware? If so, what kind of malware?

Yes, win32 trojan-spy-agent