Incident Report: IM-10288-Malware Analysis

Date: 10-16-2021

Executive summary:

I was tasked with analyzing malware. The tool I used for this story was HashMyFiles. Another tool I used was wireshark to find the hostname, IP address, and destination port.

Indicators of Compromise (IOC's):

1. 2e515f89c1e57a82f439f160bdc91045 (packet 2324 INFECTED Script.Trojan.43769)

Hostname: tonmatdoanminh.com Content Type:text/html

Destination Port: 80

IP address: 10.2.8.101

2. ca1f1746de27ce574d39f7e9d0c75c4b (packet 4139 INFECTED Backdoor.Meterpreter.152)

Hostname: 198.211.10.238:8080 Content Type: application/octet-stream

Destination Port: 8080

IP address: 10.2.8.101

3. 81f1bad1f8f01c561e83204f40f19a76 (packet 2993 INFECTED Trojan.MSOffice.SDrop.b!c, HEUR:Trojan-Dropper.MSOffice.SDrop.gen, HEUR:Trojan.Script.Generic)

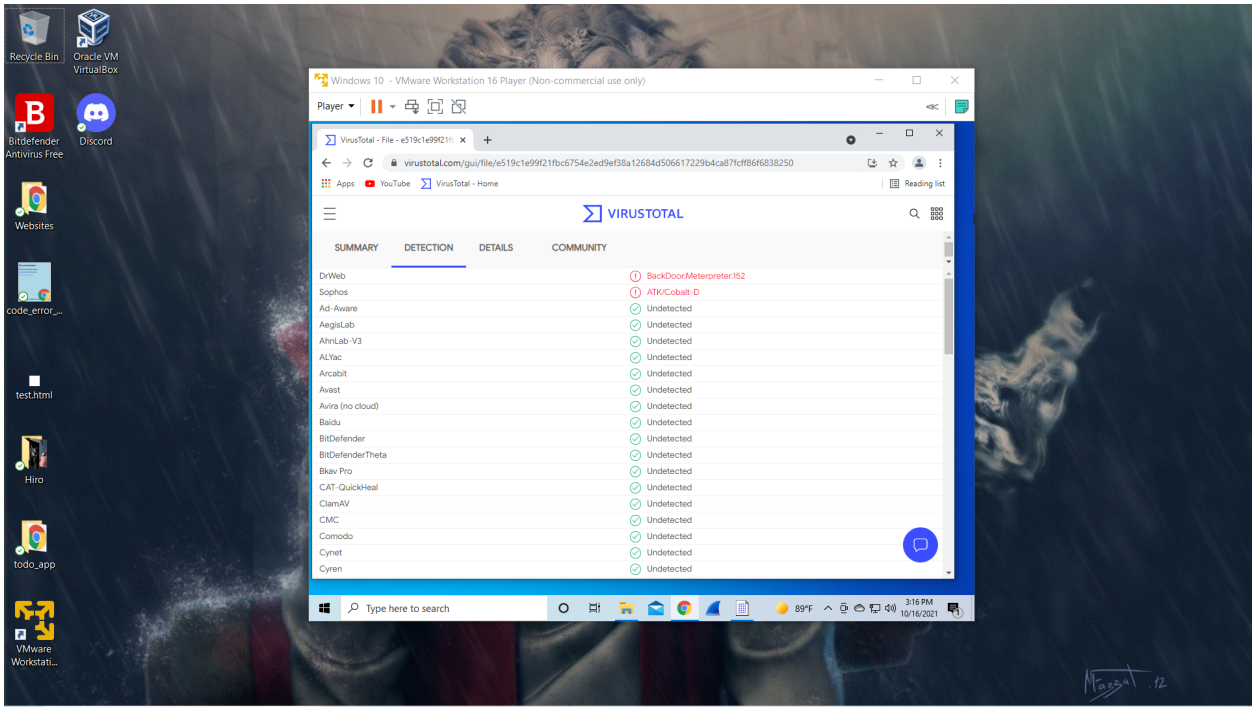
Hostname: tonmatdoanminh.com Content Type:text/html

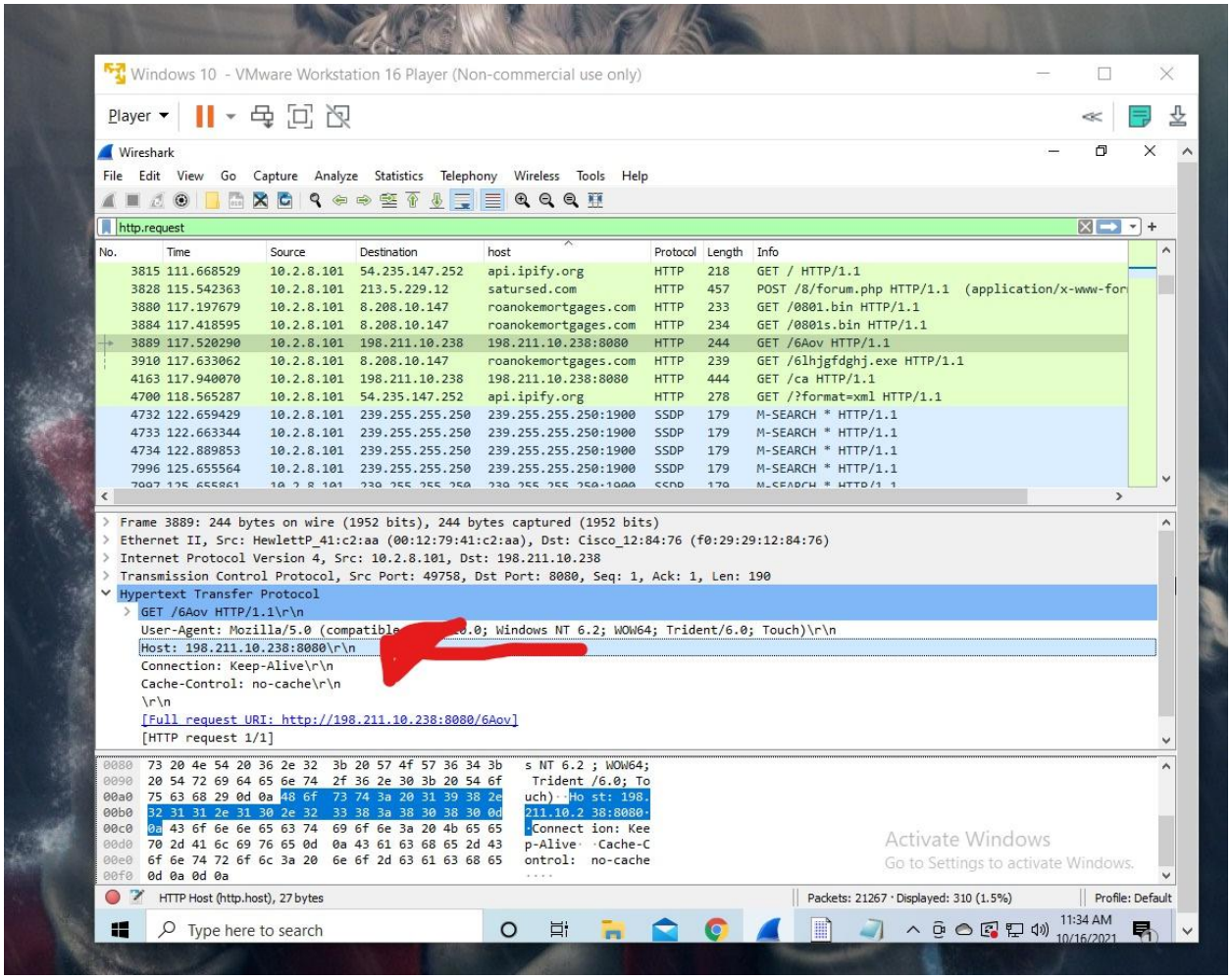
Destination Port: 80

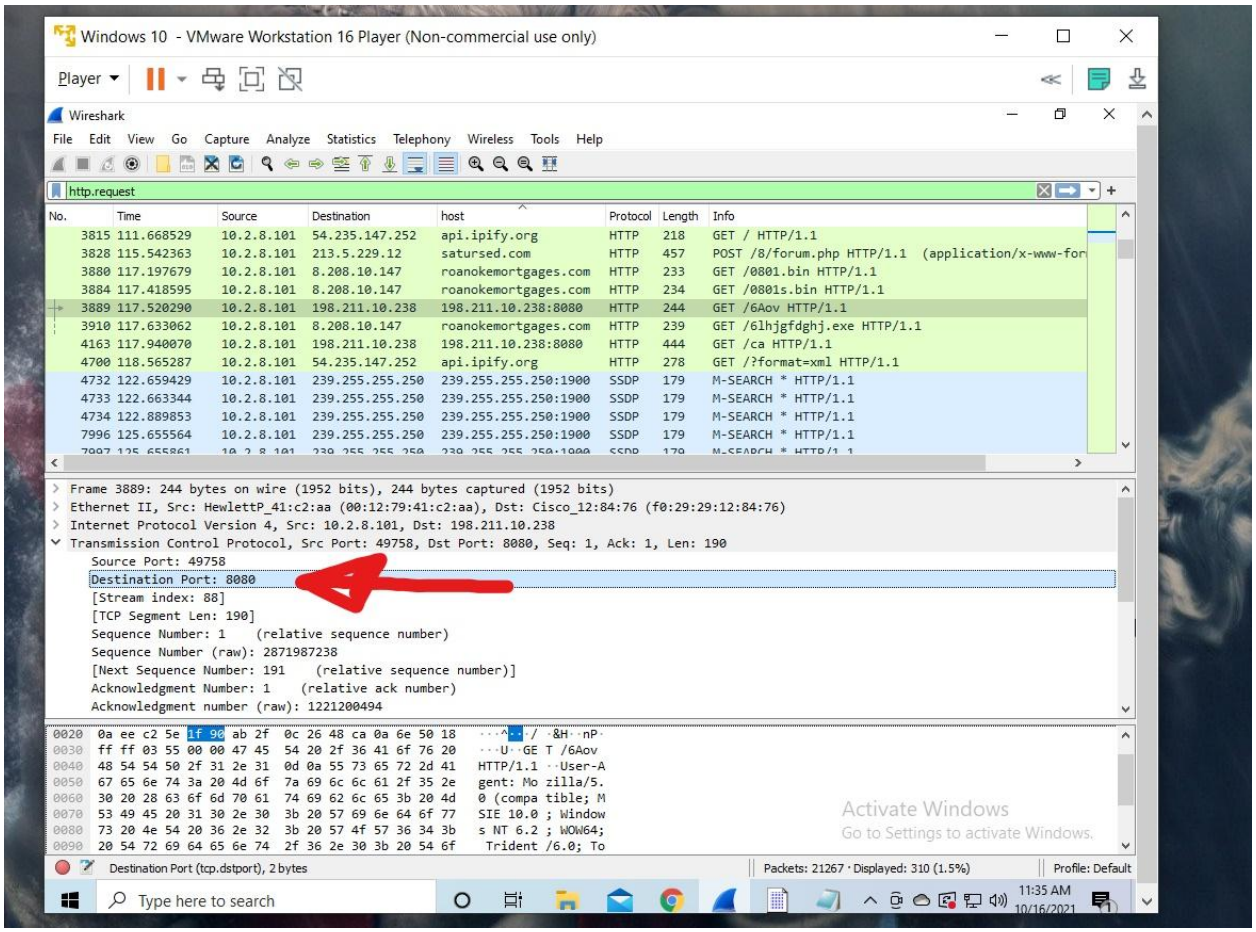
IP address: 10.2.8.101

Conclusion:

As stated earlier, I was tasked with analyzing malware. I was able to locate some packets that were deemed to be infected. Using WireShark and HashMyFiles were the tools that I used to locate these files. Once i located the files i was able to locate the rest of the information needed to complete this task




Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Player
Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination host Protocol Length Info
3815 111.668529 10.2.8.101 54.235.147.252 api.ipify.org HTTP 218 GET / HTTP/1.1
3828 115.542363 10.2.8.101 213.5.229.12 saturated.com HTTP 457 POST /8/forum.php HTTP/1.1 (application/x-www-for
3880 117.197679 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 233 GET /0801.bin HTTP/1.1
3884 117.418595 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 234 GET /0801s.bin HTTP/1.1
3889 117.520290 10.2.8.101 198.211.10.238 198.211.10.238:8080 HTTP 244 GET /6Aov HTTP/1.1
3910 117.633062 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 239 GET /6lhjgfdghj.exe HTTP/1.1
4163 117.940070 10.2.8.101 198.211.10.238 198.211.10.238:8080 HTTP 444 GET /ca HTTP/1.1
4700 118.565287 10.2.8.101 54.235.147.252 api.ipify.org HTTP 278 GET /?format=xml HTTP/1.1
4732 122.659429 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
4733 122.663344 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
4734 122.889853 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
7996 125.655564 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
Frame 3889: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
Ethernet II, Src: HewlettP_41:c2:aa (00:12:79:41:c2:aa), Dst: Cisco_12:84:76 (f0:29:29:12:84:76)
Internet Protocol Version 4, Src: 10.2.8.101, Dst: 198.211.10.238
Transmission Control Protocol, Src Port: 49758, Dst Port: 8080, Seq: 1, Ack: 1, Len: 190
Hypertext Transfer Protocol
GET /6Aov HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (compatible
.0; Windows NT 6.2; WOW64; Trident/6.0; Touch)\r\n
Host: 198.211.10.238:8080\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://198.211.10.238:8080/6Aov]
[HTTP request 1/1]
0080 73 20 4e 54 20 36 2e 32 3b 20 57 4f 57 36 34 3b s NT 6.2 ; WOW64;
0090 20 54 72 69 64 65 6e 74 2f 36 2e 30 3b 20 54 6f Trident /6.0; To
00a0 75 63 68 29 0d 0a 48 6f 73 74 3a 20 31 39 38 2e uch)··Ho st: 198.
00b0 32 31 31 2e 31 30 2e 32 33 38 3a 38 30 38 30 0d 211.10.2 38:8080·
00c0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 ·Connect ion: Kee
00d0 70 2d 41 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 p-Alive· ·Cache-C
00e0 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 ontrol: no-cache
00f0 0d 0a 0d 0a ····
Activate Windows
Go to Settings to activate Windows.
HTTP Host (http.host), 27 bytes
Packets: 21267 · Displayed: 310 (1.5%)
Profile: Default
Type here to search
11:34 AM
10/16/2021


Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Player
Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination host Protocol Length Info
3815 111.668529 10.2.8.101 54.235.147.252 api.ipify.org HTTP 218 GET / HTTP/1.1
3828 115.542363 10.2.8.101 213.5.229.12 satursed.com HTTP 457 POST /8/forum.php HTTP/1.1 (application/x-www-for
3880 117.197679 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 233 GET /0801.bin HTTP/1.1
3884 117.418595 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 234 GET /0801s.bin HTTP/1.1
3889 117.520290 10.2.8.101 198.211.10.238 198.211.10.238:8080 HTTP 244 GET /6Aov HTTP/1.1
3910 117.633062 10.2.8.101 8.208.10.147 roanokemortgages.com HTTP 239 GET /6lhjgfdghj.exe HTTP/1.1
4163 117.940070 10.2.8.101 198.211.10.238 198.211.10.238:8080 HTTP 444 GET /ca HTTP/1.1
4700 118.565287 10.2.8.101 54.235.147.252 api.ipify.org HTTP 278 GET /?format=xml HTTP/1.1
4732 122.659429 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
4733 122.663344 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
4734 122.889853 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
7996 125.655564 10.2.8.101 239.255.255.250 239.255.255.250:1900 SSDP 179 M-SEARCH * HTTP/1.1
Frame 3889: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
Ethernet II, Src: HewlettP_41:c2:aa (00:12:79:41:c2:aa), Dst: Cisco_12:84:76 (f0:29:29:12:84:76)
Internet Protocol Version 4, Src: 10.2.8.101, Dst: 198.211.10.238
Transmission Control Protocol, Src Port: 49758, Dst Port: 8080, Seq: 1, Ack: 1, Len: 190
Source Port: 49758
Destination Port: 8080
[Stream index: 88]
[TCP Segment Len: 190]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2871987238
[Next Sequence Number: 191 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1221200494
0020 0a ee c2 5e 1f 90 ab 2f 0c 26 48 ca 0a 6e 50 18
0030 ff ff 03 55 00 00 47 45 54 20 2f 36 41 6f 76 20
0040 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41
0050 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e
0060 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d
0070 53 49 45 20 31 30 2e 30 3b 20 57 69 6e 64 6f 77
0080 73 20 4e 54 20 36 2e 32 3b 20 57 4f 57 36 34 3b
0090 20 54 72 69 64 65 6e 74 2f 36 2e 30 3b 20 54 6f
Activate Windows
Go to Settings to activate Windows.
Destination Port (tcp.dstport), 2 bytes
Packets: 21267 · Displayed: 310 (1.5%)
Profile: Default
Type here to search
11:35 AM
10/16/2021