ID: 831159
Sample Name: OMnylKuNNF.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:09:07
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

Linux Analysis Report

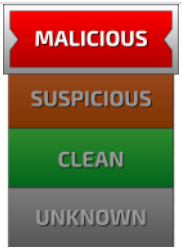
OMnylKuNNF.elf

Overview

General Information

Sample Name:	OMnylKuNNF.elf
Original Sample Name:	8406babfb9b43..
Analysis ID:	831159
MD5:	8406babfb9b43..
SHA1:	22761d5d5c43…
SHA256:	9a067e32dd6c…
Tags:	64 elf mirai
Infos:	

Detection



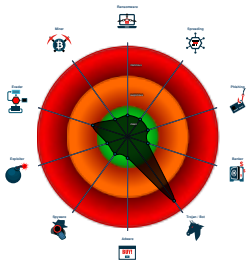
Mirai, Moobot

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Snort IDS alert for network traffic
- Connects to many ports of the same…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831159
Start date and time:	2023-03-21 07:09:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Sample file name:	OMnylKuNNF.elf
Original Sample Name:	8406babfb9b432ee244575aa2e3f63fe.elf
Detection:	MAL
Classification:	mal96.troj.linELF@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/OMnylKuNNF.elf
PID:	6227
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	done.

Copyright Joe Security LLC 2023

Standard Error:	sh: 1: cannot create 2bin/systemd: Directory nonexistent chmod: cannot access 'bin/systemd': No such file or directory

Process Tree

- **system is lnxubuntu20**
- OMnylKuNNF.elf (PID: 6227, Parent: 6126, MD5: 8406babfb9b432ee244575aa2e3f63fe) Arguments: /tmp/OMnylKuNNF.elf
  - OMnylKuNNF.elf New Fork (PID: 6228, Parent: 6227)
  - sh (PID: 6228, Parent: 6227, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >2\\xffbin/systemd && mv /tmp/OMnylKuNNF.elf bin/systemd; chmod 777 bin/systemd"
    - sh New Fork (PID: 6229, Parent: 6228)
    - rm (PID: 6229, Parent: 6228, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 6230, Parent: 6228)
    - mkdir (PID: 6230, Parent: 6228, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6231, Parent: 6228)
    - chmod (PID: 6231, Parent: 6228, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/systemd
  - OMnylKuNNF.elf New Fork (PID: 6232, Parent: 6227)
    - OMnylKuNNF.elf New Fork (PID: 6233, Parent: 6232)
    - OMnylKuNNF.elf New Fork (PID: 6234, Parent: 6232)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	http://osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	http://https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Name	Description	Attribution	Blogpost URLs	Link
MooBot		No Attribution	http://https://blog.netlab.360.com/ddos-botnet-moobot-en/https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949bhttps://unit42.paloaltonetworks.com/moobot-d-link-devices/	http://https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
OMnylKuNNF.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
OMnylKuNNF.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
OMnylKuNNF.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xce48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xceac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcec0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xced4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcee8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcefc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf10:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf24:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf38:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf4c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf60:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf88:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfb0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfc4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfd8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
OMnylKuNNF.elf	Linux_Trojan_Gafgyt_9e9530a7	unknown	unknown	• 0x912c:$a: F6 48 63 FF B8 36 00 00 00 0F 05 48 3D 00 F0 FF FF 48 89 C3
OMnylKuNNF.elf	Linux_Trojan_Gafgyt_807911a2	unknown	unknown	• 0x97df:$a: FE 48 39 F3 0F 94 C2 48 83 F9 FF 0F 94 C0 84 D0 74 16 4B 8D
Click to see the 11 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
6227.1.0000000000400000.000000000040f000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6227.1.0000000000400000.000000000040f000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6227.1.0000000000400000.000000000040f000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xce48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xce98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xceac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcec0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xced4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcee8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcefc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf10:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf24:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf38:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf4c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf60:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf88:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcf9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfb0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfc4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xcfd8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6227.1.0000000000400000.000000000040f000.r-x.sdmp	Linux_Trojan_Gafgyt_9e9530a7	unknown	unknown	• 0x912c:$a: F6 48 63 FF B8 36 00 00 00 0F 05 48 3D 00 F0 FF FF 48 89 C3
6227.1.0000000000400000.000000000040f000.r-x.sdmp	Linux_Trojan_Gafgyt_807911a2	unknown	unknown	• 0x97df:$a: FE 48 39 F3 0F 94 C2 48 83 F9 FF 0F 94 C0 84 D0 74 16 4B 8D
Click to see the 12 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.39.195.63

Timestamp:	192.168.2.23197.39.195.6355812372152835222 03/21/23-07:11:34.483333
SID:	2835222
Source Port:	55812
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.234.59.53

Timestamp:	192.168.2.23197.234.59.5340346372152835222 03/21/23-07:10:23.199102
SID:	2835222
Source Port:	40346
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 147.46.122.92

Timestamp:	192.168.2.23147.46.122.9236620372152835222 03/21/23-07:11:56.415741
SID:	2835222
Source Port:	36620

Copyright Joe Security LLC 2023

Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.233.131.219

Timestamp:	192.168.2.2341.233.131.21952978372152835222 03/21/23-07:10:55.747017
SID:	2835222
Source Port:	52978
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.23 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.238.8.8.854536532023883 03/21/23-07:09:52.583756
SID:	2023883
Source Port:	54536
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 156.224.24.249 - Destination IP: 192.168.2.23

Timestamp:	156.224.24.249192.168.2.2356999477962030489 03/21/23-07:11:48.637846
SID:	2030489
Source Port:	56999
Destination Port:	47796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.36.213.188

Timestamp:	192.168.2.2341.36.213.188391383372152835222 03/21/23-07:10:30.344361
SID:	2835222
Source Port:	39138
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.39.34.188

Timestamp:	192.168.2.23197.39.34.18859102372152835222 03/21/23-07:10:07.047772
SID:	2835222
Source Port:	59102
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 86.69.66.253

Timestamp:	192.168.2.2386.69.66.253588443721528352222 03/21/23-07:10:54.644031
SID:	2835222
Source Port:	58844
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 157.157.112.175

Timestamp:	192.168.2.23157.157.112.175546563721528352222 03/21/23-07:09:59.757322
SID:	2835222
Source Port:	54656
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2023

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 172.65.204.144	
Timestamp:	192.168.2.23172.65.204.14443698372152835222 03/21/23-07:11:38.525358
SID:	2835222
Source Port:	43698
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.39.190.244	
Timestamp:	192.168.2.23197.39.190.24448276372152835222 03/21/23-07:11:01.870921
SID:	2835222
Source Port:	48276
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.62.43.160	
Timestamp:	192.168.2.2341.62.43.16047544372152835222 03/21/23-07:11:51.897568
SID:	2835222
Source Port:	47544
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.39.167.71	
Timestamp:	192.168.2.23197.39.167.7139372372152835222 03/21/23-07:10:39.495843
SID:	2835222
Source Port:	39372
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.148.89.120	
Timestamp:	192.168.2.23197.148.89.12049098372152835222 03/21/23-07:11:41.620198
SID:	2835222
Source Port:	49098
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1) - Source IP: 192.168.2.23 - Destination IP: 156.224.24.249	
Timestamp:	192.168.2.23156.224.24.24947796569992030490 03/21/23-07:09:52.816652
SID:	2030490
Source Port:	47796
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 213.176.10.176	
Timestamp:	192.168.2.23213.176.10.17653290372152835222 03/21/23-07:11:34.410258
SID:	2835222
Source Port:	53290
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Copyright Joe Security LLC 2023

AV Detection

- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic
- Connects to many ports of the same IP (likely port scanning)
- Uses known network protocols on non-standard ports

System Summary

- Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

- Sets full permissions to files and/or directories

Hooking and other Techniques for Hiding and Protection

- Uses known network protocols on non-standard ports

Stealing of Sensitive Information

- Yara detected Mirai
- Yara detected Moobot

Remote Access Functionality

- Yara detected Mirai
- Yara detected Moobot

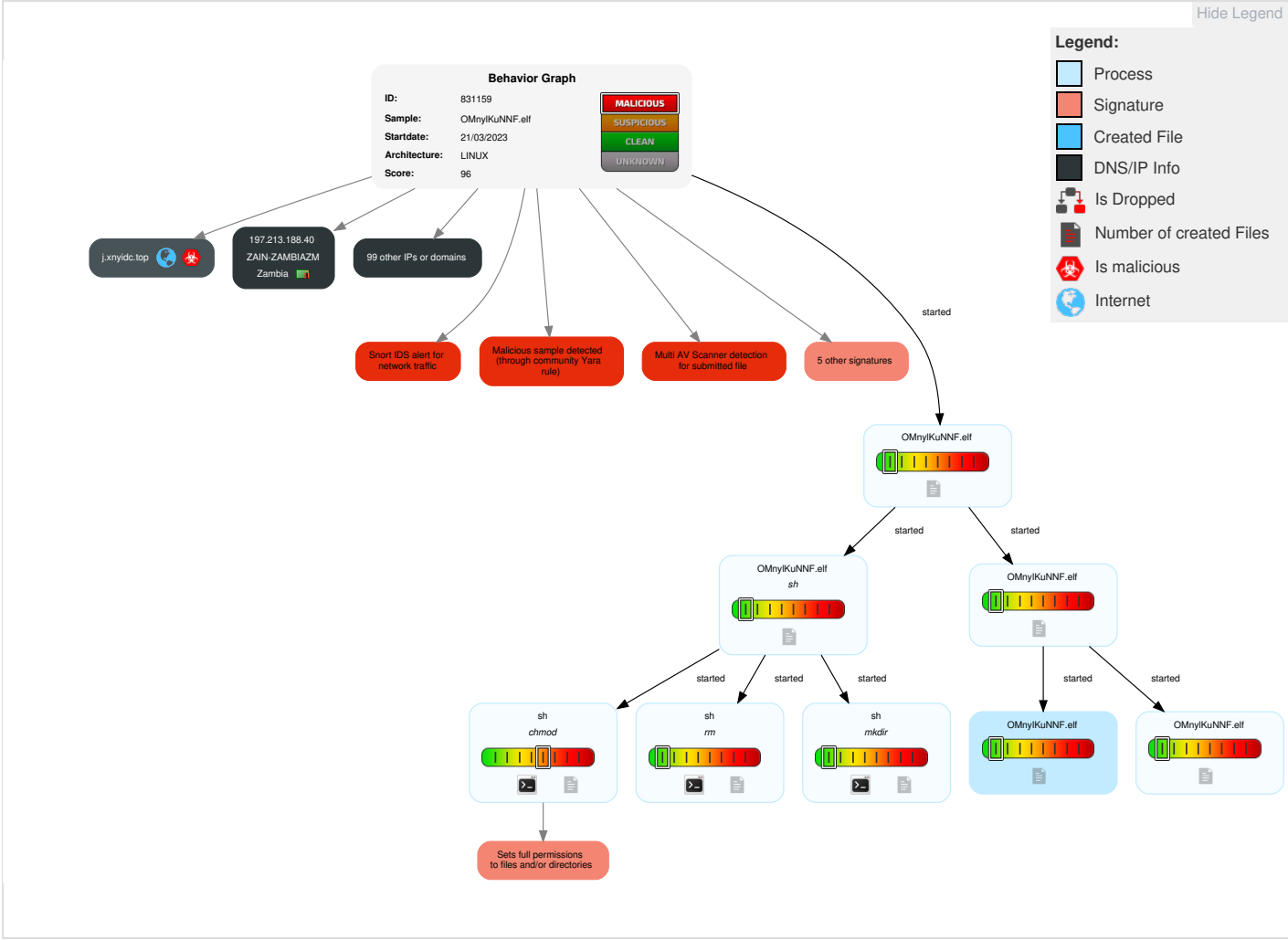
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	Path Interception	1 File and Directory Permissions Modification	1 OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 File Deletion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OMnylKuNNF.elf	56%	ReversingLabs	Linux.Trojan.Gafgyt	
OMnylKuNNF.elf	58%	Virustotal		Browse
OMnylKuNNF.elf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
j.xnyidc.top	13%	Virustotal		Browse

Copyright Joe Security LLC 2023

URLs

No Antivirus matches

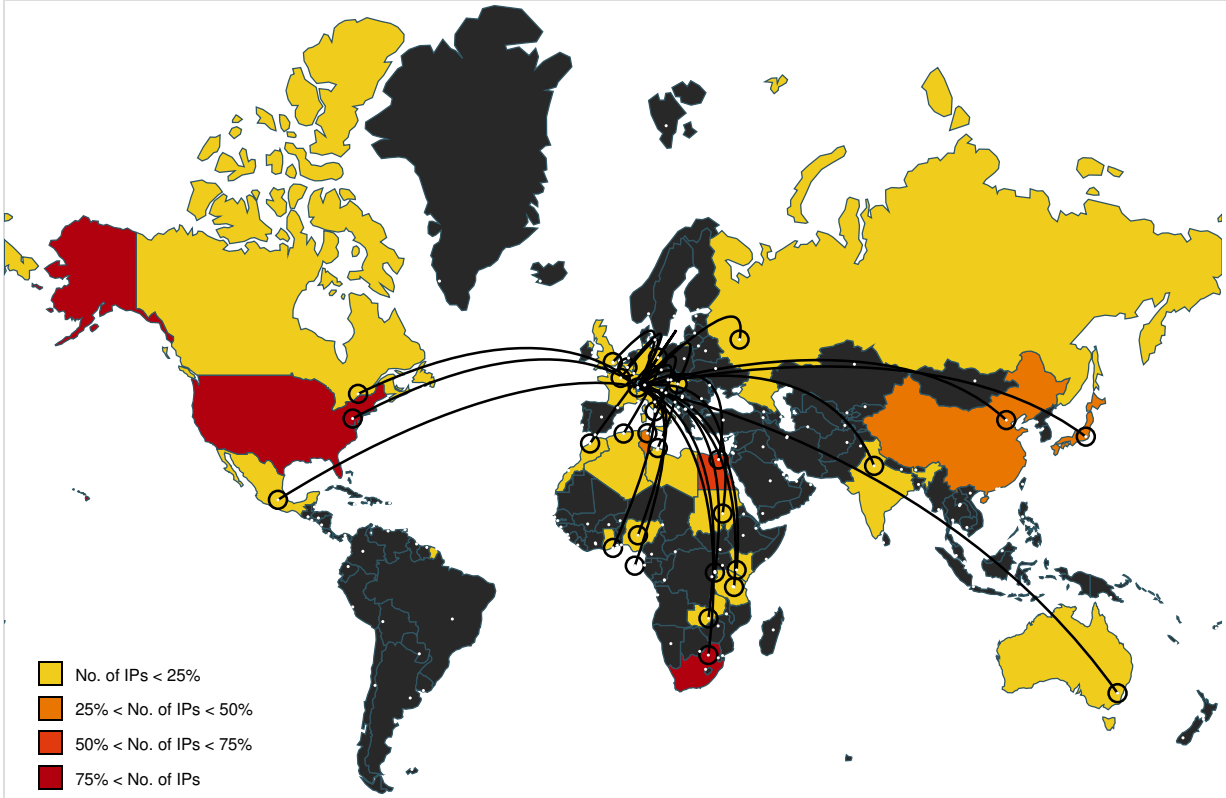
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
j.xnyidc.top	156.224.24.249	true	true	• 13%, Virustotal, Browse	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.182.219.13	unknown	United States		12118	WVUUS	false
41.145.46.68	unknown	South Africa		5713	SAIX-NETZA	false
157.181.17.237	unknown	Hungary		2012	ELTENETELTENETHU	false
41.240.15.46	unknown	Sudan		36998	SDN-MOBITELSD	false
197.21.53.59	unknown	Tunisia		37693	TUNISIANATN	false
41.35.69.95	unknown	Egypt		8452	TE-ASTE-ASEG	false
39.145.25.203	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
71.197.70.235	unknown	United States		7922	COMCAST-7922US	false
197.77.89.90	unknown	South Africa		16637	MTNNS-ASZA	false
197.95.1.86	unknown	South Africa		10474	OPTINETZA	false
157.7.0.253	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
157.170.12.73	unknown	United States		22192	SSHENETUS	false
204.81.97.207	unknown	Canada		17120	NBDOE-ORGCA	false
183.168.225.48	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false

Copyright Joe Security LLC 2023

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.86.185.127	unknown	Tanzania United Republic of		22354	UNIV-DARTZ	false
157.120.16.193	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
41.73.84.241	unknown	unknown		37004	Suburban-Broadband-ASNG	false
197.193.207.47	unknown	Egypt		36992	ETISALAT-MISREG	false
41.64.208.72	unknown	Egypt		36992	ETISALAT-MISREG	false
64.254.157.166	unknown	United States		16941	CENTURYLINK-LEGACY-FUSEPOINT-CTS-CANADA-POPUS	false
197.237.113.184	unknown	Kenya		15399	WANANCHI-KE	false
41.57.232.49	unknown	Ghana		37103	BUSYINTERNETGH	false
41.35.69.81	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.24.66.201	unknown	South Africa		36994	Vodacom-VBZA	false
104.80.188.21	unknown	United States		20940	AKAMAI-ASN1EU	false
105.49.113.103	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.228.40.230	unknown	South Africa		37457	Telkom-InternetZA	false
182.42.172.84	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
41.245.242.102	unknown	Nigeria		328050	Intercellular-Nigeria-ASNG	false
41.206.191.253	unknown	South Africa		6453	AS6453US	false
41.138.190.27	unknown	Nigeria		20598	CYBERSPACE-ASAutonomousSystemnumberforCyberSpaceIL	false
157.119.196.248	unknown	China		2516	KDDIKDDICORPORATIONJP	false
41.129.114.57	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.208.144.185	unknown	Sudan		36998	SDN-MOBITELSD	false
146.35.183.63	unknown	United States		197938	TRAVIANGAMESDE	false
197.159.165.38	unknown	Sao Tome and Principe		328191	CST-NET-ASST	false
217.42.122.175	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
157.222.228.74	unknown	United States		4704	SANNETRakutenMobileIncJP	false
131.148.28.104	unknown	United States		33363	BHN-33363US	false
41.168.23.217	unknown	South Africa		36937	Neotel-ASZA	false
157.29.93.250	unknown	Italy		8968	BT-ITALIAIT	false
157.29.93.252	unknown	Italy		8968	BT-ITALIAIT	false
157.28.126.236	unknown	Italy		8968	BT-ITALIAIT	false
197.193.207.28	unknown	Egypt		36992	ETISALAT-MISREG	false
197.115.12.123	unknown	Algeria		36947	ALGTEL-ASDZ	false
64.60.19.216	unknown	United States		14265	US-TELEPACIFICUS	false
197.213.188.40	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
41.201.35.221	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.28.73.132	unknown	Tunisia		37492	ORANGE-TN	false
41.254.111.167	unknown	Libyan Arab Jamahiriya		21003	GPTC-ASLY	false
41.120.42.102	unknown	South Africa		16637	MTNNS-ASZA	false
157.112.124.47	unknown	Japan		58793	NIFCLOUD-NETFUJITSUCLOUDTECHNOLOGIESLIMITEDJP	false
219.105.240.250	unknown	Japan		4704	SANNETRakutenMobileIncJP	false
41.28.30.180	unknown	South Africa		29975	VODACOM-ZA	false
157.43.70.3	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.92.68.241	unknown	South Africa		10474	OPTINETZA	false
41.11.91.57	unknown	South Africa		29975	VODACOM-ZA	false
197.141.7.87	unknown	Algeria		36891	ICOSNET-ASDZ	false
197.146.218.167	unknown	Morocco		36884	MAROCCONNECTMA	false
157.40.196.111	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false

Copyright Joe Security LLC 2023

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.109.122.55	unknown	South Africa		37168	CELL-CZA	false
41.152.167.29	unknown	Egypt		36992	ETISALAT-MISREG	false
41.186.134.49	unknown	Rwanda		36890	MTNRW-ASNRW	false
157.194.15.74	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.71.111.144	unknown	South Africa		37053	RSAWEB-ASZA	false
41.122.213.28	unknown	South Africa		16637	MTNNS-ASZA	false
122.90.247.197	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
197.10.101.30	unknown	Tunisia		5438	ATI-TN	false
41.35.105.63	unknown	Egypt		8452	TE-ASTE-ASEG	false
2.95.221.135	unknown	Russian Federation		3216	SOVAM-ASRU	false
157.109.131.144	unknown	Japan		37919	SEGASEGAHoldingsCoLtdJP	false
197.192.97.8	unknown	Egypt		36992	ETISALAT-MISREG	false
137.103.117.92	unknown	United States		11776	ATLANTICBB-JOHNSTOWNUS	false
161.121.51.16	unknown	United States		786	JANETJiscServicesLimitedGB	false
197.255.13.181	unknown	Nigeria		35074	COBRANET-ASLB	false
164.190.149.31	unknown	United States		27064	DNIC-ASBLK-27032-27159US	false
157.243.207.135	unknown	France		25789	LMUUS	false
197.211.138.42	unknown	South Africa		22750	BCSNETZA	false
41.129.151.32	unknown	Egypt		24863	LINKdotNET-ASEG	false
157.202.188.60	unknown	United States		1759	TSF-IP-CORETeliaFinlandOyjEU	false
194.49.23.90	unknown	Germany		42184	TKRZ-ASDE	false
41.169.37.92	unknown	South Africa		36937	Neotel-ASZA	false
157.211.83.127	unknown	Australia		7573	UTASTheUniversityofTasmaniaAU	false
197.123.124.20	unknown	Egypt		36992	ETISALAT-MISREG	false
197.93.232.146	unknown	South Africa		10474	OPTINETZA	false
197.0.2.28	unknown	Tunisia		37705	TOPNETTN	false
41.228.82.100	unknown	Tunisia		37492	ORANGE-TN	false
157.162.179.20	unknown	Germany		22192	SSHENETUS	false
157.146.249.255	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
85.4.217.132	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
157.193.139.197	unknown	Belgium		2611	BELNETBE	false
189.207.91.25	unknown	Mexico		6503	AxtelSABdeCVMX	false
169.18.126.94	unknown	United States		37611	AfrihostZA	false
157.182.219.38	unknown	United States		12118	WVUUS	false
157.50.48.74	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
157.105.159.172	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
197.205.103.249	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.74.15.31	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
197.129.48.122	unknown	Morocco		6713	IAM-ASMA	false
209.146.51.20	unknown	United States		395753	KKRUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.274262520522586
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	OMnyIKuNNF.elf
File size:	63296
MD5:	8406babfb9b432ee244575aa2e3f63fe
SHA1:	22761d5d5c43e0251bab907054066239a8f35b61
SHA256:	9a067e32dd6c25053c302de7caf61cdc0f3982289eb91d06c449fe08a47fc6d3
SHA512:	c2b9ac112b18050fb243b65a5b220d706c2100df0b55b93c6876f1623fee42c67696cd0fd855b4164aca9025174a2e386a6060f1f7bec96bef9b73e727fd6ba5
SSDEEP:	1536:dpmbSQ6U3q7cCBT/lZsK/0DiQNLiKimfFoktCe3fYRMD:WShU3q7cEDlCK/0D19i8Fok06fYRw
TLSH:	0B534B17B58280FDC09AC1744B2BBA3AD93775FD0378B2A677D0EB262CA6D211E1DD44
File Content Preview:	.ELF.....>.....@.....@.....@.8...@.....@.....@.....P.....P.....Q.td.....H...._... .:...H.....

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	

Copyright Joe Security LLC 2023

ELF header	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x4000e8	0xe8	0x13	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x400100	0x100	0xc866	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x40c966	0xc966	0xe	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x40c980	0xc980	0x2390	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x50f000	0xf000	0x10	0x0	0x3	WA	0	0	8
.dtors	PROGBITS	0x50f010	0xf010	0x10	0x0	0x3	WA	0	0	8
.data	PROGBITS	0x50f040	0xf040	0x440	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x50f480	0xf480	0x2a10	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xf480	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0xed10	0xed10	6.4016	0x5	R E	0x100000		.init .text .fini .rodata
LOAD	0xf000	0x50f000	0x50f000	0x480	0x2e90	2.1644	0x6	RW	0x100000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x8		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23197.39.195.635581237215283522203/21/23-07:11:34.483333	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55812	37215	192.168.2.23	197.39.195.63
192.168.2.23197.234.59.534034637215283522203/21/23-07:10:23.199102	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40346	37215	192.168.2.23	197.234.59.53
192.168.2.23147.46.122.923662037215283522203/21/23-07:11:56.415741	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36620	37215	192.168.2.23	147.46.122.92
192.168.2.2341.233.131.219529783721528352220 3/21/23-07:10:55.747017	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52978	37215	192.168.2.23	41.233.131.219
192.168.2.238.8.8.854536532023883 03/21/23-07:09:52.583756	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	54536	53	192.168.2.23	8.8.8.8
156.224.24.249192.168.2.2356999477962030489 03/21/23-07:11:48.637846	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	47796	156.224.24.249	192.168.2.23
192.168.2.2341.36.213.188393837215283522203/21/23-07:10:30.344361	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39138	37215	192.168.2.23	41.36.213.188
192.168.2.23197.39.34.188590237215283522203/21/23-07:10:07.047772	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59102	37215	192.168.2.23	197.39.34.188

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2386.69.66.253 58844372152835222 03/21/23-07:10:54.644031	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58844	37215	192.168.2.23	86.69.66.253
192.168.2.23157.157.112.175546563721528352222 03/21/23-07:09:59.757322	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54656	37215	192.168.2.23	157.157.112.175
192.168.2.23172.65.204.144436983721528352222 03/21/23-07:11:38.525358	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43698	37215	192.168.2.23	172.65.204.144
192.168.2.23197.39.190.244482763721528352222 03/21/23-07:11:01.870921	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48276	37215	192.168.2.23	197.39.190.244
192.168.2.2341.62.43.160 47544372152835222 03/21/23-07:11:51.897568	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47544	37215	192.168.2.23	41.62.43.160
192.168.2.23197.39.167.7 139372372152835222 03/21/23-07:10:39.495843	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39372	37215	192.168.2.23	197.39.167.71
192.168.2.23197.148.89.120490983721528352222 03/21/23-07:11:41.620198	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49098	37215	192.168.2.23	197.148.89.120
192.168.2.23156.224.24.249477965699920304900 03/21/23-07:09:52.816652	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	47796	56999	192.168.2.23	156.224.24.249
192.168.2.23213.176.10.176532903721528352222 03/21/23-07:11:34.410258	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53290	37215	192.168.2.23	213.176.10.176

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 07:09:52.583755970 CET	192.168.2.23	8.8.8.8	0xb28d	Standard query (0)	j.xnyidc.top	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 07:09:52.602952957 CET	8.8.8.8	192.168.2.23	0xb28d	No error (0)	j.xnyidc.top		156.224.24.249	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: OMnylKuNNF.elf PID: **6227**, Parent PID: **6126**

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/tmp/OMnylKuNNF.elf
Arguments:	/tmp/OMnylKuNNF.elf
File size:	63296 bytes
MD5 hash:	8406babfb9b432ee244575aa2e3f63fe

Analysis Process: OMnylKuNNF.elf PID: **6228**, Parent PID: **6227**

General	
Start time:	07:09:51
Start date:	21/03/2023
Path:	/tmp/OMnylKuNNF.elf
Arguments:	n/a
File size:	63296 bytes
MD5 hash:	8406babfb9b432ee244575aa2e3f63fe

Analysis Process: sh PID: **6228**, Parent PID: **6227**

General	
Start time:	07:09:51
Start date:	21/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/systemd && mkdir bin; >2\\xffbin/systemd && mv /tmp/OMnylKuNNF.elf bin/systemd; chmod 777 bin/systemd"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6229**, Parent PID: **6228**

General	
Start time:	07:09:51
Start date:	21/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6229**, Parent PID: **6228**

General	
Start time:	07:09:51
Start date:	21/03/2023
Path:	/usr/bin/rm
Arguments:	rm -rf bin/systemd
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: sh PID: **6230**, Parent PID: **6228**

General	
Start time:	07:09:51
Start date:	21/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **6230**, Parent PID: **6228**

General	
Start time:	07:09:51

Copyright Joe Security LLC 2023

Start date:	21/03/2023
Path:	/usr/bin/mkdir
Arguments:	mkdir bin
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

Analysis Process: sh PID: 6231, Parent PID: 6228

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: 6231, Parent PID: 6228

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/systemd
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Analysis Process: OMnylKuNNF.elf PID: 6232, Parent PID: 6227

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/tmp/OMnylKuNNF.elf
Arguments:	n/a
File size:	63296 bytes
MD5 hash:	8406babfb9b432ee244575aa2e3f63fe

Analysis Process: OMnylKuNNF.elf PID: 6233, Parent PID: 6232

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/tmp/OMnylKuNNF.elf
Arguments:	n/a
File size:	63296 bytes
MD5 hash:	8406babfb9b432ee244575aa2e3f63fe

File Activities

File Read

Directory Enumerated

Analysis Process: OMnylKuNNF.elf PID: 6234, Parent PID: 6232

General

Start time:	07:09:51
Start date:	21/03/2023
Path:	/tmp/OMnylKuNNF.elf
Arguments:	n/a
File size:	63296 bytes
MD5 hash:	8406babfb9b432ee244575aa2e3f63fe