ID: 679639
Sample Name: notabotnet.arm6
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:00:21
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

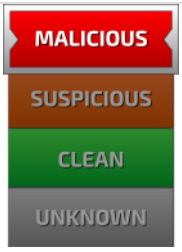
notabotnet.arm6

Overview

General Information

Sample Name:	notabotnet.arm6
Analysis ID:	679639
MD5:	15b8885e01b36d.
SHA1:	ce2cbb334f644c…
SHA256:	4d2f8ca7808ac8…
Tags:	Mirai
Infos:	

Detection



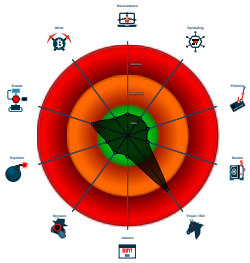
Mirai

Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Sample contains strings indicative o…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture.

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

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679639
Start date and time: 06/08/202208:00:21	2022-08-06 08:00:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	notabotnet.arm6
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
Detection:	MAL
Classification:	mal56.troj.linARM6@0/0@0/0

Runtime Messages

Command:	/tmp/notabotnet.arm6
PID:	6231
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False

Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - core dumped

Process Tree

- **system is lnxubuntu20**
  - notabotnet.arm6 (PID: 6231, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/notabotnet.arm6
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
notabotnet.arm6	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x15638:$xo1: Dfs`eeh&<'9 • 0x156b0:$xo1: Dfs`eeh&<'9 • 0x15724:$xo1: Dfs`eeh&<'9 • 0x15794:$xo1: Dfs`eeh&<'9 • 0x157e0:$xo1: Dfs`eeh&<'9
notabotnet.arm6	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6231.1.00007f067c017000.00007f067c02d000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x15638:$xo1: Dfs`eeh&<'9 • 0x156b0:$xo1: Dfs`eeh&<'9 • 0x15724:$xo1: Dfs`eeh&<'9 • 0x15794:$xo1: Dfs`eeh&<'9 • 0x157e0:$xo1: Dfs`eeh&<'9
6231.1.00007f067c017000.00007f067c02d000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
Process Memory Space: notabotnet.arm6 PID: 6231	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

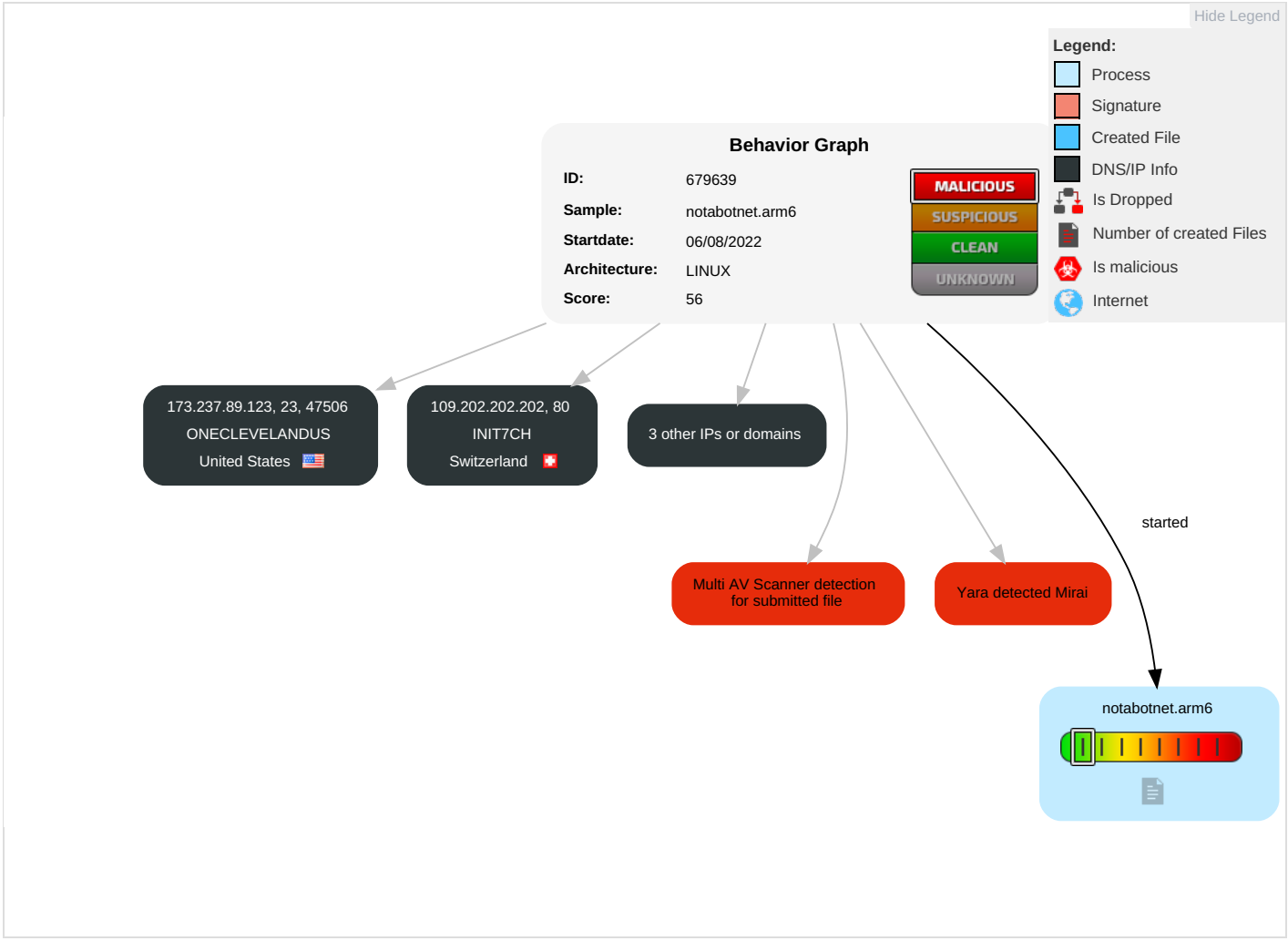
Mitre Att&ck Matrix

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	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	1 1 Security Software 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	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
notabotnet.arm6	51%	Virustotal		Browse
notabotnet.arm6	59%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://cnc.fearfulcats.tk/notabotnet/notabotnet.arm7	9%	Virustotal		Browse
http://cnc.fearfulcats.tk/notabotnet/notabotnet.arm7	100%	Avira URL Cloud	malware	

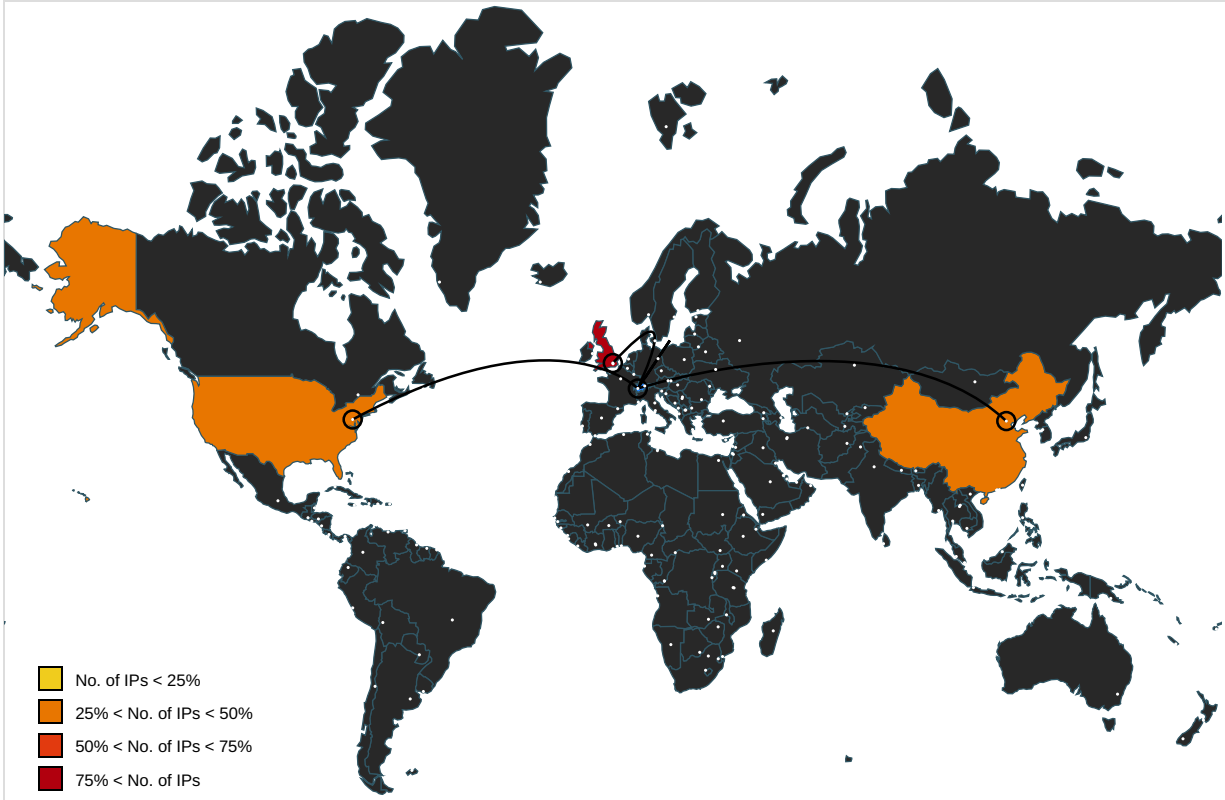
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.237.89.123	unknown	United States		19009	ONECLEVELANDUS	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
60.20.44.123	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	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 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.082599753088192
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	notabotnet.arm6
File size:	91440
MD5:	15b8885e01b36d260d68f181a8ad234b
SHA1:	ce2cbb334f644c3f906921a84af315ef8bde768a
SHA256:	4d2f8ca7808ac88293ea0bbf579e7dc3d2dbe70971a18701f7d58bf44d4c72a6
SHA512:	9170825222786ea370304daf7a4d54e50f45e0a3553f0250e748812d8cb9b2736fdc24aa368da243b6fe16faafacc9e28e6cf8da66956e643a8a5dff6e6ddafc
SSDEEP:	1536:Z2NnKIfKjRGp7qs9GwHlGM0ZCuyj7wFWJ70q9dyCgIEHzUlhiqmk7myifIv:ZNIiVIqkGgdyCujGYq9kC0mk7myi
TLSH:	459319C6BC409E14C6C616B7FA2F108E3302579DE2DEB352CD155F747BCA82B0E2A55A
File Content Preview:	.ELF.....(.....T...4...Pc.....4. ...(..... \.. \.....`...`...`.....Q.td.....-...L.....@-.,@...0....S.....0....S...../..0...0...@..../..b.....`....-.@0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8154
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	90960
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x141ac	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1c25c	0x1425c	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1c26c	0x1426c	0x19b4	0x0	0x2	A	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.init_array	INIT_ARRAY	0x26004	0x16008	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x26008	0x1600c	0x4	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x26010	0x16014	0x74	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x26084	0x16088	0x258	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x262dc	0x162e0	0x27c4	0x0	0x3	WA	0	0	4
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x162e0	0x10	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x162f0	0x5d	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	0x8000	0x8000	0x15c20	0x15c20	6.1393	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x16004	0x26004	0x26000	0x2dc	0xaa9c	3.6598	0x6	RW	0x8000		.init_array .fini_array .got .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 14

- 23 (Telnet)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: notabotnet.arm6 PID: **6231**, Parent PID: **6123**

General

Start time:	08:01:04
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm6
Arguments:	/tmp/notabotnet.arm6
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read