ID: 679632
Sample Name: MUuRNNXESN
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:35:37
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

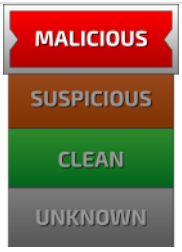
MUuRNNXESN

Overview

General Information

Sample Name:	MUuRNNXESN
Analysis ID:	679632
MD5:	99edb6a756fdffc..
SHA1:	22d88f2e2e1e19..
SHA256:	53daedfc1abe34..
Tags:	32 elf mirai renesas
Infos:	

Detection



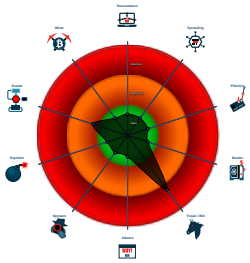
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara signature match
- Sample contains strings that are po…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Sample listens on a socket
- Sample contains strings indicative o…

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679632
Start date and time: 06/08/202207:35:37	2022-08-06 07:35:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MUuRNNXESN
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:	mal64.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/MUuRNNXESN
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- MUuRNNXESN (PID: 6230, Parent: 6125, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/MUuRNNXESN
  - MUuRNNXESN New Fork (PID: 6232, Parent: 6230)
  - MUuRNNXESN New Fork (PID: 6233, Parent: 6230)
  - MUuRNNXESN New Fork (PID: 6235, Parent: 6230)
    - MUuRNNXESN New Fork (PID: 6238, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6239, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6243, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6245, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6246, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6247, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6248, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6253, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6254, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6255, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6256, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6261, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6263, Parent: 6235)
    - MUuRNNXESN New Fork (PID: 6264, Parent: 6235)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
MUuRNNXESN	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	0x19f38:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19fa8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a018:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a088:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a0f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a368:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a3bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a410:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a464:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a4b8:$xo1: oMXKNNC\x0D\x17\x0C\x12
MUuRNNXESN	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6230.1.00007f4db442c000.00007f4db442d000.rw-.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	0x584:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x5f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x66c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x6e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x754:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x9d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xadc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6233.1.00007f4db4400000.00007f4db441b000.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	0x19f38:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19fa8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a018:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a088:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a0f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a368:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a3bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a410:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a464:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a4b8:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6233.1.00007f4db4400000.00007f4db441b000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6230.1.00007f4db4400000.00007f4db441b000.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	• 0x19f38:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19fa8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a018:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a088:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a0f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a368:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a3bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a410:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a464:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a4b8:$xo1: oMXKNNC\x0D\x17\x0C\x12
6230.1.00007f4db4400000.00007f4db441b000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 1 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

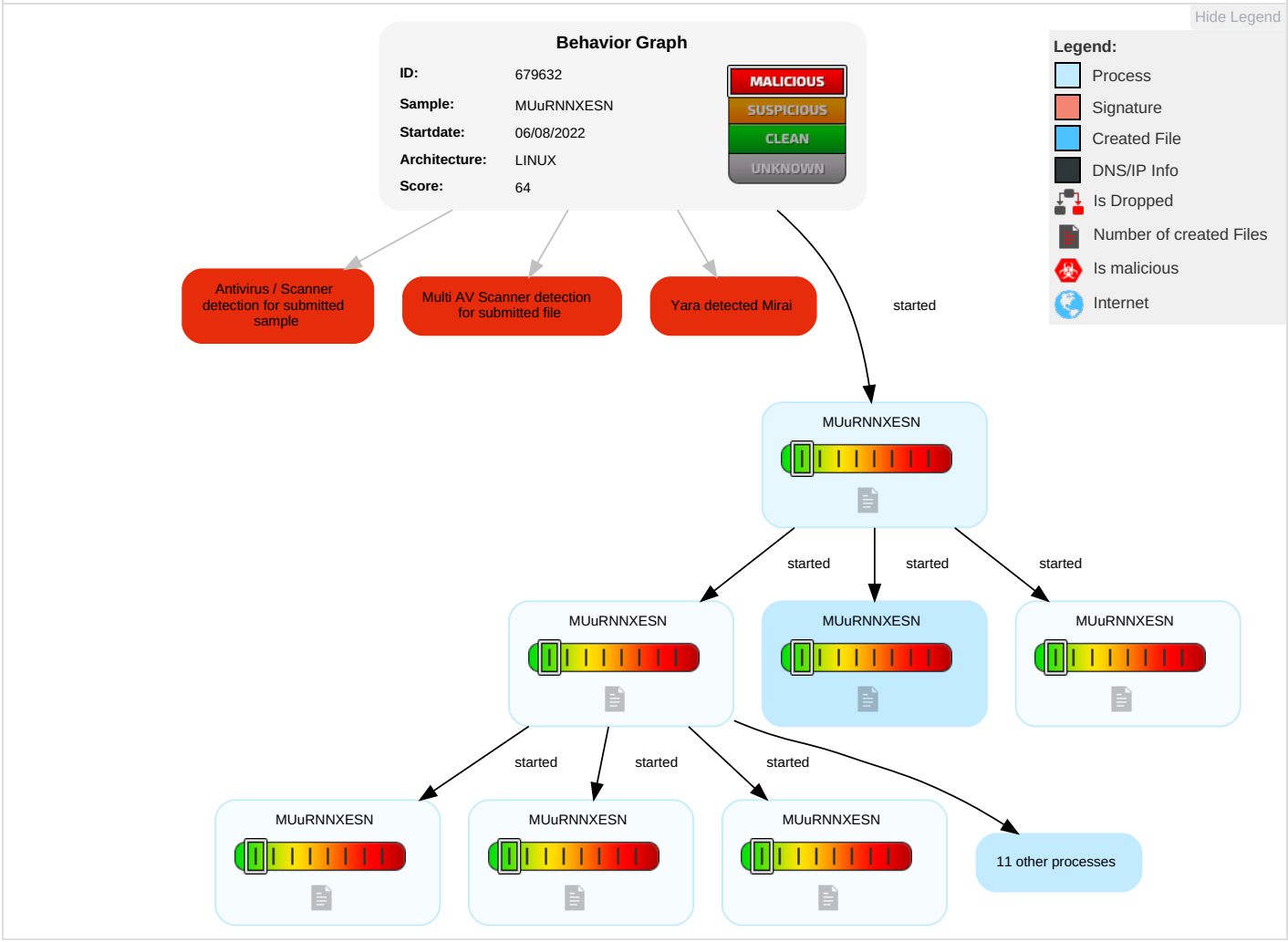
Mitre Att&ck Matrix

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	1 Command and Scripting Interpreter	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MUuRNNXESN	51%	Virustotal		Browse
MUuRNNXESN	52%	ReversingLabs	Linux.Trojan.Mirai	
MUuRNNXESN	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://46.23.109.47/Cloud/Gpon.sh	19%	Virustotal		Browse
http://46.23.109.47/Cloud/Gpon.sh	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.x86	18%	Virustotal		Browse
http://46.23.109.47/Cloud/Cloud.x86	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://46.23.109.47/Cloud/Comtrend.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&sessionKey=1039230114	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Netlink.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&waninf=1_INTERNET_R_VI	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mpsl;chmod	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mips;	100%	Avira URL Cloud	malware	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://0.0.0.0/Cloud/Cloud.x86	0%	Avira URL Cloud	safe	
http://46.23.109.47/Cloud/Dlink.sh%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs

No contacted IP infos

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, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.842017488315144
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	MUuRNNXESN
File size:	111724
MD5:	99edb6a756fdffce917217e1b5804ddf
SHA1:	22d88f2e2e1e19e78fda1a4963d74117c1a076c2
SHA256:	53daedfc1abe3477c33ecdedb8a8243fabcd5e5bb6bff55e8da14dc75fdc7efb
SHA512:	439cbbf92451d89ddf4ace00b958137d33a15a946be07bdea2e963d8347c02ffb93c4d4749d8d4a3a982958d156a647371db292f6766eea8f66c265183e635a0
SSDEEP:	1536:XYaPcU+0/umiqAL6s179culEl0zGGytofs34S6E/ZjJuJtmGtICkgEy2R:IgcUp2mn7s179cuAOf+4zEfjuJtmGtI
TLSH:	68B39E21D0E0EDE4C2604634B2E1E93EC336DD0874972DF6F645CA99504BED8F5A93BA
File Content Preview:	.ELF.....*.....@.4.....4. ... (.....@...@.....B...B.....Q.td....././"O.n.....#.*@.....#.*@.....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	111324
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0x180c0	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x4181a0	0x181a0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4181c4	0x181c4	0x2ae4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x42b000	0x1b000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x42b008	0x1b008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x42b014	0x1b014	0x288	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x42b29c	0x1b29c	0xa70	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1b29c	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	0x1aca8	0x1aca8	6.8939	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1b000	0x42b000	0x42b000	0x29c	0xd0c	2.9373	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: MUuRNNXESN PID: 6230, Parent PID: 6125

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	/tmp/MUuRNNXESN
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: MUuRNNXESN PID: 6232, Parent PID: 6230

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: MUuRNNXESN PID: 6233, Parent PID: 6230

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: 6235, Parent PID: 6230

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: 6238, Parent PID: 6235

General

Start time:	07:36:23

Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6239**, Parent PID: **6235**

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6243**, Parent PID: **6235**

General

Start time:	07:36:23
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6245**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6246**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6247**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6248**, Parent PID: **6235**

General

Start time:	07:36:24

Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6253**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6254**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6255**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6256**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6261**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6263**, Parent PID: **6235**

General

Start time:	07:36:24

Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: MUuRNNXESN PID: **6264**, Parent PID: **6235**

General

Start time:	07:36:24
Start date:	06/08/2022
Path:	/tmp/MUuRNNXESN
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9