ID: 626438
Sample Name: NE8O7liu0s
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:14:54
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

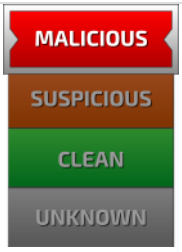
NE8O7liu0s

Overview

General Information

Sample Name:	NE8O7liu0s
Analysis ID:	626438
MD5:	2bbe3dc5b85619..
SHA1:	ef6be828cf9071e..
SHA256:	598e89a664e3e6.
Tags:	32 elf mips mirai
Infos:	

Detection



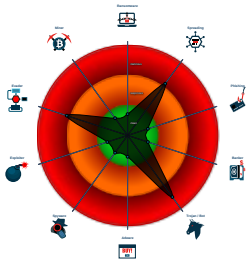
Mirai

Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely that the sample will exhibit less behavior.

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626438
Start date and time: 14/05/202202:14:54	2022-05-14 02:14:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NE8O7liu0s
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:	mal92.spre.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/NE8O7liu0s
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	kebabware installed

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- NE8O7liu0s (PID: 6225, Parent: 6124, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/NE8O7liu0s
  - NE8O7liu0s New Fork (PID: 6227, Parent: 6225)
    - NE8O7liu0s New Fork (PID: 6229, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6230, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6232, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6233, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6237, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6239, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6241, Parent: 6227)
    - NE8O7liu0s New Fork (PID: 6243, Parent: 6227)
- gnome-session-binary New Fork (PID: 6283, Parent: 1477)
  - sh (PID: 6283, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6283, Parent: 1477, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6289, Parent: 6283)
      - gsd-print-notifications New Fork (PID: 6290, Parent: 6289)
        - gsd-printer (PID: 6290, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- xfce4-session New Fork (PID: 6313, Parent: 1900)
  - rm (PID: 6313, Parent: 1900, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
NE8O7liu0s	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x8600:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x866f:$s2: $Id: UPX • 0x8620:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6225.1.000000000ef6297b.000000006d73a7a2.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	• 0x14f0:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1560:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1620:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
6229.1.000000000ef6297b.000000006d73a7a2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x14f0:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1560:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1620:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3

Source	Rule	Description	Author	Strings
6225.1.00000000c39c139a.00000000c17c93de.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	• 0x201f0:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x2024c:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x202e8:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
6225.1.00000000c39c139a.00000000c17c93de.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x1f470:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
6225.1.00000000c39c139a.00000000c17c93de.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Snort Signatures

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.188.50

Timestamp:	192.168.2.23172.65.188.5044500555552027153 05/14/22-02:15:56.359731
SID:	2027153
Source Port:	44500
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.193.152.180

Timestamp:	192.168.2.2388.193.152.18034398802027121 05/14/22-02:15:59.312151
SID:	2027121
Source Port:	34398
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.198.26.37

Timestamp:	192.168.2.2388.198.26.3738100802027121 05/14/22-02:15:44.516920
SID:	2027121
Source Port:	38100
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.250.122.25

Timestamp:	192.168.2.23156.250.122.2554380528692027339 05/14/22-02:15:57.938396
SID:	2027339
Source Port:	54380
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.169.95

Timestamp:	192.168.2.23172.65.169.9544990555552027153 05/14/22-02:16:03.335900
SID:	2027153
Source Port:	44990
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.221.144.129	
Timestamp:	192.168.2.2388.221.144.12941178802027121 05/14/22-02:15:49.661036
SID:	2027121
Source Port:	41178
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.67.150	
Timestamp:	192.168.2.23172.65.67.15059474555552027153 05/14/22-02:15:56.352112
SID:	2027153
Source Port:	59474
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.90.176.237	
Timestamp:	192.168.2.2388.90.176.23744584802027121 05/14/22-02:15:51.846554
SID:	2027121
Source Port:	44584
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.85.234.170	
Timestamp:	192.168.2.2388.85.234.17050988802027121 05/14/22-02:15:55.583622
SID:	2027121
Source Port:	50988
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.163.115.235	
Timestamp:	192.168.2.2388.163.115.23545742802027121 05/14/22-02:15:51.797913
SID:	2027121
Source Port:	45742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.150.139	
Timestamp:	192.168.2.23172.65.150.13942616555552027153 05/14/22-02:16:03.318542
SID:	2027153
Source Port:	42616
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.71.210	
Timestamp:	192.168.2.23172.65.71.21054402555552027153 05/14/22-02:15:56.342447
SID:	2027153
Source Port:	54402
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.39.149	
Timestamp:	192.168.2.23172.65.39.14960752555552027153 05/14/22-02:15:53.260356
SID:	2027153
Source Port:	60752

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.193.168.207	
Timestamp:	192.168.2.2388.193.168.20742388802027121 05/14/22-02:15:49.632801
SID:	2027121
Source Port:	42388
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.79.192	
Timestamp:	192.168.2.23172.65.79.19236744555552027153 05/14/22-02:15:53.242553
SID:	2027153
Source Port:	36744
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.226.58.60	
Timestamp:	192.168.2.23156.226.58.6036698528692027339 05/14/22-02:15:56.717589
SID:	2027339
Source Port:	36698
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.178.37	
Timestamp:	192.168.2.23172.65.178.3742472555552027153 05/14/22-02:15:44.534691
SID:	2027153
Source Port:	42472
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.30.39	
Timestamp:	192.168.2.23172.65.30.39436765555552027153 05/14/22-02:15:48.668722
SID:	2027153
Source Port:	43676
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.130.160	
Timestamp:	192.168.2.23172.65.130.16035856555552027153 05/14/22-02:15:53.242653
SID:	2027153
Source Port:	35856
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.245.44.43	
Timestamp:	192.168.2.23156.245.44.4350224528692027339 05/14/22-02:16:04.452185
SID:	2027339
Source Port:	50224
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.125.107.25

Timestamp:	192.168.2.2388.125.107.2537604802027121 05/14/22-02:15:51.892368
SID:	2027121
Source Port:	37604
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.7.26

Timestamp:	192.168.2.23172.65.7.2655700555552027153 05/14/22-02:15:46.602305
SID:	2027153
Source Port:	55700
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.184.34

Timestamp:	192.168.2.23172.65.184.3435476555552027153 05/14/22-02:15:48.685886
SID:	2027153
Source Port:	35476
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.148.69.67

Timestamp:	192.168.2.2388.148.69.6734326802027121 05/14/22-02:16:01.433501
SID:	2027121
Source Port:	34326
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.247.118.29

Timestamp:	192.168.2.2388.247.118.2940302802027121 05/14/22-02:15:58.044039
SID:	2027121
Source Port:	40302
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.228.227.251

Timestamp:	192.168.2.2388.228.227.25145998802027121 05/14/22-02:15:49.667990
SID:	2027121
Source Port:	45998
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

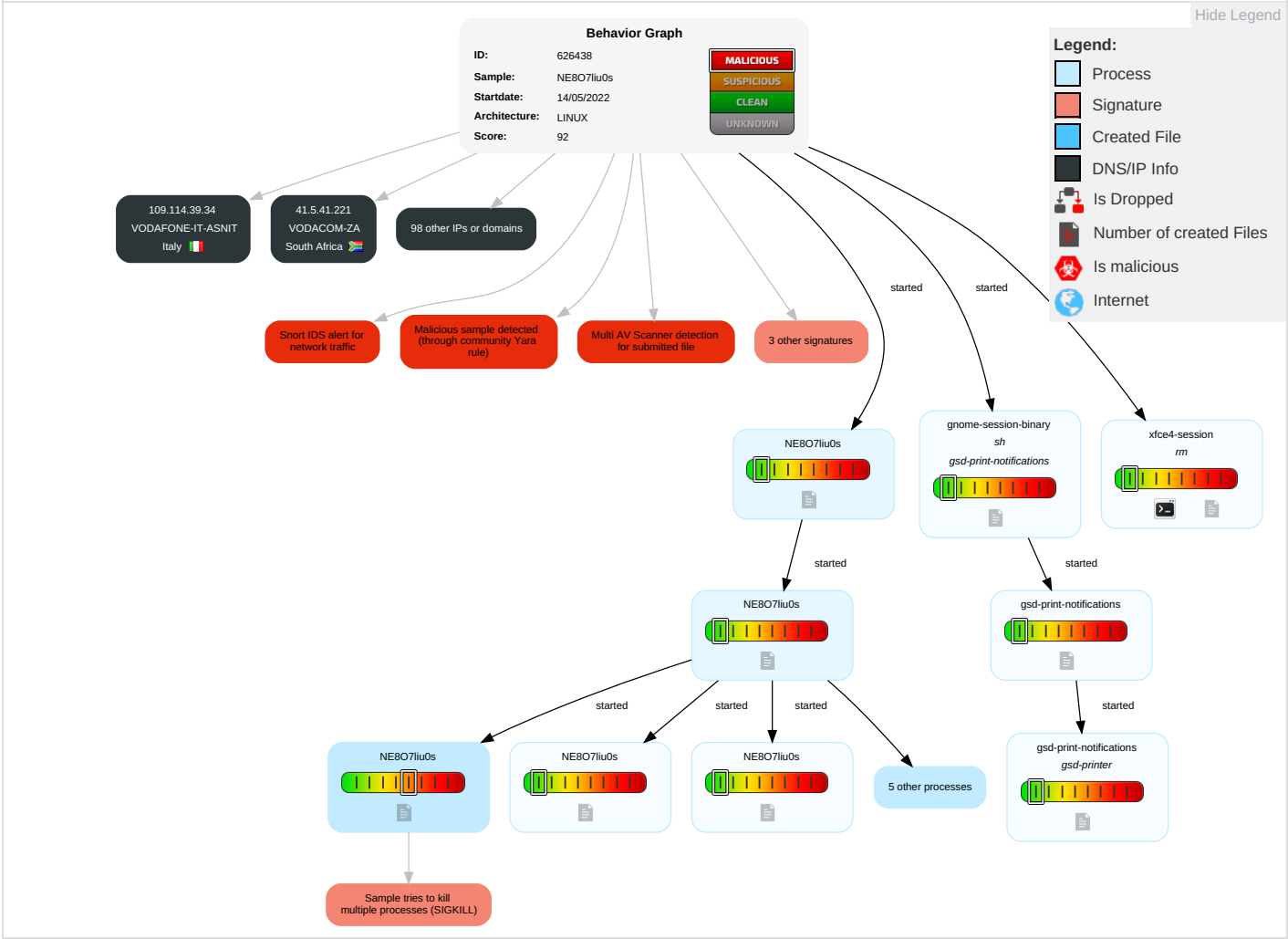
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	1 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	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	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)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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	4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	3 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NE8O7liu0s	28%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:80/tmUnblock.cgi	0%	Virustotal		Browse
http://127.0.0.1:80/tmUnblock.cgi	0%	Avira URL Cloud	safe	
http://103.136.43.52/bin	0%	Avira URL Cloud	safe	
http://103.136.43.52/zyxel.sh;	0%	Avira URL Cloud	safe	
http://103.136.43.52/bins/Tsunami.mips;	0%	Avira URL Cloud	safe	
http://103.136.43.52/bins/Tsunami.x86	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

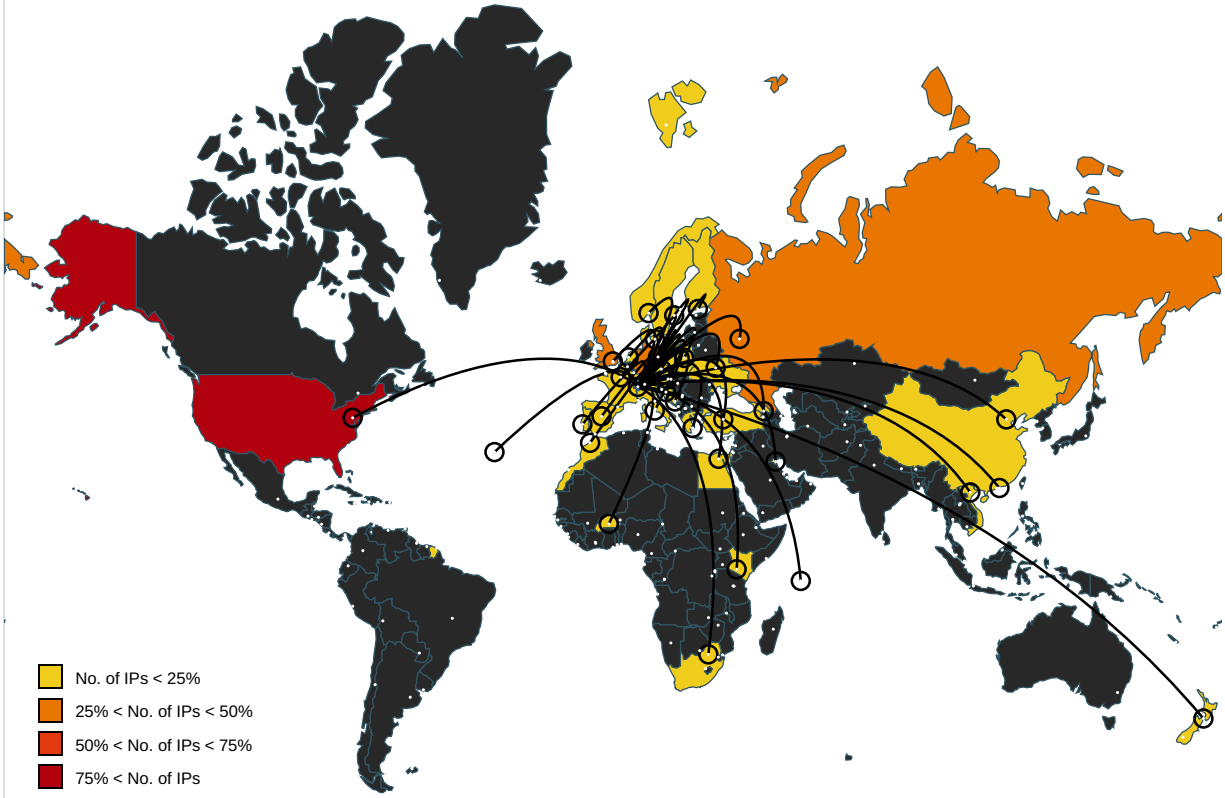
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/tmUnblock.cgi	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.139.26.110	unknown	United States		3356	LEVEL3US	false
85.71.136.30	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
85.25.248.125	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
85.18.200.236	unknown	Italy		12874	FASTWEBIT	false
85.21.46.64	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
157.214.20.165	unknown	United States		4704	SANNETRakutenMobileIncJP	false
94.250.37.203	unknown	Bosnia and Herzegowina		25144	TELEKOM-SRPSKE-ASKraljaPetraIKaradjordjevica61aBA	false
172.55.124.7	unknown	United States		21928	T-MOBILE-AS21928US	false
184.77.151.6	unknown	United States		16509	AMAZON-02US	false
98.27.141.240	unknown	United States		10796	TWC-10796-MIDWESTUS	false
98.206.117.102	unknown	United States		7922	COMCAST-7922US	false
184.43.77.0	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
42.117.139.131	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false
172.72.181.240	unknown	United States		11426	TWC-11426-CAROLINASUS	false
31.179.180.12	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
212.157.35.227	unknown	France		702	UUNETUS	false
79.12.221.153	unknown	Italy		3269	ASN-IBSNAZIT	false
62.187.196.200	unknown	European Union		34456	RIALCOM-ASRU	false
79.169.109.126	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
62.145.208.26	unknown	Netherlands		33915	TNF-ASNL	false
62.118.118.92	unknown	Russian Federation		8359	MTSRU	false
88.243.145.6	unknown	Turkey		9121	TTNETTR	false
156.223.192.114	unknown	Egypt		8452	TE-ASTE-ASEG	false
62.152.157.231	unknown	Poland		1902	PAN-NETDeutscheTelekomPan-NetsroSK	false
62.219.245.8	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
85.182.60.117	unknown	Germany		6805	TDDE-ASN1DE	false
172.12.143.81	unknown	United States		7018	ATT-INTERNET4US	false
94.128.103.33	unknown	Kuwait		47589	KTC3GKW	false
31.196.12.210	unknown	Italy		3269	ASN-IBSNAZIT	false
212.13.196.8	unknown	United Kingdom		8943	JUMPGB	false
31.118.153.247	unknown	United Kingdom		12576	EELtdGB	false
41.116.238.229	unknown	South Africa		16637	MTNNS-ASZA	false
41.214.230.3	unknown	Morocco		36925	ASMediMA	false
94.69.81.96	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
184.237.135.2	unknown	United States		10507	SPCSUS	false
184.37.225.200	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
94.153.184.212	unknown	Ukraine		15895	KSNET-ASUA	false
94.114.237.26	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
31.134.158.117	unknown	Russian Federation		42668	NEVALINK-ASRU	false
31.230.126.168	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
156.223.192.121	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.172.168.202	unknown	South Africa		36937	Neotel-ASZA	false
184.37.225.208	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
31.233.207.174	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
62.122.49.242	unknown	Russian Federation		47530	NVTC-ASRU	false
172.65.108.217	unknown	United States		13335	CLOUDFLARENETUS	false
178.195.108.155	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
184.62.170.5	unknown	United States		7155	VIASAT-SP-BACKBONEUS	false
95.121.137.208	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
94.250.142.185	unknown	Croatia (LOCAL Name: Hrvatska)		12810	VIPNET-AS3GGSMandInternetServiceProviderHR	false
41.114.147.165	unknown	South Africa		16637	MTNNS-ASZA	false
184.13.229.62	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
172.115.197.166	unknown	United States		20001	TWC-20001-PACWESTUS	false
184.158.254.154	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
62.80.165.193	unknown	Ukraine		25386	INTERTELECOM-ASUA	false
85.136.26.144	unknown	Spain		12357	COMUNITELSPAINES	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.87.78.101	unknown	United States		393951	HORTONS-TVUS	false
95.252.144.239	unknown	Italy		3269	ASN-IBSNAZIT	false
212.76.212.201	unknown	Germany		12571	INCAS-ASKrefeldGermanyDE	false
94.22.197.197	unknown	Finland		15527	ANVIASilmukkatie6VaasaFinlandFI	false
172.72.181.219	unknown	United States		11426	TWC-11426-CAROLINASUS	false
31.212.88.218	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
31.253.231.71	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
197.232.116.123	unknown	Kenya		36866	JTLKE	false
212.188.118.230	unknown	Russian Federation		49154	MTS-DOM-ASRU	false
98.153.132.43	unknown	United States		20001	TWC-20001-PACWESTUS	false
95.81.253.240	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
62.23.59.142	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
184.179.195.6	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
62.105.89.80	unknown	United Kingdom		5413	AS5413GB	false
31.146.6.154	unknown	Georgia		35805	SILKNET-ASGE	false
94.9.108.45	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
85.90.55.64	unknown	United Kingdom		39116	TELEHOUSEGB	false
95.55.190.176	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
184.63.30.65	unknown	United States		7155	VIASAT-SP-BACKBONEUS	false
94.54.78.135	unknown	Turkey		47524	TURKSAT-ASTR	false
95.166.18.160	unknown	Denmark		3292	TDCTDCASDK	false
37.58.70.142	unknown	Netherlands		36351	SOFTLAYERUS	false
184.236.201.56	unknown	United States		10507	SPCSUS	false
118.28.71.41	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
85.136.26.133	unknown	Spain		12357	COMUNITELSPAINES	false
210.55.200.54	unknown	New Zealand		4648	SPARK-NZGlobal-GatewayInternetNZ	false
5.205.27.174	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
42.200.120.220	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	false
157.249.142.116	unknown	Norway		224	UNINETTUNINETTTheNorwegianUniversityResearchNetwork	false
184.73.107.159	unknown	United States		14618	AMAZON-AESUS	false
31.121.171.220	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
98.105.141.154	unknown	United States		6167	CELLCO-PARTUS	false
95.53.226.227	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
184.89.14.254	unknown	United States		33363	BHN-33363US	false
41.216.159.6	unknown	Burkina Faso		37073	IPP-burkina-asBF	false
156.249.231.186	unknown	Seychelles		26484	IKGUL-26484US	false
41.5.41.221	unknown	South Africa		29975	VODACOM-ZA	false
184.172.50.13	unknown	United States		36351	SOFTLAYERUS	false
157.186.91.142	unknown	Russian Federation		22192	SSHENETUS	false
85.226.77.39	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
109.114.39.34	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
79.93.89.21	unknown	France		15557	LDCOMNETFR	false
85.126.133.246	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
31.163.227.21	unknown	Russian Federation		12389	ROSTELECOM-ASRU	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.92256083220724
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	NE8O7liu0s
File size:	36540
MD5:	2bbe3dc5b85619b7207ec547f6a78508
SHA1:	ef6be828cf9071e4514628bbea20d281d549e70c
SHA256:	598e89a664e3e67a264dc70c0c2328dc56359e05ad6061fc34d8c15770971ba5
SHA512:	ffcfac0ec66bdbed4986a2b56f7f7bdcb94660558182be6ed41a76a85bcb87edea10b98092e5d2263b10131ef725a9d5b30be1d05d118864df15a11505035f78
SSDEEP:	768:QzbT6ykD0dgr/v11BbBLmFRlf3XGo4cWuwNE/WO:QzSykDpr/v1bJmp2C
TLSH:	FEF2E0DFB2903B98C93D1C79158E2F692D50A2DC32DE0768E7065CCCFA0A55BF2081B6
File Content Preview:	.ELF.....Pz..4.....4. ... (.....T...T.C.T.C.....xUPX!d.....D...D.....V.....?.E.h;....#.....b.L#32..z..NXk.....u...*.);.....,E..B.....@S...9...u...<.....v.....p?

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0

ELF header	
Entry Point Address:	0x107a50
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x8d8d	0x8d8d	4.1753	0x5	R E	0x10000		
LOAD	0x1f54	0x431f54	0x431f54	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Snort IDS Alerts

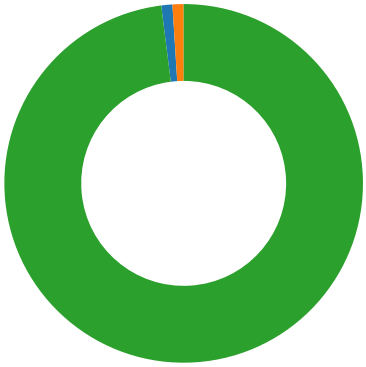
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.188.504450055555202715305/14/22-02:15:56.359731	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44500	55555	192.168.2.23	172.65.188.50
192.168.2.2388.193.152.18034398802027121 05/14/22-02:15:59.312151	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34398	80	192.168.2.23	88.193.152.180
192.168.2.2388.198.26.3738100802027121 05/14/22-02:15:44.516920	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38100	80	192.168.2.23	88.198.26.37
192.168.2.23156.250.122.2554380528692027339 05/14/22-02:15:57.938396	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54380	52869	192.168.2.23	156.250.122.25
192.168.2.23172.65.169.954499055552027153 05/14/22-02:16:03.335900	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44990	55555	192.168.2.23	172.65.169.95
192.168.2.2388.221.144.12941178802027121 05/14/22-02:15:49.661036	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41178	80	192.168.2.23	88.221.144.129
192.168.2.23172.65.67.1505947455552027153 05/14/22-02:15:56.352112	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59474	55555	192.168.2.23	172.65.67.150
192.168.2.2388.90.176.23744584802027121 05/14/22-02:15:51.846554	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44584	80	192.168.2.23	88.90.176.237
192.168.2.2388.85.234.17050988802027121 05/14/22-02:15:55.583622	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50988	80	192.168.2.23	88.85.234.170
192.168.2.2388.163.115.23545742802027121 05/14/22-02:15:51.797913	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45742	80	192.168.2.23	88.163.115.235
192.168.2.23172.65.150.1394261655552027153 05/14/22-02:16:03.318542	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42616	55555	192.168.2.23	172.65.150.139

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.71.210544025555202715305/14/22-02:15:56.342447	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54402	55555	192.168.2.23	172.65.71.210
192.168.2.23172.65.39.149607525555202715305/14/22-02:15:53.260356	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60752	55555	192.168.2.23	172.65.39.149
192.168.2.2388.193.168.207424388802027121 05/14/22-02:15:49.632801	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42388	80	192.168.2.23	88.193.168.207
192.168.2.23172.65.79.192367445555202715305/14/22-02:15:53.242553	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	36744	55555	192.168.2.23	172.65.79.192
192.168.2.23156.226.58.603669852869202733905/14/22-02:15:56.717589	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	36698	52869	192.168.2.23	156.226.58.60
192.168.2.23172.65.178.374247255555202715305/14/22-02:15:44.534691	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42472	55555	192.168.2.23	172.65.178.37
192.168.2.23172.65.30.394367655555202715305/14/22-02:15:48.668722	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43676	55555	192.168.2.23	172.65.30.39
192.168.2.23172.65.130.160358565555202715305/14/22-02:15:53.242653	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35856	55555	192.168.2.23	172.65.130.160
192.168.2.23156.245.44.435022452869202733905/14/22-02:16:04.452185	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50224	52869	192.168.2.23	156.245.44.43
192.168.2.2388.125.107.25376048020271215/14/22-02:15:51.892368	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37604	80	192.168.2.23	88.125.107.25
192.168.2.23172.65.7.2655700555552027153 05/14/22-02:15:46.602305	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55700	55555	192.168.2.23	172.65.7.26
192.168.2.23172.65.184.343547655555202715305/14/22-02:15:48.685886	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35476	55555	192.168.2.23	172.65.184.34
192.168.2.2388.148.69.6734326802027121 05/14/22-02:16:01.433501	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34326	80	192.168.2.23	88.148.69.67
192.168.2.2388.247.118.2940302802027121 05/14/22-02:15:58.044039	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40302	80	192.168.2.23	88.247.118.29
192.168.2.2388.228.227.25145998802027121 05/14/22-02:15:49.667990	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45998	80	192.168.2.23	88.228.227.251

Network Port Distribution

Total Packets: 100

- 37215 undefined
- 80 (HTTP)
- 443 (HTTPS)



TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80
- 192.168.0.14:80

System Behavior

Analysis Process: NE8O7liu0s PID: **6225**, Parent PID: **6124**

General

Start time:	02:15:40
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	/tmp/NE8O7liu0s
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: NE8O7liu0s PID: **6227**, Parent PID: **6225**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6229**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a

File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6230**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6232**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6233**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6237**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6239**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6241**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a

File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: NE8O7liu0s PID: **6243**, Parent PID: **6227**

General

Start time:	02:15:41
Start date:	14/05/2022
Path:	/tmp/NE8O7liu0s
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: **6283**, Parent PID: **1477**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6283**, Parent PID: **1477**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6283**, Parent PID: **1477**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6289**, Parent PID: **6283**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a

File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: **6290**, Parent PID: **6289**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

Directory Enumerated

Analysis Process: gsd-printer PID: **6290**, Parent PID: **1**

General

Start time:	02:17:01
Start date:	14/05/2022
Path:	/usr/libexec/gsd-printer
Arguments:	/usr/libexec/gsd-printer
File size:	31120 bytes
MD5 hash:	7995828cf98c315fd55f2ffb3b22384d

File Activities

File Read

Analysis Process: xfce4-session PID: **6313**, Parent PID: **1900**

General

Start time:	02:17:33
Start date:	14/05/2022
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: rm PID: **6313**, Parent PID: **1900**

General

Start time:	02:17:33
Start date:	14/05/2022
Path:	/usr/bin/rm
Arguments:	rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read