ID: 877738
Sample Name: yvweY4vsVq.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:52:36
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

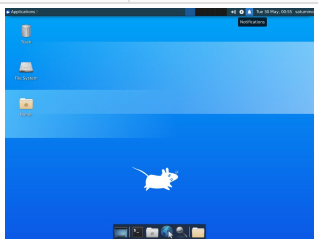
Linux Analysis Report

yvweY4vsVq.elf

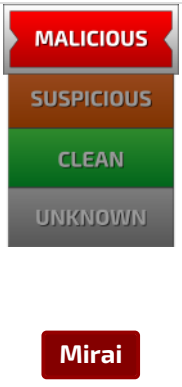
Overview

General Information

Sample Name:	yvweY4vsVq.elf
Original Sample Name:	7592df37fb3fea..
Analysis ID:	877738
MD5:	7592df37fb3fea..
SHA1:	bd612669bbc8…
SHA256:	4e97dfb181ef3…
Tags:	32 arm elf mirai
Infos:	



Detection



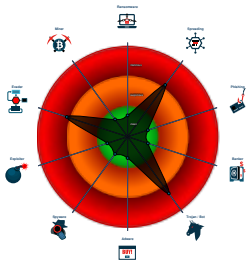
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Deletes log files
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Executes commands using a shell c…
- Executes the "systemctl" command…

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877738
Start date and time:	2023-05-30 00:52:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 14s
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:	yvweY4vsVq.elf
Original Sample Name:	7592df37fb3fea64a0994ac342f319f4.elf
Detection:	MAL
Classification:	mal68.spre.troj.evad.linELF@0/49@0/0

Warnings

Runtime Messages

Command:	/tmp/yvweY4vsVq.elf
PID:	6291
Exit Code:	0
Exit Code Info:	

Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 6198, Parent: 1)
- logrotate (PID: 6198, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 6240, Parent: 6198)
  - gzip (PID: 6240, Parent: 6198, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 6241, Parent: 6198)
  - sh (PID: 6241, Parent: 6198, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
    - sh New Fork (PID: 6242, Parent: 6241)
    - invoke-rc.d (PID: 6242, Parent: 6241, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 6243, Parent: 6242)
      - runlevel (PID: 6243, Parent: 6242, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 6245, Parent: 6242)
      - systemctl (PID: 6245, Parent: 6242, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 6249, Parent: 6242)
      - ls (PID: 6249, Parent: 6242, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 6250, Parent: 6242)
      - systemctl (PID: 6250, Parent: 6242, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 6251, Parent: 6198)
  - gzip (PID: 6251, Parent: 6198, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 6252, Parent: 6198)
  - sh (PID: 6252, Parent: 6198, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 6253, Parent: 6252)
    - rsyslog-rotate (PID: 6253, Parent: 6252, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 6254, Parent: 6253)
      - systemctl (PID: 6254, Parent: 6253, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 6199, Parent: 1)
- install (PID: 6199, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 6205, Parent: 1)
- find (PID: 6205, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 6207, Parent: 1)
- mandb (PID: 6207, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- yvweY4vsVq.elf (PID: 6291, Parent: 6127, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/yvweY4vsVq.elf
  - yvweY4vsVq.elf New Fork (PID: 6293, Parent: 6291)
  - yvweY4vsVq.elf New Fork (PID: 6295, Parent: 6291)
  - yvweY4vsVq.elf New Fork (PID: 6297, Parent: 6291)
    - yvweY4vsVq.elf New Fork (PID: 6299, Parent: 6297)
    - yvweY4vsVq.elf New Fork (PID: 6301, Parent: 6297)
    - yvweY4vsVq.elf New Fork (PID: 6303, Parent: 6297)
- **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

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

System Summary

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

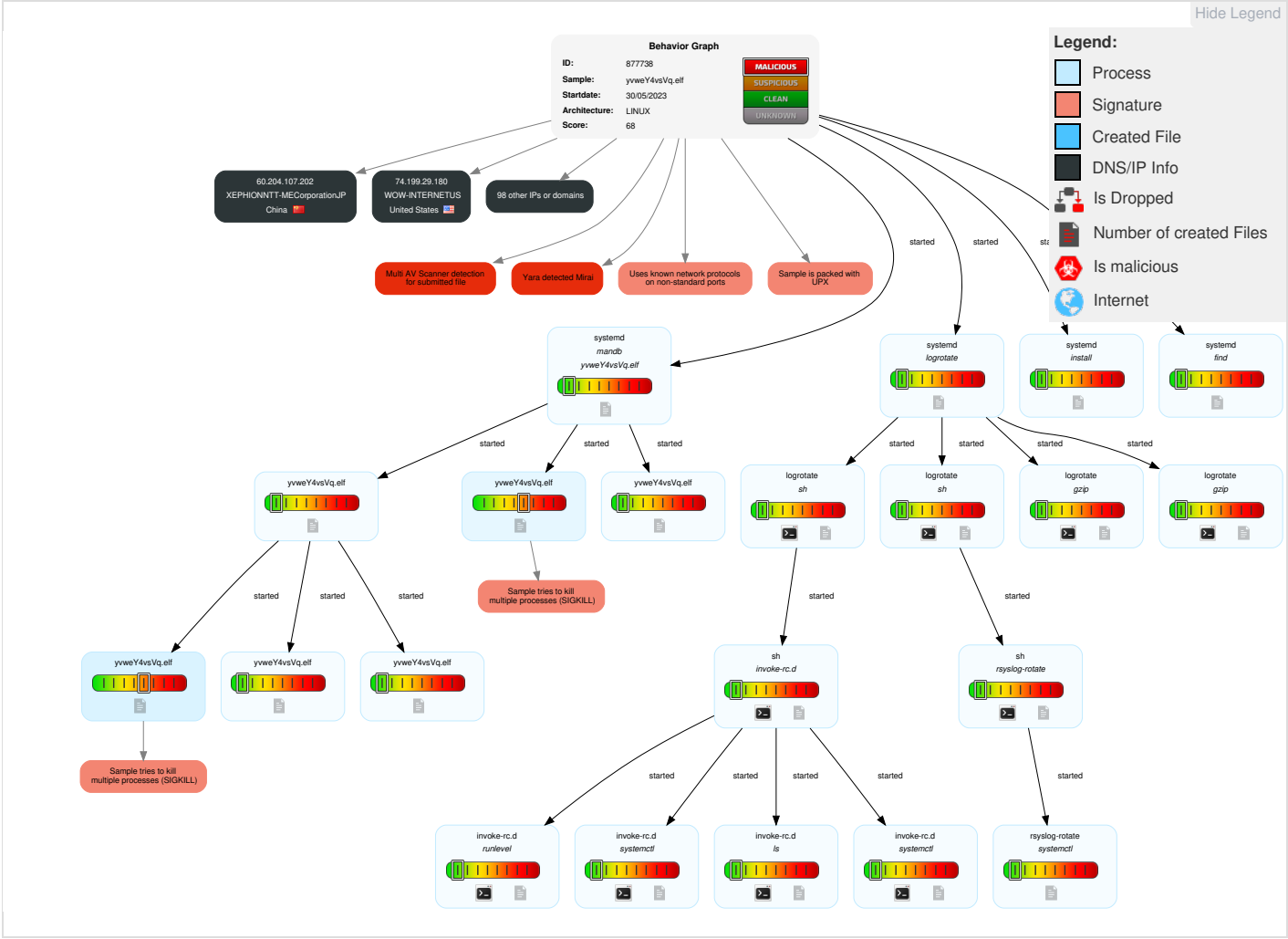
Mitre Att&ck Matrix

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	1 Scripting	1 Systemd Service	1 Systemd Service	1 Scripting	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 Indicator Removal on Host	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 1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

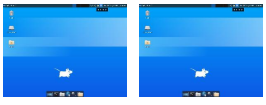
Behavior Graph

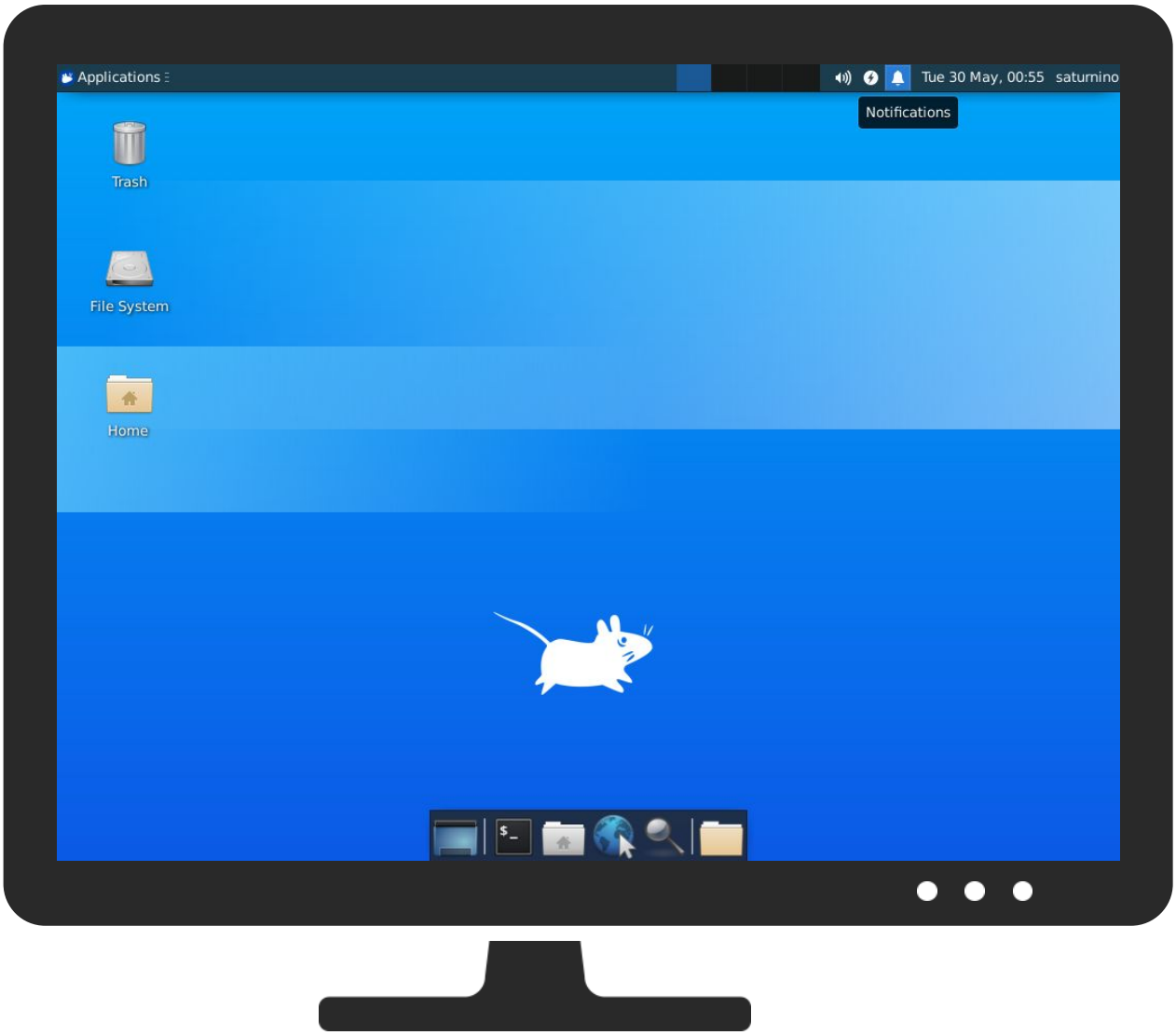


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
yvweY4vsVq.elf	54%	ReversingLabs	Linux.Trojan.Mirai	
yvweY4vsVq.elf	51%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

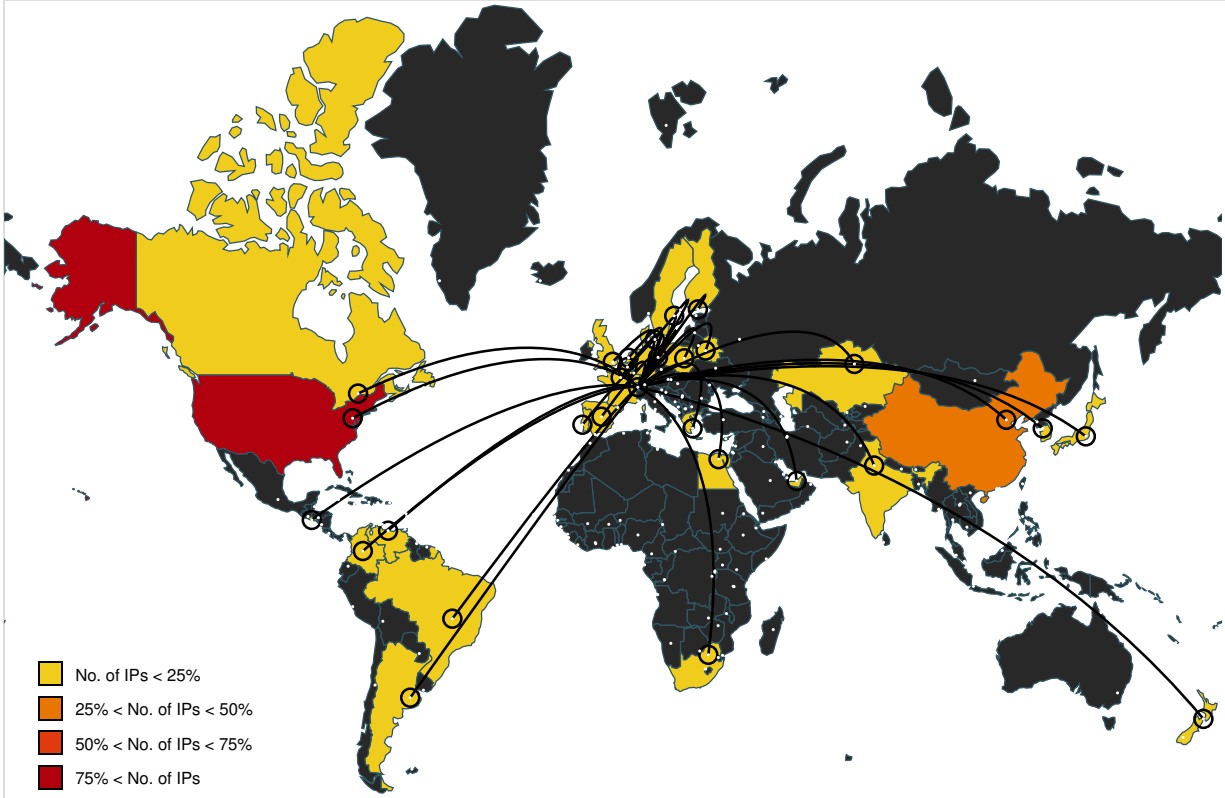
Domains and IPs

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
91.72.178.153	unknown	United Arab Emirates		15802	DU-AS1AE	false
19.194.56.75	unknown	United States		3	MIT-GATEWAYSUS	false
176.81.232.119	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
75.131.165.178	unknown	United States		20115	CHARTER-20115US	false
66.44.1.18	unknown	United States		6079	RCN-ASUS	false
216.151.48.52	unknown	United States		31869	LL-BEANUS	false
119.70.232.53	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
186.223.112.108	unknown	Brazil		28573	CLAROSABR	false
1.119.108.59	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
245.31.144.9	unknown	Reserved		unknown	unknown	false
144.24.166.220	unknown	Greece		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
118.17.139.140	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
71.82.115.201	unknown	United States		20115	CHARTER-20115US	false
152.38.145.32	unknown	United States		81	NCRENUS	false
161.212.230.79	unknown	Venezuela		6306	TELEFONICAVENEZOLANACAVE	false
146.74.158.132	unknown	United States		30051	SCCGOVUS	false
94.40.89.117	unknown	Poland		20960	TKTELEKOM-ASPL	false
95.23.180.230	unknown	Spain		12479	UNI2-ASES	false
195.249.12.67	unknown	Denmark		3292	TDCTDCASDK	false
198.207.62.225	unknown	United States		17007	OATK-AS1US	false
196.167.93.110	unknown	South Africa		328065	Vast-Networks-ASZA	false
120.64.203.192	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
241.71.207.167	unknown	Reserved		unknown	unknown	false
136.25.206.10	unknown	United States		19165	WEBPASSUS	false
204.214.223.26	unknown	United States		1239	SPRINTLINKUS	false
161.165.43.90	unknown	United States		10695	WAL-MARTUS	false
74.199.29.180	unknown	United States		12083	WOW-INTERNETUS	false
195.205.241.144	unknown	Poland		5617	TPNETPL	false
38.229.203.53	unknown	United States		23028	TEAM-CYMRUUS	false
23.121.55.94	unknown	United States		7018	ATT-INTERNET4US	false
27.231.45.76	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
205.198.24.195	unknown	United States		133847	ICT-AS-APAnppleTechEnterpriseMY	false
171.190.191.247	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
117.79.59.230	unknown	China		55990	HWCSNETHuaweiCloudServicedatacenterCN	false
48.162.218.62	unknown	United States		2686	ATGS-MMD-ASUS	false
191.45.88.178	unknown	Brazil		7738	TelemarNorteLesteSABR	false
116.62.52.238	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
181.55.62.16	unknown	Colombia		10620	TelmexColombiaSACO	false
60.204.107.202	unknown	China		9595	XEPHIONNTT-MECorporationJP	false
105.217.216.229	unknown	South Africa		16637	MTNNS-ASZA	false
78.216.161.1	unknown	France		12322	PROXADFR	false
94.104.57.239	unknown	Belgium		47377	ORANGE_BELGIUM_SAKPNBelgiumBusinessNVhasbeenacquired	false
251.32.191.44	unknown	Reserved		unknown	unknown	false
155.14.152.106	unknown	United States		40155	APLLIUS	false
113.230.156.33	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
169.203.96.4	unknown	United States		22920	BIAEDNET-INTERNETUS	false
103.224.219.136	unknown	India		135226	JEECOM-ASJeecommunicationsIN	false
110.162.48.72	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
190.139.248.21	unknown	Argentina		7303	TelecomArgentinaSAAR	false
23.234.164.53	unknown	United States		54905	DIGITAL-LANDSCAPEUS	false
243.11.93.252	unknown	Reserved		unknown	unknown	false
156.190.95.246	unknown	Egypt		36992	ETISALAT-MISREG	false
86.143.83.13	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
148.72.226.86	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
105.37.93.217	unknown	Egypt		37069	MOBINILEG	false
13.40.198.228	unknown	United States		7018	ATT-INTERNET4US	false
37.250.156.26	unknown	Sweden		44034	HI3GSE	false
19.175.149.177	unknown	United States		3	MIT-GATEWAYSUS	false
144.95.227.31	unknown	Netherlands		32023	ANADARKOUS	false
121.243.246.201	unknown	India		17908	TCISLTataCommunicationsIN	false
57.98.26.31	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
245.51.97.122	unknown	Reserved		unknown	unknown	false
145.221.28.61	unknown	Netherlands		15625	ING-ASAmsterdamNL	false
190.150.134.219	unknown	El Salvador		27773	MILLICOMCABLEELSALVADORSADECVSV	false
84.155.227.30	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
194.142.114.69	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.157.219.169	unknown	Canada		36493	295CA-TOR-ASNCA	false
53.18.189.84	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
82.147.226.38	unknown	Denmark		15516	DK-DANSKKABELTVDK	false
207.123.162.138	unknown	United States		3356	LEVEL3US	false
194.47.5.189	unknown	Sweden		1653	SUNETSUNETSwedishUniversityNetworkEU	false
255.65.102.126	unknown	Reserved		unknown	unknown	false
195.76.65.49	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
207.136.225.200	unknown	United States		5738	SOVER-ASNUS	false
93.85.251.206	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
164.150.30.65	unknown	South Africa		37130	SITA-ASZA	false
152.36.229.246	unknown	United States		31715	ABTME-ASUS	false
63.195.7.190	unknown	United States		7018	ATT-INTERNET4US	false
170.115.152.134	unknown	United States		11205	CITY-OF-PHILADELPHIAUS	false
2.73.95.133	unknown	Kazakhstan		29355	KCELL-ASKZ	false
248.133.109.69	unknown	Reserved		unknown	unknown	false
197.53.207.221	unknown	Egypt		8452	TE-ASTE-ASEG	false
216.95.76.109	unknown	United States		701	UUNETUS	false
91.41.111.144	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
139.174.47.177	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
110.156.82.185	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
95.120.112.167	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
57.124.200.251	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
217.85.150.41	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
246.109.142.99	unknown	Reserved		unknown	unknown	false
163.130.240.50	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
125.108.202.31	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
111.69.66.133	unknown	New Zealand		23655	SNAP-NZ-ASSnapInternetLimitedNZ	false
78.216.67.239	unknown	France		12322	PROXADFR	false
246.211.208.229	unknown	Reserved		unknown	unknown	false
12.253.252.114	unknown	United States		8030	WORLDNET5-10US	false
188.81.116.228	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
116.189.252.212	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
71.246.41.123	unknown	United States		5650	FRONTIER-FRTRUS	false
74.80.40.146	unknown	United States		25921	LUS-FIBER-LCGUS	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

/var/cache/man/cs/6207

/var/cache/man/cs/index.db.rLDrkz

/var/cache/man/da/6207

/var/cache/man/da/index.db.Wu1kvv

/var/cache/man/de/6207

/var/cache/man/de/index.db.jdb2Cv

/var/cache/man/es/6207

/var/cache/man/es/index.db.sQb6Uw

/var/cache/man/fi/6207

/var/cache/man/fi/index.db.apftZv

/var/cache/man/fr.ISO8859-1/6207

/var/cache/man/fr.ISO8859-1/index.db.CCD6Ox

/var/cache/man/fr.UTF-8/6207

/var/cache/man/fr.UTF-8/index.db.ccta5y

/var/cache/man/fr/6207

/var/cache/man/fr/index.db.KxVL9x

/var/cache/man/hu/6207

/var/cache/man/hu/index.db.CuSdly

/var/cache/man/it/6207

/var/cache/man/it/index.db.F21dcx

/var/cache/man/ja/6207

/var/cache/man/ja/index.db.2C2iJw

/var/cache/man/ko/6207

/var/cache/man/ko/index.db.B4yPiz

/var/cache/man/nl/6207

/var/cache/man/nl/index.db.0onckz

/var/cache/man/pl/6207

/var/cache/man/pl/index.db.8E68Xx

/var/cache/man/pt/6207

/var/cache/man/pt/index.db.HAXyNv

/var/cache/man/pt_BR/6207

/var/cache/man/pt_BR/index.db.EkCw1w

/var/cache/man/ru/6207

/var/cache/man/ru/index.db.7KBHmx

/var/cache/man/sl/6207

/var/cache/man/sl/index.db.WQMMfz

/var/cache/man/sr/6207

/var/cache/man/sr/index.db.ssllBx

/var/cache/man/sv/6207

/var/cache/man/sv/index.db.JL2zSv

/var/cache/man/tr/6207

/var/cache/man/tr/index.db.dHLmPw

/var/cache/man/zh_CN/6207

/var/cache/man/zh_CN/index.db.Z4jDnz

/var/cache/man/zh_TW/6207

/var/cache/man/zh_TW/index.db.5ouSHz

/var/lib/logrotate/status.tmp

/var/log/cups/access_log.1.gz

/var/log/syslog.1.gz

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, no section header
Entropy (8bit):	7.929395181499569
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	yvweY4vsVq.elf
File size:	25004
MD5:	7592df37fb3fea64a0994ac342f319f4
SHA1:	bd612669bbc816883907689411667f34b471259f
SHA256:	4e97dfb181ef3db9a59094b5f468255ee7dc5d5e52543730d8394270a434b162

SHA512:	6e1d35eed67210fb5aeefeae47a876e58bcc38f233618ad1c2487db810467f0697ce5cc0825b51ff0a552c5ce9b9af2f61adc3493db9665e5021daf8ca53e8c7
SSDEEP:	384:cZ0X9nxn8o9ir/nSdoijsN2e4JQkCD2EjKb3prhymdGUop5h1:5X9nxn8o9wnBoWzEQf2EjKb3prs3UozP
TLSH:	5FB2C0717015B8B2CAE1007B6AEEDA43FB801EF8D0E873391465099DEAD5D42BAF1547
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....`..`.....^.....Q.td.....CvUPX!.....0...0.....R.....?.E.h;.}...^.....f.Z.6.. (fw....&.x:.E.....oe.`.S..T.....n..

Static ELF Info

ELF header

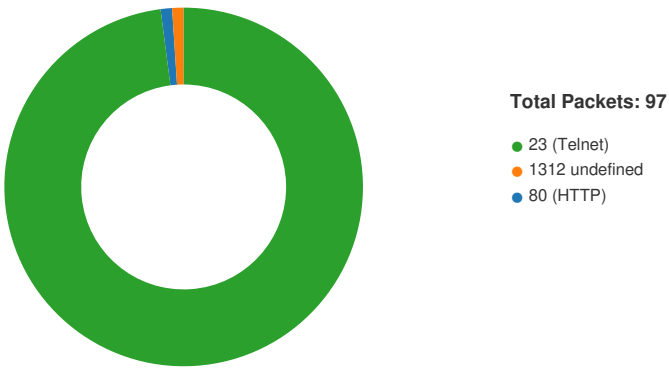
Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

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	0x60bf	0x60bf	7.9335	0x5	R E	0x8000		
LOAD	0x5ee0	0x1dee0	0x1dee0	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: systemd PID: 6198, Parent PID: 1

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 6198, Parent PID: 1

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities

- File Deleted
- File Read
- File Written
- File Moved
- Owner / Group Modified
- Permission Modified

Analysis Process: logrotate PID: 6240, Parent PID: 6198

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 6240, Parent PID: 6198

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

- File Read
- File Written

Analysis Process: logrotate PID: 6241, Parent PID: 6198

General

Start time:	00:53:08
Start date:	30/05/2023

Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: **6241**, Parent PID: **6198**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6242**, Parent PID: **6241**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: **6242**, Parent PID: **6241**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: invoke-rc.d PID: **6243**, Parent PID: **6242**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: **6243**, Parent PID: **6242**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/sbin/runlevel
Arguments:	/sbin/runlevel
File size:	996584 bytes

MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: **6245**, Parent PID: **6242**

General

Start time:	00:53:09
Start date:	30/05/2023
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **6245**, Parent PID: **6242**

General

Start time:	00:53:09
Start date:	30/05/2023
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-enabled cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: **6249**, Parent PID: **6242**

General

Start time:	00:53:10
Start date:	30/05/2023
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: **6249**, Parent PID: **6242**

General

Start time:	00:53:10
Start date:	30/05/2023
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities

File Read

Analysis Process: invoke-rc.d PID: **6250**, Parent PID: **6242**

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 6250, Parent PID: 6242

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: logrotate PID: 6251, Parent PID: 6198

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 6251, Parent PID: 6198

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 6252, Parent PID: 6198

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 6252, Parent PID: 6198

General

Start time:	00:53:11
Start date:	30/05/2023
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6253**, Parent PID: **6252**

General

Start time:	00:53:12
Start date:	30/05/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: **6253**, Parent PID: **6252**

General

Start time:	00:53:12
Start date:	30/05/2023
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: rsyslog-rotate PID: **6254**, Parent PID: **6253**

General

Start time:	00:53:12
Start date:	30/05/2023
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **6254**, Parent PID: **6253**

General

Start time:	00:53:12
Start date:	30/05/2023
Path:	/usr/bin/systemctl
Arguments:	systemctl kill -s HUP rsyslog.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: systemd PID: **6199**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: **6199**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/bin/install
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man
File size:	158112 bytes
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54

Analysis Process: systemd PID: **6205**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: **6205**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/bin/find
Arguments:	/usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
File size:	320160 bytes
MD5 hash:	b68ef002f84cc54dd472238ba7df80ab

Analysis Process: systemd PID: **6207**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: **6207**, Parent PID: **1**

General

Start time:	00:53:08
Start date:	30/05/2023
Path:	/usr/bin/mandb
Arguments:	/usr/bin/mandb --quiet
File size:	142432 bytes
MD5 hash:	1dda5ea0027ecf1c2db0f5a3de7e6941

File Activities

- File Deleted
- File Read
- File Written
- File Moved
- Directory Enumerated
- Owner / Group Modified
- Permission Modified

Analysis Process: yvweY4vsVq.elf PID: **6291**, Parent PID: **6127**

General

Start time:	00:53:24

Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	/tmp/yvweY4vsVq.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: yvweY4vsVq.elf PID: **6293**, Parent PID: **6291**

General

Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: yvweY4vsVq.elf PID: **6295**, Parent PID: **6291**

General

Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: yvweY4vsVq.elf PID: **6297**, Parent PID: **6291**

General

Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: yvweY4vsVq.elf PID: **6299**, Parent PID: **6297**

General

Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: yvweY4vsVq.elf PID: **6301**, Parent PID: **6297**

General	
Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: yvweY4vsVq.elf PID: **6303**, Parent PID: **6297**

General	
Start time:	00:53:25
Start date:	30/05/2023
Path:	/tmp/yvweY4vsVq.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1