ID: 557427
Sample Name: apL.mips-20220121-0317
Cookbook: defaultlinuxfilecookbook.jbs
Time: 04:42:43
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

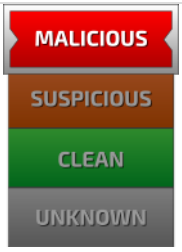
apL.mips-20220121-0317

Overview

General Information

Sample Name:	apL.mips-20220121-0317
Analysis ID:	557427
MD5:	13e8ba90e042ab.
SHA1:	c7dbaf4b95ad10..
SHA256:	37b5a5d9d5ab50.
Infos:	

Detection



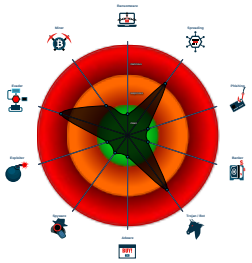
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Opens /proc/net/* files useful for fin…
- Deletes all firewall rules
- Sample deletes itself
- Sample is packed with UPX
- Deletes security-related log files
- Tries to stop the "iptables" service
- Executes the "kill" or "pkill" comma…
- Sample contains only a LOAD segm…
- Reads CPU information from /sys in…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	557427
Start date:	21.01.2022
Start time:	04:42:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	apL.mips-20220121-0317
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:	mal80.spre.troj.evad.linMIPS-20220121-0317@0/2@0/0

Runtime Messages

Command:	/tmp/apL.mips-20220121-0317
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Gosh your fatter then a tree
Standard Error:	Failed to stop iptables.service: Unit iptables.service not loaded. Failed to stop firewalld.service: Unit firewalld.service not loaded. sh: 1: history: not found

Process Tree

- **system is lnxubuntu20**
- apL.mips-20220121-0317 (PID: 5216, Parent: 5112, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/apL.mips-20220121-0317
  - apL.mips-20220121-0317 New Fork (PID: 5218, Parent: 5216)
  - apL.mips-20220121-0317 New Fork (PID: 5219, Parent: 5216)
    - apL.mips-20220121-0317 New Fork (PID: 5222, Parent: 5219)
      - apL.mips-20220121-0317 New Fork (PID: 5224, Parent: 5222)
      - sh (PID: 5224, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
        - sh New Fork (PID: 5226, Parent: 5224)
        - rm (PID: 5226, Parent: 5224, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/apL.mips-20220121-0317 /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/tmp.qtPPbjdkIb /tmp/tmp.tvSNtKHMtv /tmp/tmp.xTL7lOZ5v5 /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jlxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
      - apL.mips-20220121-0317 New Fork (PID: 5231, Parent: 5222)
      - sh (PID: 5231, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
        - sh New Fork (PID: 5233, Parent: 5231)
        - rm (PID: 5233, Parent: 5231, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
      - apL.mips-20220121-0317 New Fork (PID: 5234, Parent: 5222)
      - sh (PID: 5234, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
        - sh New Fork (PID: 5236, Parent: 5234)
        - rm (PID: 5236, Parent: 5234, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
      - apL.mips-20220121-0317 New Fork (PID: 5237, Parent: 5222)
      - sh (PID: 5237, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
        - sh New Fork (PID: 5239, Parent: 5237)
        - rm (PID: 5239, Parent: 5237, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
      - apL.mips-20220121-0317 New Fork (PID: 5240, Parent: 5222)
      - sh (PID: 5240, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -F"
        - sh New Fork (PID: 5242, Parent: 5240)
        - iptables (PID: 5242, Parent: 5240, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -F
      - apL.mips-20220121-0317 New Fork (PID: 5246, Parent: 5222)
      - sh (PID: 5246, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
        - sh New Fork (PID: 5248, Parent: 5246)
        - pkill (PID: 5248, Parent: 5246, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
      - apL.mips-20220121-0317 New Fork (PID: 5254, Parent: 5222)
      - sh (PID: 5254, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
        - sh New Fork (PID: 5256, Parent: 5254)
        - pkill (PID: 5256, Parent: 5254, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
      - apL.mips-20220121-0317 New Fork (PID: 5258, Parent: 5222)
      - sh (PID: 5258, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
        - sh New Fork (PID: 5260, Parent: 5258)
        - pkill (PID: 5260, Parent: 5258, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
      - apL.mips-20220121-0317 New Fork (PID: 5263, Parent: 5222)
      - sh (PID: 5263, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service iptables stop"
        - sh New Fork (PID: 5265, Parent: 5263)
        - service (PID: 5265, Parent: 5263, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service iptables stop
          - service New Fork (PID: 5266, Parent: 5265)
          - basename (PID: 5266, Parent: 5265, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5267, Parent: 5265)
          - basename (PID: 5267, Parent: 5265, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5268, Parent: 5265)
          - systemctl (PID: 5268, Parent: 5265, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
          - service New Fork (PID: 5269, Parent: 5265)
            - service New Fork (PID: 5270, Parent: 5269)
            - systemctl (PID: 5270, Parent: 5269, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
            - service New Fork (PID: 5271, Parent: 5269)
            - sed (PID: 5271, Parent: 5269, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
        - systemctl (PID: 5265, Parent: 5263, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop iptables.service
      - apL.mips-20220121-0317 New Fork (PID: 5272, Parent: 5222)
      - sh (PID: 5272, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "/sbin/iptables -F; /sbin/iptables -X"
        - sh New Fork (PID: 5274, Parent: 5272)
        - iptables (PID: 5274, Parent: 5272, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -F
        - sh New Fork (PID: 5275, Parent: 5272)
        - iptables (PID: 5275, Parent: 5272, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: /sbin/iptables -X
      - apL.mips-20220121-0317 New Fork (PID: 5276, Parent: 5222)
      - sh (PID: 5276, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "service firewalld stop"
        - sh New Fork (PID: 5278, Parent: 5276)
        - service (PID: 5278, Parent: 5276, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: service firewalld stop
          - service New Fork (PID: 5279, Parent: 5278)
          - basename (PID: 5279, Parent: 5278, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
          - service New Fork (PID: 5280, Parent: 5278)

- basename (PID: 5280, Parent: 5278, MD5: 3283660e59f128df18bec9b96fbd4d41) Arguments: basename /usr/sbin/service
- service New Fork (PID: 5281, Parent: 5278)
- systemctl (PID: 5281, Parent: 5278, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active multi-user.target
- service New Fork (PID: 5282, Parent: 5278)
- service New Fork (PID: 5283, Parent: 5282)
- systemctl (PID: 5283, Parent: 5282, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl list-unit-files --full --type=socket
- service New Fork (PID: 5284, Parent: 5282)
- sed (PID: 5284, Parent: 5282, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
- systemctl (PID: 5278, Parent: 5276, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl stop firewalld.service
- apL.mips-20220121-0317 New Fork (PID: 5287, Parent: 5222)
- sh (PID: 5287, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf ~/.bash_history"
- sh New Fork (PID: 5289, Parent: 5287)
- rm (PID: 5289, Parent: 5287, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /root/.bash_history
- apL.mips-20220121-0317 New Fork (PID: 5290, Parent: 5222)
- sh (PID: 5290, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "history -c"

- dash New Fork (PID: 5294, Parent: 4331)
- cat (PID: 5294, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.qtPPbjdkIb
- dash New Fork (PID: 5295, Parent: 4331)
- head (PID: 5295, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5296, Parent: 4331)
- tr (PID: 5296, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5297, Parent: 4331)
- cut (PID: 5297, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5298, Parent: 4331)
- cat (PID: 5298, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.qtPPbjdkIb
- dash New Fork (PID: 5299, Parent: 4331)
- head (PID: 5299, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5300, Parent: 4331)
- tr (PID: 5300, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5301, Parent: 4331)
- cut (PID: 5301, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5302, Parent: 4331)
- rm (PID: 5302, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.qtPPbjdkIb /tmp/tmp.tvSNtKHMtv /tmp/tmp.xTL7lOZ5v5
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
apL.mips-20220121-0317	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x8d28:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x8d97:$s2: $Id: UPX • 0x8d48:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
5219.1.00000000f7f1692e.000000004729ffe7.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5216.1.00000000f7f1692e.000000004729ffe7.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5218.1.00000000f7f1692e.000000004729ffe7.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Spreading

Opens /proc/net/* files useful for finding connected devices and routers

Networking

Deletes all firewall rules

Tries to stop the "iptables" service

Data Obfuscation

Sample is packed with UPX

Persistence and Installation Behavior

Deletes all firewall rules

Tries to stop the "iptables" service

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Malware Analysis System Evasion

Deletes security-related log files

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

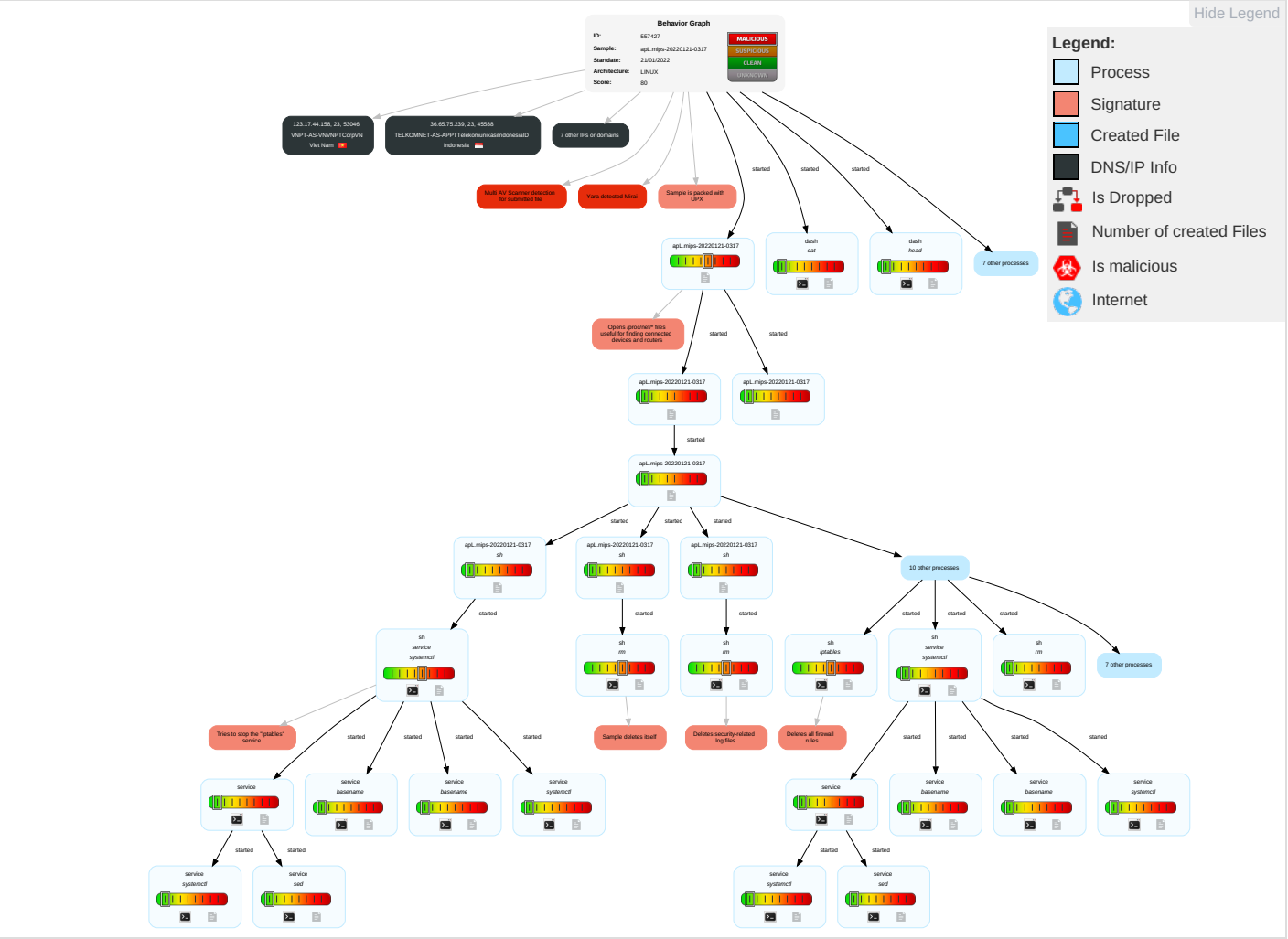
Mitre Att&ck Matrix

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	1 Systemd Service	1 Systemd Service	1 Disable or Modify Tools	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	Modify System Partition
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	1 Remote System 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 System Network Configuration Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Disable or Modify System Firewall	NTDS	1 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Indicator Removal on Host	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 File Deletion	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
apL.mips-20220121-0317	28%	Virustotal		Browse
apL.mips-20220121-0317	26%	ReversingLabs	Linux.Trojan.Gafgyt	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

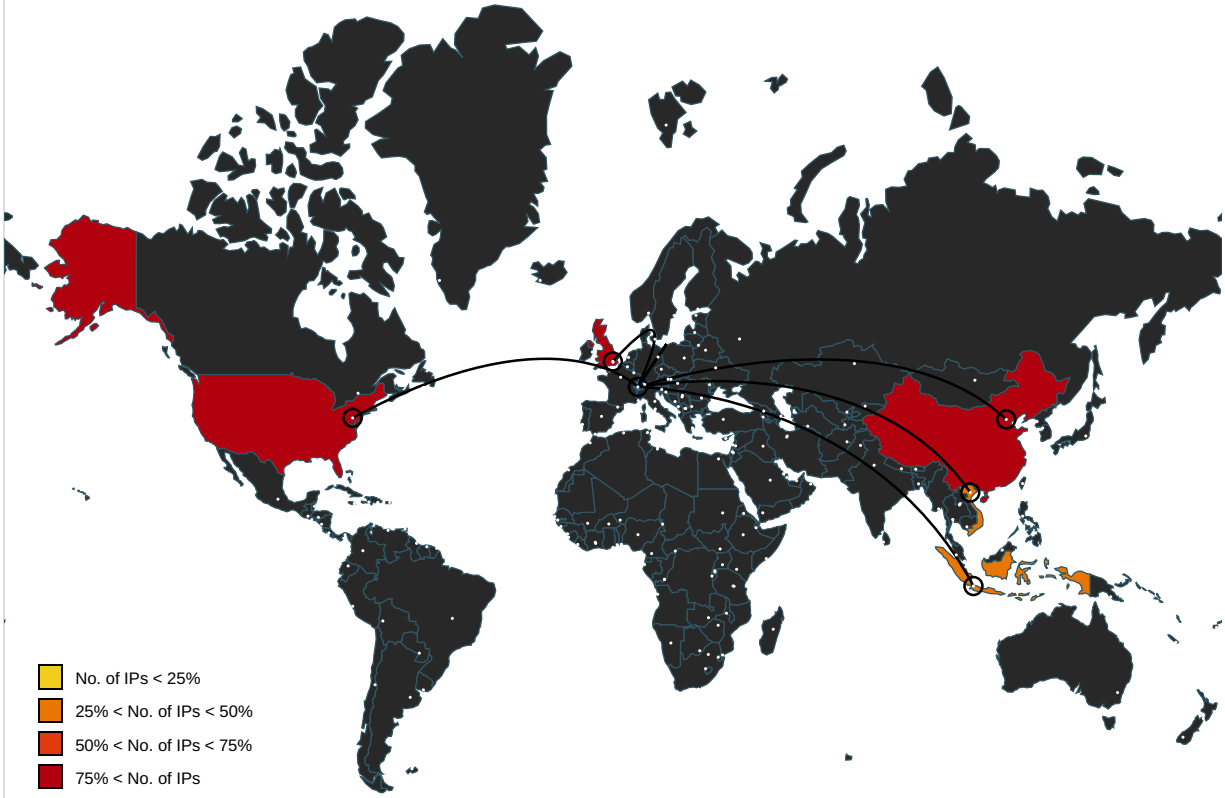
Domains and IPs

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
54.171.230.55	unknown	United States		16509	AMAZON-02US	false
123.178.234.190	unknown	China		4809	CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr	false
36.65.75.239	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
192.236.160.175	unknown	United States		54290	HOSTWINDSUS	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
123.17.44.158	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
60.220.215.198	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

/run/systemd/resolve/stub-resolv.conf

/tmp/qemu-open.JEqahA (deleted)

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.946793281986122
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	apL.mips-20220121-0317
File size:	46204
MD5:	13e8ba90e042ab6bbc3821fad3cf1837
SHA1:	c7dbaf4b95ad104e35570b287b74f8375f1e5d01
SHA256:	37b5a5d9d5ab50a8dff649678a9f10f26a5923186c97d1a623902b68e795abdc
SHA512:	ceb092fbdfd3ad39f6a49ee9dbf9d212ea7d3c9eec014dcc2bc5ba83bc6b1ab8f02965c453b1c076979c128011dfda8f12f32d6f4e363d7af8c4f951243a9cc7
SSDEEP:	768:r5FMs2rPZhkq92ZVHGWVLQttQwuHcIB085oYk6N50IwumgJgGlzDpbuR1JAnAtlZ:p2rd9CmKLstQwuYvYj7hw8VJuLaihT
File Content Preview:	.ELF.....x...4.....4. ...(...._|.F_|.F_|.....UPX!.d.....b.....?.E.h4...@b..) ..]..0..ap%d>.>y....\._.....@.....g#`.....o2Z.....x.....-"...i..;%...GT..e1.3".....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x108178
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52

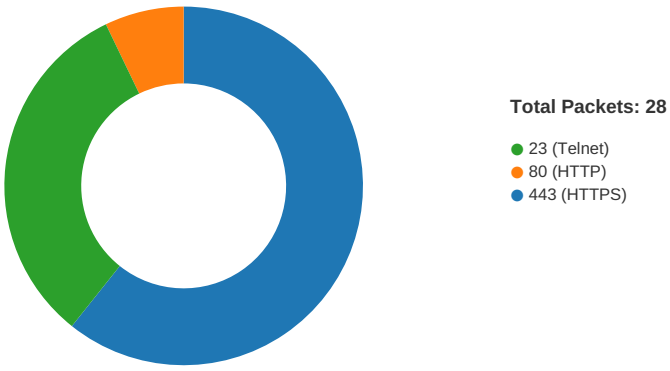
ELF header	
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0x94bc	0x94bc	4.1385	0x5	R E	0x10000		
LOAD	0x5f7c	0x465f7c	0x465f7c	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 21, 2022 04:43:55.715353966 CET	54.171.230.55	443	192.168.2.23	33608	CN=motd.ubuntu.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 22 12:20:38 CET 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Feb 20 12:20:37 CET 2022 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4866-4867-4865-49196-49200-163-159-52393-52392-52394-49327-49325-49315-49311-49245-49249-49239-49235-49195-49199-162-158-49326-49324-49314-49310-49244-49248-49238-49234-49188-49192-107-106-49267-49271-196-195-49187-49191-103-64-49266-49270-190-189-49162-49172-57-56-136-135-49161-49171-51-50-69-68-157-49313-49309-49233-156-49312-49308-49232-61-192-60-186-53-132-47-65-255,0-11-10-35-22-23-13-43-45-51,29-23-30-25-24,0-1-2	fb4726d465c5f28b84cd6d14cedd13a7
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

System Behavior

Analysis Process: apL.mips-20220121-0317 PID: **5216**, Parent PID: **5112**

General

Start time:	04:43:26
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	/tmp/apL.mips-20220121-0317
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

- File Deleted
- File Read
- File Written

Analysis Process: apL.mips-20220121-0317 PID: **5218**, Parent PID: **5216**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: apL.mips-20220121-0317 PID: **5219**, Parent PID: **5216**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a

File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: apL.mips-20220121-0317 PID: **5222**, Parent PID: **5219**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Written

Analysis Process: apL.mips-20220121-0317 PID: **5224**, Parent PID: **5222**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5224**, Parent PID: **5222**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: **5226**, Parent PID: **5224**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5226**, Parent PID: **5224**

General

Start time:	04:43:27
Start date:	21/01/2022
Path:	/usr/bin/rm

Arguments:	rm -rf /tmp/apL.mips-20220121-0317 /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/tmp.qtPPbjdkIb /tmp/tmp.tvSNtKHMtv /tmp/tmp.xTL7lOZ5v5 /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jIxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Directory Enumerated

Analysis Process: apL.mips-20220121-0317 PID: **5231**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5231**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf /var/log/wtmp"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5233**, Parent PID: **5231**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5233**, Parent PID: **5231**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /var/log/wtmp
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5234**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5234**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf /tmp/*"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: **5236**, Parent PID: **5234**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5236**, Parent PID: **5234**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/*
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5237**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5237**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf /bin/netstat"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5239**, Parent PID: **5237**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5239**, Parent PID: **5237**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /bin/netstat
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5240**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5240**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "iptables -F"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5242**, Parent PID: **5240**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5242**, Parent PID: **5240**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5246**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5246**, Parent PID: **5222**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5248**, Parent PID: **5246**

General

Start time:	04:43:35

Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **5248**, Parent PID: **5246**

General

Start time:	04:43:35
Start date:	21/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 busybox
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: apL.mips-20220121-0317 PID: **5254**, Parent PID: **5222**

General

Start time:	04:43:37
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5254**, Parent PID: **5222**

General

Start time:	04:43:37
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5256**, Parent PID: **5254**

General

Start time:	04:43:38
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **5256**, Parent PID: **5254**

General

Start time:	04:43:38
Start date:	21/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 perl

File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: apL.mips-20220121-0317 PID: **5258**, Parent PID: **5222**

General

Start time:	04:43:40
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5258**, Parent PID: **5222**

General

Start time:	04:43:40
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5260**, Parent PID: **5258**

General

Start time:	04:43:40
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **5260**, Parent PID: **5258**

General

Start time:	04:43:40
Start date:	21/01/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 python
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: apL.mips-20220121-0317 PID: **5263**, Parent PID: **5222**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317

Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5263**, Parent PID: **5222**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "service iptables stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5265**, Parent PID: **5263**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: **5265**, Parent PID: **5263**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	service iptables stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: **5266**, Parent PID: **5265**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: **5266**, Parent PID: **5265**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5267, Parent PID: 5265

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: 5267, Parent PID: 5265

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: 5268, Parent PID: 5265

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5268, Parent PID: 5265

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: 5269, Parent PID: 5265

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: **5270**, Parent PID: **5269**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **5270**, Parent PID: **5269**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: **5271**, Parent PID: **5269**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: **5271**, Parent PID: **5269**

General

Start time:	04:43:42
Start date:	21/01/2022
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: **5265**, Parent PID: **5263**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl stop iptables.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5272**, Parent PID: **5222**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5272**, Parent PID: **5222**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "/sbin/iptables -F; /sbin/iptables -X"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5274**, Parent PID: **5272**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5274**, Parent PID: **5272**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/sbin/iptables
Arguments:	/sbin/iptables -F
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: sh PID: **5275**, Parent PID: **5272**

General

Start time:	04:43:44
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5275**, Parent PID: **5272**

General

Start time:	04:43:44

Start date:	21/01/2022
Path:	/sbin/iptables
Arguments:	/sbin/iptables -X
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5276**, Parent PID: **5222**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5276**, Parent PID: **5222**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "service firewalld stop"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5278**, Parent PID: **5276**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: **5278**, Parent PID: **5276**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	service firewalld stop
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: service PID: **5279**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022

Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: **5279**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: **5280**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: basename PID: **5280**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/bin/basename
Arguments:	basename /usr/sbin/service
File size:	39256 bytes
MD5 hash:	3283660e59f128df18bec9b96fbd4d41

File Activities

File Read

Analysis Process: service PID: **5281**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **5281**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active multi-user.target
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: service PID: **5282**, Parent PID: **5278**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: service PID: **5283**, Parent PID: **5282**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **5283**, Parent PID: **5282**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl list-unit-files --full --type=socket
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Directory Enumerated

Analysis Process: service PID: **5284**, Parent PID: **5282**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/sbin/service
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: **5284**, Parent PID: **5282**

General

Start time:	04:43:45
Start date:	21/01/2022
Path:	/usr/bin/sed
Arguments:	sed -ne s/\\.socket\\s*[a-z]*\\s*$/.socket/p
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: systemctl PID: **5278**, Parent PID: **5276**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl stop firewalld.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5287**, Parent PID: **5222**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5287**, Parent PID: **5222**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf ~/.bash_history"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5289**, Parent PID: **5287**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5289**, Parent PID: **5287**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /root/.bash_history
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: apL.mips-20220121-0317 PID: **5290**, Parent PID: **5222**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/tmp/apL.mips-20220121-0317
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **5290**, Parent PID: **5222**

General

Start time:	04:43:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "history -c"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: dash PID: **5294**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5294**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.qtPPbjdkIb
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5295**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5295**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5296**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5296**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: **5297**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5297**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: **5298**, Parent PID: **4331**

General

Start time:	04:43:55

Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5298**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.qtPPbjdkIb
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5299**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5299**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5300**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5300**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes

MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: **5301**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5301**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: **5302**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5302**, Parent PID: **4331**

General

Start time:	04:43:55
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.qtPPbjdkIb /tmp/tmp.tvSNtKHMtv /tmp/tmp.xTL7lOZ5v5
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read