ID: 635041
Sample Name: hwLFomKm8k
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:33:16
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

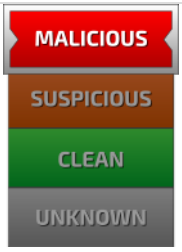
hwLFomKm8k

Overview

General Information

Sample Name:	hwLFomKm8k
Analysis ID:	635041
MD5:	038da709550f5fa.
SHA1:	62c70c834e0a65..
SHA256:	9e35c0b5c81202..
Tags:	32 elf mips
Infos:	

Detection



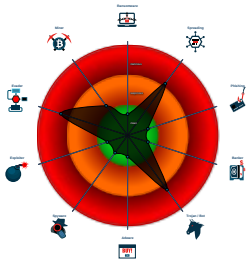
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Sample deletes itself
- Sample is packed with UPX
- Deletes security-related log files
- Opens /proc/net/* files useful for fin…
- Executes the "kill" or "pkill" comma…
- Sample contains only a LOAD segm…
- Reads CPU information from /sys in…
- Yara signature match
- Deletes log files
- Uses the "uname" system call to qu…

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:	34.0.0 Boulder Opal
Analysis ID:	635041
Start date and time: 27/05/202211:33:16	2022-05-27 11:33:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hwLFomKm8k
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal64.spre.troj.evad.lin@0/1@0/0

Warnings

Process Tree

- **system is lnxubuntu20**
- hwLFomKm8k (PID: 6234, Parent: 6126, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/hwLFomKm8k
  - hwLFomKm8k New Fork (PID: 6236, Parent: 6234)
  - hwLFomKm8k New Fork (PID: 6238, Parent: 6234)
    - hwLFomKm8k New Fork (PID: 6240, Parent: 6238)

- hwLFomKm8k New Fork (PID: 6242, Parent: 6240)
- sh (PID: 6242, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
  - sh New Fork (PID: 6245, Parent: 6242)
  - rm (PID: 6245, Parent: 6242, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/hsperfdata_root /tmp/hwLFomKm8k /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/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
- hwLFomKm8k New Fork (PID: 6254, Parent: 6240)
- sh (PID: 6254, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
  - sh New Fork (PID: 6256, Parent: 6254)
  - rm (PID: 6256, Parent: 6254, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
- hwLFomKm8k New Fork (PID: 6257, Parent: 6240)
- sh (PID: 6257, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
  - sh New Fork (PID: 6259, Parent: 6257)
  - rm (PID: 6259, Parent: 6257, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
- hwLFomKm8k New Fork (PID: 6260, Parent: 6240)
- sh (PID: 6260, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
  - sh New Fork (PID: 6262, Parent: 6260)
  - rm (PID: 6262, Parent: 6260, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
- hwLFomKm8k New Fork (PID: 6263, Parent: 6240)
- sh (PID: 6263, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
  - sh New Fork (PID: 6265, Parent: 6263)
  - pkill (PID: 6265, Parent: 6263, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
- hwLFomKm8k New Fork (PID: 6270, Parent: 6240)
- sh (PID: 6270, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
  - sh New Fork (PID: 6272, Parent: 6270)
  - pkill (PID: 6272, Parent: 6270, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
- hwLFomKm8k New Fork (PID: 6273, Parent: 6240)
- sh (PID: 6273, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
  - sh New Fork (PID: 6275, Parent: 6273)
  - pkill (PID: 6275, Parent: 6273, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
- hwLFomKm8k New Fork (PID: 6278, Parent: 6240)
- sh (PID: 6278, Parent: 6240, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -A INPUT -j DROP"
  - sh New Fork (PID: 6280, Parent: 6278)
  - iptables (PID: 6280, Parent: 6278, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -A INPUT -j DROP

- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
hwLFomKm8k	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x99a0:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x9a0f:$s2: $Id: UPX • 0x99c0:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6238.1.0000000087779f1c.0000000053d66254.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6236.1.0000000087779f1c.0000000053d66254.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6234.1.0000000087779f1c.0000000053d66254.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Spreading

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

Data Obfuscation

Sample is packed with UPX

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

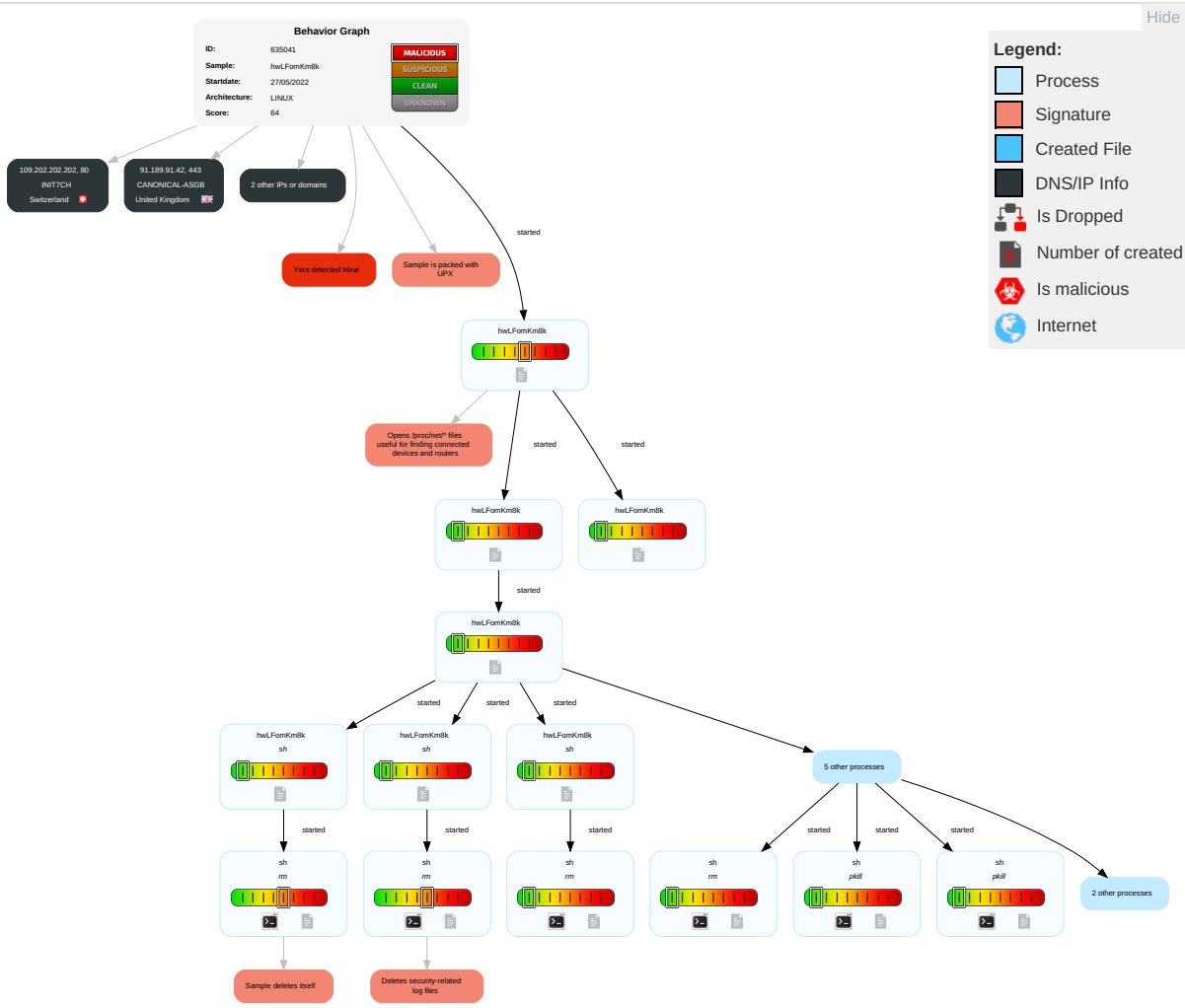
Mitre Att&ck Matrix

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 Scripting	Path Interception	Path Interception	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	1 System Information 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 1 Indicator Removal on Host	Security Account Manager	1 Remote System 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)	1 Obfuscated Files or Information	NTDS	System Network Configuration 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 File Deletion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	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

No Antivirus matches

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

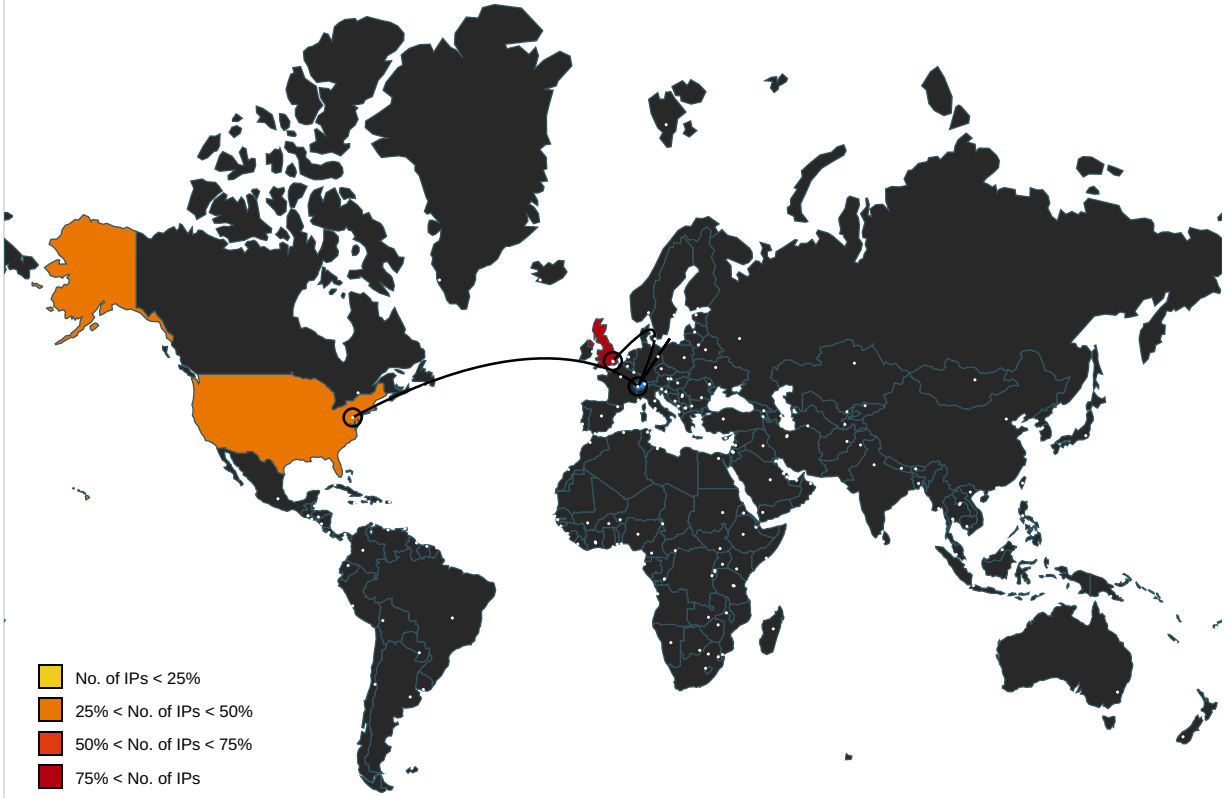
Domains and IPs

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
172.245.210.119	unknown	United States		36352	AS-COLOCROSSINGUS	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	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

/tmp/qemu-open.WSG3Jy (deleted)

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.953579492955063
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	hwLFomKm8k
File size:	49692
MD5:	038da709550f5fa2fb58077767bce04b
SHA1:	62c70c834e0a65db09099aa1d2b465244222816f
SHA256:	9e35c0b5c812027d6698b662bb771ada7c1d40cf04050f450feebcbbdbff6b9a
SHA512:	b31807c00059ed1fc06a0a52cce5173f38e6e58d2294da48ef1a2c391231ad1e6a855c65caafd1751f458062b18fb2ae818bd705061d20721576a9fdbc350763
SSDEEP:	768:fQI83S0syxxgtCD66K6qOOONkpm1xRrBeuLJgGlzDpbuR1JruR+bDGnLFTLBw:fD8v9wtsK6qOOONkpm1xZVJuEAnQs
TLSH:	A623F1E9100838C6CE87FDBE62E453961B3D19F2666BDD497846EF89DC060A13B83DC4
File Content Preview:	.ELF.....4.....4. ...(.....4...4.....|.F.|.F.|.....P.cUPX!.d.....`.....?.E.h4...@b..) ..]..0..a....|.. G.....o#?.Z/=..7N.u.....IM.3.Ms....('x...%=5..\.....+.....R....

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:	0x108df0
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	0xa134	0xa134	4.1546	0x5	R E	0x10000		
LOAD	0xc37c	0x46c37c	0x46c37c	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution

Total Packets: 11

- 80 (HTTP)
- 443 (HTTPS)
- 17372 undefined

TCP Packets

System Behavior

Analysis Process: hwLFomKm8k PID: 6234, Parent PID: 6126

General

Start time:	11:34:02
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	/tmp/hwLFomKm8k
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

- File Deleted
- File Read
- File Written

Analysis Process: hwLFomKm8k PID: 6236, Parent PID: 6234

General

Start time:	11:34:02
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hwLFomKm8k PID: 6238, Parent PID: 6234

General

Start time:	11:34:02
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hwLFomKm8k PID: **6240**, Parent PID: **6238**

General

Start time:	11:34:03
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hwLFomKm8k PID: **6242**, Parent PID: **6240**

General

Start time:	11:34:03
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6242**, Parent PID: **6240**

General

Start time:	11:34:03
Start date:	27/05/2022
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: **6245**, Parent PID: **6242**

General

Start time:	11:34:03
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	11:34:03
Start date:	27/05/2022
Path:	/usr/bin/rm

Arguments:	rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/hsperfdata_root /tmp/hwLFomKm8k /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/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: hwLFomKm8k PID: **6254**, Parent PID: **6240**

General

Start time:	11:34:13
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6254**, Parent PID: **6240**

General

Start time:	11:34:13
Start date:	27/05/2022
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: **6256**, Parent PID: **6254**

General

Start time:	11:34:13
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6256**, Parent PID: **6254**

General

Start time:	11:34:13

Start date:	27/05/2022
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: hwLFomKm8k PID: **6257**, Parent PID: **6240**

General

Start time:	11:34:13
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6257**, Parent PID: **6240**

General

Start time:	11:34:13
Start date:	27/05/2022
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: **6259**, Parent PID: **6257**

General

Start time:	11:34:14
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6259**, Parent PID: **6257**

General

Start time:	11:34:14
Start date:	27/05/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /tmp/*
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: hwLFomKm8k PID: **6260**, Parent PID: **6240**

General	
Start time:	11:34:14
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6260**, Parent PID: **6240**

General	
Start time:	11:34:14
Start date:	27/05/2022
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: **6262**, Parent PID: **6260**

General	
Start time:	11:34:14
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6262**, Parent PID: **6260**

General	
Start time:	11:34:14
Start date:	27/05/2022
Path:	/usr/bin/rm
Arguments:	rm -rf /bin/netstat
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: hwLFomKm8k PID: **6263**, Parent PID: **6240**

General	
Start time:	11:34:14
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6263**, Parent PID: **6240**

General	
Start time:	11:34:14

Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6265**, Parent PID: **6263**

General

Start time:	11:34:14
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **6265**, Parent PID: **6263**

General

Start time:	11:34:14
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 busybox
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: hwLFomKm8k PID: **6270**, Parent PID: **6240**

General

Start time:	11:34:16
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6270**, Parent PID: **6240**

General

Start time:	11:34:16
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 perl"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6272**, Parent PID: **6270**

General

Start time:	11:34:16

Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **6272**, Parent PID: **6270**

General

Start time:	11:34:16
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 perl
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: hwLFomKm8k PID: **6273**, Parent PID: **6240**

General

Start time:	11:34:18
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6273**, Parent PID: **6240**

General

Start time:	11:34:18
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "pkill -9 python"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6275**, Parent PID: **6273**

General

Start time:	11:34:18
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: **6275**, Parent PID: **6273**

General

Start time:	11:34:18
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill -9 python

File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read

Directory Enumerated

Analysis Process: hwLFomKm8k PID: **6278**, Parent PID: **6240**

General

Start time:	11:34:21
Start date:	27/05/2022
Path:	/tmp/hwLFomKm8k
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6278**, Parent PID: **6240**

General

Start time:	11:34:21
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "iptables -A INPUT -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6280**, Parent PID: **6278**

General

Start time:	11:34:21
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **6280**, Parent PID: **6278**

General

Start time:	11:34:21
Start date:	27/05/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -A INPUT -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read