

Task 1

Firstseen (UTC)	SHA256 hash	Tags	Reporter
2024-10-21 12:30:59	 8efa7b0d0208441e67a9c...	elf 	 abuse_ch
2024-10-21 12:26:21	 36e7b76cbead676754b3...	elf 	 abuse_ch
2024-10-21 12:26:19	 b9d543298f37bfc67e77...	elf 	 abuse_ch
2024-10-21 12:26:18	 5309a55ba7d7bba1fac6...	elf 	 abuse_ch
2024-10-21 12:26:17	 0b5188fbb6d18f527e062...	elf 	 abuse_ch
2024-10-21 12:26:16	 954df513ff1e7a9838215f...	elf 	 abuse_ch
2024-10-21 12:26:14	 6fcc6776e7943969cb7ce...	elf 	 abuse_ch
2024-10-21 12:26:10	 bfde22e4be21f3e42881b...	elf 	 abuse_ch
2024-10-21 12:26:07	 4ce9ea3c411e29cdfef285...	elf 	 abuse_ch
2024-10-21 12:26:06	 7fd591bc32fa36106f303...	elf 	 abuse_ch
2024-10-21 12:26:05	 9a08e144f0e53f903a83e...	elf 	 abuse_ch
2024-10-21 12:26:03	 75224ee98d25854715b2...	elf 	 abuse_ch
2024-10-21 12:26:02	 747379882d25f684f48bc...	elf 	 abuse_ch
2024-10-21 12:25:57	 55b8c05e5e3aaec2fc3ef1...	elf 	 abuse_ch

Task 2

SHA256 hash:	 8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99
SHA3-384 hash:	 abaf33a1b5789faec1807bc630a7d6017a295066c6148e418c6e78307afcb3c1f984fab63c4d2a18528c3aafa04f5ff5
SHA1 hash:	 2737f1fdf0f40573b9381ac73bd54b695603d2c2
MD5 hash:	 5818ac08a993e1fa6676ee3ea2da27ce
humanhash:	 gee-comet-nine-earth
File name:	aisuru.mips
Download:	 download sample
Signature ⓘ	 
File size:	105'424 bytes
First seen:	2024-10-21 12:30:59 UTC
Last seen:	2024-10-21 15:37:03 UTC
File type:	 elf
MIME type:	application/x-executable
ssdeep ⓘ	 1536:XJv3fI5C6oqnpebB3MWd30103Yy03L9mdP+QZHBXqKSk4Dskg7OoBX:Rlo6968APxXkskg7Ool
TLSH ⓘ	 T1FEA3B71E6D219FECF36D82314BB74E31A35823A516E1C684D2ECD9106F6038E585FB89

Downloads

8efa7b0d0208441e67a9cf4d79b0b917974131734136cc...

Open file

Policy Paper #2.pdf

Open file

See more

Task 6

HTTP Requests		Connections		DNS Requests		Threats		Filter by PID, name or url		PCAP
Time	Headers	Rep	PID	Process name	CN	URL	Content			
RE	GET 200: OK	✓	5488	MoUsocoreWorker.exe		http://crl.microsoft.com/pki/crl/produc...	1 Kb	↓	binary	
RE	GET 200: OK	✓	5488	MoUsocoreWorker.exe		http://www.microsoft.com/pkiops/crl/...	973 b	↓	binary	
RE	GET 200: OK	✓	-	-		http://crl.microsoft.com/pki/crl/produc...	1 Kb	↓	binary	
RE	GET 200: OK	✓	-	-		http://ocsp.digicert.com/MFEwTzBNM...	313 b	↓	binary	

HTTP Requests		Connections		DNS Requests		Threats		Filter by PID, domain, name or ip		PCAP
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	UDP	✓	4	System		192.168.100.255	137	-	-	↑ 966 b ↓
BEFORE	TCP	✓	2660	RUXIMICS.exe		51.104.136.2	443	settings-win...	MICROSOFT...	No Data
BEFORE	TCP	✓	-	-		51.104.136.2	443	settings-win...	MICROSOFT...	↑ 1 Kb ↓
BEFORE	TCP	✓	-	-		51.104.136.2	443	settings-win...	MICROSOFT...	↑ 2 Kb ↓

HTTP Requests		Connections		DNS Requests		Threats		Filter by IP or domain		PCAP
Timeshift	Status	Rep	Domain		IP					
BEFORE	Responded	✓	settings-win.data.microsoft.com		51.104.136.2					
BEFORE	Responded	✓	crl.microsoft.com		2.16.164.120					
BEFORE	Responded	✓	google.com		142.250.185.238					

HTTP Requests		8		Connections		47		DNS Requests		18		Threats		0		Filter by message		PCAP	
Timeshift		Class				PID		Process name				Message							
No data																			

Task 7

IOC

IOCs

Summary of indicators of compromises 227

Copy selected

Main object – 8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99.zip

? SHA256

8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99.zip
fc1bb0b31a0d2a6dc0ec26f3a302d26a9fe4d00b97a7275bc116ab8149ef7883

Dropped executable file (189)

? SHA256

8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99.elf
8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99

? SHA256

C:\Users\admin\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat
a8bd235303668981563dfb5aae338cb802817c4060e2c199b7c84901d57b7e1e

? SHA256

C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{4bb40a93-b426-4a61-9159-1a228f420ca7}\0.2.filtertrie.intermediate.txt
d65b6a3bf11a27a1ced1f7e98082246e40cf01289fd47fe4a5ed46c221f2f73f

? SHA256

C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{4bb40a93-b426-4a61-9159-1a228f420ca7}\Apps.ft
ca45caa7de38cb805ec43edc8b9332e1e95124a27fbb6e5bd3ddd5e8a526afc7

? SHA256

C:\Windows\Logs\waasmedicapsule\WaasRemediation.003.etl
9faa75f166cfdd869d3549b76139dddb6a50790a5c6cc81b2084a432d7d60f

? SHA256

C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{4bb40a93-b426-4a61-9159-1a228f420ca7}\0.1.filtertrie.intermediate.txt

Text Report

General Info

File name:	8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99.zip
Full analysis:	https://app.any.run/tasks/c658ab34-c1d3-4a1b-a5fe-627729c0248a
Verdict:	No threats detected
Analysis date:	October 21, 2024 at 12:19:28
OS:	Windows 10 Professional (build: 19045, 64 bit)
MIME:	application/zip
File info:	Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
MD5:	D2AC5505BF60746D9B50EFB7B66A38E7
SHA1:	2209067DA33895F030B2DEBFB51DA003B6043DCA
SHA256:	FC1BB0B31A0D2A6DC0EC26F3A302D26A9FE4D00B97A7275BC116AB8149EF7883
SSDEEP:	1536:vFvdP3IUcuPI1cCRPFeeJT4g2R4iJh66i9V6ZB:dvdPYUNP4tetTRnli9V67

1168

"C:\Program Files\WinRAR\WinRAR.exe"
C:\Users\admin\AppData\Local\Temp\8efa7b0d0208441e67a9cf4d79b0b917974131734136ccb48b2d8cd4bcd23e99.zip

C:\Program Files\WinRAR\WinRAR.exe

explorer.exe

Information

User:adminCompany:Alexander Roshal

Integrity Level: MEDIUMDescription: WinRAR archiver

Version: 5.91.0

Modules

Images

c:\program files\winrar\winrar.exe

c:\windows\system32\ntdll.dll

c:\windows\system32\kernel32.dll

c:\windows\system32\kernelbase.dll

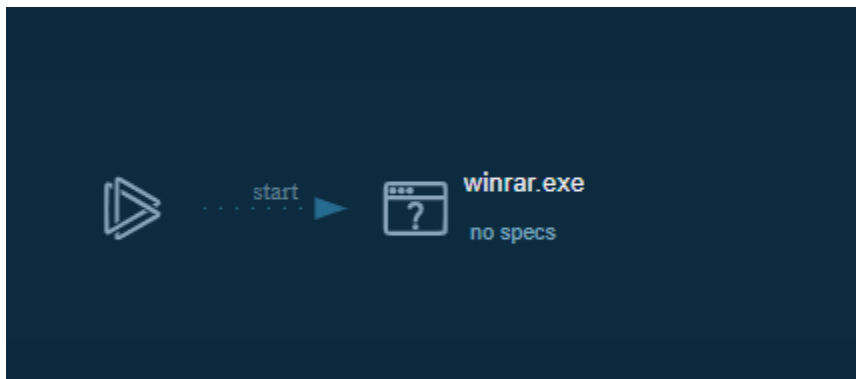
c:\windows\system32\user32.dll

c:\windows\system32\win32u.dll

c:\windows\system32\gdi32.dll

c:\windows\system32\gdi32full.dll

Graph



ATT&CK

MITRE ATT&CK Matrix

All tactics

Tactics 0 | Techniques 0 | Events 0

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
----------------	-----------	-------------	----------------------	-----------------	-------------------	-----------	------------------	------------	-------	--------------	--------

No indicators fall under the category

Task 8

Based on the the text report and the information I've collected on this sample, this malware is generally harmless to users. Some characteristics that lead to this conclusion include no suspicious files being injected during packet transfer, and no hints at any malicious activity while the application was running.

Task 9

The main characteristics of this malware sample include a threat score of 20%, a few suspicious activities from the text report, and nomalicious activities.

Task 10

The difference between the Marai and VIPKeyLogger malwares is that the VIPKeylogger is more of a threat due to the nature of how the application is ran. It is used to record what keys are pressed at a certain time, while the Marai malware is relatively harmless.