

Task One:

MALWARE bazaar

🔍 Browse

📁 Upload

🔎 Hunting

🔗 API

📄 Export

📊 Statistics

📖 FAQ

📄 About

👤 Login

See search syntax see below, example: tag:TrickBot

Search

Search Syntax

Search: Mini

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-10-22 21:25	0685efff3bc7a29fe4e077...	sh		malware	abuse_ch	
2024-10-23 23:36	71864cf35bd1f85f0b8fe...	elf	Malware	elf malware	abuse_ch	
2024-10-23 23:16	2597a3db3169a3fb5fd4d...	elf	Malware	elf malware	abuse_ch	
2024-10-23 18:41	a7b23985271a5367a2ac...	elf	Malware	elf malware	abuse_ch	
2024-10-23 18:11	04e95cea42bebe788483...	elf	Malware	elf malware	abuse_ch	
2024-10-23 17:51	f57742429adca02b45d12...	elf	Malware	elf malware	abuse_ch	
2024-10-23 17:46	9a1c88f0d90e651fcd65f3...	elf	Malware	elf malware	abuse_ch	
2024-10-23 17:41	5b7be271c2a864158115...	elf	Malware	elf malware	abuse_ch	
2024-10-23 17:31	d47f0ab862a38df72eb8a...	elf	Malware	elf malware	abuse_ch	
2024-10-23 17:06	a15bdc8b6b62d68cdac9...	elf	Malware	elf malware	abuse_ch	
2024-10-23 12:14	60f38e76f44ceed9f9bb4...	elf	Malware	32 elf malware macthundera	zbtcheckin	
2024-10-23 12:14	6f7f924f7b82ca7a730729...	elf	Malware	32 elf malware powersploit	zbtcheckin	
2024-10-23 12:14	de137a2b6427df64a622...	elf	Malware	32 arm elf malware	zbtcheckin	
2024-10-23 12:14	4ad74d314f7261b0467...	elf	Malware	32 elf malware renmas	zbtcheckin	
2024-10-23 12:14	ed91a9136f2754371fb94...	elf	Malware	32 elf malware sploit	zbtcheckin	
2024-10-23 11:36	3c850e331dea512d6b80...	elf	Malware	elf malware	abuse_ch	

Task Two:

Cropped out the files and such on the left so that only what was needed is in the screenshot

📁

2597a3db3169a3fb5fd4d...
b5f64d07f72e94c
7db55d4de0a6f7
7c8039c6583a3...

Task Six:

Connections

	HTTP Requests	7	Connections	57	DNS Requests	19	Threats	0	Filter by PID, domain, name or ip			PCAP
NETWORK	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
	BEFORE	TCP	✓	6944	svchost.exe	🇮🇹	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 898 b	↓ -
FILES	BEFORE	UDP	✓	4	System	🇵🇪	192.168.100.255	137	-	-	↑ 898 b	↓ -
	BEFORE	TCP	✓	4360	SearchApp.exe	🇩🇪	2.16.110.121	443	www.bing.com	Akamai International B.V.	No Data	-
DEBUG	BEFORE	TCP	✓	4360	SearchApp.exe	🇩🇪	2.16.110.121	443	www.bing.com	Akamai International B.V.	No Data	-
	BEFORE	TCP	✓	5488	MolUsaCoreWorker.exe	🇮🇹	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data	-
	BEFORE	TCP	✓	3952	RUXOMICS.exe	🇮🇹	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data	-
	BEFORE	UDP	✓	4	System	🇵🇪	192.168.100.255	138	-	-	↑ 2 Kb	↓ -
	7923 ms	TCP	✓	6944	svchost.exe	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb	↓ 8 Kb
	7928 ms	TCP	✓	6944	svchost.exe	🇩🇪	23.216.77.6	80	crl.microsoft.com	Akamai International B.V.	↑ 216 b	↓ 1 Kb

DNS Requests:

HTTP Requests 7 Connections 57 DNS Requests 19 Threats 0										Filter by IP or domain		PCAP
NETWORK	Timeshift	Status	Rep	Domain		IP						
	BEFORE	Responded	✓	settings-win.data.microsoft.com		4.231.128.59						
FILES	BEFORE	Responded	✓	www.bing.com		2.16.110.121						
	BEFORE	Responded	✓	google.com		142.250.186.78						
DEBUG	7911 ms	Responded	✓	settings-win.data.microsoft.com		51.104.136.2						
	7912 ms	Responded	✓	crl.microsoft.com		23.216.77.6						
						23.216.77.28						
	7913 ms	Responded	✓	www.microsoft.com		184.30.21.171						
						40.126.32.68						
						20.190.160.17						

HTTP Requests:

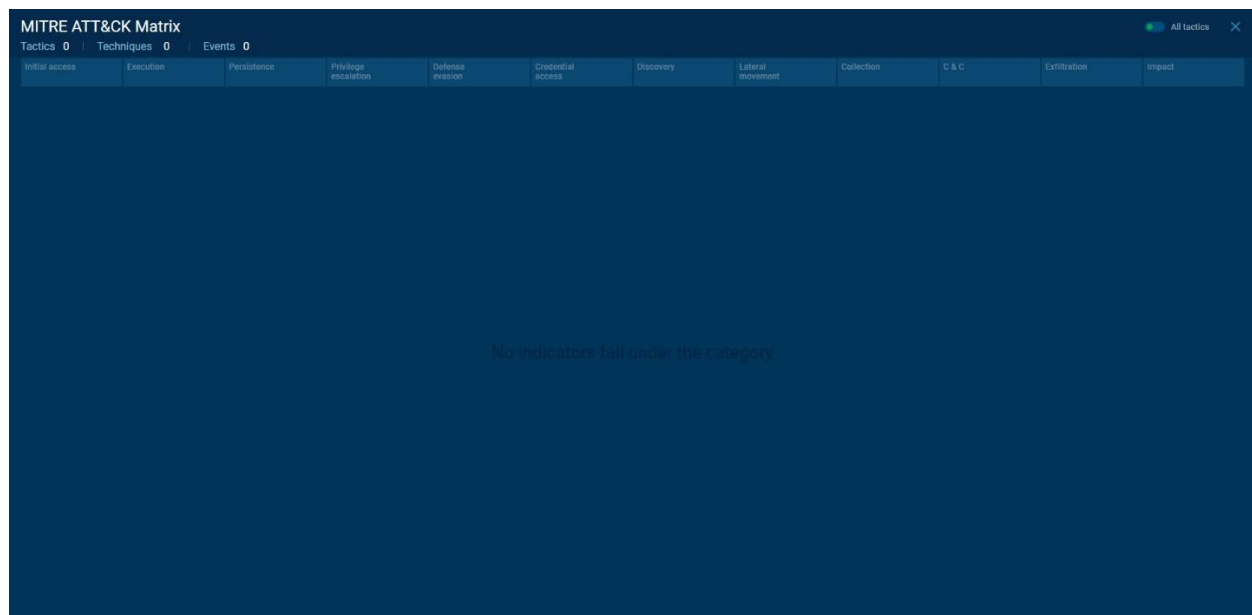
	HTTP Requests	7	Connections	57	DNS Requests	19	Threats	0	Filter by PID, name or url			PCAP
NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content				
	7929 ms	GET 200: OK	✓	6944	svchost.exe	🇩🇪	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	1 Kb	↓ binary			
FILES	7936 ms	GET 200: OK	✓	6944	svchost.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b	↓ binary			
	21255 ms	GET 200: OK	✓	5852	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUAABSAUQYBMq2awn...	471 b	↓ binary			
DEBUG	21263 ms	GET 200: OK	✓	4360	SearchApp.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUAABBTjrydRyt%2BApF...	312 b	↓ binary			
	27349 ms	GET 200: OK	✓	3772	backgroundTaskHost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUAABQ50obx%2Fh02it%...	471 b	↓ binary			
	27357 ms	GET 200: OK	✓	1372	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Cert...	419 b	↓ binary			
	28340 ms	GET 200: OK	✓	1372	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Se...	408 b	↓ binary			

Threats:

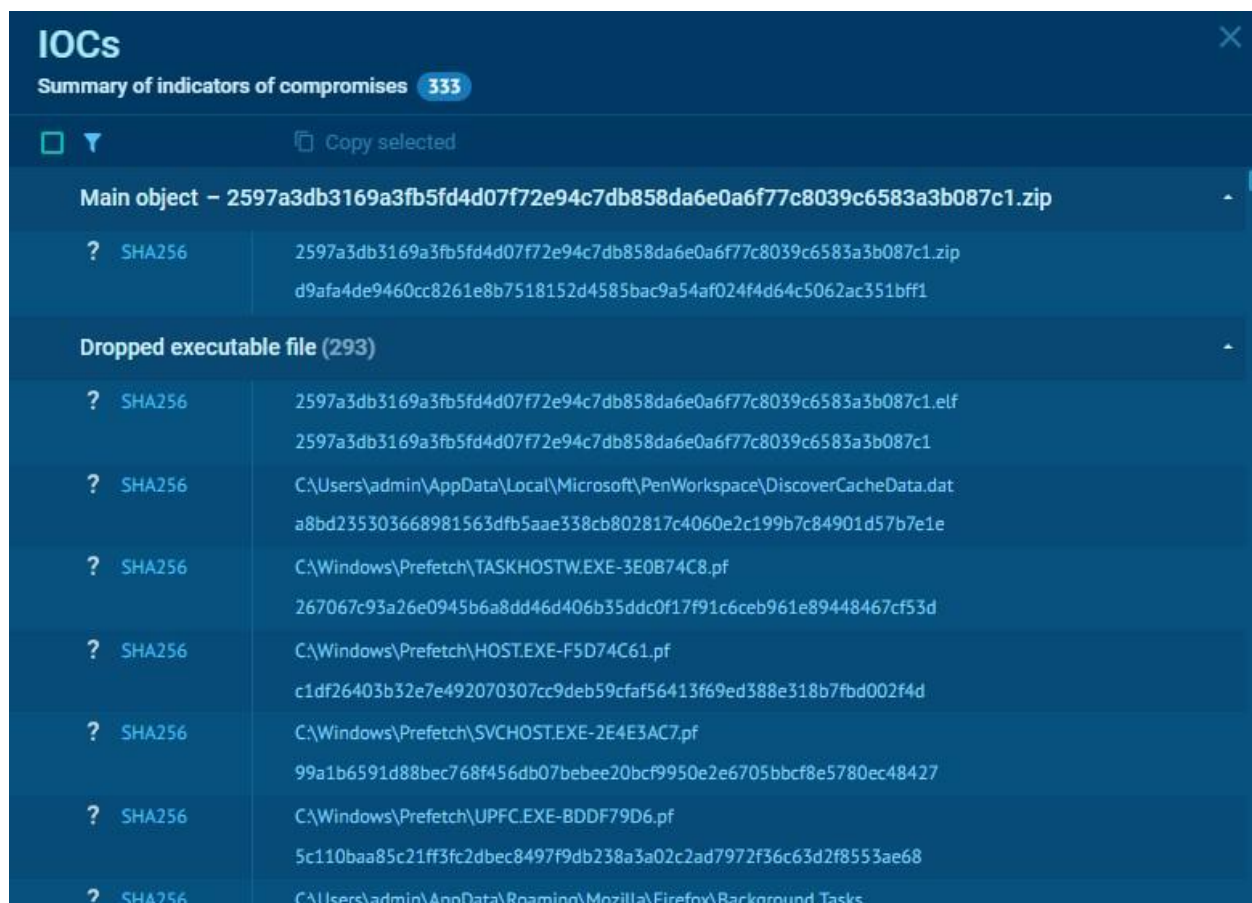
		HTTP Requests		7	Connections		57	DNS Requests		19	Threats		0	Filter by message		PCAP
		Timeshift		Class				PID		Process name		Message				
NETWORK																
FILES																
DEBUG																
		No data														

Task Seven:

No indicators were shown under the attack category



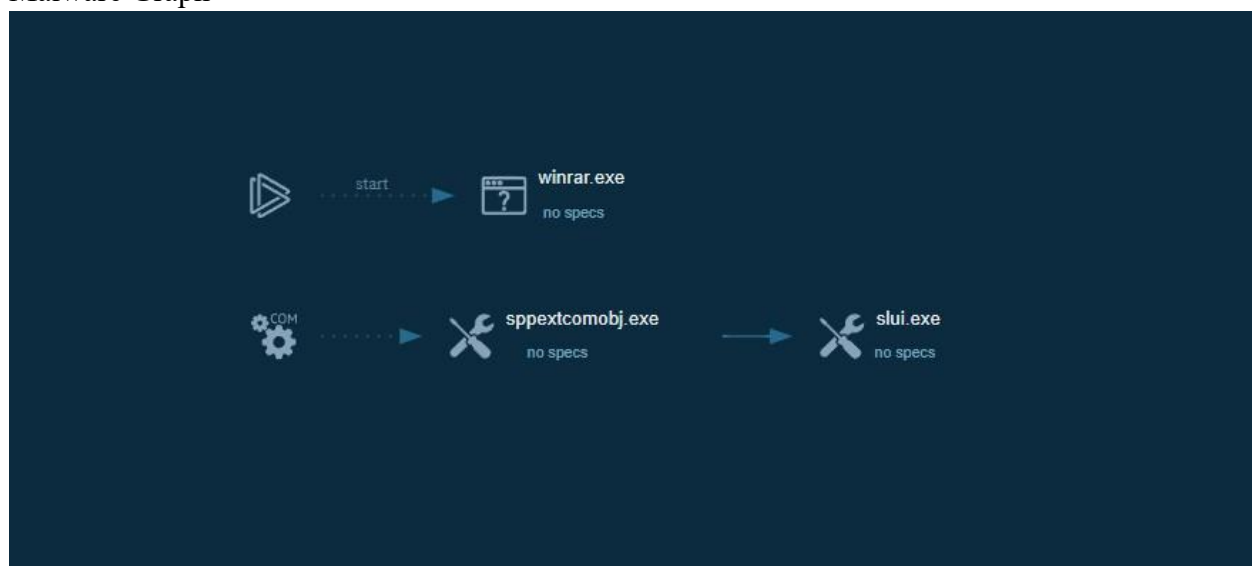
Over 290 dropped executable files



Indicated seven http requests, mainly Microsoft and digicert websites

IOCs	
Summary of indicators of compromises 333	
<input type="checkbox"/>	Copy selected
IP	4.175.87.197
IP	20.223.36.55
IP	104.126.37.131
IP	23.52.120.96
IP	20.103.156.88
IP	239.255.255.250
HTTP/HTTPS requests (7)	
URL	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl
URL	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl
URL	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDL7190VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D
URL	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTjrjydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdIUkHMEWNpYim8S8YCEAI5PUJXAKJafLQcAAso18o%3D
URL	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBQ50otx%2Fh0Ztl%2Bz8SIPI7wEWVxDIQUTIJUIBIV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdI6vHL3O1J0%3D
URL	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl
URL	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl

Malware Graph



General info from text report, no threats detected

ANYRUN

INTERACTIVE MALWARE ANALYSIS

General

Behavior

MalConf

Static information

Video

Screenshots

System events

Network

General Info

Add for printing

File name:

2597a3db3169a3fb5fd4d07f72e94c7db858da6e0a6f77c8039c6583a3b087c1.zip

Full analysis:

<https://app.any.run/tasks/fa0846bd-c2eb-45e5-b1b0-99b0ff358826>

Verdict:

No threats detected

Analysis date:

October 23, 2024 at 22:04:52

OS:

Windows 10 Professional (build: 19045, 64 bit)

Indicators:

MIME:

application/zip

File info:

Zip archive data, at least v5.1 to extract, compression method=AES Encrypted

MD5:

9B9622027A487EED3B38252C04DAC2C9

SHA1:

D51A8F4A43E860AACFE23D97E6E87BF9E602D806

SHA256:

D9AFA4DE9460CC8261E8B7518152D4585BAC9A54AF024F4D64C5062AC351BFF1

SSDEEP:

768:IXTr+hKbkvx9fRmx/j5JHHIEVxS7J9VhsXqKyEBWIMd8I8ahYc2W:IXTBhAg9Ub5Jtwxy9fsSXqrG1C9J

ANY.RUN

is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is.

ANY.RUN

does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Modification events from text report shows over 1,700 logged events

Total events

Read events

Write events

Delete events

1 739

1 733

6

0

Modification events

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: C:\Users\admin\Desktop\GoogleChromeEnterpriseBundle64.zip

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArchHistory

Name: 1

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: C:\Users\admin\AppData\Local\Temp\2597a3db3169a3fb5fd4d07f72e94c7db858da6e0a6f77c8039c6583a3b087c1.zip

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArchHistory

Name: 0

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: 120

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths

Name: name

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: 80

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths

Name: size

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: 120

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths

Name: type

(PID) Process: (6264) WinRAR.exe

Operation: write

Value: 100

Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths

Name: mtime

Files activity

Add for printing

Executable files

Suspicious files

Text files

Unknown types

0

0

0

0

Dropped files

Task Eight

The malware sample I found was a Mirai sample, which is a type of botnet that will use vulnerable devices to commit DDoS attacks. We can see in the analysis that the malware sent numerous connection requests, as well as some HTTP and DNS requests to connect to vulnerable devices and networks, with some succeeding. Despite this, it did not seem to pose any threat according to the analysis which stated it detected no threats. In addition, there were a few logged modification events that can be seen above, so it seems the malware sample did modify a few files.

Task Nine

Connections

		HTTP Requests		7		Connections		51		DNS Requests		22		Threats		0		Filter by PID, domain, name or ip				PCAP	
NETWORK	FILES	DEVELO	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	✓	6944	svchost.exe	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data										
			BEFORE	TCP	✓	1752	RUXIMICS.exe	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data										
			BEFORE	TCP	✓	5488	MoUsCoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data										
			BEFORE	TCP	✓	-	-	🇩🇪	184.86.251.27	443	www.bing.com	Akamai International B.V.	No Data										
			BEFORE	TCP	✓	-	-	🇩🇪	184.86.251.27	443	www.bing.com	Akamai International B.V.	No Data										
			163 ms	UDP	✓	4	System	🇮🇹	192.168.100.255	138	-	-	↑	2 Kb	↓	-							
			7383 ms	TCP	✓	6944	svchost.exe	🇮🇹	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑	2 Kb	↓	8 Kb							
			7387 ms	TCP	✓	6944	svchost.exe	🇩🇪	23.216.77.6	80	crl.microsoft.com	Akamai International B.V.	↑	216 B	↓	1 Kb							

DNS Requests

		HTTP Requests		7	Connections		51	DNS Requests		22	Threats		0	Filter by IP or domain		PCAP
NETWORK	Timeshift	Status	Rep	Domain								IP				
	BEFORE	Responded	✓	settings-win.data.microsoft.com								51.104.136.2				
FILES	BEFORE	Responded	✓	www.bing.com								184.86.251.27				
												184.86.251.19				
DEBUG	BEFORE	Responded	✓	google.com								142.250.184.238				
	7371 ms	Responded	✓	settings-win.data.microsoft.com								40.127.240.158				
	7372 ms	Responded	✓	crl.microsoft.com								23.216.77.6				
	7373 ms	Responded	✓	www.microsoft.com								184.30.21.171				

HTTP Requests

HTTP Requests										7	Connections		51	DNS Requests		22	Threats		0	Filter by PID, name or url		± PCAP
NETWORK	Timeshift		Headers		Rep	PID	Process name	CN	URL				Content									
	7389 ms	GET	200: OK		6944	svchost.exe		http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_011_03_22.crl				1 Kb	+	binary								
	7396 ms	GET	200: OK		6944	svchost.exe		http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl				973 b	+	binary								
	21726 ms	GET	200: OK		944	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBmq2awn...				471 b	+	binary								
	21770 ms	GET	200: OK		4360	SearchApp.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTjrydRy%28ApF...				312 b	+	binary								
	27328 ms	GET	200: OK		6000	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Cer...				419 b	+	binary								
	27330 ms	GET	200: OK		6000	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Se...				408 b	+	binary								
	32426 ms	GET	200: OK		7076	backgroundTaskHost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSQ0ote%20Fh0zt%...				471 b	+	binary								
FILES																						
DEBUG																						

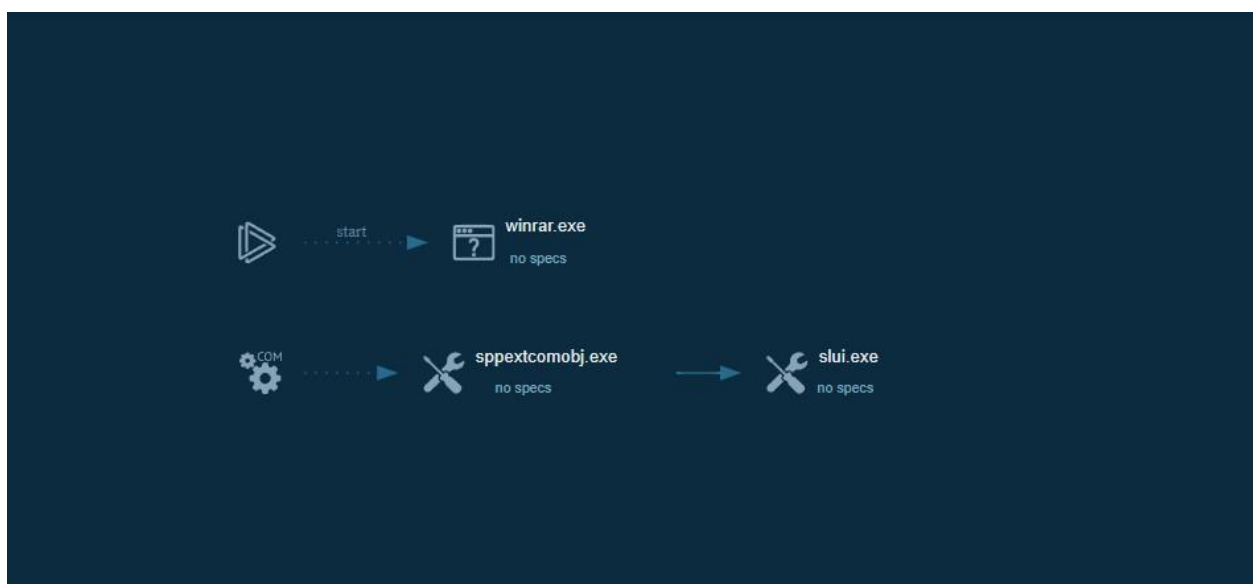
Threats

HTTP Requests 7Connections 51DNS Requests 22Threats 0											Filter by message	PCAP	
TimeshiftClassPIDProcess nameMessage													
NETWORK													
FILES													
DEBUG													
No data													

Attack Matrix

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											

Malware graph



IOC's that showed some compromise

IOCs

Summary of indicators of compromises **335**

☐

Copy selected

Main object – a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237.zip

? SHA256

a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237.zip
fe1f1b7e2453f4a2b8ec35f138f800648afabf1beb06b99c40199a9d4b571233

Dropped executable file (294)

? SHA256

a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237.vbs
a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237

? SHA256

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

? SHA256

C:\Windows\Prefetch\SVCHOST.EXE-2E4E3AC7.pf
961cd96dfd704a6b92ec5ec0607ffdc3feb3c35ee2a625bcb3e887d6df237b1

? SHA256

C:\Windows\Prefetch\TASKHOSTW.EXE-3E0B74C8.pf
9457a352022903ed27604202ea054d390e1774bbfbd7ccb35ba05e1b90fcc00b

? SHA256

C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Background Tasks
Profiles\93u99co2.MozillaBackgroundTask-308046B0AF4A39CB-
defaultagent\datareporting\glean\db\data.safe.tmp
81c14432135b2a50dc505904e87781864ca561efef9e94baeca3704d04e6db3d

? SHA256

C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Background Tasks
Profiles\93u99co2.MozillaBackgroundTask-308046B0AF4A39CB-

IOCs

Summary of indicators of compromises **335**

☐

Copy selected

IP

40.115.3.253

? IP

20.223.36.55

IP

192.229.221.95

? IP

20.199.58.43

IP

2.23.209.133

IP

239.255.255.250

HTTP/HTTPS requests (7)

URL

http://crLmicrosoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl

URL

http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl

URL

http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDL7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D

URL

http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tlpPmhxdIuNkHMEWNPYim8S8YCEAI5PUjXAkJafLQcAAso18o%3D

URL

http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl

URL

http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl

URL


http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSQ50otx%2Fh0Ztl%2Bz8SiPI7wEWWxDIQQUTIJUIBIV5uNu5g%2F6%2BrkS7QYXjkCEAn5bsKVVV8kd6vHl3O1J0%3D


IOCs	
Summary of indicators of compromises 335	
<input type="checkbox"/>	Copy selected
	1B96859CE5D
	0e73ee907584f4060d12dfadb893113b3433ff030aaebd935dc1d396dcf4340c
? SHA256	C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
	e07fd75ccbfea5f8459dfe4c169b8707b4a8838a789168ddea29d1db69f77527
? SHA256	C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
	b465b3ddab160ac52b47da44e6aca51f6013beac5b9feafb898783afdf1b7f1e
? SHA256	C:\Users\admin\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
	c7b3fe594bd3dc2c760f53a0ab396111dd837cb076072af5a41847e4e52b9a61
? SHA256	C:\Users\admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-1693682860-607145093-2874071422-1001\Preferred
	89ba9f020db5e7432f71682cb1d1e2a5147cc4c4d730f17b06ea47b2fd11d05b
? SHA256	C:\Users\admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-1693682860-607145093-2874071422-1001\73f1831e-c462-4736-8022-8725c3a4c667
	863406d38c6092db8bdf687d9d8b6c9d7b04d07da921776b17d3f9f52b751184
? SHA256	C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
	f62bcb68768ef90fa05490240bb9315d8a63cd2e0c1757b56fe4f520610cd4dc
? SHA256	C:\Windows\Prefetch\RUNTIMEBROKER.EXE-660365C8.pf

IOCs	
Summary of indicators of compromises 335	
<input type="checkbox"/>	Copy selected
? SHA256	C:\Users\admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-1693682860-607145093-2874071422-1001\73f1831e-c462-4736-8022-8725c3a4c667
	863406d38c6092db8bdf687d9d8b6c9d7b04d07da921776b17d3f9f52b751184
? SHA256	C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
	f62bcb68768ef90fa05490240bb9315d8a63cd2e0c1757b56fe4f520610cd4dc
? SHA256	C:\Windows\Prefetch\RUNTIMEBROKER.EXE-660365C8.pf
	06a20a746db85e07f9a075b79ec92582a91e5dfcaf07635aa19c957327306dd7
? SHA256	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.Client.CBS_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A
	af5f650894956db4985acf8ac0e76f24ccce7cb6f82189a9afa307866e64336f
? SHA256	C:\Windows\Prefetch\SVCHOST.EXE-86AA6B35.pf
	b53c5fc72a5b841ceb4b77877cb6f6b54463b536fba6f7466fcc4eac548af185
? SHA256	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.Client.CBS_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A
	9e0c7c61ace58fca8a215f093ec1d1630c5983e4a057e70b07bc45685fbd4bb
? SHA256	C:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\V01.chk
	b2d6d7d0f5d5f974846047017b410c98569596c683c9cc051b2016d591c9716a
? SHA256	C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf

Text report showed nothing strange

General Info

☒ Add for printing 

File name: a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237.zip
Full analysis: <https://app.any.run/tasks/0071cfda-e613-47f6-ab1f-2cba6c681730>
Verdict: **No threats detected**
Analysis date: October 23, 2024 at 22:54:16
OS: Windows 10 Professional (build: 19045, 64 bit)
Tags: arch-scr
Indicators: 
MIME: application/zip
File info: Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
MD5: 08991C20581769F1FBD3010BB3CBE50
SHA1: ECED2C40F1AC25FFCF8582D660A64B2C7318458E
SHA256: FE1F1B7E2453F4A2B8EC35F138F800648AFABF1BEB06B99C40199A9D4B571233
SSDEEP: 12288:hAzBcCtHTuWiaNv7Zz0FOGAKsJRo5clPPGsK/hAzBcCJTuWMI7i0fzAKsJRo5clPPGsK/

 ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

☒ Add for printing 

MALICIOUS


Generic archive extractor
• WinRAR.exe (PID: 5508)

SUSPICIOUS


No suspicious indicators.

INFO

No info indicators.

 Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#) 

Registry activity

☒ Add for printing 

Total events	Read events	Write events	Delete events
1 746	1 740	6	0

Modification events

(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory
Operation: write	Name: 1
Value: C:\Users\admin\Desktop\GoogleChromeEnterpriseBundle64.zip	
(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory
Operation: write	Name: 0
Value: C:\Users\admin\AppData\Local\Temp\1a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237.zip	
(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write	Name: name
Value: 120	
(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write	Name: size
Value: 80	
(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write	Name: type
Value: 120	
(PID) Process: (5508) WinRAR.exe	Key: HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write	Name: mtime

This was a keylogger, which logs the keystrokes on a users device to find passwords. We can see it attempting to connect a few times but not being able to, hence it posing very little threats from the analysis.

Task 10:

These two forms of malware may seem very different, but they do share some similarities. Their graphs and methods of attack seemed to be similar, attempting to find points of vulnerability to exploit devices. However, they both do very different things when it comes to attacking, as the Mirai botnet tries to exploit devices for DDoS attacks while the keylogger tries to find devices to log passwords from.