ID: 528001
Sample Name: cRC6TZG6Wx
Cookbook: default.jbs
Time: 16:49:28
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

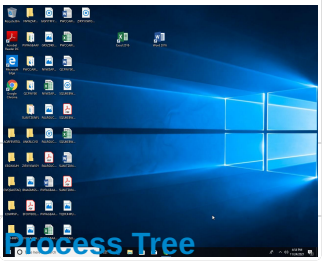
Windows Analysis Report cRC6TZG6Wx

Overview

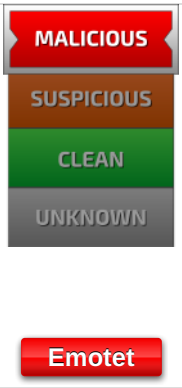
General Information

Sample Name:	cRC6TZG6Wx (renamed file extension from none to dll)
Analysis ID:	528001
MD5:	8f6552b136a4dd8.
SHA1:	fea5b1d5e44dc58.
SHA256:	03995882170eb6..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

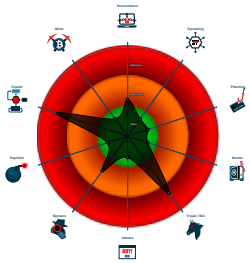


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Changes security center settings (no…
- Machine Learning detection for samp…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



- **System is w10x64**
- svchost.exe (PID: 7156 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- loaddll32.exe (PID: 1464 cmdline: loaddll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6412 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4516 cmdline: rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5000 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6384 cmdline: rundll32.exe C:\Users\user\Desktop\cRC6TZG6Wx.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5776 cmdline: rundll32.exe C:\Users\user\Desktop\cRC6TZG6Wx.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6620 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zrrbzia\fotuyl.lzj",HSFp MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 4720 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Zrrbzia\fotuyl.lzj",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- SgrmBroker.exe (PID: 6456 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6444 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5528 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2528 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 2148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5336 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1952 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2464 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6284 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "Public Key": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ],
  "C2 list": [
    "51.178.61.60:443",
    "168.197.250.14:80",
    "45.79.33.48:8080",
    "196.44.98.190:8080",
    "177.72.80.14:7080",
    "51.210.242.234:8080",
    "185.148.169.10:8080",
    "142.4.219.173:8080",
    "78.47.204.80:443",
    "78.46.73.125:443",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "191.252.103.16:80",
    "54.38.242.185:443",
    "85.214.67.203:8080",
    "54.37.228.122:443",
    "207.148.81.119:8080",
    "195.77.239.39:8080",
    "66.42.57.149:443",
    "195.154.146.35:443"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000003.360457905.0000000003396000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.290674131.0000000000576000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.289238760.0000000000D86000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.809828703.0000000003396000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000003.289903082.0000000000576000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.3.rundll32.exe.576c48.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.576c48.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.d86b70.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.9c77f0.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.3.rundll32.exe.576c48.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 12 entries

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

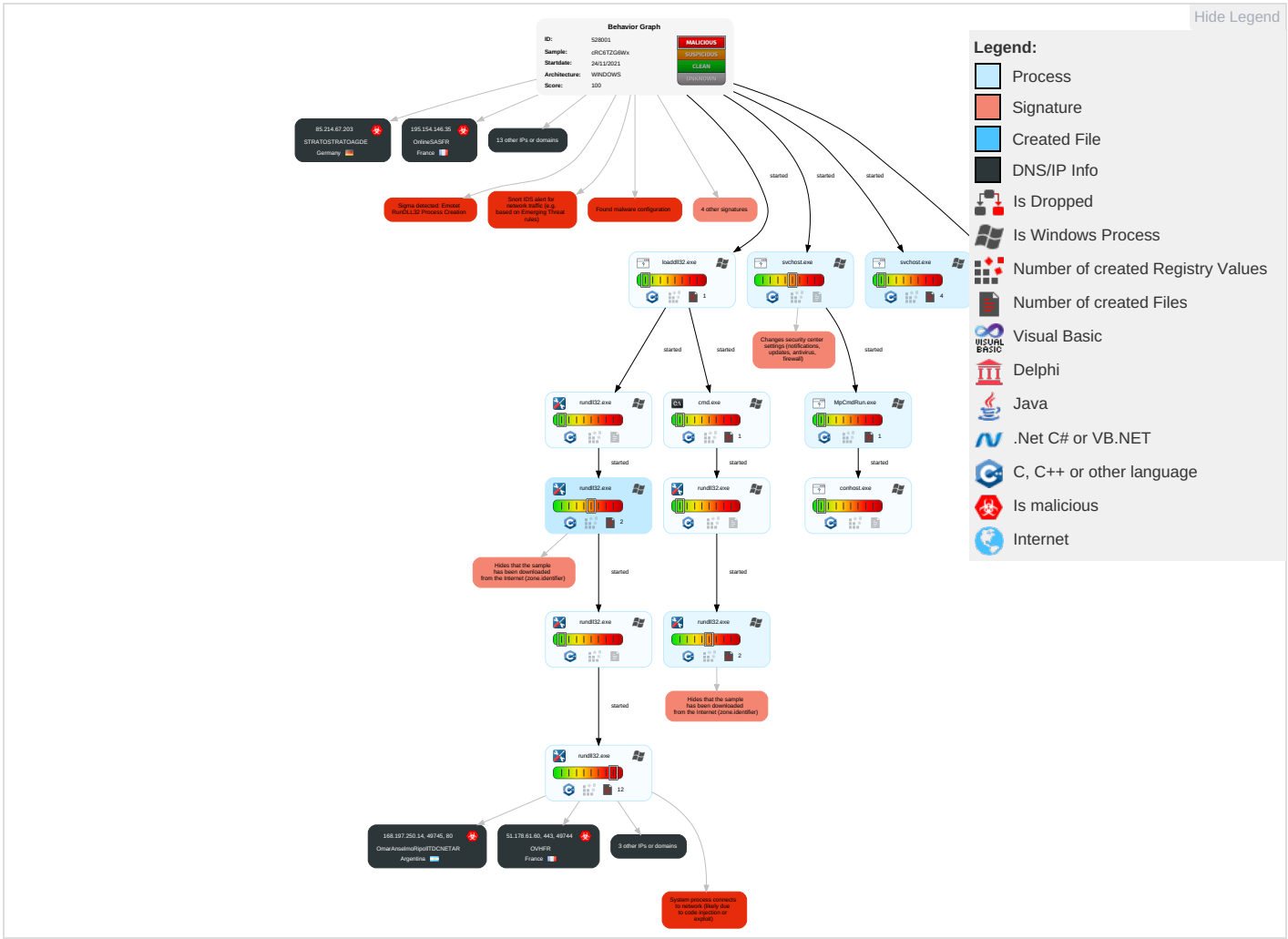
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 2	Masquerading 2 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eave Insec Netw Comi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Security Software Discovery 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	Explo Track Locat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	System Information Discovery 2 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

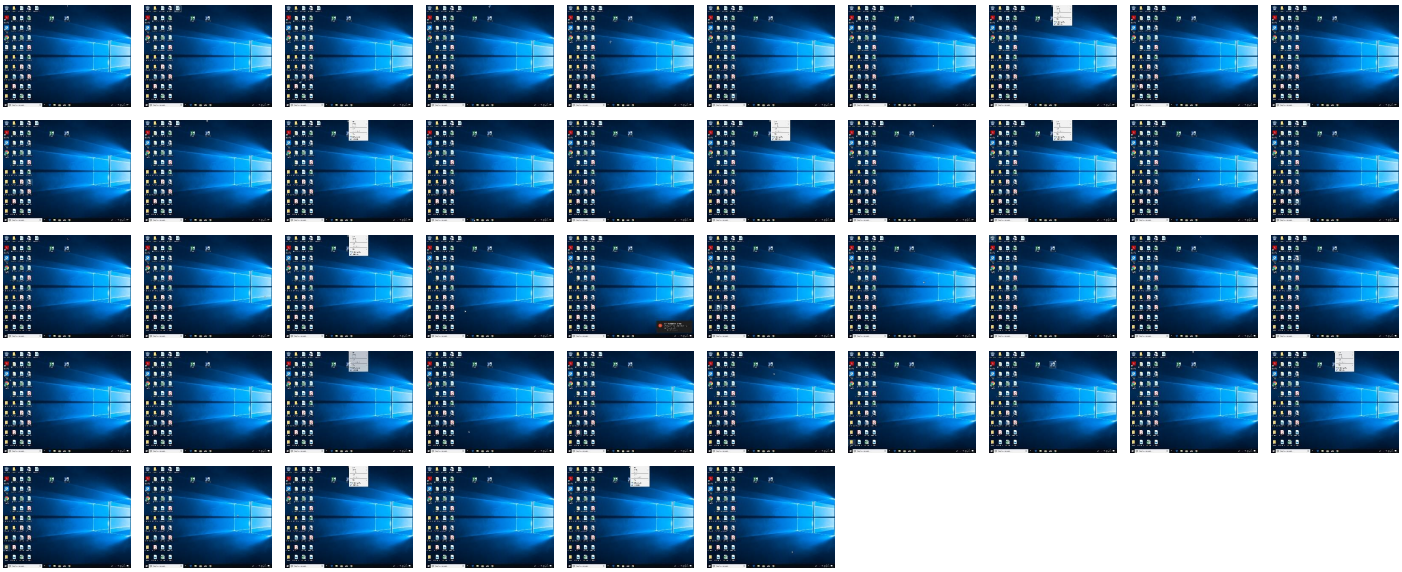
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cRC6TZG6Wx.dll	18%	Virustotal		Browse
cRC6TZG6Wx.dll	18%	ReversingLabs	Win32.Trojan.Mansabo	
cRC6TZG6Wx.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.33a6b88.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.3.rundll32.exe.33a6b88.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.9c77f0.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.3.rundll32.exe.33a6b88.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://51.178.61.60/cOCoCBOnwtlaPwqgYJsibWlqGyXElLKsrFlsKtesNMVjGBKbplkpiwohTqB	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://51.178.61.60/cOCoCBOnwtlaPwqgYJsibWlqGyXElLKsrFlsKtesNMVjGBKbplkpiwohTqB	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
45.79.33.48	unknown	United States		63949	LINODE-APLinodeLLCUS	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
51.178.61.60	unknown	France		16276	OVHFR	true
177.72.80.14	unknown	Brazil		262543	NewLifeFibraBR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.210.242.234	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528001
Start date:	24.11.2021
Start time:	16:49:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cRC6TZG6Wx (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@26/9@0/20
EGA Information:	Failed
HDC Information:	• Successful, ratio: 76.4% (good quality ratio 67.5%) • Quality average: 70.3% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:51:24	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
16:51:30	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKltBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	
	2n64VXT08V.dll	Get hash	malicious	Browse	
196.44.98.190	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKltBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	
	2n64VXT08V.dll	Get hash	malicious	Browse	

Domains

No context

ASN

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 66.42.57.149
	AWB_NO_9284730932.exe	Get hash	malicious	Browse	• 45.32.28.45
	arm6-20211124-0649	Get hash	malicious	Browse	• 44.168.42.223
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	bomba.arm	Get hash	malicious	Browse	• 44.168.169.161
	44E401AAF0B52528AA033257C1A1B8A09A2B10EDF26ED.exe	Get hash	malicious	Browse	• 149.28.253.196
	77012C024869BA2639B54B959FAB1E10EBAAF8EBB9BFC.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	5giHvDqMaL	Get hash	malicious	Browse	• 45.63.53.236
	22BA4262D93379DE524029DAFC7528E431E56A22CB293.exe	Get hash	malicious	Browse	• 149.28.253.196
	6PZ6S2YGPB	Get hash	malicious	Browse	• 45.63.53.204
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 149.28.253.196
	QABYgAqa5Z.exe	Get hash	malicious	Browse	• 149.28.253.196
	ZrAv540yA4.exe	Get hash	malicious	Browse	• 216.128.137.31
	6Xtf11WnP2.exe	Get hash	malicious	Browse	• 216.128.137.31
	M9WBCy4NNi.exe	Get hash	malicious	Browse	• 216.128.137.31
	aBGNeDS7yM.exe	Get hash	malicious	Browse	• 149.28.253.196
EcobandGH	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 196.44.98.190
	1711.doc	Get hash	malicious	Browse	• 196.44.98.190
	n6J7QJs4bk.dll	Get hash	malicious	Browse	• 196.44.109.73
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 196.44.98.190
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 196.44.98.190
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 196.44.98.190
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 196.44.98.190
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 196.44.98.190
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 196.44.98.190
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 196.44.98.190
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 196.44.98.190
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 196.44.98.190
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 196.44.98.190
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 196.44.98.190
	a65FgjVus4.dll	Get hash	malicious	Browse	• 196.44.98.190
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 196.44.98.190
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	• 196.44.98.190
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 196.44.98.190
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 196.44.98.190
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 51.178.61.60
	ReadMe[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	cTplVWrqRR.dll	Get hash	malicious	Browse	• 51.178.61.60
	NErdgsNsKR.vbs	Get hash	malicious	Browse	• 51.178.61.60
	F.A.Q[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	Q1KL4ickDw.dll	Get hash	malicious	Browse	• 51.178.61.60
	yZGYbaJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	1711.doc	Get hash	malicious	Browse	• 51.178.61.60
	cs.exe	Get hash	malicious	Browse	• 51.178.61.60
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 51.178.61.60
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 51.178.61.60
	bbyGAgHI9O.dll	Get hash	malicious	Browse	• 51.178.61.60
	Vs6ZDk0LMC.dll	Get hash	malicious	Browse	• 51.178.61.60
	sTh52oTZDh.dll	Get hash	malicious	Browse	• 51.178.61.60
	loveTubeLike.dll	Get hash	malicious	Browse	• 51.178.61.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2SR3psYDHQ.js	Get hash	malicious	Browse	• 51.178.61.60
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 51.178.61.60
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 51.178.61.60
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 51.178.61.60
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U....''<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.''.Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.''.g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y...,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.112261679299932
Encrypted:	false
SSDEEP:	6:kKKszk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:fz9kPlE99SNxAhUeYlUSA/t
MD5:	105D91694D8C910B9C43CE5444D9EB69
SHA1:	8ED3CC412C96AAA24D5D5F750475586CD329DA92
SHA-256:	F0B825D17862A0F7201EC6FC9A37388D059A6E9BCF4954C3D2D063253DD074F2
SHA-512:	490ECAB75B25B352BC29DF15AC027F94B1A2E826EE2E38BC54A8B4605A0E1B40E0260C9AFA0E2437BDA4540BA55780A7FB4AEC342E12CC97850F492C66D00A 99
Malicious:	false
Preview:	p..... .....(..... .....q.\].....&.....h.t.t.p.:.//./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i. c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...''.0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0.''...

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11037577422479908
Encrypted:	false
SSDEEP:	12:262zXm/Ey6q9995ONq3qQ10nMCldimE8eawHjcwKv:26jl68sgLyMCldzE9BHjcwa
MD5:	5E797ECA2ECA23F42CA6FF4C3B51CE4E
SHA1:	7C795E48E6FDB31F426DC71881A5A90AE6C57AAF
SHA-256:	C67A70F2116D90654B44E1CC9CE071D27F9A721B4DBE4391132AE2A7A456E4BC
SHA-512:	4F52016A6D2DFF0116F6893DFB8C77627E05B966BA613959E98358AC3FC0460AF4987A601E94723A31F1EB18CB4913340221A7B9DD67CCF9072DCD6B605C6294
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Preview:	.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....|..... .....n.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s .\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....,..R..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11304172349420055
Encrypted:	false
SSDEEP:	12:HPzXm/Ey6q9995Ew1miM3qQ10nMCldimE8eawHza1miId/Cf:HSl682w1tMLyMCldzE9BHza1tlU
MD5:	BB87AC16DE738F66D5FDCDB7C1FD127B
SHA1:	4EAC0B32D34BE169387793A2ED8BC5760BA43B22
SHA-256:	756BF567603EA99F9C9028CD4EA537EDC285A805560A24CFF36810EEC5C423F2
SHA-512:	852EA9349AEF417727DC3974C2612DEEF233B3DD6A9A5A3A3EDC64CF984FE6668C3E5A60C502DD23A2AA4D5740EC0AE50AC52A90C8CCAF6BFC6D2AC8D91C DE1
Malicious:	false
Preview:	.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....|..... ...../.m.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....,..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11267034534910954
Encrypted:	false
SSDEEP:	12:OVXm/Ey6q999551mK2P3qQ10nMCldimE8eawHza1mKhX:O4l68n1iPLyMCldzE9BHza1R
MD5:	3DE57E9FAC960F1E165B5DBB6E753B3C
SHA1:	A3E4EDE7BF342690C36C8F9DDA04C005CABB990A
SHA-256:	AF8DDE8B05FC7E4511CF58545BB9DCA4275847A0A25C154D18D826DBE79AA65F
SHA-512:	076CE6FFD88142CFC6C30455F9E3329A44C40C07511A1416EF54ACB6F4D370A0EEFF8196592CFCD5617A7F226501482117FEE7BE771B3BF5D30A8895EC13242
Malicious:	false
Preview:	.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....|..... .....m..m.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....,..S..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001S (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11037577422479908
Encrypted:	false
SSDEEP:	12:262zXm/Ey6q9995ONq3qQ10nMCldimE8eawHjcwKv:26jl68sgLyMCldzE9BHjcwa
MD5:	5E797ECA2ECA23F42CA6FF4C3B51CE4E
SHA1:	7C795E48E6FDB31F426DC71881A5A90AE6C57AAF
SHA-256:	C67A70F2116D90654B44E1CC9CE071D27F9A721B4DBE4391132AE2A7A456E4BC
SHA-512:	4F52016A6D2DFF0116F6893DFB8C77627E05B966BA613959E98358AC3FC0460AF4987A601E94723A31F1EB18CB4913340221A7B9DD67CCF9072DCD6B605C6294
Malicious:	false
Preview:	.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....|..... .....n.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s .\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....,..R..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11304172349420055
Encrypted:	false
SSDEEP:	12:HPzXm/Ey6q9995Ew1miM3qQ10nMCldimE8eawHza1miId/Cf:HSl682w1tMLyMCldzE9BHza1tIU
MD5:	BB87AC16DE738F66D5FDCDB7C1FD127B
SHA1:	4EAC0B32D34BE169387793A2ED8BC5760BA43B22
SHA-256:	756BF567603EA99F9C9028CD4EA537EDC285A805560A24CFF36810EEC5C423F2
SHA-512:	852EA9349AEF417727DC3974C2612DEEF233B3DD6A9A5A3A3EDC64CF984FE6668C3E5A60C502DD23A2AA4D5740EC0AE50AC52A90C8CCAF6BFC6D2AC8D91CDE1
Malicious:	false
Preview:	....,..........................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2..@.t.z.r.e.s...d.l.l.,.-.2.1.1..|..... ....../.m...........U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.......P.P.....,..

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001EL (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11267034534910954
Encrypted:	false
SSDEEP:	12:OVXm/Ey6q999551mK2P3qQ10nMCldimE8eawHza1mKhX:O4l68n1iPLyMCldzE9BHza1R
MD5:	3DE57E9FAC960F1E165B5DBB6E753B3C
SHA1:	A3E4EDE7BF342690C36C8F9DDA04C005CABB990A
SHA-256:	AF8DDE8B05FC7E4511CF58545BB9DCA4275847A0A25C154D18D826DBE79AA65F
SHA-512:	076CE6FFD88142CFC6C30455F9E3329A44C40C07511A1416EF54ACB6F4D370A0EEFF8196592CFCD5617A7F226501482117FEE7BE771B3BF5D30A8895EC132426
Malicious:	false
Preview:	....,..........................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2..@.t.z.r.e.s...d.l.l.,.-.2.1.1..|..... .....m..m...........U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.......P.P.....,...S..

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.165699623106661
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zx+W:j+s+v+b+P+m+0+Q+q+i+W
MD5:	601D8BC3D547A5DEF8E8E76CCFE073BA
SHA1:	6E0401D998F2E8BDAC169DA4FECD04040353A0D2
SHA-256:	F98FD86D79F4446C813B9BD6A17A242577E1060E32BB8D5C1E47BB47667DE03A
SHA-512:	D5AC8967912DA1EFB26ED4F8E7EF499BDD53F8F2F1BAA535B9CF4B6B24EBC89D6B31EA7837DEB2C29AEDC67BB5A8B861BA006D6710DDE766AEAE4E1EA9DF1CCD
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.428775723092986

General

TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	cRC6TZG6Wx.dll
File size:	425984
MD5:	8f6552b136a4dd8719c898f90df1ba44
SHA1:	fea5b1d5e44dc58be42e472254e9b62b5caec532
SHA256:	03995882170eb6ebacaa47f77fc0c2e8fd78e17ab5427fbe3c70b2f91f46e44d
SHA512:	6aafb9415c8073e3a71c045543813d8d558c10ef5ee15c26dc175b7ef036873fbd2a3aa41e82c25e574cd8c5274320a812ea1e57eda8e8e42339504d221c4c5d
SSDEEP:	6144:1ACzUEcRRKxe0DUAldEzpLWE0sepO8+wM:1lxemHQtWE0sLvd
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....A.a.....!....T...P.....H....@.....S..P..

File Icon

Icon Hash:	64da98ecd2ceead4

Static PE Info

General

Entrypoint:	0x1001cab0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619E410C [Wed Nov 24 13:41:32 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ef559179cbfc08fc57c1e24c241992ea

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.flat	0x1000	0x446	0x600	False	0.643229166667	data	5.67523607022	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text	0x2000	0x252cb	0x25400	False	0.536086933725	data	5.88986915783	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x28000	0x1d9da	0x1da00	False	0.494923523207	data	5.10028459369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x46000	0x1aab0	0x17e00	False	0.51547161322	data	4.96846164351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x61000	0xb7b8	0xb800	False	0.177564538043	data	3.89759299523	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6d000	0x10f0	0x1200	False	0.782335069444	data	6.41113333729	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-16:50:34.878985	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49744	443	192.168.2.3	51.178.61.60
11/24/21-16:50:36.087592	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49745	80	192.168.2.3	168.197.250.14
11/24/21-16:50:37.891481	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49746	8080	192.168.2.3	45.79.33.48
11/24/21-16:50:58.967060	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49749	8080	192.168.2.3	196.44.98.190
11/24/21-16:51:20.009169	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49753	7080	192.168.2.3	177.72.80.14
11/24/21-16:51:20.547585	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	7080	49753	177.72.80.14	192.168.2.3

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 51.178.61.60

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49744	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 15:50:35 UTC	0	OUT	GET /cOCoCBOnwtlaPwqgYJsibWlqGyXElLKsrFlsKtesNMVjGBKbplkpiwohTqB HTTP/1.1 Cookie: CkaS=ZjwItdmT1ECYLtgJezxI3JoumM8yxrkDUD9XymD7kyc8EbFQVqQJDR+HcOYSYNuqm3GMHu9tyWocT2ebwQjCT6CFKOh4yFKGfmNQGEMjfJcGVJjfSjxi61uxl8IdZPCLFGO75XaQUz9hc2k46HlLfbLprvARhND47YDAUKst2lWTLUjdHo81K4H5Zdm6jP/AHUWKX74rhhb7vRaxi+yY5yVTZPMAbash8y0fiFtequ8CyFQdGqZu5JTKVCv/0hHilAyjkgSllkQi Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-24 15:50:35 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 24 Nov 2021 15:50:35 GMT Content-Type: text/html Content-Length: 162 Connection: close
2021-11-24 15:50:35 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: 7156 Parent PID: 572

General

Start time:	16:50:21
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: loaddll32.exe PID: 1464 Parent PID: 4808

General

Start time:	16:50:22

Start date:	24/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll"
Imagebase:	0xc50000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: SgrmBroker.exe PID: 6456 Parent PID: 572

General

Start time:	16:50:22
Start date:	24/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff689410000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6412 Parent PID: 1464

General

Start time:	16:50:22
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6444 Parent PID: 572

General

Start time:	16:50:22
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5528 Parent PID: 572

General

Start time:	16:50:23
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6384 Parent PID: 1464

General

Start time:	16:50:23
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\cRC6TZG6Wx.dll,Control_RunDLL
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4516 Parent PID: 6412

General

Start time:	16:50:23
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",#1

Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.289238760.0000000000D86000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5776 Parent PID: 6384

General

Start time:	16:50:23
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\cRC6TZG6Wx.dll,Control_RunDLL
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.293376232.00000000009BF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000003.289024016.00000000009C7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 5000 Parent PID: 4516

General

Start time:	16:50:24
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\cRC6TZG6Wx.dll",Control_RunDLL
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.290674131.0000000000576000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000003.289903082.0000000000576000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000003.289844390.0000000000576000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6620 Parent PID: 5776

General

Start time:	16:50:25
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zrrbzia\fotuyl.lzj",HSFp
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.296343256.00000000031D6000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 4720 Parent PID: 6620

General

Start time:	16:50:27
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Zrrbzia\fotuyl.lzj",Control_RunDLL
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000003.360457905.0000000003396000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.809828703.0000000003396000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000003.413105360.0000000003396000.00000004.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5336 Parent PID: 572

General

Start time:	16:50:31
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1952 Parent PID: 572

General

Start time:	16:50:47
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 2464 Parent PID: 572

General

Start time:	16:51:05
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 2528 Parent PID: 5528

General

Start time:	16:51:23
Start date:	24/11/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff757660000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 2148 Parent PID: 2528

General

Start time:	16:51:24
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6284 Parent PID: 572

General

Start time:	16:51:29
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Disassembly

Code Analysis