ID: 528005
Sample Name: pYebrdRKvR
Cookbook: default.jbs
Time: 16:54:23
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

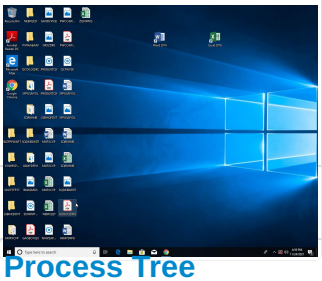
Windows Analysis Report pYebrdRKvR

Overview

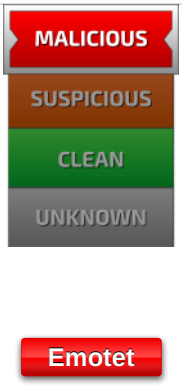
General Information

Sample Name:	pYebrdRKvR (renamed file extension from none to dll)
Analysis ID:	528005
MD5:	3102132775b47d..
SHA1:	8d54c54e8eff10b..
SHA256:	5c4d9d71040604..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

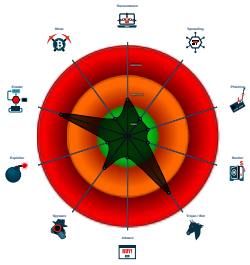


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- 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…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5848 cmdline: loaddll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4828 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4624 cmdline: rundll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5808 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5116 cmdline: rundll32.exe C:\Users\user\Desktop\pYebrdRKvR.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4692 cmdline: rundll32.exe C:\Users\user\Desktop\pYebrdRKvR.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4248 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Olcnhkjrspgysi\kpevmak.bsr",xeRCFILGA MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 4316 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Olcnhkjrspgysi\kpevmak.bsr",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 3216 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5196 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6988 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6644 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6768 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS 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
00000005.00000003.360524597.0000000000A76000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000003.361688769.0000000000A46000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.367502574.0000000003696000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.882777684.0000000000D12000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.364197169.0000000000A3A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.a46e78.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.d16c20.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.a76c68.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.3.rundll32.exe.a76c68.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.a76c68.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 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)

Stealing of Sensitive Information:

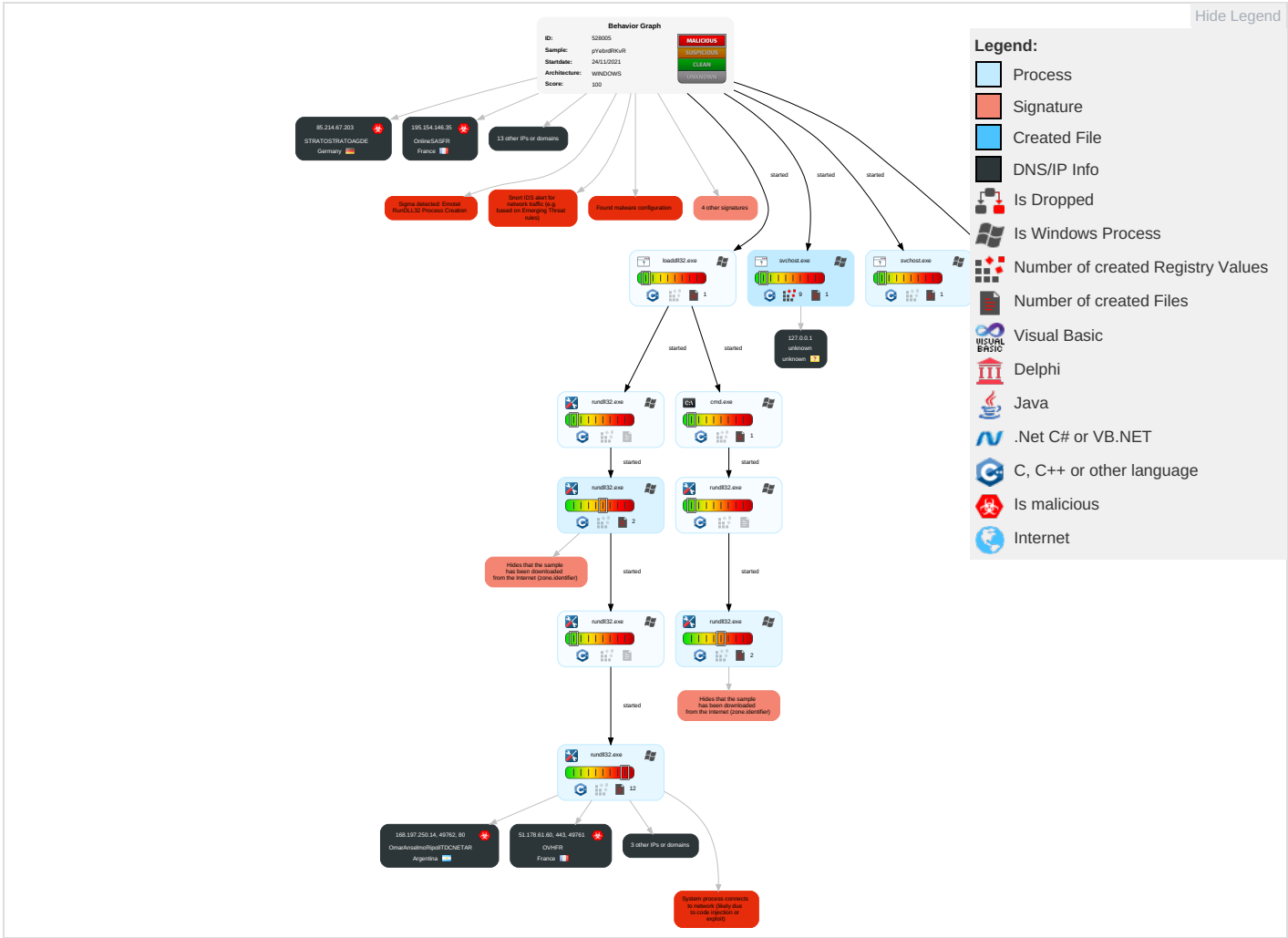
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdr Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Car Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

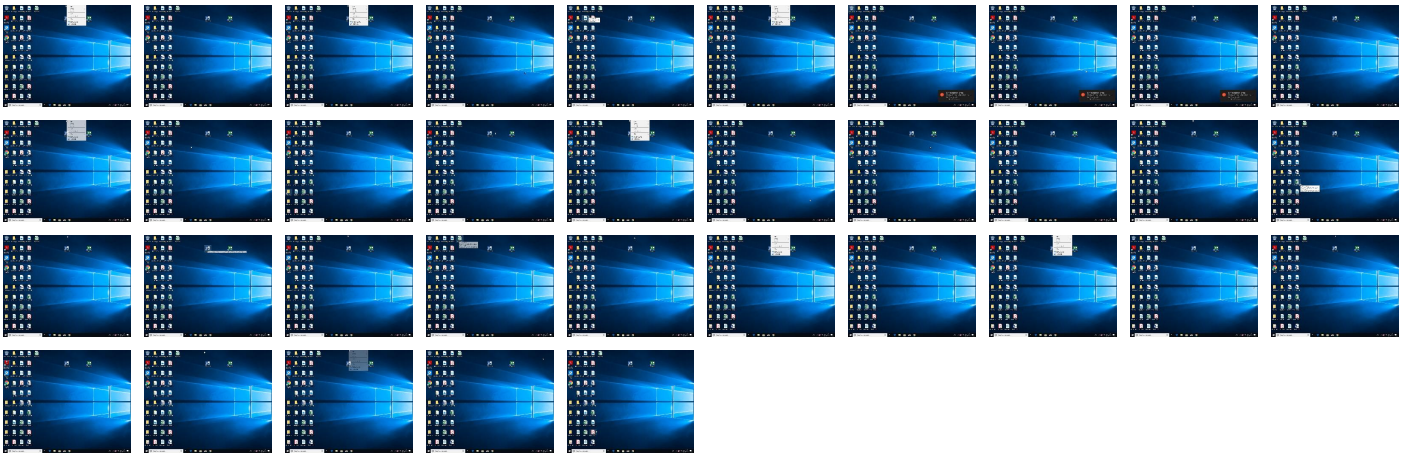
Behavior Graph



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
pYebrdRKvR.dll	18%	Virustotal		Browse
pYebrdRKvR.dll	18%	ReversingLabs	Win32.Trojan.Mansabo	
pYebrdRKvR.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.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/wxXNBTtFVptEPyBMyhxzytUrLNSymmMWHdjZgweBcTxtKLUZGczVLXNxnireROs	0%	Avira URL Cloud	safe	
http://https://177.72.80.14/akR=	0%	Avira URL Cloud	safe	
http://https://168.197.250.14:80/qeEsRQYaDgRwXDJjRsnTiXgQ~Y	0%	Avira URL Cloud	safe	
http://https://177.72.80.14:7080/VoY	0%	Avira URL Cloud	safe	
http://https://168.197.250.14:80/qeEsRQYaDgRwXDJjRsnTiXgQlY	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://196.44.98.190/	0%	Avira URL Cloud	safe	
http://https://196.44.98.190/)k	0%	Avira URL Cloud	safe	
http://https://177.72.80.14/	0%	Avira URL Cloud	safe	
http://https://196.44.98.190:8080/cRBQvElvVswAKMbGJRCeWFEoAKWVURRoDepPZnuTejOhPOKJ	0%	Avira URL Cloud	safe	
http://https://177.72.80.14:7080/kp	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/wxXNBTtFVptEPyBMyhxzytUrLNSymmMWHdjZgweBcTxtKLUZGczVLXNxnireROs5	0%	Avira URL Cloud	safe	
http://https://177.72.80.14:7080/k	0%	Avira URL Cloud	safe	
http://https://168.197.250.14/lhQ	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://196.44.98.190:8080/	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/	0%	Avira URL Cloud	safe	
http://https://177.72.80.14:7080/	0%	Avira URL Cloud	safe	
http://https://168.197.250.14/khX	0%	Avira URL Cloud	safe	
http://https://45.79.33.48/	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/rLNSymmMWHdjZgweBcTxtKLUZGczVLXNxnireROs	0%	Avira URL Cloud	safe	
http://https://45.79.33.48:8080/GEGDSODavaAMfbQXuktdlcgqQGPldhWooFcQtRsikthZVdhkisiiQD	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://177.72.80.14:7080/kst	0%	Avira URL Cloud	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://168.197.250.14:80/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://51.178.61.60/wxXNBTtFVptEPyBMyhxzytUrLNSymmMWHdjZgweBcTxtKLUZGczVLXNxnireROs	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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528005
Start date:	24.11.2021
Start time:	16:54:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pYebrdRKvR (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:	25
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@20/7@0/21
EGA Information:	Failed
HDC Information:	• Successful, ratio: 75.2% (good quality ratio 65.7%) • Quality average: 69% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 91% • 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
16:56:28	API Interceptor	10x 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	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	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	
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
196.44.98.190	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 78.47.204.80
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 78.47.204.80
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 78.47.204.80
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 78.47.204.80
	copy_tt_inv_10192ne.exe	Get hash	malicious	Browse	• 49.12.42.56
	FACTURAS.exe	Get hash	malicious	Browse	• 116.202.203.61
	wE3YzRd1IZ.exe	Get hash	malicious	Browse	• 135.181.163.109
	wCkjCMnGrO	Get hash	malicious	Browse	• 116.203.73.1
	79GRrdea5l.exe	Get hash	malicious	Browse	• 159.69.123.221
	MtCsSK9TK2.exe	Get hash	malicious	Browse	• 95.216.4.252
	0331C7BCA665F36513377FC301CBB32822FF35F925115.exe	Get hash	malicious	Browse	• 5.9.164.117
	C54CA1DF46D817348C9BDF18F857459D7CA05C51F7F30.exe	Get hash	malicious	Browse	• 135.181.129.119
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 5.9.162.45
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 5.9.162.45
	0K31jgS20G.exe	Get hash	malicious	Browse	• 5.9.162.45
	vAsfZhw32P.exe	Get hash	malicious	Browse	• 5.9.162.45
	YwZpT3p5Rh.msi	Get hash	malicious	Browse	• 88.99.32.114
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
	ugeLMlEROB.exe	Get hash	malicious	Browse	• 116.202.14.219
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
AS-CHOOPAUS	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 66.42.57.149
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 66.42.57.149
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 66.42.57.149
	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
EcobandGH	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 196.44.98.190
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 196.44.98.190
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 196.44.98.190
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 196.44.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	FlyE6huzxV.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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 51.178.61.60
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 51.178.61.60
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 51.178.61.60
	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
	2SR3psYDHQ.js	Get hash	malicious	Browse	• 51.178.61.60
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24937883611665626
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4p:BJiRdwfu2SRU4p
MD5:	702AF954D4EF11D4F5DB2EC68C91FBF6
SHA1:	2ED89AB1CBFD678062621AA2F6FF402BEC03D4C0
SHA-256:	CADD95EABFFB496A4927D6CC935FCE02A8A07301FF5AD1C4768D76949BF17683
SHA-512:	74426B31F46AEA7DD12A96EB7D1493A0B47E0E8407FE0C251B52C656BA542C6AAA600057F07435D09EE782D29A5F9AE68D83079EAF068DC1B3613730C8942A8
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x7ccc75ac, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505134410665448
Encrypted:	false
SSDEEP:	384:WHz+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:WHASB2nSB2RSjlK/+mLesOj1J2
MD5:	497DB6EBFC8FEA018C2466F4A6A36093
SHA1:	E7025D6C75282AEE05DDADB886909EDA0E67B210
SHA-256:	F8DAC24AEBFD44E801361824A75A356693F274685DCA869988A68DA81AF436DE
SHA-512:	05114F24518D625FCCFF4083916285594E25278B5C1520BDE24CD915263D5475872A4AEF0FCC028C85170C52F79B4A95A57D9BFBF253FADDF5F1C2E3B5904CF
Malicious:	false
Preview:	|.u.... .....e.f.3...w.....).....3;...y..)8...yS.h.(.....3;...y....).....3...w.....B.....@..... ....3;...y.....3;...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07259979872370396
Encrypted:	false
SSDEEP:	3:k7vMdZjTL/llXB4+TP7+YtFQlUiL/llall3Vkttlmlnl:krMbXll+3x3ulA3
MD5:	484B9E7B5EFDA3148543BA647B248A44
SHA1:	4483A82D4AAE8DD9BB80267840AAB7948C88351D
SHA-256:	53D20C1034813E1559E4667B528C040364F2C1710B0DA651F60E31A2AD476238
SHA-512:	C5E89A454439D1AE967C7503B9FCD9174E4DC6284EC4FF9EC538A148FBBF16B82AB14620467A0C06D0338B105CF330DCBF9B7937A900C8FEA256F86A43896A8
Malicious:	false
Preview:	7.....3...w..)8...yS.3;...y.....3;...y..3;...y....U.3;...yoy.....3;...y..... ....

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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):	3.1122616792999316
Encrypted:	false
SSDEEP:	6:kKRzk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:5z9kPlE99SNxAhUeYlUSA/t
MD5:	C66736E92765D6954E0E4373830E0002
SHA1:	C0D3BBFE9F4262FDD513096F8B3ED26D05576F54
SHA-256:	4509EC8C66427F16B4C0E64999CD756E3361C37EE35D5B7E485057AF1079F15A
SHA-512:	9D3A1AF6990711BA20A90831BFDF0533D1DE72740764D916D74E1137FEFF1D26257E084F63465F9CA092610E735516E13FECFDCAEC3390F07B87B2C76877EDA7
Malicious:	false
Preview:	p..... .....N.D....(..... .....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:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.428778908504156
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:	pYebrdRKvR.dll
File size:	425984
MD5:	3102132775b47d2ff1c40a2b5293ba60

General

SHA1:	8d54c54e8eff10bf087236af120367620b61a622
SHA256:	5c4d9d71040604f2a6cd8fa3e69a3af1f79590348729cd0d90abbb8ea51a05a9
SHA512:	ca05549daa48c7de1c5cb1daf2eb041f5807bc0376fa6f79b94f65e93eaf3d00d53119689e9b22dce0eae6e3fc12f2b9cd58de29d827927f343bdcbb385b6d59
SSDEEP:	6144:1ACzUEcRRKxe0DUAldEzpL/E0sepO8+wM:1lxemHQt/E0sLvd
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	4.96852629791	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.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
11/24/21-16:55:38.215416	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49761	443	192.168.2.6	51.178.61.60
11/24/21-16:55:38.808048	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49762	80	192.168.2.6	168.197.250.14
11/24/21-16:55:40.651171	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49763	8080	192.168.2.6	45.79.33.48
11/24/21-16:56:02.741600	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49767	8080	192.168.2.6	196.44.98.190
11/24/21-16:56:23.809188	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49774	7080	192.168.2.6	177.72.80.14
11/24/21-16:56:24.351151	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	7080	49774	177.72.80.14	192.168.2.6

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	192.168.2.6	49761	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 15:55:38 UTC	0	OUT	GET /wxXNBTtFVptEPyBMyhxzytUrLNSymmMWHdjZgweBcTxtKLUZGczVLXNxnireROs HTTP/1.1 Cookie: JmIuwWBWPToZ=XDGTMkmFZ9hr0CeEgG7gEpD9hs4Omotho6+57napLIrRc+yLhr6jDd+kXDv4veMC3uDo4 8E0KYz8mat8uVA0WXuFnsw4hzFORPBn7MrucHVcn/hm73RFPQ0NYNqRr6rNpXumiYPSOimYLiR2Tu6sMdw82U3DBUu DHRe9h1WQb6f1GDhoy5QtZ0z4paXtdMAW8mO9u70ywe2JFmJ1lqhLDJPKOuQAbbEec0hu7deLYD9sE1A= Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-11-24 15:55:38 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 24 Nov 2021 15:55:38 GMT Content-Type: text/html Content-Length: 162 Connection: close
2021-11-24 15:55:38 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: loaddll32.exe PID: 5848 Parent PID: 5440

General

Start time:	16:55:25
Start date:	24/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll"
Imagebase:	0x3b0000
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: cmd.exe PID: 4828 Parent PID: 5848

General

Start time:	16:55:25
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\pYebrdRKvR.dll",#1
Imagebase:	0x2a0000
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: rundll32.exe PID: 5116 Parent PID: 5848

General

Start time:	16:55:26
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pYebrdRKvR.dll,Control_RunDLL
Imagebase:	0x1160000
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: 4624 Parent PID: 4828

General

Start time:	16:55:26
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\pYebrdRKvR.dll",#1
Imagebase:	0x1160000
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: 00000004.00000002.362028571.0000000003516000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4692 Parent PID: 5116

General

Start time:	16:55:26
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pYebrdRKvR.dll,Control_RunDLL
Imagebase:	0x1160000

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: 00000005.00000003.360524597.0000000000A76000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.364197169.0000000000A3A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 5808 Parent PID: 4624

General

Start time:	16:55:27
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\pYebrdRKvR.dll",Control_RunDLL
Imagebase:	0x1160000
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: 00000006.00000003.361688769.0000000000A46000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.362088501.0000000000A46000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4248 Parent PID: 4692

General

Start time:	16:55:28
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Olcnhkjrspgysi\kpevmak.bsr",xeRCFILGA
Imagebase:	0x1160000
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: 00000007.00000002.367502574.0000000003696000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4316 Parent PID: 4248

General

Start time:	16:55:30
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Olcnhkjrspgysi\kpevmak.bsr ",Control_RunDLL
Imagebase:	0x1160000
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: 00000008.00000002.882777684.0000000000D12000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000003.615469269.0000000000D12000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3216 Parent PID: 560

General

Start time:	16:55:30
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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: 5196 Parent PID: 560

General

Start time:	16:55:51
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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: 6988 Parent PID: 560

General

Start time:	16:56:07
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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: 6644 Parent PID: 560

General

Start time:	16:56:26
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:	0x7ff6b7590000
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: 6768 Parent PID: 560

General

Start time:	16:56:40
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
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

Registry Activities Show Windows behavior

Disassembly

Code Analysis