ID: 528351
Sample Name: tUJXpPwU27
Cookbook: default.jbs
Time: 05:11:12
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

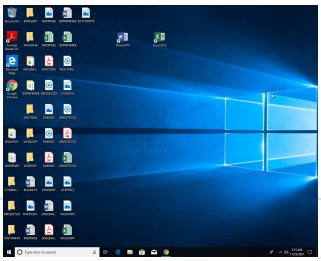
Windows Analysis Report tUJXpPwU27

Overview

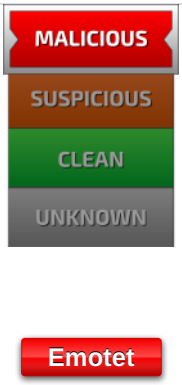
General Information

Sample Name:	tUJXpPwU27 (renamed file extension from none to dll)
Analysis ID:	528351
MD5:	15239e7be7ce6b..
SHA1:	55dc2a27f408bf6..
SHA256:	79036368e6229fa.
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

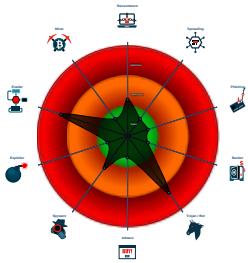


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Sigma detected: Emotet RunDLL32 …
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Deletes files inside the Windows fold…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6984 cmdline: loaddll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6996 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7016 cmdline: rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6044 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7004 cmdline: rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6696 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cilqlpbnkp\gwjznuxweg.czu",ligDrVSARhbsLaD MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5904 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cilqlpbnkp\gwjznuxweg.czu",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7068 cmdline: rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,aocchppr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4972 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7088 cmdline: rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,atibsyaucowikobny MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4664 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7128 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6336 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6424 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5252 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
00000000.00000002.1000235837.000000000099C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.977580541.0000000002CEA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.997848622.0000000002E95000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.997168710.00000000006AA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.1134773374.0000000000A6A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.a85f00.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.6c4390.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.8b4350.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.6c4390.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.8b4350.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 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

Networking:

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)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Stealing of Sensitive Information:

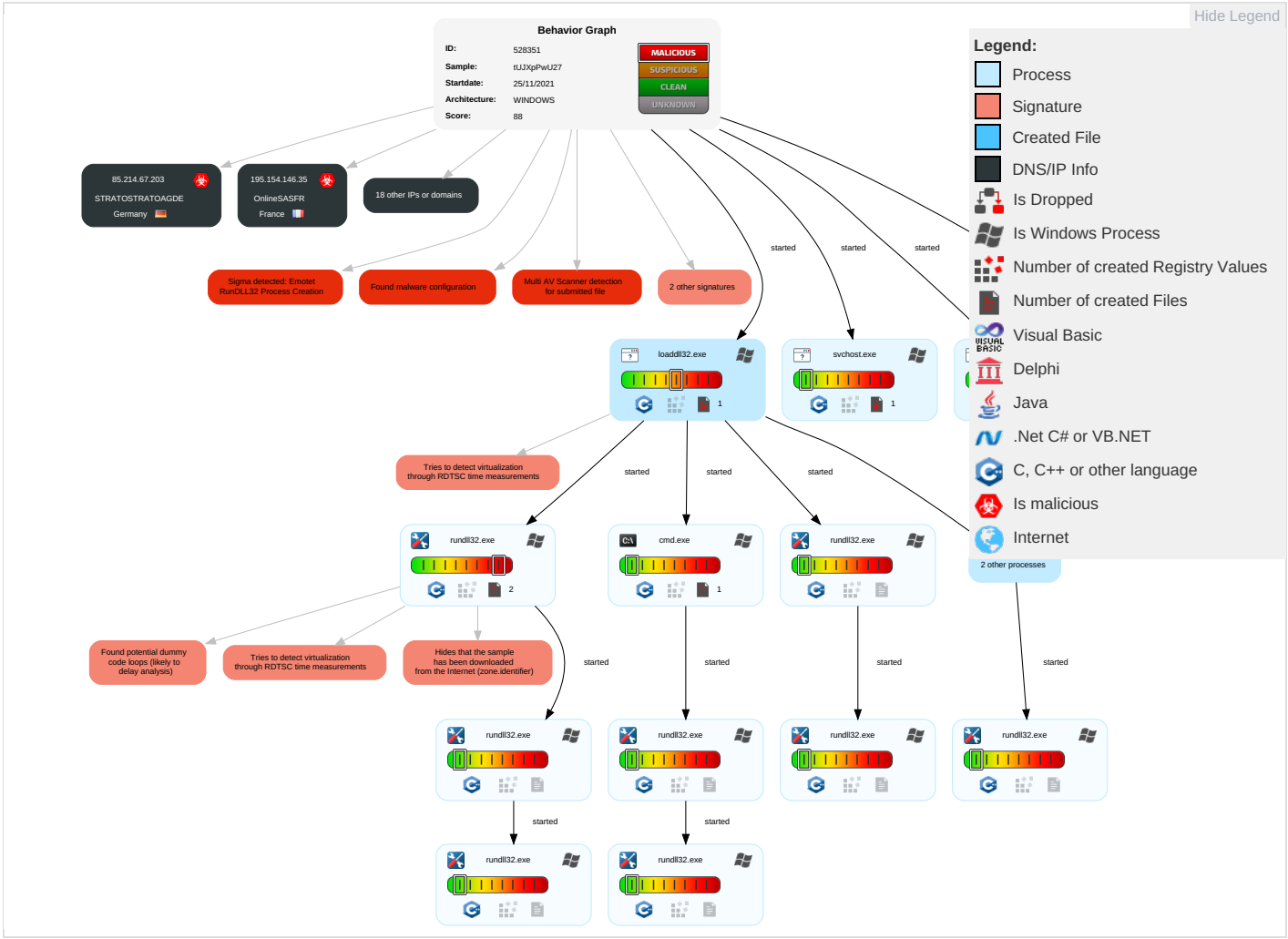
Yara detected Emotet

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	Application Shimming 1	Process Injection 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	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Security Software Discovery 2 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card 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	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

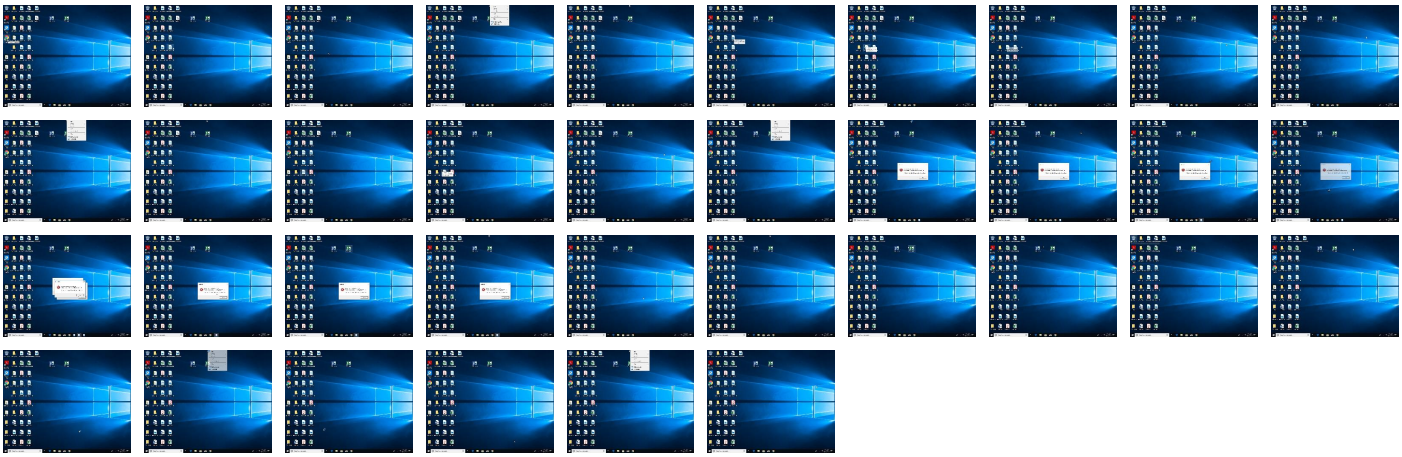
Behavior Graph



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
tUJXpPwU27.dll	42%	Virustotal		Browse
tUJXpPwU27.dll	49%	ReversingLabs	Win32.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.9e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.630000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.810000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.2c60000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.910000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.7b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

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:	528351

Start date:	25.11.2021
Start time:	05:11:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tUJXpPwU27 (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:	21
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:	mal88.troj.evad.winDLL@26/0@0/20
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14% (good quality ratio 12.5%) • Quality average: 67.9% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 69% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	pYebrdRKvR.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
196.44.98.190	pYebrdRKvR.dll	Get hash	malicious	Browse	
	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	
78.46.73.125	pYebrdRKvR.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 5.9.162.45
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 5.9.162.45
	exe.exe	Get hash	malicious	Browse	• 116.202.203.61
	J73PTzDghy.exe	Get hash	malicious	Browse	• 94.130.138.146
	piPvSLcFXV.exe	Get hash	malicious	Browse	• 88.99.210.172
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 116.202.14.219

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	.#U266bvmail-478314QOZVOYBY30.htm	Get hash	malicious	Browse	• 168.119.38.214
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 78.47.204.80
	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	• 135.181.16 3.109
	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
AS-CHOOPAUS	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 149.28.253.196
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1 272E3.exe	Get hash	malicious	Browse	• 149.28.253.196
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C 932E2.exe	Get hash	malicious	Browse	• 149.28.253.196
	asbestos_safety_and_eradication_agency_enterprise_ agreement 41573 .js	Get hash	malicious	Browse	• 45.76.154.237
	23062BA932165210EBB3FFCD15474E79F19E6AD7 4869F.exe	Get hash	malicious	Browse	• 149.28.253.196
	DA8063D9EB60622915D492542A6A8AE318BC87B4 C5F89.exe	Get hash	malicious	Browse	• 155.138.20 1.103
	asbestos_safety_and_eradication_agency_enterprise_ agreement 64081 .js	Get hash	malicious	Browse	• 45.76.154.237
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 66.42.57.149
	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
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E05 2F615.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
	44E401AAF0B52528AA033257C1A1B8A09A2B10ED F26ED.exe	Get hash	malicious	Browse	• 149.28.253.196
	77012C024869BA2639B54B959FAB1E10EBAAF8EB B9BFC.exe	Get hash	malicious	Browse	• 149.28.253.196
EcobandGH	pYebrdRKvR.dll	Get hash	malicious	Browse	• 196.44.98.190
	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
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.1578551978819025
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	tUJXpPwU27.dll
File size:	481792
MD5:	15239e7be7ce6bfaf0681eb66bcde356
SHA1:	55dc2a27f408bf6437224ecfc62cc01a3311ec08
SHA256:	79036368e6229fa1c4eb724a34e4d10973feaa85628058f4ac1eaac6c1fcf19c
SHA512:	366168368edc0dae19f071431deb1b5a8a9141179ebf8423e8053a00915dc69ec941273658a6c2a94f897f2fc053767774a310ccf4964d3e37d545ab1ad93fa
SSDEEP:	6144:m3M5xEQPjPLlMcp8gvSaX5EAoiAO0X1Ah8JOKXDebPG0+Z0C4OGUBbiA1:m3M5Bj5Mcp8QlwiaiYe6DZrzGyWA1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k...8...8...8...9...8...9...8...9...8...9...8...9...8...9...8...9...8...9...8...8]..8/..9...8/..9...8/..8...8..e8...8/..9...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10014ee6
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:	0x619C8049 [Tue Nov 23 05:46:49 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:	f81a3c8b673ca7b3a7f6c06eaa20660c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x389dc	0x38a00	False	0.532840956126	data	6.65955400705	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3a000	0x13970	0x13a00	False	0.462567177548	data	5.41826950668	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4e000	0x252c	0x1800	False	0.224446614583	data	3.84154709275	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x51000	0x24410	0x24600	False	0.810030068729	data	7.73179054959	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x76000	0x3324	0x3400	False	0.706280048077	data	6.57246100993	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6984 Parent PID: 5432

General

Start time:	05:11:59
Start date:	25/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll"
Imagebase:	0xdb0000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000002.1000235837.000000000099C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6996 Parent PID: 6984

General

Start time:	05:12:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",#1
Imagebase:	0x11d0000
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: 7004 Parent PID: 6984

General

Start time:	05:12:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,Control_RunDLL
Imagebase:	0xb70000
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: 00000002.00000002.997848622.0000000002E95000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7016 Parent PID: 6996

General

Start time:	05:12:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",#1
Imagebase:	0xb70000
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: 00000003.00000002.977580541.0000000002CEA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7068 Parent PID: 6984

General

Start time:	05:12:04
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,aocchppr
Imagebase:	0xb70000
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: 00000004.00000002.997168710.00000000006AA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7088 Parent PID: 6984

General

Start time:	05:12:09
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\tUJXpPwU27.dll,atibsyaucowikobny
Imagebase:	0xb70000
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: 00000005.00000002.998474628.000000000089A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6044 Parent PID: 7016

General

Start time:	05:14:32
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL
Imagebase:	0xb70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 6696 Parent PID: 7004

General

Start time:	05:14:34
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cilqlpbnkp\gwjznuxweg.czu",ligDrVSARhbsLaD
Imagebase:	0xb70000
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: 00000008.00000002.1134773374.0000000000A6A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4972 Parent PID: 7068

General

Start time:	05:14:39
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL
Imagebase:	0xb70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 4664 Parent PID: 7088

General

Start time:	05:14:42
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL
Imagebase:	0xb70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 7128 Parent PID: 6984

General

Start time:	05:14:43
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\tUJXpPwU27.dll",Control_RunDLL
Imagebase:	0xb70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 6336 Parent PID: 568

General

Start time:	05:15:05
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 6424 Parent PID: 568

General

Start time:	05:15:37
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: rundll32.exe PID: 5904 Parent PID: 6696

General

Start time:	05:15:46
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cilqlpbnkp\gwjznuxweg.czu" ,Control_RunDLL
Imagebase:	0xb70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5252 Parent PID: 568

General

Start time:	05:15:56
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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