ID: 532048
Sample Name: 2gyA5uNl6VPQUA.dll
Cookbook: default.jbs
Time: 17:28:01
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

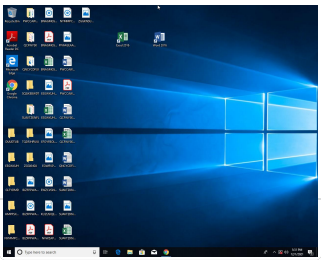
Windows Analysis Report 2gyA5uNl6VPQUA.dll

Overview

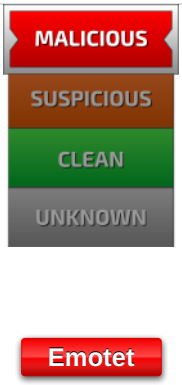
General Information

Sample Name:	2gyA5uNl6VPQUA.dll
Analysis ID:	532048
MD5:	5e20cb3466b66a..
SHA1:	28ef4facb366de1..
SHA256:	208939e34f46846.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



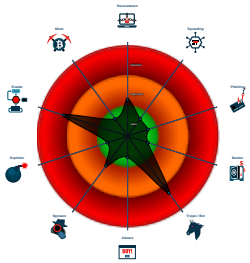
Emotet

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Changes security center settings (no…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fold…
- Checks if Antivirus/Antispyware/Fire…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- svchost.exe (PID: 5528 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- loaddll32.exe (PID: 5816 cmdline: loaddll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5988 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6804 cmdline: rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5704 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6816 cmdline: rundll32.exe C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4624 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cyyah\ysrainvzaakh.dkv",pczodXjTBX MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4424 cmdline: rundll32.exe C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6688 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1880 cmdline: rundll32.exe C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6680 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 3540 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6868 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6848 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6164 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6332 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 2364 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 3376 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 156 -p 5816 -ip 5816 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5796 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 508 -p 5816 -ip 5816 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "46.55.222.11:443",
    "104.245.52.73:8080",
    "41.76.108.46:8080",
    "103.8.26.103:8080",
    "185.184.25.237:8080",
    "103.8.26.102:8080",
    "203.114.109.124:443",
    "45.118.115.99:8080",
    "178.79.147.66:8080",
    "58.227.42.236:80",
    "45.118.135.203:7080",
    "103.75.201.2:443",
    "195.154.133.20:443",
    "45.142.114.231:8080",
    "212.237.5.209:443",
    "207.38.84.195:8080",
    "104.251.214.46:8080",
    "212.237.17.99:8080",
    "212.237.56.116:7080",
    "216.158.226.206:443",
    "110.232.117.186:8080",
    "158.69.222.101:443",
    "107.182.225.142:8080",
    "176.104.106.96:8080",
    "81.0.236.90:443",
    "50.116.54.215:443",
    "138.185.72.26:8080",
    "51.68.175.8:8080",
    "210.57.217.132:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.628861831.0000000002D7A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000000.662292442.00000000007C0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000000.601509063.000000000083D000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.602280537.000000000047A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.623586957.0000000002C30000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.843b70.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.0.loaddll32.exe.7c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.6a0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.0.loaddll32.exe.7c0000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2f20000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 25 entries				

Sigma Overview

No Sigma rule has matched

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

Hooking and other Techniques for Hiding and Protection:

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

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

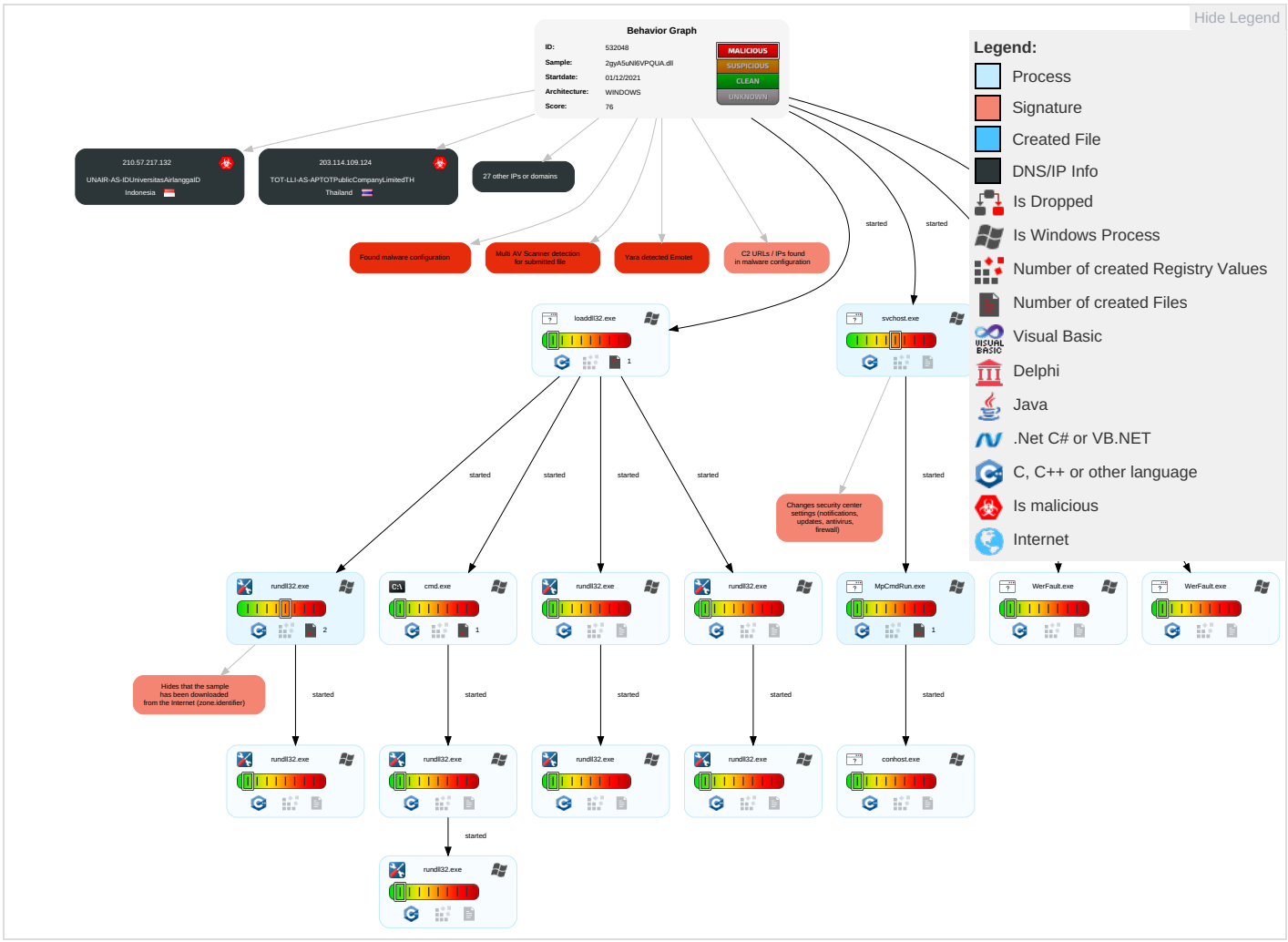
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Security Software Discovery 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
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	Rogue (Base St

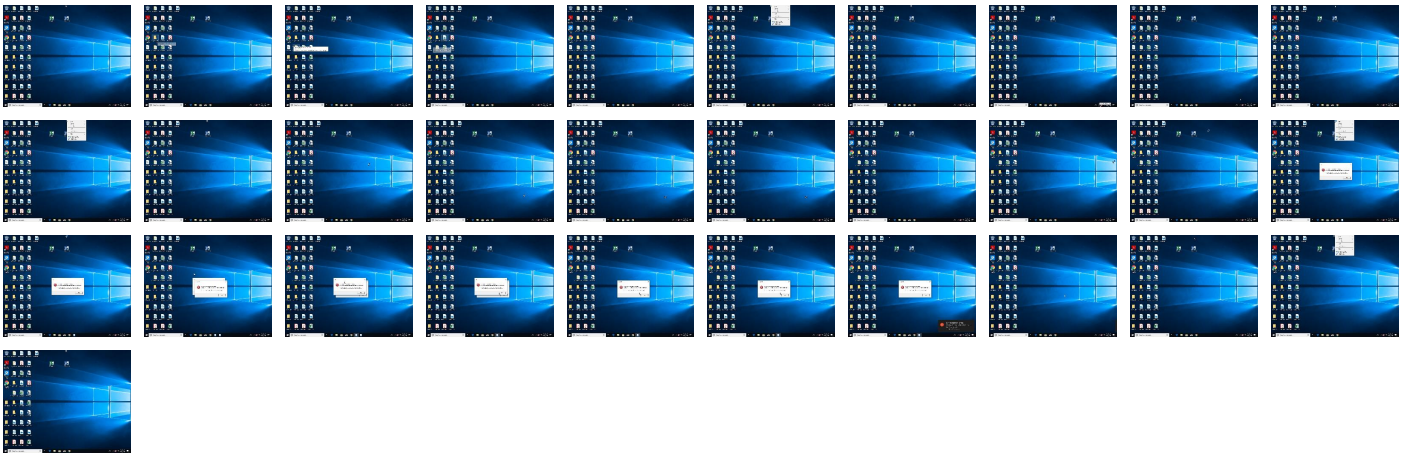
Behavior Graph



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
2gyA5uNl6VPQUA.dll	18%	Virustotal		Browse
2gyA5uNl6VPQUA.dll	26%	ReversingLabs	Win32.Trojan.Midie	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.6a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.7c0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.2f20000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.7c0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.2c30000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.30f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.2.loaddll32.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dynamic.t	0%	URL Reputation	safe	
http://www.bingmapsportal.comsv	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.154.133.20	unknown	France		12876	OnlineSASFR	true
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
104.245.52.73	unknown	United States		63251	METRO-WIRELESSUS	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
81.0.236.90	unknown	Czech Republic		15685	CASABLANCA-ASInternetCollocationProviderCZ	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikalD	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
51.68.175.8	unknown	France		16276	OVHFR	true
103.8.26.102	unknown	Malaysia		132241	SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
41.76.108.46	unknown	South Africa		327979	DIAMATRIXZA	true
103.8.26.103	unknown	Malaysia		132241	SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
212.237.5.209	unknown	Italy		31034	ARUBA-ASNIT	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
212.237.56.116	unknown	Italy		31034	ARUBA-ASNIT	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
210.57.217.132	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.184.25.237	unknown	Turkey		209711	MUVHOSTTR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
104.251.214.46	unknown	United States		54540	INCERO-HVVCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532048
Start date:	01.12.2021
Start time:	17:28:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2gyA5uNl6VPQUA.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	22
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:	mal76.troj.evad.winDLL@35/8@0/30
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.6% (good quality ratio 23.8%) • Quality average: 72.7% • Quality standard deviation: 24.2%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:30:29	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	9sQccNfqAR.dll	Get hash	malicious	Browse	
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	
	U4pi8WRxNJ.dll	Get hash	malicious	Browse	
	oERkAQeB4d.dll	Get hash	malicious	Browse	
	FC9fpZrma1.dll	Get hash	malicious	Browse	
	Z4HpRSQD6I.dll	Get hash	malicious	Browse	
	uLCt7sc5se.dll	Get hash	malicious	Browse	
	rGF1Xgw9Il.dll	Get hash	malicious	Browse	
	nBtjFS1D08.dll	Get hash	malicious	Browse	
	q8HPR8Yypk.dll	Get hash	malicious	Browse	
	mZuFa05xCp.dll	Get hash	malicious	Browse	
	TEm3oBxeXS.dll	Get hash	malicious	Browse	
	ma9Kq24IDH.dll	Get hash	malicious	Browse	
	U8GZ7uVALA.dll	Get hash	malicious	Browse	
	nq136LQEds.dll	Get hash	malicious	Browse	
212.237.17.99	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	
	U4pi8WRxNJ.dll	Get hash	malicious	Browse	
	oERkAQeB4d.dll	Get hash	malicious	Browse	
	FC9fpZrma1.dll	Get hash	malicious	Browse	
	Z4HpRSQD6I.dll	Get hash	malicious	Browse	
	uLCt7sc5se.dll	Get hash	malicious	Browse	
	rGF1Xgw9Il.dll	Get hash	malicious	Browse	
	nBtjFS1D08.dll	Get hash	malicious	Browse	
	q8HPR8Yypk.dll	Get hash	malicious	Browse	
	mZuFa05xCp.dll	Get hash	malicious	Browse	
	TEm3oBxeXS.dll	Get hash	malicious	Browse	
	ma9Kq24IDH.dll	Get hash	malicious	Browse	
	U8GZ7uVALA.dll	Get hash	malicious	Browse	
	nq136LQEds.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 212.237.56.116
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 212.237.56.116
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	• 212.237.56.116
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 212.237.56.116
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 212.237.56.116
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 212.237.56.116
	QUOTATION FORM.exe	Get hash	malicious	Browse	• 62.149.128.45
	MA4UA3e5xe	Get hash	malicious	Browse	• 46.37.10.252
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	• 212.237.56.116
	seL794VuEm	Get hash	malicious	Browse	• 31.14.139.79
	b6GJG5t0kg	Get hash	malicious	Browse	• 31.14.139.51
	U4pi8WRxNJ.dll	Get hash	malicious	Browse	• 212.237.56.116
	oERkAQeB4d.dll	Get hash	malicious	Browse	• 212.237.56.116
	FC9fpZrma1.dll	Get hash	malicious	Browse	• 212.237.56.116
	Z4HpRSQD6I.dll	Get hash	malicious	Browse	• 212.237.56.116
	uLCt7sc5se.dll	Get hash	malicious	Browse	• 212.237.56.116
	rGF1Xgw9Il.dll	Get hash	malicious	Browse	• 212.237.56.116
	nBtjFS1D08.dll	Get hash	malicious	Browse	• 212.237.56.116
	q8HPR8Yypk.dll	Get hash	malicious	Browse	• 212.237.56.116
	mZuFa05xCp.dll	Get hash	malicious	Browse	• 212.237.56.116
OnlineSASFR	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 195.154.133.20
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 195.154.146.35
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 195.154.146.35
	AtlanticareINV25-67431254.htm	Get hash	malicious	Browse	• 51.15.17.195
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 195.154.133.20
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	• 195.154.133.20
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 195.154.133.20
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 195.154.133.20
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 195.154.133.20
	67MPsax8fd.exe	Get hash	malicious	Browse	• 163.172.208.8
	Linux_x86	Get hash	malicious	Browse	• 212.83.174.79
	184285013-044310-Factura pendiente (2).exe	Get hash	malicious	Browse	• 212.83.130.20
	MTjXit7IJn	Get hash	malicious	Browse	• 51.158.219.54
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	• 195.154.133.20
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 195.154.146.35
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 195.154.146.35
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 195.154.146.35
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 195.154.146.35
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 195.154.146.35
	X2XCewI2Yy.dll	Get hash	malicious	Browse	• 195.154.146.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	0.11007315410389254
Encrypted:	false
SSDEEP:	12:261PjXm/Ey6q9995GNq3qQ10nMCldimE8eawHjcScrf:261Cl68sgLyMCldzE9BHjcd
MD5:	F509464584BDE228AC6200E4AAF46791
SHA1:	910529F0944A946D8A04101F68A7974FFC21AA2C

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
SHA-256:	1EF2E59D09B4C131FA935931AEDF926EABA1A22C4BE340B643697D690FB22982
SHA-512:	2BC237F4E2FDB86A44478B6D9311150E7685E60BEA2620743E8E6C4A004ED20B38544D1676354EC7280B77BB20F69B66DD31F2EB2B7DFC4C3F93BA45BF7F620
Malicious:	false
Preview:	.....6R7.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....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.....i>R7..... ....

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):	0.1127203686131934
Encrypted:	false
SSDEEP:	12:80jXm/Ey6q9995c1miM3qQ10nMCldimE8eawHza1miINtCP:8xl68K1tMLyMCldzE9BHza1tIri
MD5:	3E1816AC72E02624CA0A277C24E5AFCD
SHA1:	0BC7E702D5E870AE4365D3BFAD3F28B107F0F1AE
SHA-256:	C8CF94490DF4D5F9310AAFFF0D788A63DD6FD1E56A8EF5990057A8041FB283AD
SHA-512:	91AD8BC73D1B764707229A5FFF5CECABBBB915632CF65402E68147F58ADECEADEB030B10407419A8875AB7039AED56F395F5923739F5CC7B00979C265CD0E6E 9
Malicious:	false
Preview:	.....6Q7.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....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.....D>Q7..... ....

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):	0.11264702181093222
Encrypted:	false
SSDEEP:	12:8YjXm/Ey6q9995c1mK2P3qQ10nMCldimE8eawHza1mK0ssP:8Nl68K1iPLyMCldzE9BHza18
MD5:	0BD3A781A3DED6D0FDFBD5E332077DDE
SHA1:	0D810BF920322816C05D5C666A777928490EC26B
SHA-256:	CA36BDFD0B937952C0839CC0EB8D030628EFA7D59F5E48C731B9B0B20D5923F6
SHA-512:	0B76F7304E044501254180F259C23B5E9F410150F6468574029D757FB2E845F1E98C8FA25D3B991CD4276718BDC010BA1AB60FB6603DC1FA051B048DB90F3D94
Malicious:	false
Preview:	.....>wP7.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....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.....P7..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001YS (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11007315410389254
Encrypted:	false
SSDEEP:	12:261PjXm/Ey6q9995GNq3qQ10nMCldimE8eawHjcScrf:261Cl68sgLyMCldzE9BHjcd
MD5:	F509464584BDE228AC6200E4AAF46791
SHA1:	910529F0944A946D8A04101F68A7974FFC21AA2C
SHA-256:	1EF2E59D09B4C131FA935931AEDF926EABA1A22C4BE340B643697D690FB22982
SHA-512:	2BC237F4E2FDB86A44478B6D9311150E7685E60BEA2620743E8E6C4A004ED20B38544D1676354EC7280B77BB20F69B66DD31F2EB2B7DFC4C3F93BA45BF7F620
Malicious:	false
Preview:	.....6R7.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....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.....i>R7..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1127203686131934
Encrypted:	false
SSDEEP:	12:80jXm/Ey6q9995c1miM3qQ10nMCldimE8eawHza1miINtCP:8xl68K1tMLyMCldzE9BHza1tIri
MD5:	3E1816AC72E02624CA0A277C24E5AFCD
SHA1:	0BC7E702D5E870AE4365D3BFAD3F28B107F0F1AE
SHA-256:	C8CF94490DF4D5F9310AAFFF0D788A63DD6FD1E56A8EF5990057A8041FB283AD
SHA-512:	91AD8BC73D1B764707229A5FFF5CECABBBB915632CF65402E68147F58ADECEADEB030B10407419A8875AB7039AED56F395F5923739F5CC7B00979C265CD0E6E 9
Malicious:	false
Preview:	....6Q7.....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.. ....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.........D>Q7.. ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11264702181093222
Encrypted:	false
SSDEEP:	12:8YjXm/Ey6q9995c1mK2P3qQ10nMCldimE8eawHza1mK0ssP:8Nl68K1iPLyMCldzE9BHza18
MD5:	0BD3A781A3DED6D0FDFBD5E332077DDE
SHA1:	0D810BF920322816C05D5C666A777928490EC26B
SHA-256:	CA36BDFD0B937952C0839CC0EB8D030628EFA7D59F5E48C731B9B0B20D5923F6
SHA-512:	0B76F7304E044501254180F259C23B5E9F410150F6468574029D757FB2E845F1E98C8FA25D3B991CD4276718BDC010BA1AB60FB6603DC1FA051B048DB90F3D94
Malicious:	false
Preview:	....>wP7.....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.. ....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...........P7.. ....

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):	3.1617821983611605
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zk+R:j+s+v+b+P+m+0+Q+q+T+R
MD5:	1F848228A9E566D1A67D38C8FE9B378F
SHA1:	E75E77DD3FFD300A3379CF5EADEA0262D9E49DDD
SHA-256:	A9A59EC953B5242D3AC70E1336D94242065298DA0DB24DDF043F866FE0D12DAE
SHA-512:	D0DAA3E313E3C56C1F349B68859881E2BA15DBCA942BEE8CF919C2C02714128CF20689EF5A31045CC0AC5FF1E1603A419EED16BFC5912750B7A046C91BCA33 B
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.....- .-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_012855_088.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7907703522626073
Encrypted:	false
SSDEEP:	96:4CAMbAwo+lE5uI9c2YkUCp0I2lShhk/S4ZAT2BYFzOUMC0rJReC8l5hbMCWl5IbZ:Lxe7/p2wvn2COkaCiC1CYC9MCo

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_012855_088.etl	
MD5:	5621673E95B1159150EC48C66E1CE423
SHA1:	D345CDE13248322172A7B2D4C5A3E79E25C801A3
SHA-256:	A1F0EA666036D07976C3C831D6B406CBCE55E944C2C04A13ABB11A75FE1BFC7C
SHA-512:	81471CDDFFC812FFA0EFB6F96ADF1433865B50E522D8771F0FB837998AF00A1AC2F0356E83FCD3F3C29DF30A6457D5EBF9F91471A6B3CC99B33A616947963913
Malicious:	false
Preview:	....!.....s.....B.....Zb.. ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....D2.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.1.1.2.0.2._.0.1.2.8.5.5._.0.8.8...e.t.l.....P.P.....s..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.970960867517191
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:	2gyA5uNl6VPQUA.dll
File size:	387072
MD5:	5e20cb3466b66a9cdeac1ac74d9862e4
SHA1:	28ef4facb366de1fc7da62b975c8967997527c36
SHA256:	208939e34f46846c7c95383c6fea7813038b4dea87ea3819c157ccfbbf8aa09a
SHA512:	594039a003ac0c22a0a91c219c5cf50520994ead32f02efcfd8d79e57313c8ae041376fd0c3dcdfadf0472bee87363b28242a1d677e29cecb69127411fc6e722
SSDEEP:	6144:zBYrPMTsY8GR3j4fubnY6Zs/Bv6yM6aSTsfA2qL6jpXNcc6CEteuQJPlgtlpZ5L:yhmT4GbnYks/BJNWo2LjpScDEteuOloZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...Q...Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q..E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001cac1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A73B52 [Wed Dec 1 09:07:30 2021 UTC]
TLS Callbacks:	0x1000c340
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6

General

Subsystem Version Minor:	0
Import Hash:	609402ef170a35cc0e660d7d95ac10ce

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x28bb4	0x28c00	False	0.53924822661	data	6.1540438823	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2a000	0x32362	0x32400	False	0.817805503731	data	7.40645381596	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5d000	0x1ba4	0x1200	False	0.287109375	data	2.60484752417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x5f000	0x4c4	0x600	False	0.360677083333	AmigaOS bitmap font	2.17228109861	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x60000	0x1bc0	0x1c00	False	0.7880859375	data	6.62631718459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

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

General

Start time:	17:28:54
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
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: loaddll32.exe PID: 5816 Parent PID: 3428

General

Start time:	17:28:55
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll"
Imagebase:	0xcf0000
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: 00000001.00000000.662292442.00000000007C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.601509063.000000000083D000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.718738083.00000000007C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.611809755.00000000007C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.611849506.000000000083D000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.719186470.000000000083D000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.670664388.000000000083D000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.601464399.00000000007C0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3540 Parent PID: 572

General

Start time:	17:28:55
Start date:	01/12/2021
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: cmd.exe PID: 5988 Parent PID: 5816

General

Start time:	17:28:55
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.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: rundll32.exe PID: 6816 Parent PID: 5816

General

Start time:	17:28:55
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll,Control_RunDLL
Imagebase:	0x8a0000
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: 00000004.00000003.564390758.0000000003019000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.619081801.0000000002F20000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6804 Parent PID: 5988

General

Start time:	17:28:55
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",#1
Imagebase:	0x8a0000
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: 00000005.00000002.602689535.00000000030F0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.610271162.00000000032A3000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 6868 Parent PID: 572

General

Start time:	17:28:55
Start date:	01/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7e4d60000
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: svchost.exe PID: 6848 Parent PID: 572

General

Start time:	17:28:56
Start date:	01/12/2021
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: rundll32.exe PID: 4424 Parent PID: 5816

General

Start time:	17:29:00
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2gyA5uNI6VPQUA.dll,axamexdrqyrgb
Imagebase:	0x8a0000
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: 00000008.00000002.628861831.0000000002D7A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.623586957.0000000002C30000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1880 Parent PID: 5816

General

Start time:	17:29:07
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2gyA5uNI6VPQUA.dll,bhramccfbdd
Imagebase:	0x8a0000
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: 00000009.00000002.602280537.000000000047A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.602326812.00000000006A0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6164 Parent PID: 572

General

Start time:	17:29:09
Start date:	01/12/2021
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

Registry Activities

Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 6332 Parent PID: 6164

General

Start time:	17:30:23
Start date:	01/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7702f0000
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: 5752 Parent PID: 6332

General

Start time:	17:30:26
Start date:	01/12/2021
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: rundll32.exe PID: 5704 Parent PID: 6804

General

Start time:	17:31:00
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4624 Parent PID: 6816

General

Start time:	17:31:11
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cyyah\ysrainvzaakh.dkv",pczodXjTBX
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6688 Parent PID: 4424

General

Start time:	17:31:16
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 6680 Parent PID: 1880

General

Start time:	17:31:20
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\2gyA5uNl6VPQUA.dll",Control_RunDLL
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 2364 Parent PID: 572

General

Start time:	17:31:20
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes

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

Analysis Process: WerFault.exe PID: 3376 Parent PID: 2364

General

Start time:	17:31:21
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 156 -p 5816 -ip 5816
Imagebase:	0x270000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5796 Parent PID: 2364

General

Start time:	17:31:33
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 508 -p 5816 -ip 5816
Imagebase:	0x270000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis