ID: 532429
Sample Name: UioA2E9DBG
Cookbook: default.jbs
Time: 09:19:08
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

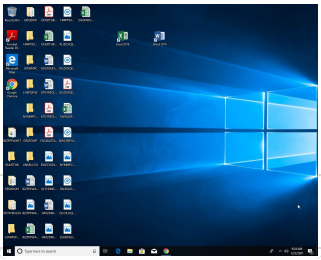
Windows Analysis Report UioA2E9DBG

Overview

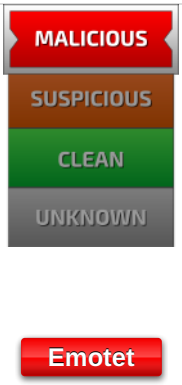
General Information

Sample Name:	UioA2E9DBG (renamed file extension from none to dll)
Analysis ID:	532429
MD5:	6988533cf7cbdcc..
SHA1:	27836d3e04a315..
SHA256:	8d6912a12fdccb3..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

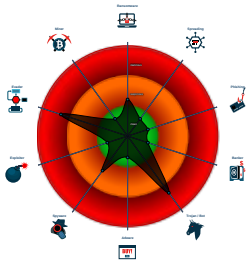


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- 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
- Queries the volume information (nam…
- 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: 6956 cmdline: loaddll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 7012 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7056 cmdline: rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5544 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7040 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5368 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jsczeisswlgpw\ifzwhxr.fpp",gqJNgJRYaqyk MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7092 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,agrwqhxohbh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7108 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,aoydsyidkopcdbcv MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5192 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5064 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6708 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **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
00000006.00000002.684418715.0000000000380000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000002.696991092.0000000000D90000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.828298416.000000000008E0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.694340801.0000000000A30000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.684454921.000000000006DA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.113eef0.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.2.loaddll32.exe.113eef0.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.d64248.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.6f4270.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.2.loaddll32.exe.d90000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 15 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)

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:

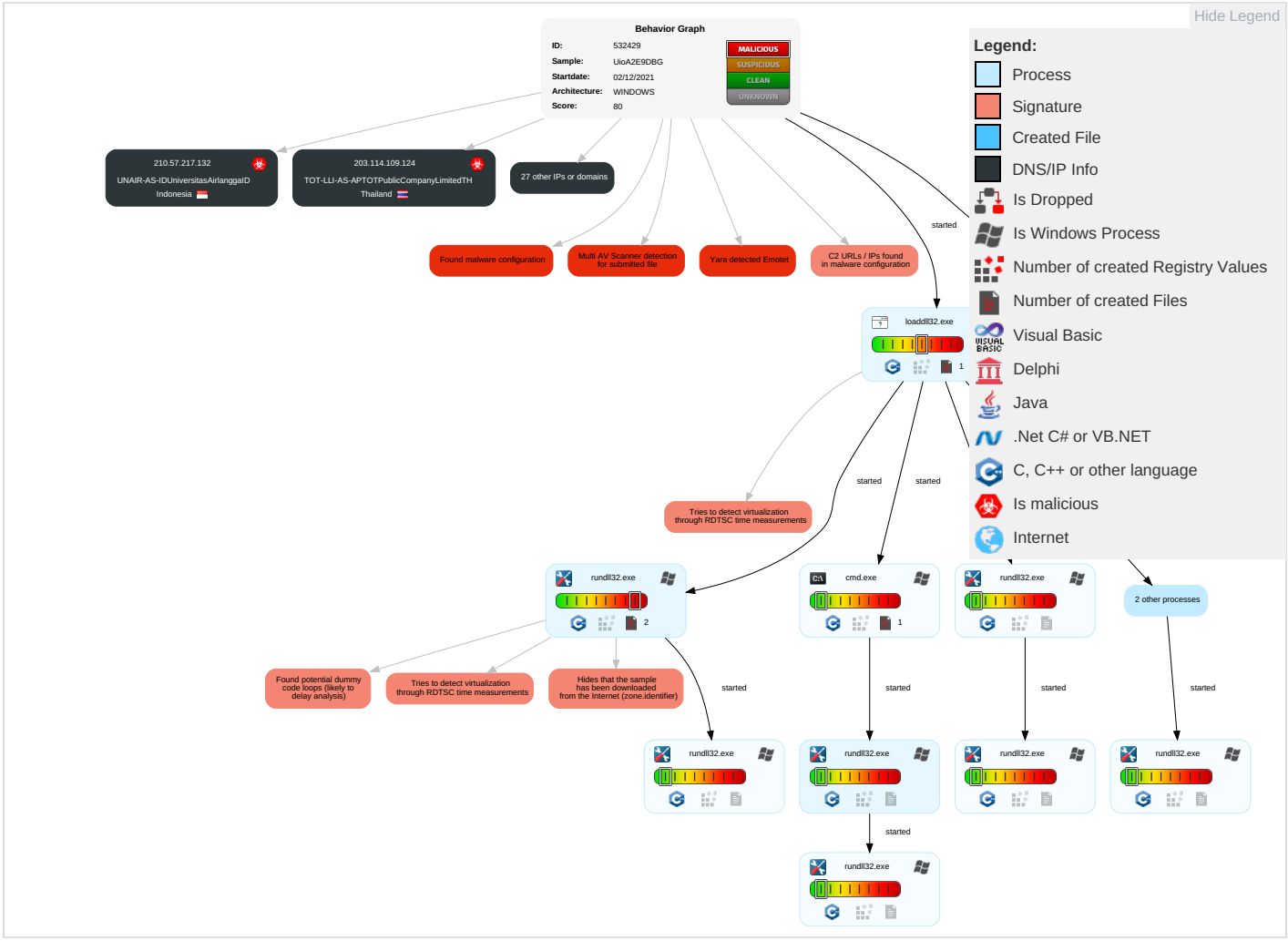
Yara detected Emotet

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	Path Interception	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 Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 2 1	LSASS Memory	Security Software Discovery 2 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic 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	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Information Discovery 1 4 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F 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

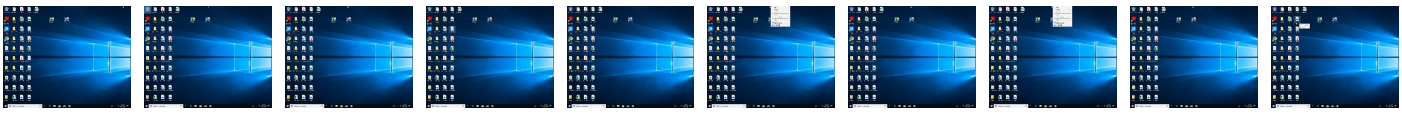
Behavior Graph

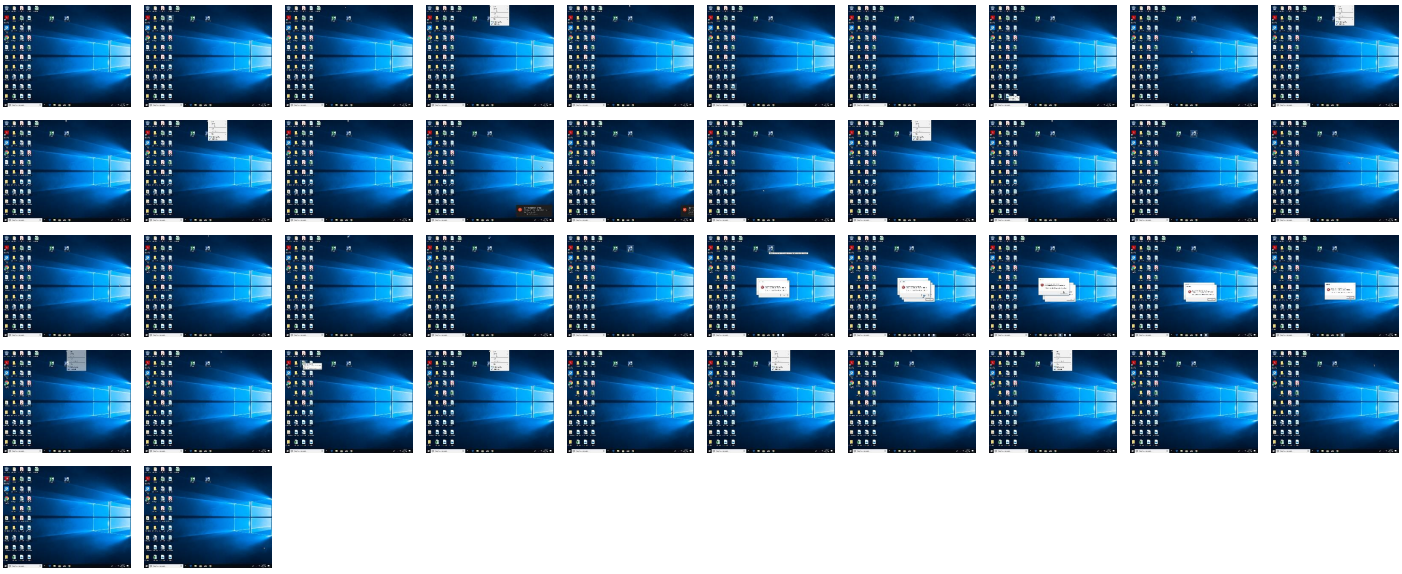


Screenshots

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
UioA2E9DBG.dll	23%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.1130000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.2.loaddll32.exe.d90000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.b10000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.380000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.a30000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.ver)	0%	Avira URL Cloud	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-IDPTCitraJelajahInformatikaID	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
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532429
Start date:	02.12.2021
Start time:	09:19:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UioA2E9DBG (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:	20
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:	mal80.troj.evad.winDLL@22/4@0/30
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.8% (good quality ratio 4.6%) • Quality average: 73.1% • Quality standard deviation: 25%
HCA Information:	• Successful, ratio: 70% • 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
09:21:52	API Interceptor	2x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	916Q89rlYD.dll	Get hash	malicious	Browse	
	9izNuvE61W.dll	Get hash	malicious	Browse	
	P5LROPCURK.dll	Get hash	malicious	Browse	
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	
	snBYiBAMB2.dll	Get hash	malicious	Browse	
	6zAcNlJXo7.dll	Get hash	malicious	Browse	
	6zAcNlJXo7.dll	Get hash	malicious	Browse	
	mal.dll	Get hash	malicious	Browse	
	mal2.dll	Get hash	malicious	Browse	
	mal.dll	Get hash	malicious	Browse	
	mal2.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	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	
212.237.17.99	916Q89rlYD.dll	Get hash	malicious	Browse	
	9izNuvE61W.dll	Get hash	malicious	Browse	
	P5LROPCURK.dll	Get hash	malicious	Browse	
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	
	snBYiBAMB2.dll	Get hash	malicious	Browse	
	6zAcNlJXo7.dll	Get hash	malicious	Browse	
	6zAcNlJXo7.dll	Get hash	malicious	Browse	
	mal.dll	Get hash	malicious	Browse	
	mal2.dll	Get hash	malicious	Browse	
	mal.dll	Get hash	malicious	Browse	
	mal2.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	916Q89rlYD.dll	Get hash	malicious	Browse	• 212.237.56.116
	9izNuvE61W.dll	Get hash	malicious	Browse	• 212.237.56.116
	P5LROPCURK.dll	Get hash	malicious	Browse	• 212.237.56.116
	zTGtLv4pTO.dll	Get hash	malicious	Browse	• 94.177.217.88
	zTGtLv4pTO.dll	Get hash	malicious	Browse	• 94.177.217.88
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 212.237.56.116
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 212.237.56.116
	snBYiBAMB2.dll	Get hash	malicious	Browse	• 212.237.56.116
	6zAcNlJXo7.dll	Get hash	malicious	Browse	• 212.237.56.116
	6zAcNlJXo7.dll	Get hash	malicious	Browse	• 212.237.56.116
	DHL DOCUMENT FOR #504.exe	Get hash	malicious	Browse	• 62.149.128.40
	RqgAGRvHNwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RqgAGRvHNwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	dFUOuTxFQrXAwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RbrKCqqjDPUwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	dFUOuTxFQrXAwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RbrKCqqjDPUwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	mal.dll	Get hash	malicious	Browse	• 212.237.56.116
	mal2.dll	Get hash	malicious	Browse	• 212.237.56.116
	mal.dll	Get hash	malicious	Browse	• 212.237.56.116
OnlineSASFR	916Q89rlYD.dll	Get hash	malicious	Browse	• 195.154.133.20
	9izNuvE61W.dll	Get hash	malicious	Browse	• 195.154.133.20
	P5LROPCURK.dll	Get hash	malicious	Browse	• 195.154.133.20
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	• 51.15.17.195
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 195.154.133.20
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 195.154.133.20
	snBYiBAMB2.dll	Get hash	malicious	Browse	• 195.154.133.20
	6zAcNlJXo7.dll	Get hash	malicious	Browse	• 195.154.133.20
	6zAcNlJXo7.dll	Get hash	malicious	Browse	• 195.154.133.20
	mal.dll	Get hash	malicious	Browse	• 195.154.133.20
	mal2.dll	Get hash	malicious	Browse	• 195.154.133.20
	mal.dll	Get hash	malicious	Browse	• 195.154.133.20
	mal2.dll	Get hash	malicious	Browse	• 195.154.133.20
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 195.154.133.20
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	0.24858787689396322
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4X:BJiRdwfu2SRU4X
MD5:	E68626B82BA10B2BF7CE82EFE32E165D
SHA1:	E9427E7262FCDBB2915462BD8D0D0AAC1DCDFC09

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SHA-256:	D533100EB675B3D0FA2989D23884436A6AC0DB6670486CA666885181E4F86BCC
SHA-512:	87633999CAC16D4EBC5614172E0061FB5135316C2BB69B61C61577120C4086F32E888BC06CA87E71AE1A950F16F57D5C492F50E1B30D415720BE00DD6A369512
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 engine DataBase, version 0x620, checksum 0x52f1f60b, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25072727150045127
Encrypted:	false
SSDEEP:	384:8+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:jSB2nSB2RSjlK/+mLesOj1J2
MD5:	B7E37638BA471F8F6F75CFF2137C3B64
SHA1:	A940F1AF6850A1323B637D09DF7EEA0A73770CD2
SHA-256:	A29BD18D97BAF7D7672C344F780536C9A06039312A7C5E81A7C74822BCB2BE42
SHA-512:	63C7B8B1A69088C5FE4EA0419C5ED23F8A231EE6E162362680F1D260D0E0C47759691334BA57B104EF4B180E4C8912559CC135455DDA43A07BC686E3BC00444
Malicious:	false
Preview:	R..... .....e.f.3...w.....&.....w..5....y..h.(.....3...w.....B.....@..... ....3...w..... .....N5....y.u.....5....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07727570710710759
Encrypted:	false
SSDEEP:	3:3/t7EvQBnB+hl/bJdAtiDCQTltlall3VkttlmlnI:PtiQBnit4kC+tA3
MD5:	0ABC927E030E5B12F91111B4688C9DB8
SHA1:	0F565D9C62B05FB127DC5768E670047D26D6A2AC
SHA-256:	8B2DF592248D557DE249459C3FEDD134CB5B67D821DD163E3A05D2D7F030924E
SHA-512:	9B9D1B69420D67066D1C70674F22D06FF60DAE83A985BD44042DBC6F5533568219E327981E558AC7BCF3856298066F483B43EB6240F65DEFE9C3A459DBEB7057
Malicious:	false
Preview:	.T.7.....3...w..5....y.....w.....w.....w....:O....w.....5....y..... ....

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):	7.196240298834973
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:	UioA2E9DBG.dll
File size:	473600
MD5:	6988533cf7cbdccd0ea429571e0441a9
SHA1:	27836d3e04a31548fa09ec8537ba50777a73a42a
SHA256:	8d6912a12fdccb3d6d55980c3b1fd20cc97a2736d3381e315657a3d6f2f8d1b3
SHA512:	2d48c1b8ef38ad9d0a68650896b5ee69bdcea2caeddfe5e8cadd7b5f411311a8a43a09ce33ca5d6b5e341f38f30fbe41a0aa91048a8b2c5a2a663013f8b1e40
SSDEEP:	12288:mFyGBDytNZAR5Myju+qQuj/J+7C6Dg8stHb1h:mF92e/jEk7zDg8stJh
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....A~.. ... ...F... ...F..D ...U... ...U... ...U... ...F... ...F... ...F... ... ..< ... .TU... ..TU... ..TU... ... .TU... .

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10014c2e
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:	0x61A7B2E7 [Wed Dec 1 17:37:43 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:	057d91f9747659ff50a0558e0aed5a44

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x385cc	0x38600	False	0.542072304601	data	6.65370681685	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3a000	0x12520	0x12600	False	0.497967155612	data	5.51962067899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4d000	0x23d4	0x1600	False	0.2265625	data	3.93138515856	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x50000	0x24448	0x24600	False	0.788874570447	data	7.67571153778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x75000	0x2d78	0x2e00	False	0.740913722826	data	6.57934659057	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	
Russian	Russia	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6956 Parent PID: 6032

General

Start time:	09:20:08
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll"
Imagebase:	0x8c0000
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: 00000001.00000002.696991092.0000000000D90000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.697195816.000000000111B000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 7012 Parent PID: 6956

General

Start time:	09:20:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.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: 7040 Parent PID: 6956

General

Start time:	09:20:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,Control_RunDLL
Imagebase:	0x12c0000
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: 00000004.00000002.694340801.0000000000A30000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.694486235.0000000000AB6000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7056 Parent PID: 7012

General

Start time:	09:20:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1
Imagebase:	0x12c0000
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: 00000005.00000002.683073019.0000000000DBA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.683120624.0000000001130000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7092 Parent PID: 6956

General

Start time:	09:20:13
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,agrwqhxohbh
Imagebase:	0x12c0000
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: 00000006.00000002.684418715.0000000000380000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.684454921.00000000006DA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7108 Parent PID: 6956

General

Start time:	09:20:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,aoydsyidkopcdbcv
Imagebase:	0x12c0000
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: 00000007.00000002.696143071.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.696221862.0000000000D4A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6708 Parent PID: 572

General

Start time:	09:21:50
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff70d6e0000
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

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5544 Parent PID: 7056

General

Start time:	09:23:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL
Imagebase:	0x12c0000
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: 5368 Parent PID: 7040

General

Start time:	09:23:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jsczeisswlgpw\ifzwhxr.fpp" ,gqJNgJRYaqyk

Imagebase:	0x12c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.828298416.00000000008E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.828605995.00000000009D5000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5240 Parent PID: 7092

General

Start time:	09:23:07
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL
Imagebase:	0x12c0000
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: 5192 Parent PID: 7108

General

Start time:	09:23:12
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL
Imagebase:	0x12c0000
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: 5064 Parent PID: 6956

General

Start time:	09:23:13

Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL
Imagebase:	0x12c0000
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

Disassembly

Code Analysis