ID: 532438
Sample Name: 3pO1282Kpx.dll
Cookbook: default.jbs
Time: 09:46:35
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

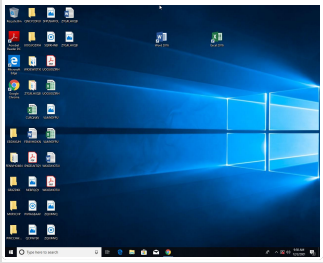
Windows Analysis Report 3pO1282Kpx.dll

Overview

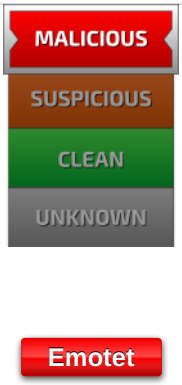
General Information

Sample Name:	3pO1282Kpx.dll
Analysis ID:	532438
MD5:	173345845a2a7d..
SHA1:	35ed97b5ac5a3e..
SHA256:	9ed58848f0a7b35.
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

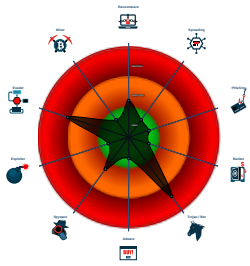


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- 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…
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- Contains functionality to query CPU …
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6544 cmdline: loaddll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4652 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6256 cmdline: rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6040 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6088 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5280 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Tbiyedppjzsf\xswipktkmrv.drt",WgszfYRBINQe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4532 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4112 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6612 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1508 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3520 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6544 -s 324 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 3424 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6544 -s 332 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6920 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7160 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6936 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6544 -ip 6544 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6800 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6544 -ip 6544 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5636 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1040 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6264 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.693163248.0000000001210000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.693163248.0000000001210000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000000.638369835.000000000131B000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000000.638310393.0000000001210000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000000.638310393.0000000001210000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.2e221e0.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.2e221e0.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.0.loaddll32.exe.1210000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.0.loaddll32.exe.1210000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
1.2.loaddll32.exe.1333540.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 63 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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)

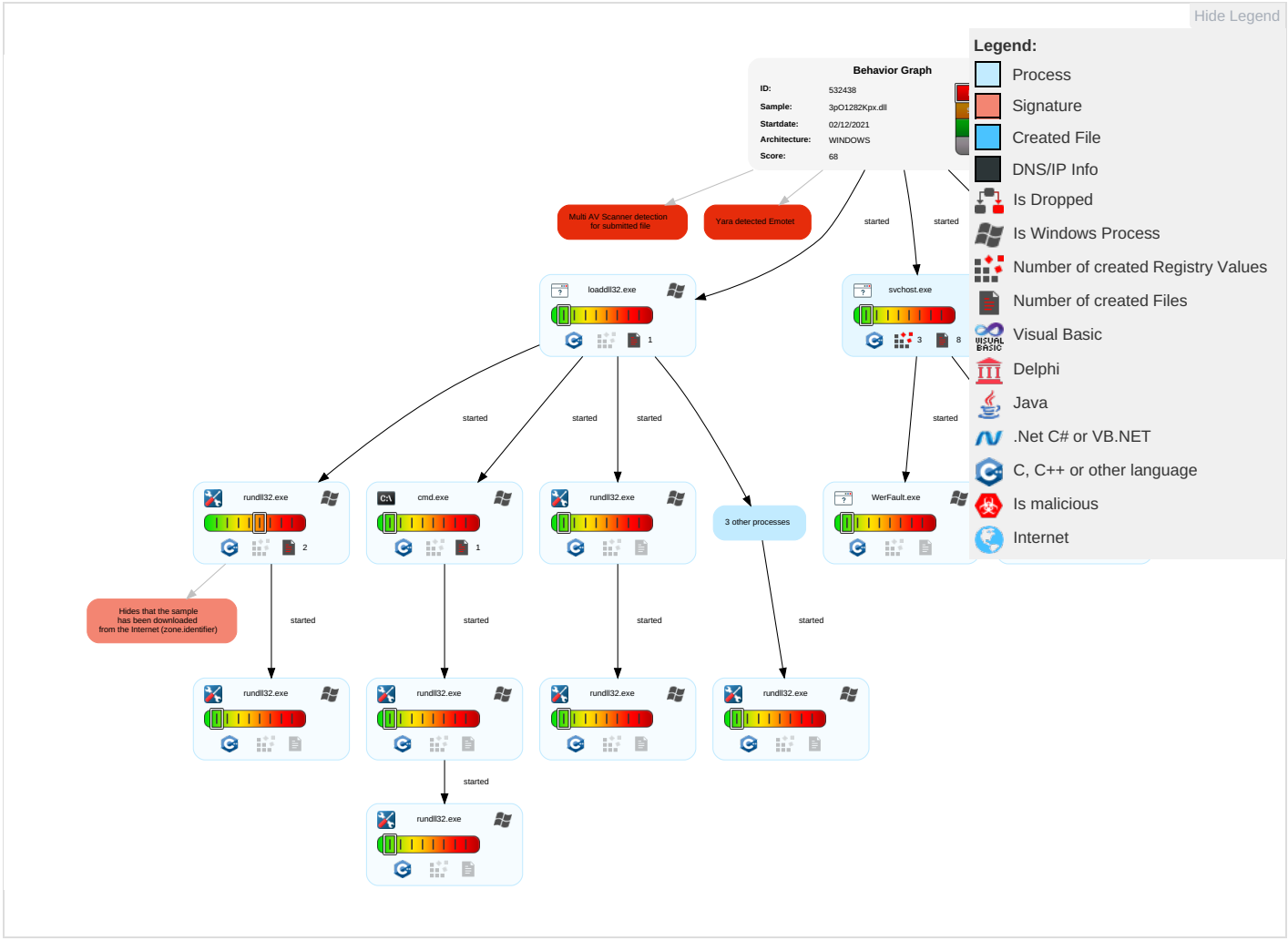
Stealing of Sensitive Information:

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 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 on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Security Software Discovery 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	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 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	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 Communication
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 3 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

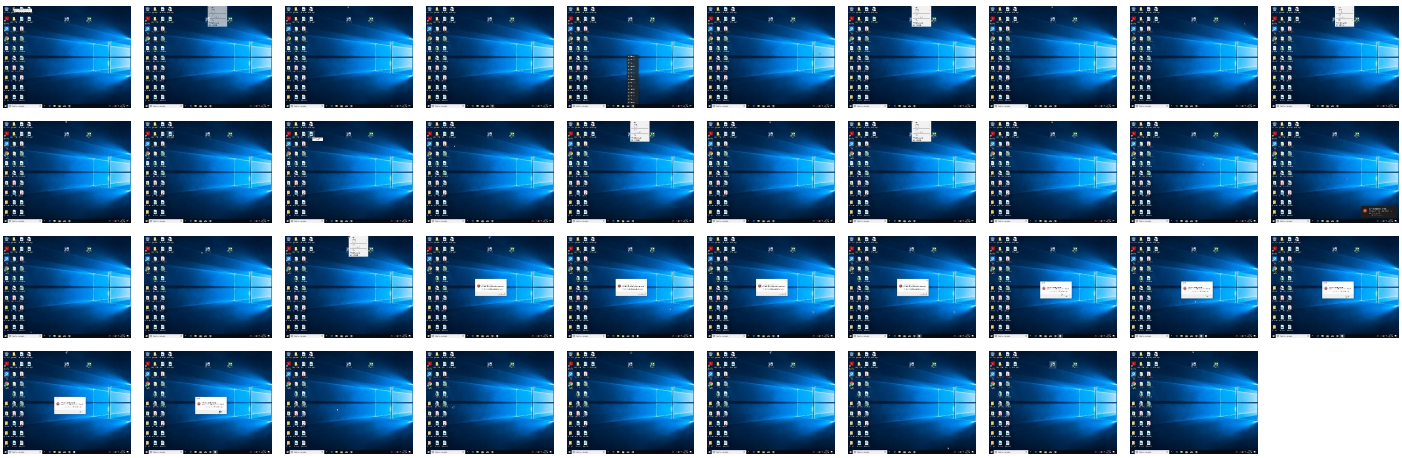
Behavior Graph



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
3pO1282Kpx.dll	23%	Virustotal		Browse
3pO1282Kpx.dll	18%	ReversingLabs	Win32.Trojan.Phonzy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.loaddll32.exe.1210000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.3200000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.b90000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.1210000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.3100000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.2.loaddll32.exe.1210000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.1210000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.0.loaddll32.exe.1210000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.ver)	0%	Avira URL Cloud	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://schemas.xmlso	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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532438
Start date:	02.12.2021
Start time:	09:46:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3pO1282Kpx.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	27
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:	mal68.troj.evad.winDLL@34/18@0/1

EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.8% (good quality ratio 14.6%) • Quality average: 73.1% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 66% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:48:56	API Interceptor	1x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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):	0.2486016457556919
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4j:BJiRdwfu2SRU4j
MD5:	18B070EFED14C96073A9B936EFE79913
SHA1:	821E818F84ABA70502A904DB87FC94D6510B820F
SHA-256:	5DAA0308D33857351BC3D7337291607FAE447F85786CFED7948A1A5D538FE49E
SHA-512:	EEBE8099FB1AE0AD891A59281E791EA3B783983FE68145E1E655BF4B41FA00327C7328DDFC48E4C1100ED948F7AE15B44A2A6C4F629943C01E6C779025559E7(
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x1e63e422, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071093797838945
Encrypted:	false
SSDEEP:	384:s+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:zSB2nSB2RSjlK/+mLesOj1J2
MD5:	3B35ECABDA4B6946E7118FC8CFE61520
SHA1:	BF8ABDD5A198CBAF0B7BE0A9C403DC732E3A84F2
SHA-256:	6CB5F094A3B162EA38B7C1B3E0FC0111B82A44F9BB0D953AE613614A26E0F58E
SHA-512:	D7CFFF816D976ACF7AF992837F81917EA176DAC20FBCAD523F01E7E30ABB8B00B4FDBB1DF5834FE7AA82362A13FE7D05D802840685A6C274248ED0650DE56F C
Malicious:	false
Preview:	.c."... .....e.f.3...w.....&.....w..80...y..h.(.....3...w.....B.....@..... ....3...w..... .....80...y.y.....i.f80...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07728180241167973
Encrypted:	false
SSDEEP:	3:dPlTEvden4t+j8l/bJdAtiGeltoll3VkttlmlnI:dYX+j8t4wlG3
MD5:	092DF1FAA6DB821C33C9BBF01F73FDCF
SHA1:	35D7F10F684DA4913402E647E3342CD5313BAC76
SHA-256:	CF3D5794FFC0B16C33F0C77BABDF860EA8930679E0593BA1E4E51D1CD855C0F5
SHA-512:	46A1EBF84DF5725FBC3D109980AE232725694583CE5FCDD3883FC2F2F4552FD8CCCB7057E39436761DA3D3989684A891EC61AC88B9221CA09EAE766AA08775E
Malicious:	false
Preview:	.1.....3...w..80...y.....w.....w.....w....:O....w.....i.f80...y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb87a191e6babfe54825d1747bdca62202fdccd_d70d8aa6_0ce3f3fd\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):	0.6753133274689476
Encrypted:	false
SSDEEP:	96:WmcePpSZqymy9hkoyt7JfHpXIQcQ5c6A2cE2cw33+a+z+HbHg0VG4rmMOyWZAXGD:WBBaHnM28jjIq/u7slS274ItW
MD5:	EC4AD4206ADB820AA65890173145C0DE
SHA1:	244049840822C83C1555922E9C079698D2A6A462
SHA-256:	59D0B88DC3EE09B85F98B87B6F80EF0909857B148E649C5BAA85AF909ACBDA72
SHA-512:	4412E3FB67648A3A82F605DA9C4101C8788DE89322F7B6214BEF25DE500BCBC5C3CD1F8A99AD395548292950E60722BF74B01ACA3F4CC71568094C5B9AA9CE1
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.=.1.3.2.8.2.9.4.0.9.9.6.8.6.6.0.8.9.4.....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.=.4.0.0.1.b.9.4.e.-.8.6.5.c.-.4.a.4.c.-.8.d.2.e.-.9.9.c.6.e.5.f.6.9.e.b.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.=.4.6.f.3.9.f.b.4.-.e.8.5.1.-.4.f.9.2.-.9.c.6.8.-.2.e.f.8.a.f.a.6.b.a.7.2.....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.=.0.0.0.0.1.9.9.0.-.0.0.0.1.-.0.0.1.7.-.9.a.0.6.-.b.3.a.e.a.4.e.7.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_0c442de9\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0c442de9\Report.wer

File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.678619951881378
Encrypted:	false
SSDEEP:	96:gVF6qdpSZqyty9hk1Dg3fWpXIQcQxc6VcEzcw3VR+a+z+HbHg0VG4rmMOyWZAXGp:oQ7B9HPRZvjIq/u7slS274ItW
MD5:	2314D313E55933A1C818394150FC79E4
SHA1:	D3136EB940E73470078AB3BCACA65B5BD880CFD9
SHA-256:	98A940EC0D96CE6C7AFED935B3F6328FA74809CCE0A5E065C8B346AF5C627809
SHA-512:	9A4C52AB66D4694A98F44DFFBFF83628167420BD2953706A0D470F44C46C3153F48421ED450EA7CC52F81B104A6B5761C705154179D8F20D280841916AA74269
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.=.1.3.2.8.2.9.4.1.0.0.4.5.5.2.3.0.7.7.....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.=.1.3.2.8.2.9.4.1.0.1.0.5.9.9.1.4.2.2.....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.=.3.c.5.2.4.9.6.3.-.5.0.8.6.-.4.3.7.8.-.a.a.d.e.-.5.0.7.c.3.c.c.a.5.5.0.1.....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.=.3.7.e.a.6.7.3.e.-.a.d.3.c.-.4.1.4.a.-.b.6.c.1.-.5.3.5.d.6.4.4.2.1.3.3.8.....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.=.0.0.0.0.1.9.9.0.-.0.0.0.1.-.0.0.1.7.-.9.a.0.6.-.b.3.a.e.a.4.e.7.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\WER581.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 17:50:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059068
Entropy (8bit):	1.3679296955934206
Encrypted:	false
SSDEEP:	1536:dILzfDvWSJtpmlrUHpOAzih5uVCPAtJdKo5X37kK5xTmnRGe72Ut1yQB:dqrp2rUHp4hoVCI77DmR/2Ut8QB
MD5:	2B3BB1E73F5417CBBA94BAB5F9A23BE0
SHA1:	8989F49B15E937D37902F99BE2D5F66DD8BF16FF
SHA-256:	28B33D4BC476E6C48894EA4319D920D6FAB817FB200950E82BD8A335D30C4B38
SHA-512:	A5940083CD8666F0929A2DF36148FAA949C3E9515236F5A9356A1DAC88E15ABBBF9E136DDE15E5CB86F958A26E799745A07BBB8F98435A54EF0C7DAF851836B
Malicious:	false
Preview:	MDMP..... .....M..a.....4.....H.....$.....`.....8.....T.....@.....U.....B.....p.... ...GenuineIntelW.....T.....a-.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .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\WER7A6E.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49808
Entropy (8bit):	3.07751871746348
Encrypted:	false
SSDEEP:	1536:DuHSxfEFmVPNlZAHxHULSmK5GIZ4y9Tjt7:DuHSxfEFmVPNlZAHxHULSmK5GU4y9TjJ
MD5:	F995B8EA53E910527A1E58DA26B8284A
SHA1:	3CB5A70A02ACE3EFA7BC1D70EA3E3E2B3E1EA470
SHA-256:	E2AFA4CA5DFF1D395E8D79430BE0C470BEEA612038C2C46EA1D5D1229BEE2E85
SHA-512:	ABEB857B348000653131BC1ECC6265B53580437DA6C707A2DECACB02D862FD24B2B0BAB9130BF0A4C32B2EB81D1CB169A63A17F26B81EC3086AFD919B303F16B
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\WER7E86.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6957528855021784
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E86.tmp.txt	
SSDEEP:	96:9GiZYWG0RCqDYGYU9WgH5YEZYytriFFF+yww0GsKY+ar+JVA3zIPN3:9jZDGQRStLBar+JVAsPN3
MD5:	AA12A49C17735F575F9DE21252764DD4
SHA1:	CC9A6030CAE13BF2C329A62F31AAE3AD4A0B4B52
SHA-256:	34E73D5BD3E9374D110BEBB17FD76F1765FFF38F0436A0296F3F5DD8FC83C7BC
SHA-512:	30F9766C5B52315532B11F453BF7246228B0A182726913959ED68815B6F9011363AC5FD5688D6955955D95E7F1A43A8A1EF6B89BD2B121121B1079516D5026F5
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\WER9C9E.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49396
Entropy (8bit):	3.078326445297238
Encrypted:	false
SSDEEP:	1536:FHHXB0lKQAoKQl/A8vmR/KLRKZZyaTvVza:FHHXB0lKQAoKQl/A8vmR/KLRyZyaTvVe
MD5:	FD378F80D58B8AAD5C6F5E84D1F2DFAF
SHA1:	B56A8068AD34286D1F1215CBDE79712C24E1D61F
SHA-256:	8B9F7F03D85C396CE636EB03979233641431E06BE003AD1AE5DF0283BDB133C6
SHA-512:	5F4E95869BE4D3C486600EBCE62035BE11AC4F9DFEE97A56D010841E5B5402EF4D88A47869F46DD92DBFEC89107BD73D785319D32F1E4B2182F2A53C61F0692
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\WERA058.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6964294121392984
Encrypted:	false
SSDEEP:	96:9GiZYWTL0Yje6Y6YosW2uH3QYEZ9SetrilFL+7wpTBGOLa4LLEO38I6h3:9jZDfu6tWSBoSa4LLEOr6h3
MD5:	F69960077705207D0A27B349E85CFFA3
SHA1:	BFB7F1A8F40A243569D3F6443E29ABC42398790F
SHA-256:	BE84D114B0306040AA411393E07A0267AEFAC81126EA2F8D17E22816BE964E00
SHA-512:	58DD60608487332D74A69C08E8FF47F3415EFFB0719874B03E52E15D8637DE5095004179FC55C29798727E9034BC23FC3EBD03464C69D07E4C9659E7B2BEAB80
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\WERD24.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):	8300
Entropy (8bit):	3.6932020895656654
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipE6G6YJxSUqlkgmfL8GSICpD589bXmsfC9m:RrlsNiK6G6YvSUukgmfLrSeXFfB
MD5:	AE14C04A846BA9F8E1A399D339973C09
SHA1:	C4AF4168EA0A92659C8AB476A2AC61D27F5B3383
SHA-256:	85A4D174D37F8F1FD6087BBAD159C3033B63ED686EFFE5EFB3979005CF101985
SHA-512:	7E589FB4B8476C667DEE5BFC9625EB22B86D5AC9DD7A82874F80B8944DF49D89305E5209F5FB12EB77EBD7210EA76AB11A391D7EC5232315A9A565984F2CD49
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD24.tmp.WERInternalMetadata.xml	
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.>.6.5.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE74B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 17:49:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26052
Entropy (8bit):	2.557444551215252
Encrypted:	false
SSDEEP:	192:O0MutBHlO1YHOeR/cxmlCKCxKhe3Sa7NQ+ebAoIef7:C2BFZueaMlCKCxKY3SgNQ+uR
MD5:	313E5A54D53DE9B03EA81A0DC6C74362
SHA1:	226871018B652C200572A17376C02D68140F3D8F
SHA-256:	7A358BAFF2720D68857BBDABFCBF8D5375E8BF2108F8B286C3875FD07C2F32BC
SHA-512:	6C82D6EE04F562E25E979082723EA220DF18D5CF64A8FD64B08FAF168B31961B613D2328773A6166573859248607F47FD8A6006632EA68BDA84B529DF70DEAAC
Malicious:	false
Preview:	MDMP..... .....E..a.....4.....H.....$.....`.....8.....T.....h...\Y.....U.....B.....p.... ...GenuineIntelW.....T.....a-.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .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\WEREAC7.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):	8340
Entropy (8bit):	3.702994961193325
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNip269F6YJ1SUH2wgmfzSzDCpBT89b8msfk0m:RrlsNio6v6Y7SUWwgmfzSz98Ffu
MD5:	94E36D19C7B1AE8116E13D87D0BFA46C
SHA1:	CF3550788F302BA4168344F47860F3BDEAA8C889
SHA-256:	7073CE4D5B84FF2971A510C01AF94BE96330772E25CC6332A85049F99EDD9E43
SHA-512:	FA1156B10F425670F64477585ECAB84E9A4DDFF7D3EA465C534425AB51242A3270191B6F6F611EC8AA4A2616C5FDED8A74DC5397E8854173B8292A0A39314B5C
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.>.6.5.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDB6.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):	4.474652743364087
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI98HSWSC8BR8fm8M4J2ygZFqz+q84WU00KcQIcQwQhdd:ulTfw3TSNAJ22znDKkwQhdd
MD5:	D8D4EAEA78C61107B59A2731E1EE8DD5
SHA1:	4EAA41A60968B9446ADA7C564928A740EA0518BC
SHA-256:	5909AF7589AE7395E8554A2BD08C7EC7BA3FB7CF47F6DBC0E529EB689976C1DB
SHA-512:	CFDA51D901B98EB7A2A42C92E066D57EB818EB7B13AF5F0A856B300CE314B856EE87F4922DBC37C1C73E8412332612166928451DB67B4F0C731B09A338C23672
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="1280340" />.. <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\WERFA5.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):	4.428374721600115
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI98HSWSC8Bv8fm8M4J2yGtF13+q84tjY0KcQIcQwQhdd:uITfw3TSNOJElx/KkwQhdd
MD5:	C912B85A3294A83B66C998EAEF5693A0
SHA1:	3C0C3D52C71CF8E552B6BBC76CEE9F29B024B851
SHA-256:	AAD01C9659E9AD7DF5FC5C7CF0B64D8F968DEA6AA2751CD19A45EC580D2119F1
SHA-512:	7A4B84231764DC7EFDA9FFE31B4DC74B28A8D05722509A0DAEDBED7D2FD0A972ABFE50B43D4CAA41A3B081ACEC819D648D9D9CF5F0031E8D6789FB7DB6C10C2
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="1280340" />.. <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:\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
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

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):	4.215262851555234
Encrypted:	false
SSDEEP:	12288:fMHzwKQAANrn2YHLBqf4xZfjaISv7xwJioCNkiA5NazzSllYdILlw6:UHzwKQAANr2YHL9CEi/+
MD5:	8E4C33C4642BF7E0D2C0E86932998446
SHA1:	B8759064BC4BFE3972DD22F341907C32DF19CF23
SHA-256:	6B7B0DB45FCBA932A140E79DA8EEDF54A2DEDF9014B318E4637354B6579BE839
SHA-512:	2E3AE18E24E3906DF07657D3BEEBD27F355B3137F376294E78EE9E6FA0AF621649045027B93A36E68C28BF5D1BB3BACB553523B53D9FBE399B39311834E34261
Malicious:	false
Preview:	regfW...W...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..D..... .....@Y..... .....

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):	2.8943954365148468
Encrypted:	false
SSDEEP:	192:kXU1SQpUxo8Y85FSETpq/bDIpn8h8K1ZV6nGoak:or5dAIpn88KTVgGVk
MD5:	F4C44BE066D026642C5F33588EA97DF9
SHA1:	A19D74170090798C8E753ABC9C47926ABDB8CAD5
SHA-256:	3F9D6E489C50FC1A73184DE11C8ACFBF04080A640B678D5943332021D74F4061

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SHA-512:	8D8AC751389A229ADC649226B2F812B91C63E34360D93FE51FC338178C97A1CDA04BA0118CB29ABFDB69857AFCDF0A20CCF31B67DA58BEE2A00CAD63353399D
Malicious:	false
Preview:	regfV...V...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..D..... ....@YHvLE.>.....V.....g...C....F..0_.....p.....hbin.....p.\..,.....nk,.RLG..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .RLG..... ....Z.....Root.....lf.....Root....nk .RLG.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.067331172246508
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:	3pO1282Kpx.dll
File size:	372736
MD5:	173345845a2a7d0d99c17bdc5445df90
SHA1:	35ed97b5ac5a3ed0fdc00eabff20f3bfcdfc8a7c
SHA256:	9ed58848f0a7b354a32d4ef67ea9ff70ba75f9238c39d9f1af88fae6811cb504
SHA512:	c67f4a25b4538ea45291636f4eb1c845bbe5ab68ae32971 32f2e4bbde7f941a11eb276d5bdebe8179f412fd2e63a53 46d53890c1e6aeacca88c7a84bde35bda4
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyt6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLQRQKqV4epRmxAvAD
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:	0x1001a401
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:	0x61A7100E [Wed Dec 1 06:02:54 2021 UTC]
TLS Callbacks:	0x1000c500
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	0x264f4	0x26600	False	0.546620521173	data	6.29652715831	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x28000	0x313fa	0x31400	False	0.822468868972	data	7.43227371512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5a000	0x1844	0xe00	False	0.270647321429	data	2.60881097454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x5c000	0x66c	0x800	False	0.3583984375	data	2.21689595795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x5d000	0x1bb0	0x1c00	False	0.784598214286	data	6.62358237634	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6544 Parent PID: 5616

General

Start time:	09:47:32
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll"
Imagebase:	0xd50000
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, Description: Yara detected Emotet, Source: 00000001.00000002.693163248.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.693163248.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.638369835.000000000131B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.638310393.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.638310393.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.662291713.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.662291713.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.663123528.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.663123528.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.693214956.000000000131B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.641147134.000000000131B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.663179674.000000000131B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.662403503.000000000131B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.640836289.0000000001210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.640836289.0000000001210000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4652 Parent PID: 6544

General

Start time:	09:47:32
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\3pO1282Kpx.dll",#1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6088 Parent PID: 6544

General

Start time:	09:47:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,Control_RunDLL
Imagebase:	0xc60000
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, Description: Yara detected Emotet, Source: 00000004.00000002.637148475.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.637148475.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000003.597595639.0000000003259000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000003.597595639.0000000003259000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6256 Parent PID: 4652

General

Start time:	09:47:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1
Imagebase:	0xc60000
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: 00000005.00000002.636690720.00000000032EA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.636271952.0000000003100000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.636271952.0000000003100000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4532 Parent PID: 6544

General

Start time:	09:47:37
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,ajkaibu
Imagebase:	0xc60000

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, Description: Yara detected Emotet, Source: 00000006.00000002.638357953.0000000000650000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.638357953.0000000000650000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.638392292.00000000006FA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6612 Parent PID: 6544

General

Start time:	09:47:41
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,akyncbgollmj
Imagebase:	0xc60000
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: 00000007.00000002.634927199.0000000002E0A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.634790004.0000000000B90000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.634790004.0000000000B90000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6920 Parent PID: 560

General

Start time:	09:48:54
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6040 Parent PID: 6256

General

Start time:	09:49:32
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\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0xc60000
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: 5280 Parent PID: 6088

General

Start time:	09:49:32
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Tbiyedppjzsf\xswipktkmrv.drt",WgszfYRBINQe
Imagebase:	0xc60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4112 Parent PID: 4532

General

Start time:	09:49:43
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\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0xc60000
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: 1508 Parent PID: 6612

General

Start time:	09:49:47
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\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0xc60000
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: 7160 Parent PID: 560

General

Start time:	09:49:49
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6936 Parent PID: 7160

General

Start time:	09:49:50
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6544 -ip 6544
Imagebase:	0xea0000
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: 3520 Parent PID: 6544

General

Start time:	09:49:52
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6544 -s 324
Imagebase:	0xea0000
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: 6800 Parent PID: 7160

General

Start time:	09:50:01
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6544 -ip 6544
Imagebase:	0xea0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5636 Parent PID: 560

General

Start time:	09:50:02
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

Analysis Process: WerFault.exe PID: 3424 Parent PID: 6544

General

Start time:	09:50:02
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6544 -s 332
Imagebase:	0xea0000
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: 1040 Parent PID: 560

General

Start time:	09:50:27
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 6264 Parent PID: 560

General

Start time:	09:50:35

Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Disassembly

Code Analysis