ID: 491651
Sample Name:
Auftragsbest#U00e4tigung
Dringend.exe
Cookbook: default.jbs
Time: 19:27:41
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

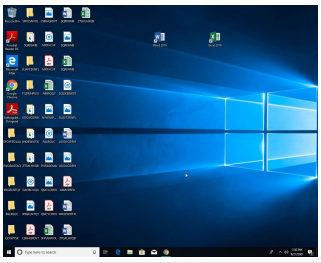
Windows Analysis Report Auftragsbest#U00e4tigung Dr…

Overview

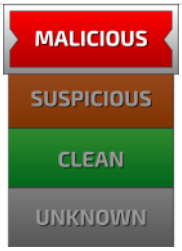
General Information

Sample Name:	Auftragsbest#U00e4tigung Dringend.exe
Analysis ID:	491651
MD5:	b8d99b6c405fc56..
SHA1:	0ba8da5d51a777..
SHA256:	e2bf9e2c787866d.
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection



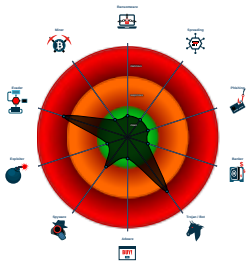
DBatLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected DBatLoader
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- One or more processes crash
- PE file contains strange resources
- Uses code obfuscation techniques (…
- Checks if the current process is bein…
- Monitors certain registry keys / valu…

Classification



Process Tree

- **System is w10x64**
- Auftragsbest#U00e4tigung Dringend.exe (PID: 6584 cmdline: 'C:\Users\user\Desktop\Auftragsbest#U00e4tigung Dringend.exe' MD5: B8D99B6C405FC56BD8A1448421D64EAC)
  - WerFault.exe (PID: 7008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6584 -s 1968 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.358219235.000000000241 4000.00000004.00000001.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000001.00000002.398644926.000000000241 4000.00000004.00000001.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000001.00000000.361969007.000000000241 4000.00000004.00000001.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

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

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

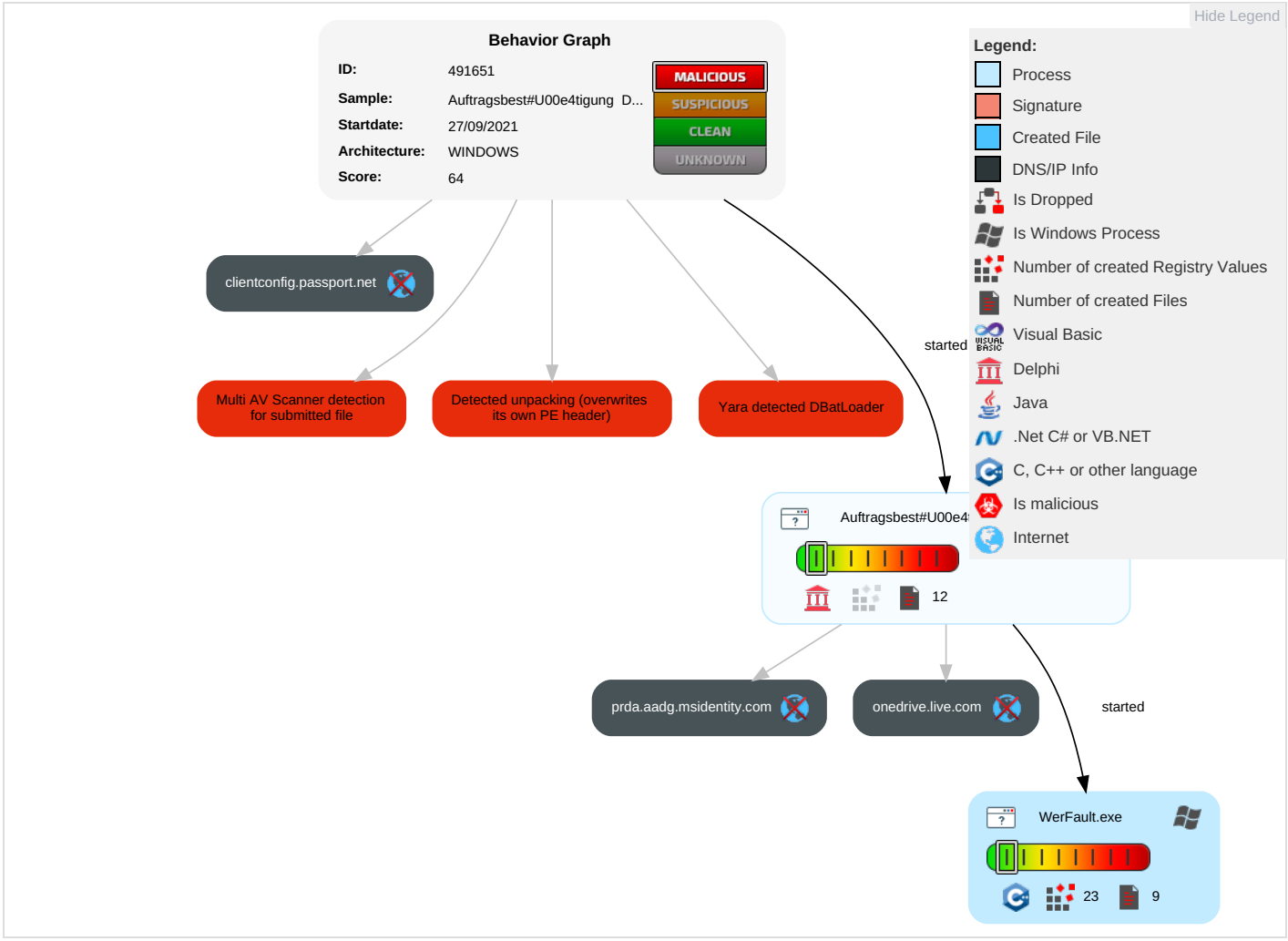
Yara detected DBatLoader

Detected unpacking (overwrites its own PE header)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 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)	Obfuscated Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
Auftragsbest#U00e4tigung Dringend.exe	59%	Virustotal		Browse
Auftragsbest#U00e4tigung Dringend.exe	40%	Metadefender		Browse
Auftragsbest#U00e4tigung Dringend.exe	79%	ReversingLabs	Win32.Trojan.Delf	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://lgincdnmsftuswe2.azureed	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msftauth.net/	0%	Virustotal		Browse
http://https://acctcdn.msftauth.net/	0%	Avira URL Cloud	safe	
http://https://login.mic	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033__M8MTZS7Nv0I1zR18wdR-g2.css	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_3ParxANZ-MNmIfU_UoPk	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.29174.3/images/f	0%	Avira URL Cloud	safe	
http://https://account.liv	0%	Avira URL Cloud	safe	
http://https://lgincdnvzeuno.BB	0%	Avira URL Cloud	safe	
http://https://login.l	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.29174.3/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033__M8MTZS7Nv0I1zR18wd	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.29174.3/images/Windows_Live_v_thumb.jpg	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/js/Conver	0%	Avira URL Cloud	safe	
http://https://lgincdnvzeuno.B	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/js/ConvergedLogin_PCore_OjveJe7WDNHIjSCucBEfkA2.js	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net	0%	URL Reputation	safe	
http://https://onedrive.live.coTR	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
clientconfig.passport.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491651
Start date:	27.09.2021
Start time:	19:27:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Auftragsbest#U00e4tigung Dringend.exe
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:	24
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:	mal64.troj.evad.winEXE@2/4@2/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:28:41	API Interceptor	1x Sleep call for process: Auftragsbest#U00e4tigung Dringend.exe modified
19:29:03	API Interceptor	1x Sleep call for process: WerFault.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\Windows\WER\ReportQueue\AppCrash_Auftragsbest#U00_e3b95c6b267aed71e39879d4727ca63bf4c9e8_fd6e1fa4_1b86a4fb\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14064
Entropy (8bit):	3.767654774062426
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Auftragsbest#U00_e3b95c6b267aed71e39879d4727ca63bf4c9e8_fd6e1fa4_1b86a4fb\Report.wer	
SSDEEP:	192:6etOZmDHnmHBUZMXyB/jrhk8Zd/u7sMS274ItX8Z9:pfreBUZMXojrd/u7sMX4Itg9
MD5:	A9DD6FB10E8A1B2645D66656251B6973
SHA1:	FFD66819B8F28462B080355C410E6DF3A9275EB1
SHA-256:	BDF0D2A0BA22A2CF7F564B89E31BF2516856AEF611B8D4316E26AE515CA3251A
SHA-512:	82D2C3038E3A85FF8FF2C2F3A509F5B5CDA63D6CBAF52A622A86DA288FBA923D4705CC6E9777422C10FADE2E85E94F003545F137C98C46BEF50C6CA2AB7D65F
Malicious:	false
Reputation:	low
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.=.1.3.2.7.7.2.6.9.7.3.1.6.4.6.3.6.3.8.....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.=.1.3.2.7.7.2.6.9.7.4.1.9.9.6.2.0.3.0.....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.=.e.3.9.3.3.8.b.a.-.9.0.d.3.-.4.f.2.8.-.8.f.4.b.-.c.4.b.8.8.4.5.1.d.b.1.0.....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.c.8.4.c.7.5.c.-.b.1.2.c.-.4.6.2.f.-.8.e.4.0.-.2.b.b.d.8.c.5.9.8.3.7.8.....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.=.A.u.f.t.r.a.g.s.b.e.s.t.#.U.0.0.e.4.t.i.g.u.n.g. . .D.r.i.n.g.e.n.d...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.b.8.-.0.0.0.1.-.0.0.1.7.-.0.1.9.a.-.9.c.8.c.1.0.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.7.5.8.1.f.c.e.c.9.6.c.4.f.a.6.5.7.4.b.d.7.5.3.e.c.0.d.c.3.a.0.0.0.0.0.f.f.f.f.!.0.0.0.0.0.b.a.8.d.a.5.d.5.1.a.7.7.7.9.8.0.1.0.e.6.b.1.a.2.a.8.e.7.5.9.c.8.b.c.b.e.7.f.a.!.A.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER76A8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 02:28:54 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	122024
Entropy (8bit):	2.019226623063448
Encrypted:	false
SSDEEP:	384:Qld43d2u9Y2A9DCSWxLQEV8qMtD148k6emGJUFWzBqn7S5MKUpuSN2c/d:a3dvi2A9eSWVQEV8qMtD1bYCOGVKApNh
MD5:	BE5DC4C8BED8089A77BAD3319FCA90CD
SHA1:	A29FCF7B28153394A7FF563C96E758B4D00F6907
SHA-256:	53FFE8158802F96B74B5DD6974F0A0363E5980B2C4C2745E664A3F96EAB484C6
SHA-512:	CF1E75D832E857838BD2730DD3A456A329BA1716374F005D11ACEE0E18FFCB9702C2F6664D3CC6D7ED9B7C73B1028077C42AEFD311269DA1E9E8831B35D916
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....}Ra.....U.....B.....p'.....GenuineIntelW.....T.....}Ra.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER83F7.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):	8454
Entropy (8bit):	3.7055577938875466
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiQ6X6IhSE6YJ7SUU1Ip9mgmfUbS0rCprx89bItsfRFYm:RrlsNiH6IhJ6YlSUU1IqgmfwS0dImf5
MD5:	CD37FC88E8C40A20E4071DCB65297A2C
SHA1:	BDB3CFA8B8DAFC17BAEA3E914EF25CB95AB188B3
SHA-256:	4903CCCF34E2FEC7C58A196D2B1BB41E13391A67F8F62233490927705B3D5628
SHA-512:	D89112998C191826401319C4E9E2463942F7B317653F3BCA9753F3C29D62948B7F24E61F108C19F63F1313DF1FDFEFCA75812ED6C6161075C05FA9AC8F850076
Malicious:	false
Reputation:	low
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.>.6.5.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4723
Entropy (8bit):	4.5260388795915745
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWl9TMSWSC8Bj8fm8M4JpAJEZFmo+q821UBTuuZuWd:uITfJkMzSNaJpA2qoZeBTuuZuWd
MD5:	D66B381C132AF1BB55E33CFE82CC3BA0
SHA1:	CB5A8ADFF3F726B42463E0D413AE2BCBBF761267

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDF.tmp.xml	
SHA-256:	47789E0E275A26A926365A0C811912D5859F676E0804E97C878BA0F4425E4412
SHA-512:	D6B4BA38EC4D155CD79C09E03B67F4D57A1D8A44BACE81A10DB5CAC50ED61A65DC67BD815AD9F65453C0CB70FED606C57D3E8850D2764F94A4DD7FE1C5B449A
Malicious:	false
Reputation:	low
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="1185819" />.. <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" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.785741094468421
TrID:	• Win32 Executable (generic) a (10002005/4) 99.38% • InstallShield setup (43055/19) 0.43% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	Auftragsbest#U00e4tigung Dringend.exe
File size:	831488
MD5:	b8d99b6c405fc56bd8a1448421d64eac
SHA1:	0ba8da5d51a77798010e6b1a2a8e759c8bcbe7fa
SHA256:	e2bf9e2c787866d86fc1ae939c378f7d22fab268a00ae163fff1b79332df2088
SHA512:	5b1408332ce31003708a5de87bb2b7e3df4731d1d978a39dab992a12ccea57ab04239955fd3a56af867fd160ede3d3830826231352bacd0416f887e4e3c070f
SSDEEP:	24576:DMvnUyU3fec2QPesTHGIZHrIzvlZwXI7Dyj3SaH+MJF:DqUjes
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	0a121272a98ce659

Static PE Info

General

Entrypoint:	0x4668bc
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General

Subsystem Version Minor:	0
Import Hash:	ff0bb68e944131943365efbe4d5b9737

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x643c0	0x64400	False	0.526362316864	data	6.54514333706	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x66000	0x904	0xa00	False	0.573046875	data	5.83221478683	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x67000	0x1dbc	0x1e00	False	0.413802083333	data	3.99870200843	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x69000	0x388c	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x6d000	0x2574	0x2600	False	0.320106907895	data	5.16694007124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x70000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x71000	0x18	0x200	False	0.05078125	data	0.170145652003	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	0x6eb4	0x7000	False	0.624337332589	data	6.67037544234	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x79000	0x5a800	0x5a800	False	0.245144164365	data	5.96186308461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 19:28:35.151721954 CEST	192.168.2.6	8.8.8.8	0x2e0b	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Sep 27, 2021 19:28:42.812701941 CEST	192.168.2.6	8.8.8.8	0x2e23	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:28:35.202702999 CEST	8.8.8.8	192.168.2.6	0x2e0b	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:28:42.882693052 CEST	8.8.8.8	192.168.2.6	0x2e23	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:28:43.727102995 CEST	8.8.8.8	192.168.2.6	0x6ca	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Auftragsbest#U00e4tigung Dringend.exe PID: 6584 Parent PID: 5176

General

Start time:	19:28:40
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Auftragsbest#U00e4tigung Dringend.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Auftragsbest#U00e4tigung Dringend.exe'
Imagebase:	0x400000
File size:	831488 bytes
MD5 hash:	B8D99B6C405FC56BD8A1448421D64EAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000001.00000000.358219235.0000000002414000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000001.00000002.398644926.0000000002414000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000001.00000000.361969007.0000000002414000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: WerFault.exe PID: 7008 Parent PID: 6584

General

Start time:	19:28:48
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6584 -s 1968
Imagebase:	0x1160000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis