ID: 528756
Sample Name:
8XMlaeHQXZ.exe
Cookbook: default.jbs
Time: 18:35:37
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 8XMlaeHQXZ.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 3
System Summary: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 11
Data Directories 11
Sections 11
Resources 11
Version Infos 11
Possible Origin 11
Network Behavior 12
Code Manipulations 12
Statistics 12
Behavior 12
System Behavior 12
Analysis Process: 8XMlaeHQXZ.exe PID: 5856 Parent PID: 2248 12
General 12
Analysis Process: WerFault.exe PID: 1916 Parent PID: 5856 12
General 12
File Activities 12
File Created 12
File Deleted 13
File Written 13
Registry Activities 13
Key Created 13
Key Value Created 13
Disassembly 13
Code Analysis 13

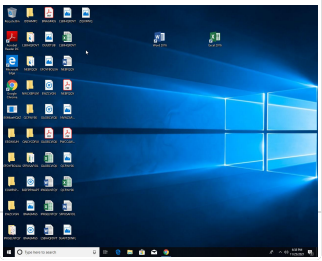
Windows Analysis Report 8XMlaeHQXZ.exe

Overview

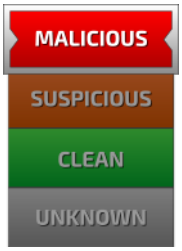
General Information

Sample Name:	8XMlaeHQXZ.exe
Analysis ID:	528756
MD5:	5643bf734d793e8.
SHA1:	4415ad682fd64ba.
SHA256:	db79e0c2243229..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

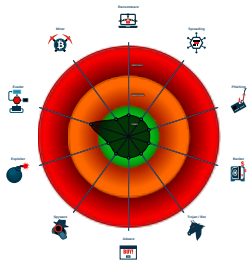


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- PE file has nameless sections
- Machine Learning detection for samp…
- Uses 32bit PE files
- AV process strings found (often use…
- PE file does not import any functions
- Sample file is different than original …
- One or more processes crash
- PE file contains an invalid checksum
- Checks if the current process is bein…
- PE file contains sections with non-s…
- Binary contains a suspicious time st…
- PE file overlay found

Classification



Process Tree

- **System is w10x64**
- 8XMlaeHQXZ.exe (PID: 5856 cmdline: "C:\Users\user\Desktop\8XMlaeHQXZ.exe" MD5: 5643BF734D793E845166A228F3DF83B3)
  - WerFault.exe (PID: 1916 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5856 -s 212 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

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

Machine Learning detection for sample

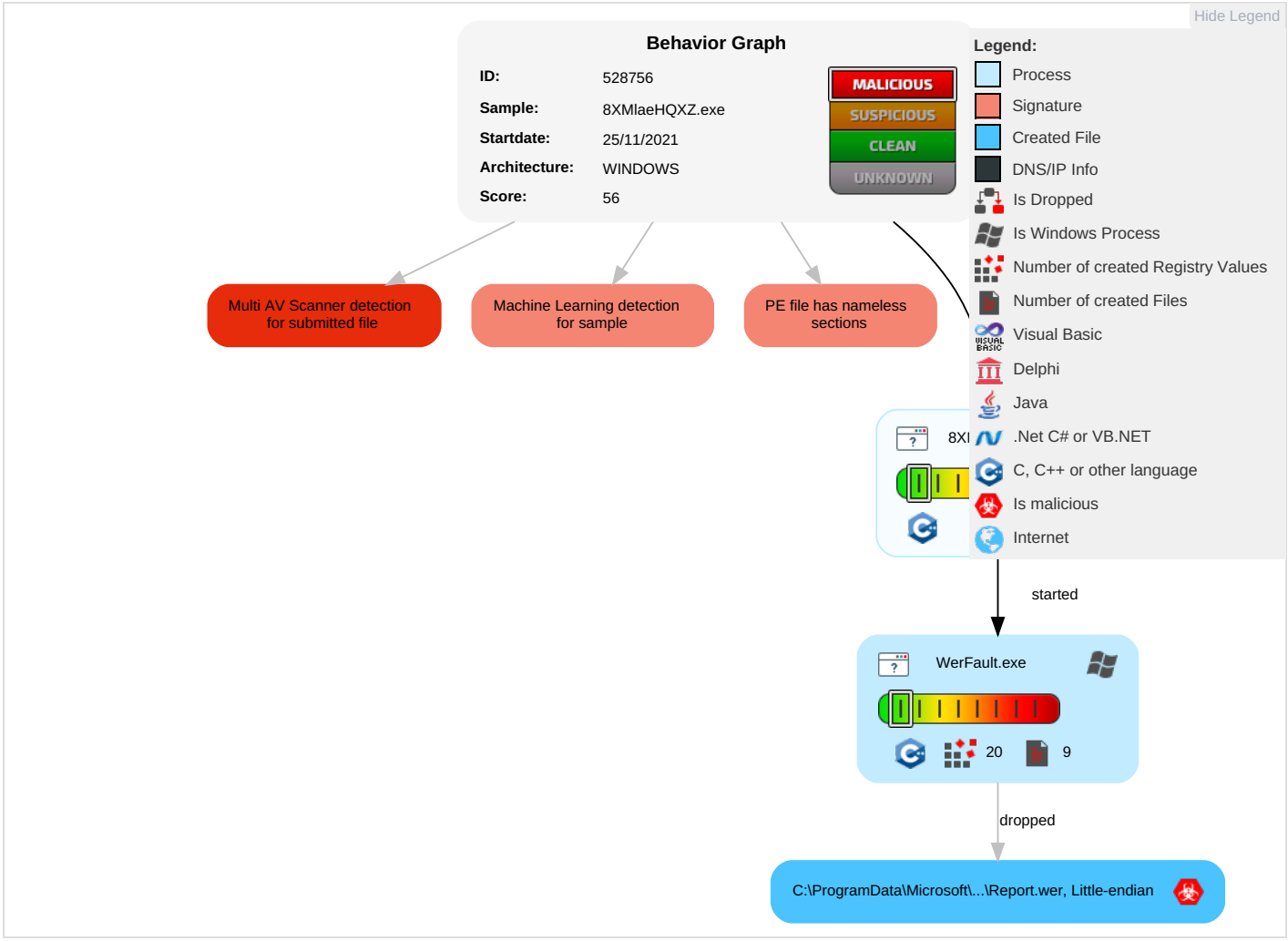
System Summary:

PE file has nameless sections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 2	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

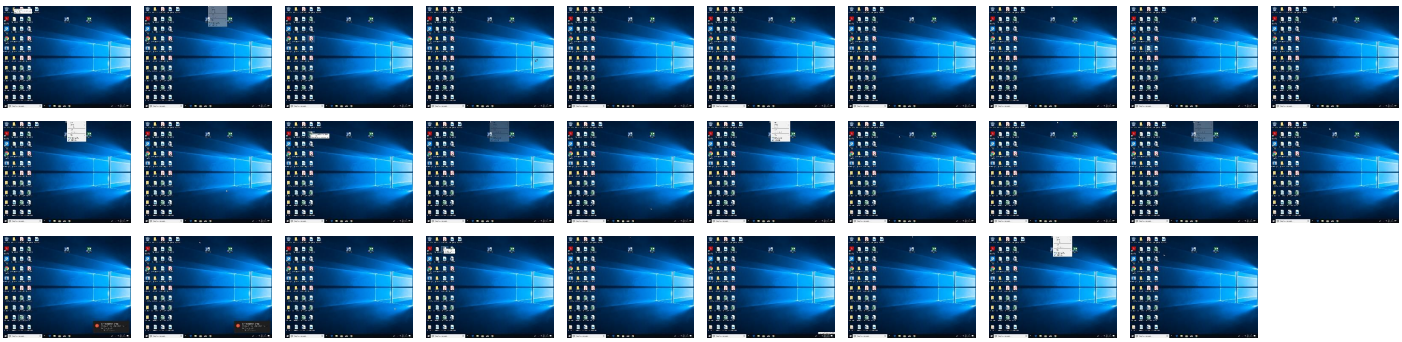
Behavior Graph



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
8XMlaeHQXZ.exe	21%	Virustotal		Browse
8XMlaeHQXZ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528756
Start date:	25.11.2021
Start time:	18:35:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8XMlaeHQXZ.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:	10
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:	mal56.winEXE@2/6@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 68.5% • Quality standard deviation: 31.5%
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
18:36:56	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_8XMlaeHQXZ.exe_eef3a584e8e34ce43e333fc8ab4acb864824d3c_c1f65c8e_06d2b942\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):	0.6313016091472089
Encrypted:	false
SSDEEP:	96:W3FtNhEp4zH6DfhoDt7NflpXIQcQvc6QcEDMcw3DL+HbHg6ZAXGng5FMTPSkvPke:cv4KLHBUZMXojE/u7sVS274Itg
MD5:	59BEEB6007AA16EE8DD6E04C05F8724A
SHA1:	14B7FDE3F601CB3410B0FD81A451C47FA8E25B11
SHA-256:	43B53CC38F652E473C59FF83A6BF48AC4C38EF0E5875CBD295B8DB26D92CCA0D
SHA-512:	D50C699D78BDDDB1C4526D7E52BCBF3FD6BE27C9E3B397F8F6031226AB8B7378A779B4B2BA4B992AB9DF22C65F73FB587463CD612DA37F346517B94158A7195
Malicious:	**true**
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.=.1.3.2.8.2.3.6.7.8.1.0.9.6.6.7.8.6.4.....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.=.1.3.2.8.2.3.6.7.8.1.4.9.1.9.8.9.4.4.....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.=.b.4.1.8.8.3.a.6.-.0.5.c.8.-.4.d.f.8.-.8.f.8.a.-.b.7.3.b.5.2.4.2.c.c.9.d.....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.=.d.6.9.1.8.7.d.4.-.5.0.a.a.-.4.a.f.2.-.9.3.1.2.-.9.a.f.f.8.c.b.e.5.a.c.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.=.8.X.M.l.a.e.H.Q.X.Z...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.a.n.t.s.u.i.t.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.e.0.-.0.0.0.1.-.0.0.1.7.-.1.c.a.e.-.5.c.7.5.6.e.e.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.c.7.a.d.a.8.c.9.2.6.6.3.e.6.0.e.e.c.0.e.1.9.1.d.3.c.0.1.2.9.a.0.0.0.0.0.0.0.0.!.0.0.0.0.4.4.1.5.a.d.6.8.2.f.d.6.4.b.a.e.d.f.5.c.2.0.9.b.c.0.c.2.a.3.b.6.1.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA26E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 26 02:36:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18328
Entropy (8bit):	2.1675762975716704
Encrypted:	false
SSDEEP:	96:5Y8iv8Q/rL7FxvhGttQi7kQEGh5kzQtzfnO7W+tEA4pFM8h2+WInWIX4I4R5WM/X:xijrLJ5hrOoSkBW+t4f1h2XRpbDv
MD5:	520FEA3EDBB3884191A64436807E5978
SHA1:	F6D9E55C34495F399A728D8A85FDABE0BEB4A6F0
SHA-256:	602E379DE09F016EDC896EA3CD501FEEF42C9EBC3A3EF166F635439517893802
SHA-512:	FEEDFA4F5C9083C4902B5D7BA707FE58B4F21AB56BF0449175CBC14C5531F7962BDC6A87C339894A0E97343E6EE89A09D689B3BBF661D71B1D6DFC15DD99C4A
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA26E.tmp.dmp	
Preview:	MDMP..... .....CH.a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....?H.a.....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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4C1.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):	8288
Entropy (8bit):	3.700842112712281
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNip667uu6YJ4SU1NYWgmfsSUFCprt89bc0sf30m:RrlsNik67n6YmSUXYWgmfsSUncnfR
MD5:	A3C71DAB0C4F9D3701ABD6C6CC81A96D
SHA1:	0BA7CB3174C504A56862DEDC336CC85FFCBB11BB
SHA-256:	19019B9AFB7627FCC5F5E14896D0A717378133FD8FD70EC555E61EA875AE3776
SHA-512:	310C73C7947FA075E92FBE3F7EFF401797FAC80F2DA80BD97978487CB548E94EBD3EE1F7B0B7618BD4874E5318F27480C13F04760808A3571315EF4A21859AD5
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.>.5.8.5.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA752.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.46810111754898
Encrypted:	false
SSDEEP:	48:cvIwSD8zsctJgtWI97TWSC8Bm38fm8M4J2dmHaZFY++q8D6lEWHS4SESSd:ulTfcHYiSNxJsbkWHmvSd
MD5:	C0B7BE8F43E5D5B07E98B12FA8494262
SHA1:	C78D3DEA05DD8103994984A5FECB8E5626192716
SHA-256:	02908B5D7336F9E557EC47019B70EF5740D187E93DCA31C492CC71FDE16B0354
SHA-512:	6915CE1139F4E254EA532F1A39A95E0B68FAE9DD16D9EC749B9ABB6C0E2570E69A380C1F90991D79D5D26F3F93D945A501A88C62A68190BD2728895827C6A01
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="1270787" />.. <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\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):	4.215835067795784
Encrypted:	false
SSDEEP:	12288:0FLQX1Dz7+fmKMJLZgp291NAz3W/kZPmFrSWvj2cxF73CBkHecoDoG:uLQX1Dz7+fDMJLzaej7y
MD5:	C6F4263BA9B026736FAFE1454B900AC8
SHA1:	E206BC1022C6D5BF29CDC25CE3E060ADC9E67450
SHA-256:	3FE7B9A7B93C2E9125195071E903486106877B841531F455BBBE59C635DF13D6
SHA-512:	211C9D8F752BEF48F56F6CFEE5C8D9AF384653CD295E7C43C7C4E0410FF92A0E7FD53D317255D0EB2C55E72917D1316C75410391D10F38E5EFD5799B29C4AC1
Malicious:	false
Reputation:	low
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...vn.....+.....

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):	20480
Entropy (8bit):	3.4657596273367517
Encrypted:	false
SSDEEP:	384:JBD5VLIpnc8WTVgGNKDfUXfmndwK57rSaNtK:79tSc80VgGc4XOniKFNt
MD5:	AF4CE95146E6AA70B7395E57B882ACB0
SHA1:	9322A9F42AEDEAAA1AEA50F48619446FD0018B61
SHA-256:	A5F3E7009D4247F12856AE76688E8888A6B2C1371961074EAD2C88DEAEED7AE5
SHA-512:	05C140B6F25DD902576594907FB8C852A1E0704D271F0F2B1F6B9294577A91233530B38D4843E7436DCBF8728C1E367694044840FCE935B3F7C0E2FB1567BF42
Malicious:	false
Reputation:	low
Preview:	regfU...U...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...vn..... ....+HvLE.N.....U.....A..D..`....2.....`... ..hbin.....p.\..,.....nk,.??.vn..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .??.vn..... ....Z.....Root.....lf.....Root....nk .??.vn.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9827946846106395
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	8XMlaeHQXZ.exe
File size:	178783
MD5:	5643bf734d793e845166a228f3df83b3
SHA1:	4415ad682fd64baedf5c209bc0c2a3b619cf03e2
SHA256:	db79e0c2243229f8ba6a52deede597287b93801aa182af42f278542f31fb3324
SHA512:	f144347f7f636e64d2373a3f72a65c17534cc3692939ab6dfa071ddb2ec204801271440597ad327897638b032e1e3cfb3de4c23a4f5f1fdc293e1feca0fb433e
SSDEEP:	3072:ZZTL5fTrvJNV/8aoc42iA/ZFDqLQN3N2GvshHDiRCxc9Vlale6fWmPCuRE3B2:ZZJrrvJY1szqLQNgASGEcPleVhP430
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....0..... ... .@.. .....`@.. ...!... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x402000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE

General

Time Stamp:	0xFBDADAB2 [Sun Nov 25 08:54:10 2103 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
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x2000	0x1a000	0x8e00	False	1.00057768486	data	7.99485148323	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1c000	0x2000	0x400	False	1.0107421875	data	7.80837604511	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1e000	0x2000	0x200	False	0.81640625	data	6.18655348449	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x20000	0x4000	0x600	False	1.00716145833	data	7.87119921588	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x24000	0x2000	0x200	False	1.021484375	data	7.59715435366	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x2000	0xa00	False	0.305859375	data	3.58730721769	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x28000	0x28a000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x2b2000	0x106000	0x104c00	False	1.00037704324	data	7.99861729183	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.m8o02uE	0x3b8000	0x4c000	0x4a600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x404000	0x2000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Version Infos

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 8XMlaeHQXZ.exe PID: 5856 Parent PID: 2248

General

Start time:	18:36:47
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\8XMlaeHQXZ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8XMlaeHQXZ.exe"
Imagebase:	0x400000
File size:	178783 bytes
MD5 hash:	5643BF734D793E845166A228F3DF83B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 1916 Parent PID: 5856

General

Start time:	18:36:49
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5856 -s 212
Imagebase:	0xd10000
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