ID: 528756
Sample Name:
8XMlaeHQXZ.exe
Cookbook: default.jbs
Time: 18:41:33
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

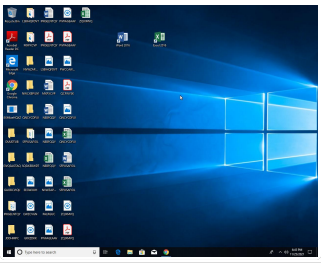
Windows Analysis Report 8XMlaeHQXZ.exe

Overview

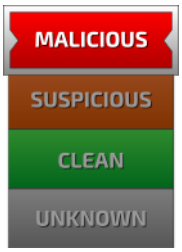
General Information

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

Most interesting Screenshot:



Detection

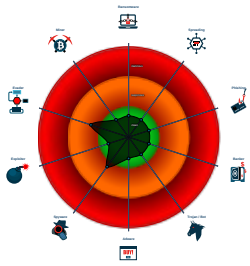


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- PE file has nameless sections
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- 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…
- Monitors certain registry keys / valu…
- PE file overlay found

Classification



Process Tree

- **System is w10x64**
- 8XMlaeHQXZ.exe (PID: 5476 cmdline: "C:\Users\user\Desktop\8XMlaeHQXZ.exe" MD5: 5643BF734D793E845166A228F3DF83B3)
  - WerFault.exe (PID: 6648 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -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:

Machine Learning detection for sample

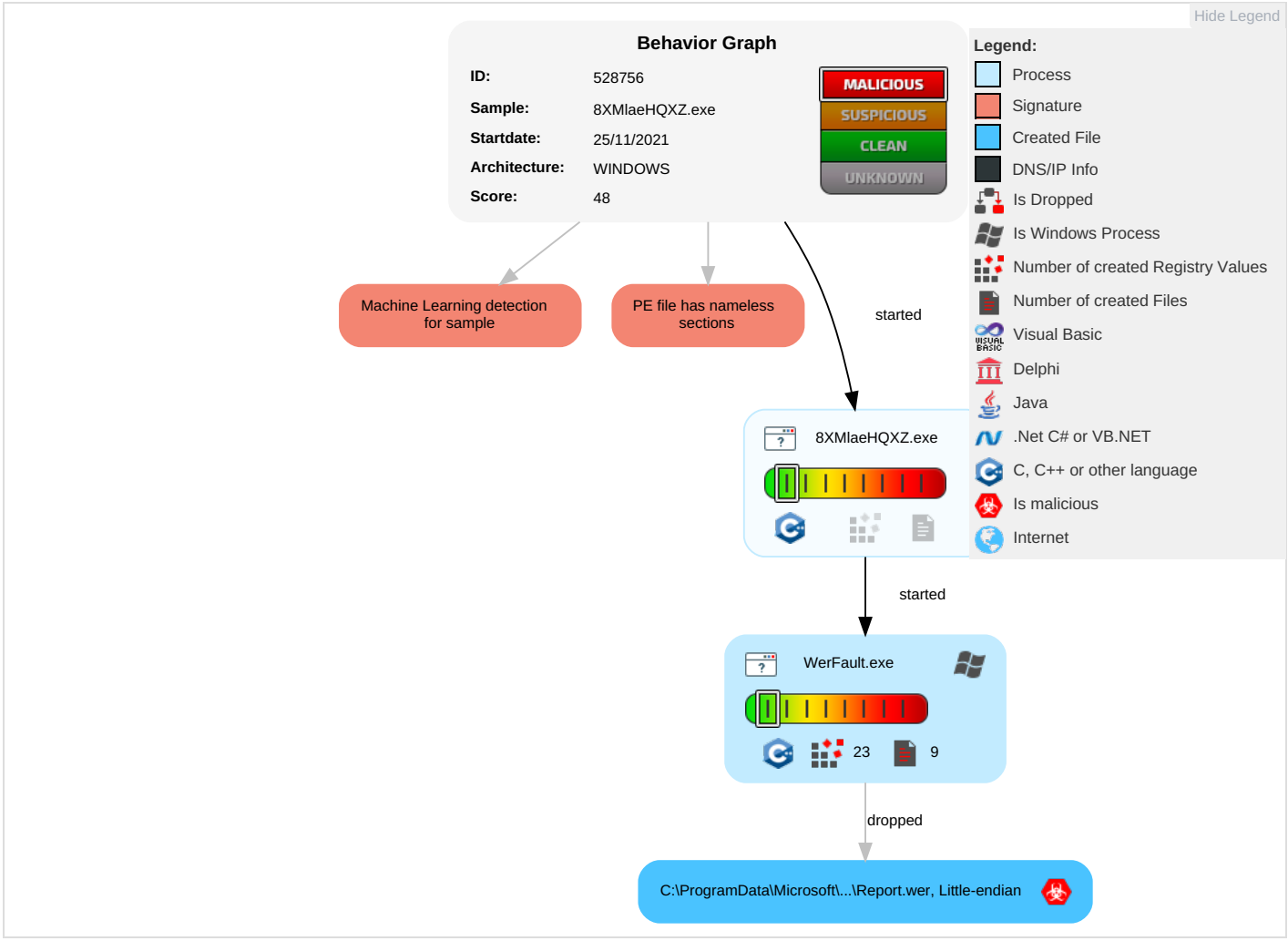
System Summary:

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	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	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	Security Software Discovery 2 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	Virtualization/Sandbox Evasion 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	System Information 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 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

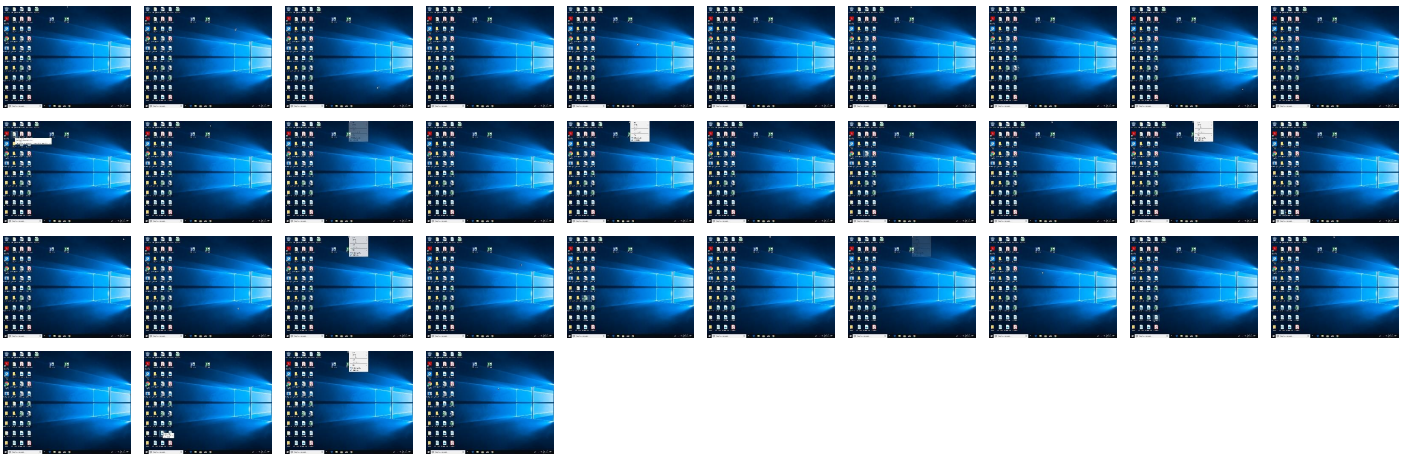
Behavior Graph



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	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:	18:41:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	19
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:	mal48.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 • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

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_18866dcb\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):	0.6304077596503469
Encrypted:	false
SSDEEP:	96:p04qtFcLEz4zH6DfhoDt7NflpXIQcQvc6QcEDMcw3DT+HbHg6ZAXGng5FMTPSkvt:4RoLHBUZMXQjE/u7spS274Itk
MD5:	F1DC039B554AB890258EC09467DB6C24
SHA1:	9DE682535714470077C857B83C0EE23239302C46
SHA-256:	1141883D1E50A954C4DBB6B053069AE03E791D311B897BD966AB40F6684C0508
SHA-512:	196BA3EF666620563FDE48E274A757F71EABD53E2B99EDB1CB8C977219018A72955A25C4C5007DECA68E6794C406AAF11F85706BC4C95E6273E6530BF9FF3594
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.=.1.3.2.8.2.3.3.5.7.5.6.1.8.7.4.3.6.2.....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.=.1.3.2.8.2.3.3.5.7.6.0.9.8.4.3.3.9.8.....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.=.8.3.d.0.9.4.5.4.-.f.2.6.d.-.4.a.f.a.-.8.3.a.f.-.4.f.8.c.4.5.b.d.e.c.b.7.....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.=.7.1.3.f.5.4.0.3.-.d.d.b.5.-.4.9.b.e.-.8.7.f.3.-.5.1.9.4.b.f.b.2.7.d.7.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.5.6.4.-.0.0.0.1.-.0.0.1.b.-.6.c.e.0.-.0.d.d.3.2.3.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\WER5561.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 25 17:42:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18328
Entropy (8bit):	2.1641229775618633
Encrypted:	false
SSDEEP:	96:558ib85GYJP5Hh5XF1Bi7kZdyvuqaRCMAEAmVLmtPi2WI9AIX4I455mtDD2:Ei4JRHLZOYyeRCEAHPiP5sVD2
MD5:	D8FEB31937852F9EE1C60A37EC4FC21D
SHA1:	05CECB87B4587ADB1845974F9D919263D82C6E7F
SHA-256:	E1680A8D9A1AFD37519000F198FFC2F6D2EC049998CBD8995F014089F4FB7DA8
SHA-512:	FFF5DA7DBD203A947BB4FCF91ACE98C13BBBAAA5D449CAD4702147D1826088C7FF85AEBA25D55E45ED23EFC37568E251783EACE9E1773AFB1A0D9310C1006EE
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5561.tmp.dmp	
Reputation:	low
Preview:	MDMP..... .....a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....d.....a.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER57B4.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):	8290
Entropy (8bit):	3.703152281919351
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXd6RuW6YroSUSc/gmfsSb+pra89bxgsfF7m:RrlsNiN6Rf6YkSUSc/gmfsS8xzfU
MD5:	A46B781979DC0E5691DFB61F9FBAF0C0
SHA1:	F4F732F491767AE66C5C19B781DF5C5758E0995A
SHA-256:	8262F032BE88AE2D934DF2E18E973ED5E91C9FAE257412B4CB65490E3D6698A4
SHA-512:	782A69263EAE0FCA12FDC3E95AAC31CDFDA2343EC316512195C18A7E4C6C4D21ADF253B0BCFC086F876B5CF01087562889D48AF5E35715905B986EEC8416862
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.>.5.4.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A16.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):	4.472291243795573
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9OjsWSC8B48fm8M4J2dmHaZFE+q8D6lEEHS4SESKd:uITfCNjFSNrJsokEHmvKd
MD5:	31D97342DF63ECDB23A535339416ADCF
SHA1:	18A56F887B7C70A5B417FF5E2C5B77F0FF637BBB
SHA-256:	A6286CC1F02B83AD8A0F326E2DEAADD54D45F5167E92D1CC174F522A5D9EAEE7
SHA-512:	B1D26825A656CDFC50602D59C97CD10AB5C445AB83F526384E5F8922A91D7947FA7DDB55C3344D1ED887C934778DD2882B6074181FE96B2FF4BB1DE95DBCF4
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="1270253" />.. <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):	4.2443178379206605
Encrypted:	false
SSDEEP:	12288:bQNromkFU+mGUMsSF+91cBMpmoQ3vycGLa3gDDJ3KCE7EMTc:MNromkFU+mJMsSYXm
MD5:	518E34E6AF9A3C808A4F2997E1553053
SHA1:	AAB369444CE6E9C6A4BE56CA8DE4E4D26AB47171
SHA-256:	93B9496270FBD85CAD54089F9C98A5547B9C32616716269CF5B8FB128238C23F
SHA-512:	3F6142F644E875E348835B17ABD739D072736743F0F36FF16A3F749C3F1DDD57EDEC9040DA9460BB0D895E4A670EA3E050086AA2E241CC5705523965B1D71969
Malicious:	false
Reputation:	low

C:\Windows\appcompat\Programs\Amcache.hve	
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm^...#..... .....=0..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.7636913015141964
Encrypted:	false
SSDEEP:	768:n/2JONT2Xd5sCgQwqhQ4g/eeDze6NYtjdGKw6ksK:0OkXNfQ9hDYc
MD5:	578A8605EBFB68DE0665EEFB540C7A12
SHA1:	DA5A7C98CD2F07DF3F466736E24260BBA2029473
SHA-256:	270BCDE1586464434CE203C339694E3C730974A218A8C61184E3C6868AF8E2BF
SHA-512:	B03E1D9AD5B5F608D838766C95F9E59B4358E9AF04813142DD61EDBCCE94B9C4C328F9071AA1FD516872643F28C3566EC6FBF8FB2F4D87EC60DB22422191745
Malicious:	false
Reputation:	low
Preview:	regfG...G...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^...#..... .....;0.HvLE.n.....G.....A]#..z.G_.=u..... ....hbin.....p.\..,.....nk,..s..#..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..s..#..... ....Z.....Root.....lf.....Root....nk ..s..#..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck...

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:	db79e0c2243229f8ba6a52deede597287b93801aa182af4 2f278542f31fb3324
SHA512:	f144347f7f636e64d2373a3f72a65c17534cc3692939ab6 dfa071ddb2ec204801271440597ad327897638b032e1e3 cfb3de4c23a4f5f1fdc293e1feca0fb433e
SSDEEP:	3072:ZZTL5fTrvJNV/8aoc42iA/ZFDqLQN3N2GvshHDiR Cxc9Vlale6fWmPCuRE3B2:ZZJrrvJY1szqLQNgASGEc PleVhP430
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .....0..... ... .@.. .....`@.. ...!... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x402000

General

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

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: 5476 Parent PID: 5480

General

Start time:	18:42:32
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: 6648 Parent PID: 5476

General

Start time:	18:42:34
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -s 212
Imagebase:	0x1180000
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