ID: 528754
Sample Name:
ZM80M76Nwv.exe
Cookbook: default.jbs
Time: 18:35:35
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

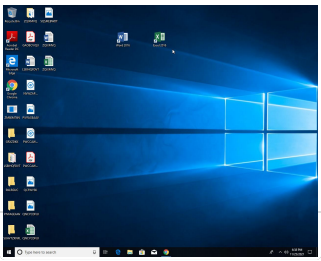
Windows Analysis Report ZM80M76Nwv.exe

Overview

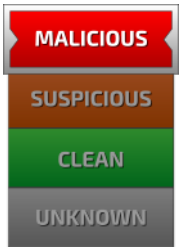
General Information

Sample Name:	ZM80M76Nwv.exe
Analysis ID:	528754
MD5:	3c93f57536f1504..
SHA1:	a7b4f2c0390ebc7..
SHA256:	493ea8db7e8d85..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

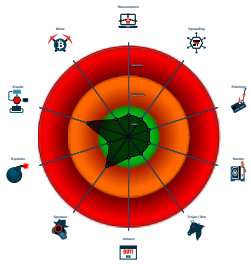


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- PE file has nameless sections
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- AV process strings found (often use…
- PE file does not import any functions
- One or more processes crash
- PE file contains an invalid checksum
- Uses code obfuscation techniques (…
- Checks if the current process is bein…
- PE file contains sections with non-s…
- Monitors certain registry keys / valu…

Classification



Process Tree

- **System is w10x64**
- ZM80M76Nwv.exe (PID: 796 cmdline: "C:\Users\user\Desktop\ZM80M76Nwv.exe" MD5: 3C93F57536F15046B52F4340EDBA42DA)
  - WerFault.exe (PID: 6392 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 796 -s 208 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

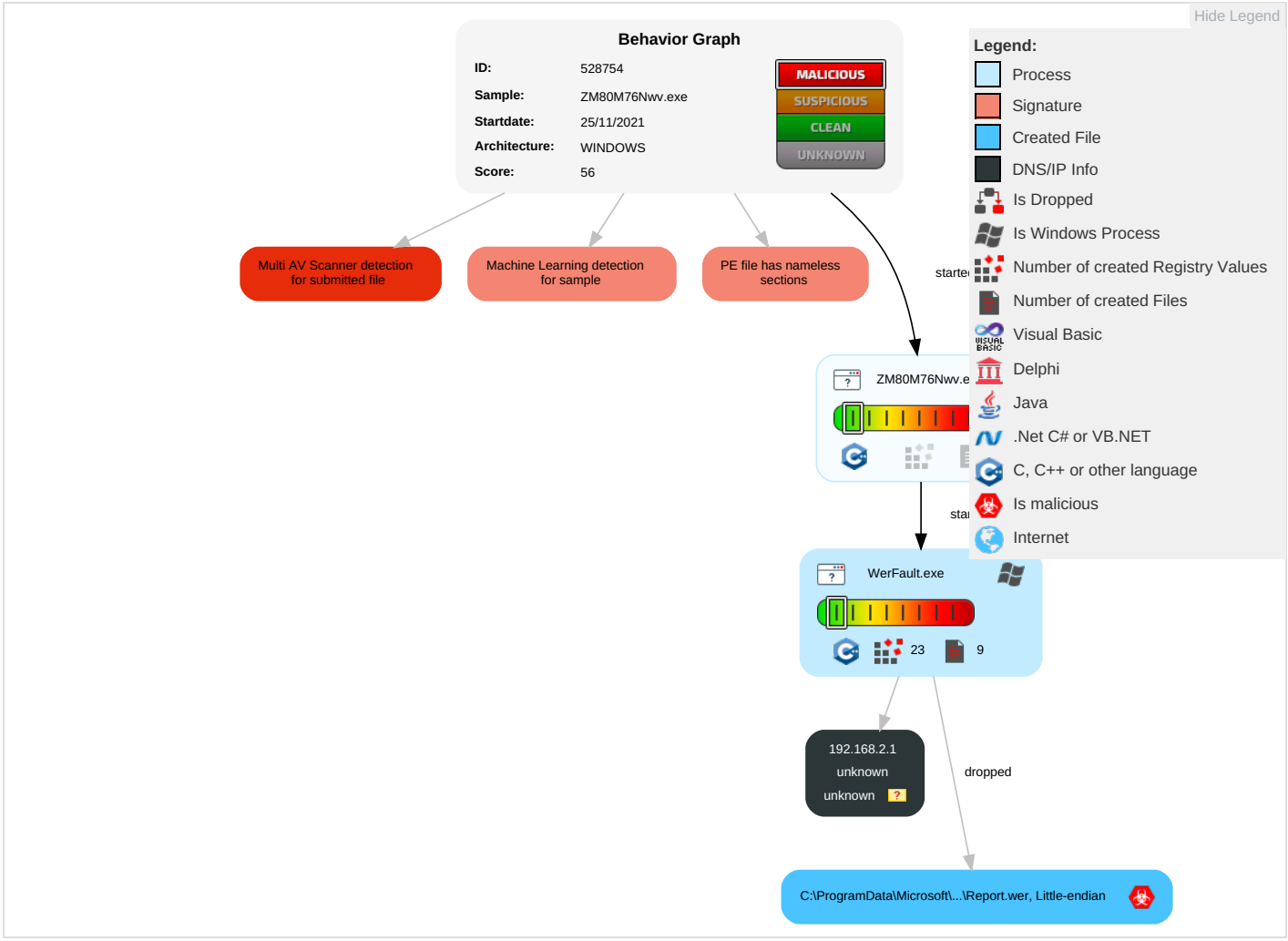
System Summary:

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	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)	Obfuscated Files or Information 2	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	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

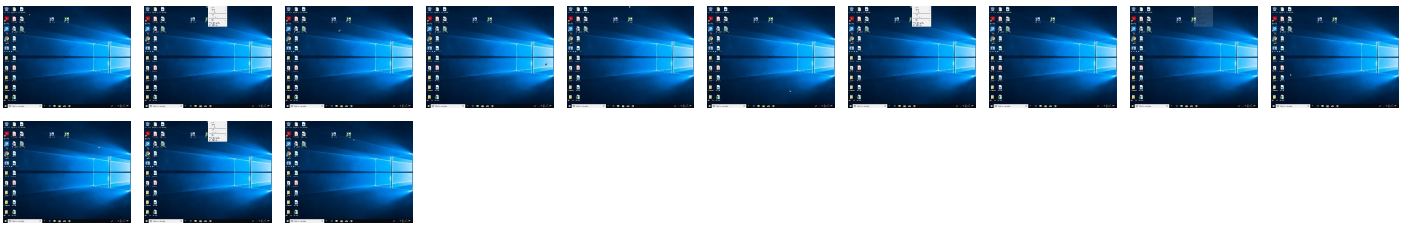
Behavior Graph



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
ZM80M76Nwv.exe	36%	Virustotal		Browse
ZM80M76Nwv.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

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528754
Start date:	25.11.2021
Start time:	18:35:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZM80M76Nwv.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:	18
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@0/1
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
18:36:48	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_ZM80M76Nwv.exe_16b24cad3a6a942c6be01f412bd01d9b9f91c865_350d898a_180624ca\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):	0.6253742074260888
Encrypted:	false
SSDEEP:	96:rKgFol6JhDsoL7DsNfBpXIQcQvc6QcEDMcw3DT+HbHg6ZAXGng5FMTPSkvPkpXmI:7Sl1/tHBUZMXQjE/u7siS274It0
MD5:	27A1475D9B2C2945E79FC17171E2E6F5
SHA1:	72C6910A056ACAADEEB5FE5982368CD10B2D67BD
SHA-256:	C2EA9CC7654314A0681105C0E63AAD352E22477E6F42436721C4BDA8A0C9514A
SHA-512:	89CF4277BBCA265DE36C357F87F2DB0A832190961D113EF70040BE2EFD5F3252D2FD04E18D71E8121E633F5F5530175FB34E4491FFE0FF9F7484AD433BA07C01
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.=.1.3.2.8.2.3.3.5.4.0.1.9.3.5.2.8.5.7.....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.=.1.3.2.8.2.3.3.5.4.0.6.8.2.5.9.2.1.8.....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.=.4.f.5.8.8.0.b.8.-.0.c.7.5.-.4.0.9.6.-.b.6.2.4.-.e.f.a.0.d.c.4.f.2.3.8.4.....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.=.c.c.8.b.9.3.a.2.-.1.e.1.4.-.4.d.7.b.-.a.4.f.2.-.0.8.4.7.a.0.e.8.b.0.2.a.....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.=.Z.M.8.0.M.7.6.N.w.v...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.3.1.c.-.0.0.0.1.-.0.0.1.b.-.2.1.c.9.-.e.2.f.f.2.2.e.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.3.6.5.7.2.b.b.6.2.4.6.4.8.3.c.3.b.7.7.1.0.e.7.1.6.7.4.c.d.5.4.0.0.0.0.f.f.f.f.!.0.0.0.0.a.7.b.4.f.2.c.0.3.9.0.e.b.c.7.c.4.b.7.a.a.5.b.b.f.b.b.6.0.5.0.3.a.b.a.0.8.9.5.5.!.Z.M.8.0.M.7.6.N.w.v...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1173.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4568
Entropy (8bit):	4.467661344802117
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9ptWSC8BC8fm8M4Js5TlFgFHo+q8RbmkWR5taKVd:ulTfTOcSN1JVIGIaKVd

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1173.tmp.xml	
MD5:	6BCF8B5212194E159B189848E0762F6E
SHA1:	DA66068E437C27294B6BA5B9797B499F86EEFCE3
SHA-256:	D2C1A1702D0A447898BA068A547FBCAD0E108FA06AC16BD5618EDA5662CF88A0
SHA-512:	53376297F9C665E1A7B707749285148345E6A3B8EADE188159AE3FD979033B1F7C7E20926B711D12E7793288ECF4F1DD20A035B290C97B74DE883510CC467FF5
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="1270247" />.. <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\WERC02.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 25 17:36:42 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18276
Entropy (8bit):	2.1636177054427765
Encrypted:	false
SSDEEP:	96:5V8il8+GYqP5vH40i7k2pSiqrRgAmfLSJAlzWlnWIXoIxy2dmO+7:AiZqRvHdOjSzRgAtAlVykK7
MD5:	0C23D61DF57CC229A64119FC95ADC6F1
SHA1:	6DB8161A1D4BD01A86539A9E7B360A33CE48C306
SHA-256:	955C2780E0B8E701BCC68127E8F0F6E343246DC51E54CE49F772E8772074767C
SHA-512:	A964ADC773A82DB3BFEA20A297BF8ED1E4228498BEF0F53CEEC7D2B6F5C82A73686C0BB8CC6345BD2A3F1A07A667D0D37A90A2FB296DF9C63CCC217FC5A91CE6
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2.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):	3.7002049520527085
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNid06x116Yr+SUfMYZygmfQS5+pry89b59sfyzm:RrlsNiO6x116YCSUfMYZygmfQSm52ff
MD5:	1B9CC6D0D7B9F8DC25FC0419188D6C2C
SHA1:	3B8C123B795BB63EA3B1664D5E0FF153877BFB6F
SHA-256:	4A79EF51651C81AC04C4EDD812AF29ECBDC9EBE6311E24834BBDB4D7F3EF36BC
SHA-512:	1DE4B457905188EC8C9151DFFECBA27B8DB179503558B8F7F22F73611F42164853B218108265D4BC9750607F08A537B26776427FD153EA747CADAD414AC7AF51
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.>.7.9.6.</.P.i.d.>.....

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):	4.241540396008965
Encrypted:	false
SSDEEP:	12288:c9DyRrVStP4YsYxoQT9p1g5rJ/fDwf8t/KzLvHH/mqxVM085:yDyRrVStP4XYxoAIJ
MD5:	E0EEA1D188D636649479AE4AE432E3A6
SHA1:	419529BF1A17DDAB5AA7E55505FAD428E476CEBF
SHA-256:	7457F1E84B2EB9821456BE108F03F137CD0A85A3FD15AC3F00630DF7FC5F3599

C:\Windows\appcompat\Programs\Amcache.hve	
SHA-512:	C80DC0BF5557C9DF774B9FCC26D007900828EB6CDF7D94B3F5AB3B8936FCADA8BFB496DEC4E9A7719A2D823AD20618C34B7FC42D36D9F5EE24D5AAA37B8E 616
Malicious:	false
Reputation:	low
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.6..#..... ....\..... .....

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):	3.363092622106805
Encrypted:	false
SSDEEP:	384:Ijp5K5SPv4KgnVVEeDzeF1NKZtj9T8G/w/1BMerP:Y3Kwg/EeDze/NYtjiG/w/Eer
MD5:	A700267FB783D1695EEBF6DA65C08B14
SHA1:	77999B3F85D8118E6053CFA8D9F91380FF94F710
SHA-256:	B3FD9DC64A3A88FF941CA2C11E109D8B9A3148E8A5B33EFB976FB69B2E987478
SHA-512:	87646DEF596EC87FEA39C6E6F9FC9487D2ED65A8BFACEF0EA1583355150C7B438657FAB803313FE9760EB6C2AA8DEB4E02C21EDD920C6C1D7584B7A7BAD80 5D
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.6..#..... ....\HvLE.N.....G.....E..o.. ..n%..... ..hbin.....p.\..,.....nk,..6..#.....@..... .....&...{ad79c032-a2ea-f756-e377- 72fb9332c3ae}.....nk ..6..#..... ....Z.....Root.....lf.....Root....nk ..6..#..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.997292727076848
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	ZM80M76Nwv.exe
File size:	236703
MD5:	3c93f57536f15046b52f4340edba42da
SHA1:	a7b4f2c0390ebc7c4b7aa5bbfbb60503aba08955
SHA256:	493ea8db7e8d8554d3f3c1dcbcf661dc5027892b02d262d fdcb58372e257191b
SHA512:	ef0370f11683092dd06e96b387e031a2966a90d3aad94fd 161442af23350b05244cf69798d3eda425b010ba662076 5cf41726cd99a489c625da359dfaee7793
SSDEEP:	6144:SOIiujNUOuPzzt0z6IVl0mEoP/RYjwYbylp:S0uvG yuGmzPSjwYbylp
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L.... 0.a.....4.....P.....P....@.....po..... V.B.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x425000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x61993087 [Sat Nov 20 17:29:43 2021 UTC]
TLS Callbacks:	
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:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x21fc2	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x23000	0x1306	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x25000	0xf000	0x7a00	False	1.00051229508	data	7.99401104881	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x34000	0x2000	0x400	False	1.0107421875	data	7.78065343968	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x36000	0x26966a	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x2a0000	0x40a000	0x3dc000	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6aa000	0x1000	0x600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.AqWcUFG	0x6ab000	0x4b000	0x4aa00	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x6f6000	0x1000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ZM80M76Nwv.exe PID: 796 Parent PID: 5200

General

Start time:	18:36:38
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\ZM80M76Nwv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ZM80M76Nwv.exe"
Imagebase:	0x400000
File size:	236703 bytes
MD5 hash:	3C93F57536F15046B52F4340EDBA42DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 6392 Parent PID: 796

General

Start time:	18:36:40
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 796 -s 208
Imagebase:	0xc40000
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