ID: 528755
Sample Name: g3r7OOQiri.exe
Cookbook: default.jbs
Time: 18:35:36
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

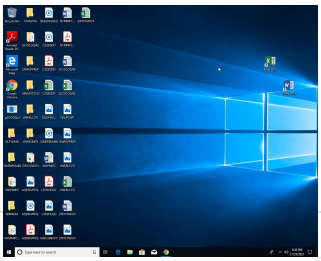
Windows Analysis Report g3r7OOQiri.exe

Overview

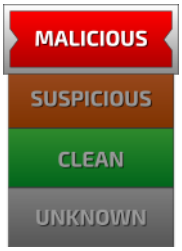
General Information

Sample Name:	g3r7OOQiri.exe
Analysis ID:	528755
MD5:	523928f18d5110a.
SHA1:	741c67937cc564…
SHA256:	aef6752333e99c7.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

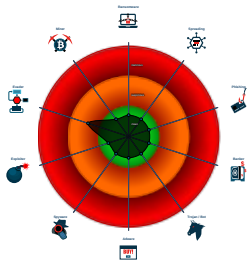


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- 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…
- PE file contains more sections than …
- Monitors certain registry keys / valu…

Classification



Process Tree

- **System is w10x64**
- g3r7OOQiri.exe (PID: 4440 cmdline: "C:\Users\user\Desktop\g3r7OOQiri.exe" MD5: 523928F18D5110AE858049B3E8E7FFE1)
  - WerFault.exe (PID: 6192 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4440 -s 224 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

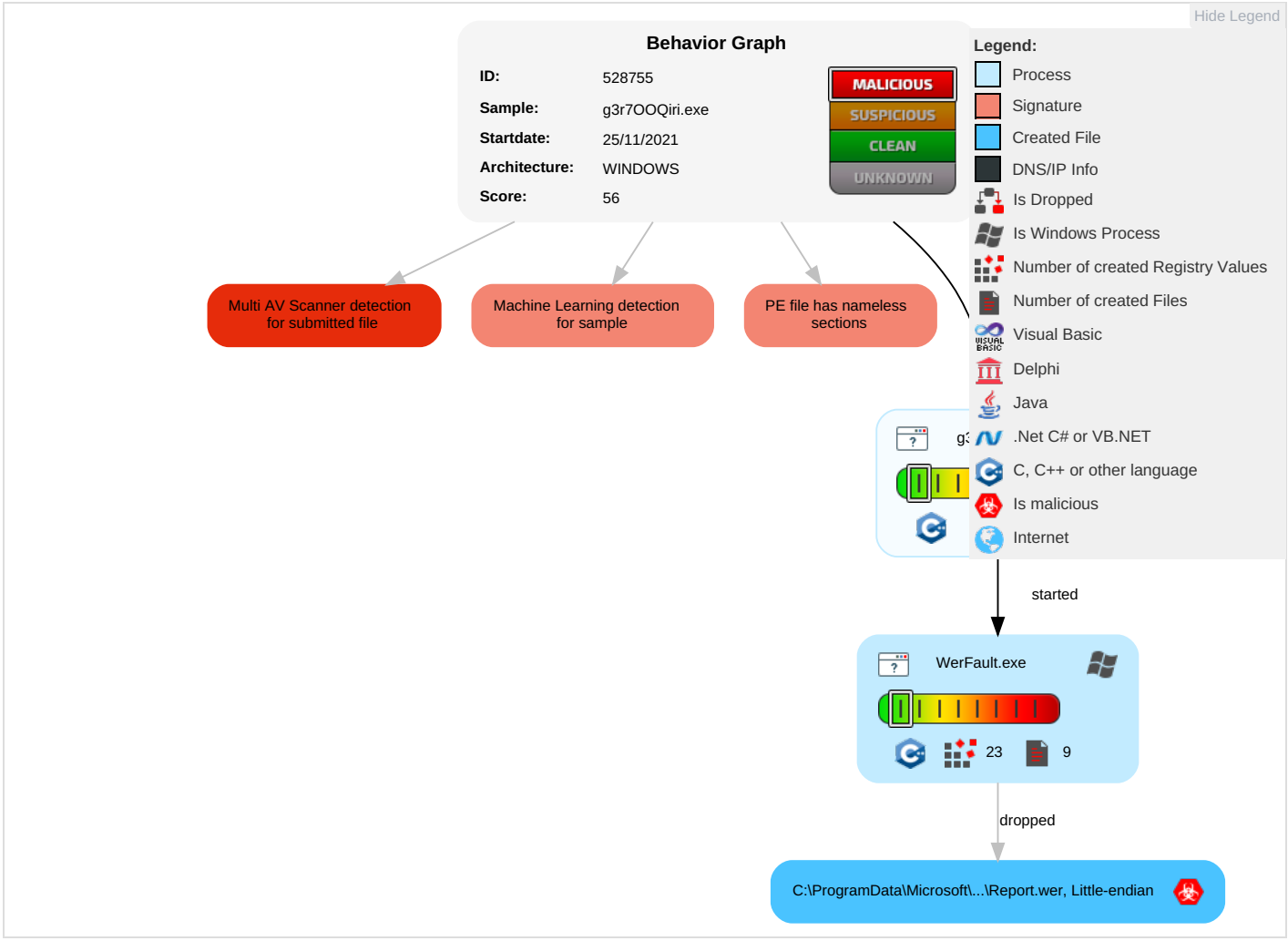
System Summary:

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	Query Registry 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	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	

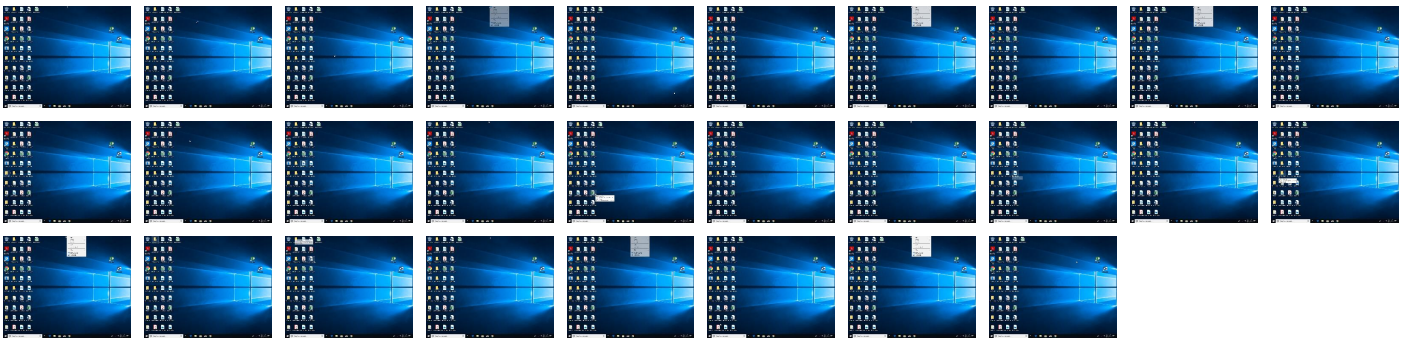
Behavior Graph



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
g3r7OOQiri.exe	15%	Virustotal		Browse
g3r7OOQiri.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:	528755
Start date:	25.11.2021
Start time:	18:35:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	g3r7OOQiri.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:	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
18:36:54	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_g3r7OOQiri.exe_6fba63fe01877644fdd43b959d3cffddf565b3_997a46bd_1936a0ba\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):	0.6241266377482673
Encrypted:	false
SSDEEP:	96:gUagF995paPhGd7DfmpXIQcQvc6QcEDMcw3Db+HbHg6ZAXGng5FMTPSkvPkpXmTM:Z9wHBUZMXYjE/u7sVS274Itgn
MD5:	E7B022F1F7AE6337AC0572AA09BF3083
SHA1:	EC70AE5E4A85344E16C14B8E7E56DC869050F1B8
SHA-256:	E28673B9C8FBFAB5DC3DBB87271E4C42DB809DAD74AFB8D2ED7018E58A820536
SHA-512:	5A099E82D9D18B4A0B4B5809F417DF1342407BAA6370617B13285B60F8D2ADC5B048BCED154DBD21A35E7055535A21EE7BF26E94737246911A435D202388F7E2
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.=.1.3.2.8.2.3.6.7.8.0.8.1.1.8.0.7.1.1.....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.=.1.3.2.8.2.3.6.7.8.1.2.5.2.4.2.8.3.9.....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.a.b.a.a.9.5.9.-.4.9.c.0.-.4.c.8.e.-.a.9.5.b.-.b.8.7.7.1.0.0.f.9.9.3.6.....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.=.6.9.7.4.6.7.2.3.-.c.5.3.9.-.4.6.e.3.-.9.f.5.7.-.a.1.f.2.9.3.e.1.8.8.0.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.=.g.3.r.7.O.O.Q.i.r.i...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.5.8.-.0.0.0.1.-.0.0.1.6.-.a.d.f.1.-.7.7.7.3.6.e.e.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.5.4.b.8.c.e.2.7.b.f.7.1.f.1.5.2.e.9.9.6.5.f.b.5.3.3.3.6.8.c.f.0.0.0.0.f.f.f.f.!.0.0.0.0.7.4.1.c.6.7.9.3.7.c.c.5.6.4.d.2.d.0.b.b.9.8.9.a.b.0.9.9.9.7.f.f.d.6.b.e.1.2.9.6.!.g.3.r.7.O.O.Q.i.r.i...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER891B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 26 02:36:48 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18328
Entropy (8bit):	2.166593177098292
Encrypted:	false
SSDEEP:	96:5L8iR8Q/fQgasF+WllJJ66i7k4gENmXAOUG0RnsjoWInWIXQI4+Eh8hPPt:iiRIgpF1p66OT8AXGqnyt+EO9Pt
MD5:	D924F58BF55B37DE23085C44048FF3BD
SHA1:	CC8AD18688F236F9957C58E869B6E5D2F474464C
SHA-256:	FECC421D70B00F890386F7C0A8F7E8F3AAED8A18E8C45B2CB6CA85E240207F50
SHA-512:	DD3DCC508B10FCB1FEC75520736208AB20C3A47C6B09E719ADD2509DFE308AD0AE43C7E082FE1CC791CE0D59F96121502D8AA4D376E4574B77C16C4E998F6F
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER891B.tmp.dmp	
Preview:	MDMP..... .....@H.a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....X...<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\WER8B6E.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):	8286
Entropy (8bit):	3.695614090084149
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi376rQN6YIXnSUVpgmfdS5Cprw89bs6sfLkm:RrlsNiL6e6YYnSUVpgmfdSMsZfN
MD5:	1406063F6C66EE318CDF78B6F9D8FB66
SHA1:	68E47F73AAB46D755A6F86CE3A9CF98FE3367656
SHA-256:	41134DC1E40CFE771491DC9519A5737C79CE979974E0F2D42F37430070E620E1
SHA-512:	63398A56AE5DEA31B6EDBAE19B0A3264920E7D9A24FFC35F58C2A8D01CF7BE30E45B00B9B05E19599EDEC053929B09F609046083DC149AE81EC813BEC26335A9
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.>.4.4.4.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E5D.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):	4.465510694824119
Encrypted:	false
SSDEEP:	48:cvIwSD8zsctJgtWI9OwWSC8BJe8fm8M4JwZfdIhBAeFyG+q81rutDEqI5Rr8d:uITfcH1JSNHbJwVcoqIDr8d
MD5:	0B42EC7AD7DF8FE58407ED4198AD55EA
SHA1:	C0EC8072E569BBBA1756A276136297E6EB40A05F
SHA-256:	C77700D60028760F0E0C792E077A9CC52A9E0F09CC87CBC9DF192F04C815A536
SHA-512:	B05AD198C0D3E6C645B8AF0A9DF545ED98947B7F5ACE65B73245AD36C04A9C521FCAC39F72A6A501F0C2BDD4124B8CBA0EA95CA02A50B314A20795436F55AEFF
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):	4.2641981063323025
Encrypted:	false
SSDEEP:	12288:JNmVShTWOamHq2wTzTe7qkYoUADCNUwQZBqF+36puLUBM8Boo5DPmMBp:3mVShTWOamHq2wTW5DIp
MD5:	5C1D4AF108D8FE202B86AA586DE86368
SHA1:	0F092E390334D4F55897C279FF5534D4CACFF6C5
SHA-256:	60B1E987837AB13F91A55781305B813492CB9676447CA62B8CE4877FE0E5A254
SHA-512:	B68EAFEABD02DCC9502D0B3F06F0A18478EB11CCE0656E35AB949AC32FAE9AD1BD67D104032BE1C93AE7DFE5CA0CDD962C950F77FB5CD44BE4E13DF061B54811
Malicious:	false
Reputation:	low

C:\Windows\appcompat\Programs\Amcache.hve	
Preview:	regfQ...Q...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.rmtm2.'un..... .....#(..... .....

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):	24576
Entropy (8bit):	3.796754391984824
Encrypted:	false
SSDEEP:	384:T04s5LZrdVdXx5hQp8XXtnxOf2oOPmxwp75GjZmGO+sDTTess5N5mBWMB:whVrFXxYpYgf2odxwplWmGO9TeNN5yWM
MD5:	521D69228F614DC472693EDFA7BC448B
SHA1:	FA6E0C7F95E5FCACBBC4B5D2605E49B925AFF33B
SHA-256:	074D30DFB1C6B4D3DBC22701D67B99AFEDEB43C5D41689E5EE5FDA7C5D003E5A
SHA-512:	B218B5A5346CD7F5B12DC176DE16E38427FBA20573530D3E3F642D2470766C7BE0755DF2810FFBFED130CA400B412CF47FEC4C8DDAFD3F288900F355B94DD5 1
Malicious:	false
Reputation:	low
Preview:	regfP...P...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.rmtm2.'un..... ....#(HvLE.^.....P.....g..".....8vcc..... ..hbin.....p.\..,.....nk,...*un.....h..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...*un..... .....P..... .....Z.....Root.....lf.....Root....nk ...*un.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.991066870441378
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:	g3r7OOQiri.exe
File size:	87559
MD5:	523928f18d5110ae858049b3e8e7ffe1
SHA1:	741c67937cc564d2d0bb989ab09997ffd6be1296
SHA256:	aef6752333e99c747f01eb9345f03ccbc6a162054dfb705afd7c3040e8219e45
SHA512:	b7adc70f18711dbab88da4dce3e81cf377a7877823cf0b3e3b3f587ad804079d8803f904a5a82f48450b246e57dbff60f1860d6eb63b8aeb518b4b491ca0dd69
SSDEEP:	1536:XX0in1aqQPp3k1LQ87rqMH5mkmIyE5cKFOc21Liirwg0BvnfmnPS18S0xIGFD:HLaqaSP7uUlkmMrc1FrwxB3mnK18S4RR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(.$tl.wtl.wtl.w`".vyl.w`".v.l.w`".vbl.w&<.vel.w&<.v`l.w&<.v>l.w`".vql.wtl.w(l.w.<.vul.w.<.wul.w.<.vul.wRichtl.w.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	

General

Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x61964D82 [Thu Nov 18 12:56:34 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:	

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x22000	0x11a00	False	1.00042941046	data	7.9974253827	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x23000	0x2000	0xa00	False	1.004296875	data	7.92908677458	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x25000	0xf000	0x6200	False	1.00097595599	data	7.98297122027	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x34000	0x2000	0x400	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x36000	0x8e000	0x71a00	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xc4000	0x2000	0x1600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xc6000	0x1000	0x200	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xc7000	0x4000	0x600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xcb000	0x1000	0x200	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xcc000	0x1000	0x600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xcd000	0x1f4000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x2c1000	0xc0000	0xbec00	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ShqA6WN	0x381000	0x4b000	0x4a600	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x3cc000	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: g3r7OOQiri.exe PID: 4440 Parent PID: 1688

General

Start time:	18:36:44
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\g3r7OOQiri.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\g3r7OOQiri.exe"
Imagebase:	0x400000
File size:	87559 bytes
MD5 hash:	523928F18D5110AE858049B3E8E7FFE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 6192 Parent PID: 4440

General

Start time:	18:36:46
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4440 -s 224
Imagebase:	0xb10000
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