ID: 528755
Sample Name: g3r7OOQiri.exe
Cookbook: default.jbs
Time: 18:41:55
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

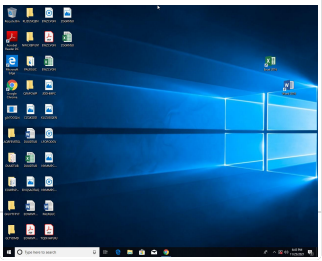
Windows Analysis Report g3r7OOQiri.exe

Overview

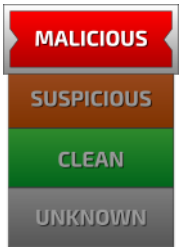
General Information

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

Most interesting Screenshot:



Detection

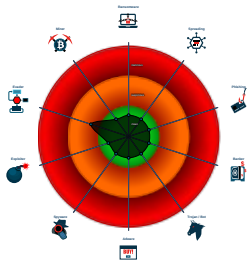


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- 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…
- PE file overlay found

Classification



Process Tree

- **System is w10x64**
- g3r7OOQiri.exe (PID: 6240 cmdline: "C:\Users\user\Desktop\g3r7OOQiri.exe" MD5: 523928F18D5110AE858049B3E8E7FFE1)
  - WerFault.exe (PID: 6352 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6240 -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

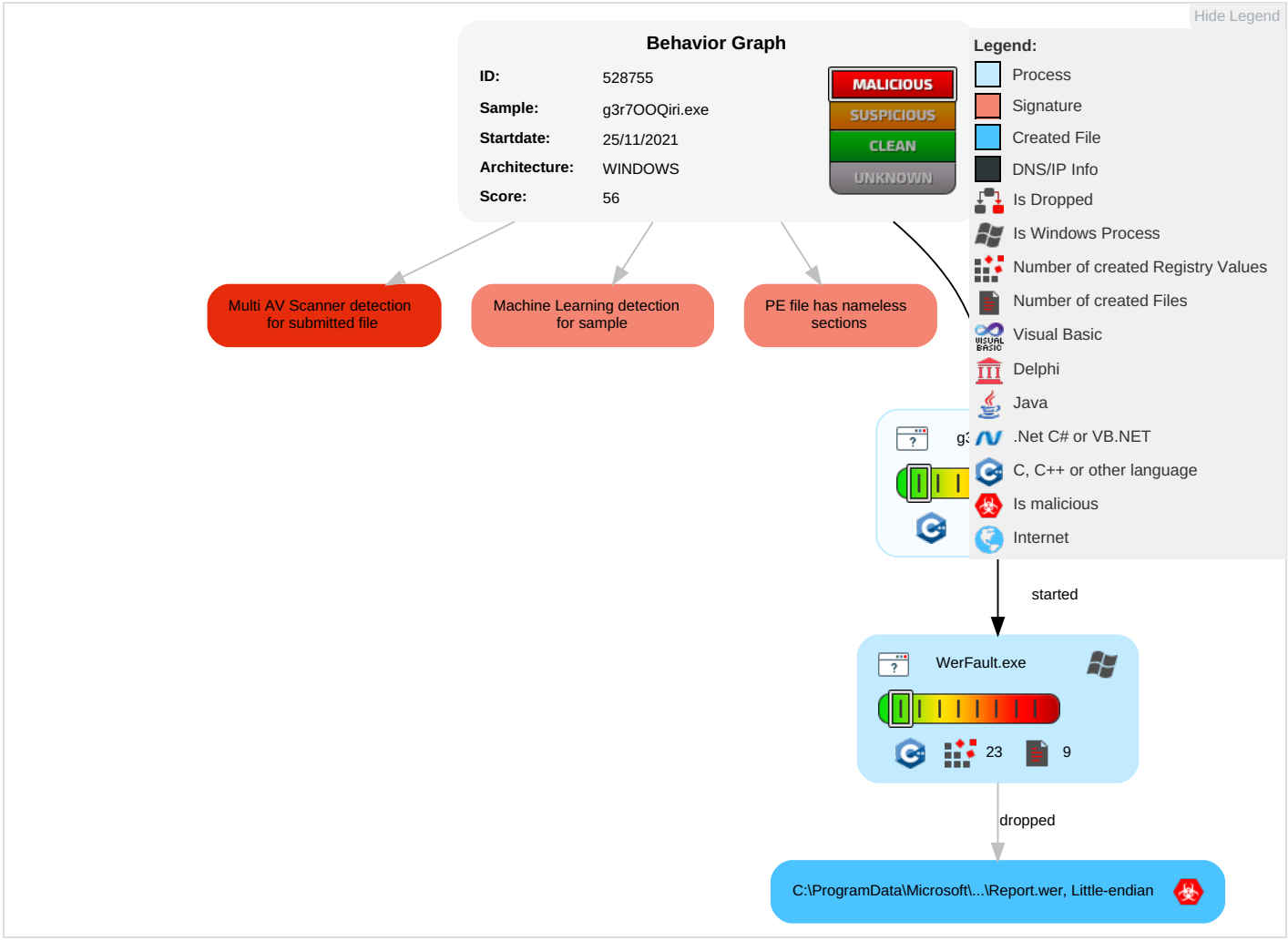
System Summary:

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	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 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	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

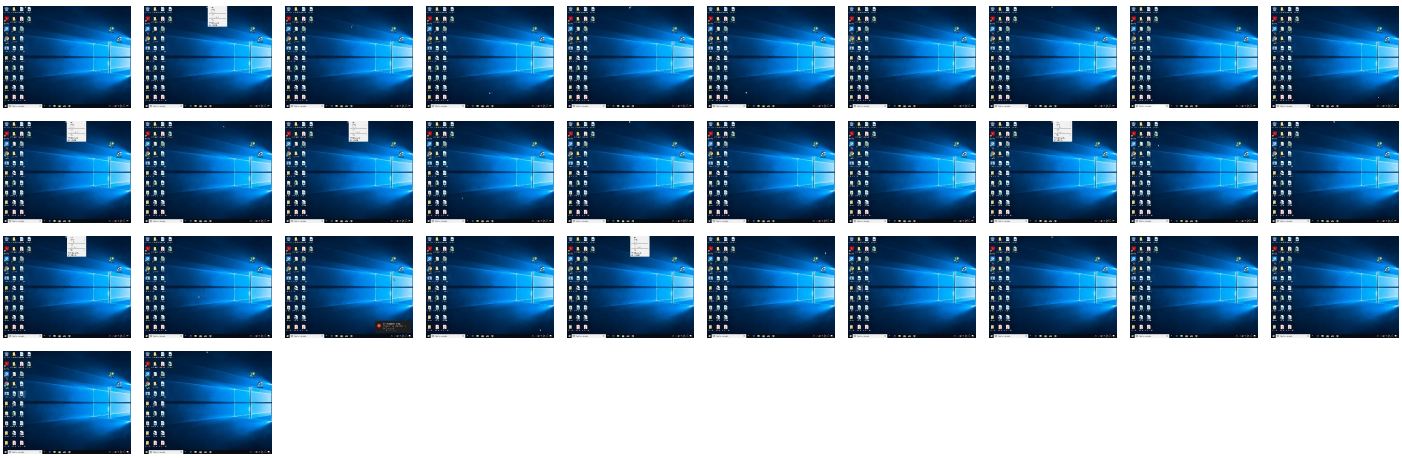
Behavior Graph



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:	18:41:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	33
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 • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
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_g3r7OOQiri.exe_6fba63fe01877644fdd43b959d3cffddf565b3_997a46bd_19e22886\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):	0.624169887502897
Encrypted:	false
SSDEEP:	96:oRFFmpuPhGd7DfmpXIQcQvc6QcEDMcw3Db+HbHg6ZAXGng5FMTPSkvPkpXmTA/fn:UnAEHBUZMXYjE/u7s2S274Itgn
MD5:	B784AACD43F79C49A57EC46983BE0019
SHA1:	EAD3F19D6ACD6B372CF087C40E82CB37BCFFF689
SHA-256:	C943ADD758E4C4746CB2058CE29CAF15C643D2E50601C383DEE34F07E518C54A
SHA-512:	7AC8FA5B57577E574932A2282FC90306393CC16A8EE3C405E88AA9B85AF0F76F8B67D1F3A482328FFD55A6DB70A2A3DC36035439DBC531756DD2B484CD14AC9
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.=.1.3.2.8.2.3.6.8.1.7.5.2.4.4.0.8.4.9.....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.=.1.3.2.8.2.3.6.8.1.8.0.1.0.3.4.4.6.9.....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.=.4.d.4.c.6.5.0.c.-.e.c.7.c.-.4.0.6.6.-.a.4.6.b.-.9.e.5.f.8.9.f.5.1.0.9.4.....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.=.0.a.e.7.0.a.b.0.-.b.4.7.b.-.4.e.3.7.-.b.1.3.b.-.6.f.7.b.3.b.d.7.0.4.a.4.....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.=.0.0.0.0.1.8.6.0.-.0.0.0.1.-.0.0.1.6.-.8.3.1.6.-.7.a.4.e.6.f.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\WER1108.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):	3.693971038550539
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiDn6f6YIpSUESxgmfdSrCprE89bjMsfIhm:RrlsNiD6f6YWSUESxgmfdSSjffz
MD5:	14EC749862F0329718E02BF66F378BB1
SHA1:	6176C03E85D0E000CCF2BB1F6BE1B2D09A7E9E45
SHA-256:	A1FA8E54918F5006D7B6A912B285E9C953DE8DE9F5E8BBEF587F0479623366BE
SHA-512:	1FA1762E5047B91FDB081FEDB0DCE6B0EF712F416134C5645822A9F9B03466420F78668511A0675732053753E3B65B3E28C68A2F5FC4A140D7D6B09684EA1A52
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1108.tmp.WERInternalMetadata.xml	
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.>.6.2.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1435.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):	4.460260654569432
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtWI9PPWSC8BK8fm8M4JwZfdIhBAeFn+q81rutDEiy5RrEd:uITf5keSNpJwVooiyDrEd
MD5:	3DB1275D4EB50E5389ED057C99B628E9
SHA1:	9F8F3C50BB81571FBCB135A43566D1CF6F85FED4
SHA-256:	5303785AD746A58F565F7CC9D46244472093F7ABAE342A3DDCA1318279DE9D17
SHA-512:	97BD561189897CCB5F51E86AF3C6550609473A9C2023818B6388EB9ABF88FF10A70595D15E035020887F3F5A6B6D798BE5EE34A852FFEE887C6D8673AB2CCA61
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="1270793" />.. <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\WEREE4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 26 02:42:55 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18328
Entropy (8bit):	2.16646607239918
Encrypted:	false
SSDEEP:	96:5j8il88Q/oasdrLPS6i7kQJoudmXAptGbVOasf7aWInWIX5x4H5xESrDk:Wi2opRTS6OZousAjG5zsDjHzESrDk
MD5:	2973008C3464AE66CCEC3BA9DD8A97EC
SHA1:	6E00C8E0D090C1ED347DF49FDE2022DBE394399D
SHA-256:	FD8D203E1AFC12FE0B776F6E757EDE43A9CD3C1DB0600E21239CDEF7BFC623DD
SHA-512:	5C1B929FBC1CCAC2C6D99E49DCF10255DF75F62E7BE113A87B6787FF9D82C3F5D3651C6EA444A1CB1BCB54675135D215650E512EEEBCD8CC82F80C16CE26A4F
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....I.a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....`....I.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:\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):	4.2637283990813595
Encrypted:	false
SSDEEP:	12288:GRFGuNDdXdVhbFmV7AHDViWtnwY9BNMKomT9jKlY6XvtYGDQNdDZq/x5:oFGuNDdXdVhbFmV0YHh5
MD5:	F48A7268FA38A81C30F2F9CE74EF1985
SHA1:	3F77B27E0FE3A74D414871952BDE353C440602A8
SHA-256:	6555E612399340EF23D73E46EA986DEDDA059C9A716A22F89DF12B0EF172BBD8
SHA-512:	0380B16E9C17D335883A68374C9E8A150A8FD7AD095EA63774BF0915219C10525FBBC71A4626F1B05785485012379C8486289E1BB5B8AE37803D30D959B91840
Malicious:	false
Reputation:	low
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.rmtm..2Po.....6.....

C:\Windows\appcompat\Programs\Amcache.hve

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):	3.7958907170487497
Encrypted:	false
SSDEEP:	384:YIN5VZrd3dXx5zQp8XXtnxOf2oYPmxwp15GjZmGOGDTTeA5N56BWMN:TTPrzXxGpYgf2ojxwpfWmGOMTeEN52WM
MD5:	08587182DC2B50DAEA202633D1565982
SHA1:	4F69E6018756534971FEE4EF523B4DB70B8EBB4A
SHA-256:	A1C8DCB43B205EAF612BBF7FCD8DEC4BDBA8247D83D9C2C5E383B2133DF57E8F
SHA-512:	6456F3FB7977620C26B5DE021AD895FA4753933E3E0223E805A07E13215164BCF6A012BEC1AE5D354F4169626D6D2DB175C5DB8BECDDFDAE7803740CE4C55CB
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.rmtm..2Po..... ....6.HvLE.^.....P.....V*&..)w`..*..d..... ..hbin.....p.\.,.....nk,...2Po..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...2Po..... .....P..... .....Z.....Root.....lf.....Root....nk ...2Po.....}..... .....*.....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: 6240 Parent PID: 5228

General

Start time:	18:42:51
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: 6352 Parent PID: 6240

General

Start time:	18:42:53
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6240 -s 212
Imagebase:	0x10c0000
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