ID: 800790
Sample Name:
cambridge.shareholdersuite.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 19:53:29
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

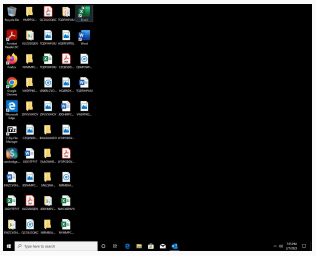
Windows Analysis Report

cambridge.shareholdersuite.exe

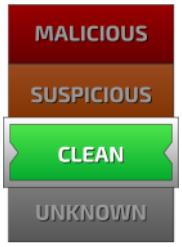
Overview

General Information

Sample Name:	cambridge.shareholdersuite.exe
Analysis ID:	800790
MD5:	36a2a6c6f6ba3..
SHA1:	b5dbb9cef3950..
SHA256:	d7e7a93d2642...



Detection

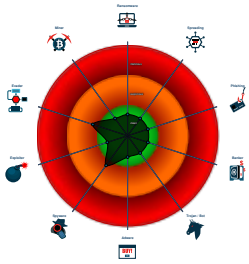


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Uses 32bit PE files
- Queries the volume information (nam...
- One or more processes crash
- Checks if the current process is bei...

Classification



Process Tree

- **System is w10x64_ra**
- cambridge.shareholdersuite.exe (PID: 6440 cmdline: C:\Users\alfredo\Desktop\cambridge.shareholdersuite.exe MD5: 36A2A6C6F6BA38708F501ACCE1176F1C)
  - WerFault.exe (PID: 6592 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6440 -s 808 MD5: 28D356B668C66115EA55135D24EEFB2C)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

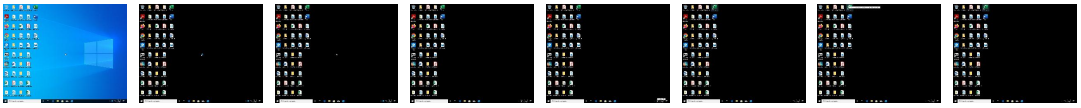
Mitre Att&ck Matrix

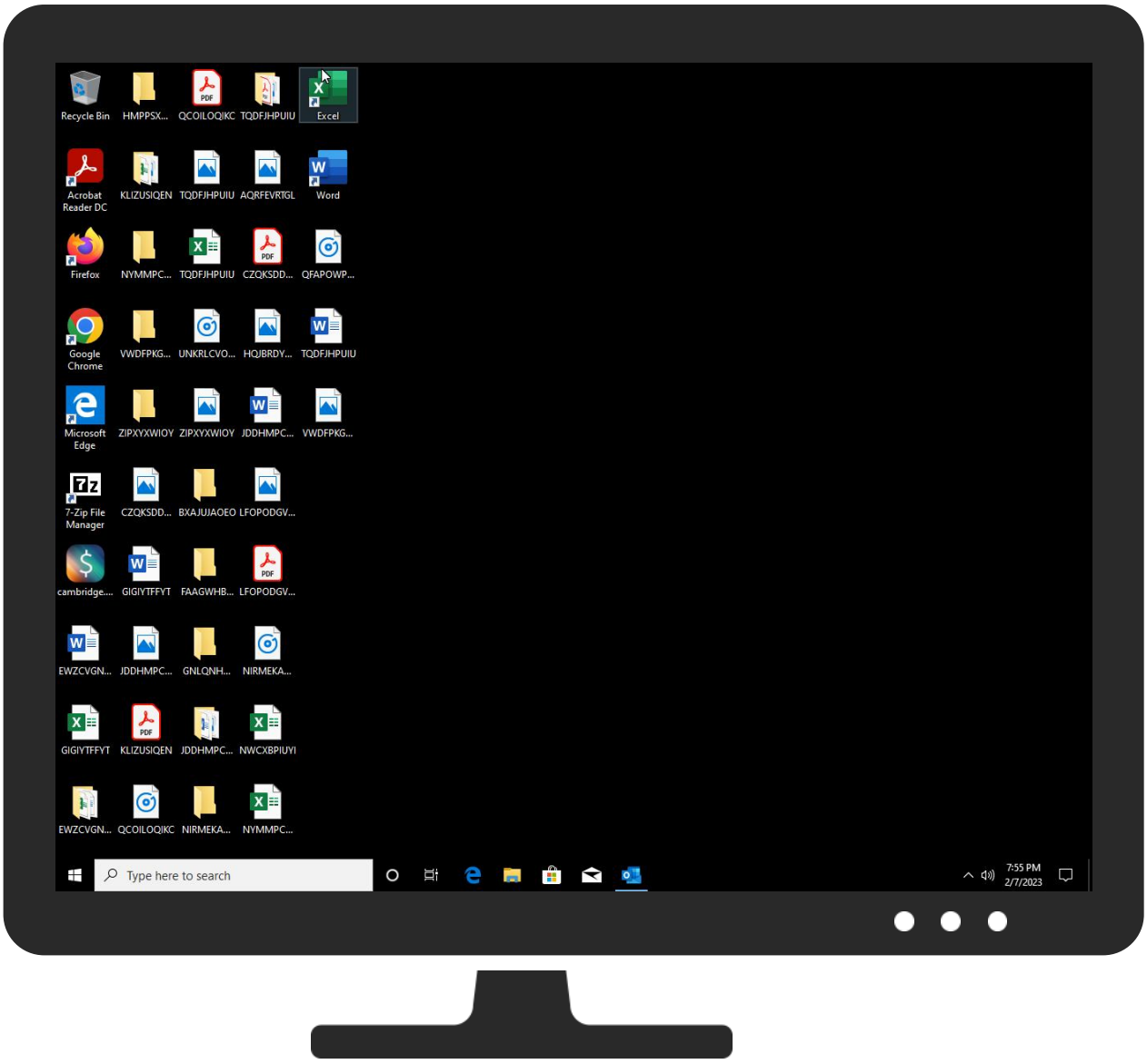
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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
cambridge.shareholdersuite.exe	0%	ReversingLabs		
cambridge.shareholdersuite.exe	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

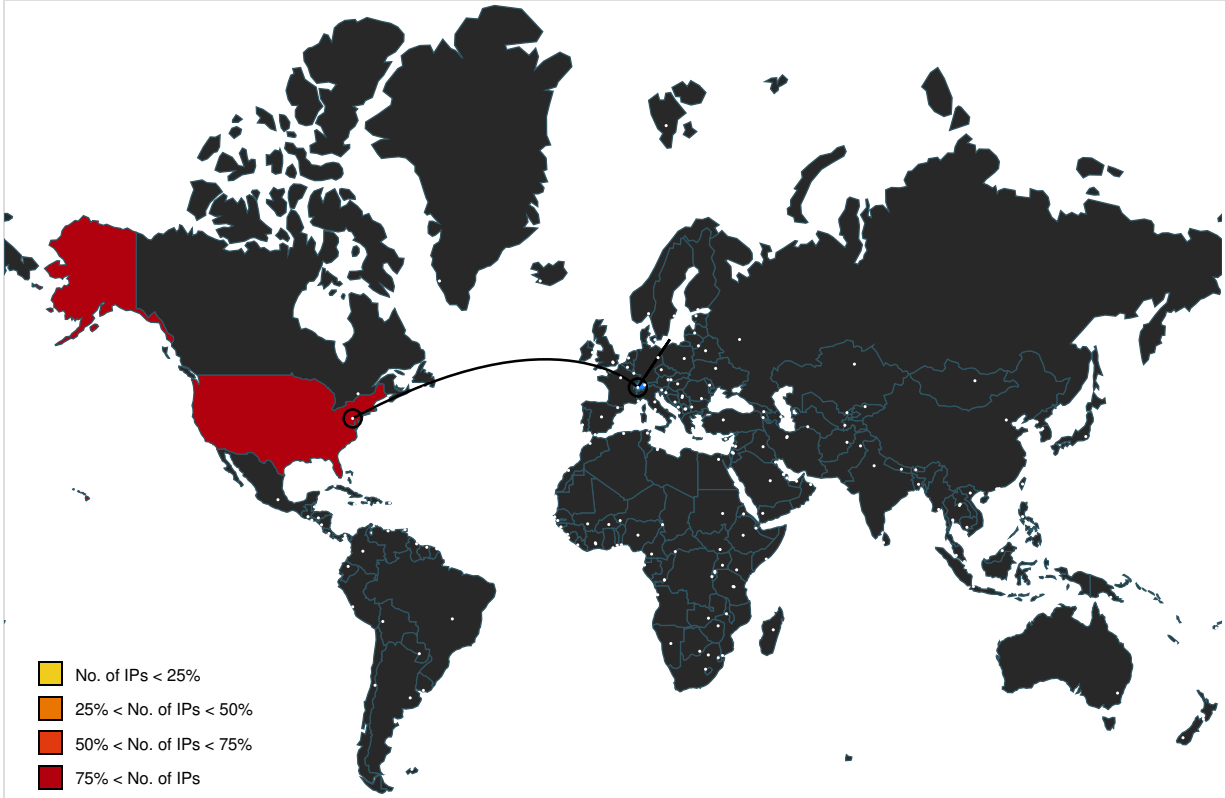
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.189.173.20	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800790
Start date and time:	2023-02-07 19:53:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	7
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout

Sample file name:	cambridge.shareholdersuite.exe
Detection:	CLEAN
Classification:	clean2.winEXE@2/6@0/10
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, SIHClient.exe
- Excluded IPs from analysis (whitelisted): 40.126.32.76, 40.126.32.140, 40.126.32.74, 40.126.32.68, 40.126.32.134, 20.190.160.20, 20.190.160.17, 40.126.32.72, 20.189.173.20
- Excluded domains from analysis (whitelisted): prda.aadg.msidentity.com, slscr.update.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, watson.telemetry.microsoft.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Report size getting too big, too many NtSetInformationFile calls found.

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cambridge.shareh_b0b1b6854f979e9e27d3f079aaadcb4db67090f2_dd0f84fe_82132d7a-9be1-4710-9e0b-377f233cb68f\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8917153966165613
Encrypted:	false
SSDEEP:	
MD5:	3E2D5B3851F33FFF32AEA5C7B4FDEECF
SHA1:	6770424C9C5627FC61E0086EEAE01BE40029EF4B
SHA-256:	1CCB3014B0CA0A72A27BAEA4AD8126258261DDDF7534ECCBE9713463A31B857D
SHA-512:	CCC84B359C56F135E86F77B01015BE3CA45B68433E51D06BCC3A1637F5156A5489BE3951B73697057F9CEEE4B4D7EF12EF33CE780DCF5B3C2EA7C2EA77C23667
Malicious:	false
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.=.1.3.3.2.0.2.6.9.6.4.9.3.1.4.2.7.2.3.....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.=.1.3.3.2.0.2.6.9.6.5.0.1.1.4.2.7.4.3.....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.=.8.2.1.3.2.d.7.a.-.9.b.e.1.-.4.7.1.0.-.9.e.0.b.-.3.7.7.f.2.3.3.c.b.6.8.f.....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.=.9.e.0.b.7.d.4.e.-.f.d.3.5.-.4.2.1.f.-.8.b.7.a.-.c.2.d.a.3.9.8.a.9.c.9.c.....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.=.c.a.m.b.r.i.d.g.e...s.h.a.r.e.h.o.l.d.e.r.s.u.i.t.e...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.a.m.b.r.i.d.g.e...S.h.a.r.e.h.o.l.d.e.r.S.u.i.t.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.2.8.-.0.0.0.1.-.0.0.1.5.-.f.b.9.2.-.6.b.8.c.2.5.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.3.a.d.3.e.e.3.1.a.6.9.2.9.6.c.f.3.3.c.1.3.7.e.c.d.a.8.5.f.5.f.0.0.0.0.0.0.0.0.!.0.0.0.0.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER74FA.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Feb 7 18:54:09 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	129193
Entropy (8bit):	3.531005970180092
Encrypted:	false
SSDEEP:	
MD5:	FF6F1E3F19AB71C225CB991B994C34FF
SHA1:	CADB4FA29C4547F6445DD3D3698DC52932AEBADA
SHA-256:	F458B18533869EEBE844961F764D7D82A35C659F7D62D42D91D1B035A58D1A86
SHA-512:	88FF4BEB027FFC4D0F970A7A398D3F1238D72AFDFAA1FFC54CAFC971F54D9396B54066D3102C5A479E87A994306B5CD01B6F0D9719D59E2A5CAFCC770217400C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....Q..c.....\.....-.....T.....8.....T..... .....X.....D.....U.....G.....GenuineIntelW.....T.....(...K..c.....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.....1.8.3.6.2...1...a.m.d.6.4.f.r.e...1.9.h.1._.r.e.l.e.a.s.e...1.9.0.3.1.8.-.1.2.0.2.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER76EF.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8402
Entropy (8bit):	3.6990298569740547
Encrypted:	false
SSDEEP:	
MD5:	686092FE4DB868C06EC2A0CF1D2AC552
SHA1:	D0433D72A2204683C7AFCB5FD7D97B240B5AA25D
SHA-256:	A88AD7AAD3167A33C4601CD3DC7B8492554F6D86DB9DA6BA72CCDBE902B1E432
SHA-512:	999088CC262345DFA71C25546972006FF5871EFF6D191AC40580C28A7D9F9EDBF2A120AFAA873F301D37EED14D0B4980CDB8BFE905B6B484994AF384866AADC D
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.>.1.8.3.6.3.<./.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.>.1.8.3.6.2...4.1.8...a.m.d.6.4.f.r.e...1.9.h.1._.r.e.l.e.a.s.e...1.9.0.3.1.8.- .1.2.0.2.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.4.1.8.<./.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.>.6.4.4.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER775D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4767
Entropy (8bit):	4.517850488965283
Encrypted:	false
SSDEEP:	
MD5:	A917353E79A3B717A88486AB951C8EAA
SHA1:	CA16B3F8592E8AC1BAE88DD8DF42D7D4342F5D00
SHA-256:	B989E34C7966D2199B681E144F2190F6EF7A154178A9DFA4FA9E6533A9EDE3FD
SHA-512:	D58A8A858E191A8A2DB6AB49157421360BA3F8B7FE166723E111EB8DB711A73A1FB8C6D3FDB9F7132CF62D30E8FEE16A0A843633CEAEC1A73CE47C4E9AF3D 32E
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="18363" />.. <arg nm="vercsdbld" val="418" />.. <arg nm="verqfe" val="418" />.. <arg nm="csdbld" val="418" />.. <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="894518" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.418.18362.0-11. 0.155" />.. <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):	1048576
Entropy (8bit):	4.264313122457509
Encrypted:	false
SSDEEP:	
MD5:	73A7039D1DE2708FC35819C74B2DCA20
SHA1:	77C00358A95635CDE1761C33C50A01BE65D516AE
SHA-256:	1A270B345777385671F6C5E3AD8EE8CA6D63BD153593DCAE22CC1B311F896FFD
SHA-512:	7FDE7D042FD5E3DEBB5C3B52489AEE727668FFFB33B1AEEC3762963A626A2B90E2230EF5B906FBDA4A5C242DFD6B19F44632867F71B9B958FAE57E2657A297 59
Malicious:	false
Reputation:	low
Preview:	regfC...C...L....S..... .....\.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...`.....`.....a.....rmtm6.f.%;..... ....x..... .....

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):	3.513830756732477
Encrypted:	false
SSDEEP:	
MD5:	8B30E7D9B14A6B1FE6EBED54579E7FEA
SHA1:	741FA3DFEA4095BB53B875252394DAE1896C8DEA
SHA-256:	9EE6F4B955826247F14429E7A165D8B15A2C4296FFD64246CD985D51632773AE
SHA-512:	2BFE0983F0FDA8EDAE0C37B898B59E6F15AE9D67808A4CBF1091250A1CD3EAE9751DC1A202492528C99C897DF72B0BDB4309A880155E35903F839BD52E5693F0
Malicious:	false
Reputation:	low
Preview:	regfB...B...L....S..... .....\.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...`.....`.....a.....rmtm6.f.%;..... .....x.HvLE.n.....B.....Q9OO.dZ...2x.;.....@... ....hbin.....L....S.....nk,..j.%;..... .....&...{11517B7C-E79D-4e20-961B-75A811715ADD}..p...sk.. ... ...(...t.....\...h.....H.....?.....?.....?..... ... .nk ..j.%;..... .....X..... .....:..... .....Root.....lh..(.....A.....nk ..j.%;..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.064007115455676
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	cambridge.shareholdersuite.exe
File size:	16980992
MD5:	36a2a6c6f6ba38708f501acce1176f1c
SHA1:	b5dbb9cef3950df5ad736367fc402f4a2cd8f741
SHA256:	d7e7a93d26422463c14fe026463ba369fd02e538df3fc379007135fe8a301b41
SHA512:	f2e5029d11e18eb748738feb87619b92063aaf01320eec0f895ebbeccb265b7bc4d63ad9c51b609a90e7a417c908ef8f7103800a06137ed0b8c1ee42f9cb70cc
SSDEEP:	98304:ceJ3hNLMJf65l50LD77w5Nv5rgvB2ANt01vMJqMJ:1xsLHM5NBrK2Bvr
TLSH:	9D072901A2A0CB29E57A5FF4E02400F543F5BD59F92AF21F9D817DE73D72B80981A627
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...wM.c.....0..... .....@.. .....`.....

File Icon

Icon Hash:	b2f1fbf3e7f397ce

Static PE Info

General

Entrypoint:	0x141a58e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63A34D77 [Wed Dec 21 18:16:23 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x101a53c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x101c000	0x19188	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1036000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x101a404	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1018594	0x1018600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x101c000	0x19188	0x19200	False	0.9572255907960199	data	7.866811806016482	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1036000	0xc	0x200	False	0.044921875	data	0.11836963125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x101c148	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 11811 x 11811 px/m		
RT_ICON	0x101c5c0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304, resolution 11811 x 11811 px/m		
RT_ICON	0x101cf58	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 11811 x 11811 px/m		
RT_ICON	0x101e010	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 11811 x 11811 px/m		
RT_ICON	0x10205c8	0x1475f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x1034d38	0x4c	data		
RT_VERSION	0x1034d94	0x3f0	SysEx File - OctavePlateau		

Imports

DLL	Import
mscoree.dll	_CorExeMain