ID: 1375
Sample Name: Unreal.exe
Cookbook: default.jbs
Time: 20:51:18
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

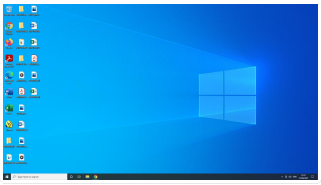
Windows Analysis Report Unreal.exe

Overview

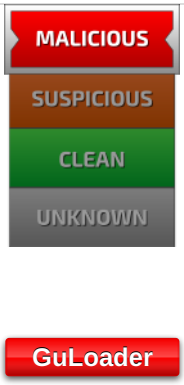
General Information

Sample Name:	Unreal.exe
Analysis ID:	1375
MD5:	35a93d1f2edc044.
SHA1:	c29f2524ae4bd23.
SHA256:	88d3b3a6564e25..
Infos:	

Most interesting Screenshot:



Detection

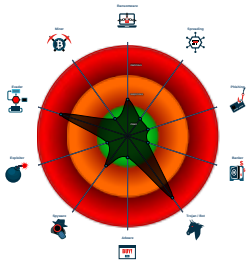


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64native**
- Unreal.exe (PID: 5360 cmdline: 'C:\Users\user\Desktop\Unreal.exe' MD5: 35A93D1F2EDC044B3D8289ABFEB17A43)
  - RegAsm.exe (PID: 6992 cmdline: 'C:\Users\user\Desktop\Unreal.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 7000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - WerFault.exe (PID: 3316 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6992 -s 1260 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=dow"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.18420827212.0000000001 1A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000000.18430470714.0000000001 1A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000002.18569185029.0000000001 1A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

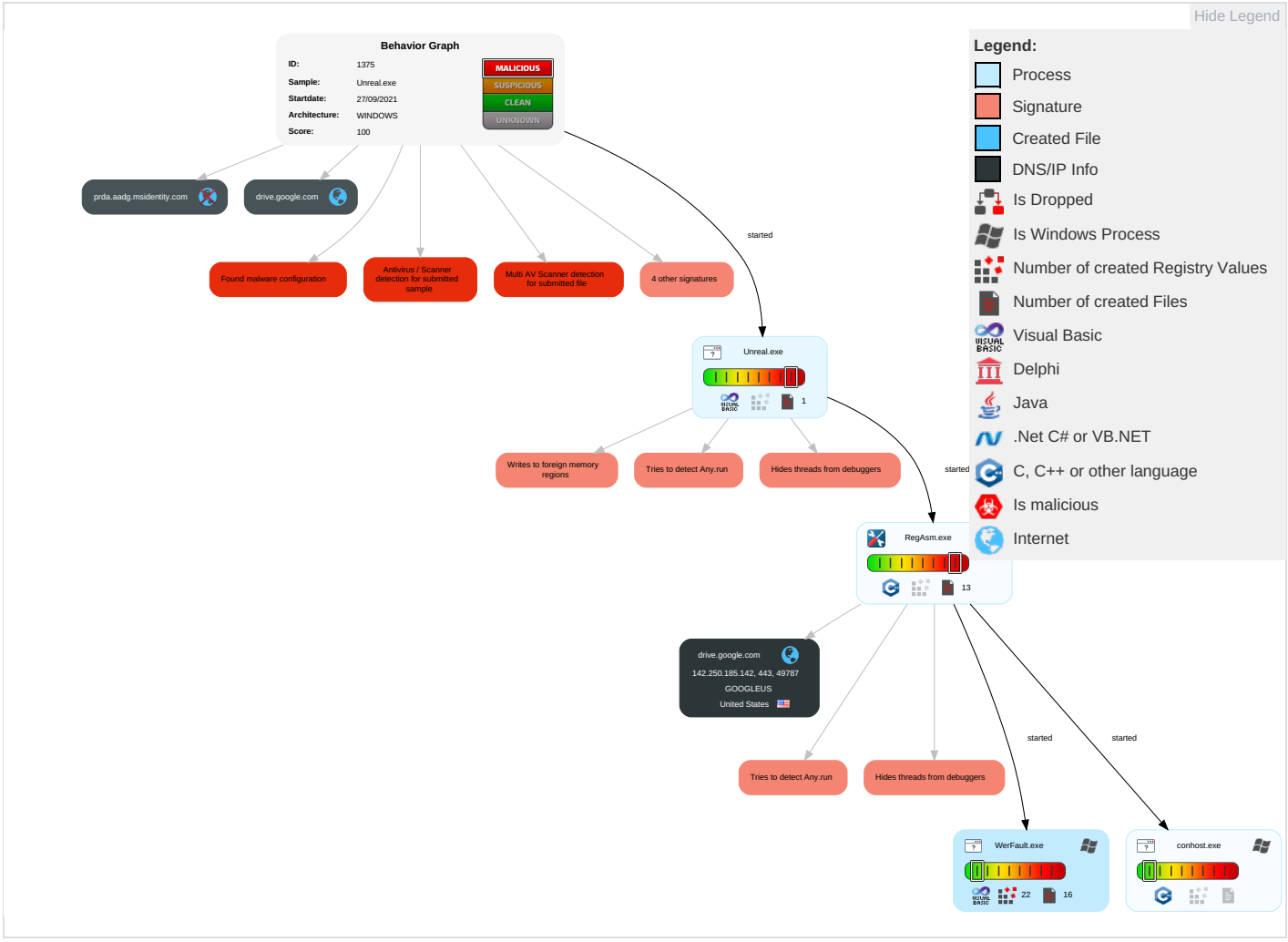
GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic

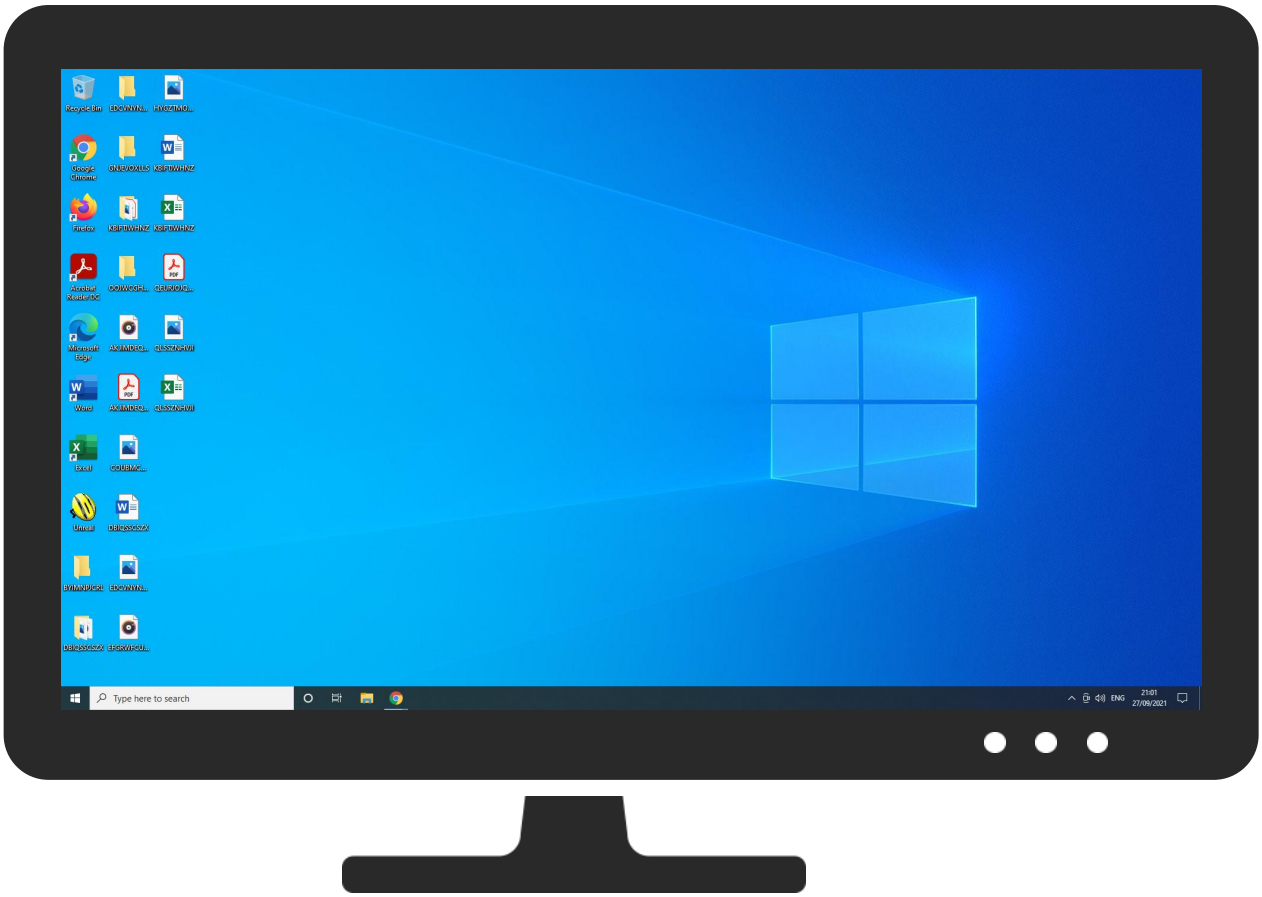
Behavior Graph



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
Unreal.exe	41%	Virustotal		Browse
Unreal.exe	13%	ReversingLabs	Win32.Trojan.Ursu	
Unreal.exe	100%	Avira	TR/AD.Nekark.hrjdi	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Unreal.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.hrjdi		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.142	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.142	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1375
Start date:	27.09.2021
Start time:	20:51:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Unreal.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	22
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:	mal100.troj.evad.winEXE@5/4@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 65% • 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
20:54:18	API Interceptor	1x Sleep call for process: RegAsm.exe modified
20:58:28	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	EITyS0c1l1.exe	Get hash	malicious	Browse	• 142.250.185.142
	fTset285bI.exe	Get hash	malicious	Browse	• 142.250.185.142
	ejecutable.exe	Get hash	malicious	Browse	• 142.250.185.142
	gmT455QDI6.exe	Get hash	malicious	Browse	• 142.250.185.142
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 142.250.185.142
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 142.250.185.142
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 142.250.185.142
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 142.250.185.142
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 142.250.185.142
	LISTA DE PEDIDO DE COMPRA.exe	Get hash	malicious	Browse	• 142.250.185.142
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 142.250.185.142
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	Get hash	malicious	Browse	• 142.250.185.142
	PO-003785GMHN.exe	Get hash	malicious	Browse	• 142.250.185.142
	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	• 142.250.185.142
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 142.250.185.142
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709213390.exe	Get hash	malicious	Browse	• 142.250.185.142
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 142.250.185.142
	PO-003785GMHN.exe	Get hash	malicious	Browse	• 142.250.185.142
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 142.250.185.142
	svchost.exe	Get hash	malicious	Browse	• 142.250.185.142

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegAsm.exe_29bf8efa3d478bed9ebb8bc4694e8e89a3debe79_e9e275a3_fdc547f4-9504-4479-9625-faeed7b4411d\Report.wer

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

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegAsm.exe_29bf8efa3d478bed9ebb8bc4694e8e89a3debe79_e9e275a3_fdc547f4-9504-4479-9625-faeed7b4411d\Report.wer

File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14176
Entropy (8bit):	3.766425811864498
Encrypted:	false
SSDEEP:	192:O6tb1o4TmSaAa403TaU5QPmRtDu76DfAIO8ErP6G:LLoFSaA4aU++tDu76DfAIO8wPb
MD5:	5FC0B172E812246939CC8B1BE390DDA7
SHA1:	93A535B66F6ED314ECCA3B4427CADDA9A0DBD0CF
SHA-256:	91D0643FDBC69EEAF4F4AFDCA15A887747B87A9A38DDC3316ED9C13E702492A7
SHA-512:	56032C67E020E08DAA388912387D21288DBF4798D9769B0EC5569406408C32CC2789584B5BC64D4EE4C223D3F04BA3BA90EFC41D144C0BA7EBB57CBC0393AB3E
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.=.1.3.2.7.7.2.4.6.3.0.2.8.8.6.6.7.2.6.....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.=.1.3.2.7.7.2.4.6.3.0.5.3.8.6.0.6.0.9.....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.=.f.d.c.5.4.7.f.4.-.9.5.0.4.-.4.4.7.9.-.9.6.2.5.-.f.a.e.e.d.7.b.4.4.1.1.d.....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.=.e.d.4.d.0.8.b.8.-.1.e.f.b.-.4.d.4.6.-.b.4.9.3.-.7.d.7.f.b.d.2.7.b.c.4.e.....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.=.R.e.g.A.s.m...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.e.g.A.s.m...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.5.0.-.0.0.0.1.-.0.0.1.0.-.9.5.f.4.-.3.c.6.2.d.9.b.3.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.e.e.e.8.b.2.5.7.3.f.7.1.e.8.d.5.c.3.e.e.7.e.5.3.a.f.3.e.6.7.7.2.e.0.9.0.d.0.f.3.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF3A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Sep 27 19:58:24 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	80022
Entropy (8bit):	2.1265006630353493
Encrypted:	false
SSDEEP:	384:93oS+EOkPo9WxGmYCCGLEKgWMc4z65CqRW:doQzoKgJGAc2W5Cr
MD5:	8BCEB4454D9819731E1761C2A6E972AE
SHA1:	1401A7F262B6763CF4C727B709397324C47D421E
SHA-256:	4F9F778860BD4BB3F900F956164809B012E88D2163B810640757BD4B3106AB34
SHA-512:	0AA178BC5101D4C39A11570E68C86849E930A472672CA513FF0D3D2592514FC45AA311039EE2D0E2CC7AA92DE46A802E2C1484E5591C6C9F4124D05A8601D60
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... .....`"Ra.....bJ.....(.....GenuineIntel.....T.....P...J!Ra.....0.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.9.0.4.1...5.4.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4AA.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):	6364
Entropy (8bit):	3.7295034335846666
Encrypted:	false
SSDEEP:	192:R9l7lZNiKS6RuYzlN4aKpDN89bU5yVsfgcm:R9lnNi/6YYpbUdf6
MD5:	C463A3A75710B11F01E340F0278E3405
SHA1:	91550756DC5D55787972FF1F1CD4392E1B0C9984
SHA-256:	7CC178D9A1900EC7EC2995D8D28D01CC12EDD3B0B0C91633D49D5EC722E8D6E0
SHA-512:	C09A00D3FAE29B339BC69A29463A39AFFCB832F467451ED6B675BA072161751DD032CBA4791ECC5A428849D531E23DF64EF7FD1AB8E317A5692545DC68D6632
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.>.1.9.0.4.2.<./.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.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.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.>.6.9.9.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5D4.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5D4.tmp.xml	
Size (bytes):	4831
Entropy (8bit):	4.520189012806639
Encrypted:	false
SSDEEP:	48:cvlwwtl8zs/fe702I7VFJ5WS2CfjkZs3rm8M4JfuDmQOqFX+q8oBXzOGt/ELu88x:uILf/27GySPfRJfuDzv5Jau84u8rd
MD5:	A260A2CC7C8DCE6EC732391835E709CF
SHA1:	4C51312ADCE38B3D765FB4B74EDA76C0BAC7B02A
SHA-256:	D8A17C4A1E416BBD7B28A2AB01026BFFC2C8FC0093AA87B216F0797816366CD4
SHA-512:	13B08952B12C9D1670438FAE7F2E45BFDD210EABE5F003AAACF0276D20907548FBF23CFA3B6F5971F421556AF61E6D5C8AE48D42DC08E81387F35CA3CC44BD 7
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="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <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="221284720" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.281321845122127
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	Unreal.exe
File size:	102400
MD5:	35a93d1f2edc044b3d8289abfeb17a43
SHA1:	c29f2524ae4bd239c849720b1fc6ce5c13bee93b
SHA256:	88d3b3a6564e25b63b31f4a00361384fd294f228763b3bde4e3162144971d385
SHA512:	dab0233817f1a28f0e1d15eb449d9c3c364796f6ddd66ced4307f3359635c29f38f80edd5e348bba03dd01d5522d358df1abd6d59e9ae94e750238af53b04bff
SSDEEP:	1536:yS+Spugs2L010fBhmNDLI41mFLHvHWJbrZk5Le5O3VzM/:F5puZA01iBYNh1m1HvHwfZkRz0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1.....1.....0...~...0.....0...Rich1.....PE..L...UL[W.....P...0.....`....@.....

File Icon

Icon Hash:	78f8d6d4ac88d0e2

Static PE Info

General

Entrypoint:	0x4012d4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x575B4C55 [Fri Jun 10 23:25:09 2016 UTC]
TLS Callbacks:	

General

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:	1eb0aaa4f15bbd841e91215ce68e26d2

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14788	0x15000	False	0.563720703125	data	6.65071196081	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x9f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1cb8	0x2000	False	0.26416015625	data	3.4642899067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:54:19.046786070 CEST	192.168.11.20	1.1.1.1	0xd244	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:54:19.055619955 CEST	1.1.1.1	192.168.11.20	0xd244	No error (0)	drive.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Sep 27, 2021 20:58:26.661173105 CEST	1.1.1.1	192.168.11.20	0x120e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49787	142.250.185.142	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:54:19 UTC	0	OUT	GET /uc?export=download&id=1JZajQIQdUbLIFKGrWeKAj7F2g5cgApuC HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache
2021-09-27 18:54:19 UTC	0	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 x-chromium-appcache-fallback-override: disallow-fallback P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-zmJa6o19NNZGxnDADiVTMg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Date: Mon, 27 Sep 2021 18:54:19 GMT Expires: Mon, 27 Sep 2021 18:54:19 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=ODlPQgXqu4fdjG6ZuHTs0XNElZYDpXm1vg6AmQltuVvHl0JsiakjSgV63pH6LJnzsT27OH d1ZwOj3TF0GiES08RkNtz9RFmZ-4zBpdXmGWfyTjPaYTA5Duyff1r4XtXVZBFi2lZx3mEw_9SnPrYs2NcLj3JlA4yz X0915aFt1IY; expires=Tue, 29-Mar-2022 18:54:19 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-09-27 18:54:19 UTC	1	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#00000
2021-09-27 18:54:19 UTC	1	IN	Data Raw: 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 0"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2021-09-27 18:54:19 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Unreal.exe PID: 5360 Parent PID: 7912

General

Start time:	20:53:09
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Unreal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Unreal.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	35A93D1F2EDC044B3D8289ABFEB17A43
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 6992 Parent PID: 5360

General

Start time:	20:53:46
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Unreal.exe'
Imagebase:	0xdd0000
File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.18420827212.00000000011A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.18430470714.00000000011A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000002.18569185029.00000000011A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 7000 Parent PID: 6992

General

Start time:	20:53:47
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6719c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 3316 Parent PID: 6992

General

Start time:	20:58:17
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6992 -s 1260
Imagebase:	0x9c0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis