ID: 1369
Sample Name: Unreal.exe
Cookbook: default.jbs
Time: 16:30:00
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

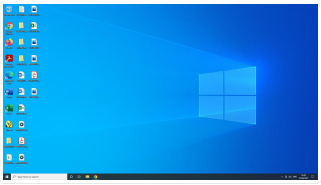
Windows Analysis Report Unreal.exe

Overview

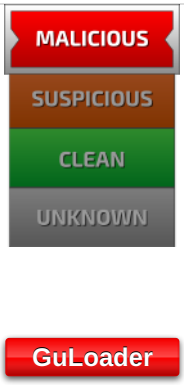
General Information

Sample Name:	Unreal.exe
Analysis ID:	1369
MD5:	35a93d1f2edc044.
SHA1:	c29f2524ae4bd23.
SHA256:	88d3b3a6564e25..
Infos:	

Most interesting Screenshot:



Detection

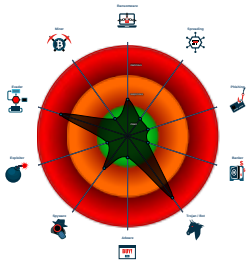


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- 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
- One or more processes crash
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64native**
- Unreal.exe (PID: 9076 cmdline: 'C:\Users\user\Desktop\Unreal.exe' MD5: 35A93D1F2EDC044B3D8289ABFEB17A43)
  - RegAsm.exe (PID: 6940 cmdline: 'C:\Users\user\Desktop\Unreal.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
  - RegAsm.exe (PID: 7508 cmdline: 'C:\Users\user\Desktop\Unreal.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 7772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - WerFault.exe (PID: 3384 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7508 -s 828 MD5: 40A149513D721F096DDF50C04DA2F01F)
- mpam-20b5c938.exe (PID: 6140 cmdline: 'C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-20b5c938.exe' /q WD MD5: 4CF0EA82FA547953BAA24CEB4AFDE935)
  - MpSigStub.exe (PID: 9104 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe /stub 1.1.1 8500.10 /payload 1.349.1496.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-20b5c938.exe /q WD MD5: 01F92DC7A766FF783AE7AF40FD0334FB)
- wevtutil.exe (PID: 5464 cmdline: C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\A491FE0B-CBB3-0812-A9E9-28E6069853FA.man MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 8100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- wevtutil.exe (PID: 6516 cmdline: C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\A491FE0B-CBB3-0812-A9E9-28E6069853FA.man '/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 3060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.5646431545.0000000000D50000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000008.00000000.5536067468.0000000000D50000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000008.00000000.5526072916.0000000000D50000.00000040.00000001.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

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

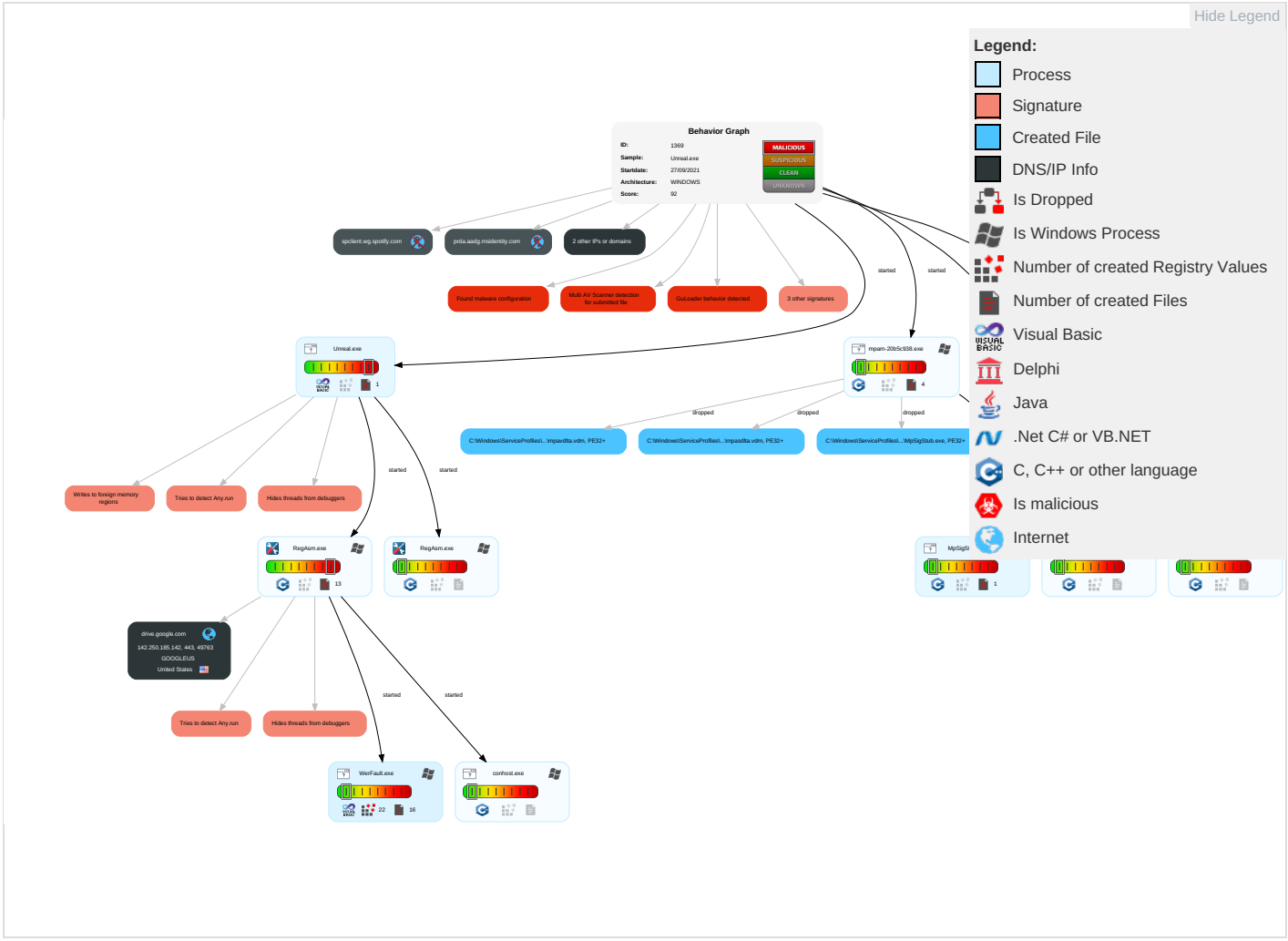
Stealing of Sensitive Information:

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	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Masquerading 3	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 1	Eavesdr Insecure Network Commun
Default Accounts	Service Execution 2	DLL Side-Loading 1	Windows Service 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 3	Access Token Manipulation 1	Security Account Manager	Security Software Discovery 3 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	DLL Side-Loading 1	Process Injection 1 1 3	NTDS	Virtualization/Sandbox Evasion 2 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

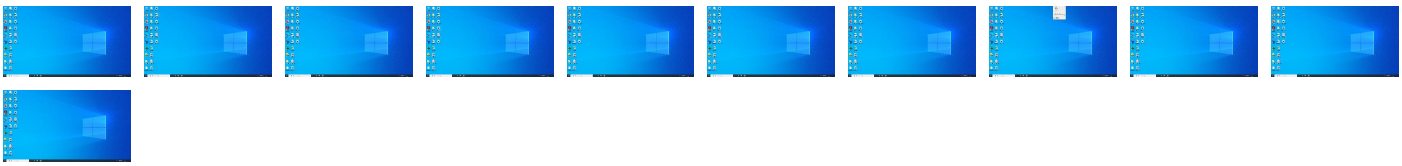
Behavior Graph

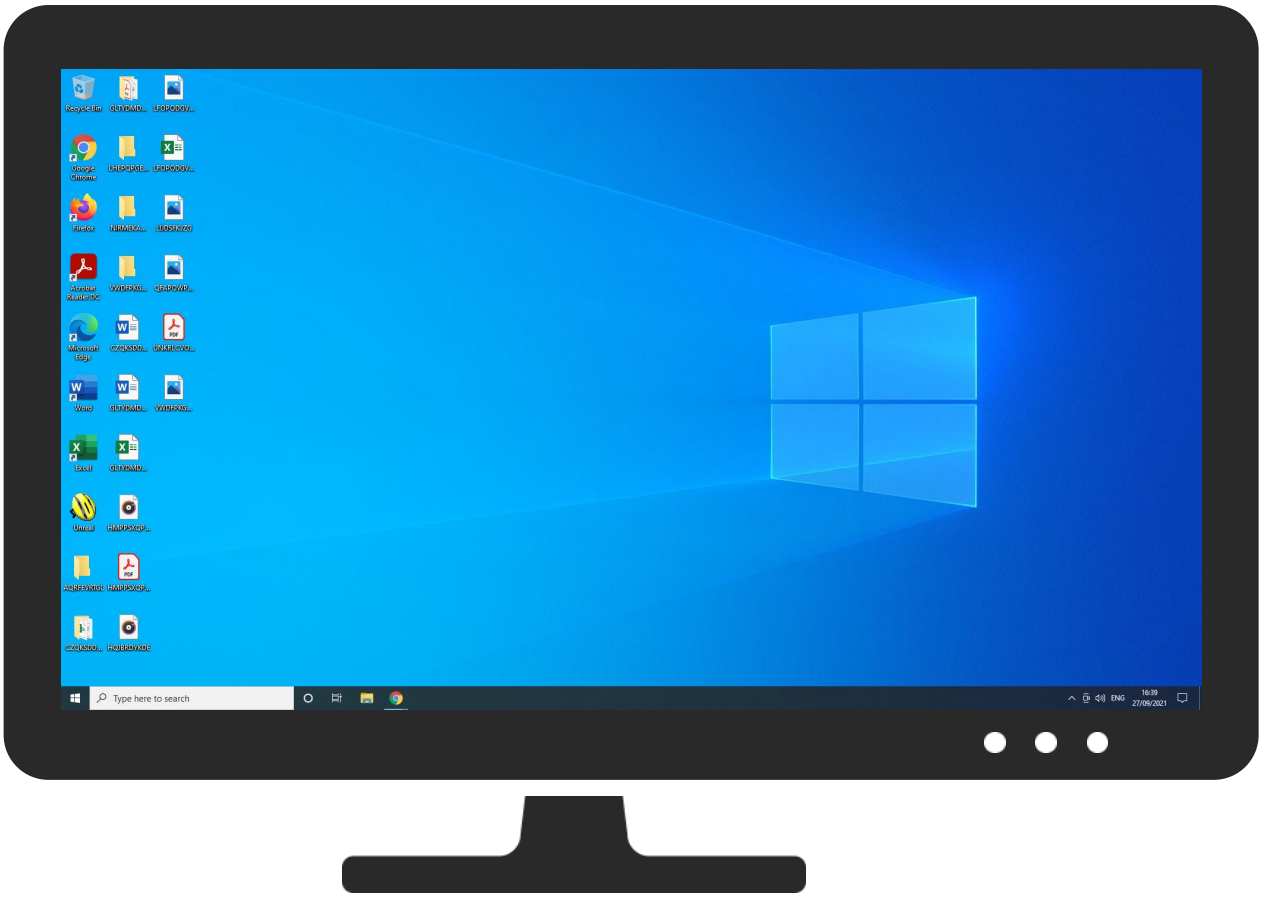


Screenshots

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	13%	ReversingLabs	Win32.Trojan.Ursu	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe	0%	Virustotal		Browse
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\mpasdlta.vdm	0%	Virustotal		Browse
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\mpavdlta.vdm	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

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
edge-web.dual-gslb.spotify.com	35.186.224.25	true	false		high
spclient.wg.spotify.com	unknown	unknown	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:	1369
Start date:	27.09.2021
Start time:	16:30:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 44s
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:	30
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:	mal92.troj.evad.winEXE@14/8@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:33:03	API Interceptor	1x Sleep call for process: RegAsm.exe modified

Time	Type	Description
16:37:10	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
edge-web.dual-gslb.spotify.com	hVlpEajflR.exe	Get hash	malicious	Browse	• 35.186.224.25

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	• 142.250.185.142
	7XmWGse79x.exe	Get hash	malicious	Browse	• 142.250.185.142
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 142.250.185.142
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 142.250.185.142
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 142.250.185.142
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 142.250.185.142
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 142.250.185.142
	BXTOD28N3I.exe	Get hash	malicious	Browse	• 142.250.185.142
	Kapitu.exe	Get hash	malicious	Browse	• 142.250.185.142
	SebwAujas5.exe	Get hash	malicious	Browse	• 142.250.185.142
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 142.250.185.142
	Payment_Advice.exe	Get hash	malicious	Browse	• 142.250.185.142
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 142.250.185.142
	k5THcVgINl.exe	Get hash	malicious	Browse	• 142.250.185.142
	b2i2IopgOC.exe	Get hash	malicious	Browse	• 142.250.185.142
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 142.250.185.142
	Dokument VAT I - 85926 09 2021 MAG-8.exe	Get hash	malicious	Browse	• 142.250.185.142
	qOsClQD1uR.exe	Get hash	malicious	Browse	• 142.250.185.142
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 142.250.185.142
	p0FDRanFUE.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_bf83f564e97574c9bbf23ac35112572b5de6d5_e9e275a3_bac2586d-6b28-40ad-af6b-2dc7bcda6e5d\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14172
Entropy (8bit):	3.7655413027301523
Encrypted:	false
SSDEEP:	192:bmNk2b1Q4TmSaAa403TaU5QPmRtDu76PfAIO8ErPf:yNkAQFSaA4aU++tDu76PfAIO8wPf
MD5:	EB077F8A99E22283743F463500155C8B
SHA1:	72A799BACC0F6537298B6EE2B8E78706F85FB711
SHA-256:	F3D1AF47BA08A576BA22D99FB21B2C0C8ECA0909C1182D7330DF4A741F7A62FA
SHA-512:	BDA7B9AD678F33CD47E102E0FF23F2DBCB4896D50C85BFAF6F5536B7A2D535989EBD17755C626FDD8F4242DD30D68F626A86F82BD3891A2F9DB184ACC73A28D
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.=.1.3.2.7.7.2.3.0.6.2.6.7.2.9.5.4.4.7.....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.=.1.3.2.7.7.2.3.0.6.2.9.0.8.8.3.5.1.3.....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.=.b.a.c.2.5.8.6.d.-.6.b.2.8.-.4.0.a.d.-.a.f.6.b.-.2.d.c.7.b.c.d.a.6.e.5.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.=.c.e.0.e.f.6.6.e.-.2.1.a.9.-.4.6.a.7.-.9.8.d.3.-.8.9.7.f.6.9.3.e.c.5.4.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.d.5.4.-.0.0.0.1.-.0.0.1.0.-.5.5.5.a.-.f.5.e.2.b.4.b.3.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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\WEREA47.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Sep 27 15:37:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	76462
Entropy (8bit):	2.1964997599695373
Encrypted:	false
SSDEEP:	384:TCRsn5gyGXQHCT4PE6ipvxx518uKlDp5kK:TTn5gyg7TsETxHBIDp5kK
MD5:	70F9CA1B43425219D7E8BE4CE40F89B5
SHA1:	762B772DB4621C73A0BF077706A35333F955611F
SHA-256:	4B1D46C06B7270351D218F0E559F31D36DF5424EDD0DD84071BB250FA8FD9B1B
SHA-512:	46C963CEC4BBD273D9329A9B7A40A916F54B4BC998962A31D127C689ACB774116425671B6B59F6FEAB7023B52BF3A237D84F1C5D8F66E26C2CA92B5840DA2F4
Malicious:	false
Preview:	MDMP..a..... .....#.Qa.....bJ.....(.....GenuineIntel.....T.....T.....Qa.....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\WEREFC6.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):	6362
Entropy (8bit):	3.72809936357387
Encrypted:	false
SSDEEP:	192:R9l7lZNi0l6TbtYzFN4acpDR89bf/sbsfM1m:R9lnNi76TbtYp5fLfT
MD5:	7397ACE7BCE045EB5049FB6C752EE5C7
SHA1:	D428A0E75DDE5AD16804515C35008CB01BF580CF
SHA-256:	83AC34525B6AA26568FE0DC7F6A964831247844677A84EE585AD18567362BCAB
SHA-512:	44C5D442D586EF438112177D22257D20BA3B8F0BE3DE937CF74E550A3393155C6685806BB4B37862F12A15E1178CCECC97B49D28F51CE628C33300B222237E21
Malicious:	false
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.>.7.5.0.8.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF092.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF092.tmp.xml	
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4830
Entropy (8bit):	4.5178125588485045
Encrypted:	false
SSDEEP:	48:cvIwwtl8zs/Me702I7VFJ5WS2CfjkMs3rm8M4JfuDm4OqFl/u+q8oBX/OFH/ELu1:uILf/x7GySPf+Jfuvp2vtSHau84uWrd
MD5:	D065B32D803F90219D2FA5BAB571DDD2
SHA1:	DC90C8EA75C341C4DBF75A3E100F4227D2A2CA44
SHA-256:	4B5CA7DFF2D32147039A8EAF1615B961EED5779F3EE1BCDCD8EE169D11FD7496
SHA-512:	943D2F5268F30F0AA912A8B0EE4C0D7F3CB503BF9818886DEC81249480A6F56BD8B4BC216E418585DB28DB07E9FD4D5BD319CDFE2F5F3F87C0F3900BEC7C950
Malicious:	false
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="221284459" />.. <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="

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-20b5c938.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	803176
Entropy (8bit):	6.37118649960636
Encrypted:	false
SSDEEP:	24576:Ghj1QlBYDgtUUvie3n+pB3+ojRlcD1VyZTFXk:GhpQlBHtBYla1VyZpU
MD5:	01F92DC7A766FF783AE7AF40FD0334FB
SHA1:	45D7B8E98E22F939ED0083FE31204CAA9A72FA76
SHA-256:	FA42B9B84754E2E8368E8929FA045BE86DBD72678176EE75814D2A16D23E5C26
SHA-512:	BEA5F3D7FB0984C4A71720F25644CE3151FCDC95586E1E2FFE804D04567AAF30D8678608110E241C7DDF908F94882EDDD84A994573B0C808D1C064F0E135A583
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..#...#...#..EV...#...Q...#...Q...#...Q...#...Q...#...#..."..EV..#..EV N..#..EV...#..Rich.#.....PE..d.....P....."....`.....@.....0.....-....`..... .....t..d..... .....D... ..h!... .....d...p..... (.....8.....0.....text...2R.....`..... ..`.rdata.....p... ...p.....@..@.data..../..... .....@....pdata...D.....P.....@..@.rsrc... ....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\mpasdlta.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-20b5c938.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7754168
Entropy (8bit):	**7.999076442471787**
Encrypted:	**true**
SSDEEP:	196608:YXO9SVxVkHWgVLfT19HDihdTNpwvjAkE36nywlAVILpzyyaW27:YZXmHdBfpMjUlywlAat3Bm
MD5:	8B78E09BD2D0734CF4EDB44C68F22368
SHA1:	E9C0F6D912ED28066201118AA296493A738E8D7F
SHA-256:	7FEA9243F8AFF82658D32716D7D668EFD6986D78E15C5E3E35CDD94B565BA32A
SHA-512:	36C255E4768179257F0B5A9B9B15C21113FED29633144302B6FD90C96D7AD9D5116CD77E9822F0389A4B7904A739F8B295513D5528B354CD9EC70DA7D5AF160F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d.....Qa....." .....v..... .....Pv.....v...`..... ..8+v.....0v..!.....rdata..p..... ....@..@.rsrc...8+v.. ...,v.....@..@.....Qa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ..x*v..rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\mpavdlta.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-20b5c938.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	modified
Size (bytes):	5016504
Entropy (8bit):	**7.997724088667752**

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\mpavdlta.vdm	
Encrypted:	**true**
SSDEEP:	98304:HHeb+Ze66NXRdSKHWdezWUTIm0GXodoubtS8RVZGgA7ASskPCDL5MeS8YjN:H+aZN6NXRdSdCWUTILGI3pGXdrP8LPSl
MD5:	C64D6E20AF376A357E27E01E81023E58
SHA1:	348B30450CA17871D3957502CF28183B1B3FD8C1
SHA-256:	8D427A5CB59EFC21A66E8A7E2EBCDE0F7B1E71EA0E4627B04443667C6992614D
SHA-512:	52E5BDA32BE278C578B5377FD08EBD928B88802E8883B50F06FC6EDF45E287831BC5D2245F2984E5AECD67BC24BC293BF3FC9C266E91D3FAABB092D598F8A9 4
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........<..R...R...R......R..P...R.Rich..R.PE..d.....Qa.........." ....hL........... ....................................L......GM...`.. ...eL..........jL..!...rdata..p...................... ....@..@.rsrc....eL.. ...fL.................@..@......Qa........T........................rdata......T....rdata$zzzdbg.... ....rsrc$01..... ...dL..rsrc$02... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	6856
Entropy (8bit):	3.555984344338531
Encrypted:	false
SSDEEP:	96:BRKisMYmA2KxoZvHoBYETZWDzrH+LBWjz5f0hSsFX:nKioD2Kx0HoNer0GB0vl
MD5:	9A80E0210B6CC8C743A2B0286A426983
SHA1:	614CA8E4EA8E2DE3A141C1BB7CFA03EE27259CEA
SHA-256:	D410EF955BDCD1127A2D87A70AE04285B1B609B8C5F0C6AD31E6DA6164A351FF
SHA-512:	51FD352689AFA312917EC50A8DFF35179E13181B9D0DEF7B0647E2A8975F371DB0C345E2B69D0A08908D6DF0DE157BCAF7FEA38686811701F2C75F1ACD57785
Malicious:	false
Preview:	..-.....S.t.a.r.t. .t.i.m.e.:. .2.0.2.1.-.0.9.-.2.7. .1.5.:.3.8.:.0.3.Z. ....P.r.o.c.e.s.s.:. .2.3.9.0...1.d.7.b.3.b.5.a.8.d.2.b.a.0.c.....C.o.m.m.a.n.d.:. ./.s.t.u.b. .1...1...1.8.5.0.0...1.0. ./.p.a.y.l.o.a.d. .1...3.4.9...1.4.9.6...0. ./.p.r.o.g.r.a.m. .C.:.\. W.i.n.d.o.w.s.\.S.E.R.V.I.C.~.1.\.N.E.T.W.O.R.~.1.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.m.p.a.m.-.2.0.b.5.c.9.3.8...e.x.e. ./.q. .W.D.....A.d.m.i.n.i.s.t.r.a.t.o.r.:. .n.o.....V.e.r.s.i.o. n.:. .1...1...1.8.5.0.0...1.0.........=. .P.r.o.d.u.c.t.S.e.a.r.c.h. .=. =.=.=.=.=.=.=.=.=......... . . . . .M.i.c.r.o.s.o.f.t. .W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r. .(.R.S.1.+.).:. . . . . .S.t.a.t.

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:	88d3b3a6564e25b63b31f4a00361384fd294f228763b3bd e4e3162144971d385
SHA512:	dab0233817f1a28f0e1d15eb449d9c3c364796f6ddd66ce d4307f3359635c29f38f80edd5e348bba03dd01d5522d35 8df1abd6d59e9ae94e750238af53b04bff
SSDEEP:	1536:yS+Spugs2L010fBhmNDLI41mFLHvHWJbrZk5Le 5O3VzM/:F5puZA01iBYNh1m1HvHwfZkRz0
File Content Preview:	MZ......................@..!..L.!Th is 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:	
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 16:33:03.836004019 CEST	192.168.11.20	1.1.1.1	0x7402	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 16:36:16.852319002 CEST	192.168.11.20	1.1.1.1	0x7634	Standard query (0)	spclient.wg.spotify.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 16:33:03.844651937 CEST	1.1.1.1	192.168.11.20	0x7402	No error (0)	drive.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Sep 27, 2021 16:36:16.860439062 CEST	1.1.1.1	192.168.11.20	0x7634	No error (0)	spclient.wg.spotify.com	edge-web.dual-gslb.spotify.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 16:36:16.860439062 CEST	1.1.1.1	192.168.11.20	0x7634	No error (0)	edge-web.dual-gslb.spotify.com		35.186.224.25	A (IP address)	IN (0x0001)
Sep 27, 2021 16:37:10.343050957 CEST	1.1.1.1	192.168.11.20	0xacc3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.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	49763	142.250.185.142	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 14:33:04 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 14:33:04 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-MIVbPGF4ZuXsZ2NZTTzVEQ' '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 14:33:04 GMT Expires: Mon, 27 Sep 2021 14:33:04 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=kWh_xUioAXmCXt6QIW6Mm4DtzPI9_fAr2WiFKEmXPAjZvuWqXj1I7phnbwK5qVZOA3KA2D wc9IGtRHUtfxRy-aBcUQZ4zKf-uCz414_kuMrvIGUe_DgGauW80ouL5dhtM9v6jgmzo75QoUqo2k6HSanF5BaWh7W1 UvFmn1Szn94; expires=Tue, 29-Mar-2022 14:33:04 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"; ma=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 14:33:04 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 14:33:04 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 14:33:04 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: 9076 Parent PID: 2216

General

Start time:	16:31:53
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: 6940 Parent PID: 9076

General

Start time:	16:32:31
Start date:	27/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Unreal.exe'
Imagebase:	0xb0000
File size:	53248 bytes
MD5 hash:	A64DACA3CFBCD039DF3EC29D3EDDD001
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegAsm.exe PID: 7508 Parent PID: 9076

General

Start time:	16:32:31
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:	0x980000
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: 00000008.00000002.5646431545.0000000000D50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000008.00000000.5536067468.0000000000D50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000008.00000000.5526072916.0000000000D50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 7772 Parent PID: 7508

General

Start time:	16:32:31
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff664700000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 3384 Parent PID: 7508

General

Start time:	16:37:01
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7508 -s 828
Imagebase:	0x480000
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

Analysis Process: mpam-20b5c938.exe PID: 6140 Parent PID: 8212

General

Start time:	16:38:00
Start date:	27/09/2021
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-20b5c938.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-20b5c938.exe' /q WD
Imagebase:	0x7ff7fe970000
File size:	13390280 bytes
MD5 hash:	4CF0EA82FA547953BAA24CEB4AFDE935
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MpSigStub.exe PID: 9104 Parent PID: 6140

General

Start time:	16:38:03
Start date:	27/09/2021
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\029C0225-A9FE-4247-9FEB-6A4C69D031CD\MpSigStub.exe /stub 1.1.18500.10 /payload 1.349.1496.0 /program C :\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-20b5c938.exe /q WD
Imagebase:	0x7ff742dc0000
File size:	803176 bytes
MD5 hash:	01F92DC7A766FF783AE7AF40FD0334FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: wevtutil.exe PID: 5464 Parent PID: 3144

General

Start time:	16:38:04
Start date:	27/09/2021
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\A491FE0B-CBB3-0812-A9E9-28E6069853FA.man
Imagebase:	0x7ff7baff0000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 8100 Parent PID: 5464

General

Start time:	16:38:05
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff664700000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wevtutil.exe PID: 6516 Parent PID: 3144

General

Start time:	16:38:06
Start date:	27/09/2021
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\A491FE0B-CBB3-0812-A9E9-28E6069853FA.man '/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll'
Imagebase:	0x7ff7baff0000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 3060 Parent PID: 6516

General

Start time:	16:38:06
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff664700000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis