ID: 1364
Sample Name: Kapitu.exe
Cookbook: default.jbs
Time: 15:06:05
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

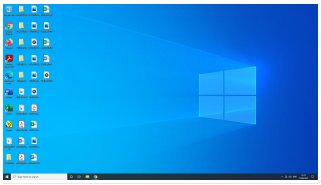
Windows Analysis Report Kapitu.exe

Overview

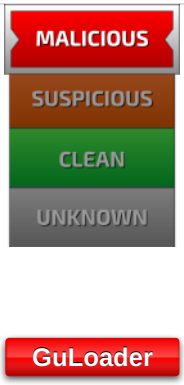
General Information

Sample Name:	Kapitu.exe
Analysis ID:	1364
MD5:	149b6bd6b0d3dd..
SHA1:	33cdaa42e1a5c1..
SHA256:	b622dbe8021483..
Infos:	

Most interesting Screenshot:



Detection

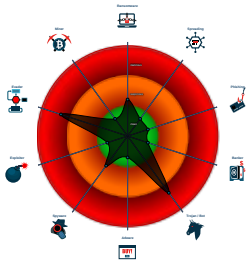


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- One or more processes crash
- PE file contains strange resources

Classification



Process Tree

- **System is w10x64native**
- Kapitu.exe (PID: 6732 cmdline: 'C:\Users\user\Desktop\Kapitu.exe' MD5: 149B6BD6B0D3DD2B0FBB111632D59FCC)
  - RegAsm.exe (PID: 6972 cmdline: 'C:\Users\user\Desktop\Kapitu.exe' MD5: A64DACA3CFBCD039DF3EC29D3EDDD001)
    - conhost.exe (PID: 6980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - WerFault.exe (PID: 5608 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6972 -s 1356 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.19109903808.0000000001100000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000000.18979643782.0000000001100000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000000.18969783001.0000000001100000.00000040.00000001.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

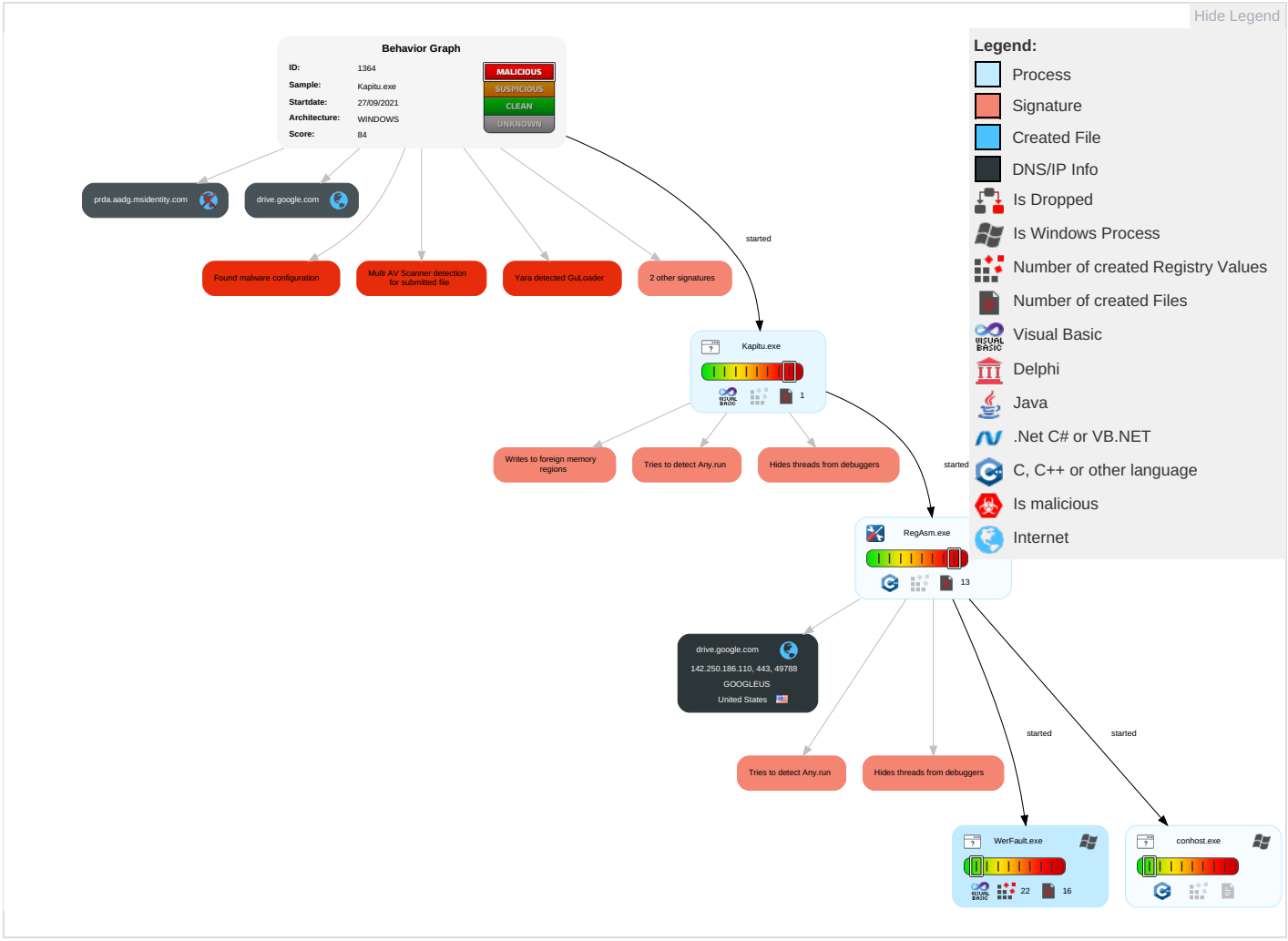
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

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 1 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Card Swap

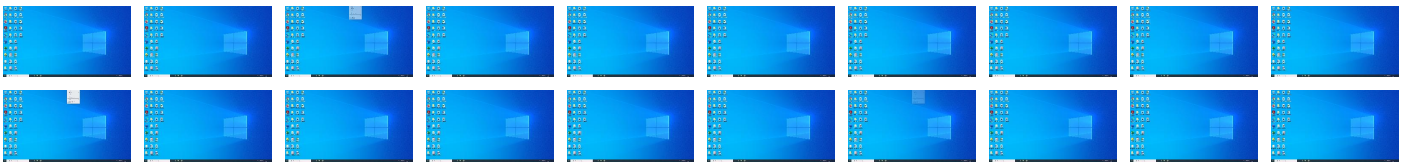
Behavior Graph



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
Kapitu.exe	20%	Virustotal		Browse
Kapitu.exe	9%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://watson.telemet	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.186.110	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1364
Start date:	27.09.2021
Start time:	15:06:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Kapitu.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:	mal84.troj.evad.winEXE@5/4@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 60% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:08:49	API Interceptor	1x Sleep call for process: RegAsm.exe modified
15:12:58	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	SebwAujas5.exe	Get hash	malicious	Browse	• 142.250.186.110
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 142.250.186.110
	Payment_Advice.exe	Get hash	malicious	Browse	• 142.250.186.110
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 142.250.186.110
	k5THcVgINl.exe	Get hash	malicious	Browse	• 142.250.186.110
	b2i2IopgOC.exe	Get hash	malicious	Browse	• 142.250.186.110
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 142.250.186.110
	Dokument VAT I - 85926 09 2021 MAG-8.exe	Get hash	malicious	Browse	• 142.250.186.110
	qOsCIQD1uR.exe	Get hash	malicious	Browse	• 142.250.186.110
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 142.250.186.110
	p0FDRanFUE.exe	Get hash	malicious	Browse	• 142.250.186.110
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	• 142.250.186.110
	rJPkGz9DpL.exe	Get hash	malicious	Browse	• 142.250.186.110
	GVXEsDOGHX.exe	Get hash	malicious	Browse	• 142.250.186.110
	IAWCl9VgWq.exe	Get hash	malicious	Browse	• 142.250.186.110
	BRl35oWria.exe	Get hash	malicious	Browse	• 142.250.186.110
	UcmKadhoIn.exe	Get hash	malicious	Browse	• 142.250.186.110
	oGLE7fjvYA.exe	Get hash	malicious	Browse	• 142.250.186.110
	ZbhUS5doEw.exe	Get hash	malicious	Browse	• 142.250.186.110
	dEYSAsBcE8.exe	Get hash	malicious	Browse	• 142.250.186.110

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegAsm.exe_8e77c7606944d14a4a77d55b81e0b269ca1184a3_e9e275a3_cbb8e5b7-b486-4e03-a377-23ec05ba81b4\Report.wer

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

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegAsm.exe_8e77c7606944d14a4a77d55b81e0b269ca1184a3_e9e275a3_cbb8e5b7-b486-4e03-a377-23ec05ba81b4\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14174
Entropy (8bit):	3.7659925989635616
Encrypted:	false
SSDEEP:	192:0oLiCb1o4zmSaAa403TaU5QPmRtDu76MfAIO8ErPM:a0olSaA4aU++tDu76MfAIO8wPM
MD5:	DA404030CE19F1BBA13D8E4E56253CE9
SHA1:	C5AA9F42085D9805EE411E8482CA3AB8731E6A29
SHA-256:	F5B6655BF5F0FA7CBF328A83AFBA3BAEB22635B5F964C28FA9DFBFD2A9842EBE
SHA-512:	25EE3FEB9BCEF83B3771A591C4A89BCBAC54B6952E0ADFF9E33C14142596DEDE98476354BA821D6F59C11EC6A125EF43D623DF2BFC819FB8B7E4AA8F47B24285
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.=.1.3.2.7.7.2.2.5.5.7.3.4.1.6.3.1.4.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.7.2.2.5.5.7.5.5.0.9.5.8.0.2.....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.=.c.b.b.8.e.5.b.7.-.b.4.8.6.-.4.e.0.3.-.a.3.7.7.-.2.3.e.c.0.5.b.a.8.1.b.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.=.0.7.0.c.3.3.6.a.-.e.0.9.2.-.4.d.2.9.-.b.0.9.6.-.3.d.f.3.9.2.a.5.e.8.8.6.....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.3.c.-.0.0.0.1.-.0.0.1.0.-.7.0.1.8.-.9.2.2.2.a.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\WERECCC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Sep 27 14:12:54 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	77274
Entropy (8bit):	2.1873454119378852
Encrypted:	false
SSDEEP:	192:b97zc1lXfM++84XRr9WCgyDv6W/GCpjYRz7An5N2aKf3hHddI+ha6GaBPXuwHY7r:b938G+3G9WCPGCWywhfDiZ8PtHY7Kg
MD5:	92E5E849DE9B165B358CAB49E4379A1D
SHA1:	71D4200030C91F2E1973A99279A2E8B0CE9BAC4D
SHA-256:	76655AEE6B2EA0D2870503F7101E7BE88159FBC194032E6411400C1EAE11CE69
SHA-512:	80C686D44CE6D6238723BC082AFDAE7BC9584C0C071559877988615FBF8DF42C727C593C56EF27B4AF49AEB1F2C0CC7181CA3D69850F42710340A52D40B7AA6
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... .....f.Qa.....bJ.....(.....GenuineIntel.....T.....<...X.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\WERF180.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):	3.726221093864917
Encrypted:	false
SSDEEP:	96:R7lU6o7lZt3i0t6QszTYzxXTilqw4f1OvzcuujulBZaMQUm89bIIsfztGm:R9l7lZNi0t6pYzlN4aBpDm89bIIsfzYm
MD5:	BF0431B1450429DE61AAE2F1227D870F
SHA1:	016A4DBACFB52275E9787D6C6D7580610BB98D12
SHA-256:	958FE7FAF707624A01978864515EA9E09865F753BF00A2D9E7E2DEDCFF4AF9B5
SHA-512:	66DCF438B84C50761DFAE34DB12C3001D133B05B670E6B52DDFA7406ABC0C0EC787B269C8BA38E4633274767010E6BC2867F02D54D8766E5AFCBDA753771CB4
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.>.6.9.7.2.</./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF24C.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\WERF24C.tmp.xml	
Size (bytes):	4831
Entropy (8bit):	4.517021049579082
Encrypted:	false
SSDEEP:	48:cvlwwtl8zs/WEe702I7VFJ5WS2CfjkKs3rm8M4JfuDmgOqF0+q8oBXvOR5/ELu8W:uILf/Wp7GySPf8Jfufgv1y5au84u8rd
MD5:	7334475FBAF6479D83C63961C74E9137
SHA1:	F0F3F7A43259C96EAA73960FB4C8C1CB7366713F
SHA-256:	40677DF1FFD16F49BE05D49D4384B0172698E853CCD8A7D2C98D4844EFDAE91F
SHA-512:	411A48956C1EDBBB1184BA856A7F4F32AFB8D4FAD43EE075FF19588D281F702118E63B6519B49B8CA8A371529C9A488963B7419A6836F8E0EFE47EACF2DA0CA5
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="221284375" />.. <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):	6.2510687218535645
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:	Kapitu.exe
File size:	102400
MD5:	149b6bd6b0d3dd2b0fbb111632d59fcc
SHA1:	33cdaa42e1a5c1fad1aa4f38dd9ad6ea75113aa7
SHA256:	b622dbe802148305104ef456835748d2fc0d8edeffa64787c43c78bcb1914b2f
SHA512:	d2783ef1112d892b9501cf0e8ce6e74277d0d55d0eb9cd3841802381682bc1e7631389c24a2f6f297a82f406fdb6c942ae7987df96f227d00e73ebbc6d01c51f
SSDEEP:	1536:RMigxMWRwt1aaGhFNEAAF9vq/eVlQ4F5kOrpdh/:aicCQhFWfFqWlQa19d1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....G.....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:	0x47939ED5 [Sun Jan 20 19:19:49 2008 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	0x14548	0x15000	False	0.564581008185	data	6.64813091297	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	0.264526367188	data	3.48286092723	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 15:08:50.381459951 CEST	192.168.11.20	1.1.1.1	0xab1d	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 15:08:50.390096903 CEST	1.1.1.1	192.168.11.20	0xab1d	No error (0)	drive.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Sep 27, 2021 15:12:57.105799913 CEST	1.1.1.1	192.168.11.20	0x3e86	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	49788	142.250.186.110	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 13:08:50 UTC	0	OUT	GET /uc?export=download&id=1a0WYfccpP_tzw3yrsNqkLeIjHmcdMRod 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 13:08:50 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-MvTTUjqOi+ULm6tB1JBGlA' '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 13:08:50 GMT Expires: Mon, 27 Sep 2021 13:08:50 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=abKi0BWgcemcd0d8wm9mOlAU2B3arxsDTzzIYttMhyEZI6BWiC6XRhQKgWHtgX8WrOJul0 8K92QFhtYs9xjnosQK86HWAE8VXopjAbsMkP7rWufpF19a4IJLb_GGIG6TaDkuZEY-t6WXx_m0czyrRfhtLyX5RoUF 5UVTrZ9K2D8; expires=Tue, 29-Mar-2022 13:08:50 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 13:08:50 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 13:08:50 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 13:08:50 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: Kapitu.exe PID: 6732 Parent PID: 5944

General

Start time:	15:07:55
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Kapitu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Kapitu.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	149B6BD6B0D3DD2B0FBB111632D59FCC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 6972 Parent PID: 6732

General

Start time:	15:08:24
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\Kapitu.exe'
Imagebase:	0xc80000
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: 00000005.00000002.19109903808.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.18979643782.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.18969783001.0000000001100000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 6980 Parent PID: 6972

General

Start time:	15:08:24
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff73c180000
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: 5608 Parent PID: 6972

General

Start time:	15:12:48
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6972 -s 1356
Imagebase:	0x7ff79c420000
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