ID: 491916
Sample Name: 9JbJZPtaKF.exe
Cookbook: default.jbs
Time: 07:22:16
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

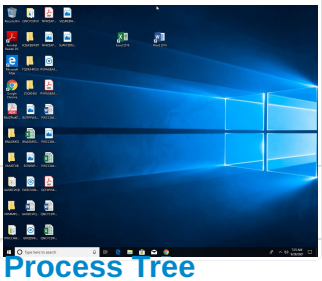
Windows Analysis Report 9JbJZPtaKF.exe

Overview

General Information

Sample Name:	9JbJZPtaKF.exe
Analysis ID:	491916
MD5:	133c10454108aa..
SHA1:	21439179cb8700..
SHA256:	de0cb500125d73..
Tags:	BitRAT exe RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

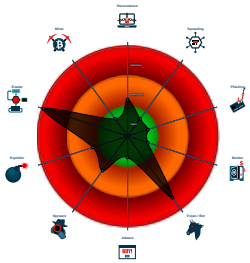
AsyncRAT BitRAT

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

Signatures

- Yara detected BitRAT
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Multi AV Scanner detection for dropp…
- Hides threads from debuggers
- Sample uses process hollowing tech…
- Sigma detected: Bad Opsec Default…
- Creates multiple autostart registry ke…
- Sigma detected: Suspicious Script E…
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64**
- 9JbJZPtaKF.exe (PID: 6972 cmdline: 'C:\Users\user\Desktop\9JbJZPtaKF.exe' MD5: 133C10454108AA86301F79A03AA24046)
  - RegAsm.exe (PID: 7040 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 7084 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - cmd.exe (PID: 4348 cmdline: 'C:\Windows\System32\cmd.exe' /c start /b powershell ExecutionPolicy Bypass Start-Process -FilePath "C:\Users\user\AppData\Local\Temp\mmybgd.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 2132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 720 cmdline: powershell ExecutionPolicy Bypass Start-Process -FilePath "C:\Users\user\AppData\Local\Temp\mmybgd.exe" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - mmybgd.exe (PID: 4776 cmdline: 'C:\Users\user\AppData\Local\Temp\mmybgd.exe' MD5: BDC628B212725C5FD4287591393CB44E)
          - RegAsm.exe (PID: 4676 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- ct.exe (PID: 4644 cmdline: 'C:\Users\user\AppData\Roaming\cf\ct.exe' MD5: 133C10454108AA86301F79A03AA24046)
  - RegAsm.exe (PID: 5916 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- ct.exe (PID: 5344 cmdline: 'C:\Users\user\AppData\Roaming\cf\ct.exe' MD5: 133C10454108AA86301F79A03AA24046)
  - RegAsm.exe (PID: 6740 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6756 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- bg.exe (PID: 6184 cmdline: 'C:\Users\user\AppData\Roaming\bp\bg.exe' MD5: BDC628B212725C5FD4287591393CB44E)
  - RegAsm.exe (PID: 2532 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 5276 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6580 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 3176 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- bg.exe (PID: 7072 cmdline: 'C:\Users\user\AppData\Roaming\bp\bg.exe' MD5: BDC628B212725C5FD4287591393CB44E)
  - RegAsm.exe (PID: 6748 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6696 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6764 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000003.307140566.00000000006F4000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000003.325430436.000000000723000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000B.00000003.306946941.00000000006DF000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000000.00000003.280115518.00000000007EF000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000B.00000003.306899015.00000000006EA000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 42 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.3.ct.exe.739714.2.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
14.3.ct.exe.739714.2.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.3.9JbJZPtaKF.exe.7ee9c8.3.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.3.9JbJZPtaKF.exe.8051e4.1.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
11.3.ct.exe.6f4934.1.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 24 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: PowerShell Script Run in AppData

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Connects to many ports of the same IP (likely port scanning)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Data Obfuscation:

Suspicious powershell command line found

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Creates files in alternative data streams (ADS)

Malware Analysis System Evasion:

Yara detected AntiVM3

Yara detected AsyncRAT

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:

Sample uses process hollowing technique

Writes to foreign memory regions

Bypasses PowerShell execution policy

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

Yara detected BitRAT

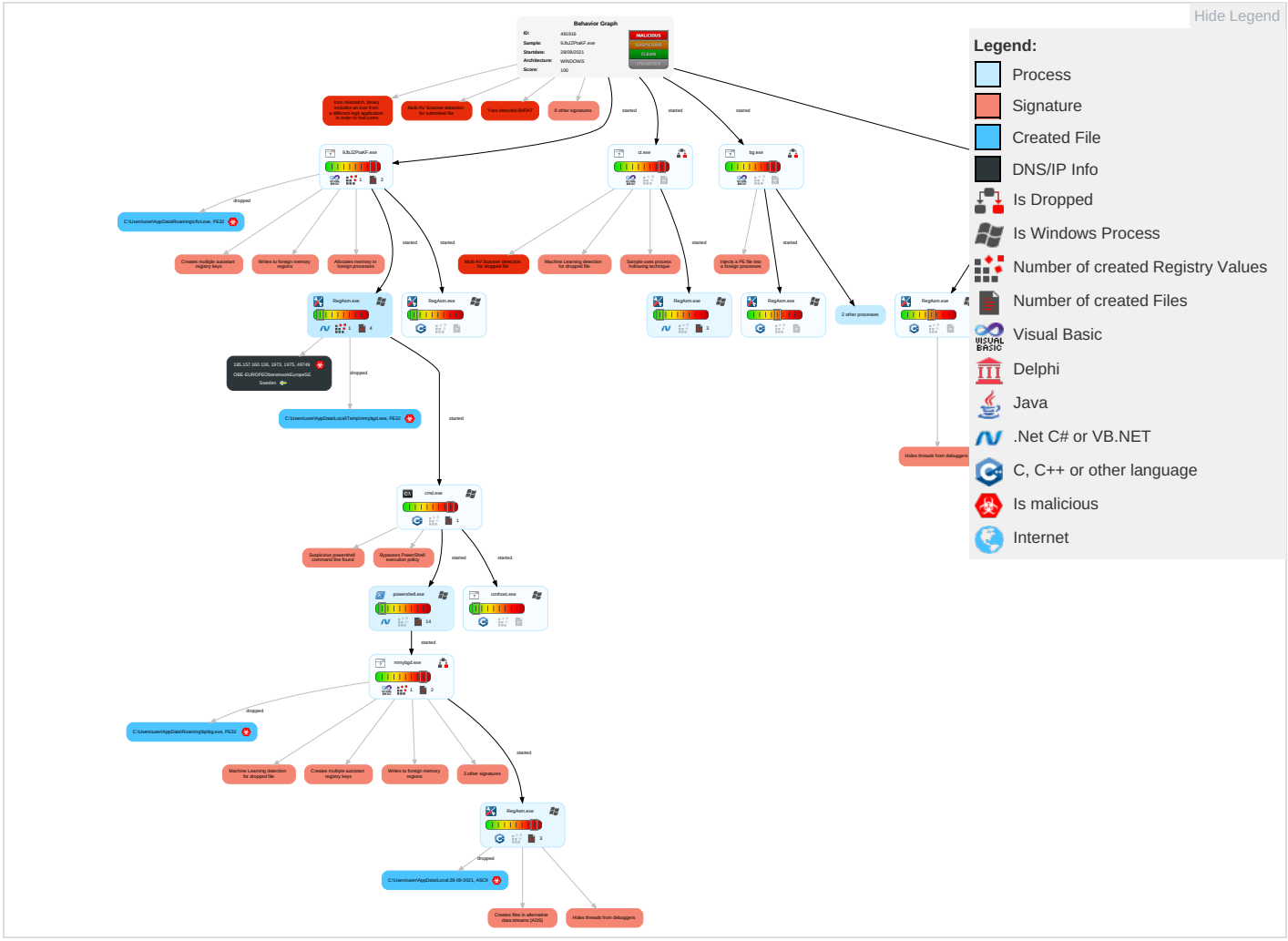
Remote Access Functionality:

Yara detected BitRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Scheduled Task/Job 1	Process Injection 4 1 2	Obfuscated Files or Information 1 2 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls
Domain Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1 1	Scheduled Task/Job 1	Software Packing 1 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Explo Track Local
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 1	DLL Side-Loading 1	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	NTFS File Attributes 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

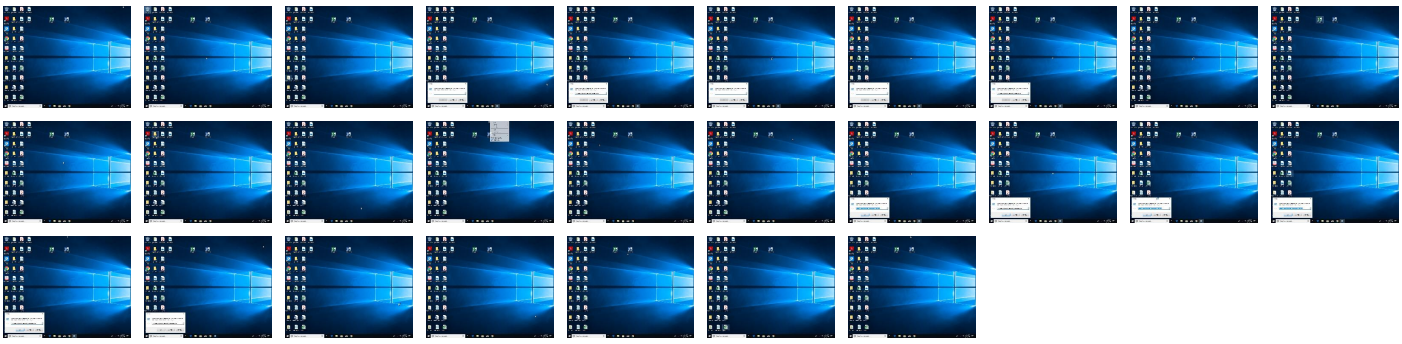
Behavior Graph



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
9JbJZPtaKF.exe	35%	Virustotal		Browse
9JbJZPtaKF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\bp\bg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cf\ct.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\mmybgd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cf\ct.exe	40%	ReversingLabs	Win32.Trojan.Sabsik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.3.ct.exe.739714.1.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
0.3.9JbJZPtaKF.exe.8051e4.1.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
14.3.ct.exe.739714.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
37.2.RegAsm.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140205		Download File
41.2.RegAsm.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140205		Download File
31.2.RegAsm.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140205		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.3.ct.exe.6f4934.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
0.3.9JbJZPtaKF.exe.8051e4.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
11.3.ct.exe.6f4934.1.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
17.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.160.136	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491916
Start date:	28.09.2021
Start time:	07:22:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9JbJZPtaKF.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:	44
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@38/9@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:23:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run cp C:\Users\user\AppData\Roaming\cf\ct.exe
07:23:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run cp C:\Users\user\AppData\Roaming\cf\ct.exe
07:24:14	API Interceptor	26x Sleep call for process: powershell.exe modified
07:24:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run bm C:\Users\user\AppData\Roaming\bp\bg.exe
07:24:27	API Interceptor	379x Sleep call for process: RegAsm.exe modified
07:24:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run bm C:\Users\user\AppData\Roaming\bp\bg.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local:28-09-2021	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Local:28-09-2021	
Category:	dropped
Size (bytes):	128
Entropy (8bit):	4.936164137895121
Encrypted:	false
SSDEEP:	3:itC+AgK4mH8ogt03wrH8ogt0tJlZpKDBWJln:ioDgYH8ogt1vgtoppSc3
MD5:	F272081EB6D5BDF88A7CDDE29E8AC150
SHA1:	EB718AB1BE89F9EB73AC8F1A19D82157DC6E309F
SHA-256:	078B6A10730E390E9D44581EA9948AD370D0FC9615EC9598AFEAFF412B6A1CAD
SHA-512:	90AA2580785EB0F867D92356D97807759A2CC509ED898B50F9EEAFEF1696D857D55FA997F2ADC6BB5BE319F6B207CEC4E24E9D436FA842C1453883A10B3E1A8
Malicious:	**true**
Reputation:	unknown
Preview:	<block><data>CkNsaXBib2FyZCBkYXRhOiBbQ0xJUEJPQVJEX1NUQVJUXTBbQ0xJUEJPQVJEX0VORF0K</data></block><block><data>cg==</data></block>

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16444
Entropy (8bit):	5.57046790718648
Encrypted:	false
SSDEEP:	384:dt9HXJTXEnrm6RpSBKnEul6SE7Y9gbprcQTDYZy:IRp4KEuljcxRTEI
MD5:	9C5740419512622E220DE5BBAF6FA1EC
SHA1:	0EAE04DCFA63BB866F7ECFFF9126338A96A26F33
SHA-256:	E3800672313D0EC981794F8F0E9E4487EE4704FBBE63006CCC317A9A7DCCD32C
SHA-512:	9E15658FEA652B440D51C183F95D90DC8FACFA6F56A9DC7026BB1E4F72A4D07AE023A8F82FFE93E9B6ACD3348AB5D1F5B1A7C84263036296796C0DFA73E93A B
Malicious:	false
Reputation:	unknown
Preview:	@...e.....?.7.7.....%.....@.....H.....<@.^.L."My....'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)s.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F. <;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wp4lsxaf.jau.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wp4lsxaf.jau.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yyk0woll.01u.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp\mmybgd.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4731304
Entropy (8bit):	7.880890582164195
Encrypted:	false
SSDEEP:	98304:YC2pE1Qeauo7Bnr3VGKkN2YxQ6BmvS4KB0hUXTMpJgGFwN6bmNNuRhEt:YC2pEieC7BL2Cvsah/pJgTN6bmNkDEt
MD5:	BDC628B212725C5FD4287591393CB44E
SHA1:	AE1D2F0C1480C0CBD02703D41AE76C36FC011BE8
SHA-256:	78F869F3203033C6B2D25C30D545F8BB6D701357B4D870E2707F92A68790DCE9
SHA-512:	6EDCA221CCC9DB764A88898CA1AA7FF6C3E50C4720321EA59C811D7876749428AEF9261486F7AC7B1D6C0DDEFA1B6399A105449885C7D20CA591CA3645A1FA D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	 MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....Rich.....PE..L.....Oa..... ..... 4..... ....@.....@.....6H.....T...(....p.....(... .....d.....text..... ..`.da ta...HJ... ....@....rsrc.....p.....0.....@..@..^.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\bp\bg.exe	
Process:	C:\Users\user\AppData\Local\Temp\mmybgd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4731304
Entropy (8bit):	7.880890582164195
Encrypted:	false
SSDEEP:	98304:YC2pE1Qeauo7Bnr3VGKkN2YxQ6BmvS4KB0hUXTMpJgGFwN6bmNNuRhEt:YC2pEieC7BL2Cvsah/pJgTN6bmNkDEt
MD5:	BDC628B212725C5FD4287591393CB44E
SHA1:	AE1D2F0C1480C0CBD02703D41AE76C36FC011BE8
SHA-256:	78F869F3203033C6B2D25C30D545F8BB6D701357B4D870E2707F92A68790DCE9
SHA-512:	6EDCA221CCC9DB764A88898CA1AA7FF6C3E50C4720321EA59C811D7876749428AEF9261486F7AC7B1D6C0DDEFA1B6399A105449885C7D20CA591CA3645A1FA D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\bp\bg.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....Rich.....PE..L.....Oa..... ..... 4..... ....@.....@.....6H.....T...(....p.....(... .....d.....text..... ..`.da ta...HJ... ....@....rsrc.....p.....0.....@..@..^.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\cf\ct.exe	
Process:	C:\Users\user\Desktop\9JbJZPtaKF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	666024
Entropy (8bit):	6.300855326189978
Encrypted:	false
SSDEEP:	6144:Xsh7P4K387yYg9ihPBJ1G08ozfjqXXTewGJX/MHeKPwE+8sS6rU8jcxJ8:8h7l38OKJBWkzfwS/M+KGtLHX
MD5:	133C10454108AA86301F79A03AA24046
SHA1:	21439179CB8700406D57332079AB311D08B0C9BF
SHA-256:	DE0CB500125D733BECBDEB53CF7B3F1BACE4DC91E54805007718970124EF6797
SHA-512:	8B2A492A5732C89C2E347270E9B1DF4DB26B79FEFD6FEAE115B35A22B0851C7973FB0ECC9B6C6187791BF720D71A7B69374D81ABF63F0ED73FAED4EFBEE79FBE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....Rich.....PE..L.....Oa..... 4..... ....@.....Z.....T...(...p...3.....(... .....d.....text..... ..`.da ta...HJ... ....@....rsrc....3...p...@...0.....@..@..^.....MSVBVM60.DLL..... ....

C:\Users\user\Documents\20210928\PowerShell_transcript.088753.vlQ_yutw.20210928072352.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1023
Entropy (8bit):	5.163353160334551
Encrypted:	false
SSDEEP:	24:BxSA45xvBnVvx2DOXVVoWdeW9HjeTKKjX4Clym1ZJXUPVoWdfnxSAZ3:BZovhVvoOFGu9qDYB1Z2PGUZZ3
MD5:	6A130F3DDD89490FE85813ED0C44A58F
SHA1:	34FEEAA9FA7E877B4FE3ED5380FF6F9F84A56AC9
SHA-256:	81FFC9EA5A3E0F3D7F2ECDAA463259A4A39EA6190375892D90A8DBB35D82E1AC
SHA-512:	3B611F782E322C40274ADA7F938E16401BFCEB6DB861F2F700CBE40C0ABB5C89CF4ECEAD67357FF456C82469089CE1DD7160E54CD99F3878083F1D7FBD521D7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210928072409..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 088753 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell .ExecutionPolicy Bypass Start-Process -FilePath 'C:\Users\user\AppData\Local\Temp\mmybgd.exe'..Process ID: 720..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210928072409..**********..PS>Start-Process -FilePath 'C:\Users\user\AppData\Local\Temp\mmybgd.exe'..**********..Command start time: 20210928072740..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210928072740..*

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.300855326189978
TrID:	• Win32 Executable (generic) a (10002005/4) 98.72% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • InstallShield setup (43055/19) 0.42% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	9JbJZPtaKF.exe
File size:	666024

General

MD5:	133c10454108aa86301f79a03aa24046
SHA1:	21439179cb8700406d57332079ab311d08b0c9bf
SHA256:	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797
SHA512:	8b2a492a5732c89c2e347270e9b1df4db26b79fefd6feae115b35a22b0851c7973fb0ecc9b6c6187791bf720d71a7b69374d81abf63f0ed73faed4efbee79fbe
SSDEEP:	6144:Xsh7P4K387yYg9ihPBJ1G08ozfjqXXTewGJX/MHeKPwE+8sS6rU8jcxJ8:8h7l38OKJBWkzfwS/M+KGtLHX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....Rich.....PE..L.....Oa.....4..... ....@.....

File Icon

Icon Hash:	eccccd4d4e8e096

Static PE Info

General

Entrypoint:	0x4034f0
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:	0x614F12F6 [Sat Sep 25 12:15:50 2021 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:	835f485ca718411734d873f35af1695e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x801c8	0x81000	False	0.334565391836	data	6.2183301582	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x82000	0x4a48	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x87000	0x133f8	0x14000	False	0.338671875	data	5.02760964735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

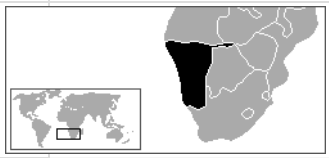
Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	
Danish	Denmark	
Afrikaans	South Africa	
Afrikaans	Namibia	
Arabic	Jordan	

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 9JbJZPtaKF.exe PID: 6972 Parent PID: 4768

General

Start time:	07:23:07
Start date:	28/09/2021

Path:	C:\Users\user\Desktop\9JbJZPtaKF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\9JbJZPtaKF.exe'
Imagebase:	0x400000
File size:	666024 bytes
MD5 hash:	133C10454108AA86301F79A03AA24046
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.280115518.00000000007EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.280183910.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278483376.00000000007D7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278249926.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278304939.0000000000805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278201980.00000000007FA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278470265.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278264012.00000000007EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.280278807.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278240068.00000000007EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000003.278220853.00000000007D7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegAsm.exe PID: 7040 Parent PID: 6972

General

Start time:	07:23:08
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x2e0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 7084 Parent PID: 6972

General

Start time:	07:23:08
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xad0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.544974477.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000003.356231512.00000000061A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.554990912.0000000002EE8000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: ct.exe PID: 4644 Parent PID: 3352

General

Start time:	07:23:20
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\cf\ct.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\cf\ct.exe'
Imagebase:	0x400000
File size:	666024 bytes
MD5 hash:	133C10454108AA86301F79A03AA24046
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.307140566.00000000006F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.306946941.00000000006DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.306899015.00000000006EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.306958807.00000000006FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.308889804.00000000006FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.306989450.00000000006DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.306923152.00000000006C7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.308874401.00000000006DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000003.308858373.00000000006FF000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: RegAsm.exe PID: 5916 Parent PID: 4644

General

Start time:	07:23:21
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc50000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000C.00000002.322158875.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: ct.exe PID: 5344 Parent PID: 3352

General

Start time:	07:23:28
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\cf\ct.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\cf\ct.exe'
Imagebase:	0x400000
File size:	666024 bytes
MD5 hash:	133C10454108AA86301F79A03AA24046
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325430436.0000000000723000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.327182152.0000000000744000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325299126.000000000070C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325371450.0000000000744000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325340924.0000000000723000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.327210322.0000000000723000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.327236288.0000000000744000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325501534.0000000000739000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000003.325118501.000000000072F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: RegAsm.exe PID: 6740 Parent PID: 5344

General

Start time:	07:23:30
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x3c0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6756 Parent PID: 5344

General

Start time:	07:23:30
Start date:	28/09/2021

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x680000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000002.340503270.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 4348 Parent PID: 7084

General

Start time:	07:23:48
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c start /b powershell ExecutionPolicy Bypass Start-Process -FilePath "C:\Users\user\AppData\Local\Temp\mmybgd.exe" & exit
Imagebase:	0xd80000
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 Show Windows behavior

Analysis Process: conhost.exe PID: 2132 Parent PID: 4348

General

Start time:	07:23:48
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: powershell.exe PID: 720 Parent PID: 4348

General

Start time:	07:23:49
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell ExecutionPolicy Bypass Start-Process -FilePath "C:\Users\user\AppData\Local\Temp\mmybgd.exe"
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: mmybgd.exe PID: 4776 Parent PID: 720

General

Start time:	07:24:21
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Temp\mmybgd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\mmybgd.exe'
Imagebase:	0x400000
File size:	4731304 bytes
MD5 hash:	BDC628B212725C5FD4287591393CB44E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegAsm.exe PID: 4676 Parent PID: 4776

General

Start time:	07:24:23
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x890000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: 0000001F.00000002.544923977.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: bg.exe PID: 6184 Parent PID: 3352

General

Start time:	07:24:32
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\bp\bg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bp\bg.exe'
Imagebase:	0x400000
File size:	4731304 bytes
MD5 hash:	BDC628B212725C5FD4287591393CB44E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: 00000021.00000003.462953448.00000000034F0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: RegAsm.exe PID: 2532 Parent PID: 6184

General

Start time:	07:24:34
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x560000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 5276 Parent PID: 6184

General

Start time:	07:24:35
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x330000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 6580 Parent PID: 6184

General

Start time:	07:24:35
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x250000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 3176 Parent PID: 6184

General

Start time:	07:24:36
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xbc0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: 00000025.00000002.476289404.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: bg.exe PID: 7072 Parent PID: 3352

General

Start time:	07:24:41
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\bp\bg.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\bp\bg.exe'
Imagebase:	0x400000
File size:	4731304 bytes
MD5 hash:	BDC628B212725C5FD4287591393CB44E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic

Analysis Process: RegAsm.exe PID: 6748 Parent PID: 7072

General

Start time:	07:24:42
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x610000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 6696 Parent PID: 7072

General

Start time:	07:24:43
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x500000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 6764 Parent PID: 7072

General

Start time:	07:24:43
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc80000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BitRAT, Description: Yara detected BitRAT, Source: 00000029.00000002.491911455.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis