ID: 299740
Sample Name:
6FNEaMg3dNB7sGi.exe
Cookbook: default.jbs
Time: 08:35:16
Date: 18/10/2020
Version: 30.0.0 Red Diamond

Table of Contents

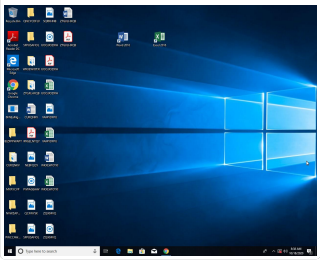
Analysis Report 6FNEaMg3dNB7sGi.exe

Overview

General Information

Sample Name:	6FNEaMg3dNB7sGi.exe
Analysis ID:	299740
MD5:	fbf6c63acd92d19..
SHA1:	74ce9041a05b41..
SHA256:	2ac56457e5dfd88.
Tags:	DHL exe nVpn RAT Remcos RAT

Most interesting Screenshot:



Detection

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

Signatures

- Detected Remcos RAT
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Remcos RAT
- Contains functionality to capture and…
- Contains functionality to inject code …
- Contains functionality to steal Chrom…
- Contains functionality to steal Firefo…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Uses dynamic DNS services
- Uses schtasks.exe or at.exe to add …
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…
- Contains functionality for read data f…
- Contains functionality to download a…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to enumerate …
- Contains functionality to launch a co…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the cli…
- Contains functionality to shutdown / …
- Contains functionality to simulate m…

Classification

Startup

- **System is w10x64**
- 6FNEaMg3dNB7sGi.exe (PID: 5668 cmdline: 'C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe' MD5: FBF6C63ACD92D191FB1A77F15B90850C)
  - schtasks.exe (PID: 2456 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QDsgqHC' /XML 'C:\Users\user\AppData\Local\Temp\tmp2759.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 6FNEaMg3dNB7sGi.exe (PID: 3080 cmdline: C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe MD5: FBF6C63ACD92D191FB1A77F15B90850C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.924829798.000000000400000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000005.00000002.924829798.000000000400000.00000040.00000001.sdmp	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
00000005.00000002.924829798.000000000400000.00000040.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
00000000.00000002.673950548.000000000327000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.673950548.000000000327000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.6FNEaMg3dNB7sGi.exe.400000.0.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
5.2.6FNEaMg3dNB7sGi.exe.400000.0.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...

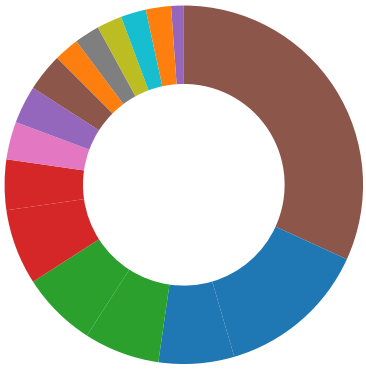
Source	Rule	Description	Author	Strings
5.2.6FNEaMg3dNB7sGi.exe.400000.0.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
5.2.6FNEaMg3dNB7sGi.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
5.2.6FNEaMg3dNB7sGi.exe.400000.0.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Remcos RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to capture and log keystrokes

E-Banking Fraud:

- Yara detected Remcos RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject code into remote processes
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Remcos RAT
- Contains functionality to steal Chrome passwords or cookies
- Contains functionality to steal Firefox passwords or cookies

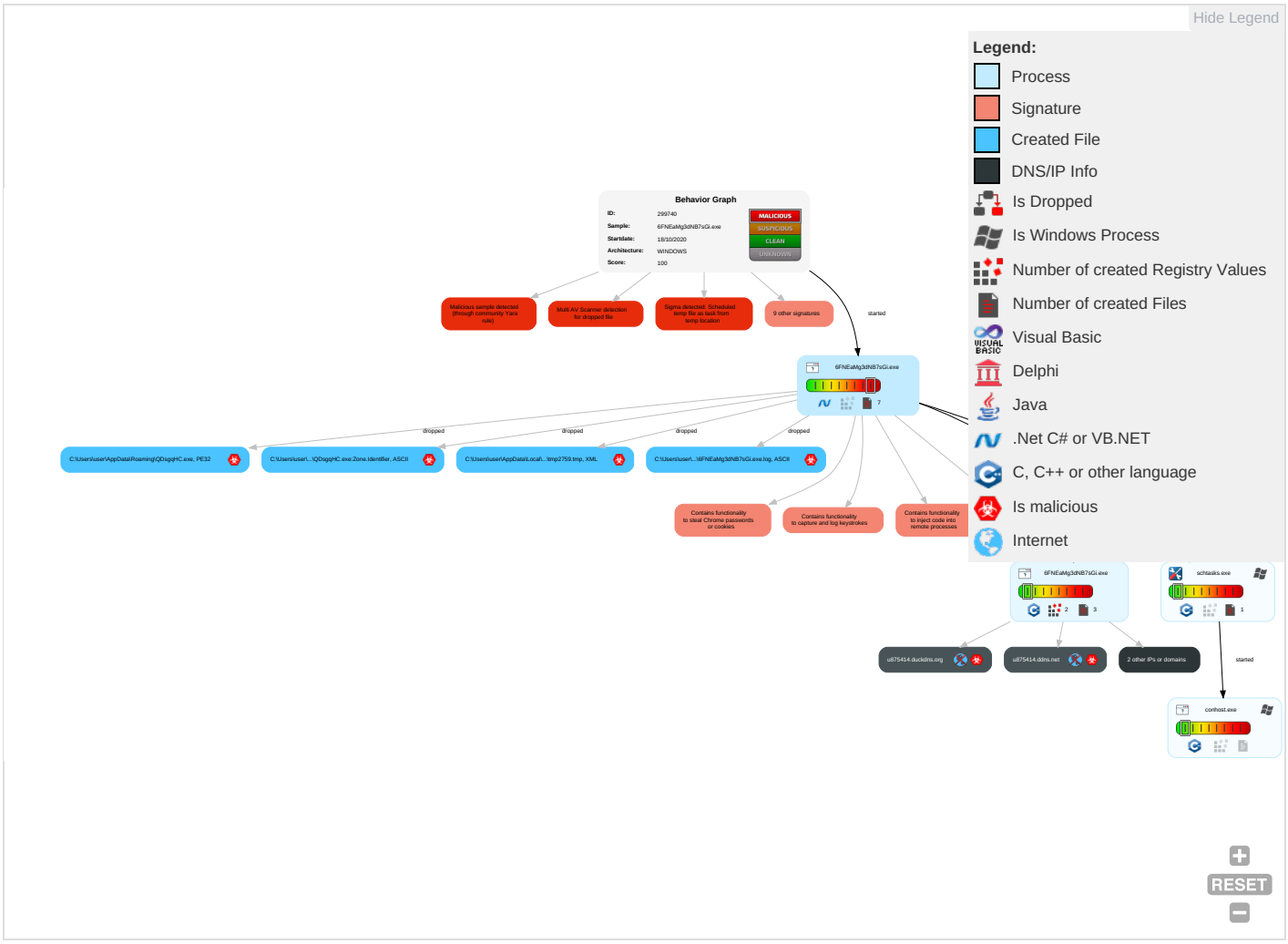
Remote Access Functionality:

- Detected Remcos RAT
- Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Windows Service 1	Obfuscated Files or Information 3	Credentials In Files 2	System Service Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration
Local Accounts	Service Execution 2	Logon Script (Mac)	Process Injection 2 2 2	Software Packing 2	NTDS	File and Directory Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Scheduled Task/Job 1	Masquerading 1	LSA Secrets	System Information Discovery 4 3	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Security Software Discovery 2 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 2 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

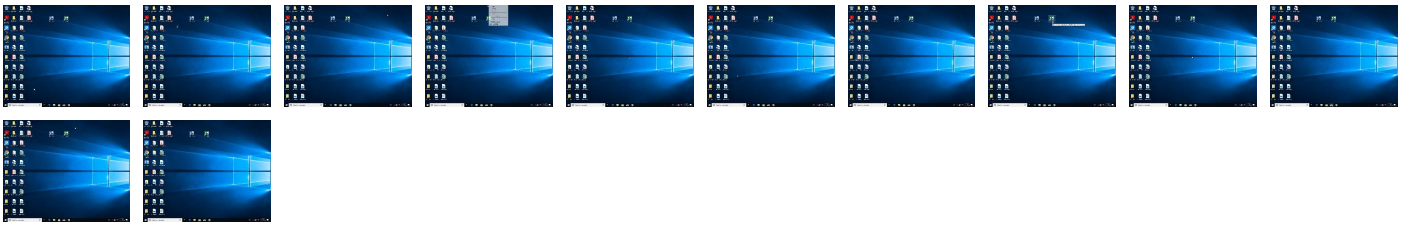
Behavior Graph



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
6FNEaMg3dNB7sGi.exe	24%	Virustotal		Browse
6FNEaMg3dNB7sGi.exe	25%	ReversingLabs	Win32.Trojan.AgentTesla	
6FNEaMg3dNB7sGi.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QDsgqHC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\QDsgqHC.exe	25%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.6FNEaMg3dNB7sGi.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
u875414.nvpn.to	1%	Virustotal		Browse
u875414.nsupdate.info	1%	Virustotal		Browse
u875414.ddns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microsoft.A	0%	Avira URL Cloud	safe	
http://tempuri.org/ScrapDBDataSet.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

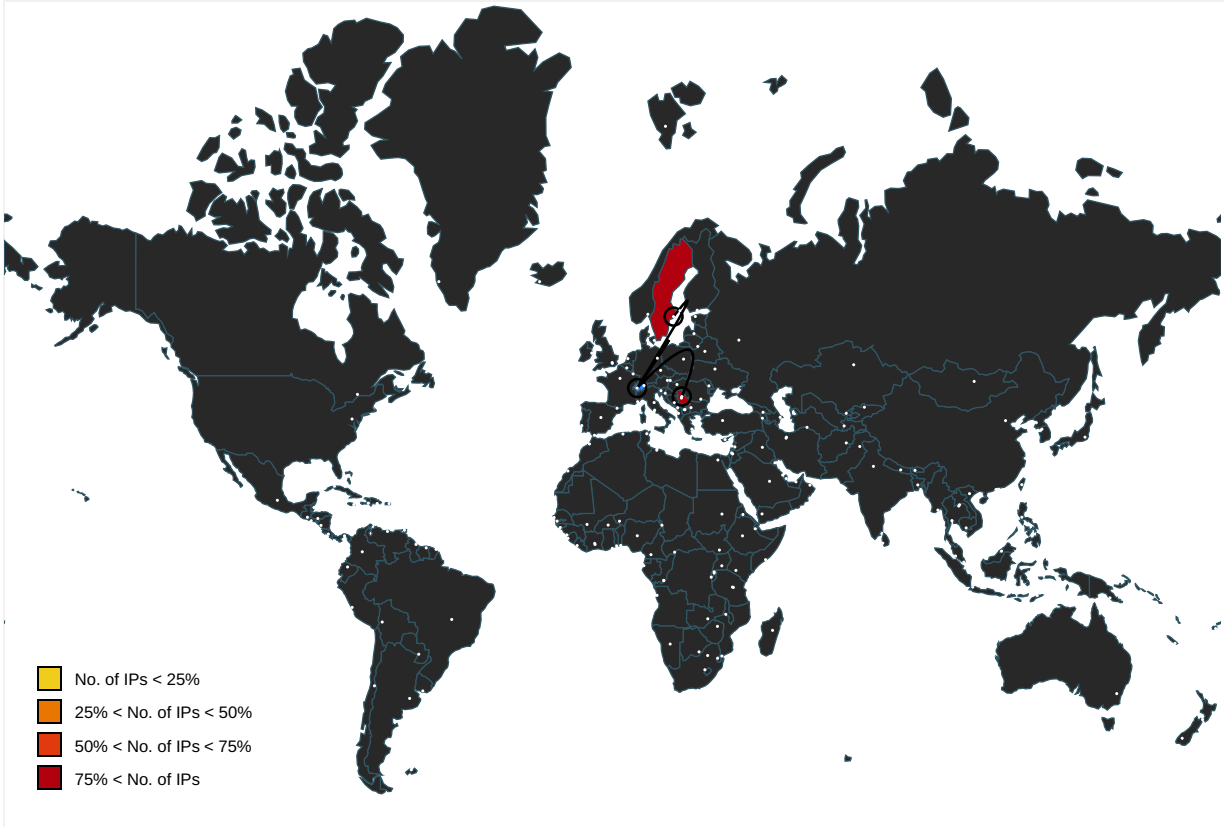
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
u875414.nvpn.to	185.140.53.228	true	false	• 1%, Virustotal, Browse	unknown
u875414.nsupdate.info	91.193.75.93	true	false	• 1%, Virustotal, Browse	unknown
u875414.ddns.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
u875414.duckdns.org	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.microsoft.A	6FNEaMg3dNB7sGi.exe, 00000000.00000002.674238422.00000000042790000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	6FNEaMg3dNB7sGi.exe, 00000000.00000002.673950548.00000000032710000.00000004.00000001.sdmp	false		high
http://tempuri.org/ScrapDBDataSet.xsd	6FNEaMg3dNB7sGi.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
185.140.53.228	Sweden		209623	DAVID_CRAIGGG	false
91.193.75.93	Serbia		209623	DAVID_CRAIGGG	false

General Information

Joe Sandbox Version:	30.0.0 Red Diamond
Analysis ID:	299740
Start date:	18.10.2020
Start time:	08:35:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6FNEaMg3dNB7sGi.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:	7
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.spyw.evad.winEXE@6/5@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 41.9% (good quality ratio 32.4%) • Quality average: 56.8% • Quality standard deviation: 40%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, backgroundTaskHost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 205.185.216.10, 205.185.216.42 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.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
08:36:12	API Interceptor	1032x Sleep call for process: 6FNEaMg3dNB7sGi.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.228	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	
	DHL scan.exe	Get hash	malicious	Browse	
	DHL scan.exe	Get hash	malicious	Browse	
	XXTOvq5aLpY1whm.exe	Get hash	malicious	Browse	
91.193.75.93	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	
	DHL scan.exe	Get hash	malicious	Browse	
	DHL scan.exe	Get hash	malicious	Browse	
	XXTOvq5aLpY1whm.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
u875414.nsupdate.info	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	• 91.193.75.93
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	• 91.193.75.93
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	• 91.193.75.93
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	• 91.193.75.93
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	• 91.193.75.93
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	• 91.193.75.93
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	XXTOvq5aLpY1whm.exe	Get hash	malicious	Browse	• 91.193.75.93
u875414.nvpn.to	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	• 185.140.53.228
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	• 185.140.53.228
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	• 185.140.53.228
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	• 185.140.53.228
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	• 185.140.53.228
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	• 185.140.53.228
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	• 185.140.53.228
	DHL scan.exe	Get hash	malicious	Browse	• 185.140.53.228
	DHL scan.exe	Get hash	malicious	Browse	• 185.140.53.228
	XXTOvq5aLpY1whm.exe	Get hash	malicious	Browse	• 185.140.53.228
	UPS Details.exe	Get hash	malicious	Browse	• 23.105.131.185
	Xfltdrn_Signed_.exe	Get hash	malicious	Browse	• 23.105.131.185

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Quotation 52908.exe	Get hash	malicious	Browse	• 185.165.153.243
	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	• 91.193.75.93
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	• 91.193.75.93
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	• 91.193.75.93
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	• 91.193.75.93
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.30.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1610202037463,pdf.exe	Get hash	malicious	Browse	• 91.193.75.246
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL_746361.exe	Get hash	malicious	Browse	• 185.165.153.126
	SMFPQm4vpC4IwA3.exe	Get hash	malicious	Browse	• 185.140.53.68
	SCB_MT103_83638T2000028212_0534281.PDF.exe	Get hash	malicious	Browse	• 185.244.30.121
	DHL_091995.exe	Get hash	malicious	Browse	• 185.165.153.126
	Proforma.exe	Get hash	malicious	Browse	• 185.165.153.249
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	• 91.193.75.93
	Best#U00e4tigung der Kontodaten,rar.exe	Get hash	malicious	Browse	• 185.244.30.3
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	Order 20015639 15-10-2020,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	2020101508898,pdf.exe	Get hash	malicious	Browse	• 185.165.153.245
DAVID_CRAIGGG	Quotation 52908.exe	Get hash	malicious	Browse	• 185.165.153.243
	36bgu0AlofWEwXq.exe	Get hash	malicious	Browse	• 91.193.75.93
	Sjykvu95w2zmmQr.exe	Get hash	malicious	Browse	• 91.193.75.93
	eyV78Kl9ybgBwge.exe	Get hash	malicious	Browse	• 91.193.75.93
	z3ZOEume404sYCn.exe	Get hash	malicious	Browse	• 91.193.75.93
	1lXgHRALOGfjaD2.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.30.39
	1610202037463,pdf.exe	Get hash	malicious	Browse	• 91.193.75.246
	xNFUgCJB5e4SLEw.exe	Get hash	malicious	Browse	• 91.193.75.93
	DHL_746361.exe	Get hash	malicious	Browse	• 185.165.153.126
	SMFPQm4vpC4IwA3.exe	Get hash	malicious	Browse	• 185.140.53.68
	SCB_MT103_83638T2000028212_0534281.PDF.exe	Get hash	malicious	Browse	• 185.244.30.121
	DHL_091995.exe	Get hash	malicious	Browse	• 185.165.153.126
	Proforma.exe	Get hash	malicious	Browse	• 185.165.153.249
	PssSvDilfp5BvnU.exe	Get hash	malicious	Browse	• 91.193.75.93
	Best#U00e4tigung der Kontodaten,rar.exe	Get hash	malicious	Browse	• 185.244.30.3
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	Order 20015639 15-10-2020,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135
	DHL scan.exe	Get hash	malicious	Browse	• 91.193.75.93
	2020101508898,pdf.exe	Get hash	malicious	Browse	• 185.165.153.245

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6FNEaMg3dNB7sGi.exe.log	
Process:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6FNEaMg3dNB7sGi.exe.log	
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2759.tmp	
Process:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.182002637488805
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGxNtn:cbhK79lNQR/rydbz9l3YODOLNdq32n
MD5:	34463D4BA8D4A54F0E7F539369BA6510
SHA1:	D5BE7F9E370C30AB9689177C5440599E2E8D2587
SHA-256:	520F65B9281060A3DE993B8789D8F673B1930A0C1BF672C24F1021761E9D6514
SHA-512:	B41F0ECEFBBBF2F2E34608CEB40926DA9C57800CFCDB90D4AE38D6B59B5A14A46A8B306BF65EDB91BF5795C0664F6A9B871502CFB7FB65576A4E152B7C85B522
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\QDsgqHC.exe	
Process:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	7.181874643507636
Encrypted:	false
SSDEEP:	12288:0gEcQd3STz36T4IBIZT9oPb6Gxbql62ebKcJUwAbjYFbgAiaiZ:0gEd38jc1i5oPb6Gx2lf5Db0fC
MD5:	FBF6C63ACD92D191FB1A77F15B90850C
SHA1:	74CE9041A05B4195660D3CE5AC1F6F620F14818D
SHA-256:	2AC56457E5DFD887F318AB16BBC8FA9711095B8CB4CAE99F5A34358C9A8502F0
SHA-512:	1AEB9E6E609C47CF3E83BDE6316A334EBA37DE70695E86F4F545C88F16818855248AA3B9F7123E9EB923FC1788A308BC109DAE04FEE3FBBCAC1BD70DCEE19093
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 25%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.P..... .....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....f...h.....X....d.....0..#.....+.&...(....(.....(.....o.....*.....0..r.....+.&..8Y.....88....8r.....1a.+3..2a.+"..-a8.....+XE.....@....,(.....+.....+.....&...+...)YE.....'...`....-(.....+.+...(.....+.....&...8z.....'XE.....(...1..@...O...k.....8A...85.....8,.....8#.....8.....8..... (.....8.....(.....8.....(....+..8.....'(.....8.....(....+.(..

C:\Users\user\AppData\Roaming\QDsgqHC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.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

C:\Users\user\AppData\Roaming\QDsgqHC.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\September\logs.dat	
Process:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
File Type:	data
Category:	dropped
Size (bytes):	143
Entropy (8bit):	6.157185476741649
Encrypted:	false
SSDEEP:	3:GhYH34qLhDhoP+Fi6sf+mYH34qLhDhoP+Fi6yUPaICdr2tnDAs/:9oqVDhoP6UuoqVDhoP6qWRCktnDV
MD5:	5EC7DFD38359AB1B9A8617900266005E
SHA1:	6595BFB9D891382E8FE8C729CFA0BF164781BB74
SHA-256:	BF7B4FE9589B74ECBF65DF2A19BFAF7D944F54F0101FFA752BE7D7F233D7DF39
SHA-512:	ACA1A1AA7B9F223085B871011B1AE4C7AADD2025918DB27C79F095451E2599749EFE03CD9D56A8183DCA287B72A9E0B274C6DDA78BBB8F390DFDB6DF0105F3FB
Malicious:	false
Reputation:	low
Preview:	.....:[C..b...{.....Pg;...U..x....P...lc....5.y.....:[C..b...{.....Pg;...U..x....P...lc....5.y.....'0...j.N@PA...8...H.Rv.(tzNX$Y.,MI>)G

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.181874643507636
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	6FNEaMg3dNB7sGi.exe
File size:	703488
MD5:	fbf6c63acd92d191fb1a77f15b90850c
SHA1:	74ce9041a05b4195660d3ce5ac1f6f620f14818d
SHA256:	2ac56457e5dfd887f318ab16bbc8fa9711095b8cb4cae99f5a34358c9a8502f0
SHA512:	1aeb9e6e609c47cf3e83bde6316a334eba37de70695e864f545c88f16818855248aa3b9f7123e9eb923fc1788a308bc109dae04fee3fbbcac1bd70dcee19093
SSDEEP:	12288:0gEcQd3STz36T4IBIZT9oPb6Gxbql62ebKcJUwAbjYFbgAiaiZ:0gEd38jc1i5oPb6Gx2lf5Db0fC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....__.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ad00e
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F8B5FF2 [Sat Oct 17 21:19:46 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], 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 [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xacfc0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xab014	0xab200	False	0.658156044558	data	7.19031633463	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x600	0x600	False	0.420572916667	data	4.06915444157	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xae090	0x30c	data		
RT_MANIFEST	0xae3ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

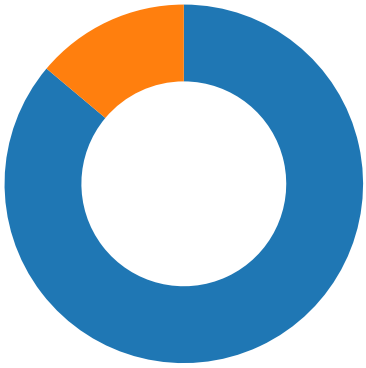
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	OhJ6.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ScrapBook
ProductVersion	1.0.0.0
FileDescription	ScrapBook
OriginalFilename	OhJ6.exe

Network Behavior

Network Port Distribution

Total Packets: 36

- 53 (DNS)
- 2404 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 18, 2020 08:36:16.707556009 CEST	49714	2404	192.168.2.4	185.140.53.228
Oct 18, 2020 08:36:16.741254091 CEST	2404	49714	185.140.53.228	192.168.2.4
Oct 18, 2020 08:36:17.246105909 CEST	49714	2404	192.168.2.4	185.140.53.228
Oct 18, 2020 08:36:17.278680086 CEST	2404	49714	185.140.53.228	192.168.2.4
Oct 18, 2020 08:36:17.795845985 CEST	49714	2404	192.168.2.4	185.140.53.228
Oct 18, 2020 08:36:17.828624964 CEST	2404	49714	185.140.53.228	192.168.2.4
Oct 18, 2020 08:36:18.128592014 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:18.329179049 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:18.329315901 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:18.331655025 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:18.574321985 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:18.577596903 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:18.817370892 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:23.576164007 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:23.578578949 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:23.954308987 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:28.592190981 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:28.595143080 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:28.841459036 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:33.598614931 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:33.601352930 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:33.847816944 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:38.612173080 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:38.614538908 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:38.860652924 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:43.618912935 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:43.622745037 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:43.868424892 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:48.622984886 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:48.625819921 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:48.872567892 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:53.631346941 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:53.634885073 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:53.880423069 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:58.645031929 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:36:58.702739000 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:58.796132088 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:36:59.054939985 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:03.649418116 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:03.652694941 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:03.899688959 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:08.663028955 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:08.667824030 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:08.912913084 CEST	2404	49715	91.193.75.93	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 18, 2020 08:37:13.665544033 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:13.667679071 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:13.914664984 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:18.681214094 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:18.684514999 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:18.924757957 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:23.683208942 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:23.687633991 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:23.932292938 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:28.689172983 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:28.692888975 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:28.937769890 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:33.700844049 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:33.705394030 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:33.949827909 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:38.713012934 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:38.715890884 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:38.962532997 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:43.726108074 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:43.729057074 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:43.975394011 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:48.743196011 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:48.746728897 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:48.997128963 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:53.751075983 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:53.755745888 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:54.001481056 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:58.752528906 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:37:58.756833076 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:37:59.003273964 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:03.765316963 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:03.768338919 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:38:04.013098955 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:08.775618076 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:08.778745890 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:38:09.022773027 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:13.789796114 CEST	2404	49715	91.193.75.93	192.168.2.4
Oct 18, 2020 08:38:13.793747902 CEST	49715	2404	192.168.2.4	91.193.75.93
Oct 18, 2020 08:38:14.042665005 CEST	2404	49715	91.193.75.93	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 18, 2020 08:36:16.628041983 CEST	51025	53	192.168.2.4	8.8.8.8
Oct 18, 2020 08:36:16.691381931 CEST	53	51025	8.8.8.8	192.168.2.4
Oct 18, 2020 08:36:17.834645033 CEST	61516	53	192.168.2.4	8.8.8.8
Oct 18, 2020 08:36:18.040585041 CEST	53	61516	8.8.8.8	192.168.2.4
Oct 18, 2020 08:36:18.047099113 CEST	49182	53	192.168.2.4	8.8.8.8
Oct 18, 2020 08:36:18.083492041 CEST	53	49182	8.8.8.8	192.168.2.4
Oct 18, 2020 08:36:18.089869022 CEST	59920	53	192.168.2.4	8.8.8.8
Oct 18, 2020 08:36:18.127068043 CEST	53	59920	8.8.8.8	192.168.2.4
Oct 18, 2020 08:36:54.749509096 CEST	57458	53	192.168.2.4	8.8.8.8
Oct 18, 2020 08:36:54.773816109 CEST	53	57458	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 18, 2020 08:36:16.628041983 CEST	192.168.2.4	8.8.8.8	0x240b	Standard query (0)	u875414.nvpn.to	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:17.834645033 CEST	192.168.2.4	8.8.8.8	0xaf6	Standard query (0)	u875414.duckdns.org	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:18.047099113 CEST	192.168.2.4	8.8.8.8	0x75d2	Standard query (0)	u875414.ddns.net	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:18.089869022 CEST	192.168.2.4	8.8.8.8	0x392d	Standard query (0)	u875414.nsupdate.info	A (IP address)	IN (0x0001)

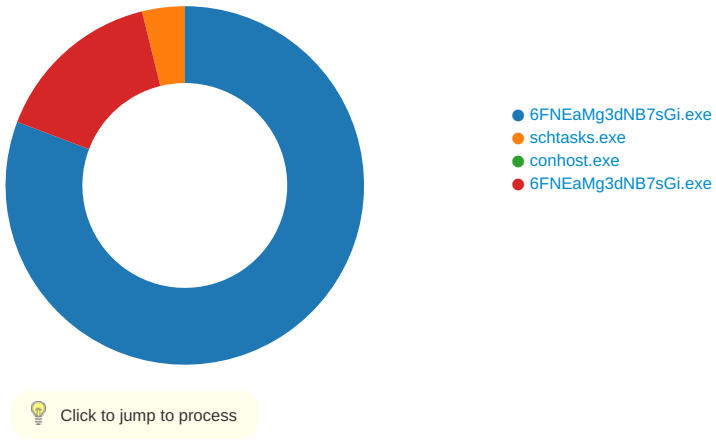
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 18, 2020 08:36:16.691381931 CEST	8.8.8.8	192.168.2.4	0x240b	No error (0)	u875414.nvpn.to		185.140.53.228	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:18.040585041 CEST	8.8.8.8	192.168.2.4	0xaf6	Name error (3)	u875414.duckdns.org	none	none	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:18.083492041 CEST	8.8.8.8	192.168.2.4	0x75d2	Name error (3)	u875414.ddns.net	none	none	A (IP address)	IN (0x0001)
Oct 18, 2020 08:36:18.127068043 CEST	8.8.8.8	192.168.2.4	0x392d	No error (0)	u875414.nsupdate.info		91.193.75.93	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 6FNEaMg3dNB7sGi.exe PID: 5668 Parent PID: 5960

General

Start time:	08:36:10
Start date:	18/10/2020
Path:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe'
Imagebase:	0xe60000
File size:	703488 bytes
MD5 hash:	FBF6C63ACD92D191FB1A77F15B90850C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.673950548.0000000003271000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.673950548.0000000003271000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.674238422.0000000004279000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\QDsgqHC.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	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\QDsgqHC.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2759.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6FNEaMg3dNB7sGi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2759.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QDsgqHC.exe	0	262144	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 80 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 50 45 00 00 4c 01 03 00 f2 5f 8b 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b2 0a 00 00 08 00 00 00 00 00 00 0e d0 0a 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...._._.......... ....P................. ....@.. ....@................	success or wait	3	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\QDsgqHC.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	6C01DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2759.tmp	unknown	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6FNEaMg3dNB7sGi.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 2456 Parent PID: 5668

General

Start time:	08:36:14
Start date:	18/10/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QDsgqHC' /XML 'C:\Users\user\AppData\Local\Temp\tmp2759.tmp'
Imagebase:	0xbb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2759.tmp	unknown	2	success or wait	1	BBAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2759.tmp	unknown	1641	success or wait	1	BBABD9	ReadFile

Analysis Process: conhost.exe PID: 984 Parent PID: 2456

General

Start time:	08:36:14
Start date:	18/10/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6FNEaMg3dNB7sGi.exe PID: 3080 Parent PID: 5668

General

Start time:	08:36:15
Start date:	18/10/2020

Path:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6FNEaMg3dNB7sGi.exe
Imagebase:	0x630000
File size:	703488 bytes
MD5 hash:	FBF6C63ACD92D191FB1A77F15B90850C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000002.924829798.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000005.00000002.924829798.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000005.00000002.924829798.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\September	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40564C	CreateDirectoryW
C:\Users\user\AppData\Roaming\September\logs.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	412D99	CreateFileW
C:\Users\user\AppData\Roaming\September	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40564C	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\September\logs.dat	unknown	51	1a 85 fd 19 3a 5b 43 f8 7f 62 e4 e4 1d 7b 90 b3 e5 b8 0c 84 11 50 67 3b f1 cc 86 0d 55 9f ad 78 fa d0 e0 b3 0f 50 04 f1 f7 6c 63 01 ec e9 ee 35 ad 79 e8	.....:[C..b...{.....Pg;....U. .x.....P...lc....5.y.	success or wait	2	412DCC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\September\logs.dat	unknown	51	success or wait	1	412E3A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\September-IJ9HLQ\	success or wait	1	40B71B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\September-IJ9HLQ	exepath	binary	54 8F 9C 2B 56 69 26 D7 3D 52 AE D5 57 5B D3 8B 83 8B 50 BE 4F 66 29 74 F2 AA 99 64 67 FA C9 33 FA A9 FF DC 03 37 15 83 B8 3F 67 60 C2 9D BD 51 B6 74 AC 14 D3 49 F8 17 4F 90 DB A7 69 90 1B 78 3E 71 D5 89 F1 0E FE CC 63 68 FF 20 37 D4 3F 15 6F 6E 70 45 37 E5	success or wait	1	40B747	RegSetValueExA
HKEY_CURRENT_USER\Software\September-IJ9HLQ	licence	unicode	FF2A5A8790D207B4AD46D43E70C9D5F5	success or wait	1	40B747	RegSetValueExA

Disassembly

Code Analysis