ID: 363869
Sample Name: Mixed Items.exe
Cookbook: default.jbs
Time: 14:26:26
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

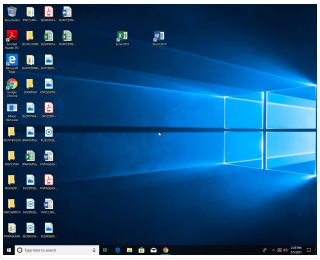
Analysis Report Mixed Items.exe

Overview

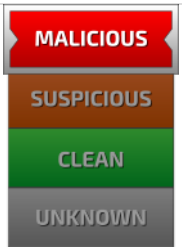
General Information

Sample Name:	Mixed Items.exe
Analysis ID:	363869
MD5:	017e52146c9131..
SHA1:	6dff831a7fd2a42...
SHA256:	26c230cde9fb754..
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection



HawkEye AgentTesla MailPassView Matiex Remcos

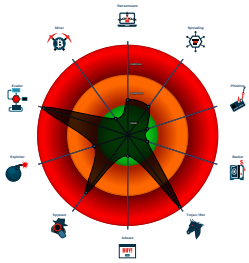
Score: 100

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

Signatures

- Antivirus detection for dropped file
- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through ...
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- System process connects to networ...
- Yara detected AgentTesla
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Yara detected Matiex Keylogger
- Yara detected Remcos RAT
- Adds a directory exclusion to Windo...
- Binary contains a suspicious time st...

Classification



Startup

- **System is w10x64**
- Mixed Items.exe (PID: 6248 cmdline: 'C:\Users\user\Desktop\Mixed Items.exe' MD5: 017E52146C9131DBC9487D834CDFC247)
  - AdvancedRun.exe (PID: 7032 cmdline: 'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7152 cmdline: 'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe' /SpecialRun 4101d8 7032 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2152 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Mixed Items.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6300 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Mixed Items.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4116 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Mixed Items.exe (PID: 7140 cmdline: C:\Users\user\Desktop\Mixed Items.exe MD5: 017E52146C9131DBC9487D834CDFC247)
  - Mixed Items.exe (PID: 6440 cmdline: C:\Users\user\Desktop\Mixed Items.exe MD5: 017E52146C9131DBC9487D834CDFC247)
  - Mixed Items.exe (PID: 1528 cmdline: C:\Users\user\Desktop\Mixed Items.exe MD5: 017E52146C9131DBC9487D834CDFC247)
    - hawkgoods.exe (PID: 1392 cmdline: 'C:\Users\user\AppData\Local\Temp\hawkgoods.exe' 0 MD5: FFDB58533D5D1362E896E96FB6F02A95)
    - Matiexgoods.exe (PID: 6780 cmdline: 'C:\Users\user\AppData\Local\Temp\Matiexgoods.exe' 0 MD5: 80C61B903400B534858D047DD0919F0E)
    - origigoods20.exe (PID: 6064 cmdline: 'C:\Users\user\AppData\Local\Temp\origigoods20.exe' 0 MD5: 61DC57C6575E1F3F2AE14C1B332AD2FB)
    - origigoods40.exe (PID: 5292 cmdline: 'C:\Users\user\AppData\Local\Temp\origigoods40.exe' 0 MD5: AE36F0D16230B9F41FFECBD3C5B1D660)
    - Purchase Order.exe (PID: 5352 cmdline: 'C:\Users\user\AppData\Local\Temp\Purchase Order.exe' 0 MD5: 4983412EC34657BAB4A9BD56617B9960)
- svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6908 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 204 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6460 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6636 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6800 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5720 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7116 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 592 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6488 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5508 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 5536 cmdline: 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' MD5: 017E52146C9131DBC9487D834CDFC247)
- svchost.exe (PID: 5540 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 5708 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5276 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 7024 cmdline: 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' MD5: 017E52146C9131DBC9487D834CDFC247)
- svchost.exe (PID: 5880 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sales1@midombo.comMARYolanmauluogwo@eversmtp.privateemail.com"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Purchase Order.exe	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
C:\Users\user\AppData\Local\Temp\Purchase Order.exe	REMCOS_RAT_variants	unknown	unknown	• 0x5eae4:$str_a1: C:\Windows\System32\cmd.exe • 0x5ea60:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5ea60:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5e088:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5e6e0:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5dc2c:$str_b2: Executing file: • 0x5ec28:$str_b3: GetDirectListeningPort • 0x5e4a0:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5e824:$str_b5: licence_code.txt • 0x5e6c8:$str_b7: \update.vbs • 0x5dc9c:$str_b9: Downloaded file: • 0x5dc68:$str_b10: Downloading file: • 0x5dc50:$str_b12: Failed to upload file: • 0x5ebf0:$str_b13: StartForward • 0x5ec10:$str_b14: StopForward • 0x5e670:$str_b15: fso.DeleteFile " • 0x5e604:$str_b16: On Error Resume Next • 0x5e6a0:$str_b17: fso.DeleteFolder " • 0x5dc40:$str_b18: Uploaded file: • 0x5dcdc:$str_b19: Unable to delete: • 0x5e638:$str_b20: while fso.FileExists("
C:\Users\user\AppData\Local\Temp\origigoods20.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
Click to see the 7 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000003.321855545.000000000436 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000024.00000002.510313698.000000000277 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000024.00000002.510313698.000000000277 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000019.00000003.328468981.00000000043C D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000025.00000002.488787782.000000000098 2000.00000002.00020000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
30.2.hawkgoods.exe.2be8a9c.4.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
30.0.hawkgoods.exe.51fa72.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
30.2.hawkgoods.exe.300a1c4.5.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
30.0.hawkgoods.exe.4c9c0d.1.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
30.2.hawkgoods.exe.51fa72.2.raw.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x1dc55:$key: HawkEyeKeylogger • 0x1fe99:$salt: 099u787978786 • 0x1e296:$string1: HawkEye_Keylogger • 0x1f0e9:$string1: HawkEye_Keylogger • 0x1fdf9:$string1: HawkEye_Keylogger • 0x1e67f:$string2: holdermail.txt • 0x1e69f:$string2: holdermail.txt • 0x1e5c1:$string3: wallet.dat • 0x1e5d9:$string3: wallet.dat • 0x1e5ef:$string3: wallet.dat • 0x1f9bd:$string4: Keylog Records • 0x1fcd5:$string4: Keylog Records • 0x1fef1:$string5: do not script --> • 0x1dc3d:$string6: \pidloc.txt • 0x1dccb:$string7: BSPLIT • 0x1dcdb:$string7: BSPLIT
Click to see the 107 entries				

Sigma Overview

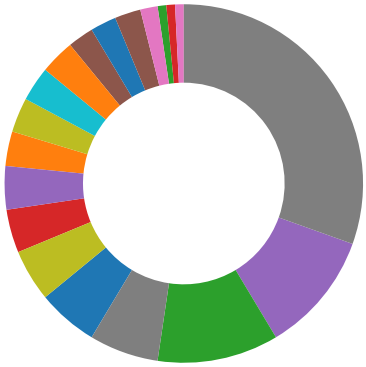
System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Machine Learning detection for dropped file

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

May check the online IP address of the machine

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Binary contains a suspicious time stamp

Yara detected Beds Obfuscator

Persistence and Installation Behavior:

Drops PE files with benign system names

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection:

Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Yara detected Matiex Keylogger
- Yara detected Remcos RAT
- Tries to harvest and steal browser information (history, passwords, etc)
- Yara detected WebBrowserPassView password recovery tool

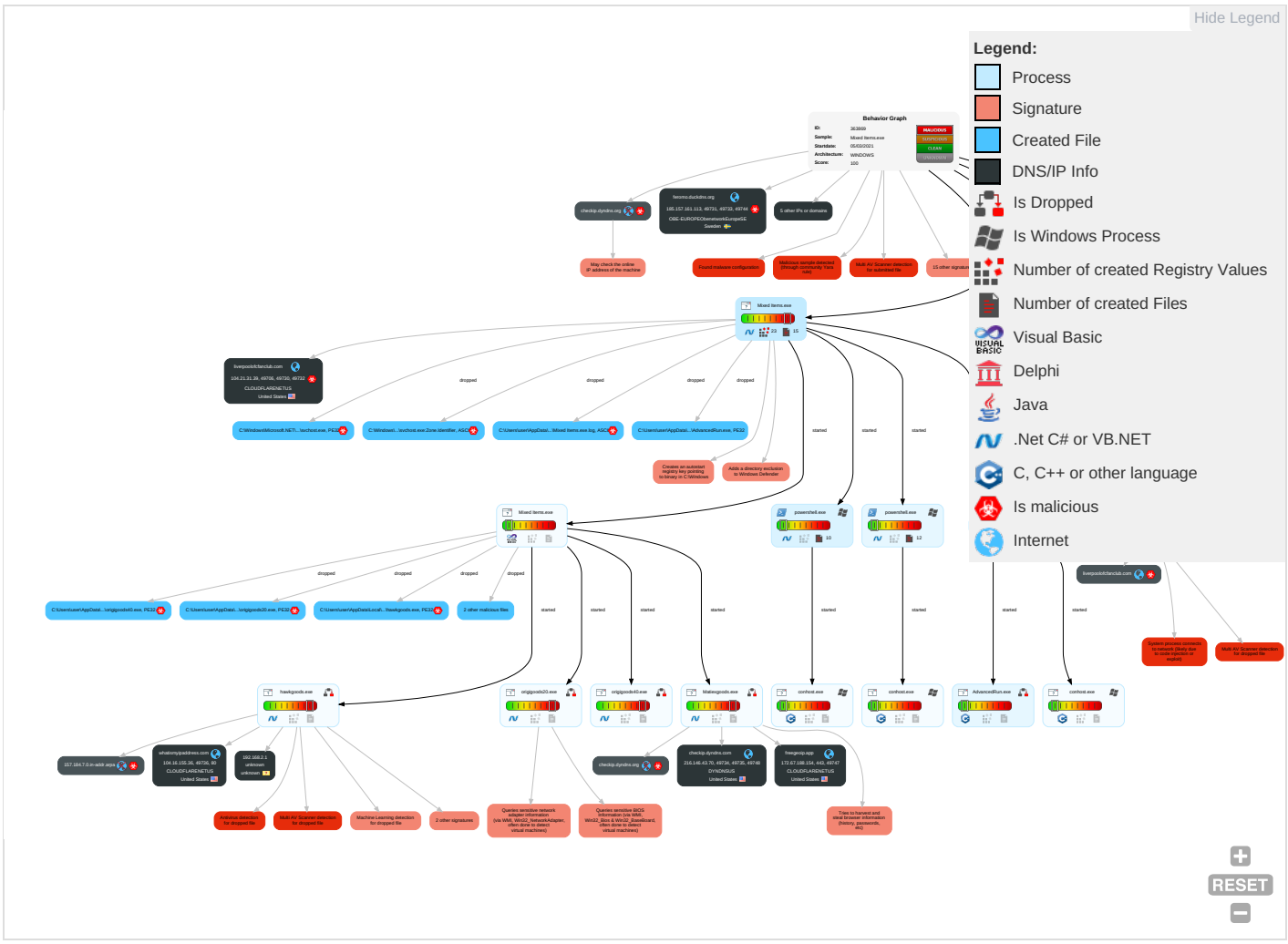
Remote Access Functionality:

- Detected HawkEye Rat
- Yara detected AgentTesla
- Yara detected HawkEye Keylogger
- Yara detected Matiex Keylogger
- Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 3 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 2 1	OS Credential Dumping 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Oth Network Medium
Default Accounts	Native API 1	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3 5	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltrati
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Timestomp 1	LSA Secrets	Security Software Discovery 2 6 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Process Injection 1 1 1	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 7	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1 1	Masquerading 2 2 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 7	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypte Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypt Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

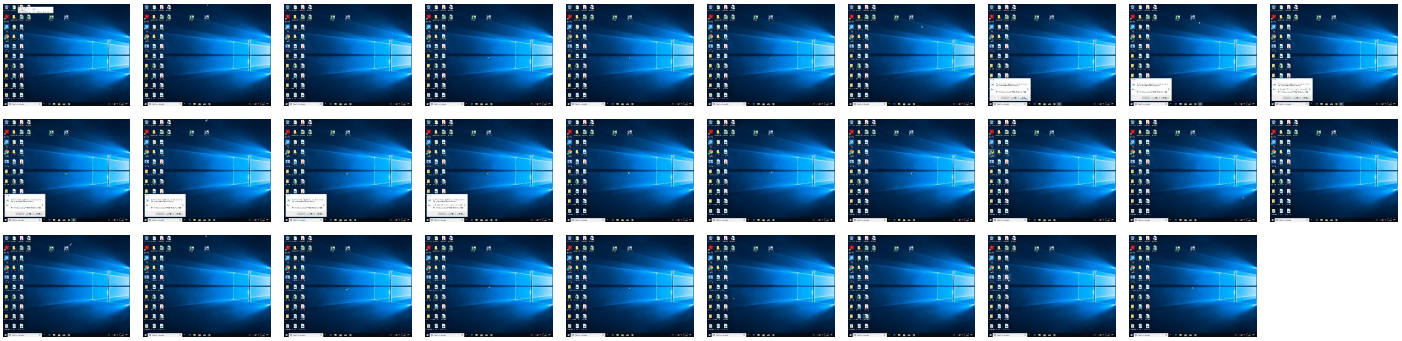
Behavior Graph



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
Mixed Items.exe	17%	ReversingLabs	ByteCode-MSIL.Downloader.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\origigoods20.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	100%	Avira	TR/Redcap.jajcu	
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\origigoods20.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\origigoods40.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Purchase Order.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	54%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	90%	ReversingLabs	ByteCode-MSIL.Trojan.MatiexKeylogger	
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	96%	ReversingLabs	ByteCode-MSIL.Trojan.Golroted	
C:\Users\user\AppData\Local\Temp\origigoods20.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\origigoods20.exe	93%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\origigoods40.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.Mixed Items.exe.4031bf.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
30.2.hawkgoods.exe.4c0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
30.2.hawkgoods.exe.4c0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.origigoods20.exe.e50000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
33.0.origigoods20.exe.e50000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
31.0.Matiexgoods.exe.4d0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
30.0.hawkgoods.exe.4c0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
30.0.hawkgoods.exe.4c0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
36.2.origigoods40.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
31.2.Matiexgoods.exe.4d0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
36.0.origigoods40.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
25.2.Mixed Items.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
25.2.Mixed Items.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
25.2.Mixed Items.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
25.2.Mixed Items.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5120AB9D8EED6517DE7E81CD470A03B1.html	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C391B584FB3EF0C3E1226CABE1FDCB1.html	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C7589177DBC0A00C03B00FCEDE09850.html	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CADB725393BA475AD7E7466656748C83.html	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrardset_CurrentDirectory-liverpo	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FC805D8F9D665A8AE96BD3B687F20834.html	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/	0%	URL Reputation	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-EBDA9D3C78F7FA5DA1492447CFEEA8B3.html	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-1031025574F544F1BD64E20EEEC4AAC7.html	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-ACE03D270F49949C304CBC49EDC5CEFA.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
feromo.duckdns.org	185.157.161.113	true	true		unknown
freegeoip.app	172.67.188.154	true	false		unknown
liverpoolofcfanclub.com	104.21.31.39	true	true		unknown
checkip.dyndns.com	216.146.43.70	true	false		unknown
checkip.dyndns.org	unknown	unknown	true		unknown
157.184.7.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

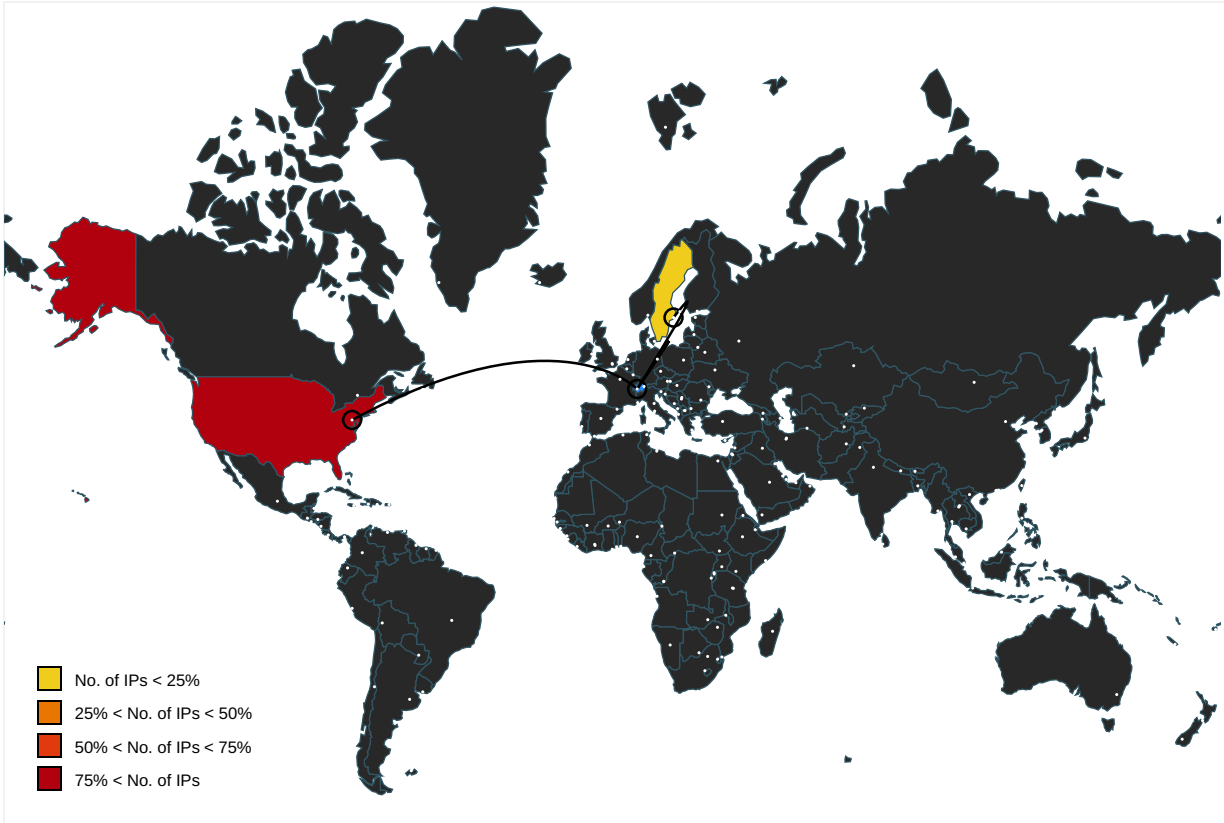
Name	Malicious	Antivirus Detection	Reputation
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5120AB9D8EED6517DE7E81CD470A03B1.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C391B584FB3EF0C3E1226CABE1FDCB1.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C7589177DBC0A00C03B00FCEDE09850.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CADB725393BA475AD7E7466656748C83.html	true	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FC805D8F9D665A8AE96BD3B687F20834.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-EBDA9D3C78F7FA5DA1492447CFEEA8B3.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-1031025574F544F1BD64E20EEEC4AAC7.html	true	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/	false		high
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-ACE03D270F49949C304CBC49EDC5CEFA.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000000A.00000002.550176281.0000000005536000.00000004.00000001.sdmp, powershell.exe, 0000000B.00000002.549247252.0000000005C06000.00000004.00000001.sdmp, powershell.exe, 0000000D.00000002.543804936.00000000054B6000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000B.00000002.528174444.0000000004CEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000000A.00000002.533087278.0000000004617000.00000004.00000001.sdmp, powershell.exe, 0000000B.00000002.528174444.0000000004CEB000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000B.00000002.528174444.0000000004CEB000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000D.00000002.543804936.00000000054B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/Icon	powershell.exe, 0000000D.00000002.543804936.00000000054B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--	Mixed Items.exe	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 0000000B.00000002.528174444.0000000004CEB000.00000004.00000001.sdmp	false		high
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrardset_CurrentDirectory-liverpo	Mixed Items.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000006.00000002.527814462.000001FC10A00000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000000A.00000002.533087278.0000000004617000.00000004.00000001.sdmp, powershell.exe, 0000000B.00000002.528174444.0000000004CEB000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000000D.00000002.543804936.00000000054B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000000A.00000002.550176281.0000000005536000.00000004.00000001.sdmp, powershell.exe, 0000000B.00000002.549247252.0000000005C06000.00000004.00000001.sdmp, powershell.exe, 0000000D.00000002.543804936.00000000054B6000.00000004.00000001.sdmp	false		high
http://https://login.yahoo.com/config/login	hawkgoods.exe	false		high
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 00000009.00000000.266715806.000000000040C000.00000002.00020000.sdmp, hawkgoods.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000A.00000002.524606863.00000000044D1000.00000004.00000001.sdmp, powershell.exe, 0000000B.00000002.517492550.0000000004BA1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
216.146.43.70	checkip.dyndns.com	United States		33517	DYNDNSUS	false
185.157.161.113	feromo.duckdns.org	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
104.21.31.39	liverpoolofcfanclub.com	United States		13335	CLOUDFLARENETUS	true
172.67.188.154	freegeoip.app	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363869
Start date:	05.03.2021
Start time:	14:26:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mixed Items.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:	40
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@52/33@22/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.8% (good quality ratio 93.5%) • Quality average: 82.9% • Quality standard deviation: 26%
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 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.139.180, 13.64.90.137, 104.43.193.48, 23.211.6.115, 8.241.121.126, 8.248.145.254, 8.241.9.126, 67.26.83.254, 8.241.9.254, 104.43.139.144, 52.255.188.83, 168.61.161.212, 184.30.20.56, 20.82.210.154, 92.122.213.194, 92.122.213.247, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report creation exceeded maximum time and may have missing behavior and disassembly information. • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/363869/sample/Mixed Items.exe

Simulations

Behavior and APIs

Time	Type	Description
14:27:17	API Interceptor	2x Sleep call for process: Mixed Items.exe modified
14:27:40	API Interceptor	2x Sleep call for process: svchost.exe modified
14:27:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce tvQKHpPrzFBMmr explorer.exe "C :\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe"
14:28:01	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce tvQKHpPrzFBMmr explorer.exe "C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe"
14:28:18	API Interceptor	492x Sleep call for process: Purchase Order.exe modified
14:28:39	API Interceptor	5x Sleep call for process: hawkgoods.exe modified
14:28:59	API Interceptor	67x Sleep call for process: powershell.exe modified
14:29:01	API Interceptor	145x Sleep call for process: origigoods20.exe modified
14:29:18	API Interceptor	9x Sleep call for process: origigoods40.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	Sample_B.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO_Invoices_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Orders.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	nzGUqSK11D.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
feromo.duckdns.org	Quotations lists.exe	Get hash	malicious	Browse	• 194.5.98.144
liverpoolofcfanclub.com	All House Details.exe	Get hash	malicious	Browse	• 172.67.174.240
whatismyipaddress.com	5ma5PAuFFD.exe	Get hash	malicious	Browse	• 66.171.248.178
	lWXDtYfNDe.exe	Get hash	malicious	Browse	• 66.171.248.178
	XAEJoIo9Uk.exe	Get hash	malicious	Browse	• 66.171.248.178
	BtPchy0J4a.exe	Get hash	malicious	Browse	• 66.171.248.178
	85NX7dSFgP.exe	Get hash	malicious	Browse	• 66.171.248.178
	2BecmYzrWW.exe	Get hash	malicious	Browse	• 66.171.248.178
	YvZ7JqSCFF.exe	Get hash	malicious	Browse	• 66.171.248.178
	7BCSrNZUC6.exe	Get hash	malicious	Browse	• 66.171.248.178
	uVrFVrRFoQ.exe	Get hash	malicious	Browse	• 66.171.248.178
	oWvF1hp3Lt.exe	Get hash	malicious	Browse	• 66.171.248.178
	2eUb95z7N6.exe	Get hash	malicious	Browse	• 66.171.248.178
	bIX28ZhNOJ.exe	Get hash	malicious	Browse	• 66.171.248.178
	pk5Gy3bzBq.exe	Get hash	malicious	Browse	• 66.171.248.178
	KXEQ8IEdd2.exe	Get hash	malicious	Browse	• 66.171.248.178
	TgJhPTMNI6.exe	Get hash	malicious	Browse	• 66.171.248.178

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5Q5HrchOCL.exe	Get hash	malicious	Browse	• 66.171.248.178
	UjKD92fA9g.exe	Get hash	malicious	Browse	• 66.171.248.178
	gfA5aWwv45.exe	Get hash	malicious	Browse	• 66.171.248.178
	V1Rn85tQNR.exe	Get hash	malicious	Browse	• 66.171.248.178
	QnGx32PlXq.exe	Get hash	malicious	Browse	• 66.171.248.178
freegeoip.app	Transfer Form.exe	Get hash	malicious	Browse	• 104.21.19.200
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO_1037_Scanned_150.doc	Get hash	malicious	Browse	• 172.67.188.154
	Consignment Shipment Guide.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 172.67.188.154
	HYUNDAI MOTORS CCPP DC & UPS SYSTEM RFQ DOCUMENT PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	URGENT ORDER AE7664A7CCD_8819A,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 104.21.19.200
	official po.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL_6368638172 documento de recebimento,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 172.67.188.154
	F1419T33_Receptor.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	parcel_document003,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	VGM DECLARATION CERTIFICATE EVERGREEN LINE BOOKING NO. 084100009876 RC# 49173.exe	Get hash	malicious	Browse	• 104.21.19.200
	TNT AWB AND INV..exe	Get hash	malicious	Browse	• 104.21.19.200
	PPG Industries PO.exe	Get hash	malicious	Browse	• 172.67.188.154

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	Transfer Form.exe	Get hash	malicious	Browse	• 216.146.43.71
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 131.186.161.70
	PO_1037_Scanned_150.doc	Get hash	malicious	Browse	• 216.146.43.71
	Consignment Shipment Guide.exe	Get hash	malicious	Browse	• 131.186.161.70
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 162.88.193.70
	purchase order.exe	Get hash	malicious	Browse	• 216.146.43.70
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 131.186.113.70
	HYUNDAI MOTORS CCPP DC & UPS SYSTEM RFQ DOCUMENT PDF.exe	Get hash	malicious	Browse	• 131.186.113.70
	telex transfer.exe	Get hash	malicious	Browse	• 216.146.43.70
	URGENT ORDER AE7664A7CCD_8819A,pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 216.146.43.70
	official po.exe	Get hash	malicious	Browse	• 216.146.43.70
	DHL_6368638172 documento de recebimento,pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 131.186.113.70
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 131.186.113.70
	F1419T33_Receptor.PDF.exe	Get hash	malicious	Browse	• 162.88.193.70
	parcel_document003,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	VGM DECLARATION CERTIFICATE EVERGREEN LINE BOOKING NO. 084100009876 RC# 49173.exe	Get hash	malicious	Browse	• 162.88.193.70
	TNT AWB AND INV..exe	Get hash	malicious	Browse	• 131.186.161.70
	PPG Industries PO.exe	Get hash	malicious	Browse	• 131.186.161.70
CLOUDFLARENETUS	nhiZa1aKSi.exe	Get hash	malicious	Browse	• 104.17.62.50
	s2qBa23HqR.exe	Get hash	malicious	Browse	• 104.17.63.50
	Transfer Form.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO_1022_Scanned_110.doc	Get hash	malicious	Browse	• 172.67.208.139
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 172.67.188.154
	All House Details.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO_1037_Scanned_150.doc	Get hash	malicious	Browse	• 172.67.188.154
	Consignment Shipment Guide.exe	Get hash	malicious	Browse	• 172.67.188.154
	Paid561571.htm	Get hash	malicious	Browse	• 104.16.19.94
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 104.16.16.194
	QO-QC201909Rev1.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	New Order.doc	Get hash	malicious	Browse	• 172.67.219.133

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO_701_36_01_27.doc	Get hash	malicious	Browse	• 172.67.208.139
	tGb2s1rgMG.exe	Get hash	malicious	Browse	• 1.1.1.1
	March 4, 2021, 055038 PM.HTM	Get hash	malicious	Browse	• 104.18.10.207
	44260.8523962963.dll	Get hash	malicious	Browse	• 104.20.184.68
	xfe.dll	Get hash	malicious	Browse	• 104.20.185.68
	pago de documento de pedido.exe	Get hash	malicious	Browse	• 162.159.133.233
	N0ir32BDve.dll	Get hash	malicious	Browse	• 104.20.184.68
	flashInstaller.dmg	Get hash	malicious	Browse	• 104.21.21.95
OBE-EUROPEObenetworkEuropeSE	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• 185.157.160.229
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• 185.157.160.229
	CN-Invoice-XXXXX9808-190111432879948.exe	Get hash	malicious	Browse	• 185.157.161.20
	Payment_MT_103_#776363_Swift_Confirmation.exe	Get hash	malicious	Browse	• 217.64.149.164
	rWqmXnEB3b.exe	Get hash	malicious	Browse	• 185.157.161.223
	ALEKO GROUP RUSSIA - PURCHASE ORDER# 610 1965.EXE	Get hash	malicious	Browse	• 185.86.106.202
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• 185.157.160.229
	FH87565635456-02-03-21.exe	Get hash	malicious	Browse	• 185.86.106.202
	Y5sjv4lnha.exe	Get hash	malicious	Browse	• 185.86.106.202
	Supply Quotes 09172020.exe	Get hash	malicious	Browse	• 185.86.106.202
	Purchase Order# 6101965.exe	Get hash	malicious	Browse	• 185.86.106.202
	SHIPMENT_ARRIVAL_NOTICE#423-XXX.exe	Get hash	malicious	Browse	• 217.64.149.164
	6jRN6Bl7U4.exe	Get hash	malicious	Browse	• 185.157.161.223
	New Order YCO HOLDINGS.exe	Get hash	malicious	Browse	• 185.86.106.202
	f7KGZ5fN6P.exe	Get hash	malicious	Browse	• 185.157.161.223
	MeBDsszqpW.exe	Get hash	malicious	Browse	• 185.157.161.104
	jsEeh4kpdD.exe	Get hash	malicious	Browse	• 185.157.161.223
	o1N0Ej5dP0.exe	Get hash	malicious	Browse	• 45.148.16.42
	Orden de compra# 675423,pdf.exe	Get hash	malicious	Browse	• 185.86.106.202
	Precio de referencia - CARMAHE,pdf.exe	Get hash	malicious	Browse	• 185.86.106.202

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Transfer Form.exe	Get hash	malicious	Browse	• 172.67.188.154
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 172.67.188.154
	All House Details.exe	Get hash	malicious	Browse	• 172.67.188.154
	Consignment Shipment Guide.exe	Get hash	malicious	Browse	• 172.67.188.154
	LogiCameraSettings_2.12.8.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 172.67.188.154
	HYUNDAI MOTORS CCPP DC & UPS SYSTEM RFQ DOCUMENT PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	statement-ID306051313.vbs	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	URGENT ORDER AE7664A7CCD_8819A,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 172.67.188.154
	official po.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL_6368638172 documento de recebimento,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order No-1021332021.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ No-2340099.exe	Get hash	malicious	Browse	• 172.67.188.154
	F1419T33_Receptor.PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	parcel_document003,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	iqKNGLP6PS.exe	Get hash	malicious	Browse	• 172.67.188.154

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	CN-Invoice-XXXXX9808-190111432879948.exe	Get hash	malicious	Browse	
	Zahlungskopie.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	Reversing Purchase Orders.exe	Get hash	malicious	Browse	
	NEW ORDERS 122020 2 x 40 HQ.exe	Get hash	malicious	Browse	
	ORDER01032021rfggfscan.exe	Get hash	malicious	Browse	
	FedEx's AWB#5305323204643.exe	Get hash	malicious	Browse	
	believehot23 cccc.exe	Get hash	malicious	Browse	
	order confirmation 6026022001.exe	Get hash	malicious	Browse	
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	RFQ - REF 208056-pdf.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	
	PRODUCT SPECIFICATION.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	
	em6eElVbOm.exe	Get hash	malicious	Browse	
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	
	Fireman.exe	Get hash	malicious	Browse	
	NEW ORDER.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5967038728698416
Encrypted:	false
SSDEEP:	6:balEk1GaD0JOCEfMuaaD0JOCEfMKQmD1JtAl/gz2cE0fMbhEZolrRSQ2hyYIIT:baNGaD0JcaaD0JwQQ1JtAg/0bjSQJ
MD5:	8FBEB3EE575D3BBA44369DDECCA49083
SHA1:	8091ECF8CBF1A04AAEE7BF5C231C7605D8F8DAC0
SHA-256:	95D82888783EA084631ADCFBB236A44236D02A8088F04376AD017E9872EBC967
SHA-512:	A51ACB1EF5483FE64293992818201966FA063D3DD36DC67E74EF27EA5443B7E93A1A51485D0C67233BBF0A322949B9FEFD244C8AA60DCA5B48248A330D4F174
Malicious:	false
Preview:	....E..h..(.....(....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....(....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xe423063f, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09585293764386119
Encrypted:	false
SSDEEP:	12:d40+jRsXO4blof+8KH40+jRsXO4blof+8K:dH2fuH2f
MD5:	7369A0D21D0345333864DF57AC91E792
SHA1:	4735E40732F7147A9FC47F59338F29FD2812F0B3
SHA-256:	217612B92D702BCF7D388AAAFE46F93481793216F8A9428A02CBDBE4540C4DC5
SHA-512:	B2A5411F24F414778F003DC15665E1B9853B623E6E79CC23E7239662DC4FCD0671D951A510FEBE646C7FA5F745BADFDCB4E14B8936582351A5FEF7D2FD69EE2
Malicious:	false
Preview:	.#.?... .....e.f.3...w.....&.....w..(....y{.h.(.....3...w.....B.....@..... ....3...w..... .....(....y{o.....-~>(....y{..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11057603056041983
Encrypted:	false
SSDEEP:	3:h5G1EvNwr+q8l/bJdAtiVFMgerltAll:PXHq8t4E+A
MD5:	476D0CB871276EDB31AF5710A70C8768
SHA1:	EFD8C0036892FC78E9C9E6B2852CCE084C415544
SHA-256:	56A70A0A16A503D1624A38ACF08AF8A7654E9999A3611A3173A48B61BD280324
SHA-512:	5696AF6ACFFBAA8E029DFD0CAAB3DE1475C6405DD6ACB9538EABBDB472EF82B65E4CE8ADB4D5EBE75604000E45BE415E955BA43E450F48C67F228610F23FF5A6
Malicious:	false
Preview:	.u.....3...w..(....y{.....w.....w.....w....:O.....w.....-~>(....y{..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._.iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1108462043257137
Encrypted:	false
SSDEEP:	6:kK7H/kwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:AwTJ6HkPlE99SNxAhUe0ht
MD5:	2355411028ACE02098EA05A848FF008B
SHA1:	2EDE017C6C12FD81FFFF0D987603C38FF0BF634D
SHA-256:	E162456000378AE119A841A1136ECBE5ECD6E5960AA1D9322DEAD68CD7EE199D4
SHA-512:	3DCD4EFC903F2C57FBA66895F7A05C4A7ADA1E9239644EBC7478C9C5EF9BBC570A2B43EB0D65683E18AE22E184B5B5E7D392FAD57EA53939A3940309FF3194A2
Malicious:	false
Preview:	p..... .....6.-.....(..... ....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Mixed Items.exe.log	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4KnKDE4KhK3VZ9pKhPKlE4oKFKHKoZAE4Kzr7r1qE4KE4j:MxHKXfvjHKnYHKhQnoPtHoxHhAHKzvrx
MD5:	4DC448082AFF363E7DB48FE0F4564674
SHA1:	BA956788D8EABC88D02119AC4B36EB16D26A2CA5
SHA-256:	0B882DACEECB3378A361B929BFF23F06DDAF5BEEF047B4BA87E8494C86899870

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Mixed Items.exe.log	
SHA-512:	0C3CC129DEAE19CC08E921E9A4C725D924539AAC2235D3FFFF6B270348E87A41318A1240C8D03422F62DB4728181BCBAC5CC7B216EE5DC34BA446F2A7233F1E
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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.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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	698
Entropy (8bit):	5.049094101509586
Encrypted:	false
SSDEEP:	12:reVGyMYx2Y5BYtmWNUc5AtYX5E4a2KryMYGH+ptsxptsOtw9O9S8:reUyMGF5ytmLcetYX5E2KryMb+zsxzsk
MD5:	B0CEEA53B3467F59FD8E87F80213BDE9
SHA1:	D9E6D1CBB480E7248658DF935648DFA733745602
SHA-256:	D9C93CB64E6F1F5BDC94581CEEA99F759EE1E35716EAF623C61962EA0152F9DD
SHA-512:	DDAA6C9FA3535B4926C60B692F8E202D10EB160D1F8BE7A9DE79239EF75AFD470403DF1D8F0CBF29A5F819E907D02E8E656BB9A52E71E30D9259987EAE881655
Malicious:	false
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation.....Invoke-OperationValidation.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11005962332311817
Encrypted:	false
SSDEEP:	12:26M7vBEzXm/Ey6q9995A+Sq3qQ10nMCldimE8eawHjc85Ev:262vLl68BLyMCldzE9BHjct
MD5:	08E0E756C0E25CF2F85281AF60D4D8D6
SHA1:	D6F1BB1FF8A041151322580BA5D2A4ACE28C9A1F
SHA-256:	767B4A3EF2DE563C663F2A0ACBA6F3D25070D9FC2CE9D8415261A523B5CFC77B
SHA-512:	2CA215A620C049089FB08761594B5E5F3AF363D455F6E1535AFDF0D00A8E0C599A0C15053628A9052E5574267DF3EA8431BCBB7D7F1FC7BF4693AF6DCA8F5464
Malicious:	false
Preview:	.....<...E.J.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....0.:-..... .....t'.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....<.....J.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11261316214328353
Encrypted:	false
SSDEEP:	12:VwEzXm/Ey6q9995A+H1miM3qQ10nMCldimE8eawHza1miIeEf:Ul68N1tMLyMCldzE9BHza1tIJ
MD5:	607110AB5B12714EDF520B297790FF69
SHA1:	1697CF656BF8DC0F7E6EFAC73306943C97FA289E
SHA-256:	4E1270D6142DCCD70ADBAA4C7D09367BE485011F43CC93F8CDB6B78A42093660
SHA-512:	800087C2DE73C41B0B944863D7148A6F87B96C4BBFDD2797DD28466E02675ECDF6ACAD350A2B470EC2A31B3E20DDAE8C953393DA92EE08DABD4999060C60FE12
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Preview:	.....<....8D.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....0.:-..... .....(.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....<...D@D..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11257437134850665
Encrypted:	false
SSDEEP:	12:b2zXm/Ey6q9995A+Hg1mK2P3qQ10nMCldimE8eawHza1mKmAf:bjl68pg1iPLyMCldzE9BHza1R
MD5:	7FF245D22E936F26367E04D77759AB57
SHA1:	3044D4690AF81CC82163B6D3404E170333909B07
SHA-256:	38292B59D919010242643EC6C778F7AC1D78C8265F4FE9056F5C45F2A43A9D2E
SHA-512:	FD0F8A8E6ED5E96300F0BC364ECDE6E825FE74226D41EE47CF3D917D48A49F5E364E302106031E6E9ED11E0A6610A818F46F07DE2D7812E55364D1EAB66AF1EB
Malicious:	false
Preview:	.....<....xA.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....0.:-..... .....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....<....A..... ....

C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: CN-Invoice-XXXXX9808-190111432879948.exe, Detection: malicious, Browse • Filename: Zahlungskopie.exe, Detection: malicious, Browse • Filename: Purchase Order.exe, Detection: malicious, Browse • Filename: Reversing Purchase Orders.exe, Detection: malicious, Browse • Filename: NEW ORDERS 122020 2 x 40 HQ.exe, Detection: malicious, Browse • Filename: ORDER01032021rfggfscan.exe, Detection: malicious, Browse • Filename: FedEx's AWB#5305323204643.exe, Detection: malicious, Browse • Filename: believehot23 cccc.exe, Detection: malicious, Browse • Filename: order confirmation 6026022001.exe, Detection: malicious, Browse • Filename: PROFORMA INVOICE.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287989.exe, Detection: malicious, Browse • Filename: RFQ - REF 208056-pdf.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287994.exe, Detection: malicious, Browse • Filename: PRODUCT SPECIFICATION.exe, Detection: malicious, Browse • Filename: DHL_document1102202068090891.exe, Detection: malicious, Browse • Filename: em6eElVbOm.exe, Detection: malicious, Browse • Filename: Purchase Order_Pdf.exe, Detection: malicious, Browse • Filename: Fireman.exe, Detection: malicious, Browse • Filename: NEW ORDER.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287993.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....).+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	455680
Entropy (8bit):	5.4156534240521
Encrypted:	false
SSDEEP:	6144:L09yLLuWoujzz/DCBGNv5lToO7OsWXiOV:L09yLyWoujHDX5QO7OvXik
MD5:	80C61B903400B534858D047DD0919F0E
SHA1:	D0AB5400B74392308140642C75F0897E16A88D60
SHA-256:	25ADE9899C000A27570B527CFFC938EC9626978219EC8A086082B113CBE4F492
SHA-512:	B3216F0E4E95C7F50BCCBA5FDCCA2AD622A42379383BE855546FA1E0BAC41A6BEEA8226F8634AD5E0D8596169E0443494018BBE70B7052F094402AECAA038BCE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 54%, Browse • Antivirus: ReversingLabs, Detection: 90%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....~.... ... ....@.. .....`..... ..@.....$...W.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....`.....H.....x.....x'...h..... .....RNK\ZJO@F.EYC.G.IOYKJ._R_CEESEPPlj}ez|"hzfSn`ssdh~DNwq//M\`tdv`|..;.....4.....Ewqus._/.....V>..%9%(:&##b?`LLJN.56(,*:.}.2=4lwY_..... .....A.{YOLI..qAL.tTDY^..v^NY

C:\Users\user\AppData\Local\Temp\Purchase Order.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	466432
Entropy (8bit):	6.58109326592699
Encrypted:	false
SSDEEP:	12288:Lp85GzC+LZ5DsOwPEsfI2Mt23o/ZMBoYC:W+LZxsJI2M03eZN
MD5:	4983412EC34657BAB4A9BD56617B9960
SHA1:	2A5F9B3FA44597CF439B10B6337A4D1D98197A71
SHA-256:	76C2025CB8251393360BAAC07498C75BAB91A4DB229667F3E6ED2EC89CBEA6D6
SHA-512:	7A786CFC1299CCA28CF3A1A96E3280531F606284392327359A8EED0ABFC47C0C3FFD9BC77C0F7828975047A65DFCD7FDFEEEC50F3BF1C87AFA24C35B2D8861B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\Purchase Order.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\Purchase Order.exe, Author: unknown
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....oj.-+..~+..~+..~..{~9..~..y~...~..x~5..~x(.~)..~f(.~*..~..M~*..~.U..1..~ .U.....~.U.....~"s.~8..~+..~2..~.U..v..~.Uu~*..~.U..*..~Rich+..~.....PE..L.....>`..... ....@.....@.....v.. .....8K.....@...8.. \..8.....\.....X\..@..... ..d.....text..... ..`.rdata...n... ...p.....@..@.data...<=..... ..@....tls.....@....gfids..0.....@..@.rsrc...8K.....L.....@..@.reloc...8...@...:.....@..B..... .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2jnw4mcb.ygh.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4s1cg2kf.1xe.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
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4zux455h.wha.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
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_f3qm3trx.u2l.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mh5wpd4r.xxq.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
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zyhy1zxg.gf4.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
Preview:	1

C:\Users\user\AppData\Local\Temp\hawkgoods.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	532992
Entropy (8bit):	6.507156751280516
Encrypted:	false
SSDEEP:	6144:DufqM5JXbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9E:uJXQtqB5urTIoYWBQk1E+VF9mOx9Ei
MD5:	FFDB58533D5D1362E896E96FB6F02A95
SHA1:	D6E4A3CA253BFC372A9A3180B5887C716ED285C6
SHA-256:	B3D02FD5C69293DB419AC03CDF6396BD5E7765682FB3B2390454D9A52BA2CA88
SHA-512:	3AE6E49D3D728531201453A0BC27436B1A4305C8EF938B2CBB5E34EE45BB9A9A88CF2A41B08E4914FDA9A96BBAA48BD999A2D2F1DFFCD39761BB1F3620CA725F
Malicious:	**true**
Yara Hits:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4..... .....@.. ..... ..@.....O.... ...2.....`..... ....H.....text..... ....`.rsrc....2... ...2.....@..@.reloc.....` ....@..B.....H.....0}..\.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....,.~.....~.....o....o.....1.~....~....o.....o....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Local\Temp\origigoods20.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\origigoods20.exe	
Category:	dropped
Size (bytes):	220672
Entropy (8bit):	6.057903449485828
Encrypted:	false
SSDEEP:	3072:SVQEat7UY8MnZGcqB5AyruUJ7XAzsNvEaEifv6yr9zRsc0qC4B0BUAE3vVAVvoUB:SytJqCUyQNX36yQqbB063cAUAW
MD5:	61DC57C6575E1F3F2AE14C1B332AD2FB
SHA1:	F52F34623048E5FD720E97A72EEDFD32358CD3A9
SHA-256:	1C7757EE223F2480FBC478AE2ECAF82E1D3C17F2E4D47581D3972416166C54AB
SHA-512:	81A7DB927F53660D3A04A161D5C18AAB17D676BCC7AE0738AB786D9BEE82B91016E54E6F70428AEC4087961744BE89B1511F9E07D8DABBE5C2A9D836722395A1
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods20.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 93%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....V.....t... .....@.. ..... ..@.....t..O..... ..... ..H.....text....T... ...V..... ..`.rsrc.....X.....@..@.reloc..... .....\.....@..B.....t.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0..,..... ..+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+.....,..... .....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\origigoods40.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221696
Entropy (8bit):	6.060343577776758
Encrypted:	false
SSDEEP:	3072:K9Wf3ouEAkhUxOCt+qqr3drw0tR5dUimnoSA7Mw4lY2hWYQQgGJrozRscS4+SOw6:KhuI3dlxUOt7IdWLOjCDUjU
MD5:	AE36F0D16230B9F41FFECBD3C5B1D660
SHA1:	88AFC2923D1EEFB70BAD3C0CD9304949954377EF
SHA-256:	CFAD1E486666FF3FB042BA0E9967634DE1065F1BBD505C61B3295E55705A2A50
SHA-512:	1E98AEE7DC693822113DCDE1446A5BED1C564B76EEF39F39F3A5D98D7D2099CF69AC92717A3297AFC7082203929F1E9437F21CB6BC690974A0EF6D6CF6E4393
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods40.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....X.....>v... .....@.. ..... .@.....u..S.....P..... ..... ..H.....text...DV... ...X..... ..`.rsrc...P.....Z.....@..@.relo c.....`.....@..B..... v.....H.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0. .,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8040704
Entropy (8bit):	3.1191276452386894
Encrypted:	false
SSDEEP:	12288:XPtD9fJHnfa0MFig4loNDgfzdUqXYJcenH8CqfykSW7CE9ZCW/V2P/MmEizNCmBi:IvbCRBKLMQtmumls0Mam
MD5:	C4193405C45F878C5E02FA4B263142B8
SHA1:	AA5E3BD8F59352C154860A9B79C3FD11FB01D10B
SHA-256:	281FB62B35A26DB9FF27EF2E651B4E854529EAD0B5853701F96C031AFE69E290
SHA-512:	95BAECF64742AABCF65B161167AB6FA7F09EFB8468A1F4691A4345D333E62D41246541AB156C15E3B5C715568AAECD474E0D478BCD6AB01E30F02096163D694
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="HhWacKtFzfukChDVbubfTrZrVbAtaVyzZbNqyntLmrIPObE.CSjJWBiTlySaukEqHedjDjyioksOeIaFe" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <HhWacKtFzfukChDVbubfTrZrVbAtaVyzZbNqyntLmrIPObE.CSjJWBiTlySaukEqHedjDjyioksOeIaFe>.. <setting name="RFMEHwInzsKqSMaWl" serializeAs="String">.. <value>77V90V144V0V3V0V0V0V4V0V0V0V255V255V0V0V184V0V0V0V0V0V0V64V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V0V128V0V0V0V14V31V186V14V0V180V9V205V33V184V1V76V205V33V84V104V105V1

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:Pm:e
MD5:	C0826819636026DD1F3674774F06C51D
SHA1:	1E768A21723E530122240FA219BFF8C3365F40B2
SHA-256:	01B23136EA7F9F8B9E72C9E125FD710301BAEC28662B0DE2168967838C79E81A
SHA-512:	8AF15968CE7287442204A26F411FF8C3AA6F43167D39A2719DF5C4540B3174D41A6C8063DB82EB49433805CD52F5BC1388BBD032C2C35260E05868C1BBA68E27
Malicious:	false
Preview:	1392

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	47
Entropy (8bit):	4.376204213693507
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAI4F:oNWXp+N23f8
MD5:	EE8C153C2C2A0850DEE1BE69D03BB011
SHA1:	2F2FBC7ABB2EEE1DF6198FF180860516D983905A
SHA-256:	15B7AAE18CB550E8A7B4210496289D53D84CF86ECDC4C175BBFEB789B08FC488
SHA-512:	CF9F63528B0D50FA85EF6E2A0364178DF20A60557038A76E32C348196B969566D5071BD272534EAC2DCA5197947FFB5A4DCD723FC8135FDB81372E657DF7A2D8
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe

C:\Users\user\Documents\20210305\PowerShell_transcript.506013.0nP0+V72.20210305142754.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):	846
Entropy (8bit):	5.310409359628285
Encrypted:	false
SSDEEP:	24:BxSA0xvBnbx2DOXUWeSuqpWeHjeTKKjX4CIym1ZJXuuqh:BZIvhboO+Sp4eqDYB1ZUph
MD5:	F69879D2324FA8DDEF956B398557F5E4
SHA1:	CF90260BB7E81F4B58E1EB0CDF7E4F7F2B315668
SHA-256:	7C8D023C9F24F0AE23102B889B376FE9EE573A51E35EDE3592D61D0A32801C96
SHA-512:	70DB8EC1AECA708B301E0C83E75BAFE8D2BA2DE6EEE26740041480763E9358EE754DD4CEE3D1DCC6EA6CBA75C35FD5C673833377C802F16EC0160B2DFC7A8037
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210305142826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Mixed Items.exe -Force..Process ID: 2152..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: 20210305142826..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Mixed Items.exe -Force..

C:\Users\user\Documents\20210305\PowerShell_transcript.506013.RPfp4n8i.20210305142756.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):	916
Entropy (8bit):	5.4360707335352405
Encrypted:	false
SSDEEP:	24:BxSAAxvBnbx2DOXUWeSuAjWoHjeTKKjX4CIym1ZJXCuAL:BZEvhboO+SVqoqDYB1ZcVL
MD5:	55B592D61FB7A30573C912A818C91951
SHA1:	9E62843D1F6A90DD6C9D5B7156F2E236AA6FC832
SHA-256:	2ADC8A9B9CCF3E327E228C7C2105F44FA93C0C25122BCCA07B26DE634E53DC1C
SHA-512:	B41D518369BCB24E2553B2728CF8B7BA56FE454F3913C6039C4632CDF9F06ABCA4F079F6F8EA7E5B7EAEC484EDD26D25F1AF4D46A5701D1F1B9D11C38A15CE36
Malicious:	false

C:\Users\user\Documents\20210305\PowerShell_transcript.506013.RPfp4n8i.20210305142756.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210305142831..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe -Force..Process ID: 4116..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..PSRemoting ProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210305142831..**********..PS>Add-Mp Preference -ExclusionPath C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe -Force..

C:\Users\user\Documents\20210305\PowerShell_transcript.506013.YRcDMrIT.20210305142756.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):	846
Entropy (8bit):	5.3022844597421495
Encrypted:	false
SSDEEP:	24:BxSAAxvBnbx2DOXUWeSuqpW5HjeTKKjX4CIym1ZJXCuqh:BZEvhboO+Sp45qDYB1Zcph
MD5:	BD2110BFCB03716BF8B4DD1A9B4FA1EC
SHA1:	C8752AAC9BE7358714B07FAE68972054E6B0C9C4
SHA-256:	714D9629E7B36AA452AE2B4DB202431320629E0BB1702116DB739D219BA91155
SHA-512:	1F50DA1C70F1465FD1A5BA4BE7663C55FD5B7D10C18CBB7F1721D72C93B2C5CDD5897B76067EE1867D580E3FF186DC72D087D1E3CD24F1C0BFFE9D1457353A8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210305142831..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Mixed Items.exe -Force..Process ID: 6300..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: 20210305142831..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Mixed Items.exe -Force..

C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	86808
Entropy (8bit):	5.248273656007456
Encrypted:	false
SSDEEP:	768:FjWGjHoODdPfUwUmsA4de1IeT0EtRwwwqe+Sk5XTsLhD:bjN5UwDsteT0wsJ
MD5:	017E52146C9131DBC9487D834CDFC247
SHA1:	6DFF831A7FD2A42EC3ABE4C1BA51F3A9C9C6A25B
SHA-256:	26C230CDE9FB7544F7E3762F1ABAC39F6C8F0D2DB0689178B223E0E68D2A6A0A
SHA-512:	0BB939ADF020A01DB26B057ADEAD21EC5A6A6FA3A081B6466BA6FC5B661D1EBEA507E17A14588FDDFEB85536674382A8CD77057F569E0EB9278C9C403D9717D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r.y.....".0..2.....Q... ..`....@.. .....W... ..@.....dQ..W....`.....>..... ....H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.reloc.....<.....@..B.....Q.....H.....<+..(&.....*F.(.....(.....*".(.....*>..r}..p.o4....*".(5....*Vs....(6...t.....*F.(.....(.....*.rL.pzrL..pzrL..pzrL..pzrL..pzrL..pzrL..pz*.rL..pzrL..pzrL..pzrL..pzrL..pz*.rL..pzrL..pzrL..pzrL..pzrL..pzrL..pzrL..pz*.rL..pzrL..pzrL..pzrL..pzrL..pzrL..pz*.rL..pzrL..pzrL..pzrL..pzrL..pzrL..pzrL..pz*~rL..pzrL..pzrL..pzrL..pzrL..pz*.0.....rL..pzrL..pzrL..pzrL

C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Mixed Items.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.248273656007456
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Mixed Items.exe
File size:	86808
MD5:	017e52146c9131dbc9487d834cdfc247
SHA1:	6dff831a7fd2a42ec3abe4c1ba51f3a9c9c6a25b
SHA256:	26c230cde9fb7544f7e3762f1abac39f6c8f0d2db0689178 b223e0e68d2a6a0a
SHA512:	0bb939adf020a01db26b057adead21ec5a6a6fa3a081b64 66ba6fc5b661d1ebea507e17a14588fddfeb85536674382 a8cd77057f569e0eb9278c9c403d97177d
SSDEEP:	768:FjWGjHoODdPfUwUmsA4de1IeT0EtRwwwqe+Sk5 XTsLhD:bjN5UwDsteT0wsJ
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L...r .y....."...0..2.....Q... ...`....@.. ..... W.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4151be
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEA799C72 [Sat Aug 28 12:54:10 2094 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=CxIXTKwSoMCLxPuWHhugs, S=lgYPTXZnvpiTkGdjupDgPoRlmhzkTzHbzenLEGqYPHbubwMQ, L=CwjVPVwJkqWwFGdmwR, T=RyzWKLBwDeWQzCUxqptR, E=zXPiPGIuTRAxwAsULVOVRHusYTQNXjGkAaVL, OU=iIVbAskroXcHwzniFtPapLluJGHoDsfundBtrSwFtel, O=muVoRorsGTceSKbnTWYDwAiBFlHcPnOIRP, CN=gvZGrBSrlMevBvcRpsHBJVQfMpkpvyqNEL
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 3/4/2021 4:46:19 PM 3/4/2022 4:46:19 PM
Subject Chain	• C=CxIXTKwSoMCLxPuWHhugs, S=lgYPTXZnvpiTkGdjupDgPoRlmhzkTzHbzenLEGqYPHbubwMQ, L=CwjVPVwJkqWwFGdmwR, T=RyzWKLBwDeWQzCUxqptR, E=zXPiPGIuTRAxwAsULVOVRHusYTQNXjGkAaVL, OU=iIVbAskroXcHwzniFtPapLluJGHoDsfundBtrSwFtel, O=muVoRorsGTceSKbnTWYDwAiBFlHcPnOIRP, CN=gvZGrBSrlMevBvcRpsHBJVQfMpkpvyqNEL
Version:	3
Thumbprint MD5:	9D1E87B33DFAD65CD7994E81536FE81B
Thumbprint SHA-1:	9121B22BFA1E034D66ECBBEF0A16A7F99FF1ED71
Thumbprint SHA-256:	B6ED10F00D23B1B6587357AD36112AE283853F098AB3557F1B7B358F01F105DB
Serial:	00FD586FE6F8FB5F9B46153E047AAE8BBA

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15164	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x13e00	0x1518	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	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	0x131c4	0x13200	False	0.223754084967	data	5.04447660027	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x610	0x800	False	0.32373046875	data	3.4701340184	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x18000	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	0x160a0	0x380	data		
RT_MANIFEST	0x16420	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 2021
Assembly Version	3.3.0.0
InternalName	MotherFuckerBitch.exe
FileVersion	3.3.0.0
CompanyName	WindowsAPI
LegalTrademarks	WindowsAPI
Comments	WindowsAPI
ProductName	WindowsAPI
ProductVersion	3.3.0.0
FileDescription	WindowsAPI
OriginalFilename	MotherFuckerBitch.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 14:27:18.536206007 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.574662924 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.574821949 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.575324059 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.617522001 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803261995 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803302050 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803325891 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803349018 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803371906 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803396940 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803422928 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803433895 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.803445101 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803467989 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803478956 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.803492069 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.803517103 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.803540945 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.804130077 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.804158926 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.804255009 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.805051088 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.805083990 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.805146933 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.806015968 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.806047916 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.806134939 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.806965113 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.807015896 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.807074070 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.807913065 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.807960033 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.808053017 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.809593916 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.809859991 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.809886932 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.809911013 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.809927940 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.809957981 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.810745001 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.810776949 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.810858965 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.811680079 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.811714888 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.811772108 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.812654018 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.812684059 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.812750101 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.843022108 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843055010 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843077898 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843100071 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843125105 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843188047 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.843262911 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.843465090 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843492985 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.843530893 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.844446898 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.844480038 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.844537973 CET	49706	80	192.168.2.3	104.21.31.39

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 14:27:18.845783949 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.845813036 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.845864058 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.849112034 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849145889 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849169016 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849191904 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849215031 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849236012 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849256039 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.849315882 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.849333048 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849354982 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.849379063 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.850135088 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.850168943 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.850217104 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.851083994 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.851118088 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.851159096 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.852065086 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.852140903 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.884360075 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.884390116 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.884510994 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.884758949 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.884787083 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.884887934 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.885612965 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.885643959 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.885736942 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.886550903 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.886584044 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.886677027 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.887463093 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.887495995 CET	80	49706	104.21.31.39	192.168.2.3
Mar 5, 2021 14:27:18.887579918 CET	49706	80	192.168.2.3	104.21.31.39
Mar 5, 2021 14:27:18.888396978 CET	80	49706	104.21.31.39	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 14:27:18.472028017 CET	192.168.2.3	8.8.8.8	0x4360	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:17.554444075 CET	192.168.2.3	8.8.8.8	0x7c2d	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:19.739914894 CET	192.168.2.3	8.8.8.8	0x553d	Standard query (0)	feromo.duc kdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:27.827776909 CET	192.168.2.3	8.8.8.8	0x1bec	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:30.171793938 CET	192.168.2.3	8.8.8.8	0xe960	Standard query (0)	feromo.duc kdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.940161943 CET	192.168.2.3	8.8.8.8	0x5c40	Standard query (0)	checkip.dy ndns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:33.072390079 CET	192.168.2.3	8.8.8.8	0x5fbc	Standard query (0)	checkip.dy ndns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:34.189199924 CET	192.168.2.3	8.8.8.8	0x21d1	Standard query (0)	157.184.7.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 5, 2021 14:28:35.951399088 CET	192.168.2.3	8.8.8.8	0xe482	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:44.782563925 CET	192.168.2.3	8.8.8.8	0x9514	Standard query (0)	feromo.duc kdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:53.300302029 CET	192.168.2.3	8.8.8.8	0xf5e8	Standard query (0)	feromo.duc kdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:53.457202911 CET	192.168.2.3	8.8.8.8	0xcb48	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:03.668133020 CET	192.168.2.3	8.8.8.8	0xd6f	Standard query (0)	feromo.duc kdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 14:29:13.234312057 CET	192.168.2.3	8.8.8.8	0x92bd	Standard query (0)	feromo.duckdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:33.390815973 CET	192.168.2.3	8.8.8.8	0x8c2c	Standard query (0)	feromo.duckdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.430285931 CET	192.168.2.3	8.8.8.8	0x23eb	Standard query (0)	157.184.7.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 5, 2021 14:29:37.693120003 CET	192.168.2.3	8.8.8.8	0xa620	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.709265947 CET	192.168.2.3	8.8.8.8	0x2461	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.761507988 CET	192.168.2.3	8.8.8.8	0xe0cd	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:38.104330063 CET	192.168.2.3	8.8.8.8	0x5914	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:43.108870029 CET	192.168.2.3	8.8.8.8	0x7060	Standard query (0)	feromo.duckdns.org	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:51.689048052 CET	192.168.2.3	8.8.8.8	0x93d6	Standard query (0)	feromo.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 14:27:18.518378019 CET	8.8.8.8	192.168.2.3	0x4360	No error (0)	liverpoolofcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 5, 2021 14:27:18.518378019 CET	8.8.8.8	192.168.2.3	0x4360	No error (0)	liverpoolofcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:17.603283882 CET	8.8.8.8	192.168.2.3	0x7c2d	No error (0)	liverpoolofcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:17.603283882 CET	8.8.8.8	192.168.2.3	0x7c2d	No error (0)	liverpoolofcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:19.957401991 CET	8.8.8.8	192.168.2.3	0x553d	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:27.876348972 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	liverpoolofcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:27.876348972 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	liverpoolofcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:30.393829107 CET	8.8.8.8	192.168.2.3	0xe960	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:32.989062071 CET	8.8.8.8	192.168.2.3	0x5c40	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:33.119859934 CET	8.8.8.8	192.168.2.3	0x5fbc	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:34.243957043 CET	8.8.8.8	192.168.2.3	0x21d1	Name error (3)	157.184.7.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 5, 2021 14:28:35.997375011 CET	8.8.8.8	192.168.2.3	0xe482	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:35.997375011 CET	8.8.8.8	192.168.2.3	0xe482	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:44.998290062 CET	8.8.8.8	192.168.2.3	0x9514	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:53.349255085 CET	8.8.8.8	192.168.2.3	0xf5e8	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:53.504070044 CET	8.8.8.8	192.168.2.3	0xcb48	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Mar 5, 2021 14:28:53.504070044 CET	8.8.8.8	192.168.2.3	0xcb48	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:03.715965033 CET	8.8.8.8	192.168.2.3	0xd6f	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:13.448314905 CET	8.8.8.8	192.168.2.3	0x92bd	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:33.609360933 CET	8.8.8.8	192.168.2.3	0x8c2c	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.476690054 CET	8.8.8.8	192.168.2.3	0x23eb	Name error (3)	157.184.7.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 5, 2021 14:29:37.743765116 CET	8.8.8.8	192.168.2.3	0xa620	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.743765116 CET	8.8.8.8	192.168.2.3	0xa620	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.757025003 CET	8.8.8.8	192.168.2.3	0x2461	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 14:29:37.810544968 CET	8.8.8.8	192.168.2.3	0xe0cd	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:38.161706924 CET	8.8.8.8	192.168.2.3	0x5914	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:38.161706924 CET	8.8.8.8	192.168.2.3	0x5914	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:43.322407007 CET	8.8.8.8	192.168.2.3	0x7060	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)
Mar 5, 2021 14:29:51.735320091 CET	8.8.8.8	192.168.2.3	0x93d6	No error (0)	feromo.duckdns.org		185.157.161.113	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- liverpoolofcfanclub.com
- checkip.dyndns.org
- whatismyipaddress.com

Code Manipulations

Statistics

Behavior

- Mixed Items.exe
- svchost.exe
- svchost.exe
- AdvancedRun.exe
- AdvancedRun.exe
- powershell.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- conhost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- Mixed Items.exe
- svchost.exe
- Mixed Items.exe
- Mixed Items.exe
- svchost.exe
- explorer.exe
- explorer.exe
- svchost.exe
- hawkgoods.exe
- Matiexgoods.exe
- svchost.exe
- origigoods20.exe
- explorer.exe
- explorer.exe
- origigoods40.exe

Click to jump to process

System Behavior

Analysis Process: Mixed Items.exe PID: 6248 Parent PID: 5648

General

Start time:	14:27:15
Start date:	05/03/2021
Path:	C:\Users\user\Desktop\Mixed Items.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Mixed Items.exe'
Imagebase:	0x3e0000
File size:	86808 bytes
MD5 hash:	017E52146C9131DBC9487D834CDFC247
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DD6CF06	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	6DD6CF06	unknown
C:\Users\user\AppData\Local\WindowsAPI	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.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	6CBBDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CBBDD66	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MixedItems.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E07C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.tmp	success or wait	1	6CBB6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	success or wait	1	6CBB6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	success or wait	1	6CBB6A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\user.config	success or wait	1	6B472684	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	40	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 75 74 66 2d 38 22 3f 3e 0d 0a	<?xml version="1.0" encoding="utf-8"?>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	17	3c 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a	<configuration>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	22	20 20 20 20 3c 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	<configSections>..	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	166	20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 47 72 6f 75 70 20 6e 61 6d 65 3d 22 75 73 65 72 53 65 74 74 69 6e 67 73 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 55 73 65 72 53 65 74 74 69 6e 67 73 47 72 6f 75 70 2c 20 53 79 73 74 65 6d 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 20 3e 0d 0a	<sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	305	20 20 20 20 20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 20 6e 61 6d 65 3d 22 48 68 57 61 63 4b 74 46 7a 66 75 6b 43 68 44 56 62 75 62 66 54 72 5a 72 56 62 41 74 61 56 79 7a 5a 62 4e 71 79 6e 74 4c 6d 72 49 50 4f 62 45 2e 43 53 6a 4a 57 42 69 54 6c 79 53 61 75 6b 45 71 48 65 64 6a 44 6a 79 69 6f 6b 73 4f 65 49 61 46 65 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 43 6c 69 65 6e 74 53 65 74 74 69 6e 67 73 53 65 63 74 69 6f 6e 2c 20 53 79 73 74 65 6d 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 20 61 6c 6c 6f 77 45 78 65 44 65 66 69 6e 69 74 69 6f 6e 3d 22	<section name="HhWacKtFzfukChDVbubfTrZrVbAtaVyzZbNqyntLmrIPObE.CSjJWBiTlySaukEqHedjDjyioksOeIaFe" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	25	20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 47 72 6f 75 70 3e 0d 0a	</sectionGroup>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	23	20 20 20 20 3c 2f 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	</configSections>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	20	20 20 20 20 3c 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	<userSettings>..	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	93	20 20 20 20 20 20 20 20 3c 48 68 57 61 63 4b 74 46 7a 66 75 6b 43 68 44 56 62 75 62 66 54 72 5a 72 56 62 41 74 61 56 79 7a 5a 62 4e 71 79 6e 74 4c 6d 72 49 50 4f 62 45 2e 43 53 6a 4a 57 42 69 54 6c 79 53 61 75 6b 45 71 48 65 64 6a 44 6a 79 69 6f 6b 73 4f 65 49 61 46 65 3e 0d 0a	<HhWacKtFzfukChDVbubf T rZrVbAtaVyzZbNqyntLmrI PObE.CSj JWBiTlySaukEqHedjDjyiok sOeIaFe>..	success or wait	4	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	4096	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 76 61 6c 75 65 3e 37 37 56 39 30 56 31 34 34 56 30 56 33 56 30 56 30 56 30 56 34 56 30 56 30 56 30 56 32 35 35 56 32 35 35 56 30 56 30 56 31 38 34 56 30 56 30 56 30 56 30 56 30 56 30 56 30 56 36 34 56 30 56 31 32 38 56 30 56 30 56 30 56 31 34 56 33 31 56 31 38 36 56 31 34 56 30 56 31 38 30 56 39 56 32 30 35 56 33 33 56 31 38 34 56 31 56 37 36 56 32 30 35 56 33 33 56 38 34 56 31 30 34 56 31 30 35 56 31 31 35 56 33 32 56 31 31 32 56 31 31 34 56 31 31 31 56 31 30 33 56 31 31 34 56 39 37 56 31 30 39 56 33 32	<value>77V90V1 44V0V3V0V0V0V4V0V0V 0V255V255V0 V0V184V0V0V0V0V0V0V 0V64V0V0V0V 0V0V0V0V0V0V0V0V0V0 V0V0V0V0V0V 0V0V0V0V0V0V0V0V0V0 V0V0V0V0V0V 0V0V128V0V0V0V14V31V 186V14V0V1 80V9V205V33V184V1V76 V205V33V84 V104V105V115V32V112V 114V111V10 3V114V97V109V32	success or wait	1962	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	94	20 20 20 20 20 20 20 20 3c 2f 48 68 57 61 63 4b 74 46 7a 66 75 6b 43 68 44 56 62 75 62 66 54 72 5a 72 56 62 41 74 61 56 79 7a 5a 62 4e 71 79 6e 74 4c 6d 72 49 50 4f 62 45 2e 43 53 6a 4a 57 42 69 54 6c 79 53 61 75 6b 45 71 48 65 64 6a 44 6a 79 69 6f 6b 73 4f 65 49 61 46 65 3e 0d 0a	</HhWacKtFzfukChDVbub f TrZrVbAtaVyzZbNqyntLmr IPObE.CS jJWBiTlySaukEqHedjDjyio ksOeIaFe>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	21	20 20 20 20 3c 2f 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	</userSettings>..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\WindowsAPI\Mixed_Items.exe_Url_4vyxcvojequ3efv0ai33sezp4mazprqx\4.152.723.137\yowqlu0x.newcfg	unknown	16	3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	</configuration>	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe	unknown	91000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 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 6f 48 ff e0 2b 29 91 b3 2b 29 91 b3 2b 29 91 b3 e8 26 ce b3 29 29 91 b3 e8 26 cc b3 39 29 91 b3 d1 0a d1 b3 28 29 91 b3 f1 0a 8d b3 20 29 91 b3 2b 29 90 b3 01 28 91 b3 d1 0a 88 b3 28 29 91 b3 0c ef e3 b3 0a 29 91 b3 0c ef ed b3 2a 29 91 b3 0c ef e9 b3 2a 29 91 b3 52 69 63 68 2b 29 91 b3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......oH..+)..+)..+)...&..)) ...&..9)......()......)..+)...(...... ().......)......*).... ..*)..Rich+)................. ........PE..L..	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 65 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 0d 0a 25 66 6d 6a 72 79 75 72 25 73 25 75 6b 64 74 78 69 71 6e 65 66 6c 66 65 25 63 25 74 6f 71 73 25 20 25 78 62 76 6a 79 25 73 25 79 6b 63 74 7a 65 6c 74 72 75 72 6c 78 25 74 25 78 64 76 72 76 74 79 25 6f 25 74 75 74 6f 66 6a 65 62 76 6f 79 67 63 6f 25 70 25 6e 6f 61 65 76 70 6b 77 72 72 72 63 66 25 20 25 6e 70 66 6b 73 64 25 77 25 6c 6a 63 6f 6e 65 70 68 25 69 25 73 69 6e 78 69 79 67 66 62 63 25 6e 25 79 6b 78 6e 62 72 70 64 71 7a 74 72 64 62 25 64 25 6d 66 75 76 75 65 65 61 6a 70 79 78 6c 61 25 65	@%nmb%e%lvjgxfcm%c %qckbdzpzhfj q%h%anbajpojymsco%o% nransp% %a qeoe%o%mitd%f%puzu%f %bjs%..%fm mjryur%s%ukdtxiqneflfe% c%toqs% %xbvjy%s%ykctzeltrurlx%t %xdvr vty%o%tutofjebvoygco%p %noaevpkwrrrcf% %npfksd%w%ljconeph%i %s inxiygfbc%n%ykxnbrpdqztr db%d%mfuvueeajpyxla%e	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	unknown	4096	72 25 73 25 6f 79 69 69 71 63 78 6f 25 63 25 6e 75 66 76 69 65 79 69 7a 78 74 78 6a 6c 25 20 25 62 6c 74 6a 6a 71 64 79 25 63 25 79 71 68 6a 6d 74 7a 66 7a 61 74 67 63 25 6f 25 6d 62 72 63 76 73 79 66 63 63 6b 66 67 72 25 6e 25 73 79 64 63 75 6c 77 65 74 65 61 25 66 25 62 66 6d 69 74 25 69 25 68 6f 69 66 7a 78 69 6d 74 67 25 67 25 63 76 61 74 25 20 25 72 6e 73 6e 77 6d 25 53 25 72 6c 73 66 25 44 25 61 70 78 78 65 64 25 52 25 78 6a 61 69 6a 68 6d 69 65 6a 79 63 71 25 53 25 67 65 63 77 7a 6c 25 56 25 65 79 7a 62 75 25 43 25 79 6d 64 76 72 66 6c 70 6d 76 25 20 25 70 71 77 62 64 6f 25 73 25 64 69 6c 71 65 61 64 68 25 74 25 61 71 67 69 7a 65 6b 76 74 69 77 78 6d 25 61 25 72 6f 77 73 74 7a 72 68 6b 64 68 71 25 72 25 63 73 77 66 6f 6f 75 65 77 25 74 25 63 73 61	r%s%oyiiqcxo%c%nufvieyi zxtxjl% %bltjjqdy%c%yqhjmtzfzatg c%o%m brcvsyfcckfgr%n%sydculw etea%f% bfmit%i%hoifzximtg%g%cv at% %rn snwm%S%rlsf%D%apxxe d%R%xjaijhm iejycq%S%gecwzl%V%ey zbu%C%ymdvrflpmv% %pqwbdo%s%dilqeadh%t %a qgizekvtiwxm%a%rowstzr hkdhq%r% cswfoouew%t%csa	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat	unknown	207	73 62 73 6d 61 64 61 25 64 25 72 65 71 75 6a 6e 25 20 25 6a 79 63 71 69 77 62 67 6c 77 6c 66 6e 25 54 25 72 6d 74 79 79 25 68 25 6d 78 70 7a 64 25 72 25 6f 74 67 25 65 25 69 66 6b 72 25 61 25 69 6b 6a 69 73 25 74 25 78 6e 6e 72 70 76 72 67 61 68 25 20 25 79 74 70 25 50 25 6f 71 63 72 25 72 25 76 6b 6f 6a 65 6a 25 6f 25 73 77 61 68 79 6d 25 74 25 6b 72 6d 64 78 75 66 73 67 78 77 65 77 6b 25 65 25 6c 73 71 69 6a 74 6d 7a 62 7a 78 6f 25 63 25 6a 78 75 25 74 25 6d 6e 64 6b 73 66 66 62 6b 66 66 68 6b 70 25 69 25 64 6d 79 7a 6b 6f 69 65 25 6f 25 63 69 76 6d 63 70 69 78 76 25 6e 25 75 63 64 25 22 25 6d 74 6c 6c 69 66 25	sbsmada%d%requjn% %jycqiwbglwl fn%T%rmtyy%h%mxpzd% r%otg%e%ifk r%a%ikjis%t%xnnrpvrgah % %ytp%P %oqcr%r%vkojej%o%swa hym%t%krmd xufsgxwewk%e%lsqijtmzb zxo%c%jx u%t%mndksffbkffhkp%i%d myzkoie% o%civmcpixv%n%ucd%"% mtllif%	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe	0	86808	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 72 9c 79 ea 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 32 01 00 00 0a 00 00 00 00 00 00 be 51 01 00 00 20 00 00 00 60 01 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 a0 01 00 00 02 00 00 57 e3 01 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...r.y........... "...0..2...........Q... ...`....@.. ....W.....@................	success or wait	1	6CBBDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.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	6CBBDD66	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Mixed Items.exe.log	unknown	1216	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 33 2c 22 53 79 73 74 65 6d 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6E07C907	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	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD45705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBB1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CBB5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CBB5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6CBBC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\Mixed Items.exe	dword	0	success or wait	1	6CBBC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CBBC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CBBC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CBBC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CBBC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	tvQKHpPrzFBMmr	unicode	explorer.exe "C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe"	success or wait	1	6CBB646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe	dword	0	success or wait	1	6CBBC075	RegSetValueExW

Analysis Process: svchost.exe PID: 6664 Parent PID: 568

General

Start time:	14:27:29
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6908 Parent PID: 568

General

Start time:	14:27:40
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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 Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 7032 Parent PID: 6248

General

Start time:	14:27:42
Start date:	05/03/2021

Path:	C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 7152 Parent PID: 7032

General

Start time:	14:27:44
Start date:	05/03/2021
Path:	C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\98ad118e-d099-425a-b583-efbd423fa467\AdvancedRun.exe' /SpecialRun 4101d8 7032
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2152 Parent PID: 6248

General

Start time:	14:27:48
Start date:	05/03/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Mixed Items.exe' -Force
Imagebase:	0xe70000
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

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	6DD6CF06	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	6DD6CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4s1cg2kf.1xe.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2jnw4mcb.ygh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\Documents\20210305	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBBBEFF	CreateDirectoryW
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.0nP0+V72.20210305142754.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4s1cg2kf.1xe.ps1	success or wait	1	6CBB6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2jnw4mcb.ygh.psm1	success or wait	1	6CBB6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4s1cg2kf.1xe.ps1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2jnw4mcb.ygh.psm1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.0nP0+V72.20210305142754.txt	unknown	3	ef bb bf	...	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.0nP0+V72.20210305142754.txt	unknown	677	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 33 30 35 31 34 32 38 32 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 30 36 30 31 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210305142826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6CBB1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD45705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD4CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD45705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD51F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6DD5203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCA03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile

Analysis Process: powershell.exe PID: 6300 Parent PID: 6248

General

Start time:	14:27:49
Start date:	05/03/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Mixed Items.exe' -Force
Imagebase:	0xe70000
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

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	6DD6CF06	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	6DD6CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mh5wpd4r.xxq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_f3qm3trx.u2l.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.YRcDMrIT.20210305142756.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mh5wpd4r.xxq.ps1	success or wait	1	6CBB6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_f3qm3trx.u2l.psm1	success or wait	1	6CBB6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mh5wpd4r.xxq.ps1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_f3qm3trx.u2l.psm1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.YRcDMrIT.20210305142756.txt	unknown	3	ef bb bf	...	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.YRcDMrIT.20210305142756.txt	unknown	677	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 33 30 35 31 34 32 38 33 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 30 36 30 31 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210305142831..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6CBB1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD45705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD4CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD45705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD51F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6DD5203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCA03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBB1B4F	ReadFile

Analysis Process: conhost.exe PID: 4144 Parent PID: 2152

General

Start time:	14:27:49
Start date:	05/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4116 Parent PID: 6248

General

Start time:	14:27:50
Start date:	05/03/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe' -Force
Imagebase:	0xe70000
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

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	6DD6CF06	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	6DD6CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4zux455h.wha.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zyhy1zxg.gf4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.RPfp4n8i.20210305142756.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBB1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4zux455h.wha.ps1	success or wait	1	6CBB6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zyhy1zxg.gf4.psm1	success or wait	1	6CBB6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4zux455h.wha.ps1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zyhy1zxg.gf4.psm1	unknown	1	31	1	success or wait	1	6CBB1B4F	WriteFile
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.RPfp4n8i.20210305142756.txt	unknown	3	ef bb bf	...	success or wait	1	6CBB1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210305\PowerShell_transcript.506013.RPfp4n8i.20210305142756.txt	unknown	712	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 33 30 35 31 34 32 38 33 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 30 36 30 31 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	********..Windows PowerShell transcript start..Start time: 20210305142831..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CBB1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD4CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCA03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD45705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD51F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6DD5203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCA03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBB1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBB1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBB1B4F	ReadFile

Analysis Process: conhost.exe PID: 5820 Parent PID: 6300

General

Start time:	14:27:50
Start date:	05/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: conhost.exe PID: 6416 Parent PID: 4116

General

Start time:	14:27:51
Start date:	05/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: svchost.exe PID: 204 Parent PID: 568

General

Start time:	14:27:52
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6460 Parent PID: 568

General

Start time:	14:27:52
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6636 Parent PID: 568

General

Start time:	14:27:55
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6800 Parent PID: 568

General

Start time:	14:27:55
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5720 Parent PID: 568

General

Start time:	14:27:56
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Mixed Items.exe PID: 7140 Parent PID: 6248

General

Start time:	14:27:56
Start date:	05/03/2021
Path:	C:\Users\user\Desktop\Mixed Items.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Mixed Items.exe
Imagebase:	0x470000
File size:	86808 bytes
MD5 hash:	017E52146C9131DBC9487D834CDFC247
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7116 Parent PID: 568

General

Start time:	14:27:56
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Mixed Items.exe PID: 6440 Parent PID: 6248

General

Start time:	14:27:57
Start date:	05/03/2021
Path:	C:\Users\user\Desktop\Mixed Items.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Mixed Items.exe
Imagebase:	0x40000
File size:	86808 bytes
MD5 hash:	017E52146C9131DBC9487D834CDFC247

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Mixed Items.exe PID: 1528 Parent PID: 6248

General

Start time:	14:27:58
Start date:	05/03/2021
Path:	C:\Users\user\Desktop\Mixed Items.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Mixed Items.exe
Imagebase:	0x9a0000
File size:	86808 bytes
MD5 hash:	017E52146C9131DBC9487D834CDFC247
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000003.321855545.0000000004361000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000003.328468981.00000000043CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000019.00000002.347873362.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000019.00000003.313769407.00000000037B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000019.00000003.313769407.00000000037B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000003.300769006.0000000000FE3000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 592 Parent PID: 568

General

Start time:	14:27:58
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6488 Parent PID: 3388

General

Start time:	14:28:02
Start date:	05/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5508 Parent PID: 792

General

Start time:	14:28:04
Start date:	05/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5540 Parent PID: 568

General

Start time:	14:28:03
Start date:	05/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: hawkgoods.exe PID: 1392 Parent PID: 1528

General

Start time:	14:28:04
Start date:	05/03/2021
Path:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\hawkgoods.exe' 0
Imagebase:	0x4c0000
File size:	532992 bytes
MD5 hash:	FFDB58533D5D1362E896E96FB6F02A95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001E.00000002.392659949.00000000004C2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001E.00000002.392659949.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001E.00000002.392659949.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001E.00000002.392659949.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001E.00000002.392659949.00000000004C2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000001E.00000002.473493158.0000000007AA0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001E.00000002.446976394.0000000003BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001E.00000002.446976394.0000000003BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001E.00000000.309264681.00000000004C2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001E.00000000.309264681.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001E.00000000.309264681.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001E.00000000.309264681.00000000004C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001E.00000000.309264681.00000000004C2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001E.00000002.445844944.0000000002FEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 96%, ReversingLabs

Analysis Process: Matiexgoods.exe PID: 6780 Parent PID: 1528

General

Start time:	14:28:05
Start date:	05/03/2021
Path:	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Matiexgoods.exe' 0
Imagebase:	0x4d0000
File size:	455680 bytes
MD5 hash:	80C61B903400B534858D047DD0919F0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 0000001F.00000002.476632403.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000001F.00000002.476632403.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 0000001F.00000000.312425541.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000001F.00000000.312425541.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.517244738.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 54%, Metadefender, Browse • Detection: 90%, ReversingLabs

Analysis Process: svchost.exe PID: 5536 Parent PID: 5508

General

Start time:	14:28:07
Start date:	05/03/2021
Path:	C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe'
Imagebase:	0x410000
File size:	86808 bytes
MD5 hash:	017E52146C9131DBC9487D834CDFC247
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 21%, ReversingLabs

Analysis Process: origigoods20.exe PID: 6064 Parent PID: 1528

General

Start time:	14:28:08
Start date:	05/03/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods20.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\origigoods20.exe' 0

Imagebase:	0xe50000
File size:	220672 bytes
MD5 hash:	61DC57C6575E1F3F2AE14C1B332AD2FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.476654920.0000000000E52000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.516404488.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000021.00000002.516404488.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods20.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 93%, ReversingLabs

Analysis Process: explorer.exe PID: 5708 Parent PID: 3388

General

Start time:	14:28:11
Start date:	05/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\jZCvibqWhOYmSqmemHIRbwmqVF\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5276 Parent PID: 792

General

Start time:	14:28:14
Start date:	05/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: origigoods40.exe PID: 5292 Parent PID: 1528

General

Start time:	14:28:14
Start date:	05/03/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods40.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\origigoods40.exe' 0
Imagebase:	0x160000
File size:	221696 bytes
MD5 hash:	AE36F0D16230B9F41FFECBD3C5B1D660
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000002.510313698.0000000002771000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000024.00000002.510313698.0000000002771000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000002.476647618.0000000000162000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000000.332943540.0000000000162000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods40.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 86%, ReversingLabs

Disassembly

Code Analysis