ID: 553435
Sample Name:
PI.1872GAT02.pdf.exe
Cookbook: default.jbs
Time: 22:21:14
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

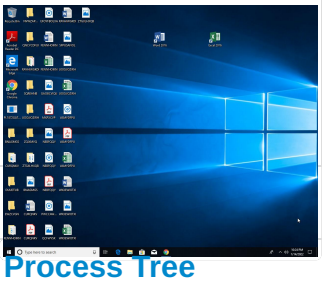
Windows Analysis Report PI.1872GAT02.pdf.exe

Overview

General Information

Sample Name:	PI.1872GAT02.pdf.exe
Analysis ID:	553435
MD5:	1396637598469e..
SHA1:	c83510c66f043c3..
SHA256:	d6f3d5fbdc9c7f6…
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

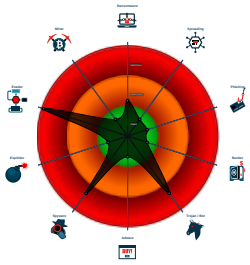
AgentTesla

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

Signatures

- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- 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…

Classification



Process Tree

- **System is w10x64**
- PI.1872GAT02.pdf.exe (PID: 6900 cmdline: "C:\Users\user\Desktop\PI.1872GAT02.pdf.exe" MD5: 1396637598469E7E918C70BE938370D5)
  - powershell.exe (PID: 5588 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3500 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmpB28A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PI.1872GAT02.pdf.exe (PID: 6360 cmdline: C:\Users\user\Desktop\PI.1872GAT02.pdf.exe MD5: 1396637598469E7E918C70BE938370D5)
- catch.exe (PID: 5320 cmdline: "C:\Users\user\AppData\Roaming\catch\catch.exe" MD5: 1396637598469E7E918C70BE938370D5)
  - powershell.exe (PID: 4656 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4592 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmp79D1.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - catch.exe (PID: 3500 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 1396637598469E7E918C70BE938370D5)
  - catch.exe (PID: 4768 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 1396637598469E7E918C70BE938370D5)
  - catch.exe (PID: 2292 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 1396637598469E7E918C70BE938370D5)
  - catch.exe (PID: 4860 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 1396637598469E7E918C70BE938370D5)
- catch.exe (PID: 2772 cmdline: "C:\Users\user\AppData\Roaming\catch\catch.exe" MD5: 1396637598469E7E918C70BE938370D5)
  - powershell.exe (PID: 5612 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6632 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmp86D2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - catch.exe (PID: 2948 cmdline: C:\Users\user\AppData\Roaming\catch\catch.exe MD5: 1396637598469E7E918C70BE938370D5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000000.500639086.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000000.500639086.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001F.00000002.512689898.0000000002E31000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000002.512689898.0000000002E31000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000020.00000000.499820218.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 53 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PI.1872GAT02.pdf.exe.2797840.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
9.0.PI.1872GAT02.pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.PI.1872GAT02.pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.0.PI.1872GAT02.pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.PI.1872GAT02.pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 62 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 submitted file

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)

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:

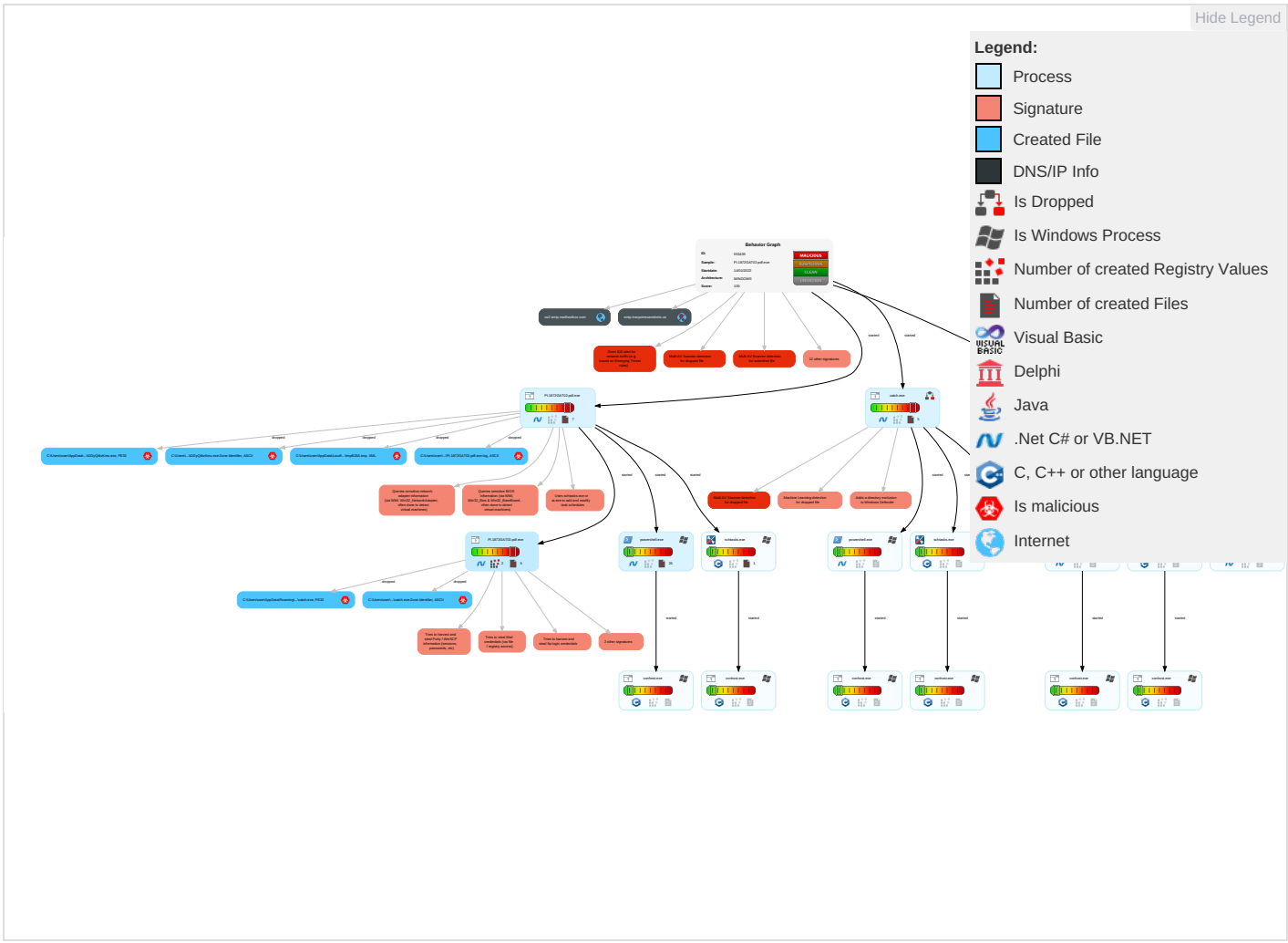
Yara detected AgentTesla

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	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	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	Scheduled Transfer	Protocol Impersonatior
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 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	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

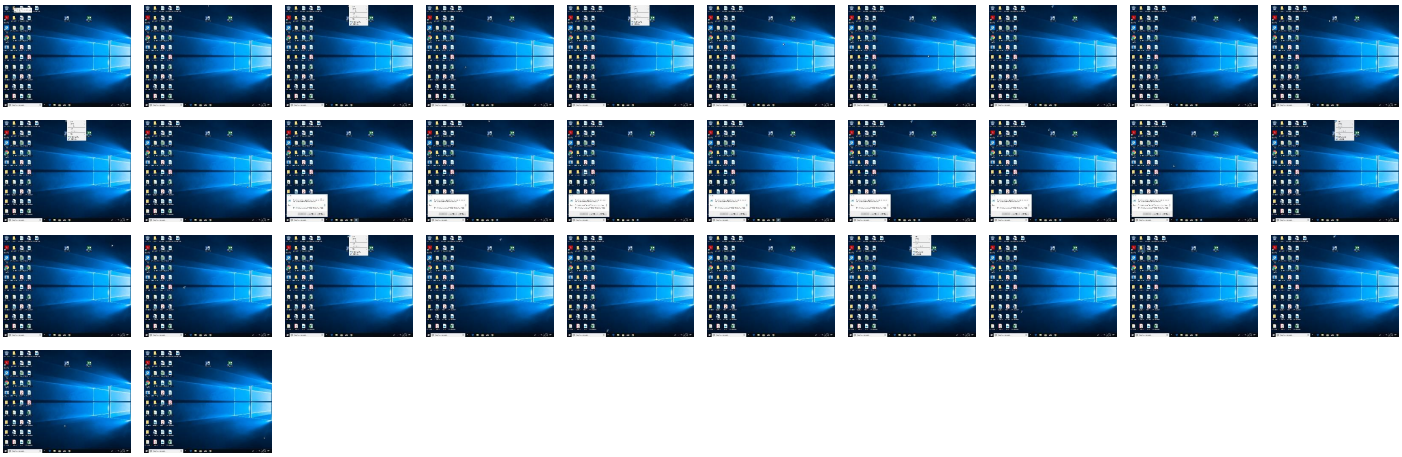
Behavior Graph



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
PI.1872GAT02.pdf.exe	48%	Virustotal		Browse
PI.1872GAT02.pdf.exe	45%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
PI.1872GAT02.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\iDGyQtItoKmu.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\catch\catch.exe	47%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\user\AppData\Roaming\iDGyQtItoKmu.exe	47%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.PI.1872GAT02.pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.catch.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.catch.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.PI.1872GAT02.pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.PI.1872GAT02.pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.PI.1872GAT02.pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.catch.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.catch.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.catch.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.2.catch.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.catch.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.PI.1872GAT02.pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.catch.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.catch.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.PI.1872GAT02.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
32.0.catch.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.catch.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.2.catch.exe.400000.0.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://https://JZAeubGsK9Sikz.org	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comt#	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.goodfont.co.kr-e	0%	Avira URL Cloud	safe	
http://fontfabrik.comY	0%	Avira URL Cloud	safe	
http://www.tiro.com5	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.kr(	0%	Avira URL Cloud	safe	
http://fontfabrik.comH	0%	URL Reputation	safe	
http://www.carterandcone.comno	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/.m	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnr-c	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sandoll.co.krs-c	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://smtp.tranpotescamdonic.us	0%	Avira URL Cloud	safe	
http://oHtnSs.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deettr	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.c	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.founder.com.cn/cnsk.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comk.	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comicr	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/r	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comk	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.carterandcone.comd	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.carterandcone.comTC	0%	URL Reputation	safe	
http://www.urwpp.deQ	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coma)	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.carterandcone.comlo	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.goodfont.co.kr.m	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnn-u?	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comtX(	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.t	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnlt8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comos	0%	Avira URL Cloud	safe	
http://www.carterandcone.comncy	0%	URL Reputation	safe	
http://www.carterandcone.comtigY	0%	Avira URL Cloud	safe	
http://www.urwpp.ded	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553435
Start date:	14.01.2022
Start time:	22:21:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI.1872GAT02.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:	41
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@33/19@2/0
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 65.1% • Quality standard deviation: 35.6%
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
22:22:20	API Interceptor	596x Sleep call for process: PI.1872GAT02.pdf.exe modified
22:22:24	API Interceptor	88x Sleep call for process: powershell.exe modified
22:22:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run catch C:\Users\user\AppData\Roaming\catch\catch.exe
22:23:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run catch C:\Users\user\AppData\Roaming\catch\catch.exe
22:23:08	API Interceptor	244x 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\PI.1872GAT02.pdf.exe.log	
Process:	C:\Users\user\Desktop\PI.1872GAT02.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
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):	22168

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Entropy (8bit):	5.6057066113124625
Encrypted:	false
SSDEEP:	384:ztCDLqyZp0WR0Xe0/RcSBKn4jultIa/paeQ99gtbcxyT1MaDZlbAV7G3WDyZBDIN:s0WRIe0C4K4Clt1Rat8hZC6fwy1VK
MD5:	53C520BE8CDC6F6BF16863F4BB562638
SHA1:	70391CC67D9B586AAC373FBF7DF6C70669BB4776
SHA-256:	8129FB32F8FCC386F60B0C6E0EF92F1322B254CAB0A4DFE00F099F140F2A4E0D
SHA-512:	A5CFCE49E18815C18805C650FCF7E6369940D88B01CE4D2F7B3D994F8836946B727F5757B4B95AB68E991AE76EB39F3C3D8D650557886BD0D87326F03D55937B
Malicious:	false
Reputation:	unknown
Preview:	@...e.....].....Q...x.v.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2qysiocw.gzb.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_ajno0yrk.14b.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_ixzoiwgh.ddw.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ixzoiwgh.ddw.ps1	
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kawb1whi.elv.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_lmd43qat.nwn.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_t2btzcjm.l41.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\tmp79D1.tmp	
Process:	C:\Users\user\AppData\Roaming\catch\catch.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1611
Entropy (8bit):	5.11715377982551
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLexvn:cgea6YrFdOFzOzN33ODOiDdKrsuTWv

C:\Users\user\AppData\Local\Temp\tmp79D1.tmp	
MD5:	3D101574D5C7C36A6FFB1733E9A405ED
SHA1:	C16D43BEB7493D4F119E60C62E5D895CD4FED054
SHA-256:	3A52CA55D7A163C15E187788137F8CB1B4A84779EC7DE748463F1AA23314E901
SHA-512:	597E2C91C729F0F284D44FE31C6AC700546624B1544A6909A87D5BDAB7D7520E126AEDD7701A8314DA2962E02A16EB848C80A3017A216FFDDD00D7445620890(
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</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmp86D2.tmp	
Process:	C:\Users\user\AppData\Roaming\catch\catch.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1611
Entropy (8bit):	5.11715377982551
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLexvn:cgea6YrFdOFzOzN33ODOiDdKrsuTWv
MD5:	3D101574D5C7C36A6FFB1733E9A405ED
SHA1:	C16D43BEB7493D4F119E60C62E5D895CD4FED054
SHA-256:	3A52CA55D7A163C15E187788137F8CB1B4A84779EC7DE748463F1AA23314E901
SHA-512:	597E2C91C729F0F284D44FE31C6AC700546624B1544A6909A87D5BDAB7D7520E126AEDD7701A8314DA2962E02A16EB848C80A3017A216FFDDD00D7445620890(
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</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmpB28A.tmp	
Process:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1611
Entropy (8bit):	5.11715377982551
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLexvn:cgea6YrFdOFzOzN33ODOiDdKrsuTWv
MD5:	3D101574D5C7C36A6FFB1733E9A405ED
SHA1:	C16D43BEB7493D4F119E60C62E5D895CD4FED054
SHA-256:	3A52CA55D7A163C15E187788137F8CB1B4A84779EC7DE748463F1AA23314E901
SHA-512:	597E2C91C729F0F284D44FE31C6AC700546624B1544A6909A87D5BDAB7D7520E126AEDD7701A8314DA2962E02A16EB848C80A3017A216FFDDD00D7445620890(
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</StartWhenAvailab

C:\Users\user\AppData\Roaming\catch\catch.exe	
Process:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	596992
Entropy (8bit):	7.236697493708965
Encrypted:	false
SSDEEP:	12288:tK777777777777N79PvlZJB1Wzf25mo+aeI73QDQYV+KS8rDblU7dhqsQ:tK777777777779hB1Wjcmo+FaQUYVQ
MD5:	1396637598469E7E918C70BE938370D5
SHA1:	C83510C66F043C3595960102AC030A3C99656768
SHA-256:	D6F3D5FBDC9C7F68E29260BADB6FD6E8F1B606798FD9FE544E0B28387F21EAF9

C:\Users\user\AppData\Roaming\catch\catch.exe	
SHA-512:	FA0CF9DCFB5F5AB5397BDDFF5642898028CC72F197B07BE439EA90CD6BCA0E8B821CE5E9BB59DE505A5F26462514CB1F3A19C517EFC9DC6784E55EB072CF9 4C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@.a.....0... ...@....@.. ....@.....0..K....@.....`.....F0..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....0.....H.....f.....E.....*.....{....*"..}....*....{....*"..}....*....{....*"..}....*....{....*"..}....*....0..... ..... ::...&..E.....0.....j.....8.... .....E....Z...x.....r...~...>...r.....Z...@...8.....(...R... ....8....8N...r...p.(..... .....:...&..(..... .....8u...8....r5..p.(..... ....8]...8....rc..p. (..... .....9@...&.9.... .....8'...8....r...p.(..

C:\Users\user\AppData\Roaming\catch\catch.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PI.1872GAT02.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\iDGyQtItoKmu.exe	
Process:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	596992
Entropy (8bit):	7.236697493708965
Encrypted:	false
SSDEEP:	12288:tK777777777777N79PvlZJB1Wzf25mo+aeI73QDQYV+KS8rDblU7dhqsQ:tK777777777771l9hB1Wjcmo+FaQUYVQ
MD5:	1396637598469E7E918C70BE938370D5
SHA1:	C83510C66F043C3595960102AC030A3C99656768
SHA-256:	D6F3D5FBDC9C7F68E29260BADB6FD6E8F1B606798FD9FE544E0B28387F21EAF9
SHA-512:	FA0CF9DCFB5F5AB5397BDDFF5642898028CC72F197B07BE439EA90CD6BCA0E8B821CE5E9BB59DE505A5F26462514CB1F3A19C517EFC9DC6784E55EB072CF9 4C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@.a.....0... ...@....@.. ....@.....0..K....@.....`.....F0..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....0.....H.....f.....E.....*.....{....*"..}....*....{....*"..}....*....{....*"..}....*....{....*"..}....*....0..... ..... ::...&..E.....0.....j.....8.... .....E....Z...x.....r...~...>...r.....Z...@...8.....(...R... ....8....8N...r...p.(..... .....:...&..(..... .....8u...8....r5..p.(..... ....8]...8....rc..p. (..... .....9@...&.9.... .....8'...8....r...p.(..

C:\Users\user\AppData\Roaming\iDGyQtItoKmu.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PI.1872GAT02.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

C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220114\PowerShell_transcript.377142.QGssXbBu.20220114222222.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):	5827
Entropy (8bit):	5.377704252121327
Encrypted:	false
SSDEEP:	96:BZRTLKN+qDo1ZPZkTLKN+qDo1ZyxDpjZdTLKN+qDo1ZPE553Zg:f
MD5:	71D228AAF492D79076B73C9D2B27013A
SHA1:	0A86EAB450B1CD81557CCF72E31E7C803F9AB44A
SHA-256:	A8517EDF2BC36DF48DF3C3E13A0BE1BA07B132AD0D1F54FC09979F9299470954
SHA-512:	893BB62391D84D9A6828EC3E1616CB6670D4A6F55ABD71D624C9B21E430F9939D08577F6F6DACEE7D3ED8FFDD33CC38E7EC6E9BD7F410C75BCA07ABABCCBC67
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114222223..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (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\iDGyQtltoKmu.exe..Process ID: 5588..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: 20220114222223..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe..**********..Windows PowerShell transcript start..Start time: 20220114222545..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20220114\PowerShell_transcript.377142.b0jiOviu.20220114222318.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):	5827
Entropy (8bit):	5.371678692143556
Encrypted:	false
SSDEEP:	96:BZcTLKNKtqDo1ZIZqTLKNKtqDo1ZIxDpjZ/TLKNKtqDo1ZZE55JZa:H
MD5:	9856AC8EDA71C81081373075C63B1FBF
SHA1:	1127A82E408E284F58970BFC492FDF3155D7F1CA
SHA-256:	67D2D901C2AE839AC5BB8A3D65AA9772BF9E469B5BFE055CDB8B12E02C1ABFBC
SHA-512:	F757EBE94C7E5248B1F858B80737A345393361E8B5B587B3FF88FCEAE7BADE7D3446FED4E838112CB59A362520B57523CFF2B0D163177C05AD0075F63D52EB22
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114222321..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (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\iDGyQtltoKmu.exe..Process ID: 5612..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: 20220114222321..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe..**********..Windows PowerShell transcript start..Start time: 20220114222631..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20220114\PowerShell_transcript.377142.dHeZQIbB.20220114222311.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):	5827
Entropy (8bit):	5.373267333914756
Encrypted:	false
SSDEEP:	96:BZ+TLKNXqDo1ZyZCTLKNXqDo1ZIxDpjZ0TLKNXqDo1ZcE554ZH:4
MD5:	85283F0F6FA628A82FFF3E0E79A83DEC
SHA1:	3917D8CD74B27A603CB7B1FCA06B2BD6522617C6
SHA-256:	81EE9C2B79D72E329B1A5B6F9043F27224D36E967C0BCBADA6E9DE1D37B7438F
SHA-512:	ABE8FEC327AB41D49175A18483020C6BE91D04863324885C4F4AD01BC275A6C17EA800D62D7D6A152AC29B0DE46D002ECFE92C2E06EA0EBC829F48307787EC1
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114222312..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (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\iDGyQtltoKmu.exe..Process ID: 4656..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: 20220114222312..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\iDGyQtltoKmu.exe..**********..Windows PowerShell transcript start..Start time: 20220114222705..Username: computer\user..RunAs User: D

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.236697493708965
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:	PI.1872GAT02.pdf.exe
File size:	596992
MD5:	1396637598469e7e918c70be938370d5
SHA1:	c83510c66f043c3595960102ac030a3c99656768
SHA256:	d6f3d5fbdc9c7f68e29260badb6fd6e8f1b606798fd9fe544e0b28387f21eaf9
SHA512:	fa0cf9dcfb5f5ab5397bddff5642898028cc72f197b07be439ea90cd6bca0e8b821ce5e9bb59de505a5f26462514cb13a19c517efc9dc6784e55eb072cf924c
SSDEEP:	12288:tK777777777777N79PvlZJB1Wzf25mo+aeI73QDQYV+KS8rDblU7dhqsQ:tK777777777771l9hB1Wjcmo+FaQUYVQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@.a.....0... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4930de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E14017 [Fri Jan 14 09:19:19 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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x910e4	0x91200	False	0.758032878445	data	7.24659563485	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x5c4	0x600	False	0.431640625	data	4.11817059658	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.0980041756627	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
01/14/22-22:24:16.780887	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49845	587	192.168.2.6	208.91.199.224
01/14/22-22:24:18.553611	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49846	587	192.168.2.6	208.91.199.224

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 22:24:15.108119965 CET	192.168.2.6	8.8.8.8	0x3206	Standard query (0)	smtp.tranpotescamdonic.us	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.266561031 CET	192.168.2.6	8.8.8.8	0x4bb1	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 14, 2022 22:24:15.262865067 CET	8.8.8.8	192.168.2.6	0x3206	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 22:24:15.262865067 CET	8.8.8.8	192.168.2.6	0x3206	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.262865067 CET	8.8.8.8	192.168.2.6	0x3206	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.262865067 CET	8.8.8.8	192.168.2.6	0x3206	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.262865067 CET	8.8.8.8	192.168.2.6	0x3206	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.432521105 CET	8.8.8.8	192.168.2.6	0x4bb1	No error (0)	smtp.tranpotescamdonic.us	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 22:24:15.432521105 CET	8.8.8.8	192.168.2.6	0x4bb1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.432521105 CET	8.8.8.8	192.168.2.6	0x4bb1	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 22:24:15.432521105 CET	8.8.8.8	192.168.2.6	0x4bb1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 14, 2022 22:24:15.432521105 CET	8.8.8.8	192.168.2.6	0x4bb1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PI.1872GAT02.pdf.exe PID: 6900 Parent PID: 1268

General

Start time:	22:22:10
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PI.1872GAT02.pdf.exe"
Imagebase:	0x2c0000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 00000000.00000002.383386260.0000000003769000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.383386260.0000000003769000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.383033038.0000000002761000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.383089116.00000000027AB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5588 Parent PID: 6900

General

Start time:	22:22:21
Start date:	14/01/2022
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\iDGyQtltoKmu.exe
Imagebase:	0xd30000
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: 1752 Parent PID: 5588

General

Start time:	22:22:22
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 3500 Parent PID: 6900

General

Start time:	22:22:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmpB28A.tmp
Imagebase:	0x20000
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: 4536 Parent PID: 3500

General

Start time:	22:22:23
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: PI.1872GAT02.pdf.exe PID: 6360 Parent PID: 6900

General

Start time:	22:22:24
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PI.1872GAT02.pdf.exe
Imagebase:	0xb60000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 00000009.00000000.377405263.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.377405263.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.378343563.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.378343563.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.610231002.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.610231002.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.379158737.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.379158737.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.606087624.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.606087624.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.379924132.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.379924132.0000000000402000.00000040.00000001.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: 5320 Parent PID: 3440

General

Start time:	22:23:02
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\catch\catch.exe"
Imagebase:	0x310000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 00000010.00000002.510080482.0000000003799000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.510080482.0000000003799000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.507778914.0000000002791000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 4656 Parent PID: 5320

General

Start time:	22:23:09
Start date:	14/01/2022
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\iDGyQtltoKmu.exe
Imagebase:	0xd30000
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: 5088 Parent PID: 4656

General

Start time:	22:23:10
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 2772 Parent PID: 3440

General

Start time:	22:23:10
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\catch\catch.exe"
Imagebase:	0x360000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 00000014.00000002.509847995.0000000003799000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.509847995.0000000003799000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.507639555.0000000002791000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 4592 Parent PID: 5320

General

Start time:	22:23:11
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmp79D1.tmp
Imagebase:	0x20000
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: 4712 Parent PID: 4592

General

Start time:	22:23:12
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 3500 Parent PID: 5320

General

Start time:	22:23:13
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0x270000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: catch.exe PID: 4768 Parent PID: 5320

General

Start time:	22:23:15
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0x3d0000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: powershell.exe PID: 5612 Parent PID: 2772

General

Start time:	22:23:17
Start date:	14/01/2022
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\iDGyQtltoKmu.exe
Imagebase:	0xd30000
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: 4368 Parent PID: 5612

General

Start time:	22:23:17
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: catch.exe PID: 2292 Parent PID: 5320

General

Start time:	22:23:17
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0x330000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 6632 Parent PID: 2772

General

Start time:	22:23:17
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iDGyQtltoKmu" /XML "C:\Users\user\AppData\Local\Temp\tmp86D2.tmp
Imagebase:	0x20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2988 Parent PID: 6632

General

Start time:	22:23:19
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: catch.exe PID: 4860 Parent PID: 5320

General

Start time:	22:23:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0x940000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 0000001F.00000000.500639086.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.500639086.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.512689898.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.512689898.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.499174008.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.499174008.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.501171531.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.501171531.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.511166140.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000002.511166140.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.502205022.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.502205022.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: catch.exe PID: 2948 Parent PID: 2772

General

Start time:	22:23:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\catch\catch.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\catch\catch.exe
Imagebase:	0x990000
File size:	596992 bytes
MD5 hash:	1396637598469E7E918C70BE938370D5
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: 00000020.00000000.499820218.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000000.499820218.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000000.501701572.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000000.501701572.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000002.606123172.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000002.606123172.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000000.502624331.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000000.502624331.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000002.609266504.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000020.00000002.609266504.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000000.500431945.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000000.500431945.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis