ID: 829690
Sample Name: pdf_novichki.rar
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 21:31:34
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report pdf_novichki.rar 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
General Information 6
Warnings 7
Created / dropped Files 7
C:\Users\alfredo\Desktop\pdf\ne trogaite.txt 7
C:\Users\alfredo\Documents\Outlook Files\Outlook Data File - NoEmail.pst 7
Static File Info 8
General 8
File Icon 8

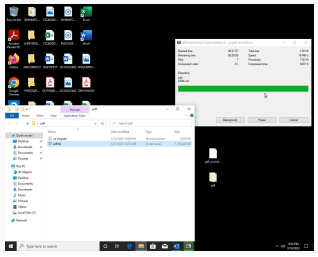
Windows Analysis Report

pdf_novichki.rar

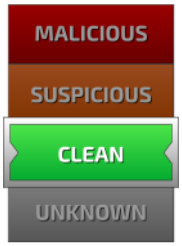
Overview

General Information

Sample Name:	pdf_novichki.rar
Analysis ID:	829690
MD5:	214c47a7948c…
SHA1:	865f07f62dcf68..
SHA256:	0a5e037e5954…



Detection

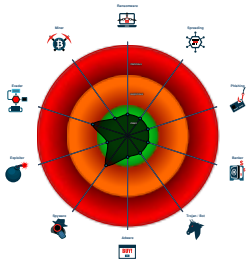


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Queries the volume information (nam…
- May sleep (evasive loops) to hinder…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 3180 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- OpenWith.exe (PID: 6576 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: 5D37A62943F1071FFFFE1DE74B8F2778)
- 7zG.exe (PID: 7128 cmdline: "C:\Program Files\7-Zip\7zG.exe" x -o"C:\Users\alfredo\Desktop\" -an -ai#7zMap27855:86:7zEvent12360 MD5: 04FB3AE7F05C8BC333125972BA907398)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

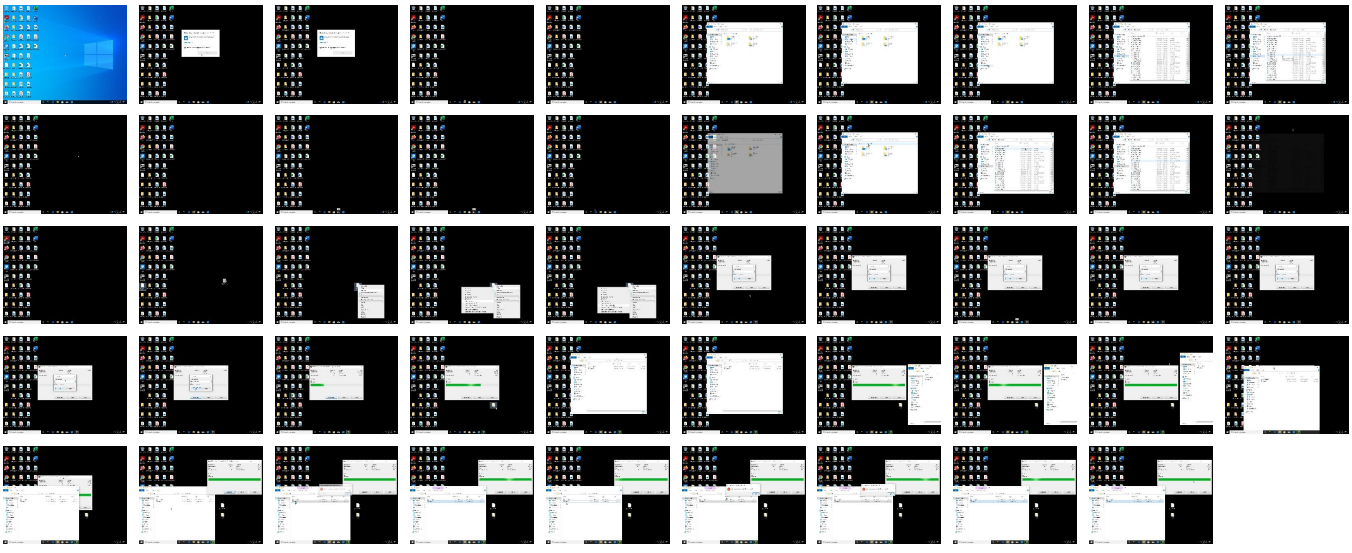
Mitre Att&ck Matrix

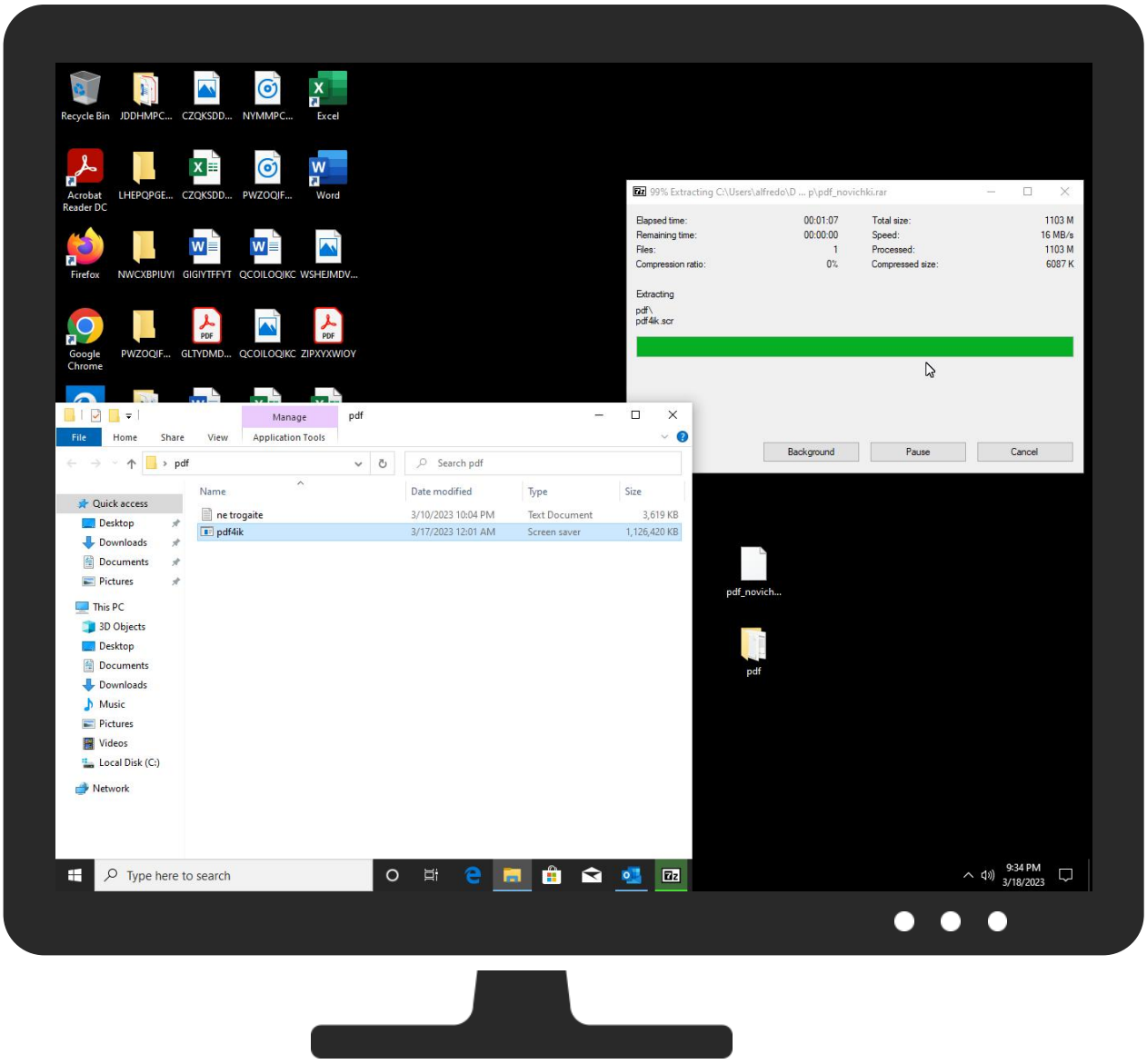
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	1 File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 1 System Information Discovery	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

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
pdf_novichki.rar	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

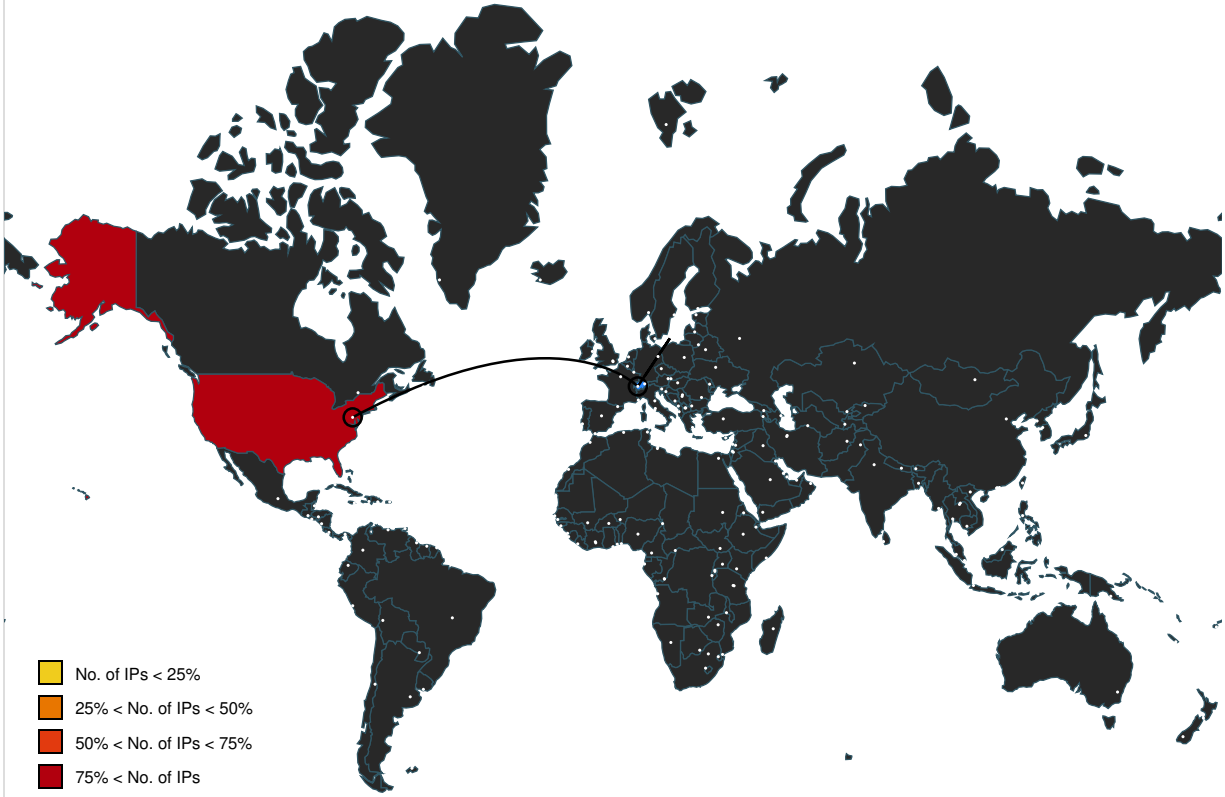
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.109.8.45	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
52.109.76.141	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829690
Start date and time:	2023-03-18 21:31:34 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled

Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	pdf_novichki.rar
Detection:	CLEAN
Classification:	clean1.winRAR@2/3@0/25

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, SIHClient.exe
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com
- 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.

Created / dropped Files

C:\Users\alfredo\Desktop\pdf\ne trogaite.txt

Process:	C:\Program Files\7-Zip\7zG.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.0, MSI Installer, Code page: 1252, Title: Installation Database, Subject: PuTTY release 0.78 installer, Author: Simon Tatham, Keywords: Installer, Comments: This installer database contains the logic and data required to install PuTTY release 0.78 (64-bit)., Template: x64;1033, Revision Number: {F5BABDF1-815A-4F73-82E1-B79790A1551E}, Create Time/Date: Fri Oct 28 19:24:49 2022, Last Saved Time/Date: Fri Oct 28 19:24:49 2022, Number of Pages: 200, Number of Words: 2, Number of Characters: 0, Name of Creating Application: Windows Installer XML Toolset (), Security: 2
Category:	dropped
Size (bytes):	3705856
Entropy (8bit):	7.837448100594935
Encrypted:	false
SSDEEP:	
MD5:	108B432C4DC0A66B657D985E180BEC71
SHA1:	262812D43303B7DDC7C04A1C243172EBE6579F00
SHA-256:	E64775374097F1B1C8FD4173F7D5BE4305B88CEC26A56D003113AFF2837AE08E
SHA-512:	5DDB97078B417F22C54DCE768564DEC58FD92A9C190F7A6CAC9C7979A0F136DD439DA1D59DD3C088E709433F5C4F79C033ABD4B6CA8989D38620C20F462338E
Malicious:	false
Reputation:	low
Preview:	.....>.....9..... ..!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D..... .....MSCF.....,.....,.....F.....k.....\Uz...HelpFile_File.....k....\U....LICENCE_File..%...q....\U...Pageant_File.0.....\U...Plink_File.....\U...PSCP_File. Y....+...\U...PSFTP_File.(...$.;...\U...PuTTY_File..Y..L.N...\U....PuTTYgen_File.%...d"X...\Uy...README_File.h....(X...\Uz...Website_File...S8....CK.}gTTI.n.s.A$....s&.J.(&l..... ..."...$.P..F.....q..1..1...C.9}....u..A.B.z..kW.].....Q...'.dhi....V7..hT.Kh8....g..$K.;.....9.....T5.

C:\Users\alfredo\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.059635826240281
Encrypted:	false
SSDEEP:	
MD5:	D838F66AF04529D38143263213F749B3
SHA1:	D4BFD311ABD40B906A0F2263AB2665F074139459
SHA-256:	1DB1C1B605712884545D222BE5F3BA5BDA6B70616F0DAD225915B6C4060E590C
SHA-512:	DF9B5830408EA6B655A575950A507AF9B5ED2A2ECED957DBA37D6C35F40E51F9F794DB7B55E926C55DFDB7A0349BEF12427ADDAF1E88DA7A8D97481591AC5F3F
Malicious:	false
Reputation:	low
Preview:	.6...AAAAAAA...AAAAA...A.A.A/ALAAAAAAAAAAAbA5AtA.!.AGA.A.bbA.A`A.].A%A.A...A AHA...AVA.A.n.AKA.A6d.A.A.A6.A~AEA...6.A.A..Ab.A...A...A...An.LA..bA...A..bA..#A..bA5..A...6#.qA.^tA..&A.5.6..A..bA..A...6`.~A.G.6N..A..bA2..A...A6#.A.-.A.#.A...A.#cA...6*#.A.*bA..A...An..A...A..A..bA..A. bA..A.tbA.SAA.AbA.S.A.6.AF..A.L.A`..A...AN.A...A..(A.}.A...A.1.A...A..A...A...AV..A..AQ.yA._.AE.MA...A|.A...AU..A...6...A...6...A.?.6...A.H.A..A.9bAK.XA...A...A...A..DA..A...A.%bAZ.A.;b.q..A.#b...7A...Aw..A68 .AAA.AtA.6.....

Static File Info

General

File type:	RAR archive data, v5
Entropy (8bit):	7.999967709504217
TrID:	• RAR Archive (5005/1) 100.00%
File name:	pdf_novichki.rar
File size:	6238622
MD5:	214c47a7948ca5d3834c3f21cd1cc208
SHA1:	865f07f62dcf68c9929baf4890328e32d7f923fa
SHA256:	0a5e037e5954adb680c726089439539073993e2e1114a9ca9e6932e7dd702d9e
SHA512:	2266ba7570fc08a77a7ea74a226ca3c81f3a934c2193f8397e85e1977b8b612dc04a29238c9ac185bd3d62ce6ee7adfc44bcd09714d02f9cb8d903d9e4cbdc70
SSDEEP:	98304:4lscwEc/FZlcjADojfq5hHLoJmx+RyzcoCsQl8N2FgF14XLqH4H:4+cwR/KUVHUJvRboCsG2pXLqH4H
TLSH:	88563392CED2C1B0826B6A311A3E9BD17B1C776590B03F129C4D35879C28E37879CD6B
File Content Preview:	Rar!.....!.....d.s\.....8..z.[.L....%..!...&\N,cJ..LJ.=..fP.#^.2....A...tIP...q..]....9.?"..,[...5...j.....C.....".c...l.j.Z.L.....5...L6...n..-.oaF.....1j..|'..cE.w...~....F1...E8:#.[-Es.`.t.....%0.O..W.... ?!...N.A.M..0..f.8".M.]%.c..6.51.>zs

File Icon

Icon Hash:	74f0e4e4e4e4e0e4