ID: 679140
Sample Name: RECHNUNG-RP0188843894.exe
Cookbook: default.jbs
Time: 10:35:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

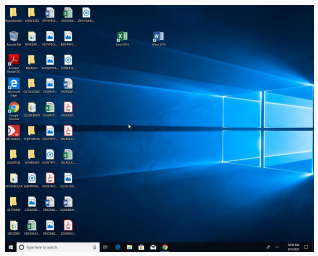
Windows Analysis Report

RECHNUNG-RP0188843894.exe

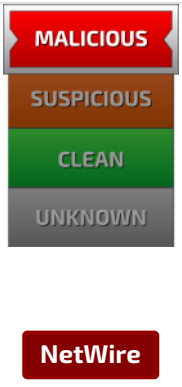
Overview

General Information

Sample Name:	RECHNUNG-RP0188843894.exe
Analysis ID:	679140
MD5:	e366f96c9b5c55…
SHA1:	8062220b613b56.
SHA256:	2a05a23d8879f9..
Tags:	exe
Infos:	



Detection



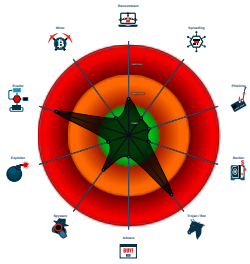
NetWire

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected NetWire RAT
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…
- Adds a directory exclusion to Windo…

Classification



Process Tree

- **System is w10x64**
- RECHNUNG-RP0188843894.exe (PID: 5900 cmdline: "C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe" MD5: E366F96C9B5C5528426A116EB49EF445)
  - powershell.exe (PID: 4684 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\rWWREmAZOgElhb.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6136 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rWWREmAZOgElhb" /XML "C:\Users\user\AppData\Local\Temp\tmp58ED.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RECHNUNG-RP0188843894.exe (PID: 5296 cmdline: C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe MD5: E366F96C9B5C5528426A116EB49EF445)
- **cleanup**

Malware Configuration

Threatname: NetWire

```
{
  "C2 list": [
    "xman2.duckdns.org:4433"
  ],
  "Password": "Password",
  "Host ID": "HostId-%Rand%",
  "Mutex": "-",
  "Startup Name": "-",
  "ActiveX Key": "-",
  "KeyLog Directory": "-"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp	MAL_unspecified_Jan18_1	Detects unspecified malware sample	Florian Roth	• 0x9e4:$s1: User-Agent: Mozilla/4.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0xaf8:$s3: [Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0xb2c:$s5: [%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]
00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Netwire_1b43df38	unknown	unknown	• 0xb08:$a1: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0xb33:$a1: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x1b1a:$a2: \Login Data • 0x1b99:$a2: \Login Data • 0x1c22:$a2: \Login Data • 0x1cb9:$a2: \Login Data • 0x1d68:$a2: \Login Data • 0x1e05:$a2: \Login Data • 0x1e5e:$a2: \Login Data • 0x99c:$a3: SOFTWARE\NetWire
00000008.00000002.520435968.0000000000436000.00000040.00000400.00020000.00000000.sdmp	MAL_unspecified_Jan18_1	Detects unspecified malware sample	Florian Roth	• 0x9e4:$s1: User-Agent: Mozilla/4.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0xaf8:$s3: [Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0xb2c:$s5: [%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]
00000008.00000002.520435968.0000000000436000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.RECHNUNG-RP0188843894.exe.400000.0.unpack	MAL_unspecified_Jan18_1	Detects unspecified malware sample	Florian Roth	• 0x34fe4:$s1: User-Agent: Mozilla/4.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x350f8:$s3: [Log Started] - [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x3512c:$s5: [%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d]
8.0.RECHNUNG-RP0188843894.exe.400000.0.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
8.0.RECHNUNG-RP0188843894.exe.400000.0.unpack	MALWARE_Win_NetWire	Detects NetWire RAT	ditekSHen	• 0x34f9c:$x1: SOFTWARE\NetWire • 0x34f44:$x2: 4E 65 74 57 69 72 65 00 53 4F 46 54 57 41 52 45 5C 00 • 0x34fe4:$s1: User-Agent: Mozilla/4.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x34fc8:$s3: GET %s HTTP/1.1 • 0x35108:$s4: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x35133:$s4: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x34e84:$s6: -m "%s" • 0x34f94:$g1: HostId • 0x35f7c:$g2: History • 0x35fcc:$g3: encrypted_key • 0x34fb0:$g4: Install Date • 0x35bd8:$g5: hostname • 0x35be4:$g6: encryptedUsername • 0x35bf8:$g7: encryptedPassword
8.0.RECHNUNG-RP0188843894.exe.400000.0.unpack	Windows_Trojan_Netwire_1b43df38	unknown	unknown	• 0x35108:$a1: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x35133:$a1: [%.2d/%.2d/%d %.2d:%.2d:%.2d] • 0x3611a:$a2: \Login Data • 0x36199:$a2: \Login Data • 0x36222:$a2: \Login Data • 0x362b9:$a2: \Login Data • 0x36368:$a2: \Login Data • 0x36405:$a2: \Login Data • 0x3645e:$a2: \Login Data • 0x34f9c:$a3: SOFTWARE\NetWire
0.2.RECHNUNG-RP0188843894.exe.50474e8.10.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 23 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

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)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Remote Access Functionality

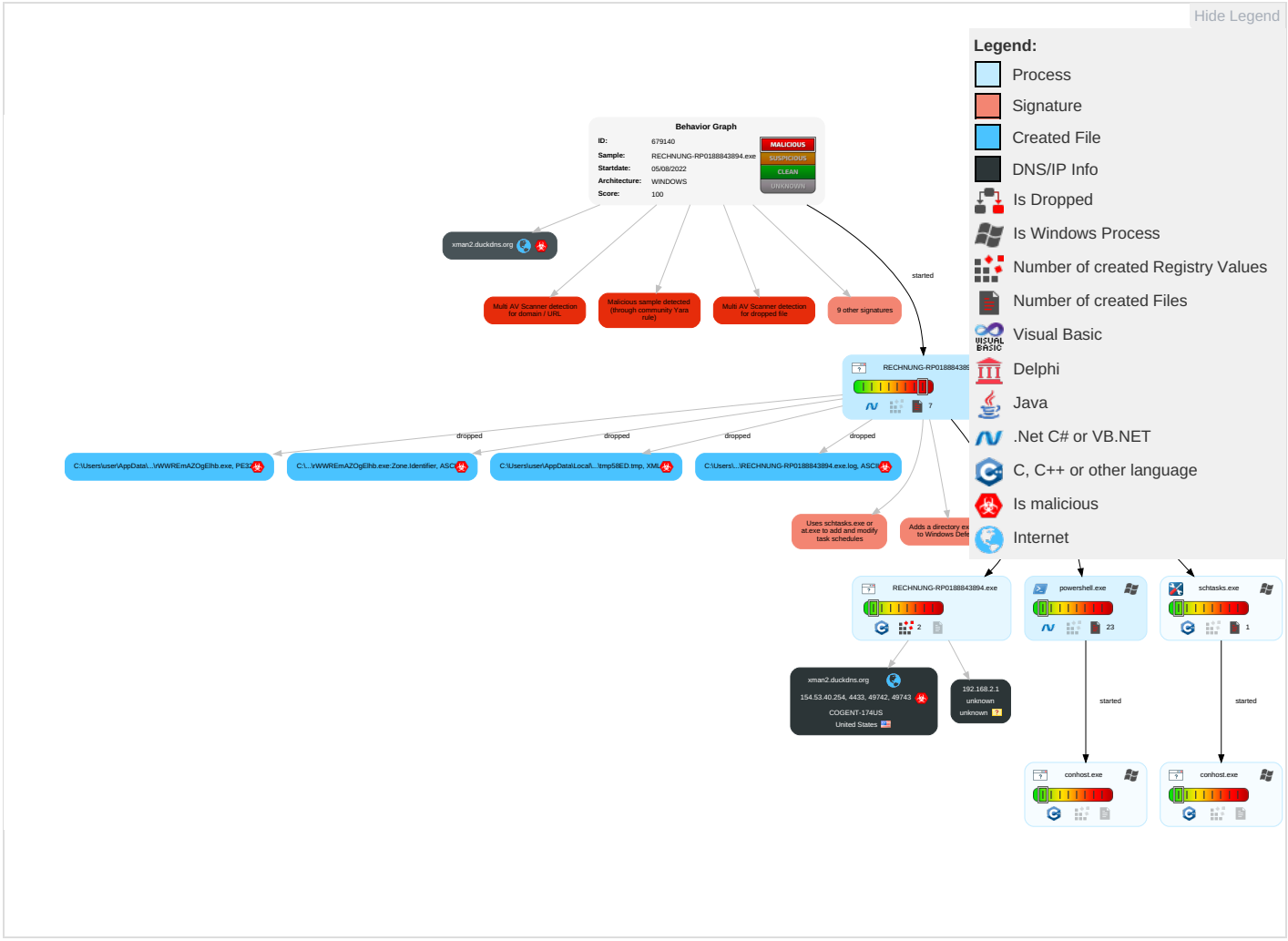
Yara detected NetWire RAT

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

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 Scheduled Task/Job	1 Scheduled Task/Job	1 1 Process Injection	1 Masquerading	2 1 Input Capture	2 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 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	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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	1 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 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory 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 2 Software Packing	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

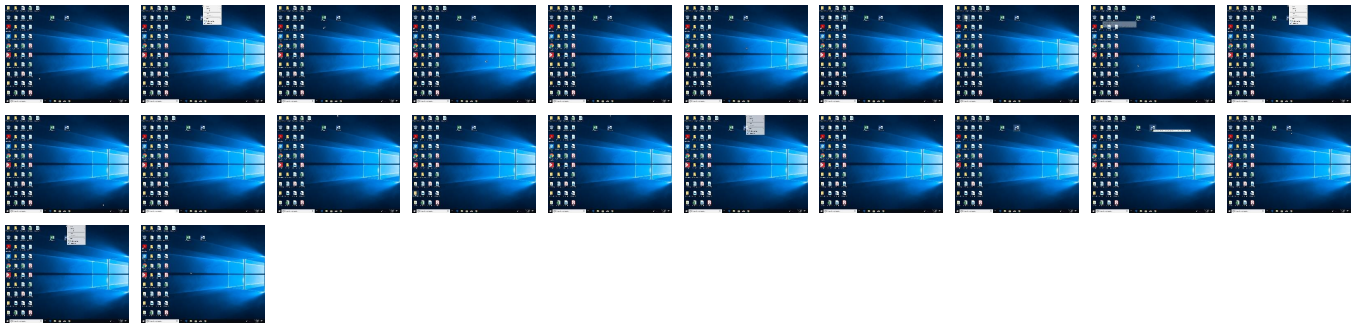
Behavior Graph



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
RECHNUNG-RP0188843894.exe	21%	Virustotal		Browse
RECHNUNG-RP0188843894.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.LokiBot	
RECHNUNG-RP0188843894.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\rWWREmAZOgElhb.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rWWREmAZOgElhb.exe	21%	Virustotal		Browse
C:\Users\user\AppData\Roaming\rWWREmAZOgElhb.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.LokiBot	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
xman2.duckdns.org	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	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://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
xman2.duckdns.org:4433	0%	Avira URL Cloud	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://www.jiyu-kobo.co.jp/	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://%s%%s%.2d-%.2d-%.4d	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xman2.duckdns.org	154.53.40.254	true	true	• 15%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
xman2.duckdns.org:4433	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://%s%%s%.2d-%.2d-%.4d	RECHNUNG-RP0188843894.exe, 00000000.00000002.294293877.00000000035D0000.00000004.00000800.00020000.00000000.sdmp, RECHNUNG-RP0188843894.exe, 00000000.00000002.298287612.0000000004FBA000.00000004.00000800.00020000.00000000.sdmp, RECHNUNG-RP0188843894.exe, 00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp, RECHNUNG-RP0188843894.exe, 00000008.00000002.520435968.0000000436000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RECHNUNG-RP0188843894.exe, 00000000.00000002.294293877.00000000035D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	RECHNUNG-RP0188843894.exe, 00000000.00000002.300524429.00000000073C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.53.40.254	xman2.duckdns.org	United States		174	COGENT-174US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679140
Start date and time: 05/08/202210:35:08	2022-08-05 10:35:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RECHNUNG-RP0188843894.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:	31
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.evad.winEXE@9/8@61/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 87% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, 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 NtDeviceIoControlFile 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
10:36:20	API Interceptor	62x Sleep call for process: RECHNUNG-RP0188843894.exe modified
10:36:27	API Interceptor	40x 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\RECHNUNG-RP0188843894.exe.log

Process:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe

File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	**true**
Reputation:	moderate, 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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22272
Entropy (8bit):	5.6027188324374535
Encrypted:	false
SSDEEP:	384:TtCD60F+x6b9TtYS0nMjsh77Y9g9SJ3xa1BMrm7Z1AV7ag464l+iyY:z65TtYTMohf9cBa4yA
MD5:	77E6E1687BDD89C7F85A8C47BF26E0E4
SHA1:	C8DCDA5CB81BD6D396C120DE2D9F49F0F7372AF9
SHA-256:	612CDA6AE4D2DD8DE394FE35782450112EE8EA0853CC4AC697B68D6DE63518E1
SHA-512:	3615659735FD74E97ECC4B6C5E78C3E426B2413AFB598DAE25EEC583118E8A6620FBC82B9ED3EEB41EC804653919F8DB6C43AFD7BCF75CD66AA64B6A486B0904
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....e.B.8.....@.B.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wk1p5wlt.kwk.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__PSScriptPolicyTest_xdm2vbum.tbe.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\tmp58ED.tmp

Process:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1601
Entropy (8bit):	5.153566916379303
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtgvVxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTgvrv
MD5:	A390F07FE0E218E00223091926488958
SHA1:	5E2D9D09FF1167925B4EF3AF96708D5CBB0574FC
SHA-256:	FE2451F076CC5EEC42D4EED783E94A8773DBEC17BA99D23BBC3FC451346060BA
SHA-512:	A274F6DFC7820032EDA8FA974901D7E9FF471ABE6128399770B5B2CCC0F049F4C66F63E1E030D5A243EC362DAF533863F41C6DCF6E0979329AA49D08BB6D2AEB
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\rWWREmAZOgElhb.exe

Process:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1299456
Entropy (8bit):	7.136675750532489
Encrypted:	false
SSDEEP:	24576:iTJpjM7KzOkDwPN2XanQBOrOlaLlpxtRYNNHV3lSpWBb62:EjW77kQNaaQB6w+tR63AEbT
MD5:	E366F96C9B5C5528426A116EB49EF445
SHA1:	8062220B613B56116D638B3D7F5DD043F3BC096E
SHA-256:	2A05A23D8879F9D001AF335779B5102DD644B08D2F106353C28C8CE303EE9B58
SHA-512:	1DC21DA10C45A5FBD5058E85D775CCCEC140A0FEC067183013457D7AB87F9BFD758429A999DF2B2BF0AFD19D44B289418C6A84576893465217 64A812A0430E9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 21%, Browse • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...=J.....0.....L.... ..`....@.. .....@.....@.....L..O....`..4..... .....L..... ....H.....text....-... ....`.rsrc...4....`.....0.....@..@.reloc..... .....@..B.....L.....H.....@...,P.....$...l....z.....}.....(.....(.....{.....o.....*....0..w.....r...p..s.....~O.....o.....r$..p..B....(.....s.....o.....s.....o.....{.....o.....&.....,..o.....*.....Tc.....]k.....0.:.....o .....,+..{....o!...o"....o#...o$....B.....(.....*...0..n.....r...p..s.....o.....r...p..B...(%.....(&.....B...('.....s.....o(.....r...p()...&...&.....,..o.....*.....KZ..

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

Process:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.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]....ZoneId=0

C:\Users\user\Documents\20220805\PowerShell_transcript.579569.W2+ITsAi.20220805103625.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):	5805
Entropy (8bit):	5.4162470391864685
Encrypted:	false
SSDEEP:	96:BZdSh7NpuqDo1Zm1ZQh7NpuqDo1Zztj1jZPh7NpuqDo1ZQIllPZs:Z63MQJ
MD5:	B137630C24F96036570C1BAA5B9239F2
SHA1:	6CC286C1FE58C6730CE716171D03956FA85200C4
SHA-256:	2E371FCC58D890D819E1CCB5F669DFBCC3DCBF8E0810787FCD597BFAFB26CD40
SHA-512:	0E85F55184B8BED1AF55AB18D3714F45A95B79C23ECA19AFE4E09095480C0DA0B70AA8DBE3C8AC4CE3975A64AEAAA24B4D5CD1D234546A02961093C267E687D9
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805103627..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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\rWWREmAZOgElhb.exe..Process ID: 4684..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: 20220805103627..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\rWWREmAZOgElhb.exe..**********..Windows PowerShell transcript start..Start time: 20220805104006..Username: computer\user..RunAs User: DESKTOP-716T

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.136675750532489
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:	RECHNUNG-RP0188843894.exe
File size:	1299456
MD5:	e366f96c9b5c5528426a116eb49ef445
SHA1:	8062220b613b56116d638b3d7f5dd043f3bc096e
SHA256:	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58
SHA512:	1dc21da10c45a5fbd5058e85d775cccec140a0fec067183013457d7ab87f9bfd758429a999df2b2bf0afd19d44b289418c6a8457689346521764a812a0430e9d
SSDEEP:	24576:iTJpjM7KzOkDwPN2XanQBOrOlaLlpxtRYNNHV3lSpWBb62:EjW77kQNaaQB6w+tR63AEbT
TLSH:	9855F1D153898B42CC6A0EB8E3122524C776EC7FEAFEC6C98DC7B8A695367C31550907
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...=J.....0.....L... ...`....@.. .....@.....@.....

File Icon

Icon Hash:	d72e9cb139dccfcf

Static PE Info

General	
Entrypoint:	0x4d4cf2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xEDF14A3D [Sun Jul 1 20:36:13 2096 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
dec eax
xor al, 46h
pop edx
push esp
inc edi
inc ebx
pop eax
cmp byte ptr [edi], dh
pop eax
xor al, 38h
inc edx
inc esi
aaa
xor al, 47h
inc edx
xor eax, 00003838h
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
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

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
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
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
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4ca0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x6a034	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x142000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd4c84	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	0xd2d10	0xd2e00	False	0.8411728475103735	data	7.588133806696738	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x6a034	0x6a200	False	0.5962322401354535	data	5.178213553665152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x142000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

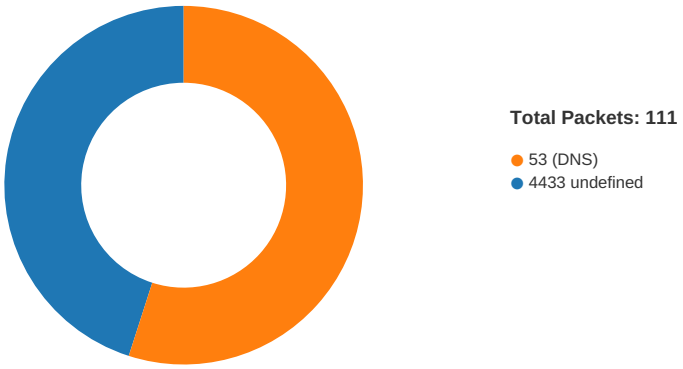
Name	RVA	Size	Type	Language	Country
RT_ICON	0xd62b0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xd6718	0x988	data		
RT_ICON	0xd70a0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4291831602, next used block 4291766318		
RT_ICON	0xd8148	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4291963945, next used block 4291897384		
RT_ICON	0xda6f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4291961375, next used block 4291898412		
RT_ICON	0xde918	0x5488	data		
RT_ICON	0xe3da0	0x94a8	data		
RT_ICON	0xed248	0x10828	data		
RT_ICON	0xfda70	0x42028	data		
RT_GROUP_ICON	0x13fa98	0x84	data		
RT_VERSION	0x13fb1c	0x32c	data		
RT_MANIFEST	0x13fe48	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:36:31.656548977 CEST	49742	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:31.785160065 CEST	4433	49742	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:32.285480022 CEST	49742	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:32.414148092 CEST	4433	49742	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:32.988645077 CEST	49742	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:33.117506027 CEST	4433	49742	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:33.416806936 CEST	49743	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:33.545722961 CEST	4433	49743	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:34.098393917 CEST	49743	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:34.227309942 CEST	4433	49743	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:34.786665916 CEST	49743	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:34.915574074 CEST	4433	49743	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:35.064102888 CEST	49744	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:35.192878962 CEST	4433	49744	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:35.785737038 CEST	49744	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:35.914422989 CEST	4433	49744	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:36.598412037 CEST	49744	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:36.727186918 CEST	4433	49744	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:37.061316967 CEST	49745	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:37.191855907 CEST	4433	49745	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:37.692172050 CEST	49745	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:37.822730064 CEST	4433	49745	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:38.395467043 CEST	49745	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:38.526202917 CEST	4433	49745	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:38.803046942 CEST	49746	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:38.932218075 CEST	4433	49746	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:39.583028078 CEST	49746	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:39.713824034 CEST	4433	49746	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:40.294439077 CEST	49746	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:40.423263073 CEST	4433	49746	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:40.592158079 CEST	49747	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:40.724276066 CEST	4433	49747	154.53.40.254	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:36:41.286220074 CEST	49747	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:41.415282011 CEST	4433	49747	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:42.005039930 CEST	49747	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:42.133578062 CEST	4433	49747	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:42.345221996 CEST	49748	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:42.474113941 CEST	4433	49748	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:43.083301067 CEST	49748	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:43.212089062 CEST	4433	49748	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:43.895879984 CEST	49748	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:44.024575949 CEST	4433	49748	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:46.123747110 CEST	49749	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:46.252482891 CEST	4433	49749	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:46.787447929 CEST	49749	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:46.916045904 CEST	4433	49749	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:47.599356890 CEST	49749	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:47.727940083 CEST	4433	49749	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:47.991723061 CEST	49750	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:48.123805046 CEST	4433	49750	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:48.786936045 CEST	49750	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:48.917444944 CEST	4433	49750	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:49.599488974 CEST	49750	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:49.729923010 CEST	4433	49750	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:49.982130051 CEST	49753	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:50.110760927 CEST	4433	49753	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:50.787128925 CEST	49753	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:50.915821075 CEST	4433	49753	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:51.599704027 CEST	49753	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:51.729322910 CEST	4433	49753	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:51.878688097 CEST	49764	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:52.009074926 CEST	4433	49764	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:52.521568060 CEST	49764	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:52.652179956 CEST	4433	49764	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:53.162271023 CEST	49764	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:53.297802925 CEST	4433	49764	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:53.473370075 CEST	49767	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:53.601818085 CEST	4433	49767	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:54.115428925 CEST	49767	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:54.243844032 CEST	4433	49767	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:54.756218910 CEST	49767	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:54.885060072 CEST	4433	49767	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:55.036801100 CEST	49768	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:55.167428017 CEST	4433	49768	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:55.678061008 CEST	49768	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:55.808562994 CEST	4433	49768	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:56.318871975 CEST	49768	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:56.449253082 CEST	4433	49768	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:56.702867031 CEST	49769	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:56.831686974 CEST	4433	49769	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:57.350337982 CEST	49769	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:57.479219913 CEST	4433	49769	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:57.990900040 CEST	49769	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:58.120034933 CEST	4433	49769	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:58.267262936 CEST	49771	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:58.398102045 CEST	4433	49771	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:58.928436041 CEST	49771	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:59.059241056 CEST	4433	49771	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:59.569082022 CEST	49771	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:36:59.699763060 CEST	4433	49771	154.53.40.254	192.168.2.3
Aug 5, 2022 10:36:59.879499912 CEST	49772	4433	192.168.2.3	154.53.40.254

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:37:00.006443977 CEST	4433	49772	154.53.40.254	192.168.2.3
Aug 5, 2022 10:37:00.506665945 CEST	49772	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:37:00.633924961 CEST	4433	49772	154.53.40.254	192.168.2.3
Aug 5, 2022 10:37:01.147384882 CEST	49772	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:37:01.274421930 CEST	4433	49772	154.53.40.254	192.168.2.3
Aug 5, 2022 10:37:01.705369949 CEST	49773	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:37:01.834167957 CEST	4433	49773	154.53.40.254	192.168.2.3
Aug 5, 2022 10:37:02.334907055 CEST	49773	4433	192.168.2.3	154.53.40.254
Aug 5, 2022 10:37:02.463685989 CEST	4433	49773	154.53.40.254	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:36:31.537233114 CEST	64851	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:31.644268990 CEST	53	64851	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:33.306726933 CEST	49316	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:33.415712118 CEST	53	49316	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:35.044496059 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:35.061969995 CEST	53	56417	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:36.911396027 CEST	55923	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:37.020839930 CEST	53	55923	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:38.692194939 CEST	57723	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:38.801831961 CEST	53	57723	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:40.571228981 CEST	58116	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:40.590759039 CEST	53	58116	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:42.295826912 CEST	57421	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:42.315216064 CEST	53	57421	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:46.095731974 CEST	65358	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:46.115034103 CEST	53	65358	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:47.882976055 CEST	49873	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:47.989651918 CEST	53	49873	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:49.872052908 CEST	53802	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:49.981059074 CEST	53	53802	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:51.858122110 CEST	49327	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:51.877913952 CEST	53	49327	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:53.451700926 CEST	58981	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:53.468983889 CEST	53	58981	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:55.015970945 CEST	64452	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:55.035500050 CEST	53	64452	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:56.591095924 CEST	61380	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:56.699117899 CEST	53	61380	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:58.245412111 CEST	52985	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:58.264786959 CEST	53	52985	8.8.8.8	192.168.2.3
Aug 5, 2022 10:36:59.858932018 CEST	58625	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:36:59.878209114 CEST	53	58625	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:01.662796021 CEST	52810	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:01.682724953 CEST	53	52810	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:04.619702101 CEST	50778	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:04.652460098 CEST	53	50778	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:06.317322016 CEST	55151	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:06.336277962 CEST	53	55151	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:07.881041050 CEST	59795	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:07.900559902 CEST	53	59795	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:09.460410118 CEST	59390	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:09.569144011 CEST	53	59390	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:11.152297020 CEST	64816	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:11.171711922 CEST	53	64816	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:12.699728966 CEST	64996	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:12.717298031 CEST	53	64996	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:37:14.259583950 CEST	53816	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:14.279328108 CEST	53	53816	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:15.823040962 CEST	52096	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:15.840471029 CEST	53	52096	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:17.631247044 CEST	60640	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:17.648741961 CEST	53	60640	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:19.297427893 CEST	49844	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:19.315130949 CEST	53	49844	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:21.475986958 CEST	51518	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:21.495111942 CEST	53	51518	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:23.301103115 CEST	49723	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:23.320753098 CEST	53	49723	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:25.064929962 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:25.086270094 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:26.827538967 CEST	56639	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:26.846600056 CEST	53	56639	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:28.562978983 CEST	50450	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:28.582564116 CEST	53	50450	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:30.299781084 CEST	62724	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:30.317589998 CEST	53	62724	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:32.129381895 CEST	55403	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:32.149024963 CEST	53	55403	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:33.799338102 CEST	61877	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:33.816740990 CEST	53	61877	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:35.426795959 CEST	64624	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:35.446317911 CEST	53	64624	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:37.056559086 CEST	50608	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:37.163552999 CEST	53	50608	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:38.849581003 CEST	58497	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:38.869132042 CEST	53	58497	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:41.844887972 CEST	62701	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:41.955061913 CEST	53	62701	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:43.851545095 CEST	61555	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:43.962873936 CEST	53	61555	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:45.681632996 CEST	64433	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:45.702647924 CEST	53	64433	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:47.396205902 CEST	54096	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:47.415527105 CEST	53	54096	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:48.989021063 CEST	63326	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:49.095340014 CEST	53	63326	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:50.657083988 CEST	60110	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:50.676486969 CEST	53	60110	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:52.247087002 CEST	49230	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:52.264116049 CEST	53	49230	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:53.914503098 CEST	57442	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:53.934427023 CEST	53	57442	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:55.519682884 CEST	51557	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:55.536693096 CEST	53	51557	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:57.280276060 CEST	65334	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:57.299637079 CEST	53	65334	8.8.8.8	192.168.2.3
Aug 5, 2022 10:37:58.863878012 CEST	52487	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:37:58.883487940 CEST	53	52487	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:00.566334963 CEST	51994	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:00.585450888 CEST	53	51994	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:02.394844055 CEST	51658	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:02.413980961 CEST	53	51658	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:04.002974033 CEST	58950	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:04.110976934 CEST	53	58950	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:05.913765907 CEST	53883	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:38:06.022942066 CEST	53	53883	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:07.601854086 CEST	59065	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:07.621037006 CEST	53	59065	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:09.176075935 CEST	55686	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:09.193387985 CEST	53	55686	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:10.723433018 CEST	64589	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:10.745327950 CEST	53	64589	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:12.292118073 CEST	64934	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:12.309509039 CEST	53	64934	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:13.843307018 CEST	55795	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:13.861007929 CEST	53	55795	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:15.391450882 CEST	64635	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:15.408987045 CEST	53	64635	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:17.311804056 CEST	55269	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:17.331228971 CEST	53	55269	8.8.8.8	192.168.2.3
Aug 5, 2022 10:38:18.986835957 CEST	63083	53	192.168.2.3	8.8.8.8
Aug 5, 2022 10:38:19.007206917 CEST	53	63083	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 10:36:31.537233114 CEST	192.168.2.3	8.8.8.8	0xc79f	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:33.306726933 CEST	192.168.2.3	8.8.8.8	0xc00e	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:35.044496059 CEST	192.168.2.3	8.8.8.8	0xfcc6	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:36.911396027 CEST	192.168.2.3	8.8.8.8	0x6221	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:38.692194939 CEST	192.168.2.3	8.8.8.8	0xbaca	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:40.571228981 CEST	192.168.2.3	8.8.8.8	0x9cb8	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:42.295826912 CEST	192.168.2.3	8.8.8.8	0x99ca	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:46.095731974 CEST	192.168.2.3	8.8.8.8	0xc292	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:47.882976055 CEST	192.168.2.3	8.8.8.8	0xf4f	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:49.872052908 CEST	192.168.2.3	8.8.8.8	0xee1f	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:51.858122110 CEST	192.168.2.3	8.8.8.8	0x3d8c	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:53.451700926 CEST	192.168.2.3	8.8.8.8	0x280a	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:55.015970945 CEST	192.168.2.3	8.8.8.8	0xacf4	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:56.591095924 CEST	192.168.2.3	8.8.8.8	0x20f1	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:58.245412111 CEST	192.168.2.3	8.8.8.8	0xafb7	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:59.858932018 CEST	192.168.2.3	8.8.8.8	0xf7f7	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:01.662796021 CEST	192.168.2.3	8.8.8.8	0x697e	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:04.619702101 CEST	192.168.2.3	8.8.8.8	0x120d	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:06.317322016 CEST	192.168.2.3	8.8.8.8	0x5c89	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:07.881041050 CEST	192.168.2.3	8.8.8.8	0x16d2	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:09.460410118 CEST	192.168.2.3	8.8.8.8	0xa4a0	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:11.152297020 CEST	192.168.2.3	8.8.8.8	0xe7a2	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:12.699728966 CEST	192.168.2.3	8.8.8.8	0x46cb	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 10:37:14.259583950 CEST	192.168.2.3	8.8.8.8	0x3685	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:15.823040962 CEST	192.168.2.3	8.8.8.8	0x6d0c	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:17.631247044 CEST	192.168.2.3	8.8.8.8	0xfe86	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:19.297427893 CEST	192.168.2.3	8.8.8.8	0xc9b	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:21.475986958 CEST	192.168.2.3	8.8.8.8	0x7be2	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:23.301103115 CEST	192.168.2.3	8.8.8.8	0x371f	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:25.064929962 CEST	192.168.2.3	8.8.8.8	0x66a9	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:26.827538967 CEST	192.168.2.3	8.8.8.8	0x3d67	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:28.562978983 CEST	192.168.2.3	8.8.8.8	0xa765	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:30.299781084 CEST	192.168.2.3	8.8.8.8	0x71d3	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:32.129381895 CEST	192.168.2.3	8.8.8.8	0xf5d	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:33.799338102 CEST	192.168.2.3	8.8.8.8	0x4585	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:35.426795959 CEST	192.168.2.3	8.8.8.8	0x9206	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:37.056559086 CEST	192.168.2.3	8.8.8.8	0x63c8	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:38.849581003 CEST	192.168.2.3	8.8.8.8	0xa6f2	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:41.844887972 CEST	192.168.2.3	8.8.8.8	0xa866	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:43.851545095 CEST	192.168.2.3	8.8.8.8	0xcd5d	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:45.681632996 CEST	192.168.2.3	8.8.8.8	0xea78	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:47.396205902 CEST	192.168.2.3	8.8.8.8	0xd829	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:48.989021063 CEST	192.168.2.3	8.8.8.8	0xdee0	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:50.657083988 CEST	192.168.2.3	8.8.8.8	0x879	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:52.247087002 CEST	192.168.2.3	8.8.8.8	0x2e5	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:53.914503098 CEST	192.168.2.3	8.8.8.8	0x5609	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:55.519682884 CEST	192.168.2.3	8.8.8.8	0xbbfe	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:57.280276060 CEST	192.168.2.3	8.8.8.8	0x724e	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:58.863878012 CEST	192.168.2.3	8.8.8.8	0x34f5	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:00.566334963 CEST	192.168.2.3	8.8.8.8	0x592c	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:02.394844055 CEST	192.168.2.3	8.8.8.8	0x83c0	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:04.002974033 CEST	192.168.2.3	8.8.8.8	0x1903	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:05.913765907 CEST	192.168.2.3	8.8.8.8	0xc26	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:07.601854086 CEST	192.168.2.3	8.8.8.8	0x81b	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:09.176075935 CEST	192.168.2.3	8.8.8.8	0xd68d	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:10.723433018 CEST	192.168.2.3	8.8.8.8	0xbf16	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:12.292118073 CEST	192.168.2.3	8.8.8.8	0xd601	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:13.843307018 CEST	192.168.2.3	8.8.8.8	0xff6a	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 10:38:15.391450882 CEST	192.168.2.3	8.8.8.8	0x360d	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:17.311804056 CEST	192.168.2.3	8.8.8.8	0x7f6b	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:18.986835957 CEST	192.168.2.3	8.8.8.8	0x1ea2	Standard query (0)	xman2.duckdns.org	A (IP address)	IN (0x0001)

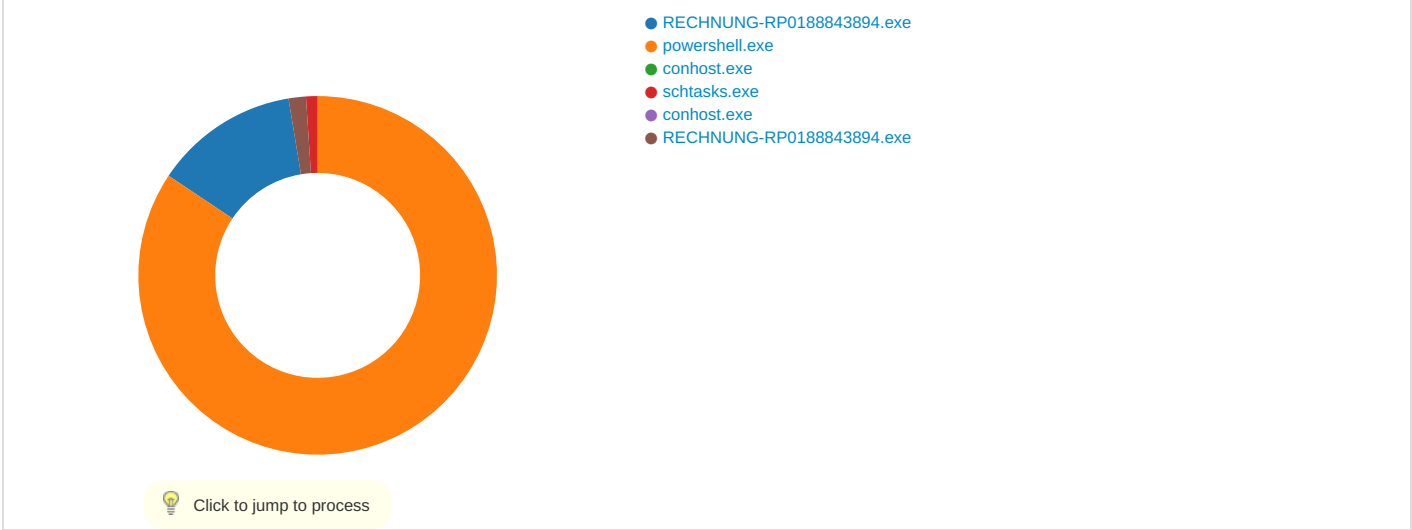
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 10:36:31.644268990 CEST	8.8.8.8	192.168.2.3	0xc79f	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:33.415712118 CEST	8.8.8.8	192.168.2.3	0xc00e	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:35.061969995 CEST	8.8.8.8	192.168.2.3	0xfcc6	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:37.020839930 CEST	8.8.8.8	192.168.2.3	0x6221	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:38.801831961 CEST	8.8.8.8	192.168.2.3	0xbaca	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:40.590759039 CEST	8.8.8.8	192.168.2.3	0x9cb8	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:42.315216064 CEST	8.8.8.8	192.168.2.3	0x99ca	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:46.115034103 CEST	8.8.8.8	192.168.2.3	0xc292	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:47.989651918 CEST	8.8.8.8	192.168.2.3	0xf4f	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:49.981059074 CEST	8.8.8.8	192.168.2.3	0xee1f	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:51.877913952 CEST	8.8.8.8	192.168.2.3	0x3d8c	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:53.468983889 CEST	8.8.8.8	192.168.2.3	0x280a	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:55.035500050 CEST	8.8.8.8	192.168.2.3	0xacf4	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:56.699117899 CEST	8.8.8.8	192.168.2.3	0x20f1	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:58.264786959 CEST	8.8.8.8	192.168.2.3	0xafb7	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:36:59.878209114 CEST	8.8.8.8	192.168.2.3	0xf7f7	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:01.682724953 CEST	8.8.8.8	192.168.2.3	0x697e	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:04.652460098 CEST	8.8.8.8	192.168.2.3	0x120d	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:06.336277962 CEST	8.8.8.8	192.168.2.3	0x5c89	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:07.900559902 CEST	8.8.8.8	192.168.2.3	0x16d2	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:09.569144011 CEST	8.8.8.8	192.168.2.3	0xa4a0	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:11.171711922 CEST	8.8.8.8	192.168.2.3	0xe7a2	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:12.717298031 CEST	8.8.8.8	192.168.2.3	0x46cb	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:14.279328108 CEST	8.8.8.8	192.168.2.3	0x3685	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:15.840471029 CEST	8.8.8.8	192.168.2.3	0x6d0c	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:17.648741961 CEST	8.8.8.8	192.168.2.3	0xfe86	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:19.315130949 CEST	8.8.8.8	192.168.2.3	0xc9b	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:21.495111942 CEST	8.8.8.8	192.168.2.3	0x7be2	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:23.320753098 CEST	8.8.8.8	192.168.2.3	0x371f	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:25.086270094 CEST	8.8.8.8	192.168.2.3	0x66a9	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 10:37:26.846600056 CEST	8.8.8.8	192.168.2.3	0x3d67	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:28.582564116 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:30.317589998 CEST	8.8.8.8	192.168.2.3	0x71d3	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:32.149024963 CEST	8.8.8.8	192.168.2.3	0xf5d	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:33.816740990 CEST	8.8.8.8	192.168.2.3	0x4585	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:35.446317911 CEST	8.8.8.8	192.168.2.3	0x9206	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:37.163552999 CEST	8.8.8.8	192.168.2.3	0x63c8	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:38.869132042 CEST	8.8.8.8	192.168.2.3	0xa6f2	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:41.955061913 CEST	8.8.8.8	192.168.2.3	0xa866	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:43.962873936 CEST	8.8.8.8	192.168.2.3	0xcd5d	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:45.702647924 CEST	8.8.8.8	192.168.2.3	0xea78	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:47.415527105 CEST	8.8.8.8	192.168.2.3	0xd829	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:49.095340014 CEST	8.8.8.8	192.168.2.3	0xdee0	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:50.676486969 CEST	8.8.8.8	192.168.2.3	0x879	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:52.264116049 CEST	8.8.8.8	192.168.2.3	0x2e5	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:53.934427023 CEST	8.8.8.8	192.168.2.3	0x5609	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:55.536693096 CEST	8.8.8.8	192.168.2.3	0xbbfe	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:57.299637079 CEST	8.8.8.8	192.168.2.3	0x724e	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:37:58.883487940 CEST	8.8.8.8	192.168.2.3	0x34f5	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:00.585450888 CEST	8.8.8.8	192.168.2.3	0x592c	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:02.413980961 CEST	8.8.8.8	192.168.2.3	0x83c0	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:04.110976934 CEST	8.8.8.8	192.168.2.3	0x1903	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:06.022942066 CEST	8.8.8.8	192.168.2.3	0xc26	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:07.621037006 CEST	8.8.8.8	192.168.2.3	0x81b	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:09.193387985 CEST	8.8.8.8	192.168.2.3	0xd68d	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:10.745327950 CEST	8.8.8.8	192.168.2.3	0xbf16	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:12.309509039 CEST	8.8.8.8	192.168.2.3	0xd601	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:13.861007929 CEST	8.8.8.8	192.168.2.3	0xff6a	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:15.408987045 CEST	8.8.8.8	192.168.2.3	0x360d	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:17.331228971 CEST	8.8.8.8	192.168.2.3	0x7f6b	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)
Aug 5, 2022 10:38:19.007206917 CEST	8.8.8.8	192.168.2.3	0x1ea2	No error (0)	xman2.duckdns.org		154.53.40.254	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: RECHNUNG-RP0188843894.exe PID: **5900**, Parent PID: **5248**

General

Target ID:	0
Start time:	10:36:12
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe"
Imagebase:	0xec0000
File size:	1299456 bytes
MD5 hash:	E366F96C9B5C5528426A116EB49EF445
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000000.00000002.294293877.00000000035D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.294293877.00000000035D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Netwire_1b43df38, Description: unknown, Source: 00000000.00000002.294293877.00000000035D0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000000.00000002.298287612.0000000004FBA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Netwire_1b43df38, Description: unknown, Source: 00000000.00000002.298287612.0000000004FBA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **4684**, Parent PID: **5900**

General

Target ID:	4
Start time:	10:36:24
Start date:	05/08/2022
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\rWWREmAZOgElhb.exe
Imagebase:	0xc40000
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	6D00CF06	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	6D00CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BDB5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BDB5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wk1p5wlt.kwk.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xdm2vbum.tbe.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE5BEFF	CreateDirectoryW
C:\Users\user\Documents\20220805\PowerShell_transcript.579569.W2+ITsAi.20220805103625.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wk1p5wlt.kwk.ps1	success or wait	1	6BE56A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xdm2vbum.tbe.psm1	success or wait	1	6BE56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wk1p5wlt.kwk.ps1	0	1	31	1	success or wait	1	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xdm2vbum.tbe.psm1	0	1	31	1	success or wait	1	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220805\PowerShell_transcript.579569.W2+ITsAi.20220805103625.txt	0	3	ff		success or wait	1	6BE51B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.579569.W2+ITsAi.20220805103625.txt	3	681	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 38 30 35 31 30 33 36 32 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 37 39 35 36 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220805103627Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 579569 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 79 14 00 00 18 00 00 00 fd 0e 65 05 42 09 38 09 17 09 00 00 40 01 42 00 06 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eyeB8@B@	success or wait	1	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D2D76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-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 16 3b 40 01 38 4d 40 01 3f 4d 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@[@NT@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	6D2D76FC	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	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CFF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22388	success or wait	1	6CFF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	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	6BE51B4F	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	6BE51B4F	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	6BE51B4F	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	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BE51B4F	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	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BE51B4F	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	637	end of file	2	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BE51B4F	ReadFile

Analysis Process: conhost.exe PID: **4700**, Parent PID: **4684**

General

Target ID:	5
Start time:	10:36:24
Start date:	05/08/2022
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: **6136**, Parent PID: **5900**

General

Target ID:	6
Start time:	10:36:24
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rWWREmAZOgElhb" /XML "C:\Users\user\AppData\Local\Temp\tmp58ED.tmp
Imagebase:	0xe30000
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\tmp58ED.tmp	unknown	2	success or wait	1	E3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp58ED.tmp	unknown	1602	success or wait	1	E3ABD9	ReadFile

Analysis Process: conhost.exe PID: **5668**, Parent PID: **6136**

General

Target ID:	7
Start time:	10:36:26
Start date:	05/08/2022

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: RECHNUNG-RP0188843894.exe PID: **5296**, Parent PID: **5900**

General

Target ID:	8
Start time:	10:36:28
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RECHNUNG-RP0188843894.exe
Imagebase:	0xa20000
File size:	1299456 bytes
MD5 hash:	E366F96C9B5C5528426A116EB49EF445
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_unspecified_Jan18_1, Description: Detects unspecified malware sample, Source: 00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Netwire_1b43df38, Description: unknown, Source: 00000008.00000000.287368211.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: MAL_unspecified_Jan18_1, Description: Detects unspecified malware sample, Source: 00000008.00000002.520435968.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000008.00000002.520435968.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Netwire_1b43df38, Description: unknown, Source: 00000008.00000002.520435968.0000000000436000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\NetWire	success or wait	1	410C86	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\NetWire	HostId	unicode	HostId-oqEmii	success or wait	1	410CB3	RegSetValueExA
HKEY_CURRENT_USER\Software\NetWire	Install Date	unicode	2022-08-05 17:36:30	success or wait	1	410CB3	RegSetValueExA

Disassembly

No disassembly