ID: 562447
Sample Name: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Cookbook: default.jbs
Time: 22:06:28
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

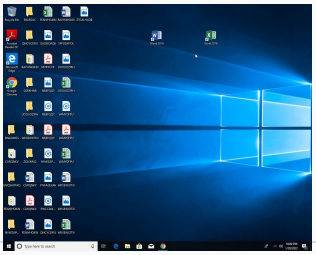
Windows Analysis Report

Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe

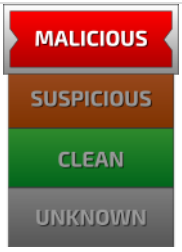
Overview

General Information

Sample Name:	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Analysis ID:	562447
MD5:	1165567a0b77f4..
SHA1:	0f9b426434142e..
SHA256:	bc79a9662ee07c..
Tags:	AgentTesla exe geo TUR
Infos:	



Detection



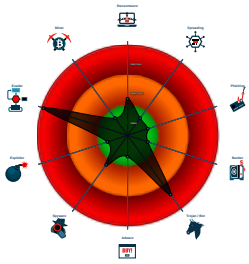
AgentTesla

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

Signatures

- Found malware configuration
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Sigma detected: Powershell Defend…
- .NET source code contains method …
- Adds a directory exclusion to Windo…
- Moves itself to temp directory

Classification



Process Tree

- **System is w10x64**
- Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe (PID: 7148 cmdline: "C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe" MD5: 1165567A0B77F4C1BB44B4E89A6AB0C6)
  - powershell.exe (PID: 5872 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe (PID: 348 cmdline: C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe MD5: 1165567A0B77F4C1BB44B4E89A6AB0C6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "genelmudur@carmar.com.tr",
  "Password": "412Abc",
  "Host": "mail.carmar.com.tr"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.609602504.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.609602504.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000000.420145183.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.420145183.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.423638484.0000000002821000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.286da80.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.286da80.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x8860:$v1: SbieDll.dll • 0x887a:$v2: USER • 0x8886:$v3: SANDBOX • 0x8898:$v4: VIRUS • 0x88e8:$v4: VIRUS • 0x88a6:$v5: MALWARE • 0x88b8:$v6: SCHMIDTI • 0x88cc:$v7: CURRENTUSER
0.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.39161d0.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.39161d0.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.39161d0.3.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2ef38:$s1: get_kbok • 0x2f86c:$s2: get_CHoo • 0x304c7:$s3: set_passwordIsSet • 0x2ed3c:$s4: get_enableLog • 0x333e3:$s8: torbrowser • 0x31dbf:$s10: logins • 0x31737:$s11: credential • 0x2e130:$g1: get_Clipboard • 0x2e13e:$g2: get_Keyboard • 0x2e14b:$g3: get_Password • 0x2f71a:$g4: get_CtrlKeyDown • 0x2f72a:$g5: get_ShiftKeyDown • 0x2f73b:$g6: get_AltKeyDown
Click to see the 27 entries				

Sigma Overview

System Summary

Sigma detected: Powershell Defender Exclusion

Jbx Signature Overview

AV Detection

Found malware configuration

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

Moves itself to temp directory

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected AgentTesla

Remote Access Functionality

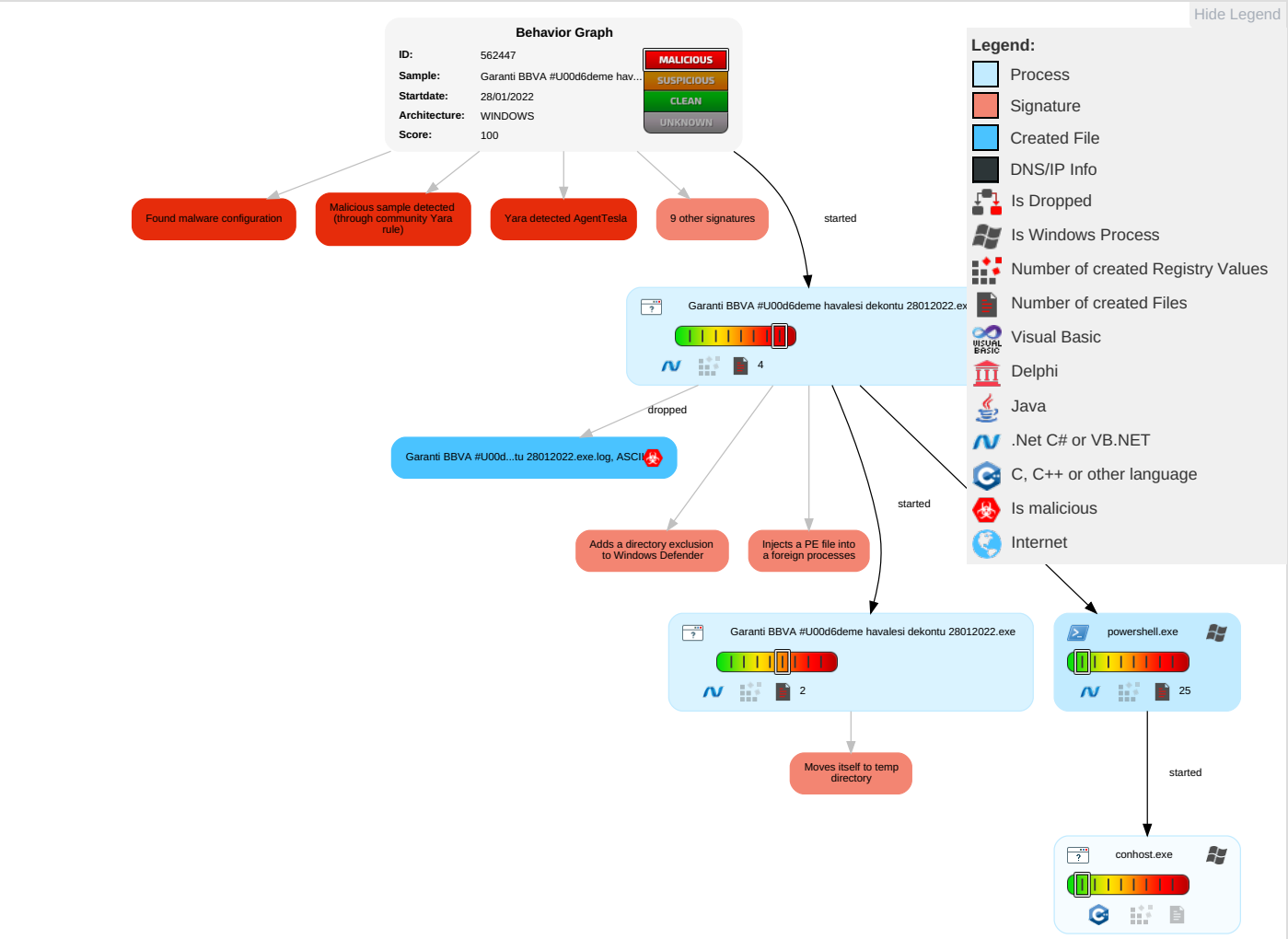
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Disable or Modify Tools	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Software Packing	DCSync	1 1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

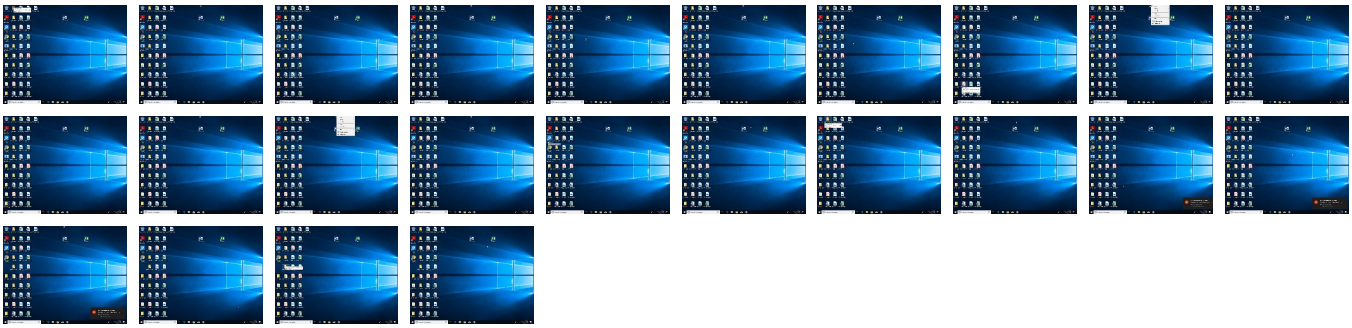
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.krom	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/(8Y	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn0	0%	Avira URL Cloud	safe	
http://fontfabrik.comH	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com-	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.carterandcone.comn-uW4	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.urwpp.de2	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrita/3t	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comuct	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.carterandcone.comoaU#	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.carterandcone.comL	0%	URL Reputation	safe	
http://www.carterandcone.comtig	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.tiro.com=4(	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnof	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krur	0%	Avira URL Cloud	safe	
http://www.fontbureau.comzana	0%	Avira URL Cloud	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.carterandcone.como.n1l	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	URL Reputation	safe	
http://www.sandoll.co.krormals	0%	Avira URL Cloud	safe	
http://jShurS.com	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnngHd0f	0%	Avira URL Cloud	safe	
http://fontfabrik.com3#	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.comona	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.urwpp.dei	0%	URL Reputation	safe	
http://www.tiro.comb7	0%	Avira URL Cloud	safe	
http://www.tiro.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnof	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.krom	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355170597.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423638484.0000000002821000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359113858.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersK	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.369152448.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.368567365.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.369355580.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comal	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358843853.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comva	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3606914 90.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.359113858.000000000582B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.359681545.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.359776827.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .360055629.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.360829535.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.36018 7492.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.360554461.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.359413477.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .358843853.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.358592373.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35828 3224.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.358447965.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.360469432.0 00000000005834000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .359301993.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.359533939.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35803 9744.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.357926320.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.358715813.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .358993784.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.359915400.000000000582B000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html.	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3702062 75.000000000584E000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.370061836.000000000584E000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/(8Y	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3553046 11.000000000582B000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.4261975 42.0000000006A22000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn0	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357806950.000000000582D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.388488428.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.366935666.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.comH	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.350869061.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355304611.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355468183.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355170597.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360329882.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersQ	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.369152448.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.370472312.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.370117885.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.370263172.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.369355580.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com-	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359681545.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359776827.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360055629.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360187492.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360469432.0000000005834000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360329882.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.347736149.0000000005812000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comn-uW4	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.382690752.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.384906841.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.351234985.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.350694608.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersers	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.367140383.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.367290287.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designerse	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.388488428.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.de2	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.365974509.0000000005833000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita/3t	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423244260.0000000000F37000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356455349.0000000005830000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.362207789.0000000005833000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comuct	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358592373.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355304611.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355468183.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355170597.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.354988403.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comoaU#	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358283224.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358039744.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357926320.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.379214344.0000000005837000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357806950.000000000582D000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358447965.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358039744.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357926320.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360329882.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423638484.0000000002821000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423919644.000000000296B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360329882.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnf	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3574299 70.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.356947618.000000000582B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.359113858.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.357084557.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .357661015.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.356455349.0000000005830000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35722 8121.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.358843853.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.358592373.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .357557721.0000000005834000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.358283224.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35622 0554.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.357806950.000000000582D 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.358447965.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .358039744.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.357926320.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35871 5813.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.358993784.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.356798724.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .358165735.000000000582B000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.4261975 42.0000000006A22000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.362207789.0000000005833000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.4245169 26.0000000003829000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000009.0000 0002.609602504.0000000000402000.00000040 .00000400.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000009.00000000.411345685.0000000000402 000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersn	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.378804706.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comL	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comtig	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358592373.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358447965.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423244260.0000000000F37000.00000004.00000020.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comt	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.347736149.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comc	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com=4(	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357347420.0000000000F3C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zhongyicts.com.cnof	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358592373.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358283224.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357806950.000000000582D000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358447965.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358039744.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357926320.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comTC	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://blog.iandreev.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423638484.0000000002821000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krur	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.354988403.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comzana	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.423244260.0000000000F37000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comt	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359681545.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359776827.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.n1l	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360691490.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359113858.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359681545.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359776827.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360055629.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360829535.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360187492.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360554461.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358843853.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358592373.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358283224.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358447965.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360469432.000000005834000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358039744.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358993784.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360329882.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.351896800.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.352102008.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.352172787.000000000583A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359681545.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359776827.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359413477.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.000000006A22000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359301993.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359533939.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.founder.com.cn/cn/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356947618.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356455349.0000000005830000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356798724.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357429970.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356947618.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357084557.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357661015.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356455349.0000000005830000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357228121.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358843853.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358592373.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357557721.000000005834000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358283224.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356220554.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357806950.000000000582D000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358447965.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.000000006A22000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356124605.0000000005834000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358039744.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357926320.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358715813.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355955515.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357986724.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.358165735.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.369990715.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.426197542.0000000006A22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnva	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357806950.000000000582D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krormals	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.355170597.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.354988403.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.377880804.000000000584E000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.377992898.000000000584E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://jShurS.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3667684 31.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.365170390.0000000005833000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.366160551.0000000005833 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.369675673.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .369152448.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.366389497.0000000005833000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.36714 0383.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.367620714.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.367773094.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .366571443.000000000582F000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.367450369.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.36954 5952.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.365638963.0000000005833 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.368567365.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .364554047.0000000005833000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.368042056.000000000582B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.36502 1902.0000000005833000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.367290287.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.365974509.0 000000005833000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .365774759.0000000005833000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.365311185.0000000005833000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnngHd0f	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3574299 70.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.356947618.000000000582B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.357084557.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.356455349.0 000000005830000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .357228121.000000000582B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.357557721.0000000005834000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.35622 0554.000000000582B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.356798724.000000000582B 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com3#	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3509619 40.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.350869061.000000000582B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.350413352.000000000582B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.350694608.0 00000000582B000.00000004.00000800.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.4261975 42.0000000006A22000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comona	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3587158 13.000000000582B000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3578069 50.000000000582D000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.4261975 42.0000000006A22000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.urwpp.dei	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3667684 31.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.366160551.0000000005833000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.366389497.0000000005833 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.366571443.0 00000000582F000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .365974509.0000000005833000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comb7	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3596815 45.000000000582B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.359776827.000000000582B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.359915400.000000000582B 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.coml	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359681545.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359776827.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.360055629.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.359915400.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers:	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.366935666.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnof	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357429970.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356947618.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357084557.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357661015.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356455349.0000000005830000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357228121.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.357557721.0000000005834000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356220554.000000000582B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.356798724.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.366768431.000000000582B000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562447
Start date:	28.01.2022
Start time:	22:06:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Garanti BBVA #U00d6deme havalesi dekontu 28012022.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:	23
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 0.9%) • Quality average: 53.3% • Quality standard deviation: 41.2%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.49.150.241, 51.104.136.2, 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe

Simulations

Behavior and APIs

Time	Type	Description
22:07:48	API Interceptor	213x Sleep call for process: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe modified
22:07:57	API Interceptor	23x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.log

Process:	C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20672
Entropy (8bit):	5.5765297390842195
Encrypted:	false
SSDEEP:	384:GtADCIBeug2bbSP8J0FYTCrRYSBKn6jultIQ77Y9gVSJ3xGT1MabZlXzQCldd:MCEMmYX4K6CltHfVcMCyfjt
MD5:	91C563A0D577593E2E01B14124FC5E20
SHA1:	4767E03D23CFC0CD89F4F0BE619F17EB0251729E
SHA-256:	468B79AF433903983B223C2C3E5FF71894F9681797D2E4CA4544C93A27185953
SHA-512:	465F3E493A58E8D86CF2D17EC323D4CDE2627C5FDB8AA19C9D606DCDAE7524F39FBFFCB88A6A9772D81FA9F268D0B64ECA3689D92B398D8B13839E14F82BBC04
Malicious:	false
Reputation:	low
Preview:	@...e.....h.....I.....@.....H.....<@.^.L."My...:B..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)v.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3xqdgrlj.qdv.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yehsm0ba.evc.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\Documents\20220128\PowerShell_transcript.141700.07yUmft4.20220128220756.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3604
Entropy (8bit):	5.309471348750791
Encrypted:	false
SSDEEP:	96:BZsTL1NeqDo1Z32Z9TL1NeqDo1ZCqad0cd0cd0+Zx:KJJN
MD5:	3C48A3BABCDE9E7049CF299C4485B560
SHA1:	7DD70A0A1FCA17ECF5EEC218370F9078ED2D955D
SHA-256:	0D3055922F956BE374BA456D1D2ED61EA921C7984319691F3AABF85C87C241AB
SHA-512:	AD5226B5E4E3372A2483CE5A638474A31A10C49B0B499A4F7CF0711701C04B5F4D746216E9AB5B487E14905D11D0E8C10412CB4534E990F130458053EE5E7A1B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220128220757..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 141700 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe..Process ID: 5872..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: 20220128220757..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe..**********..Command start time: 20220128221020..**********.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.596652033279201
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
File size:	868864
MD5:	1165567a0b77f4c1bb44b4e89a6ab0c6
SHA1:	0f9b426434142ee8e753e19844add22b4bc87bf2
SHA256:	bc79a9662ee07c43bbec9321f04e2f186d22b2d7c10c790b828b51de0df1604a

SHA512:	e031211d6106cc5a75187b74222113c9c4f00750c098d5b90a3f7f18c34783df63496f67bb4b721f3f4fc48b71a916031a5141f8e2d7b52242d47f59961f40b8
SSDEEP:	12288:9RkSo9ICKf2a38eS5GSJlXG7ySjc6d5/yjq+UznduJi+:9R3oyCm38bgSJlMzn6jq+UzCv
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a.................4...........S... ...`....@.. .... @................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d538e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F3CEED [Fri Jan 28 11:09:33 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd5340	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x5b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd52ee	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd3394	0xd3400	False	0.521329511834	data	6.6020439756	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xd6000	0x1e8	0x200	False	0.861328125	data	6.59493596605	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x5b0	0x600	False	0.424479166667	data	4.09876160434	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd80a0	0x324	data		
RT_MANIFEST	0xd83c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

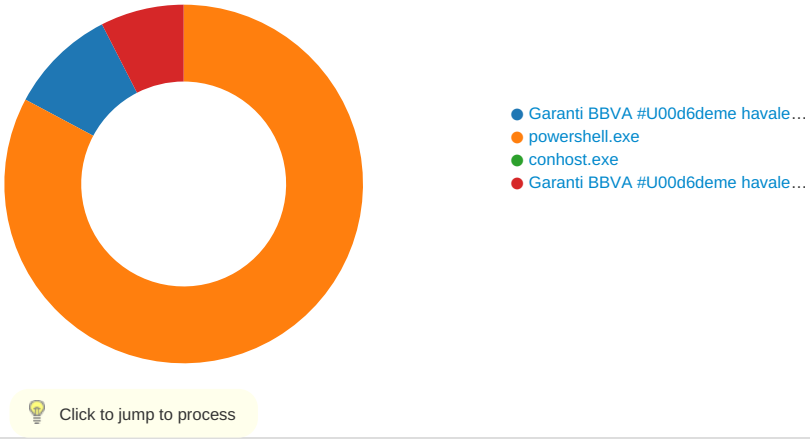
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	OffsetAndRu.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	OffsetAndRu.exe

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe PID: 7148, Parent PID: 2944

General	
Target ID:	0
Start time:	22:07:23
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe"
Imagebase:	0x3d0000
File size:	868864 bytes
MD5 hash:	1165567A0B77F4C1BB44B4E89A6AB0C6
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.423638484.0000000002821000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.423919644.000000000296B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.424516926.0000000003829000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.424516926.0000000003829000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EE9CF06	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	6EE9CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6F1AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EDD03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile

Analysis Process: powershell.exe PID: **5872**, Parent PID: **7148**

General

Target ID:	7
Start time:	22:07:55
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Garanti BBVA #U00d6deme ha valesi dekontu 28012022.exe
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EE9CF06	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	6EE9CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yehsm0ba.evc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DCE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3xqdgrlj.qdv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DCE1E60	CreateFileW
C:\Users\user\Documents\20220128	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DCEBEFF	CreateDirectoryW
C:\Users\user\Documents\20220128\PowerShell_transcript.141700.O7yUmft4.20220128220756.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DCE1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yehsm0ba.evc.ps1	success or wait	1	6DCE6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3xqdgrlj.qdv.psm1	success or wait	1	6DCE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yehsm0ba.evc.ps1	0	1	31	1	success or wait	1	6DCE1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3xqdgrlj.qdv.psm1	0	1	31	1	success or wait	1	6DCE1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.141700.O7yUmft4.20220128220756.txt	0	3	ff		success or wait	1	6DCE1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.141700.O7yUmft4.20220128220756.txt	3	717	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 38 32 32 30 37 35 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 31 34 31 37 30 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	**********Windows PowerShell transcript startStart time: 20220128220757Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 141700 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	30	6DCE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 fd 12 00 00 19 00 00 00 68 0d fd 03 fd 09 fd 09 fd 09 00 00 fd 00 fd 00 0e 00 49 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehI@	success or wait	1	6F1676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 42 00 00 00 0e 00 20 00	H<@^L"My:B	success or wait	16	6F1676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6F1676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6F1676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	00 08 00 03		success or wait	10	6F1676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 fd 01 40 00 3b 4d 40 01 fd 44 40 01 fd 44 40 01 55 00 40 00 40 4d 40 01 47 00 40 00 3c 4d 40 01 24 4d 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 38 4d 40 01 3f 4d 40 01 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 40 01 05 0e fd 00 fd 67 40 01 fd 01 40 00 fd 00 40 00 06 0e fd 00 04 0e fd 00 07 0e fd	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@@;M@D@D@U@@M@G@<M@$M@V@@@8M@?M@h8@g8@o@o@g@@@	success or wait	10	6F1676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EDD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EDD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EE75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6EE81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6EE8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EDD03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6DCE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EDD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EE75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6EE5D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6EE5D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6DCE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DCE1B4F	ReadFile

Analysis Process: conhost.exe PID: **5924**, Parent PID: **5872**

General

Target ID:	8
Start time:	22:07:55
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe PID: **348**, Parent PID: **7148**

General

Target ID:	9
Start time:	22:07:55
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Imagebase:	0x630000
File size:	868864 bytes
MD5 hash:	1165567A0B77F4C1BB44B4E89A6AB0C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.609602504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.609602504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.420145183.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.420145183.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000009.00000002.610934878.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.418715908.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.418715908.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.411345685.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.411345685.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.419685678.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.419685678.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EE9CF06	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	6EE9CF06	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DCE1B4F	ReadFile

Disassembly

No disassembly