ID: 562263
Sample Name: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Cookbook: default.jbs
Time: 17:36:05
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

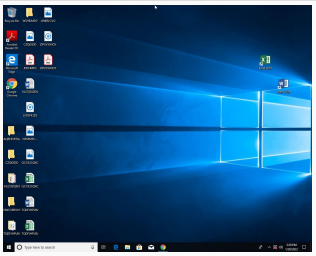
Windows Analysis Report

Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe

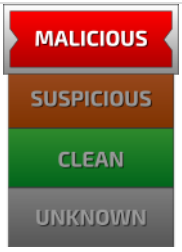
Overview

General Information

Sample Name:	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe
Analysis ID:	562263
MD5:	2c339718407688..
SHA1:	5e5bd0512a9435.
SHA256:	2ebfac5b21e3d1..
Tags:	exe
Infos:	



Detection



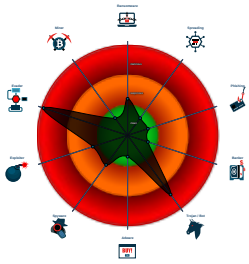
AgentTesla

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 …
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…

Classification



Process Tree

- **System is w10x64**
- Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe (PID: 6300 cmdline: "C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe" MD5: 2C33971840768888DEE0E3E714BC838DE)
  - powershell.exe (PID: 328 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: 2260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe (PID: 2548 cmdline: C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe MD5: 2C33971840768888DEE0E3E714BC838DE)
- **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
0000000D.00000000.337340320.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000000.337340320.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.343445103.0000000003371000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000D.00000002.530551824.0000000003301000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.530551824.0000000003301000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d38:$s1: get_kbok • 0x3166c:$s2: get_CHoo • 0x322c7:$s3: set_passwordIsSet • 0x30b3c:$s4: get_enableLog • 0x351e3:$s8: torbrowser • 0x33bbf:$s10: logins • 0x33537:$s11: credential • 0x2ff30:$g1: get_Clipboard • 0x2ff3e:$g2: get_Keyboard • 0x2ff4b:$g3: get_Password • 0x3151a:$g4: get_CtrlKeyDown • 0x3152a:$g5: get_ShiftKeyDown • 0x3153b:$g6: get_AltKeyDown
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
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)

.NET source code contains very large array initializations

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

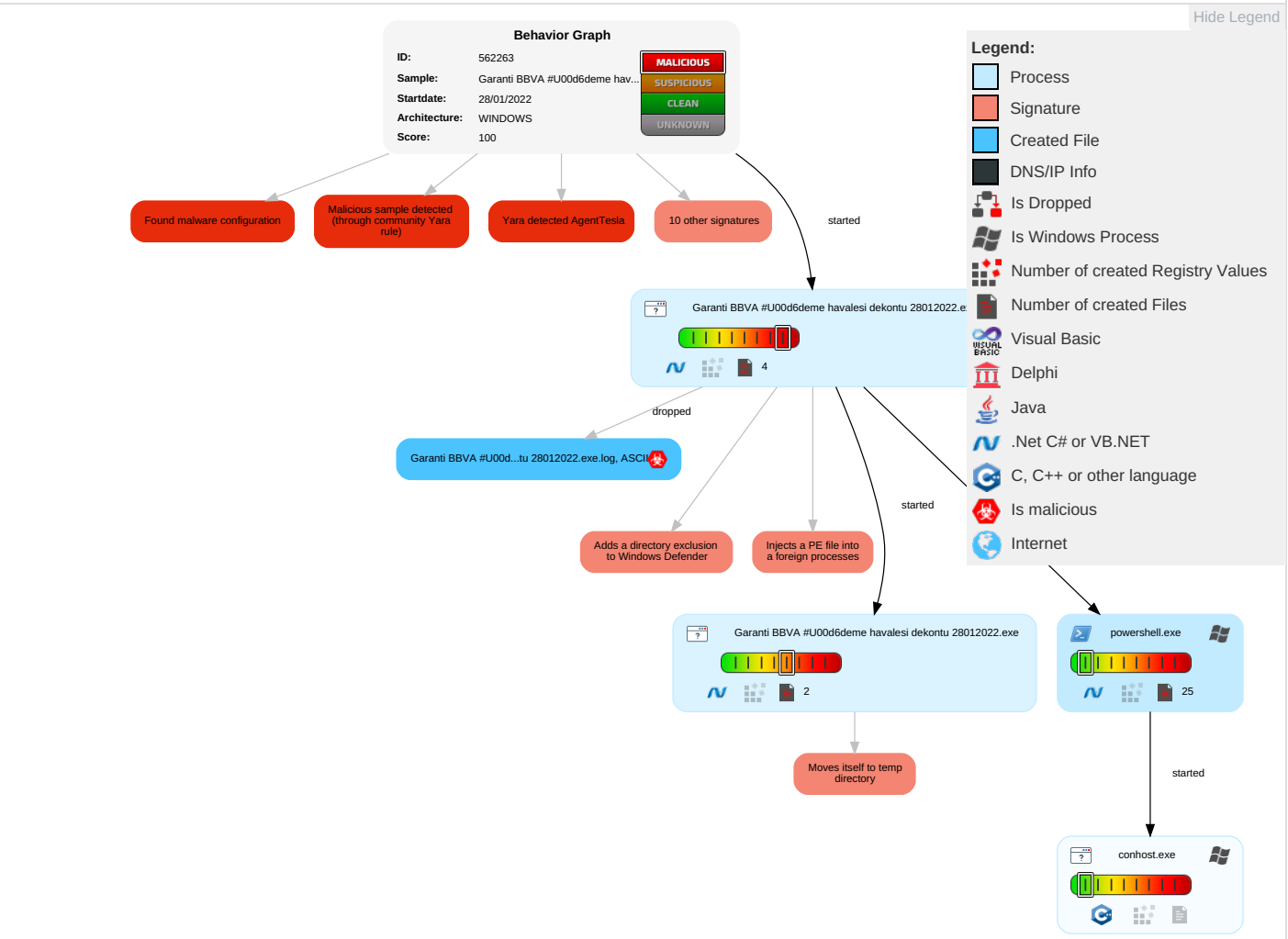
Yara detected AgentTesla

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	Path Interception	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	Boot or Logon Initialization Scripts	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	2 Obfuscated Files or Information	Cached Domain Credentials	1 Account 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 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 1 3 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

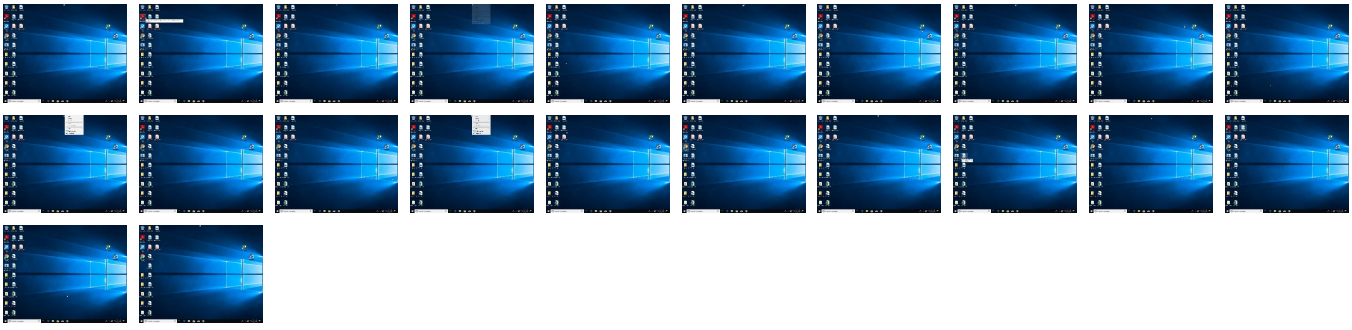
Behavior Graph



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
13.2.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdiafd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnP	0%	URL Reputation	safe	
http://www.sajatypeworks.comt#	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comtov	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/soft	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comrsiva.	0%	Avira URL Cloud	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-eT	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicd	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-p	0%	Avira URL Cloud	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.founder.com.cn/cnc	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.fontbureau.comC.TTF%	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	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://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdd	0%	Avira URL Cloud	safe	
http://www.fontbureau.commV	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sakkal.com0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/et	0%	Avira URL Cloud	safe	
http://jShurS.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comas2	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comsiva_	0%	Avira URL Cloud	safe	
http://www.sakkal.com-e	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://127.0.0.1:HTTP/1.1	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0000000D.00000002.5305518 24.0000000003301000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://blog.iandreev.com/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3434451 03.0000000003371000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdiafd	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3098067 46.0000000006227000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0002.348268546.0000000006220000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.310514871.0000000006227 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.311996097.0 000000006227000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .308414256.0000000006228000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.311201129.0000000006227000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.31173 5741.0000000006227000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnP	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2763117 24.0000000006228000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comt#	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2715647 86.000000000623B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.268854186.000000000623B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.279485450.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.277552930.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .271189293.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.276228975.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27333 4374.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.280327170.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.270078687.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .272232865.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.272420366.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27302 0901.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.269825249.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.275073345.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .271052691.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.273177047.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27988 3865.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.270459395.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.272711186.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .279286089.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.273535386.000000000623B000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comtov	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.292664608.000000000622D000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.292449695.000000000622C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/soft	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.279955937.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.282830027.000000000622D000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.282269637.000000000622D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comrsiva.	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.309806746.0000000006227000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348268546.0000000006220000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.310514871.0000000006227000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.311996097.0000000006227000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.311201129.0000000006227000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.311735741.0000000006227000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.308414256.0000000006228000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.c	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.276486970.0000000006227000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2715647 86.000000000623B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0002.348604717.0000000007432000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.268854186.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.279485450.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .277552930.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.271189293.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27622 8975.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.273334374.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.280327170.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .270078687.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.272232865.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27242 0366.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.273020901.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.269825249.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .275073345.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.271052691.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27317 7047.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.279883865.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.270459395.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .272711186.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.279286089.000000000623B000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/_	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2828300 27.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.282269637.000000000622D000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnu-eT	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2764869 70.0000000006227000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comR	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2715647 86.000000000623B000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.279485450.000000000623B000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.277552930.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.271189293.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .276228975.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.273334374.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.28032 7170.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.270078687.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.272232865.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .272420366.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.273020901.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.26982 5249.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.275073345.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.271052691.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .273177047.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.279883865.000000000623B000. 00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.27045 9395.000000000623B000.00000004.00000800. 00020000.00000000.sdmp, Garanti BBVA #U0 0d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.272711186.000000000623B 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.279286089.0 00000000623B000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .273535386.000000000623B000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.278035944.000000000623B000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comlicd	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.293615006.000000000622C000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.293966007.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.293966007.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.343445103.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.344823402.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.271564786.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.279485450.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.277552930.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.271189293.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.276228975.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.273334374.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.280327170.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.270078687.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.272232865.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.272420366.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.273020901.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.269825249.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.275073345.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.271052691.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.273177047.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.279883865.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.270459395.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.272711186.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.279286089.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.273535386.000000000623B000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.278035944.000000000623B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.348604717.0000000007432000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl-p	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.276486970.0000000006227000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
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, 00000000.00000002.3462634 28.0000000004379000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0000000D.0000 0000.337340320.0000000000402000.00000040 .00000400.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 000000D.00000000.335963128.0000000000402 000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnc	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2764869 70.0000000006227000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.276311724.0000000006228000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.278134300.0000000006227000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.277869805.0000000006227 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.292664608.000000000622D000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.293615006.000000000622C 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.292449695.0 00000000622C000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .293966007.000000000622E000.00000004.000 00800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0000000D.00000002.5305518 24.0000000003301000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/V	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2828300 27.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.282269637.000000000622D000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comC.TTF%	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.292449695.000000000622C000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comcomd	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2936150 06.000000000622C000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.293966007.000000000622E000.00000004 .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%tordir%%ha	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0000000D.00000002.5305518 24.0000000003301000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://blog.iandreev.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3434451 03.0000000003371000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdd	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2936150 06.000000000622C000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.293966007.000000000622E000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commV	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.292449695.000000000622C000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.sakkal.com0	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2829234 61.0000000006254000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.282588224.0000000006254000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.282379029.0000000006254 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.282181716.0 000000006254000.00000004.00000800.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2764869 70.0000000006227000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.276311724.0000000006228000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn0	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2760557 21.0000000006227000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/et	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2828300 27.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.282269637.000000000622D000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://jShurS.com	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0000000D.00000002.5305518 24.0000000003301000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comas2	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.292449695.000000000622C000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comm	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.3098067 46.0000000006227000.00000004.00000800.00 020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.0000 0003.310514871.0000000006227000.00000004 .00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 0 0000000.00000003.311996097.0000000006227 000.00000004.00000800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 280 12022.exe, 00000000.00000003.308414256.0 000000006228000.00000004.00000800.000200 00.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003 .311201129.0000000006227000.00000004.000 00800.00020000.00000000.sdmp, Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000 000.00000003.311735741.0000000006227000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2822696 37.000000000622D000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000002.3486047 17.0000000007432000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.comsiva_	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2926646 08.000000000622D000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sakkal.com-e	Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe, 00000000.00000003.2821817 16.0000000006254000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562263
Start date:	28.01.2022
Start time:	17:36:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
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:	24
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: 1.2% (good quality ratio 0.8%) • Quality average: 47.2% • Quality standard deviation: 41.6%
HCA Information:	• Successful, ratio: 98% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, tile-service.weather.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:37:35	API Interceptor	165x Sleep call for process: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe modified
17:37:46	API Interceptor	41x 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):	20676
Entropy (8bit):	5.57787470347618
Encrypted:	false
SSDEEP:	384:wtADhL7CY/jB0vtEcSBKnyjultI0P7Y9gZSJ3xGT1MaXZlXzoClds:N96X4KyCltzrZcMC+fj0
MD5:	7419206D84E33AAA50B66810433BE492
SHA1:	FCD18BC7BC1E8C9B353AD7C01476A280CD6965DA
SHA-256:	CEB337FBC74732F5C379AA7B79C7B7B9F2BBAFD40054A213F2ACEEB006903745
SHA-512:	BEF77C9915074054466E38389875155301E777C83345D38D456B1F0E4153C1D78C06827D12DF4D00C613DF47A367712CE805F529FF13B39CC9FA87570DA8B48E
Malicious:	false
Reputation:	low
Preview:	@...e.....h...s.m.j.....'.J.....@.....H.....<@.^.L."My...:A..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)y.....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_afrgsmzg.efd.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ef3bdb0d.hja.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\Documents\20220128\PowerShell_transcript.284992.nE+e2qXd.20220128173744.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):	3585
Entropy (8bit):	5.331900359212821
Encrypted:	false
SSDEEP:	96:BZJ/UN0oqDo1Zak2Zk/UN0oqDo1Z+FqaZ60cZ60cZ60pZO:PIIN
MD5:	692DA316572CC9D05E3F562D1D346546
SHA1:	168DFAFE4B0B23ADF8CDC1DD9CB1ECF7920E9551
SHA-256:	051D4A4C028DFD179F704C4EDBAAE759B84C26650A2F8BC9933023EF04DEBD9C
SHA-512:	15E7A1BE43F16C5C49645583914A6208C2A1D7030569C09D39EDA083ACC6E87FB2497D3D2D2DCBBB97B6004DB59968802F7F26050C470D074F8BCD9E8A31522
Malicious:	false
Reputation:	low
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220128173746..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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: 328..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: 20220128173746..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe..**********..Command start time: 20220128174112..**********..PS>Te

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.587303622326669
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:	864256
MD5:	2c3397184076888dee0e3e714bc838de
SHA1:	5e5bd0512a943596b3563bc6bb2cf4825beb8a80
SHA256:	2ebfac5b21e3d11f6ae3418af09ec1f5762f464a5b2c2d110cd918ae5b87ad3c
SHA512:	1601afe74b45456858fa3128691c8e39b915432ef358c65b240254bb677d3cecadb80115562a375566e5783c813de1828749ec5bb10037ee03793420930eee65
SSDEEP:	12288:/PJB4o9nX9XQe+EPxm9+gKRifBMXArb+L+di7hyLEFQoMo2OPjnf:8o1X9gHEPxi6iiwf+J4Ltoh2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....".....A... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d41ae
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:	0x61F3FEC7 [Fri Jan 28 14:33:43 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4160	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x5e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd410f	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	0xd21b4	0xd2200	False	0.519227998587	data	6.59256485172	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xd6000	0x1e8	0x200	False	0.861328125	data	6.60667397067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x5e0	0x600	False	0.429036458333	data	4.15516730092	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	0x354	data		
RT_MANIFEST	0xd83f4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

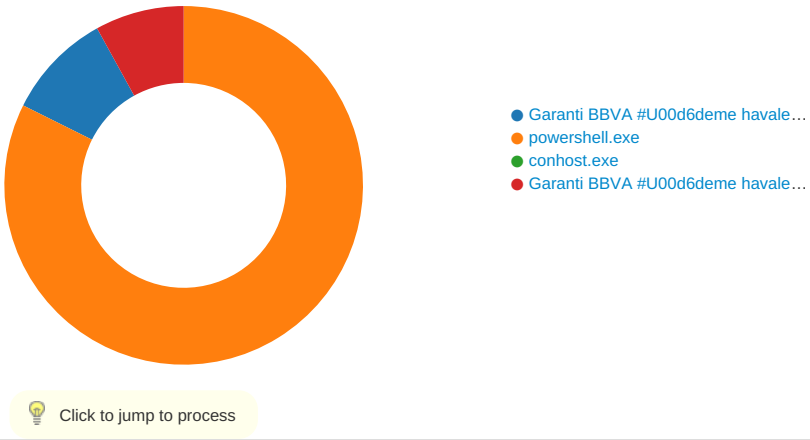
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	IDeserializationCallba.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	IDeserializationCallba.exe

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe PID: 6300, Parent PID: 5532

General

Target ID:	0
Start time:	17:37:10
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:	0xf60000
File size:	864256 bytes
MD5 hash:	2C3397184076888DEE0E3E714BC838DE
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: 00000000.00000002.343445103.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.346263428.0000000004379000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.346263428.0000000004379000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.344823402.00000000034BF000.00000004.00000800.00020000.00000000.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	6EA6CF06	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	6EA6CF06	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	6ED7C78D	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	6ED7C907	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	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile

Analysis Process: powershell.exe PID: 328, Parent PID: 6300

General

Target ID:	11
Start time:	17:37:43
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:	0x290000
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	6EA6CF06	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	6EA6CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afrgsmzg.efd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ef3bdb0d.hja.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B1E60	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	6D8BBEFF	CreateDirectoryW
C:\Users\user\Documents\20220128\PowerShell_transcript.284992.nE+e2qXd.20220128173744.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afrgsmzg.efd.ps1	success or wait	1	6D8B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ef3bdb0d.hja.psm1	success or wait	1	6D8B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afrgsmzg.efd.ps1	0	1	31	1	success or wait	1	6D8B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ef3bdb0d.hja.psm1	0	1	31	1	success or wait	1	6D8B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220128\PowerShell_transcript.284992.nE+e2qXd.20220128173744.txt	0	3	ff		success or wait	1	6D8B1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.284992.nE+e2qXd.20220128173744.txt	3	710	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 31 37 33 37 34 36 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 61 6c 66 6f 6e 73 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 61 6c 66 6f 6e 73 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 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220128173746Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 284992 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	30	6D8B1B4F	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 00 13 00 00 18 00 00 00 68 0d fd 04 73 08 6d 08 6a 08 00 00 fd 00 1d 02 27 00 4a 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehsmj'J@	success or wait	1	6ED376FC	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 41 00 00 00 0e 00 20 00	H<@^L"My:A	success or wait	16	6ED376FC	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	6ED376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6ED376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	00 08 00 03		success or wait	10	6ED376FC	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 55 00 40 00 47 00 40 00 54 01 40 00 fd 3e 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 fd 67 40 01 48 01 40 00 58 01 40 00 fd 01 40 00 fd 00 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40	U@G@T@>@V@@@@V@g@H@X@@@[@NT@HT @S@S@hT@S@S@S@\@T@T@@X@? X@T@S@ S@T@T@xT@zT@T@= M@DM@:M@"M@ M@! M@;M@D@D@@M@< M@$M@8M@? M@BM@D@m E@EM@q@q@S@%@n@	success or wait	10	6ED376FC	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	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EA4CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA4CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EA45705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6EA51F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6EA5203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E9A03DE	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	6D8B1B4F	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	6D8B1B4F	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	6D8B1B4F	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	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	106	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D8B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D8B1B4F	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	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D8B1B4F	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	6EA2D72F	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	6EA2D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D8B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D8B1B4F	ReadFile

Analysis Process: conhost.exe PID: **2260**, Parent PID: **328**

General

Target ID:	12
Start time:	17:37:43
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: **2548**, Parent PID: **6300**

General

Target ID:	13
Start time:	17:37:43
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:	0xf00000
File size:	864256 bytes
MD5 hash:	2C3397184076888DEE0E3E714BC838DE
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: 0000000D.00000000.337340320.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.337340320.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.530551824.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.530551824.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 0000000D.00000002.530551824.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.335963128.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.335963128.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.527928094.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.527928094.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.336711210.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.336711210.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.337809734.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.337809734.0000000000402000.00000040.00000400.00020000.00000000.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	6EA6CF06	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	6EA6CF06	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Garanti BBVA #U00d6deme havalesi dekontu 28012022.exe	C:\Users\user\AppData\Local\Temp\tmpG722.tmp	success or wait	1	652BD9A	MoveFileExW

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	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D8B1B4F	ReadFile

Disassembly

No disassembly