ID: 383998
Sample Name: Szallitasi adatok.tar
Cookbook: default.jbs
Time: 13:53:46
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

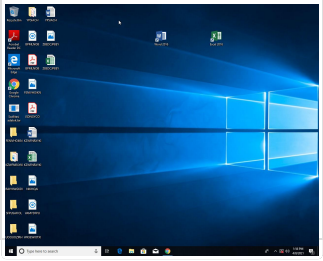
Analysis Report Szallitasi adatok.tar

Overview

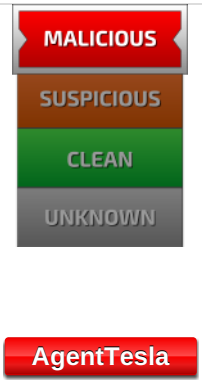
General Information

Sample Name:	Szallitasi adatok.tar
Analysis ID:	383998
MD5:	fa2c7acf057d7ec...
SHA1:	b67cd39674b6d0..
SHA256:	1b90e29a9f49905.
Infos:	

Most interesting Screenshot:



Detection

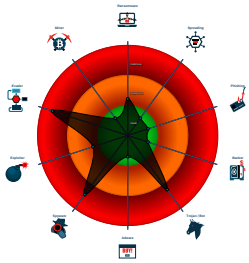


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp...
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg...
- Injects a PE file into a foreign proce...
- Machine Learning detection for dropp...
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...
- Tries to detect sandboxes and other...
- Tries to harvest and steal Putty / Wi...
- Tries to harvest and steal browser in...

Classification



Startup

- **System is w10x64**
- unarchiver.exe (PID: 6880 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\Szallitasi adatok.tar' MD5: DB55139D9DD29F24AE8EA8F0E5606901)
  - 7za.exe (PID: 6916 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s' 'C:\Users\user\Desktop\Szallitasi adatok.tar' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7008 cmdline: 'cmd.exe' /C 'C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Szallitasi adatok.exe (PID: 7056 cmdline: C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe MD5: C615C5F811E05D5743CE4DD4AFAD4055)
      - Szallitasi adatok.exe (PID: 7104 cmdline: C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe MD5: C615C5F811E05D5743CE4DD4AFAD4055)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "torremolinos3@copiplus.esvB&6mnT00r3mol2o17smtp.1and1.es"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.590323403.000000000348 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.590323403.000000000348 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000007.00000002.586946181.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.344267324.0000000003FF 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.343156984.0000000002E0 3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

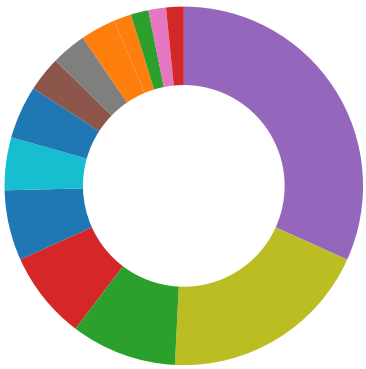
Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.Szallitasi adatok.exe.4086228.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Szallitasi adatok.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.Szallitasi adatok.exe.4086228.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.Szallitasi adatok.exe.4015208.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

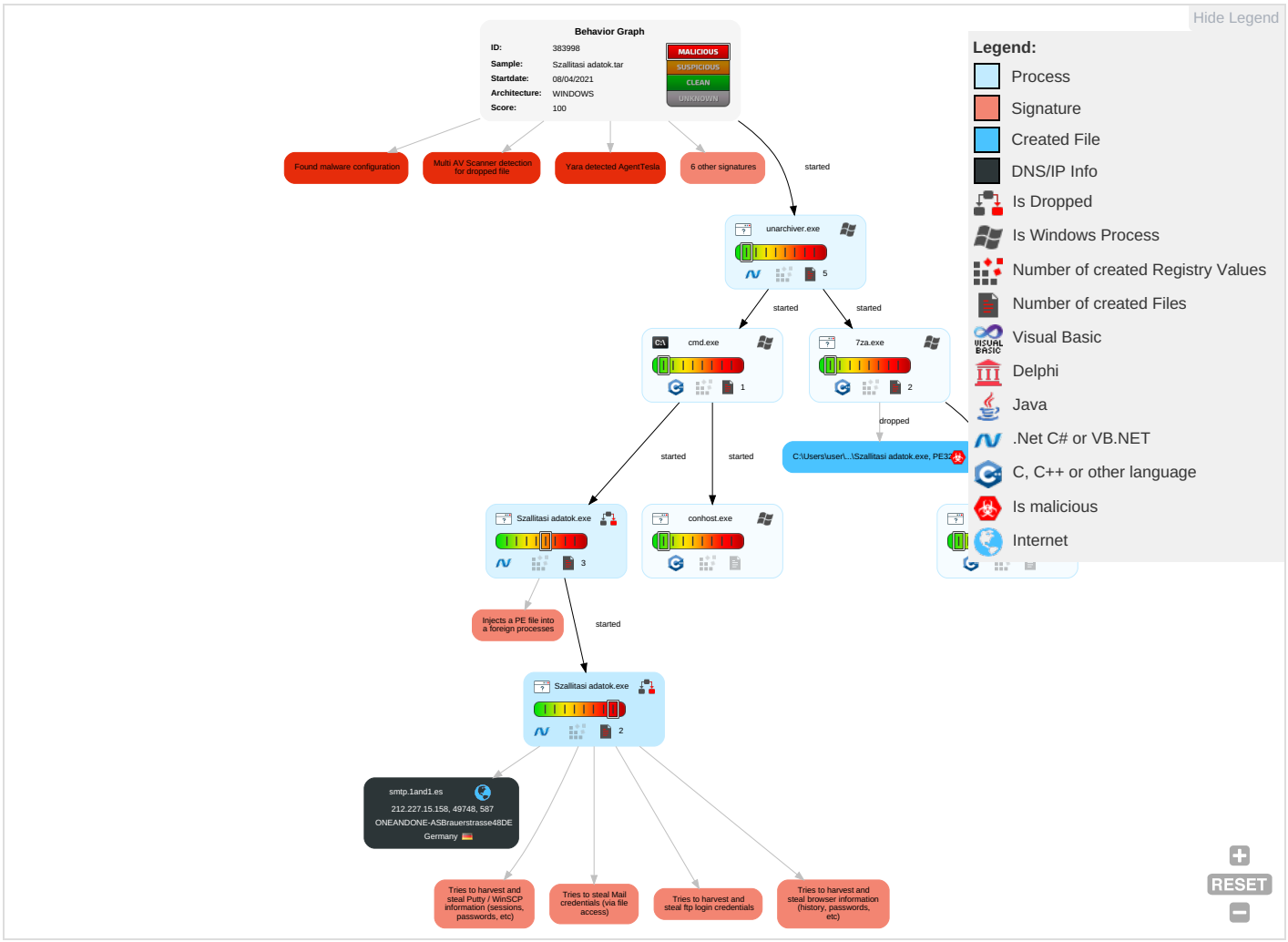
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 3 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

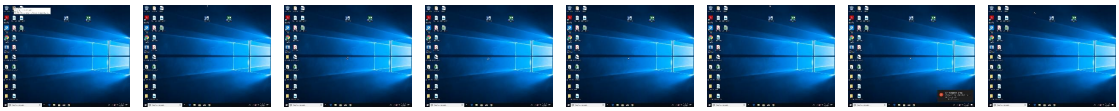
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe	19%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Szallitasi adatok.exe.400000.0.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://www.carterandcone.comn-u	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://CpKupV.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.goodfont.co.kr-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/J	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna-e	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.comasc	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr.krt-b	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	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://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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.fontbureau.comaJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.urwpp.derT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/nb-n	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cna	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://wjANZKRbswl5oYyv5U.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.1and1.es	212.227.15.158	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Szallitasi adatok.exe, 0000000 7.00000002.590323403.000000000 3481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Szallitasi adatok.exe, 0000000 6.00000002.347842702.000000000 7042000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comn-u	Szallitasi adatok.exe, 0000000 6.00000003.328833893.000000000 5E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Szallitasi adatok.exe, 0000000 6.00000002.347842702.000000000 7042000.00000004.00000001.sdmp	false		high
http://CpKupV.com	Szallitasi adatok.exe, 0000000 7.00000002.590323403.000000000 3481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr-e	Szallitasi adatok.exe, 00000006.00000003.328148680.000000005E5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	Szallitasi adatok.exe, Szallitasi adatok.exe, 00000007.00000000.340920875.0000000000F82000.00000002.00020000.sdmp, Szallitasi adatok.tar	false		high
http://www.jiyu-kobo.co.jp/jp/J	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersC	Szallitasi adatok.exe, 00000006.00000003.330822847.000000005E62000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cna-e	Szallitasi adatok.exe, 00000006.00000003.328398898.000000005E5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	Szallitasi adatok.exe, 00000006.00000002.343156984.000000002E03000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000003.334203954.0000000005E62000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Szallitasi adatok.exe, 00000006.00000003.328148680.000000005E5D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Szallitasi adatok.exe, 00000006.00000003.329128388.000000005E61000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000003.328833893.0000000005E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	Szallitasi adatok.exe, 00000006.00000003.330822847.000000005E62000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Szallitasi adatok.exe, 00000006.00000002.343156984.000000002E03000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000003.329810137.0000000005E3A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	Szallitasi adatok.exe, Szallitasi adatok.tar	false		high
http://www.fonts.com	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Szallitasi adatok.exe, 00000006.00000003.328148680.000000005E5D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	Szallitasi adatok.exe, 00000006.00000003.331404258.000000005E62000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Szallitasi adatok.exe, 00000006.00000002.343156984.000000002E03000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000002.343135328.0000000002DF1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Szallitasi adatok.exe, 00000006.00000003.329984191.000000005E62000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Szallitasi adatok.exe, 00000006.00000002.344267324.000000003FF6000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000007.00000002.586946181.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comasc	Szallitasi adatok.exe, 00000006.00000003.341878900.000000005E3A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr.krt-b	Szallitasi adatok.exe, 00000006.00000003.328148680.000000005E5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	Szallitasi adatok.exe, 00000007.00000002.590323403.000000003481000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/U	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comslnt	Szallitasi adatok.exe, 00000006.00000003.329144440.000000005E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • 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	Szallitasi adatok.exe, 00000007.00000002.590323403.000000003481000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.1and1.es	Szallitasi adatok.exe, 00000007.00000002.592552943.000000003 7DC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers~	Szallitasi adatok.exe, 00000006.00000003.331212623.000000005E62000.00000004.00000001.sdmp	false		high
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	Szallitasi adatok.exe, Szallitasi adatok.exe, 00000007.00000000.340920875.0000000000F82000.00000002.00020000.sdmp, Szallitasi adatok.tar	false		high
http://www.carterandcone.comr	Szallitasi adatok.exe, 00000006.00000003.329128388.000000005E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/C	Szallitasi adatok.exe, 00000006.00000003.329810137.000000005E3A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comaJ	Szallitasi adatok.exe, 00000006.00000003.341878900.000000005E3A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000003.329810137.0000000005E3A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.derT	Szallitasi adatok.exe, 00000006.00000003.331404258.000000005E62000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/nb-n	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Szallitasi adatok.exe, 00000006.00000003.330983935.000000005E62000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000002.347842702.0000000007042000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cna	Szallitasi adatok.exe, 00000006.00000003.328730706.000000005E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	Szallitasi adatok.exe, 00000006.00000003.333277327.000000005E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://wjANZKRbswl5oYyv5U.com	Szallitasi adatok.exe, 00000007.00000002.590323403.000000003481000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000007.00000003.544547709.00000000015E4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Szallitasi adatok.exe, 00000006.00000003.329656338.000000005E37000.00000004.00000001.sdmp, Szallitasi adatok.exe, 00000006.00000003.329458297.0000000005E34000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n	Szallitasi adatok.exe, 00000006.00000003.329810137.000000005E3A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comn-u0	Szallitasi adatok.exe, 00000006.00000003.329128388.000000005E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Szallitasi adatok.exe, 00000006.00000002.347842702.000000007042000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/i	Szallitasi adatok.exe, 00000006.00000003.330590528.000000005E62000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com.N	Szallitasi adatok.exe, 00000006.00000003.328759345.000000005E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Szallitasi adatok.exe, 00000006.00000003.330798629.000000005E62000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.227.15.158	smtp.1and1.es	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383998
Start date:	08.04.2021
Start time:	13:53:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Szallitasi adatok.tar
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:	27
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.spyw.evad.winTAR@11/4@1/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0%) • Quality average: 14% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .tar
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 20.82.210.154, 13.64.90.137, 23.10.249.43, 23.10.249.26, 52.155.217.156, 20.54.26.129, 104.43.139.144, 104.42.151.234, 52.255.188.83, 95.100.54.203 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
13:54:41	API Interceptor	778x Sleep call for process: Szallitasi adatok.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.227.15.158	Recibo de transferencia de dinero.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Geldtransferbeleg.exe	Get hash	malicious	Browse	
	Factur#U0103 pl#U0103tit#U0103.exe	Get hash	malicious	Browse	
	JUSTT1.exe	Get hash	malicious	Browse	
	Facturas pagadas.exe	Get hash	malicious	Browse	
	kjhh087.exe	Get hash	malicious	Browse	
	Facturas pagadas.exe	Get hash	malicious	Browse	
	Facturas_pagadas.exe	Get hash	malicious	Browse	
	PAG00.exe	Get hash	malicious	Browse	
	312000123.exe	Get hash	malicious	Browse	
	TRANF1.exe	Get hash	malicious	Browse	
	Orden de pago.exe	Get hash	malicious	Browse	
	Orden de pago.exe	Get hash	malicious	Browse	
	OrdenPago2.exe	Get hash	malicious	Browse	
	3d#U044f.exe	Get hash	malicious	Browse	
	Orden de pago.exe	Get hash	malicious	Browse	
	Orden de pago.exe	Get hash	malicious	Browse	
	PAP001.exe	Get hash	malicious	Browse	
	Fizetesi felszolitas.exe	Get hash	malicious	Browse	
	P0.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.1and1.es	Recibo de transferencia de dinero.exe	Get hash	malicious	Browse	• 212.227.15.158
	Geldtransferbeleg.exe	Get hash	malicious	Browse	• 212.227.15.158
	Factur#U0103 pl#U0103tit#U0103.exe	Get hash	malicious	Browse	• 212.227.15.158
	factura.exe	Get hash	malicious	Browse	• 212.227.15.142
	JUSTT1.exe	Get hash	malicious	Browse	• 212.227.15.158
	Facturas pagadas.exe	Get hash	malicious	Browse	• 212.227.15.158
	kjhh087.exe	Get hash	malicious	Browse	• 212.227.15.158
	Facturas pagadas.exe	Get hash	malicious	Browse	• 212.227.15.142
	Facturas pagadas.exe	Get hash	malicious	Browse	• 212.227.15.158
	Facturas_pagadas.exe	Get hash	malicious	Browse	• 212.227.15.158
	#U0420#U0430#U0445#U0443#U043d#U043a#U0438 #U043e#U043f#U043b#U0430#U0447#U0435#U043d#U0456.exe	Get hash	malicious	Browse	• 212.227.15.142
	PAG00.exe	Get hash	malicious	Browse	• 212.227.15.158
	312000123.exe	Get hash	malicious	Browse	• 212.227.15.158
	Facturi pl#U0103tite la scaden#U021b#U0103.exe	Get hash	malicious	Browse	• 212.227.15.142
	TRANF1.exe	Get hash	malicious	Browse	• 212.227.15.158
	Betalingsadvies Opmerking.exe	Get hash	malicious	Browse	• 212.227.15.142
	42#U0438.exe	Get hash	malicious	Browse	• 212.227.15.142
	WYX-09901.exe	Get hash	malicious	Browse	• 212.227.15.142
	Nota de aviso de pago.exe	Get hash	malicious	Browse	• 212.227.15.142
	Ordesss.exe	Get hash	malicious	Browse	• 212.227.15.142

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	mal5.exe	Get hash	malicious	Browse	• 74.208.5.15
	invoice.exe	Get hash	malicious	Browse	• 74.208.236.64
	PO7321.exe	Get hash	malicious	Browse	• 217.160.0.101
	BL01345678053567.exe	Get hash	malicious	Browse	• 74.208.236.134
	A409043090.exe	Get hash	malicious	Browse	• 74.208.5.2
	Old9BZy7jO.dll	Get hash	malicious	Browse	• 82.223.21.211
	mULT14gGmy.dll	Get hash	malicious	Browse	• 82.223.21.211
	yWA1Ay0538.dll	Get hash	malicious	Browse	• 82.223.21.211
	27XuTqKwYF.dll	Get hash	malicious	Browse	• 82.223.21.211
	Old9BZy7jO.dll	Get hash	malicious	Browse	• 82.223.21.211
	mULT14gGmy.dll	Get hash	malicious	Browse	• 82.223.21.211
	JI63JG7EMo.dll	Get hash	malicious	Browse	• 82.223.21.211
	F7aZDNx6UM.dll	Get hash	malicious	Browse	• 82.223.21.211
	yWA1Ay0538.dll	Get hash	malicious	Browse	• 82.223.21.211
	27XuTqKwYF.dll	Get hash	malicious	Browse	• 82.223.21.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NYDhNBQlYM.dll	Get hash	malicious	Browse	• 82.223.21.211
	ydKCqL4sTG.dll	Get hash	malicious	Browse	• 82.223.21.211
	F7aZDNx6UM.dll	Get hash	malicious	Browse	• 82.223.21.211
	JI63JG7EMo.dll	Get hash	malicious	Browse	• 82.223.21.211
	TI8E08zJuu.dll	Get hash	malicious	Browse	• 82.223.21.211

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.2529463157768355
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk7v:MLF20NaL329hJ5g522r0
MD5:	FF3B761A021930205BEC9D7664AE9258
SHA1:	1039D595C6333358D5F7EE5619FE6794E6F5FDB1
SHA-256:	A3517BC4B1E6470905F9A38466318B302186496E8706F1976F1ED76F3E87AF0F
SHA-512:	1E77D09CF965575EF9800B1EE8947A02D98F88DBFA267300330860757A0C7350AF857A2CB7001C49AFF1F5BD1E0AE6E90F643B27054522CADC730DD14BC3DE1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Szallitasi adatok.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1615
Entropy (8bit):	5.10186681558097

C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	
Encrypted:	false
SSDEEP:	48:CZVvUG/G3/Gb3/G3/Gpp/G//G3/GpPv/Gb1/Gcv/GP/Gu/GO/Ge/G3/G4/G3/G2a:UzBUQ
MD5:	C4B67CF81A0C227827D36C996CC306DD
SHA1:	9D9E9E32BEFB33BB6B99BF76D54960A7A9E4B8EB
SHA-256:	3027A6AE557DCC0ACC8C324F766CA3E4FC0BC463799EB8D3AA96484988BC882B
SHA-512:	560D400BEB0DDD24875233192A1E50356C96EBE2D8C4993DB0BF1530E73EA570E69B6883CDC155C4996E211E9390CBC358149F069D77B97BFAAF8D6C7972FD6
Malicious:	false
Reputation:	low
Preview:	04/08/2021 1:54 PM: Unpack: C:\Users\user\Desktop\Szallitasi adatok.tar..04/08/2021 1:54 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s..04/08/2021 1:54 PM: Received from standard out: ..04/08/2021 1:54 PM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..04/08/2021 1:54 PM: Received from standard out: ..04/08/2021 1:54 PM: Received from standard out: Scanning the drive for archives:..04/08/2021 1:54 PM: Received from standard out: 1 file, 874496 bytes (854 KiB)..04/08/2021 1:54 PM: Received from standard out: ..04/08/2021 1:54 PM: Received from standard out: Extracting archive: C:\Users\user\Desktop\Szallitasi adatok.tar..04/08/2021 1:54 PM: Received from standard out: --..04/08/2021 1:54 PM: Received from standard out: Path = C:\Users\user\Desktop\Szallitasi adatok.tar..04/08/2021 1:54 PM: Received from standard out: Type = tar..04/08/2021 1:54 PM: Received from standard out: Physical Size = 874496..04/08/20

C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	872960
Entropy (8bit):	7.186249660947472
Encrypted:	false
SSDEEP:	12288:2RWcIIK2eESLm1OYOtc7t/0t5v3QUynop8O1lDGbT1tB5IKUa/+:20/IVlOYOSUXynof1wt/IE
MD5:	C615C5F811E05D5743CE4DD4AFAD4055
SHA1:	D37B5D2BCCC12CC995B08A9D3200ECF3A7C21D37
SHA-256:	2154D40FF4FC639A9F8CE0208D0F71D75D664FFAF1D92DC6802CE9EE1DC76DB2
SHA-512:	13C828E61E7E9E12096781F4D0567EA402B42E9E01CF6B5B0CAD2A7749B9B4664A23D3F181E398FAB73D4AAB9AE1BD867868D4651636620CACE3F8E30438B6D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n`.....P.....F.....)... ...@....@.. .....@.....)..O....@...B..... ..... ..H.....text..... ..... ..`.rsrc....B...@...D.....@..@.relo c.....P.....@..B.....).....H.....?..DH.....0.....(....(.....(.....o!....*.....("....(#.....($.....(%.....(&....*N..(....ol... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~..... (3.....,lr...p.....(4...o5...s6.....~.....+..*.0.....

Static File Info

General

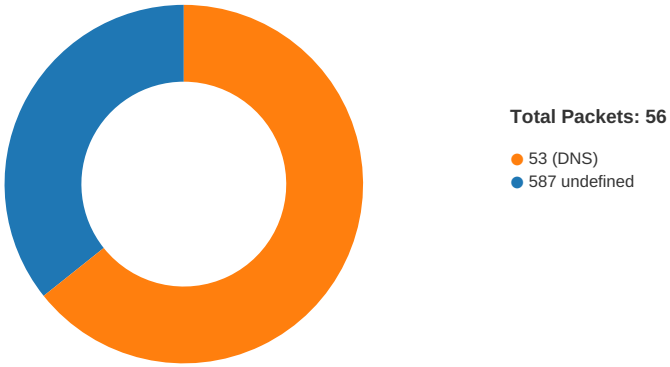
File type:	tar archive
Entropy (8bit):	7.17922383389497
TrID:	
File name:	Szallitasi adatok.tar
File size:	874496
MD5:	fa2c7acf057d7ecf693cbb13fab9b1b3
SHA1:	b67cd39674b6d039e235fbb9cf0272a103afa475
SHA256:	1b90e29a9f49905ead7832ff25d7ba91fddeb4827d7c8ca506c6c0b6f96acda7
SHA512:	c0db03c358d2e99f1a801c7fdb7a7155fadca26ac43d0cb76636d2d3962494aedf4cabc6611530138ab67ba40119421ea275c840c2c7a18fc803125a3ca5e981
SSDEEP:	12288:iRWcIIK2eESLm1OYOtc7t/0t5v3QUynop8O1lDGbT1tB5IKUa/+:i0/IVlOYOSUXynof1wt/IE
File Content Preview:	Szallitasi adatok.exe.....0000755.0000000.0000000.00003251000.14033527302.0010636.0.....

File Icon

Icon Hash:	00828e8e8686b000

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:56:24.634834051 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.655982018 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.656105995 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.680350065 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.680680037 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.700917959 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.700939894 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.701294899 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.721739054 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.763144016 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.854901075 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.877895117 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.877954006 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.877990961 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.878241062 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.882872105 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:24.903430939 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:24.945874929 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.274348021 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.294574022 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.307136059 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.327366114 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.328071117 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.354927063 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.357798100 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.391242981 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.391863108 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.415335894 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.418555021 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.439104080 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.447356939 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.447470903 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.450865984 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.450938940 CEST	49748	587	192.168.2.6	212.227.15.158
Apr 8, 2021 13:56:25.467780113 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.471020937 CEST	587	49748	212.227.15.158	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:56:25.475791931 CEST	587	49748	212.227.15.158	192.168.2.6
Apr 8, 2021 13:56:25.527986050 CEST	49748	587	192.168.2.6	212.227.15.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:54:29.310831070 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:54:29.323438883 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 8, 2021 13:54:30.150109053 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:54:30.162914991 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 8, 2021 13:54:58.056195021 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:54:58.068922043 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:00.362915993 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:00.375672102 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:01.744673014 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:01.764659882 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:15.327439070 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:15.339849949 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:16.030726910 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:16.044173956 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:16.076661110 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:16.090249062 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:16.503767014 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:16.516599894 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:16.855788946 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:16.869081020 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:17.018145084 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:17.046446085 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:17.291961908 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:17.304398060 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:17.742532969 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:17.756438971 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:17.772445917 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:17.791837931 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:18.222578049 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:18.235402107 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:18.547561884 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:18.560071945 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:19.110074997 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:19.123141050 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:20.157962084 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:20.170722961 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:20.609410048 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:20.621942043 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:24.486260891 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:24.498848915 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:25.246932983 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:25.259480000 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:26.208298922 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:26.221723080 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:27.153976917 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:27.167279959 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:31.936496019 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:31.948426962 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:33.254976988 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:33.281289101 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:35.488033056 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:35.501447916 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:45.156191111 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:45.168934107 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:46.059092999 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:46.072094917 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:48.830485106 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:48.842998981 CEST	53	51818	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:52.643460035 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:52.656511068 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:53.470834970 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:53.484002113 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 8, 2021 13:55:54.145735025 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:55:54.158551931 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 8, 2021 13:56:06.882749081 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:56:06.895538092 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 8, 2021 13:56:07.708811045 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:56:07.727602005 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 8, 2021 13:56:08.603001118 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:56:08.635907888 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 8, 2021 13:56:24.476588964 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 8, 2021 13:56:24.499018908 CEST	53	56129	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:56:24.476588964 CEST	192.168.2.6	8.8.8.8	0xb5a0	Standard query (0)	smtp.1and1.es	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:56:24.499018908 CEST	8.8.8.8	192.168.2.6	0xb5a0	No error (0)	smtp.1and1.es		212.227.15.158	A (IP address)	IN (0x0001)
Apr 8, 2021 13:56:24.499018908 CEST	8.8.8.8	192.168.2.6	0xb5a0	No error (0)	smtp.1and1.es		212.227.15.142	A (IP address)	IN (0x0001)

SMTP Packets

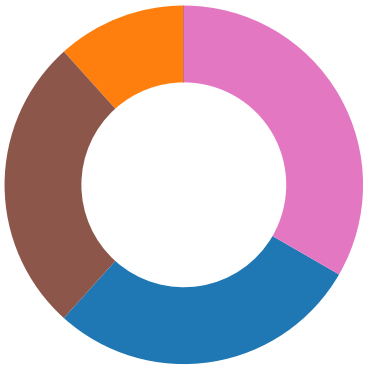
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:56:24.680350065 CEST	587	49748	212.227.15.158	192.168.2.6	220 kundenserver.de (mreue109) Nemesis ESMTP Service ready
Apr 8, 2021 13:56:24.680680037 CEST	49748	587	192.168.2.6	212.227.15.158	EHLO 899552
Apr 8, 2021 13:56:24.700939894 CEST	587	49748	212.227.15.158	192.168.2.6	250-kundenserver.de Hello 899552 [185.32.222.8] 250-8BITMIME 250-AUTH LOGIN PLAIN 250-SIZE 140000000 250 STARTTLS
Apr 8, 2021 13:56:24.701294899 CEST	49748	587	192.168.2.6	212.227.15.158	STARTTLS
Apr 8, 2021 13:56:24.721739054 CEST	587	49748	212.227.15.158	192.168.2.6	220 OK

Code Manipulations

Statistics

Behavior

- unarchiver.exe
- 7za.exe
- conhost.exe
- cmd.exe
- conhost.exe
- Szallitasi adatok.exe
- Szallitasi adatok.exe



Click to jump to process

System Behavior

Analysis Process: unarchiver.exe PID: 6880 Parent PID: 5844

General

Start time:	13:54:32
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\Szallitasi adatok.tar'
Imagebase:	0xb90000
File size:	10240 bytes
MD5 hash:	DB55139D9DD29F24AE8EA8F0E5606901
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	146A4B1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	146A5AB	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	146A4B1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	77	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 53 7a 61 6c 6c 69 74 61 73 69 20 61 64 61 74 6f 6b 2e 74 61 72 0d 0a	04/08/2021 1:54 PM: Unpack: C:\Users\user\Desktop\Szallitasi adatok.tar..	success or wait	1	146A8EF	WriteFile
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	80	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 71 76 62 70 73 78 6d 2e 35 34 73 0d 0a	04/08/2021 1:54 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s..	success or wait	1	146A8EF	WriteFile
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	50	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	04/08/2021 1:54 PM: Received from standard out: ..	success or wait	18	146A8EF	WriteFile
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	31	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	04/08/2021 1:54 PM: Get files..	success or wait	1	146A8EF	WriteFile
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	37	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	04/08/2021 1:54 PM: Nbr of files: 1..	success or wait	1	146A8EF	WriteFile
C:\Users\user\AppData\Local\Temp\mcgybaxf.vdb\unarchiver.log	unknown	117	30 34 2f 30 38 2f 32 30 32 31 20 31 3a 35 34 20 50 4d 3a 20 46 6f 75 6e 64 20 69 6e 74 65 72 65 73 74 69 6e 67 20 66 69 6c 65 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 71 76 62 70 73 78 6d 2e 35 34 73 5c 53 7a 61 6c 6c 69 74 61 73 69 20 61 64 61 74 6f 6b 2e 65 78 65 0d 0a	04/08/2021 1:54 PM: Found interesting file: C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe..	success or wait	1	146A8EF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	388	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
\Device\NamedPipe	unknown	1024	success or wait	1	146A8EF	ReadFile
\Device\NamedPipe	unknown	1024	pipe broken	2	146A8EF	ReadFile

Analysis Process: 7za.exe PID: 6916 Parent PID: 6880

General

Start time:	13:54:33
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'\'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s' 'C:\Users\user\Desktop\Szallitasi adatok.tar'
Imagebase:	0x70000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	763B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe	unknown	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 ae 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 0a 0a 00 00 46 03 00 00 00 00 00 f6 29 0a 00 00 20 00 00 00 40 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....n`......... ....P......F.......)... ...@.. ..@.. ....@.................	success or wait	7	76987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Szallitasi adatok.tar	unknown	1024	success or wait	1	7686E	ReadFile
C:\Users\user\Desktop\Szallitasi adatok.tar	unknown	512	success or wait	2	7686E	ReadFile
C:\Users\user\Desktop\Szallitasi adatok.tar	unknown	512	success or wait	1	7686E	ReadFile
C:\Users\user\Desktop\Szallitasi adatok.tar	unknown	512	end of file	1	7686E	ReadFile
C:\Users\user\Desktop\Szallitasi adatok.tar	unknown	131072	success or wait	7	7686E	ReadFile

Analysis Process: conhost.exe PID: 6964 Parent PID: 6916

General

Start time:	13:54:33
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 7008 Parent PID: 6880

General

Start time:	13:54:34
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /C 'C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7028 Parent PID: 7008

General

Start time:	13:54:34
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Szallitasi adatok.exe PID: 7056 Parent PID: 7008

General

Start time:	13:54:35
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe
Imagebase:	0xa30000
File size:	872960 bytes
MD5 hash:	C615C5F811E05D5743CE4DD4AFAD4055
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: 00000006.00000002.344267324.0000000003FF6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.343156984.0000000002E03000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, ReversingLabs
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	6DB7CF06	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	6DB7CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Szallitasi adatok.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE8C78D	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\Szallitasi adatok.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DE8C907	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	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: Szallitasi adatok.exe PID: 7104 Parent PID: 7056

General

Start time:	13:54:42
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\nqvbpsxm.54s\Szallitasi adatok.exe
Imagebase:	0xf80000
File size:	872960 bytes
MD5 hash:	C615C5F811E05D5743CE4DD4AFAD4055
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: 00000007.00000002.590323403.0000000003481000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.590323403.0000000003481000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.586946181.0000000000402000.00000040.00000001.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	6DB7CF06	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	6DB7CF06	unknown

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	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c0762b14-80f9-4b17-9e6c-06348dbc9238	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Disassembly

Code Analysis