ID: 778228
Sample Name: file.exe
Cookbook: default.jbs
Time: 08:46:10
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

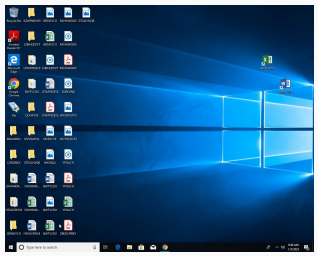
Windows Analysis Report

file.exe

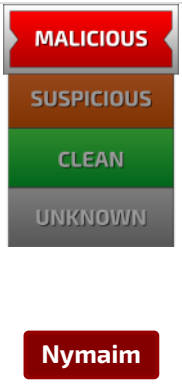
Overview

General Information

Sample Name:	file.exe
Analysis ID:	778228
MD5:	e0f8085c7cb8eb…
SHA1:	a109ebcf251a1e..
SHA256:	a28fb531e91695..
Tags:	exe
Infos:	



Detection



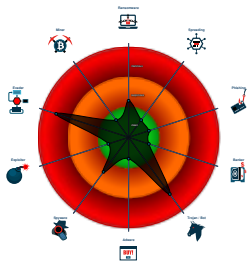
Nymaim

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (overwrites its o…
- Yara detected Nymaim
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 2148 cmdline: C:\Users\user\Desktop\file.exe MD5: E0F8085C7CB8EB9CF1C263BB12CFC6DF)
  - is-DTRND.tmp (PID: 6048 cmdline: "C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp" /SL4 $902D6 "C:\Users\user\Desktop\file.exe" 1818498 170496 MD5: E8176050192FBB976D70238E3C121F4C)
    - SplitFiles131.exe (PID: 4360 cmdline: "C:\Program Files (x86)\Split Files\SplitFiles131.exe" MD5: 361518D6CC3C25EEC2DFC1DE82B055B2)
      - KN38AzDG.exe (PID: 1960 cmdline: MD5: 3FB36CB0B7172E5298D2992D42984D06)
      - cmd.exe (PID: 1876 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "SplitFiles131.exe" /f & erase "C:\Program Files (x86)\Split Files\SplitFiles131.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - taskkill.exe (PID: 5224 cmdline: taskkill /im "SplitFiles131.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Configuration

Threatname: Nymaim

```
{
  "C2 addresses": [
    "45.139.105.1",
    "85.31.46.167",
    "107.182.129.235",
    "171.22.30.106"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.371399176.0000000000400000.00000040.00000001.01000000.00000008.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000005.00000002.372442187.000000000030C0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000005.00000002.372529330.0000000003340000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.SplitFiles131.exe.3340000.3.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
5.2.SplitFiles131.exe.400000.0.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
5.2.SplitFiles131.exe.400000.0.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
5.2.SplitFiles131.exe.3340000.3.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN GCleaner Downloader - Payload Response - Source IP: 107.182.129.235 - Destination IP: 192.168.2.5

Timestamp:	107.182.129.235192.168.2.580497062852925 01/05/23-08:47:10.017687
SID:	2852925
Source Port:	80
Destination Port:	49706
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN GCleaner Downloader Activity M8 - Source IP: 192.168.2.5 - Destination IP: 45.139.105.171

Timestamp:	192.168.2.545.139.105.17149705802041920 01/05/23-08:47:09.800462
SID:	2041920
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Fabookie.ek CnC Request M3 (GET) - Source IP: 192.168.2.5 - Destination IP: 107.182.129.235

Timestamp:	192.168.2.5107.182.129.23549706802852981 01/05/23-08:47:09.990287
SID:	2852981
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Fabookie.ek CnC Request M1 (GET) - Source IP: 192.168.2.5 - Destination IP: 107.182.129.235

Timestamp:	192.168.2.5107.182.129.23549706802852980 01/05/23-08:47:09.925610
SID:	2852980
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nymaim

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Stealing of Sensitive Information

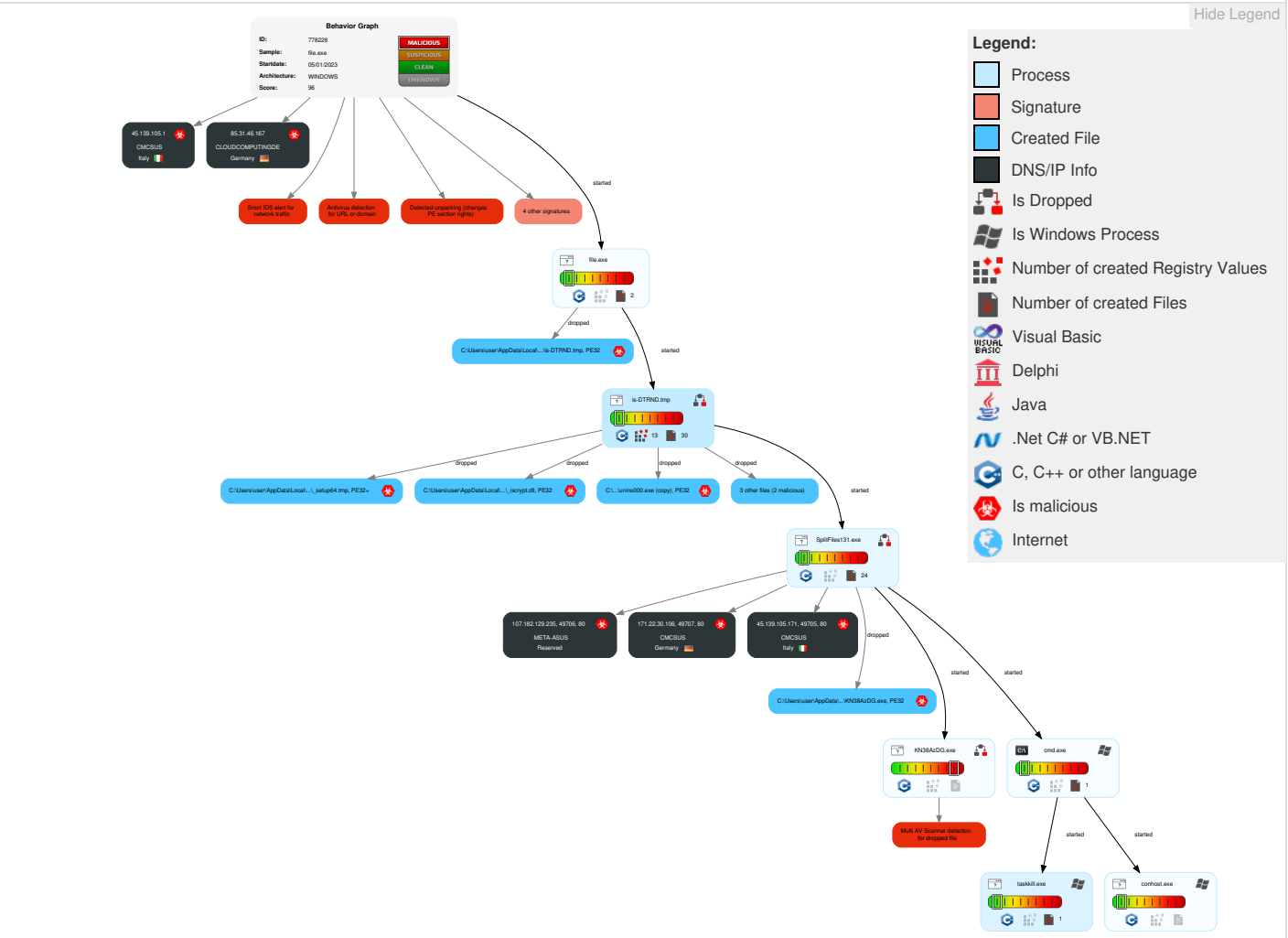
Yara detected Nymaim

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	1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 3 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 4 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Process Injection	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

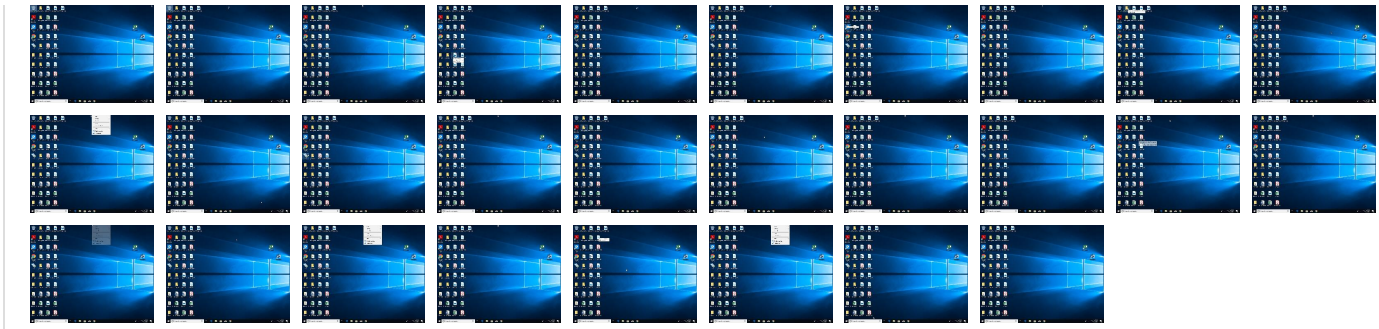
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Split Files\SplitFiles131.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_iscrypt.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_shfoldr.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\KN38AzDG.exe	50%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.SplitFiles131.exe.10000000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
1.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
5.2.SplitFiles131.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
4.2.is-DTRND.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1248792		Download File
1.0.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://www.innosetup.com/	0%	URL Reputation	safe	
http://45.139.105.171/itsnotmalware/count.php?sub=NOSUB&stream=mixtwo&substream=mixinte	0%	URL Reputation	safe	
http://107.182.129.235/storage/extension.php	0%	URL Reputation	safe	
http://www.remobjects.com/?ps	0%	URL Reputation	safe	
http://www.innosetup.com	0%	URL Reputation	safe	
http://107.182.129.235/storage/ping.php	0%	URL Reputation	safe	
http://171.22.30.106/library.php	100%	URL Reputation	malware	
http://www.remobjects.com/?psU	0%	URL Reputation	safe	
http://rus.altarsoft.com/split_files.shtml	0%	Avira URL Cloud	safe	
http://www.altarsoft.com/split_files.shtml	0%	Avira URL Cloud	safe	
http://www.altarsoft.com/split_files.shtml	2%	Virustotal		Browse
http://171.22.30.106/library.phpch	100%	Avira URL Cloud	malware	
http://www.innosetup.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://171.22.30.106/library.phpYQ	100%	Avira URL Cloud	malware	
http://171.22.30.106/library.php4	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

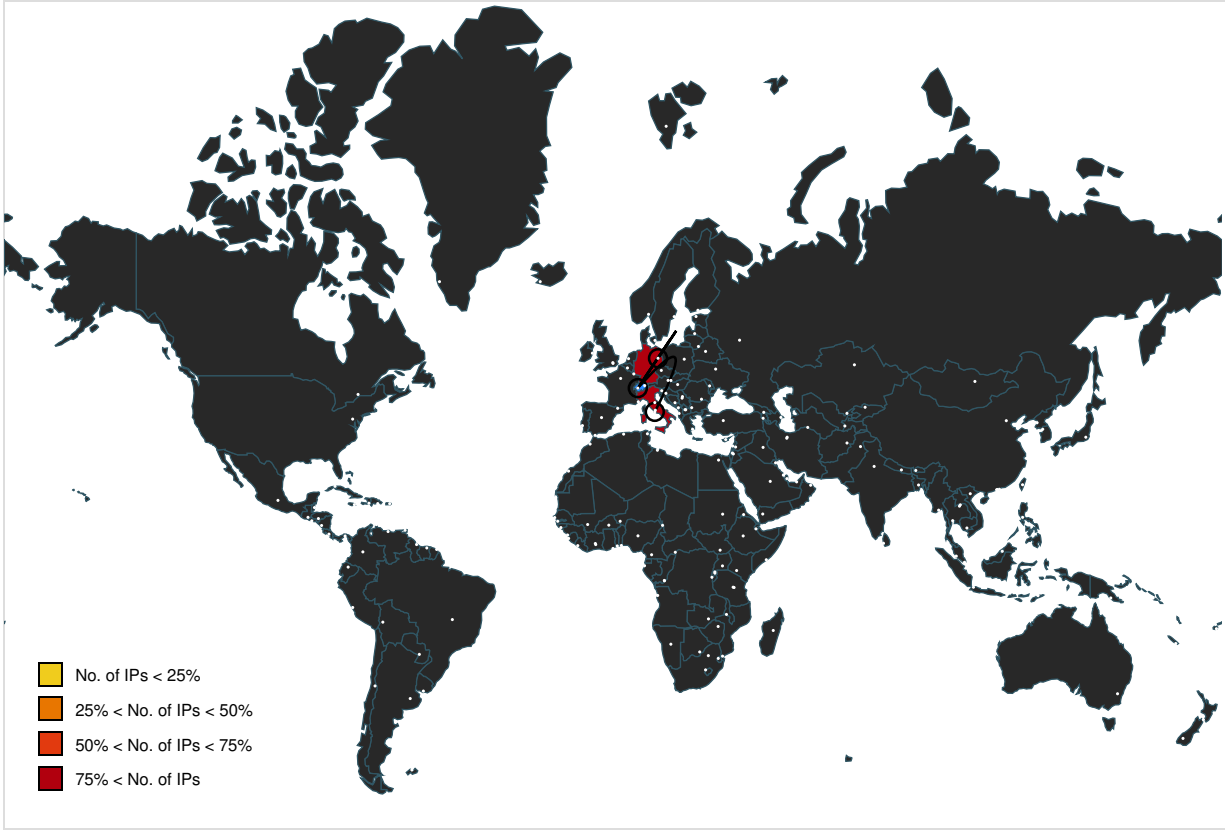
Name	Malicious	Antivirus Detection	Reputation
http://45.139.105.171/itsnotmalware/count.php?sub=NOSUB&stream=mixtwo&substream=mixinte	true	• URL Reputation: safe	unknown
http://107.182.129.235/storage/extension.php	true	• URL Reputation: safe	unknown
http://107.182.129.235/storage/ping.php	true	• URL Reputation: safe	unknown
http://171.22.30.106/library.php	true	• URL Reputation: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	is-DTRND.tmp, is-DTRND.tmp, 00000004.00000002.373506640.0000000000401000.00000020.00000001.01000000.00000005.sdmp, is-AGVDF.tmp.4.dr, is-DTRND.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.altarsoft.com/split_files.shtml	is-DTRND.tmp, 00000004.00000002.37347029 8.000000000018F000.00000004.00000010.000 20000.00000000.sdmp, is-DTRND.tmp, 00000 004.00000002.374801354.0000000004D00000. 00000004.00001000.00020000.00000000.sdmp, is-8E2LT.tmp.4.dr, is-7O3KV.tmp.4.dr, is-R2P47.t mp.4.dr, is-JMARM.tmp.4.dr, is-B20UO.tmp.4.dr, is-UJJ0L.tmp.4.dr, is-JSP8F.tmp.4.dr, is-79U67.tmp.4.dr, is-APJVT.tmp.4.dr, is-7L4JB.tmp.4.dr	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://171.22.30.106/library.phpch	SplitFiles131.exe, 00000005.00000003.354 343284.00000000043C6000.00000004.0000080 0.00020000.00000000.sdmp, SplitFiles131.exe, 00000 005.00000003.366040028.00000000043C6000. 00000004.00000800.00020000.00000000.sdmp, SplitFiles131.exe, 00000005.00000003.343762944.0 0000000043C6000.00000004.00000800.000200 00.00000000.sdmp, SplitFiles131.exe, 00000005.0000 0003.349052998.00000000043C6000.00000004 .00000800.00020000.00000000.sdmp, SplitF iles131.exe, 00000005.00000003.360534891 .00000000043C6000.00000004.00000800.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.remobjects.com/?ps	file.exe, 00000001.00000003.289027881.00 00000002058000.00000004.00001000.0002000 0.00000000.sdmp, file.exe, 00000001.0000 0003.288799915.0000000002230000.00000004 .00001000.00020000.00000000.sdmp, is-DTRND.tmp, is-DTRND.tmp, 00000004.00000002.373506640. 0000000000401000.00000020.00000001.01000 000.00000005.sdmp, is-AGVDF.tmp.4.dr, is-DTRND.tmp.1.dr	false	• URL Reputation: safe	unknown
http://rus.altarsoft.com/split_files.shtml	is-DTRND.tmp, 00000004.00000002.37347029 8.000000000018F000.00000004.00000010.000 20000.00000000.sdmp, is-DTRND.tmp, 00000 004.00000002.374801354.0000000004D00000. 00000004.00001000.00020000.00000000.sdmp, is-3OAED.tmp.4.dr, is-FBKGV.tmp.4.dr	false	• Avira URL Cloud: safe	unknown
http://www.innosetup.com	file.exe	false	• URL Reputation: safe	unknown
http://171.22.30.106/library.phpYQ	SplitFiles131.exe, 00000005.00000003.354 343284.00000000043C6000.00000004.0000080 0.00020000.00000000.sdmp, SplitFiles131.exe, 00000 005.00000003.338258725.00000000043C6000. 00000004.00000800.00020000.00000000.sdmp, SplitFiles131.exe, 00000005.00000003.366040028.0 0000000043C6000.00000004.00000800.000200 00.00000000.sdmp, SplitFiles131.exe, 00000005.0000 0003.343762944.00000000043C6000.00000004 .00000800.00020000.00000000.sdmp, SplitF iles131.exe, 00000005.00000003.349052998 .00000000043C6000.00000004.00000800.0002 0000.00000000.sdmp, SplitFiles131.exe, 00000005.00 000003.360534891.00000000043C6000.000000 04.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://171.22.30.106/library.php4	SplitFiles131.exe, 00000005.00000003.332 714577.00000000043C6000.00000004.0000080 0.00020000.00000000.sdmp, SplitFiles131.exe, 00000 005.00000003.338258725.00000000043C6000. 00000004.00000800.00020000.00000000.sdmp, SplitFiles131.exe, 00000005.00000003.343762944.0 0000000043C6000.00000004.00000800.000200 00.00000000.sdmp, SplitFiles131.exe, 00000005.0000 0003.327425336.00000000043C6000.00000004 .00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.innosetup.comDVarFileInfo$	file.exe, 00000001.00000003.289316432.00 000000020FD000.00000004.00001000.0002000 0.00000000.sdmp, file.exe, 00000001.0000 0003.288963142.00000000022D9000.00000004 .00001000.00020000.00000000.sdmp, is-DTRND.tmp, 00000004.00000002.373626287.00000000004C40 00.00000002.00000001.01000000.00000005.sdmp, is-AGVDF.tmp.4.dr, is-DTRND.tmp.1.dr	false	• Avira URL Cloud: safe	low
http://www.remobjects.com/?psU	file.exe, 00000001.00000003.289027881.00 00000002058000.00000004.00001000.0002000 0.00000000.sdmp, file.exe, 00000001.0000 0003.288799915.0000000002230000.00000004 .00001000.00020000.00000000.sdmp, is-DTRND.tmp, 00000004.00000002.373506640.00000000004010 00.00000020.00000001.01000000.00000005.sdmp, is-AGVDF.tmp.4.dr, is-DTRND.tmp.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.139.105.171	unknown	Italy		33657	CMCSUS	true
45.139.105.1	unknown	Italy		33657	CMCSUS	true
85.31.46.167	unknown	Germany		43659	CLOUDCOMPUTINGDE	true
107.182.129.235	unknown	Reserved		11070	META-ASUS	true
171.22.30.106	unknown	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778228
Start date and time:	2023-01-05 08:46:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	mal96.troj.evad.winEXE@12/39@0/5

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.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 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
08:47:09	API Interceptor	1x Sleep call for process: KN38AzDG.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:\Program Files (x86)\Split Files\ReadMe - EN.txt (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2193
Entropy (8bit):	4.702648325021821
Encrypted:	false
SSDEEP:	24:ElZ5/fnS3LWjwbf2VQZl5HXvbap4qDwGApRAboaGnMAzPelJoEhLifJy:mZ3jwbf2V25HjcwGpbpGMaelXh2g

MD5:	EA42A2F0D0B4CBE042DE38568E18F1AC
SHA1:	58B2B523D4CCB03A07F9B1CB53250F3C6BA0B771
SHA-256:	AF9B99F745D2B2F3E688336C68F69C9CADF7E85BF443100DDA4EBB507D86155A
SHA-512:	6F202138BE4B009152A72AB671A4C5D3AE5580211EDE11F4E35B89F2F1EF58E8B8DBD35E9DA1D12B7ABDD3BFD4EE342541DE8DE2437D0FCEA77A1C5782AE0E2A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Split Files 1.72....Contents:....1. Description...2. History...3. Localization...4. Contacts.....---....1. Description.....Fast and easy file splitter and joiner...Split files by parts size or parts number...Create .bat file to merge parts without program.....---....2. Development History:....17.10.2010 - update to version 1.72....- large files splitting error fix (over 2 Gb)..- new language: turkish....9.02.2010 - update to version 1.71....- split and join options in windows explorer pop-up menu....16.01.2010 - update to version 1.7....- new languages: dutch, italian, spanish..- delete input file after splitting....3.01.2010 - update to version 1.6....- compression (zip)..- drag and drop..- french language..- arabic language..- interface was changed....18.11.2008 - update to version 1.5....- large files splitting error fix (over 1 Gb)..- output folder selection..

C:\Program Files (x86)\Split Files\ReadMe - RU.txt (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with very long lines (1053), with CRLF line terminators
Category:	dropped
Size (bytes):	2942
Entropy (8bit):	5.0506474169868945
Encrypted:	false
SSDEEP:	48:mRIjSLoZpLobGyYly6y4cMUNYzLEDa3dMSsXNBIi3Dl0r4k1z9bcX4Xl9asUvn6d:IW7Lob1YEgcMiDa3WN7BW1zLV1mngV4+
MD5:	58D65074A58BC8EAE2D5A3B589399A53
SHA1:	074E7E5BFD52200086309913670D49BA664FB279
SHA-256:	2F2487EDEEEA0D35394FD1C0B72D9C1FBF617DD014ED659083BDB0EFB12F6C90
SHA-512:	C0806DFC9DCD2A620693115679057B5374DEA3930E02F2B8DD1390C843D3F7C138CA8576CA35A5BCBEEA68E5CD9F5193C8D564A942C5A179DB9C5E6CAAA0066
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Split Files 1.72..............:....1. ....2. ....3. ....---....1. ...., ...: .. .., ..., ..., ..., ...bat .... .bat .... .bat ...., ... zip ...., ...

C:\Program Files (x86)\Split Files\SplitFiles131.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	modified
Size (bytes):	3491315
Entropy (8bit):	5.600225128146387
Encrypted:	false
SSDEEP:	24576:8kvs+hjRbEtvglyhbpegN4X94JFlWchs9F4AyM1n6iuAdsGR0A2O3DyLaYtBlecd:8VQj5EtvSpZvJFlp9IM1ft22mHBldXXL
MD5:	361518D6CC3C25EEC2DFC1DE82B055B2
SHA1:	5B298ED47BDEFA0BB953F277649CCB7C3A308C3C
SHA-256:	616BB3AC1AE4651819FCD80CB8357940061AF64A21401C33E8C84CFF41679211
SHA-512:	4EFAC7D2D772FDD8D3DAC80CE7874D5E85957D39B8F1392E00CF8969F87076A1146363990212ED79E63ADEF92427514E3E7D957B2E3E3D056E5A6741D57FA03
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....~.c.........._...............................@..........................P......]m5. ....P...e...text...2........................... ..`.rdata...+.......0..................@..@.data........0 .......0..............@....tls.... ....@.......@..............@....rsrc....p...P...p...P..............@..@.ave131...+......+.................`.*... ....

C:\Program Files (x86)\Split Files\is-3OAED.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with very long lines (1053), with CRLF line terminators
Category:	dropped
Size (bytes):	2942
Entropy (8bit):	5.0506474169868945
Encrypted:	false
SSDEEP:	48:mRIjSLoZpLobGyYly6y4cMUNYzLEDa3dMSsXNBIi3Dl0r4k1z9bcX4Xl9asUvn6d:IW7Lob1YEgcMiDa3WN7BW1zLV1mngV4+
MD5:	58D65074A58BC8EAE2D5A3B589399A53

SHA1:	074E7E5BFD52200086309913670D49BA664FB279
SHA-256:	2F2487EDEEEA0D35394FD1C0B72D9C1FBF617DD014ED659083BDB0EFB12F6C90
SHA-512:	C0806DFC9DCD2A620693115679057B5374DEA3930E02F2B8DD1390C843D3F7C138CA8576CA35A5BCBEEA68E5CD9F5193C8D564A942C5A179DB9C5E6CAAA00 66
Malicious:	false
Preview:	Split Files 1.72..............:....1. ....2. ....3. ....---....1. ...., ...: .. .., ..., ..., ..., ...bat .... .bat .... .bat ...., ... zip ...., ...

C:\Program Files (x86)\Split Files\is-6QN6Q.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	data
Category:	dropped
Size (bytes):	3491315
Entropy (8bit):	5.600224518949536
Encrypted:	false
SSDEEP:	24576:3kvs+hjRbEtvgIyhbpegN4X94JFlWchs9F4AyM1n6iuAdsGR0A2O3DyLaYtBlecd:3VQj5EtvSpZvJFIp9IM1ft22mHBldXXL
MD5:	F488A4815DE52F915E37E40EA88B011F
SHA1:	16F9954F5E9FE6CB50125396B7DB524218D01237
SHA-256:	E13C9E749995269A3C45C6464B2F0BF55283288FD020FE4D0F1CA811142CC2AC
SHA-512:	04262ADC77B3126FCB9A8991612DDCFC35DF7F35988D108079A0BACF04350C57E829CA8E8C74833D0A0D9D9CD1DD480B9F4FA7145051AECF85D23C85A90667 2
Malicious:	false
Preview:	.Z......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....~.c.........._...............................@..........................P......]m5. ....P...e...text...2........................... ..`.rdata...+.......0..................@..@.data........0 .......0..............@....tls.... ....@.......@..............@....rsrc....p...P...p...P..............@..@.ave131...+......+.................`.*... ....

C:\Program Files (x86)\Split Files\is-AGVDF.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	789258
Entropy (8bit):	6.369988626022893
Encrypted:	false
SSDEEP:	12288:EpmOmg1k2bfrP437QzH/A6A40lG77NzknuGyJOxOU:emt2bfrP437QzH/A6A7E7dVPUxOU
MD5:	D3BA43B9E1B3838F28AFC558F2991D5B
SHA1:	1132F1C76760281A591F7DF99D592283103FCC87
SHA-256:	1E95FE5D06884DF82D2BEAEDA09434ECAC2A347AEC5F03E71F20E39FB6C9E0E9
SHA-512:	870371843F59B91D75B6C4D4C637075235D25CF3ABB059B58E39F9CD2833533A8F434307E7AD1175FD45082D3B4E4F0ED79F303ED77DEF553587E2819C092022
Malicious:	**true**
Preview:	MZP.....................@.......................InUn....................!..L.!..This program must be run under Win32..$7.. ..........................PE..L....^B*.....................4......X............@..@..............................%......l..................@..............................0.............................. ....CODE....l.......................... ..`DATA...............................@...BSS.....p................................idata...%.......&.................@....tls......... ....rdata ....0......................@..P.reloc..t....@......................@..P.rsrc...l..........................@..P....................................@..P.. ....

C:\Program Files (x86)\Split Files\is-JSP8F.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	MS Windows 95 Internet shortcut text (URL=<http://www.altarsoft.com/split_files.shtml>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	97
Entropy (8bit):	5.12302231676258
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/0S4UEtSNM5LTJOBCBuQpQQXXy:HRYFVm/r4UEtSeVTJuZQplHy
MD5:	DCD6923B008121BFF4C7C0AA1206286E
SHA1:	AD4EF16A96A80C8EA5DBC5933229580BC6C332E0
SHA-256:	E1E01BFA5E2B5A117A627F7E9E861CF63D852A66BCE0DF88094D59CAF61E4376
SHA-512:	EC4A399EB38A1FA64DF8990708168F134ACD0CA793930E57C6D3A260A537B20DFD9F8B7232987F32EC1C1A7CEC7EC91F15A644A63D275104D96588FC3D354B5 C
Malicious:	false

Preview:	[InternetShortcut]..URL=http://www.altarsoft.com/split_files.shtml..Modified=500425EA770BCC01B2..

C:\Program Files (x86)\Split Files\is-UJJ0L.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2193
Entropy (8bit):	4.702648325021821
Encrypted:	false
SSDEEP:	24:ElZ5/fnS3LWjwbf2VQZl5HXvbap4qDwGApRAboaGnMAzPelJoEhLifJy:mZ3jwbf2V25HjcwGpbpGMaelXh2g
MD5:	EA42A2F0D0B4CBE042DE38568E18F1AC
SHA1:	58B2B523D4CCB03A07F9B1CB53250F3C6BA0B771
SHA-256:	AF9B99F745D2B2F3E688336C68F69C9CADF7E85BF443100DDA4EBB507D86155A
SHA-512:	6F202138BE4B009152A72AB671A4C5D3AE5580211EDE11F4E35B89F2F1EF58E8B8DBD35E9DA1D12B7ABDD3BFD4EE342541DE8DE2437D0FCEA77A1C5782AE0E2A
Malicious:	false
Preview:	Split Files 1.72....Contents:....1. Description...2. History...3. Localization...4. Contacts.....----------....1. Description.....Fast and easy file splitter and joiner...Split files by parts size or parts number...Create .bat file to merge parts without program.....----------....2. Development History:....17.10.2010 - update to version 1.72....- large files splitting error fix (over 2 Gb)..- new language: turkish....9.02.2010 - update to version 1.71....- split and join options in windows explorer pop-up menu....16.01.2010 - update to version 1.7....- new languages: dutch, italian, spanish..- delete input file after splitting....3.01.2010 - update to version 1.6....- compression (zip)..- drag and drop..- french language..- arabic language..- interface was changed....18.11.2008 - update to version 1.5....- large files splitting error fix (over 1 Gb)..- output folder selection..

C:\Program Files (x86)\Split Files\language\Arabic.ini (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2266
Entropy (8bit):	5.4593359267896355
Encrypted:	false
SSDEEP:	48:HG8il+sqirh7zJ9YTHskp1r4phFAqLNnK9h:HGkSkp1r4NTKf
MD5:	4ABA9765EB3555788F5706D87A9D2DCA
SHA1:	36C0895FBF9F99690CA55C54CC56310E24513113
SHA-256:	E99B943206594C04BC0383669D04D4F191A501F46D2474FED08B997F8020B433
SHA-512:	3498485635AFC548663715D22071611BAB10C707E8E24BE0B5143EE4A27727DA7D18A5E6959E3F6DD7D0F615DDFD50CE9FC5CE8AE6DDC5BEE287B5A00A817288
Malicious:	false
Preview:	[Interface]....MFile->Caption = '...'..MExit->Caption =' ....'..MOptions->Caption = 'Options'..MSettings->Caption =' .....'..MLanguage->Caption =' .....'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption =' .....'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = '....'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption =' .....'..MAbout->Caption =' ...'....TabSheetSplit->Caption = ' ... .'..TabSheetCombine->Caption = ' ...'....GroupBoxCombine->Caption =' ... .'..LabelFirstFile->Caption = '..... .....:'..LabelOutput->Caption = '... .....:'..LabelCombineFolder->Caption =' ....:'..LabelSplitFolder->Caption = '.... .....:'..ButtonCombine->Caption =' ...'..ButtonStopCombine->Caption = '....'....GroupBoxSplit->Caption = '... .....'..LabelFileName->Caption =' ....: '..LabelSplitFolder->Caption =' ....:'

C:\Program Files (x86)\Split Files\language\Chinese.ini (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2345
Entropy (8bit):	5.847861612631974
Encrypted:	false
SSDEEP:	48:HGj2lE8qiTh7XJ9zHadtPTTD1n34q1jgun1ITq8K:HG5RDTln34qRgusK
MD5:	A5C9FEA89EFE8E2162BA477E8EA39B44
SHA1:	E6A2042C574D14786891F0C32F92C8292BBB4ACA
SHA-256:	8DDFB50DACA491296101BAB3DB9B77C7587127E684D9E22EFD6DC93F84A008FA
SHA-512:	3F7944F262717D308A1235982E741536DA6A4DF9ABEE4E2811E1151B53C3D31811EA3EB750ED39F347F7DF14AD20FF981C85CC2DA297BE745547B36D41B8FDB
Malicious:	false
Preview:	[Interface]....MFile->Caption = '...(&F)'..MExit->Caption = '.....'..MOptions->Caption = '...'..MSettings->Caption = '....'..MLanguage->Caption = '....'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = '.....'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = '....'..MAbout->Caption = '....'....TabSheetSplit->Caption = '...'..TabSheetCombine->Caption = '...'....GroupBoxCombine->Caption = ' ..... "....." .....'..LabelFirstFile->Caption = '.....'..LabelOutput->Caption = '.....'..LabelCombineFolder->Caption = '.....'..LabelSplitFolder->Caption = '.....'..ButtonCombine->Caption = '...'..ButtonStopCombine->Caption = '..'....GroupBoxSplit->Caption = ' ..... "....."..... '..LabelFileName->Caption = '.

C:\Program Files (x86)\Split Files\language\Dutch.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2687
Entropy (8bit):	5.051567814097503
Encrypted:	false
SSDEEP:	48:HGgXRVA+sqgh59WJIo4yvHIExBMHkWREHZDNbHBsBOtiSZls5crRMfiE:HGusSgEvMHfREHN9hsoiOUBiE
MD5:	D2471D35D833E2544D67365E015E6153
SHA1:	497EE8FF9519D025BD10C5AA15DDC34DFB1B334B
SHA-256:	4831DDBCFE327E2542F4565E7A948C5828D71003B8444723E1E11BA6BB43ACE7
SHA-512:	C82B30D604A679F87B8D0B1670A0D1607E25150FFCFD1C9E631241916BA93CEB5A33AFCAA9080149096ACA1913791384860F5699F2BB302B6CB190AF777EB3CI
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Programma Afsluiten'..MOptions->Caption = 'Options'..MSettings->Caption = 'Instellingen'..MLanguage->Caption = 'Kies Taal'..MLangArabic->Caption = 'Arabisch'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Nederlands'..MLangEnglish->Caption = 'Engels'..MLangFrench->Caption = 'Frans'..MLangItalian->Caption = 'Italiaans'..MLangRussian->Caption = 'Russisch'..MLangSpanish->Caption = 'Spaans'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Hulp'..MAbout->Caption = 'Info'....TabSheetSplit->Caption = 'SPLITSEN'..TabSheetCombine->Caption = 'HERENIGEN'....GroupBoxCombine->Caption = ' Drag and drop een van de te herenigen delen in 'Eerste Deel' of browse ernaartoe '..LabelFirstFile->Caption = 'Eerste Deel:'..LabelOutput->Caption = 'Output Bestandsnaam:'..LabelCombineFolder->Caption = 'Output Map:'..LabelSplitFolder->Caption = 'Output Map:'..ButtonCombine->Caption = 'HERENIGEN'..ButtonStopCombine->Caption = 'STOP'....Grou

C:\Program Files (x86)\Split Files\language\English.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2594
Entropy (8bit):	5.044497576650396
Encrypted:	false
SSDEEP:	48:HGgb5l+sqiTh7XJ9oVHo1xx0GHLVQ4ZWGAtDAEQmUDcQdWym:HGdpa1jfHLVQ4AGAtWma8H
MD5:	76776746B3CFF1CBD5D56CD44CA2DEF5
SHA1:	2F2ECA50BD7F72232BE84291EF1A7956C24098CC
SHA-256:	EC647D30931F50607CF745D958AAF0367CCEAB9999346188255CFBFB22301EE3
SHA-512:	202436C708D4F34FFCCDC3D33841246C5CEE073AC270DA547C15F9E995A08D36AE4C00982283BF60D62363046BBEAA0125D59075E4629A9D1934039CBFB00BE
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Exit Application'..MOptions->Caption = 'Options'..MSettings->Caption = 'Settings'..MLanguage->Caption = 'Language'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Help'..MAbout->Caption = 'About'....TabSheetSplit->Caption = 'SPLIT'..TabSheetCombine->Caption = 'JOIN'....GroupBoxCombine->Caption = ' Drag and drop one of the files to join in the 'First Part' box or browse to it '..LabelFirstFile->Caption = 'First Part:'..LabelOutput->Caption = 'Output File Name:'..LabelCombineFolder->Caption = 'Output Folder:'..LabelSplitFolder->Caption = 'Output Folder:'..ButtonCombine->Caption = 'JOIN'..ButtonStopCombine->Caption = 'STOP'....GroupBoxSplit->Caption = ' Drag

C:\Program Files (x86)\Split Files\language\French.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2507
Entropy (8bit):	5.040552699764577
Encrypted:	false
SSDEEP:	48:HGkOA+sq/W7Yve3EkHaBSDbSljMM+v1/D3H:HGb8hABSDbSJMBD
MD5:	336D33F55222F48FBA19EF0911732766
SHA1:	E17A78E3B48192361DB540B1E8C9D0548C9A9FFE
SHA-256:	0E955453FA27CED0D0521F0F960C7743C2090F06263D33EC8FA978B681123E0C
SHA-512:	67EC6B859BCDD66DA59CDB1DC1A4EACFBDA12C57699012EE1573DD88F5AAAB6288E1BD9015C862689F4A1A27E83B28C3A9C99B1895EDF4F47D6F94B0557CI C1F
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Fichier'..MExit->Caption = 'Quitter'..MOptions->Caption = 'Options'..MSettings->Caption = 'Settings'..MLanguage->Caption = 'Langage'..MLangArabic->Caption = 'Arabe'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Flamand'..MLangEnglish->Caption = 'Englais'..MLangFrench->Caption = 'Francais'..MLangItalian->Caption = 'Italien'..MLangRussian->Caption = 'Russe'..MLangSpanish->Caption = 'Espagnol'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Aide'..MAbout->Caption = 'A propos de ..'....TabSheetSplit->Caption = 'Scinder'..TabSheetCombine->Caption = 'Assembler'....GroupBoxCombine->Caption = ' Faire glisser un des fichiers bloc . assembler ou rechercher le par ... '..LabelFirstFile->Caption = 'Premier Fichier:'..LabelOutput->Caption = 'Fichier de sortie: '..LabelCombineFolder->Caption = 'R.pertoire Dest.'..LabelSplitFolder->Caption = 'R.pertoire Dest.'..ButtonCombine->Caption = 'Assembler'..ButtonStopCombine->Caption = 'Stop'....GroupBoxSpl

C:\Program Files (x86)\Split Files\language\Italian.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2729
Entropy (8bit):	5.029883215699414
Encrypted:	false
SSDEEP:	48:HGgS7++sqMsmQYEJK7bHExsA9GZ1MTn6btlOWH6r3zvX5c9WYN:HGjUoR9GXML6RYWH6rDRdYN
MD5:	8AFE543CB6791AA250312EBA61BF7C13
SHA1:	BFD229D43BE86728A634055AD65860157C2671BD
SHA-256:	AF5BFB663E715C48C55E24BC3BEA30FCAA9BE8EAF35133FBB75D54C5735696AC
SHA-512:	5CF85F84DD6D363B2AAC720CF10C5289350EB706DC2BF5CA824CF220C3607CC7969CDD2F4B2912DC97C7BE50CEDC24A9A01AFC585CE84B6B8CB8141915393A2
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Termina programma'..MOptions->Caption = 'Options'..MSettings->Caption = 'Impostazioni'..MLanguage->Caption = 'Seleziona Lingua'..MLangArabic->Caption = 'Arabo'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Olandese'..MLangEnglish->Caption = 'Inglese'..MLangFrench->Caption = 'Francese'..MLangItalian->Caption = 'Italiano'..MLangRussian->Caption = 'Russo'..MLangSpanish->Caption = 'Spagnolo'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Aiuto'..MAbout->Caption = 'Informazioni'....TabSheetSplit->Caption = 'DIVIDI'..TabSheetCombine->Caption = 'UNISCI'....GroupBoxCombine->Caption = ' Drag and drop una delle parti da unire nella casella 'Prima Parte' o segui percorso '..LabelFirstFile->Caption = 'Prima Parte:'..LabelOutput->Caption = 'Nome File Uscita:'..LabelCombineFolder->Caption = 'Cartella Uscita:'..LabelSplitFolder->Caption = 'Cartella Uscita:'..ButtonCombine->Caption = 'UNISCI'..ButtonStopCombine->Caption = '

C:\Program Files (x86)\Split Files\language\Russian.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2299
Entropy (8bit):	5.691502190790686
Encrypted:	false
SSDEEP:	48:HG9uhjkDYhqGQjsONHiHQgGU9dm6nclk6a1hg22mo6LD:HGnzLIQTUPmcclGsmogD
MD5:	F9F47FF3D866FFC4F38E315E41356E55
SHA1:	EFC313A99993B5FB8A454D4C5197C6F3965B5C89
SHA-256:	3A13CCE54190BF4A679D21F61466A0A18E9340287CAA1AA4EACB38C99C9D4957
SHA-512:	6EC1F1E19921C535A50254500ED01602DA74D3CC9E6DA8B5FC78D89255E42C5968BD294E56F584EE273630B9233C20CAFEBC906354CE393FE1CFFE91528F527A
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&....'..MExit->Caption = '.....'..MOptions->Caption = '.....'..MSettings->Caption = '.....'..MLanguage->Caption = '....'..MLangEnglish->Caption = '.....'..MLangRussian->Caption = '.....'..MLangArabic->Caption = '.....'..MLangChinese->Caption = '.....'..MLangDutch->Caption = '.....'..MLangFrench->Caption = '.....'..MLangItalian->Caption = '.....'..MLangSpanish->Caption = '.....'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = '.....'..MAbout->Caption = '. ....'....TabSheetSplit->Caption = '.....'..TabSheetCombine->Caption = '.....'....GroupBoxCombine->Caption = ' .... '..LabelFirstFile->Caption = '1-. ....'..LabelOutput->Caption = '.....: '..LabelCombineFolder->Caption = '.....:'..ButtonCombine->Caption = '.....'..ButtonStopCombine->Caption = '....'....GroupBoxSplit->Caption = ' .... '..LabelSplitFolder->Caption = '.....:'..LabelFileName->Caption = '... .....:'..LabelFile

C:\Program Files (x86)\Split Files\language\Spanish.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2718
Entropy (8bit):	5.057121428169199
Encrypted:	false
SSDEEP:	48:HGPWFaxAA+sqKvFYLcunHh3QxXOBp1OB5r70h3CGRsJE0laDwXCqXH5wGF5JoCPa:HGPAPZBAJU1k7Jb245xVfUMG
MD5:	21B4D47F5D851271C89310C92777FB70
SHA1:	9D85FF8F7107CFAE3F31993FAF7F249591AFCB27
SHA-256:	D88AE9E292EBC4E56767892FD451E2E8278FCE776CAD689731EE7875748D55D7
SHA-512:	46F26B51D6959A36E33266887E39CB98E7E67880052DE8DE741CB93C90ED3B28C87A224CE710E6C698FE648ED8B062E73DEDC253A6C5A8362EB3EF2792AB4FF
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Archivo'..MExit->Caption = 'Salir'..MOptions->Caption = 'Options'..MSettings->Caption = 'Herramientas'..MLanguage->Caption = 'Elegir idioma'..MLangArabic->Caption = 'Arabe'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Holand.s'..MLangEnglish->Caption = 'Ingl.s'..MLangFrench->Caption = 'Franc.s'..MLangItalian->Caption = 'Italiano'..MLangRussian->Caption = 'Ruso'..MLangSpanish->Caption = 'Espa.ol'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Ayuda'..MAbout->Caption = 'Sobre programa'....TabSheetSplit->Caption = 'SEPARAR'..TabSheetCombine->Caption = 'JUNTAR'....GroupBoxCombine->Caption = ' Drag and drop una de las partes para juntar en la celda 'Primera Parte' o navegar '..LabelFirstFile->Caption = 'Primera Parte:'..LabelOutput->Caption = 'Nombre Archivo salida:'..LabelCombineFolder->Caption = 'Carpeta salida:'..LabelSplitFolder->Caption = 'Carpeta salida:'..ButtonCombine->Caption = 'JUNTAR'..ButtonStopCombine->Caption = 'PARAR'....

C:\Program Files (x86)\Split Files\language\Turkish.ini (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2607
Entropy (8bit):	5.234177949162883
Encrypted:	false
SSDEEP:	48:HGUyjEiB0w3l+sqiTh7XJ9UeHjIDt00AoB/nheSSMpSSSxPYe:HGpNBrkGIDt0qnheS9Sx
MD5:	E1271E0DDD609CD7F9C2367D32FEBE4B
SHA1:	0A420424F1FADE0BFF002E63AAD22B5E94B86CAC
SHA-256:	AEE6B1EDFFFCE507E2207C7E2AA36DA42B2AC54CEB28B9759B2D05F1012CBA8F
SHA-512:	86A11C9E4B59F2437180F56CAD44E69CB29B03B93983EA5E35CBCC5BDD40CFC424EE1EEF519B2E44D67623C79835AF92B4B089AC29890C046CD590C1F8BFA5 74
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Dosya'..MExit->Caption = 'Uygulamay. Kapat'..MOptions->Caption = 'Se.enekler'..MSettings->Caption = 'Ayarlar'..MLanguage->Caption = 'Dil'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Yard.m'..MAbout->Caption = 'Hakk.nda'....TabSheetSplit->Caption = 'PAR.ALA'..TabSheetCombine->Caption = 'B.RLE.T.R'....GroupBoxCombine->Caption = ' .lk par.ay. s.r.kleyin yada g.zat. kullan.n '..LabelFirstFile->Caption = '.lk Par.a:'..LabelOutput->Caption = 'Birle.tirme Ad.:'..LabelCombineFolder->Caption = '..kt. Klas.r. :'..LabelSplitFolder->Caption = '..kt. Klas.r.:'..ButtonCombine->Caption = 'B.RLE.T.R'..ButtonStopCombine->Caption = 'DUR'....GroupBoxSplit->Caption = ' B.lmek istedi.iniz dosyay.

C:\Program Files (x86)\Split Files\language\is-79U67.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2718
Entropy (8bit):	5.057121428169199
Encrypted:	false
SSDEEP:	48:HGPWFaxAA+sqKvFYLcunHh3QxXOBp1OB5r70h3CGRsJE0laDwXCqXH5wGF5JoCPa:HGPAPZBAJU1k7Jb245xVfUMG
MD5:	21B4D47F5D851271C89310C92777FB70
SHA1:	9D85FF8F7107CFAE3F31993FAF7F249591AFCB27
SHA-256:	D88AE9E292EBC4E56767892FD451E2E8278FCE776CAD689731EE7875748D55D7
SHA-512:	46F26B51D6959A36E33266887E39CB98E7E67880052DE8DE741CB93C90ED3B28C87A224CE710E6C698FE648ED8B062E73DEDC253A6C5A8362EB3EF2792AB4F F
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Archivo'..MExit->Caption = 'Salir'..MOptions->Caption = 'Options'..MSettings->Caption = 'Herramientas'..MLanguage->Caption = 'Elegir idioma'..MLangArabic->Caption = 'Arabe'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Holand.s'..MLangEnglish->Caption = 'Ingl.s'..MLangFrench->Caption = 'Franc.s'..MLangItalian->Caption = 'Italiano'..MLangRussian->Caption = 'Ruso'..MLangSpanish->Caption = 'Espa.ol'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Ayuda'..MAbout->Caption = 'Sobre programa'....TabSheetSplit->Caption = 'SEPARAR'..TabSheetCombine->Caption = 'JUNTAR'....GroupBoxCombine->Caption = ' Drag and drop una de las partes para juntar en la celda 'Primera Parte' o navegar '..LabelFirstFile->Caption = 'Primera Parte:'..LabelOutput->Caption = 'Nombre Archivo salida:'..LabelCombineFolder->Caption = 'Carpeta salida:'..LabelSplitFolder->Caption = 'Carpeta salida:'..ButtonCombine->Caption = 'JUNTAR'..ButtonStopCombine->Caption = 'PARAR'....

C:\Program Files (x86)\Split Files\language\is-7L4JB.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2345
Entropy (8bit):	5.847861612631974
Encrypted:	false
SSDEEP:	48:HGj2lE8qiTh7XJ9zHadtPTTD1n34q1jgun1ITq8K:HG5RDTln34qRgusK
MD5:	A5C9FEA89EFE8E2162BA477E8EA39B44
SHA1:	E6A2042C574D14786891F0C32F92C8292BBB4ACA
SHA-256:	8DDFB50DACA491296101BAB3DB9B77C7587127E684D9E22EFD6DC93F84A008FA
SHA-512:	3F7944F262717D308A1235982E741536DA6A4DF9ABEE4E2811E1151B53C3D31811EA3EB750ED39F347F7DF14AD20FF981C85CC2DA297BE745547B36D41B8FDB
Malicious:	false
Preview:	[Interface]....MFile->Caption = '...(&F)'..MExit->Caption = '.....'..MOptions->Caption = '...'..MSettings->Caption = '....'..MLanguage->Caption = '....'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = '.....'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = '....'..MAbout->Caption = '....'....TabSheetSplit->Caption = '...'..TabSheetCombine->Caption = '...'....GroupBoxCombine->Caption = ' ..... "....." .....'..LabelFirstFile->Caption = '.....'..LabelOutput->Caption = '.....'..LabelCombineFolder->Caption = '.....'..LabelSplitFolder->Caption = '.....'..ButtonCombine->Caption = '...'..ButtonStopCombine->Caption = '..'....GroupBoxSplit->Caption = ' ..... "....."..... '..LabelFileName->Caption = '.

C:\Program Files (x86)\Split Files\language\is-703KV.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2729
Entropy (8bit):	5.029883215699414
Encrypted:	false
SSDEEP:	48:HGgS7++sqMsmQYEJK7bHExsA9GZ1MTn6btlOWH6r3zvX5c9WYN:HGjUoR9GXML6RYWH6rDRdYN
MD5:	8AFE543CB6791AA250312EBA61BF7C13
SHA1:	BFD229D43BE86728A634055AD65860157C2671BD
SHA-256:	AF5BFB663E715C48C55E24BC3BEA30FCAA9BE8EAF35133FBB75D54C5735696AC
SHA-512:	5CF85F84DD6D363B2AAC720CF10C5289350EB706DC2BF5CA824CF220C3607CC7969CDD2F4B2912DC97C7BE50CEDC24A9A01AFC585CE84B6B8CB8141915393A2
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Termina programma'..MOptions->Caption = 'Options'..MSettings->Caption = 'Impostazioni'..MLanguage->Caption = 'Seleziona Lingua'..MLangArabic->Caption = 'Arabo'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Olandese'..MLangEnglish->Caption = 'Inglese'..MLangFrench->Caption = 'Francese'..MLangItalian->Caption = 'Italiano'..MLangRussian->Caption = 'Russo'..MLangSpanish->Caption = 'Spagnolo'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Aiuto'..MAbout->Caption = 'Informazioni'....TabSheetSplit->Caption = 'DIVIDI'..TabSheetCombine->Caption = 'UNISCI'....GroupBoxCombine->Caption = ' Drag and drop una delle parti da unire nella casella 'Prima Parte' o segui percorso '..LabelFirstFile->Caption = 'Prima Parte:'..LabelOutput->Caption = 'Nome File Uscita:'..LabelCombineFolder->Caption = 'Cartella Uscita:'..LabelSplitFolder->Caption = 'Cartella Uscita:'..ButtonCombine->Caption = 'UNISCI'..ButtonStopCombine->Caption = '

C:\Program Files (x86)\Split Files\language\is-8E2LT.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2687
Entropy (8bit):	5.051567814097503
Encrypted:	false
SSDEEP:	48:HGgXRVA+sqgh59WJlo4yvHIExBMHkWREHZDNbHBsBOtiSZls5crRMfiE:HGusSgEvMHfREHN9hsoiOUBiE
MD5:	D2471D35D833E2544D67365E015E6153
SHA1:	497EE8FF9519D025BD10C5AA15DDC34DFB1B334B
SHA-256:	4831DDBCFE327E2542F4565E7A948C5828D71003B8444723E1E11BA6BB43ACE7
SHA-512:	C82B30D604A679F87B8D0B1670A0D1607E25150FFCFD1C9E631241916BA93CEB5A33AFCAA9080149096ACA1913791384860F5699F2BB302B6CB190AF777EB3CE
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Programma Afsluiten'..MOptions->Caption = 'Options'..MSettings->Caption = 'Instellingen'..MLanguage->Caption = 'Kies Taal'..MLangArabic->Caption = 'Arabisch'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Nederlands'..MLangEnglish->Caption = 'Engels'..MLangFrench->Caption = 'Frans'..MLangItalian->Caption = 'Italiaans'..MLangRussian->Caption = 'Russisch'..MLangSpanish->Caption = 'Spaans'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Hulp'..MAbout->Caption = 'Info'....TabSheetSplit->Caption = 'SPLITSEN'..TabSheetCombine->Caption = 'HERENIGEN'....GroupBoxCombine->Caption = ' Drag and drop een van de te herenigen delen in 'Eerste Deel' of browse ernaartoe '..LabelFirstFile->Caption = 'Eerste Deel:'..LabelOutput->Caption = 'Output Bestandsnaam:'..LabelCombineFolder->Caption = 'Output Map:'..LabelSplitFolder->Caption = 'Output Map:'..ButtonCombine->Caption = 'HERENIGEN'..ButtonStopCombine->Caption = 'STOP'....Grou

C:\Program Files (x86)\Split Files\language\is-APJVT.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2594
Entropy (8bit):	5.044497576650396
Encrypted:	false
SSDEEP:	48:HGgb5l+sqiTh7XJ9oVHo1xx0GHLVQ4ZWGAtDAEQmUDcQdWym:HGdpa1jfHLVQ4AGAtWma8H
MD5:	76776746B3CFF1CBD5D56CD44CA2DEF5
SHA1:	2F2ECA50BD7F72232BE84291EF1A7956C24098CC
SHA-256:	EC647D30931F50607CF745D958AAF0367CCEAB9999346188255CFBFB22301EE3
SHA-512:	202436C708D4F34FFCCDC3D33841246C5CEE073AC270DA547C15F9E995A08D36AE4C00982283BF60D62363046BBEAA0125D59075E4629A9D1934039CBFB00BE
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&File'..MExit->Caption = 'Exit Application'..MOptions->Caption = 'Options'..MSettings->Caption = 'Settings'..MLanguage->Caption = 'Language'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Help'..MAbout->Caption = 'About'....TabSheetSplit->Caption = 'SPLIT'..TabSheetCombine->Caption = 'JOIN'....GroupBoxCombine->Caption = ' Drag and drop one of the files to join in the 'First Part' box or browse to it '..LabelFirstFile->Caption = 'First Part:'..LabelOutput->Caption = 'Output File Name:'..LabelCombineFolder->Caption = 'Output Folder:'..LabelSplitFolder->Caption = 'Output Folder:'..ButtonCombine->Caption = 'JOIN'..ButtonStopCombine->Caption = 'STOP'....GroupBoxSplit->Caption = ' Drag

C:\Program Files (x86)\Split Files\language\is-B20UO.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2607
Entropy (8bit):	5.234177949162883
Encrypted:	false
SSDEEP:	48:HGUyjEiB0w3l+sqiTh7XJ9UeHjIDt00AoB/nheSSMpSSSxPYe:HGpNBrkGIDt0qnheS9Sx
MD5:	E1271E0DDD609CD7F9C2367D32FEBE4B
SHA1:	0A420424F1FADE0BFF002E63AAD22B5E94B86CAC
SHA-256:	AEE6B1EDFFFCE507E2207C7E2AA36DA42B2AC54CEB28B9759B2D05F1012CBA8F
SHA-512:	86A11C9E4B59F2437180F56CAD44E69CB29B03B93983EA5E35CBCC5BDD40CFC424EE1EEF519B2E44D67623C79835AF92B4B089AC29890C046CD590C1F8BFA574
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Dosya'..MExit->Caption = 'Uygulamay. Kapat'..MOptions->Caption = 'Se.enekler'..MSettings->Caption = 'Ayarlar'..MLanguage->Caption = 'Dil'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption = 'English'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = 'Russian'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = 'Yard.m'..MAbout->Caption = 'Hakk.nda'....TabSheetSplit->Caption = 'PAR.ALA'..TabSheetCombine->Caption = 'B.RLE.T.R'....GroupBoxCombine->Caption = ' .lk par.ay. s.r.kleyin yada g.zat. kullan.n '..LabelFirstFile->Caption = '.lk Par.a:'..LabelOutput->Caption = 'Birle.tirme Ad.:'..LabelCombineFolder->Caption = '..kt. Klas.r. :'..LabelSplitFolder->Caption = '..kt. Klas.r.:'..ButtonCombine->Caption = 'B.RLE.T.R'..ButtonStopCombine->Caption = 'DUR'....GroupBoxSplit->Caption = ' B.lmek istedi.iniz dosyay.

C:\Program Files (x86)\Split Files\language\is-FBKGV.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2299
Entropy (8bit):	5.691502190790686
Encrypted:	false
SSDEEP:	48:HG9uhjkDYhqGQjsONHiHQgGU9dm6nclk6a1hg22mo6LD:HGnzLIQTUPmcclGsmogD
MD5:	F9F47FF3D866FFC4F38E315E41356E55
SHA1:	EFC313A99993B5FB8A454D4C5197C6F3965B5C89
SHA-256:	3A13CCE54190BF4A679D21F61466A0A18E9340287CAA1AA4EACB38C99C9D4957
SHA-512:	6EC1F1E19921C535A50254500ED01602DA74D3CC9E6DA8B5FC78D89255E42C5968BD294E56F584EE273630B9233C20CAFEBC906354CE393FE1CFFE91528F527A
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&....'..MExit->Caption = '.....'..MOptions->Caption = '.....'..MSettings->Caption = '.....'..MLanguage->Caption = '....'..MLangEnglish->Caption = '.....'..MLangRussian->Caption = '.....'..MLangArabic->Caption = '.....'..MLangChinese->Caption = '.....'..MLangDutch->Caption = '.....'..MLangFrench->Caption = '.....'..MLangItalian->Caption = '.....'..MLangSpanish->Caption = '.....'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption = '.....'..MAbout->Caption = '. ....'....TabSheetSplit->Caption = '.....'..TabSheetCombine->Caption = '.....'....GroupBoxCombine->Caption = ' .... '..LabelFirstFile->Caption = '1-. ....'..LabelOutput->Caption = '.....: '..LabelCombineFolder->Caption = '.....:'..ButtonCombine->Caption = '.....'..ButtonStopCombine->Caption = '....'....GroupBoxSplit->Caption = ' .... '..LabelSplitFolder->Caption = '.....:'..LabelFileName->Caption = '... .....:'..LabelFile

C:\Program Files (x86)\Split Files\language\is-JMARM.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2266
Entropy (8bit):	5.4593359267896355
Encrypted:	false
SSDEEP:	48:HG8il+sqirh7zJ9YTHskp1r4phFAqLNnK9h:HGkSkp1r4NTKf
MD5:	4ABA9765EB3555788F5706D87A9D2DCA
SHA1:	36C0895FBF9F99690CA55C54CC56310E24513113
SHA-256:	E99B943206594C04BC0383669D04D4F191A501F46D2474FED08B997F8020B433
SHA-512:	3498485635AFC548663715D22071611BAB10C707E8E24BE0B5143EE4A27727DA7D18A5E6959E3F6DD7D0F615DDFD50CE9FC5CE8AE6DDC5BEE287B5A00A817288
Malicious:	false
Preview:	[Interface]....MFile->Caption = '...'..MExit->Caption =' ....'..MOptions->Caption = 'Options'..MSettings->Caption =' .....'..MLanguage->Caption =' .....'..MLangArabic->Caption = 'Arabic'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Dutch'..MLangEnglish->Caption =' .....'..MLangFrench->Caption = 'French'..MLangItalian->Caption = 'Italian'..MLangRussian->Caption = '....'..MLangSpanish->Caption = 'Spanish'..MLangTurkish->Caption = 'Turkish'..MHelp->Caption =' .....'..MAbout->Caption =' ...'....TabSheetSplit->Caption = ' ... .'..TabSheetCombine->Caption = ' ...'....GroupBoxCombine->Caption =' ... .'..LabelFirstFile->Caption = '.... .....:'..LabelOutput->Caption = '... .....:'..LabelCombineFolder->Caption =' ....:'..LabelSplitFolder->Caption = '.... .....:'..ButtonCombine->Caption =' ...'..ButtonStopCombine->Caption = '....'....GroupBoxSplit->Caption = '... .....'..LabelFileName->Caption =' ....: '..LabelSplitFolder->Caption =' ....:'

C:\Program Files (x86)\Split Files\language\is-R2P47.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2507
Entropy (8bit):	5.040552699764577
Encrypted:	false
SSDEEP:	48:HGkOA+sq/W7Yve3EkHaBSDbSljMM+v1/D3H:HGb8hABSDbSJMBD
MD5:	336D33F55222F48FBA19EF0911732766
SHA1:	E17A78E3B48192361DB540B1E8C9D0548C9A9FFE
SHA-256:	0E955453FA27CED0D0521F0F960C7743C2090F06263D33EC8FA978B681123E0C
SHA-512:	67EC6B859BCDD66DA59CDB1DC1A4EACFBDA12C57699012EE1573DD88F5AAAB6288E1BD9015C862689F4A1A27E83B28C3A9C99B1895EDF4F47D6F94B0557CD C1F
Malicious:	false
Preview:	[Interface]....MFile->Caption = '&Fichier'..MExit->Caption = 'Quitter'..MOptions->Caption = 'Options'..MSettings->Caption = 'Settings'..MLanguage->Caption = 'La ngage'..MLangArabic->Caption = 'Arabe'..MLangChinese->Caption = 'Chinese'..MLangDutch->Caption = 'Flamand'..MLangEnglish->Caption = 'Englais'..MLangFrench- >Caption = 'Francais'..MLangItalian->Caption = 'Italien'..MLangRussian->Caption = 'Russe'..MLangSpanish->Caption = 'Espagnol'..MLangTurkish->Caption = 'Tur kish'..MHelp->Caption = 'Aide'..MAbout->Caption = 'A propos de ..'....TabSheetSplit->Caption = 'Scinder'..TabSheetCombine->Caption = 'Assembler'....GroupBoxComb ine->Caption = ' Faire glisser un des fichiers bloc . assembler ou rechercher le par ... '..LabelFirstFile->Caption = 'Premier Fichier:'..LabelOutput->Caption = 'Fichier de sortie: '..LabelCombineFolder->Caption = 'R.pertoire Dest.'..LabelSplitFolder->Caption = 'R.pertoire Dest.'..ButtonCombine->Caption = 'Assembler'..ButtonStopCombine- >Caption = 'Stop'....GroupBoxSpl

C:\Program Files (x86)\Split Files\unins000.dat	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	InnoSetup Log Split Files {215D64A9-0240-4952-9F4D-4D0A65391F2C}, version 0x2a, 4441 bytes, 927537\user, "C:\Program Files (x86)\Split Files"
Category:	dropped
Size (bytes):	4441
Entropy (8bit):	4.697339464808845
Encrypted:	false
SSDEEP:	48:kHED69yMlLBv8rD85pPmUlrBdcoINLFhqkLVO3471hD5WpPLDfDxLDvvDHD1DoDs:k7VZp8rD85pPmaoINFhqYOIhHeSk9WI
MD5:	35B9424FD3C02A2403561DA3E5D80E26
SHA1:	B944DC166C6A5BE77937B09B3E67175C422B4337
SHA-256:	B430632DBF9232BCC488DFD294297D1A197A832FB83333C6C601D7E41A587DBE
SHA-512:	1028FFD68185DA62C2A64B1D699733F89116AA8006CBB93B80609D675E02A80E9ACC2190E22F00CCE6B1F1168875354F855DBE750B67DC4DE8F2853FA9C8D0E
Malicious:	false
Preview:	Inno Setup Uninstall Log (b).....{215D64A9-0240-4952-9F4D-4D0A65391F2C}}.....Split Files..... .....*.....Y...%.....`....r.....C... .927537.user"C:\Program Files (x86)\Split Files...../...P.. .....R.IFPS.....BOOLEAN..... ..TWIZARDFORM....TWIZARDFORM.....TPASSWORDEDIT....TPASSWORDEDIT.....!MAIN....-1..'...dll:kernel32.dll.CreateFileA.....#. ..dll:kernel32.dll.WriteFile.....!...dll:kernel32.dll.CloseHandle.....!...dll:kernel32.dll.ExitProcess.....$...dll:User32.dll.GetSystemMet

C:\Program Files (x86)\Split Files\unins000.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	789258
Entropy (8bit):	6.369988626022893
Encrypted:	false
SSDEEP:	12288:EpmOmg1k2bfrP437QzH/A6A40lG77NzknuGyJOxOU:emt2bfrP437QzH/A6A7E7dVPUxOU
MD5:	D3BA43B9E1B3838F28AFC558F2991D5B
SHA1:	1132F1C76760281A591F7DF99D592283103FCC87
SHA-256:	1E95FE5D06884DF82D2BEAEDA09434ECAC2A347AEC5F03E71F20E39FB6C9E0E9
SHA-512:	870371843F59B91D75B6C4D4C637075235D25CF3ABB059B58E39F9CD2833533A8F434307E7AD1175FD45082D3B4E4F0ED79F303ED77DEF553587E2819C092022
Malicious:	**true**
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....4.....X.....@.....@.....%.....I.....@.....0..... .....CODE....I..... ..`DATA.....@...BSS.....p.....idata...%.....&.....@....tls..... .....rdata .....0.....@..P.reloc..t....@.....@..P.rsrc...I.....@..P.....@..P..... .....

C:\Program Files (x86)\Split Files\webpage.url (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	MS Windows 95 Internet shortcut text (URL=<http://www.altarsoft.com/split_files.shtml>), ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	97
Entropy (8bit):	5.12302231676258
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/0S4UEtSNM5LTJOBCBuQpQQXXy:HRYFVm/r4UEtSeVTJuZQplHy
MD5:	DCD6923B008121BFF4C7C0AA1206286E
SHA1:	AD4EF16A96A80C8EA5DBC5933229580BC6C332E0
SHA-256:	E1E01BFA5E2B5A117A627F7E9E861CF63D852A66BCE0DF88094D59CAF61E4376
SHA-512:	EC4A399EB38A1FA64DF8990708168F134ACD0CA793930E57C6D3A260A537B20DFD9F8B7232987F32EC1C1A7CEC7EC91F15A644A63D275104D96588FC3D354B5C
Malicious:	false
Preview:	[InternetShortcut]..URL=http://www.altarsoft.com/split_files.shtml..Modified=500425EA770BCC01B2..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fuckingdllENCR[1].dll

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	data
Category:	dropped
Size (bytes):	94224
Entropy (8bit):	**7.998072640845361**
Encrypted:	**true**
SSDEEP:	1536:NsbI9W6dHdtnEXOxZpPzIUcETzNtXofjmgGTeJduLLt+YBPoJTMRmNXg30:KWW6TZVz9PNtXo8M5OR0
MD5:	418619EA97671304AF80EC60F5A50B62
SHA1:	F11DCD709BDE2FC86EBBCCD66E1CE68A8A3F9CB6
SHA-256:	EB7ECE66C14849064F462DF4987D6D59073D812C44D81568429614581106E0F4
SHA-512:	F2E1AE47B5B0A5D3DD22DD6339E15FEE3D7F04EF03917AE2A7686E73E9F06FB95C8008038C018939BB9925F395D765C9690BF7874DC5E90BC2F77C1E730D3A00
Malicious:	false
Preview:	...mi...};...F".).T..'K;....O.Y0:.....3j.\.Ij.2R.P....C...q.|.2.....iR2W.F.C=MU.....H6...A.....@..O.c...M.x8...L..- ..b..|.C...Z}.w...I.a.aT...br,...6w#.j.P.li.=.....o.....S.{..R.....5....#;....-....b+..G(.>..Q.....iN{.+y...ZC.z3sE...T..2.J...3.9U.4&..P....."wI.....@....x%>..D..'z.^....^(.....NC.[[k.....V]G..)e.....`.....K/L.Ul..F.."..8$.Ad....:i.g..0.d...[...T"l.U.M.=.0...,..,ku.W,.....7`Q.Fi=w...u..:..Q-.R.}0...L.....n...t.nv.....z....e..I.C.....9.V.~1+[]..7...xQ.....$.L..o.eQ./.b..Z.....p].;i*)...#.b...%1.....@...G..[...../.c.Z.....G.:..n..E.i.O..o.U.B.Px....1{,a.....#k.dj..L4...}.d<.....Iyy.J..f.W..,^vV.Ao.K."+OX8!F...YP...u.-..Bik.[.u...&Wt..P...m....^ ..k~.....I..o.zMV.!s..h...{.n2;z...K..?S..-...eW...c.....-V.bg..9.I..g.x.g...}.'.5..(*P...J#..:.IS..D}.v.....jK9.LQF...oOhV...).h.v^-..F...<.....Vh.1....!...!...BYc..C?..D2.....2.K(..6....B....D..ay..=|....'....[1.~.YB:./...A`...=..F..K.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\count[1].htm

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\library[1].htm

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9

SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\library[1].htm

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\ping[1].htm

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	17
Entropy (8bit):	3.1751231351134614
Encrypted:	false
SSDEEP:	3:nCmxEl:Cmc
MD5:	064DB2A4C3D31A4DC6AA2538F3FE7377
SHA1:	8F877AE1873C88076D854425221E352CA4178DFA
SHA-256:	0A3EC2C4FC062D561F0DC989C6699E06FFF850BBDA7923F14F26135EF42107C0
SHA-512:	CA94BC1338FC283C3E5C427065C29BA32C5A12170782E18AA0292722826C5CB4C3B29A5134464FFEB67A77CD85D8E15715C17A049B7AD4E2C890E97385751BE
Malicious:	false
Preview:	UwUoooIIrwgh24uuU

C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_iscrypt.dll

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2560
Entropy (8bit):	2.8818118453929262
Encrypted:	false
SSDEEP:	24:e1GSgDIX566IIB6SXvVmMPUjvhBrDsqZ:SgDKRlVImgUNBsG
MD5:	A69559718AB506675E907FE49DEB71E9
SHA1:	BC8F404FFDB1960B50C12FF9413C893B56F2E36F
SHA-256:	2F6294F9AA09F59A574B5DCD33BE54E16B39377984F3D5658CDA44950FA0F8FC
SHA-512:	E52E0AA7FE3F79E36330C455D944653D449BA05B2F9ABEE0914A0910C3452CFA679A40441F9AC696B3CCF9445CBB85095747E86153402FC362BB30AC08249A63
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.c.W.c.W.c...>.T.c.W.b.V.c.R.<.V.c.R.?.V.c.R.9.V.c.RichW.c.....PE..L....b.@.....!..... ....@.....p ..}.... ..(.....0..... .....text..... ..`.rdata..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	4608
Entropy (8bit):	4.226829458093667
Encrypted:	false
SSDEEP:	48:6Q5EWGg69eR+Xl4SH8u09tmRJ/tE/wJI/tZ/P8sB1a:32Gel4NP9tK2/wGXhHa
MD5:	9E5BA8A0DB2AE3A955BEE397534D535D
SHA1:	EF08EF5FAC94F42C276E64765759F8BC71BF88CB
SHA-256:	08D2876741F4FD5EDFAE20054081CEF03E41C458AB1C5BBF095A288FA93627FA
SHA-512:	229A9C66080D59B7D2E1E651CFF9F00DB0CBDC08703E60D645651AF0664520CA143B088C71AD73813A500A33B48C63CA1795E2162B7620453935A4C26DB96B2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o4...g...g...g).zg...g...g...g.&lg...g.&yg...gRich...g.....PE..d... 9TTB.....#.....@.....P.....!..x.....@..H..... ....text..... ..`.rdata..... .....@..@.data...,....0.....@....pdata..H....@.....@..@.....

C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_shfoldr.dll

Process:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	23312
Entropy (8bit):	4.596242908851566
Encrypted:	false
SSDEEP:	384:+Vm08QoKkiWZ76UJuP71W55iWHHoSHigH2euwsHTGHVb+VHHmnH+aHjHqLHxmoq1:2m08QotiCjJuPGw4
MD5:	92DC6EF532FBB4A5C3201469A5B5EB63
SHA1:	3E89FF837147C16B4E41C30D6C796374E0B8E62C
SHA-256:	9884E9D1B4F8A873CCBD81F8AD0AE257776D2348D027D811A56475E028360D87
SHA-512:	9908E573921D5DBC3454A1C0A6C969AB8A81CC2E8B5385391D46B1A738FB06A76AA3282E0E58D0D2FFA6F27C85668CD5178E1500B8A39B1BBAE04366AE6A86 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....IzJ^..$...$...$...%.".$.T87...$.[."...$...$...$.Rich..$.....PE ..L....\;.....#.... ...4.....'.....0.....q.....k...l)..<....@.../.....p..T.....text... {..... ....`.data...\....0.....&.....@....rsrc..../...@...0...(.....@..@.reloc.....p.....X.....@..B.....

C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	778752
Entropy (8bit):	6.357908612813808
Encrypted:	false
SSDEEP:	12288:cpmOmg1k2bfrP437QzH/A6A40lG77NzknuGyJOxOG:2mt2bfrP437QzH/A6A7E7dVPUxOG
MD5:	E8176050192FBB976D70238E3C121F4C
SHA1:	2F1FD24EFE1F3F3FEE775CC3F5255B32F8880900
SHA-256:	AB4FE42A7B708DDB648BB2088216FF47B877AE599FD52FF50359FC1DB8E11EF7
SHA-512:	27EDF7A71C6546F1AB52E7EF97E404975DDD237D6C2D1038D24A49EAB724971884510F00F427C713ADB105857A0B12C7D57CA1CA1C70A6CEFED4BE619C345F C
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....4.....X.....@.....@.....%.....l.....@.....0..... .....CODE....l..... ..`DATA.....@...BSS.....p.....idata...%.....&.....@....tls..... .....rdata .....0.....@..P.reloc..t....@.....@..P.rsrc...l.....@..P.....@..P.....

C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\KN38AzDG.exe

Process:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	6.20389308045717

Encrypted:	false
SSDEEP:	1536:bvUpDLxyxA14o3/M238r6+XfHAgbqmE8MpKdwuasZLUM7DsWIXcdyZgfmi:WDLZKa/MtXfHAgbqmEtxsfmyZgfmi
MD5:	3FB36CB0B7172E5298D2992D42984D06
SHA1:	439827777DF4A337CBB9FA4A4640D0D3FA1738B7
SHA-256:	27AE813CEFF8AA56E9FA68C8E50BB1C6C4A01636015EAC4BD8BF444AFB7020D6
SHA-512:	6B39CB32D77200209A25080AC92BC71B1F468E2946B651023793F3585EE6034ADC70924DBD751CF4A51B5E71377854F1AB43C2DD287D4837E7B544FF886F470C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.....Rich..... .....PE..L....?c.....~....._.....@.....`.....@.....(....@.....P.....8.....@..... .....text..... ..`.rdata..dY.....Z.....@..@.data..... .....@....rsrc.....@.....@..@.reloc.....P.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, InnoSetup self-extracting archive
Entropy (8bit):	7.9318000564899
TrID:	• Win32 Executable (generic) a (10002005/4) 98.88% • Inno Setup installer (109748/4) 1.08% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	2094367
MD5:	e0f8085c7cb8eb9cf1c263bb12cfc6df
SHA1:	a109ebcf251a1e69923c60330994190e40ab466c
SHA256:	a28fb531e91695081ac9a3a08bd9be333462f84a3b1e9de81dda94869fd3d32a
SHA512:	11f39030a9e5f5a095c85aa087fe949ed7e83e1a53a3df487baab09a38d5e744150a8d4e7b34eaec28678561861e640cb34231b893a7f38751f143d0ea1305d1
SSDEEP:	49152:XirWlOmsJ8sSNd3HEKBqd0yLaS1vNf+8UkqBx:XiClONJu3HEKBqd0yLaGFfvqH
TLSH:	9FA51232715472EEFCE369B0584F426D66236FB3A1A87E2E310A37365A61331F115F1A
File Content Preview:	MZP.....@.....Inno.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b8ba6cc880e1f204

Static PE Info

General

Entrypoint:	0x409820
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	e92b45c54aa05ec107d5ef90662e6b33

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
add esp, FFFFFFD4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-1Ch], eax
call 00007FC5F939961Bh
call 00007FC5F939A8C6h
call 00007FC5F939CAC9h
call 00007FC5F939CB10h
call 00007FC5F939F107h
call 00007FC5F939F26Eh
mov esi, 0040BDE0h
xor eax, eax
push ebp
push 00409F05h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 00409EBBh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [0040B014h]
call 00007FC5F939FC5Fh
call 00007FC5F939F81Eh
lea edx, dword ptr [ebp-10h]
xor eax, eax
call 00007FC5F939CF84h
mov edx, dword ptr [ebp-10h]
mov eax, 0040BDD4h
call 00007FC5F93996C7h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [0040BDD4h]
mov dl, 01h
mov eax, 00407158h
call 00007FC5F939D66Bh
mov dword ptr [0040BDD8h], eax
xor edx, edx
push ebp
push 00409E99h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
lea edx, dword ptr [ebp-18h]
mov eax, dword ptr [0040BDD8h]
call 00007FC5F939D767h
mov ebx, dword ptr [ebp-18h]
mov edx, 00000030h
mov eax, dword ptr [0040BDD8h]
call 00007FC5F939D8A1h
mov edx, esi
mov ecx, 0000000Ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc000	0x8f0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x1f558	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf000	0x0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xe000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x8f94	0x9000	False	0.6195203993055556	data	6.591638965772245	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xa000	0x248	0x400	False	0.306640625	data	2.7093261929320986	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xb000	0xe64	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xc000	0x8f0	0xa00	False	0.3953125	data	4.294209855544776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xd000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xe000	0x18	0x200	False	0.052734375	data	0.1991075177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xf000	0x884	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x1f558	0x1f600	False	0.37483659113545814	data	4.9335056025106585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1039c	0x51f3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x15590	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 0	English	United States
RT_ICON	0x25db8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 0	English	United States
RT_ICON	0x29fe0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	English	United States
RT_ICON	0x2c588	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	English	United States
RT_ICON	0x2d630	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	English	United States
RT_ICON	0x2dfb8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	English	United States
RT_STRING	0x2e420	0x2f2	data		
RT_STRING	0x2e714	0x30c	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x2ea20	0x2ce	data		
RT_STRING	0x2ecf0	0x68	data		
RT_STRING	0x2ed58	0xb4	data		
RT_STRING	0x2ee0c	0xae	data		
RT_GROUP_ICON	0x2eebc	0x68	data	English	United States
RT_VERSION	0x2ef24	0x3a8	data	English	United States
RT_MANIFEST	0x2f2cc	0x289	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, WideCharToMultiByte, TlsSetValue, TlsGetValue, MultiByteToWideChar, GetModuleHandleA, GetLastError, GetCommandLineA, WriteFile, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetSystemTime, GetFileType, ExitProcess, CreateFileA, CloseHandle
user32.dll	MessageBoxA
oleaut32.dll	VariantChangeTypeEx, VariantCopyInd, VariantClear, SysStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey, OpenProcessToken, LookupPrivilegeValueA
kernel32.dll	WriteFile, VirtualQuery, VirtualProtect, VirtualFree, VirtualAlloc, Sleep, SetLastError, SetFilePointer, SetErrorMode, SetEndOfFile, RemoveDirectoryA, ReadFile, LoadLibraryA, IsDBCSLeadByte, GetWindowsDirectoryA, GetVersionExA, GetUserDefaultLangID, GetSystemInfo, GetSystemDefaultLCID, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetFileSize, GetFileAttributesA, GetExitCodeProcess, GetEnvironmentVariableA, GetCurrentProcess, GetCommandLineA, InterlockedExchange, FormatMessageA, DeleteFileA, CreateProcessA, CreateFileA, CreateDirectoryA, CloseHandle
user32.dll	TranslateMessage, SetWindowLongA, PeekMessageA, MsgWaitForMultipleObjects, MessageBoxA, LoadStringA, ExitWindowsEx, DispatchMessageA, DestroyWindow, CreateWindowExA, CallWindowProcA, CharPrevA
comctl32.dll	InitCommonControls
advapi32.dll	AdjustTokenPrivileges

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
107.182.129.235192.168.2.580497062852925 01/05/23-08:47:10.017687	TCP	2852925	ETPRO TROJAN GCleaner Downloader - Payload Response	80	49706	107.182.129.235	192.168.2.5
192.168.2.545.139.105.171497058020419200 01/05/23-08:47:09.800462	TCP	2041920	ET TROJAN GCleaner Downloader Activity M8	49705	80	192.168.2.5	45.139.105.171
192.168.2.5107.182.129.23549706802852981 01/05/23-08:47:09.990287	TCP	2852981	ETPRO TROJAN Win32/Fabookie.ek CnC Request M3 (GET)	49706	80	192.168.2.5	107.182.129.235
192.168.2.5107.182.129.23549706802852980 01/05/23-08:47:09.925610	TCP	2852980	ETPRO TROJAN Win32/Fabookie.ek CnC Request M1 (GET)	49706	80	192.168.2.5	107.182.129.235

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:09.771787882 CET	49705	80	192.168.2.5	45.139.105.171
Jan 5, 2023 08:47:09.799809933 CET	80	49705	45.139.105.171	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:09.799943924 CET	49705	80	192.168.2.5	45.139.105.171
Jan 5, 2023 08:47:09.800462008 CET	49705	80	192.168.2.5	45.139.105.171
Jan 5, 2023 08:47:09.827680111 CET	80	49705	45.139.105.171	192.168.2.5
Jan 5, 2023 08:47:09.836986065 CET	80	49705	45.139.105.171	192.168.2.5
Jan 5, 2023 08:47:09.837126970 CET	49705	80	192.168.2.5	45.139.105.171
Jan 5, 2023 08:47:09.897756100 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:09.924849987 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:09.925086021 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:09.925610065 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:09.952578068 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:09.952980042 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:09.953092098 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:09.990287066 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.017482042 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017687082 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017736912 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017781973 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017790079 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.017816067 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017849922 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017884970 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017935991 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.017944098 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.017982960 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.017983913 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.018007994 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.018030882 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.018032074 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.018080950 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.018090963 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.018136024 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045037031 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045104027 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045137882 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045152903 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045172930 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045201063 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045212984 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045250893 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045254946 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045298100 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045305014 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045345068 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045346975 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045392990 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045394897 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045439959 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045439959 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045488119 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045490026 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045533895 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045536995 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045581102 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045583010 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045628071 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045628071 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045677900 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045680046 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045723915 CET	80	49706	107.182.129.235	192.168.2.5

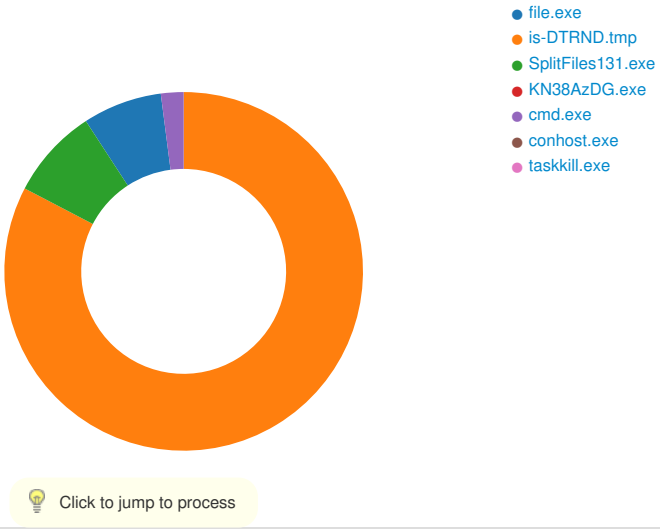
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:10.045728922 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045772076 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045772076 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045819998 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045825005 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045865059 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045869112 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045916080 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045917034 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.045964003 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.045968056 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.046013117 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.072890043 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073029995 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073051929 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073117971 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073136091 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073177099 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073189974 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073235989 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073251963 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073295116 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073312998 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073354006 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073359966 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073417902 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073420048 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073477030 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073477030 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073535919 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073538065 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073592901 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073592901 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073649883 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073651075 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073707104 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073707104 CET	80	49706	107.182.129.235	192.168.2.5
Jan 5, 2023 08:47:10.073762894 CET	49706	80	192.168.2.5	107.182.129.235
Jan 5, 2023 08:47:10.073765039 CET	80	49706	107.182.129.235	192.168.2.5

HTTP Request Dependency Graph

- 45.139.105.171
- 107.182.129.235
- 171.22.30.106

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 2148, Parent PID: 3324

General

Target ID:	1
Start time:	08:47:00
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	2094367 bytes
MD5 hash:	E0F8085C7CB8EB9CF1C263BB12CFC6DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: is-DTRND.tmp PID: 6048, Parent PID: 2148

General

Target ID:	4
Start time:	08:47:01
Start date:	05/01/2023
Path:	C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp" /SL4 $902D6 "C:\Users\user\Desktop\file.exe" 1818498 170496
Imagebase:	0x400000
File size:	778752 bytes
MD5 hash:	E8176050192FBB976D70238E3C121F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	45244F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4722F4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_shfoldr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_iscrypt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Program Files (x86)\Split Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451362	CreateDirectoryA
C:\Program Files (x86)\Split Files\unins000.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	46CD1E	CreateFileA
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\is-6QN6Q.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451362	CreateDirectoryA
C:\Program Files (x86)\Split Files\language\is-JMARM.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-7L4JB.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-8E2LT.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-APJVT.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-R2P47.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-7O3KV.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-FBKGV.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-79U67.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\language\is-B20UO.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\is-UJJ0L.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\is-3OAED.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\Split Files\is-JSP8F.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	C:\Program Files (x86)\Split Files\unins000.exe	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\is-6QN6Q.tmp	C:\Program Files (x86)\Split Files\SplitFiles131.exe	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-JMARM.tmp	C:\Program Files (x86)\Split Files\language\Arabic.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-7L4JB.tmp	C:\Program Files (x86)\Split Files\language\Chinese.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-8E2LT.tmp	C:\Program Files (x86)\Split Files\language\Dutch.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-APJVT.tmp	C:\Program Files (x86)\Split Files\language\English.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-R2P47.tmp	C:\Program Files (x86)\Split Files\language\French.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-7O3KV.tmp	C:\Program Files (x86)\Split Files\language\Italian.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-FBKGV.tmp	C:\Program Files (x86)\Split Files\language\Russian.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-79U67.tmp	C:\Program Files (x86)\Split Files\language\Spanish.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\language\is-B20UO.tmp	C:\Program Files (x86)\Split Files\language\Turkish.ini	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\is-UJJ0L.tmp	C:\Program Files (x86)\Split Files\ReadMe - EN.txt	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\is-3OAED.tmp	C:\Program Files (x86)\Split Files\ReadMe - RU.txt	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\Split Files\is-JSP8F.tmp	C:\Program Files (x86)\Split Files\webpage.url	success or wait	1	4517E3	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_setup64.tmp	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd fd 6f 34 fd fd 01 67 fd fd 01 67 fd fd 01 67 29 1a 7a 67 fd fd 01 67 fd fd 00 67 fd fd 01 67 0b 26 6c 67 fd fd 01 67 0b 26 79 67 fd fd 01 67 52 69 63 68 fd fd 01 67 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 04 00 39 54 54 42 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0c 02 00 00 00 00 00 fd 15 00 00 00 10 00 00 00 00 40 00 00 00 00 00 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$o4ggg)zgggg&lg g&yggRichgPEd9TTB#@	success or wait	1	406FBD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_isetup_shfoldr.dll	0	23312	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 49 7a 4a 5e 0d 1b 24 0d 0d 1b 24 0d 0d 1b 24 0d 0d 1b 25 0d 22 1b 24 0d 54 38 37 0d 0b 1b 24 0d 5b 13 22 0d 0c 1b 24 0d 0d 1b 24 0d 0c 1b 24 0d 52 69 63 68 0d 1b 24 0d 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 50 45 00 00 4c 01 04 00 fd fd 5c 3b 00 00 00 00 00 00 00 00 fd 00 06 23 0b 01 05 0c 00 20 00 00 00 34 00 00 00 00 00 00 fd 27 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$IzJ^$$$%"$T87$["$$$Rich$PEL\;# 4'	success or wait	1	406FBD	WriteFile
C:\Users\user\AppData\Local\Temp\is-D5FV2.tmp_iscrypt.dll	0	2560	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 13 fd 0d fd 57 fd 63 fd 57 fd 63 fd 57 fd 63 fd fd fd 3e fd 54 fd 63 fd 57 fd 62 fd 56 fd 63 fd 52 fd 3c fd 56 fd 63 fd 52 fd 3f fd 56 fd 63 fd 52 fd 39 fd 56 fd 63 fd 52 69 63 68 57 fd 63 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 62 fd 40 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 07 0a 00 02 00 00 00 04 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$WcWcWc>TcWbVcR<VcR?VcR9VcRichWcPELb@!	success or wait	1	406FBD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	0	65536	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 6e 55 6e 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@InUn!L!This program must be run under Win32$7	success or wait	12	45013C	WriteFile
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	48	4	49 6e 55 6e	InUn	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	778752	10454	49 6e 6e 6f 20 53 65 74 75 70 20 4d 65 73 73 61 67 65 73 20 28 35 2e 31 2e 30 29 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 fd 00 00 00 fd 28 00 00 29 fd fd fd fd 26 32 fd 26 41 62 6f 75 74 20 53 65 74 75 70 2e 2e 2e 00 25 31 20 76 65 72 73 69 6f 6e 20 25 32 0d 0a 25 33 0d 0a 0d 0a 25 31 20 68 6f 6d 65 20 70 61 67 65 3a 0d 0a 25 34 00 00 41 62 6f 75 74 20 53 65 74 75 70 00 59 6f 75 20 6d 75 73 74 20 62 65 20 6c 6f 67 67 65 64 20 69 6e 20 61 73 20 61 6e 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 77 68 65 6e 20 69 6e 73 74 61 6c 6c 69 6e 67 20 74 68 69 73 20 70 72 6f 67 72 61 6d 2e 00 46 6f 6c 64 65 72 20 6e 61 6d 65 73 20 63 61 6e 6e 6f 74 20 69 6e 63 6c 75 64 65 20 61 6e 79 20 6f 66 20	Inno Setup Messages (5.1.0)()&2&About Setup...%1 version %2%3%1 home page:%4About SetupYou must be logged in as an administrator when installing this program.Folder names cannot include any of	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\Split Files\is-AGVDF.tmp	789250	8	49 4d 73 67 00 fd 0b 00	IMsg	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\is-6QN6Q.tmp	0	65536	0a 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 06 00 fd 7e fd 63 00 00 00 00 00 00 00 00 fd 00 5f 02 0b 01 05 14 00 fd 06 00 00 fd fd 00 00 00 00 00 fd fd 06 00 00 10 00 00 00 00 07 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 01 00 00 00 00 00 04 00 01 00 00 00 00 00 00 50 15 01 00 10 00 00 5d 6d 35 00 02 00 00 00 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	Z@!L!This program cannot be run in DOS mode.$PEL~c_@P]m5	success or wait	54	45013C	WriteFile
C:\Program Files (x86)\Split Files\language\is-JMARM.tmp	0	2266	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 27 20 fd fd fd fd 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 27 20 fd fd fd fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 27 20 fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 69 63 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 44 75 74 63	[Interface]MFile->Caption = ''MExit->Caption =' 'MOptions->Caption = 'Options'MSettings->Caption =' 'MLanguage->Caption =' 'MLangArabic->Caption = 'Arabic'MLangChinese->Caption = ' Chinese'MLangDutch->Caption = 'Dutc	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\language\is-7L4JB.tmp	0	2345	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd 3c fd 28 26 46 29 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd f3 fd fd fd fd fd 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 61 fd fd 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 69 63 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 44 75 74 63	[Interface]MFile->Caption = '(&F)'MExit->Caption = ''MOptions->Caption = ''MSettings->Caption = ''MLanguage->Caption = ''MLangArabic->Caption = 'Arabic'MLangChinese->Caption = ''MLangDutch->Caption = 'Dutc	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\language\is-8E2LT.tmp	0	2687	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 46 69 6c 65 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 50 72 6f 67 72 61 6d 6d 61 20 41 66 73 6c 75 69 74 65 6e 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 49 6e 73 74 65 6c 6c 69 6e 67 65 6e 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4b 69 65 73 20 54 61 61 6c 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 69 73 63 68 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c	[Interface]MFile->Caption = '&File'MExit->Caption = 'Programma Afsluiten'MOptions->Caption = 'Options'MSettings->Caption = 'Instellingen'MLanguage->Caption = 'Kies Taal'MLangArabic->Caption = 'Arabisch'MLangChinese->Caption = 'Chinese'ML	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\language\is-APJVT.tmp	0	2594	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 46 69 6c 65 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 45 78 69 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 53 65 74 74 69 6e 67 73 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4c 61 6e 67 75 61 67 65 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 69 63 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e	[Interface]MFile->Caption = '&File'MExit->Caption = 'Exit Application'MOptions->Caption = 'Options'MSettings->Caption = 'Settings'MLanguage->Caption = 'Language'MLangArabic->Caption = 'Arabic'MLangChinese->Caption = 'Chinese'MLangDutch->	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\language\is-R2P47.tmp	0	2507	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 46 69 63 68 69 65 72 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 51 75 69 74 74 65 72 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 53 65 74 74 69 6e 67 73 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4c 61 6e 67 61 67 65 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 65 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e 43 61 70 74 69 6f 6e 20	[Interface]MFile->Caption = '&Fichier'MExit->Caption = 'Quitter'MOptions->Caption = 'Options'MSettings->Caption = 'Settings'MLanguage->Caption = 'Langage'MLangArabic->Caption = 'Arabe'MLangChinese->Caption = 'Chinese'MLangDutch->Caption	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\language\is-7O3KV.tmp	0	2729	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 46 69 6c 65 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 54 65 72 6d 69 6e 61 20 70 72 6f 67 72 61 6d 6d 61 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 49 6d 70 6f 73 74 61 7a 69 6f 6e 69 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 53 65 6c 65 7a 69 6f 6e 61 20 4c 69 6e 67 75 61 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 6f 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a	[Interface]MFile->Caption = '&File'MExit->Caption = 'Termina programma'MOptions->Caption = 'Options'MSettings->Caption = 'Impostazioni'MLanguage->Caption = 'Seleziona Lingua'MLangArabic->Caption = 'Arabo'MLangChinese->Caption = 'Chinese'	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\language\is-FBKGV.tmp	0	2299	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 fd fd fd fd 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd fd fd 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 45 6e 67 6c 69 73 68 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 52 75 73 73 69 61 6e 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 fd fd fd fd fd fd 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20	[Interface]MFile->Caption = '&'MExit->Caption = ''MOptions->Caption = ''MSettings->Caption = ''MLanguage->Caption = ''MLangEnglish->Caption = ''MLangRussian->Caption = ''MLangArabic->Caption =	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\language\is-79U67.tmp	0	2718	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 41 72 63 68 69 76 6f 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 53 61 6c 69 72 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 4f 70 74 69 6f 6e 73 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 48 65 72 72 61 6d 69 65 6e 74 61 73 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 45 6c 65 67 69 72 20 69 64 69 6f 6d 61 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 65 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e	[Interface]MFile->Caption = '&Archivo'MExit->Caption = 'Salir'MOptions->Caption = 'Options'MSettings->Caption = 'Herramientas'MLanguage->Caption = 'Elegir idioma'MLangArabic->Caption = 'Arabe'MLangChinese->Caption = 'Chinese'MLangDutch->	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\language\is-B20UO.tmp	0	2607	5b 49 6e 74 65 72 66 61 63 65 5d 0d 0a 0d 0a 4d 46 69 6c 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 26 44 6f 73 79 61 27 0d 0a 4d 45 78 69 74 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 55 79 67 75 6c 61 6d 61 79 fd 20 4b 61 70 61 74 27 0d 0a 4d 4f 70 74 69 6f 6e 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 53 65 fd 65 6e 65 6b 6c 65 72 27 0d 0a 4d 53 65 74 74 69 6e 67 73 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 79 61 72 6c 61 72 27 0d 0a 4d 4c 61 6e 67 75 61 67 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 44 69 6c 27 0d 0a 4d 4c 61 6e 67 41 72 61 62 69 63 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 41 72 61 62 69 63 27 0d 0a 4d 4c 61 6e 67 43 68 69 6e 65 73 65 2d 3e 43 61 70 74 69 6f 6e 20 3d 20 27 43 68 69 6e 65 73 65 27 0d 0a 4d 4c 61 6e 67 44 75 74 63 68 2d 3e 43 61	[Interface]MFile->Caption = '&Dosya'MExit->Caption = 'Uygulamay Kapat'MOptions->Caption = 'Seenekler'MSettings->Caption = 'Ayarlar'MLanguage->Caption = 'Dil'MLangArabic->Caption = 'Arabic'MLangChinese->Caption = 'Chinese'MLangDutch->Ca	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\is-UJJ0L.tmp	0	2193	53 70 6c 69 74 20 46 69 6c 65 73 20 31 2e 37 32 0d 0a 0d 0a 43 6f 6e 74 65 6e 74 73 3a 0d 0a 0d 0a 31 2e 20 44 65 73 63 72 69 70 74 69 6f 6e 2e 0d 0a 32 2e 20 48 69 73 74 6f 72 79 2e 0d 0a 33 2e 20 4c 6f 63 61 6c 69 7a 61 74 69 6f 6e 2e 0d 0a 34 2e 20 43 6f 6e 74 61 63 74 73 2e 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 0d 0a 31 2e 20 44 65 73 63 72 69 70 74 69 6f 6e 2e 0d 0a 0d 0a 46 61 73 74 20 61 6e 64 20 65 61 73 79 20 66 69 6c 65 20 73 70 6c 69 74 74 65 72 20 61 6e 64 20 6a 6f 69 6e 65 72 2e 0d 0a 53 70 6c 69 74 20 66 69 6c 65 73 20 62 79 20 70 61 72 74 73 20 73 69 7a 65 20 6f 72 20	Split Files 1.72Contents:1. Description.2. History.3. Localization.4. Contacts.- ------------------------------------- --------------------------1. Descr<wbr>iption.Fast and easy file splitter and joiner.Split files by parts size or	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\is-3OAED.tmp	0	2942	53 70 6c 69 74 20 46 69 6c 65 73 20 31 2e 37 32 0d 0a 0d 0a fd fd fd fd fd fd fd fd fd 3a 0d 0a 0d 0a 31 2e 20 fd fd fd fd fd fd fd fd 2e 0d 0a 32 2e 20 fd fd fd fd fd fd fd 2e 0d 0a 33 2e 20 fd fd fd fd fd fd fd 2e 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 0d 0a 31 2e 20 fd fd fd fd fd fd fd fd 2e 0d 0a 0d 0a fd fd fd fd fd fd fd fd fd 20 fd fd fd fd fd fd fd fd fd fd fd fd 20 fd fd fd 20 fd fd fd fd fd fd fd fd fd 20 fd fd fd fd fd fd 20 fd fd 20 fd fd fd fd fd 20 fd fd fd fd fd fd 20 fd fd fd fd fd fd 20 fd 20 fd fd fd fd fd fd fd fd fd fd fd 20 fd fd 20 fd fd fd fd fd	Split Files 1.72:1. .2. .3. .- ------------------------------------- --------------------------1. .	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\Split Files\is-JSP8F.tmp	0	97	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 74 61 72 73 6f 66 74 2e 63 6f 6d 2f 73 70 6c 69 74 5f 66 69 6c 65 73 2e 73 68 74 6d 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 35 30 30 34 32 35 45 41 37 37 30 42 43 43 30 31 42 32 0d 0a	[InternetShortcut]URL=http://www.altarsoft.com/split_files.shtmlModified=500425EA770BCC01B2	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\unins000.dat	0	448	49 6e 6e 6f 20 53 65 74 75 70 20 55 6e 69 6e 73 74 61 6c 6c 20 4c 6f 67 20 28 62 29 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 7b 32 31 35 44 36 34 41 39 2d 30 32 34 30 2d 34 39 35 32 2d 39 46 34 44 2d 34 44 30 41 36 35 33 39 31 46 32 43 7d 7d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 70 6c 69 74 20 46 69 6c 65 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Inno Setup Uninstall Log (b){215D64A9-0240-4952-9F4D-4D0A65391F2C}}Split Files	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\Split Files\unins000.dat	448	12	fd 0f 00 00 72 fd fd fd 0a fd fd fd	r	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\Split Files\SplitFiles131.exe	0	1	4d	M	success or wait	1	44149E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp	unknown	4	success or wait	1	45002C	ReadFile
C:\Users\user\Desktop\file.exe	unknown	64	success or wait	1	45002C	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	45002C	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	45002C	ReadFile
C:\Users\user\AppData\Local\Temp\is-LMEP0.tmp\is-DTRND.tmp	unknown	65536	success or wait	12	45002C	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	13	45002C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Avepoint Software	success or wait	1	42DCAD	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Avepoint Software\SplitFiles131	success or wait	1	42DCAD	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	success or wait	1	42DCAD	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Avepoint Software\SplitFiles131	Language	unicode	english	success or wait	1	46B909	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	Inno Setup: Setup Version	unicode	5.1.3-beta	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	Inno Setup: App Path	unicode	C:\Program Files (x86)\Split Files	success or wait	1	4679F8	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	InstallLocation	unicode	C:\Program Files (x86)\Split Files\	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	Inno Setup: Icon Group	unicode	Split Files	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	Inno Setup: User	unicode	alfons	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	DisplayName	unicode	Split Files 4.131	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	UninstallString	unicode	"C:\Program Files (x86)\Split Files\unins000.exe"	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	QuietUninstallString	unicode	"C:\Program Files (x86)\Split Files\unins000.exe" /SILENT	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	DisplayVersion	unicode	4.131	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	Publisher	unicode	Kksus Averun	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	NoModify	dword	1	success or wait	1	467A58	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{215D64A9-0240-4952-9F4D-4D0A65391F2C}}_is1	NoRepair	dword	1	success or wait	1	467A58	RegSetValueExA

Analysis Process: SplitFiles131.exe PID: **4360**, Parent PID: **6048**

General

Target ID:	5
Start time:	08:47:04
Start date:	05/01/2023
Path:	C:\Program Files (x86)\Split Files\SplitFiles131.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Split Files\SplitFiles131.exe"
Imagebase:	0x400000
File size:	3491315 bytes
MD5 hash:	361518D6CC3C25EEC2DFC1DE82B055B2
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000005.00000002.371399176.0000000000400000.00000040.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000005.00000002.372442187.00000000030C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000005.00000002.372529330.0000000003340000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	406855	CreateDirectoryA
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\KN38AzDG.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	42839A	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\KN38AzDG.exe	0	73728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 b0 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b fd fd fd fd fd fd fd 24 fd fd fd fd 24 fd fd fd fd fd 24 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2e fd fd fd fd fd fd 2e fd 39 fd fd fd fd 2e fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$..9.Rich	success or wait	1	421174	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\count[1].htm	0	1	30	0	success or wait	1	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\ping[1].htm	0	17	55 77 55 6f 6f 6f 49 49 72 77 67 68 32 34 75 75 55	UwUoooIIrwgh24uuU	success or wait	1	401BDA	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fuckingdllENCR[1].dll	0	1000	fd 67 0b 6d 69 fd 02 fd 7d 3b fd 18 fd 46 22 fd 29 fd 54 fd 11 27 4b 3b 1b fd fd fd 4f fd 59 30 3a fd fd fd fd 19 33 6a fd 5c 17 49 6a fd 32 52 49 50 17 fd 06 fd 43 07 19 fd 71 fd 7c fd 32 fd 0e fd fd fd 69 52 32 57 fd 46 2b 43 3d 4d 55 fd fd 16 cb fd fd 48 36 fd fd fd 41 fd 1a fd fd fd 40 7f fd 4f fd 63 1a fd fd 4d fd 78 38 94 fd fd 4c fd fd 2d 20 48 fd 62 fd fd 7c 12 43 fd fd a4 5a 7d fd 77 d4 2e fd 6c 1a 61 fd 61 54 fd fd a5 62 72 2c 19 fd 18 36 77 23 06 6a fd 50 4c 6c 69 fd 3d fd fd fd 1b 0e fd 6f fd 1e fd fd fd fd fd 53 fd 7b fd fd 52 fd fd fd fd 2e fd fd fd 35 60 15 fd fd 23 3b fd 14 fd 04 2d fd fd fd fd 62 2b 19 fd 47 28 fd 3e fd 02 51 05 fd fd fd fd 69 4e 7b fd 2b 79 0c 1d fd 5a 43	mi};F")T'K;OY0:3j\lj2RPCq|2iR2 WFC=MUH6A@OcMx8L-b|CZ}w.laaTb r,6w#jPli=oS{R.5#;-b+G(>QiN{+yZC	success or wait	92	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\library[1].htm	0	1	30	0	success or wait	6	100010BA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\library[1].htm	0	1	30	0	success or wait	5	100010BA	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: KN38AzDG.exe PID: **1960**, Parent PID: **4360**

General

Target ID:	6
Start time:	08:47:08
Start date:	05/01/2023
Path:	C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\KN38AzDG.exe
Wow64 process (32bit):	true
Commandline:	
Imagebase:	0x100000
File size:	73728 bytes
MD5 hash:	3FB36CB0B7172E5298D2992D42984D06
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 50%, ReversingLabs
Reputation:	high

Analysis Process: cmd.exe PID: **1876**, Parent PID: **4360**

General

Target ID:	7
Start time:	08:47:39
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "SplitFiles131.exe" /f & erase "C:\Program Files (x86)\Split Files\SplitFiles131.exe" & exit
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Split Files\SplitFiles131.exe	cannot delete	1	11F0374	DeleteFileW
C:\Program Files (x86)\Split Files\SplitFiles131.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: **5272**, Parent PID: **1876**

General

Target ID:	8
Start time:	08:47:39
Start date:	05/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: taskkill.exe PID: **5224**, Parent PID: **1876**

General

Target ID:	9
Start time:	08:47:39
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "SplitFiles131.exe" /f
Imagebase:	0xf40000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly