ID: 736956
Sample Name: file.exe
Cookbook: default.jbs
Time: 12:30:23
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Nymaim 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Compliance 5
Networking 5
E-Banking Fraud 5
Data Obfuscation 5
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
C:\Program Files (x86)\fnSearcher\checksums.txt (copy) 13
C:\Program Files (x86)\fnSearcher\completed.wav (copy) 13
C:\Program Files (x86)\fnSearcher\fnsearcher68.exe 13
C:\Program Files (x86)\fnSearcher\history.rtf (copy) 14
C:\Program Files (x86)\fnSearcher\is-15O1T.tmp 14
C:\Program Files (x86)\fnSearcher\is-51KLJ.tmp 14
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp 15
C:\Program Files (x86)\fnSearcher\is-7C4Q3.tmp 15
C:\Program Files (x86)\fnSearcher\is-8S345.tmp 15
C:\Program Files (x86)\fnSearcher\is-DS22N.tmp 16
C:\Program Files (x86)\fnSearcher\is-E8ARN.tmp 16
C:\Program Files (x86)\fnSearcher\is-OS12U.tmp 16
C:\Program Files (x86)\fnSearcher\is-S6A9T.tmp 16
C:\Program Files (x86)\fnSearcher\license_en.rtf (copy) 17
C:\Program Files (x86)\fnSearcher\license_ru.rtf (copy) 17
C:\Program Files (x86)\fnSearcher\reset.bat (copy) 17
C:\Program Files (x86)\fnSearcher\unins.ico (copy) 18
C:\Program Files (x86)\fnSearcher\unins000.dat 18
C:\Program Files (x86)\fnSearcher\unins000.exe (copy) 18
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ping[1].htm 19
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\count[1].htm 19

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\library[1].htm 19
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fuckingdllENCR[1].dll 19
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\count[1].htm 20
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\library[1].htm 20
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp 20
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_iscrypt.dll 21
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_setup64.tmp 21
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll 21
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp 22
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\0Jzl2az.exe 22
Static File Info 22
General 22
File Icon 23
Static PE Info 23
General 23
Entrypoint Preview 23
Data Directories 24
Sections 24
Resources 25
Imports 25
Possible Origin 26
Network Behavior 26
TCP Packets 26
HTTP Request Dependency Graph 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: file.exePID: 5676, Parent PID: 3452 28
General 28
File Activities 28
Analysis Process: is-SQE6E.tmpPID: 5624, Parent PID: 5676 29
General 29
File Activities 29
File Created 29
File Moved 30
File Written 30
File Read 37
Registry Activities 37
Key Created 37
Key Value Created 37
Analysis Process: fnsearcher68.exePID: 3080, Parent PID: 5624 39
General 39
File Activities 39
File Created 39
File Written 39
Analysis Process: 0Jzl2az.exePID: 4556, Parent PID: 3080 40
General 40
Analysis Process: cmd.exePID: 4392, Parent PID: 3080 41
General 41
File Activities 41
File Deleted 41
Analysis Process: conhost.exePID: 3328, Parent PID: 4392 41
General 41
Analysis Process: taskkill.exePID: 4692, Parent PID: 4392 41
General 41
File Activities 42
Disassembly 42

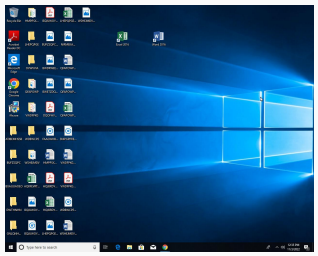
Windows Analysis Report

file.exe

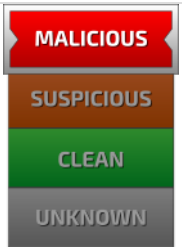
Overview

General Information

Sample Name:	file.exe
Analysis ID:	736956
MD5:	9156fa044ec274..
SHA1:	62107d1bd3cb01..
SHA256:	861751b8c762f3..
Tags:	exe
Infos:	



Detection



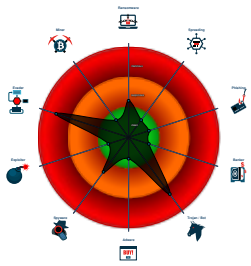
Nymaim

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

Signatures

- Multi AV Scanner detection for subm…
- 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…
- 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: 5676 cmdline: C:\Users\user\Desktop\file.exe MD5: 9156FA044EC274F670095E43E205D137)
  - is-SQE6E.tmp (PID: 5624 cmdline: "C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp" /SL4 $30224 "C:\Users\user\Desktop\file.exe" 2630911 52736 MD5: 7CD12C54A9751CA6EEE6AB0C85FB68F5)
    - fnsearcher68.exe (PID: 3080 cmdline: "C:\Program Files (x86)\fnSearcher\fnsearcher68.exe" MD5: 3FCA96750E2F656A73FBC6A896F53209)
      - 0Jzl2az.exe (PID: 4556 cmdline: MD5: 3FB36CB0B7172E5298D2992D42984D06)
      - cmd.exe (PID: 4392 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "fnsearcher68.exe" /f & erase "C:\Program Files (x86)\fnSearcher\fnsearcher68.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - taskkill.exe (PID: 4692 cmdline: taskkill /im "fnsearcher68.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Configuration

Threatname: Nymaim

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.345115638.00000000037D0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000002.00000002.343591826.0000000000400000.00000040.00000001.01000000.00000007.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.fnsearcher68.exe.37d0000.2.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.fnsearcher68.exe.400000.0.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.fnsearcher68.exe.400000.0.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.fnsearcher68.exe.37d0000.2.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nymaim

Data Obfuscation

Detected unpacking (overwrites its own PE header)

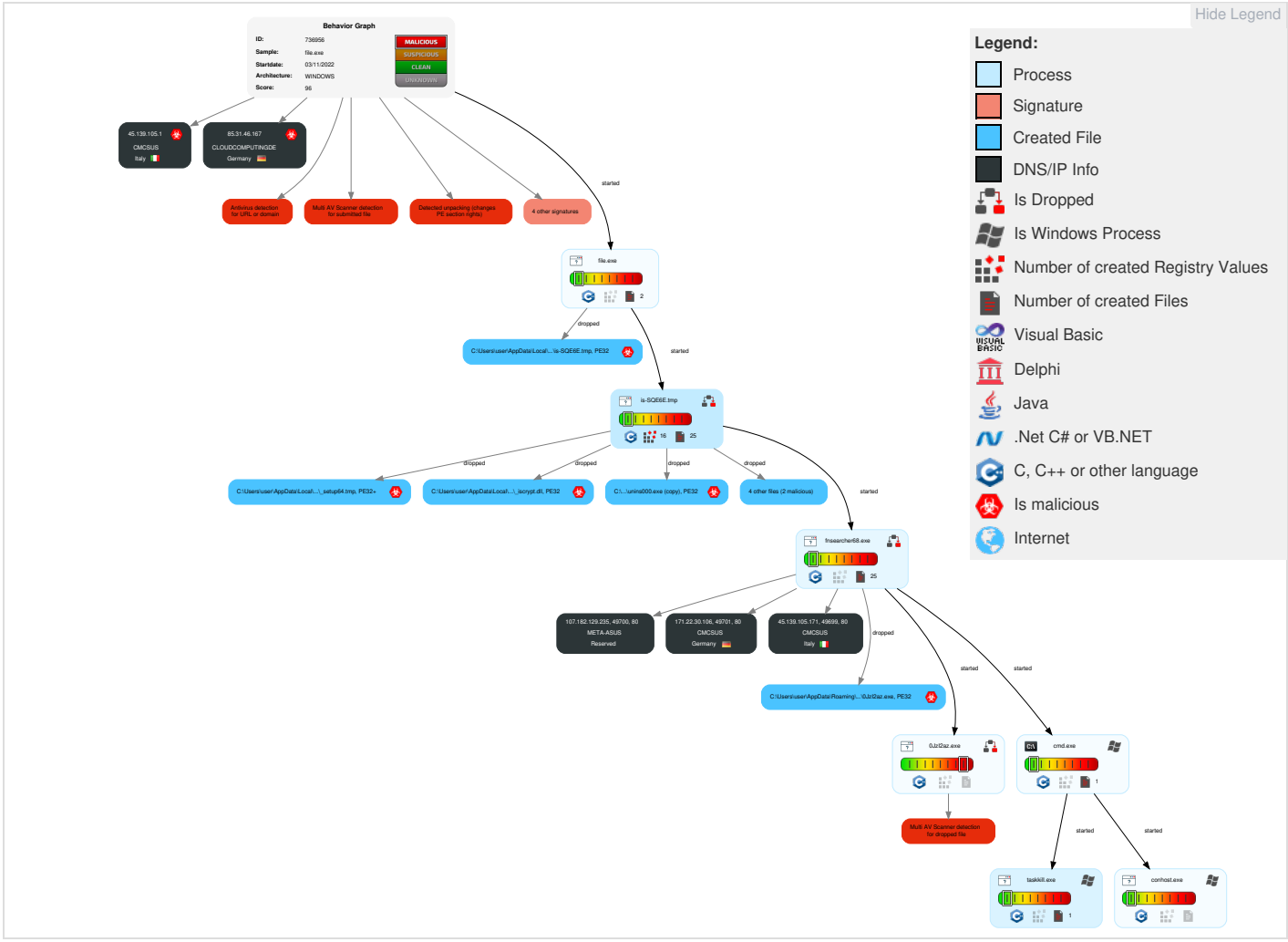
Detected unpacking (changes PE section rights)

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	1 System Shutdown/ Reboot
Default Accounts	3 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 5 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
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	3 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Process Injection	DCSync	1 1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	3 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

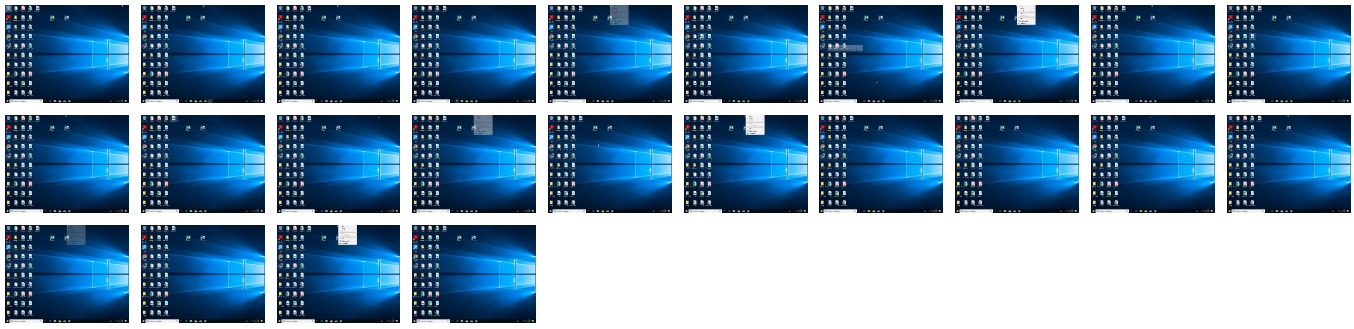
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	17%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\fnSearcher\fnsearcher68.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_iscrypt.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_iscrypt.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_setup64.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll	4%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp	8%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\0JzI2az.exe	38%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.fnsearcher68.exe.10000000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.3.file.exe.21d4000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.fnsearcher68.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
1.2.is-SQE6E.tmp.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.139.105.171/itsnotmalware/count.php?sub=NOSUB&stream=start&substream=mixinte	0%	URL Reputation	safe	
http://www.innosetup.com/	0%	URL Reputation	safe	
http://www.n-group.info	0%	URL Reputation	safe	
http://www.n-group.info	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://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://www.fn-group.info/fnsearcher/help.html1	0%	Avira URL Cloud	safe	
http://www.fn-group.info/-	0%	Avira URL Cloud	safe	
http://www.kungsoft.com	0%	Avira URL Cloud	safe	
http://www.fn-group.info/	0%	Avira URL Cloud	safe	
http://www.fn-group.info/fnsearcher/download.html	0%	Avira URL Cloud	safe	
http://www.fn-group.info/-http://www.fn-group.info/fnsearcher/help.html1http://www.fn-group.info/fns	0%	Avira URL Cloud	safe	
http://www.fn-group.info/fnsearcher/help.html	0%	Avira URL Cloud	safe	
http://www.fn-group.info/fnsearcher/help.htmlB	0%	Avira URL Cloud	safe	
http://www.fn-group.info/8	0%	Avira URL Cloud	safe	
http://www.fn-group.info/fnsearcher/download.htmlw	0%	Avira URL Cloud	safe	

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

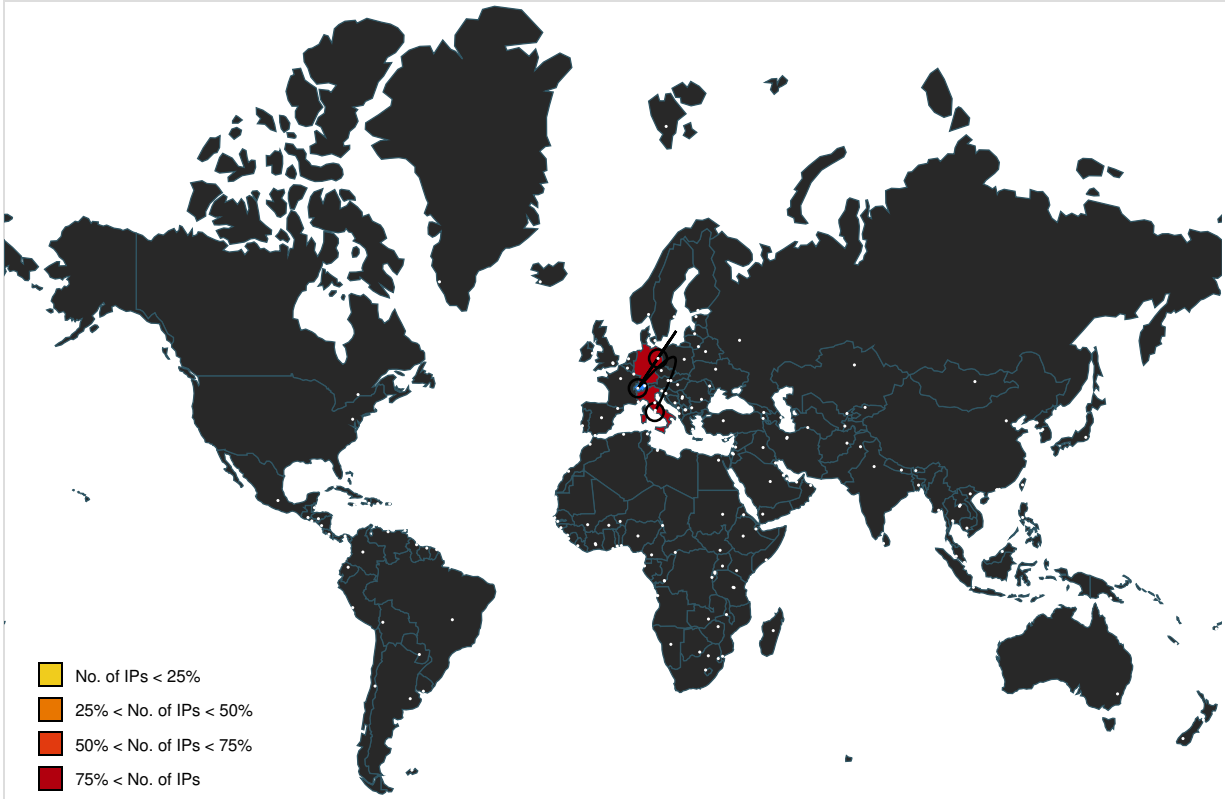
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	is-SQE6E.tmp, is-SQE6E.tmp, 00000001.00000000.251439199.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-6KAKC.tmp.1.dr, is-SQE6E.tmp.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.n-group.info	file.exe, 00000000.00000003.250397670.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.347783736.00000000021C8000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251914619.0000000003190000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000002.346974137.0000000815000.00000004.00000020.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.346249515.0000000000815000.00000004.00000020.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251984991.0000000002256000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000002.347088234.0000000002254000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.346376195.0000000000815000.00000004.00000020.00020000.00000000.sdmp, is-OS12U.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fn-group.info/-http://www.fn-group.info/fnsearcher/help.html1http://www.fn-group.info/fns	file.exe, 00000000.00000003.250397670.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251914619.0000000003190000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/fnsearcher/help.html1	file.exe, 00000000.00000003.250397670.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251914619.0000000003190000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/fnsearcher/help.html	file.exe, 00000000.00000003.347773502.00000000021C0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.250490694.00000000021C1000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251984991.0000000002256000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000002.347088234.0000000002254000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/	is-SQE6E.tmp, 00000001.00000002.347088234.0000000002254000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/fnsearcher/download.html	is-SQE6E.tmp, 00000001.00000002.347088234.0000000002254000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/-	file.exe, 00000000.00000003.250397670.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251914619.0000000003190000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.remobjects.com/?ps	file.exe, 00000000.00000003.250582680.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.250924927.00000000021D4000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, is-SQE6E.tmp, 00000001.00000000.251439199.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-6KAKC.tmp.1.dr, is-SQE6E.tmp.0.dr	false	• URL Reputation: safe	unknown
http://www.fn-group.info/fnsearcher/help.htmlB	file.exe, 00000000.00000003.347773502.00000000021C0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.250490694.00000000021C1000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.251984991.0000000002256000.00000004.00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000002.347088234.0000000002254000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kungsoft.com	fnsearcher68.exe, 00000002.00000000.2588260254.0000000001276000.00000002.00000001.01000000.00000007.sdmp, fnsearcher68.exe.1.dr, is-51KLJ.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.fn-group.info/8	is-SQE6E.tmp, 00000001.00000002.346791616.000000000079A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fn-group.info/fnsearcher/download.htmlw	is-SQE6E.tmp, 00000001.00000002.34697413 7.0000000000815000.00000004.00000020.000 20000.00000000.sdmp, is-SQE6E.tmp, 00000 001.00000003.346249515.0000000000815000. 00000004.00000020.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000003.346376195.000000 0000815000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.remobjects.com/?psU	file.exe, 00000000.00000003.250582680.00 000000023F0000.00000004.00001000.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.250924927.00000000021D4000.00000004 .00001000.00020000.00000000.sdmp, is-SQE6E.tmp, 00000001.00000000.251439199.00000000004010 00.00000020.00000001.01000000.00000004.sdmp, is-6KAKC.tmp.1.dr, is-SQE6E.tmp.0.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	false
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	false
171.22.30.106	unknown	Germany		33657	CMCSUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736956
Start date and time:	2022-11-03 12:30:23 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 59s
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:	18
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@12/31@0/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.9% (good quality ratio 23.8%) • Quality average: 80% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 97% • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
12:33:55	API Interceptor	1x Sleep call for process: 0Jzl2az.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)\fnSearcher\checksums.txt (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	4.884558011565004
Encrypted:	false
SSDEEP:	6:AySGO4KS/x4L8ThcSRFLk6XDuwOyoExvWmFuQUqvJrdt6YAhlAjyIDHAUXV4:Ayf3WPSPLkP/fEFWm/5v3t/byGgH
MD5:	461D6293779BDEF19493C351344F2B71
SHA1:	C441B7DAA5ABF8A2872D55F47585657147451C72
SHA-256:	0C2BD3D1AEB04523291BC72424C802E36C1733E0B72FA775B9DD0A4E9CADE263
SHA-512:	D41DBDF10A61CEDE90D68F1F7E351D9DA441026F7CF9C12AB6ADA017B185455DDBFED74760A3DD3D67ED10A9B1915E79F6ACFF70850B626C68CB1E2B22FC9 C25
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	All checksum in MD5....completed.wav..8e46be5a4155710361181e3b67373404..history.rtf..1bfcde2b3d557cfb8b9004055d3a90f5..license_en.rtf..1ae62f00fc36836 4a2de668b3299d793..license_ru.rtf..fe7c9c6f6e8f720f886bcc65fa2d9b20..nsearcher.exe..c5e7acbda2f8bfa49bd9580120aac7b2..reset.bat..aaa149e55ddae6393fe09 9990747da94..unins.ico..b8ed55bf81883d2becf23fc020585214

C:\Program Files (x86)\fnSearcher\completed.wav (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz
Category:	dropped
Size (bytes):	272134
Entropy (8bit):	6.156729185977344
Encrypted:	false
SSDEEP:	6144:TNKofL3cEjxCryOOYJH+8a1anwxrcSOQmlBkO+kKo:TNNzsEjxCryOOYvbnwxrcewf+1o
MD5:	8E46BE5A4155710361181E3B67373404
SHA1:	18A19A04DD6E4BFE6731E6978F2CB295E1C52174
SHA-256:	32AB0D1DF26B0DCFE78D393A1F2534D1DAA5BABC6980017303ED925682CE19D0
SHA-512:	5497EEF00048125D67551FBF22747654D97903F0622830299792159DC8532013191FB006A832E7CE2B4383EE2EC67B7B7C1D06C25CF34EEB118D050AC89DC3B7
Malicious:	false
Preview:	RIFF.&..WAVEfmt ........D.....LIST....INFOIART.... ..ICMT....mp3cut.ru ..ICRD.... ..INAM.... ..IPRD.... ..IPRT....1.ISFT....Lavf55.22.100.data.&..... ....

C:\Program Files (x86)\fnSearcher\fnsearcher68.exe

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	4448253
Entropy (8bit):	6.264319773505966
Encrypted:	false
SSDEEP:	49152:g6IGeIk/rF+FYh2VSb1+/zSYGxsnlHqeQKkZ7QhrzFJmhO+oCnFWDE:8Lh2kbuOYSilq7KkZ8ShO+vFYE
MD5:	3FCA96750E2F656A73FBC6A896F53209
SHA1:	34F711F2651D3FBAF639B3A595F9029F6AF7E245
SHA-256:	65B7C9068EBF98CEC8B955FC2D61D83EBDFA66FC656AB56C160FCE98F1F1B189
SHA-512:	2813F8E023D1BDDB564F25257909A0AD48C0A984761B2209CC383EC355A7E7B6476A4754549F9702EA420A8176C5A2AEC1732D29A659B12520A6026BCEA8E76E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....cc.....@.....@.....@.....#..... .....`..8.....text..... ..`.rdata..,8.....@.....@..A.data...`....@ .....@.....@....tls.....P.....P.....@....rsrc.....`.....`.....@..@.rfn68....(..@....(..@.....`..... ....

C:\Program Files (x86)\fnSearcher\history.rtf (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025
Category:	dropped
Size (bytes):	44381
Entropy (8bit):	4.886111144563166
Encrypted:	false
SSDEEP:	384:zDkO4WdW2OTYn/akuhSm9eDAmWZJ6Sr82Zeo75Y3kpTBLRA6AlEayr:zDEDhSm9aHZ/6A92
MD5:	1BFCDE2B3D557CFB8B9004055D3A90F5
SHA1:	678353ADC2CACD12555EF12F5D94FC03CD07707E
SHA-256:	A8FBA72D4B1FB03EE40A9472430275499E361BBD74144D9956232EF2FDA0407A
SHA-512:	DF9FDB20B2054328431AA5F0D0014D949AF4BE3BFC0CB1E3D77BEDD4626DEEA83FDA259352765C04985087E260EB03FF7B337C1D4D54878EC210EFBEA6A36A D1
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs 0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}..{\f34\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060 30204}Cambria Math;}{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 020b0604030504040204}Verdana;}..{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}..{\fhimajor\f 31502\fbidi \froman\fcharset204\fprq2{*\panose 02040503050406030204}Cambria;}{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504 05020304}Times New Roman;}..{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Rom

C:\Program Files (x86)\fnSearcher\is-15O1T.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz
Category:	dropped
Size (bytes):	272134
Entropy (8bit):	6.156729185977344
Encrypted:	false
SSDEEP:	6144:TNKofL3cEjxCryOOYJH+8a1anwxrcSOQmlBkO+kKo:TNNzsEjxCryOOYvbnwxrcewf+1o
MD5:	8E46BE5A4155710361181E3B67373404
SHA1:	18A19A04DD6E4BFE6731E6978F2CB295E1C52174
SHA-256:	32AB0D1DF26B0DCFE78D393A1F2534D1DAA5BABC6980017303ED925682CE19D0
SHA-512:	5497EEF00048125D67551FBF22747654D97903F0622830299792159DC8532013191FB006A832E7CE2B4383EE2EC67B7B7C1D06C25CF34EEB118D050AC89DC3B7
Malicious:	false
Preview:	RIFF.&..WAVEfmt .....D.....LIST....INFOIART.... ..ICMT....mp3cut.ru ..ICRD.... ..INAM.... ..IPRD.... ..IPRT....1.ISFT....Lavf55.22.100.data.&..... ....

C:\Program Files (x86)\fnSearcher\is-51KLJ.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	data
Category:	dropped
Size (bytes):	4448253
Entropy (8bit):	6.264319309636284
Encrypted:	false
SSDEEP:	49152:z6IGeIk/rF+FYh2VSb1+/zSYGxsnlHqeQKkZ7QhrzFJmhO+oCnFWDE:bLh2kbuOYSilq7KkZ8ShO+vFYE
MD5:	799061D3EB45D6E5A60FB66FBA8E305F
SHA1:	53F2740727690A4A3AF3BB1B8CB14A5CDCDDB828
SHA-256:	6FE6FA5C1C331ED9128A09B8562FEB929095D16AAC2925C2063C465BC4DE252F
SHA-512:	1BACCE17E0738A3DBBFDAD350B3D942A608E829544A3BEBA3A9D6E5E00B294B3F7666CB135EEAB91FCD5D8F4C0E3477001F1FA6D2624EDBCA02FE60801779 996
Malicious:	false

Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....cc.....@.....@.....@.....#.....`..8.....text..... ..`.rdata..,8.....@.....@..A.data...`....@.....@.....@....tls.....P.....P.....@....rsrc.....`.....`.....@..@.rfn68....(..@....(..@.....`.....

C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	683801
Entropy (8bit):	6.46625841767368
Encrypted:	false
SSDEEP:	12288:akxzRCUn4rP/37YzHXA6/YUKsGjQNw4qpRRpDWowphIxzr:RFRCUn4rP/37YzHXA6QJsoPtlpqxzr
MD5:	10529F95E0E03896C0C969F016E313AA
SHA1:	F79547E17C6EAC21781BD3EC267E39C9A8588207
SHA-256:	40AE4CA142D536558D329DF560CDBE29D2335F0F7E349C26887B3AB411E0F54D
SHA-512:	2B6A51A65735D3AF8E5D9A70A2C7CEDAB2C8920A720B71EACFDBA0ED8FAFCC6ACE7B28951B3953C4762B73B30E823A8A811744E207ACC695C70B8ABC301EF47D
Malicious:	**true**
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....@.....0.....@.....<%.....:.....P.....CODE..... ..`DATA....`.....@...BSS....`.....idata..<%.....&.....@....tls.....@.....rdata.....P.....@..P.reloc.....`.....@..P.rsrc....:.....:.....@..P.....0.....@..P.....

C:\Program Files (x86)\fnSearcher\is-7C4Q3.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025
Category:	dropped
Size (bytes):	44381
Entropy (8bit):	4.886111144563166
Encrypted:	false
SSDEEP:	384:zDkO4WdW2OTYn/akuhSm9eDAmWZJ6Sr82Zeo75Y3kpTBLRA6AlEayr:zDEDhSm9aHZ/6A92
MD5:	1BFCDE2B3D557CFB8B9004055D3A90F5
SHA1:	678353ADC2CACD12555EF12F5D94FC03CD07707E
SHA-256:	A8FBA72D4B1FB03EE40A9472430275499E361BBD74144D9956232EF2FDA0407A
SHA-512:	DF9FDB20B2054328431AA5F0D0014D949AF4BE3BFC0CB1E3D77BEDD4626DEEA83FDA259352765C04985087E260EB03FF7B337C1D4D54878EC210EFBEA6A36AD1
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}..{\f34\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060 30204}Cambria Math;}{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 020b0604030504040204}Verdana;}..{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}..{\fhimajor\f31502\fbidi \froman\fcharset204\fprq2{*\panose 02040503050406030204}Cambria;}{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504 05020304}Times New Roman;}..{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Rom

C:\Program Files (x86)\fnSearcher\is-8S345.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	3.3086949695628416
Encrypted:	false
SSDEEP:	3:lU4n:X4n
MD5:	AAA149E55DDAE6393FE099990747DA94
SHA1:	F3011A304194E8AA27E0E29E49F8F2C81EAECDBD
SHA-256:	E2C57F46196C1BA3EF69792DEDF532F2A2286BA876E5BB6091C6B173D2E7C5BB
SHA-512:	15121C5C5ECB404BE5E734BE437D744B8FCDB34DDD46D69E5F18CA23E4D74B79B605B9B4197398977243203533 2D24FFA310F78AF6F44F44C731D416F4A949A
Malicious:	false
Preview:	nSearcher.exe /reset

C:\Program Files (x86)\fnSearcher\is-DS22N.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	MS Windows icon resource - 7 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	134921
Entropy (8bit):	6.105680271090377
Encrypted:	false
SSDEEP:	1536:blivjgxiL8DUPKKh1EQ3Zeyo0aIWeTjXV0/KwIhFvyt2M5BH2w:bV4IfptKIW6F0JIzw2M5B1
MD5:	B8ED55BF81883D2BECF23FC020585214
SHA1:	43F6DE28C98380B2FFBA0B29F381EB8408E6F691
SHA-256:	C63B20B68FABD4DF695389494235345CC95CF7E1826896EE6393F0E402B565DA
SHA-512:	E1CB9501575B4CD66AFD6C67BE2AECA1615E9C37C2B37E68A645B21BB6B2CAAE88CAF0EC8BE3513AD72896AB6A870154D17A56F71E50D51581F00C706553B10D
Malicious:	false
Preview:	......00.... ..%..v... ....&..... .h....6..... .....;..... .(...1...@@.... .(B..Y..... .....(...0...`..... .....%.....<...^...x.....}...b...A...!.....X.....].....J.....3.....d.....

C:\Program Files (x86)\fnSearcher\is-E8ARN.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	4.884558011565004
Encrypted:	false
SSDEEP:	6:AySGO4KS/x4L8ThcSRFLk6XDuwOyoExvWmFuQUqvJrdt6YAhlAjyIDHAUXV4:Ayf3WPSPLkP/fEFWm/5v3t/byGgH
MD5:	461D6293779BDEF19493C351344F2B71
SHA1:	C441B7DAA5ABF8A2872D55F47585657147451C72
SHA-256:	0C2BD3D1AEB04523291BC72424C802E36C1733E0B72FA775B9DD0A4E9CADE263
SHA-512:	D41DBDF10A61CEDE90D68F1F7E351D9DA441026F7CF9C12AB6ADA017B185455DDBFED74760A3DD3D67ED10A9B1915E79F6ACFF70850B626C68CB1E2B22FC9C25
Malicious:	false
Preview:	All checksum in MD5....completed.wav..8e46be5a41557103611 81e3b67373404..history.rtf..1bfcde2b3d557cfb8b9004055d3a90f5..license_en.rtf..1ae62f00fc36836 4a2de668b3299d793..license_ru.rtf..fe7c9c6f6e8f720f886bcc65fa2d9b20..nsearcher.exe..c5e7acbda2f8bfa49bd9580120aac7b2..reset.bat..aaa149e55ddae6393fe09 9990747da94..unins.ico..b8ed55bf81883d2becf23fc020585214

C:\Program Files (x86)\fnSearcher\is-OS12U.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025
Category:	dropped
Size (bytes):	44011
Entropy (8bit):	5.026565347530582
Encrypted:	false
SSDEEP:	384:em3cWBnPz+p/zWFHQ1QDGteo75Y3kpTBLRA6AlEayF:emsuQ1WGIZ/6A9U
MD5:	1AE62F00FC368364A2DE668B3299D793
SHA1:	E4E32C3EDC269987E39FDC0883F589CECF9604B4
SHA-256:	F9FF5B54BB1EBEECCC4104A62E32CAB4556DD75A5F76260E720485D5CC39D7E8
SHA-512:	844F4116FD8FF13B144D6D16DE695F7600283DC0B573CAAB5AE74573301B235AC234CE59D1D30BE8FB8ABBA3DFD27EDF8C53A7E0CD5320C23008B5F35437757
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\f34\fbidi \froman\fcharset1\fprq2{*\panose 0204050305040603020 4}Cambria Math;}..{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 0000000000000000000 0}Verdana;}{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 0202 0603050405020304}Times New Roman;}..{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\fhimajor\f3150 2\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060302 04}Cambria;}..{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}..{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman

C:\Program Files (x86)\fnSearcher\is-S6A9T.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025

Category:	dropped
Size (bytes):	51922
Entropy (8bit):	4.912794307456054
Encrypted:	false
SSDEEP:	384:eA3cWBnPz+p/zWFHQ1Qp0SEW5FRLU+cB9nGog4jy6XFsa0eo75Y3kpTBLRA6AIE8:eAsuQ1IV75knFBV6ahZ/6A9r
MD5:	FE7C9C6F6E8F720F886BCC65FA2D9B20
SHA1:	2775F12A0BABDEE5CEEDB08452EF72732E49F13C
SHA-256:	B3F54F1D0C3EA747CC52BAD1B363815B9297088CACDF1398C8CFD7F8054CE2BB
SHA-512:	ABBFE43FBE4827C9CEDA8D1FDD3DB3B344E99E0CDC3512E4EF84F965F882BA5E3822A407AC1F974D1986F1CDA645A20C1D00CD16262200FE39574AEFF12F6A1A
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\f34\fbidi \froman\fcharset1\fprq2{*\panose 0204050305040603020 4}Cambria Math;}..{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 020b0604030504040204}Verdana;}{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 0202 0603050405020304}Times New Roman;}..{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\fhimajor\f3150 2\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060302 04}Cambria;}..{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Tim es New Roman;}{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}..{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman

C:\Program Files (x86)\fnSearcher\license_en.rtf (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025
Category:	dropped
Size (bytes):	44011
Entropy (8bit):	5.026565347530582
Encrypted:	false
SSDEEP:	384:em3cWBnPz+p/zWFHQ1QDGteo75Y3kpTBLRA6AIEayF:emsuQ1WGIZ/6A9U
MD5:	1AE62F00FC368364A2DE668B3299D793
SHA1:	E4E32C3EDC269987E39FDC0883F589CECF9604B4
SHA-256:	F9FF5B54BB1EBEECCC4104A62E32CAB4556DD75A5F76260E720485D5CC39D7E8
SHA-512:	844F4116FD8FF13B144D6D16DE695F7600283DC0B573CAAB5AE74573301B235AC234CE59D1D30BE8FB8ABBA3DFD27EDF8C53A7E0CD5320C23008B5F35437757
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\f34\fbidi \froman\fcharset1\fprq2{*\panose 0204050305040603020 4}Cambria Math;}..{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 000000000000000000}Verdana;}{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 0202 0603050405020304}Times New Roman;}..{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\fhimajor\f3150 2\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060302 04}Cambria;}..{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Tim es New Roman;}{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}..{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman

C:\Program Files (x86)\fnSearcher\license_ru.rtf (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	Rich Text Format data, version 1, ANSI, code page 1251, default middle east language ID 1025
Category:	dropped
Size (bytes):	51922
Entropy (8bit):	4.912794307456054
Encrypted:	false
SSDEEP:	384:eA3cWBnPz+p/zWFHQ1Qp0SEW5FRLU+cB9nGog4jy6XFsa0eo75Y3kpTBLRA6AIE8:eAsuQ1IV75knFBV6ahZ/6A9r
MD5:	FE7C9C6F6E8F720F886BCC65FA2D9B20
SHA1:	2775F12A0BABDEE5CEEDB08452EF72732E49F13C
SHA-256:	B3F54F1D0C3EA747CC52BAD1B363815B9297088CACDF1398C8CFD7F8054CE2BB
SHA-512:	ABBFE43FBE4827C9CEDA8D1FDD3DB3B344E99E0CDC3512E4EF84F965F882BA5E3822A407AC1F974D1986F1CDA645A20C1D00CD16262200FE39574AEFF12F6A1A
Malicious:	false
Preview:	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\f34\fbidi \froman\fcharset1\fprq2{*\panose 0204050305040603020 4}Cambria Math;}..{\f39\fbidi \fswiss\fcharset204\fprq2{*\panose 020b0604030504040204}Verdana;}{\flomajor\f31500\fbidi \froman\fcharset204\fprq2{*\panose 0202 0603050405020304}Times New Roman;}..{\fdbmajor\f31501\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}{\fhimajor\f3150 2\fbidi \froman\fcharset204\fprq2{*\panose 020405030504060302 04}Cambria;}..{\fbimajor\f31503\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Tim es New Roman;}{\flominor\f31504\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman;}..{\fdbminor\f31505\fbidi \froman\fcharset204\fprq2{*\panose 020206030504050203 04}Times New Roman

C:\Program Files (x86)\fnSearcher\reset.bat (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	3.3086949695628416
Encrypted:	false
SSDEEP:	3:lU4n:X4n
MD5:	AAA149E55DDAE6393FE099990747DA94
SHA1:	F3011A304194E8AA27E0E29E49F8F2C81EAECDBD
SHA-256:	E2C57F46196C1BA3EF69792DEDF532F2A2286BA876E5BB6091C6B173D2E7C5BB
SHA-512:	15121C5C5ECB404BE5E734BE437D744B8FCDB34DDD46D69E5F18CA23E4D74B79B605B9B41973989772432035332D24FFA310F78AF6F44F44C731D416F4A949A
Malicious:	false
Preview:	nSearcher.exe /reset

C:\Program Files (x86)\fnSearcher\unins.ico (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	MS Windows icon resource - 7 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	134921
Entropy (8bit):	6.105680271090377
Encrypted:	false
SSDEEP:	1536:blivjgxiL8DUPKKh1EQ3Zeyo0aIWeTjXV0/KwIhFvyt2M5BH2w:bV4IfptKIW6F0Jlzw2M5B1
MD5:	B8ED55BF81883D2BECF23FC020585214
SHA1:	43F6DE28C98380B2FFBA0B29F381EB8408E6F691
SHA-256:	C63B20B68FABD4DF695389494235345CC95CF7E1826896EE6393F0E402B565DA
SHA-512:	E1CB9501575B4CD66AFD6C67BE2AECA1615E9C37C2B37E68A645B21BB6B2CAAE88CAF0EC8BE3513AD72896AB6A870154D17A56F71E50D51581F00C706553B10D
Malicious:	false
Preview:	......00.... ..%..v... ....&..... .h....6..... .....;..... .(...1...@@.... .(B..Y..... .....(...0...`..... .....%..... .....<...^...x.....}...b...A...!..... .....X.....]..... .J.....3.....d.....

C:\Program Files (x86)\fnSearcher\unins000.dat

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	InnoSetup Log FNSearcher {b264a18E-91B4-4910-9006-8bf37124b695}, version 0x2d, 3779 bytes, 367706\user, "C:\Program Files (x86)\fnSearcher"
Category:	dropped
Size (bytes):	3779
Entropy (8bit):	4.4819215691462615
Encrypted:	false
SSDEEP:	48:G1q3HlyMCLBv8lD8zpjxcm5UQoIN6hqkLVO3471IGX0ya3tF7yGl4XKBXD7fDMpp:GUKp8lD8zpHJoIohqYOlhxkNFjKH
MD5:	21BE62ED5593242273AD122E0D982DDB
SHA1:	DEADE12912AED05780AAC84A59388EC09DD1B1EF
SHA-256:	3AADFCFF0A5E22977AAE09981CDFB2EA79E33945317F7429A3043B508C23C95C
SHA-512:	E805B1A637E3AC023B3864EC65C9C46193B77B9AF53BB8C0AA9B6F24AE3AC44BC15005CB8F2679D331134E710C752528A127E83A796317BDD745EE8214BFD308
Malicious:	false
Preview:	Inno Setup Uninstall Log (b).....{b264a18E-91B4-4910-9006-8bf37124b695}.....FNSearcher..... .....-.....%.....m.!$.....]..3.....A... .367706.user!C:\Program Files (x86)\fnSearcher.....!./.... .....T.IFPS.....BOOLEAN..... .TWIZARDFORM....TWIZARDFORM.....TPASSWORDEDIT....TPASSWORDEDIT.....!MAIN....-1..'...dll:kernel32.dll.CreateFileA.....#.. .dll:kernel32.dll.WriteFile.....!...dll:kernel32.dll.CloseHandle.....!...dll:kernel32.dll.ExitProcess.....$...dll:User32.dll.GetSystemMetri

C:\Program Files (x86)\fnSearcher\unins000.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	683801
Entropy (8bit):	6.46625841767368
Encrypted:	false
SSDEEP:	12288:akxzRCUn4rP/37YzHXA6/YUKsGjQNw4qpRRpDWowphIxzr:RFRCUn4rP/37YzHXA6QJsoPtlpqxzr
MD5:	10529F95E0E03896C0C969F016E313AA

SHA1:	F79547E17C6EAC21781BD3EC267E39C9A8588207
SHA-256:	40AE4CA142D536558D329DF560CDBE29D2335F0F7E349C26887B3AB411E0F54D
SHA-512:	2B6A51A65735D3AF8E5D9A70A2C7CEDAB2C8920A720B71EACFDBA0ED8FAFCC6ACE7B28951B3953C4762B73B30E823A8A811744E207ACC695C70B8ABC301EF47D
Malicious:	**true**
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....0.....@.....<%.....:.....P..... .....CODE..... ..`DATA....`.....@...BSS....`.....idata..<%.....&.....@....tls.....@.....rdata .....P.....@..P.reloc.....`.....@..P.rsrc....:.....:.....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ping[1].htm

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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\Microsoft\Windows\INetCache\IE\MEEXW4H4\count[1].htm

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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\MEEXW4H4\library[1].htm

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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\PSUEOSZZ\fuckingdllENCR[1].dll

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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:	F2E1AE47B5B0A5D3DD22DD6339E15FEE3D7F04EF03917AE2A7686E73E9F06FB95C8008038C018939BB9925F395D765C9690BF7874DC5E90BC2F77C1E730D3A0
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...l.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\WJ8I2OL4\count[1].htm

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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\WJ8I2OL4\library[1].htm

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	4.012434743866195
Encrypted:	false
SSDEEP:	48:iAnz1hEU3FR/pmqBl8/QMCBaquEMx5BCwSS4k+bkguj0K:pz1eEFNcqBC/Qrex5MSKD
MD5:	C594B792B9C556EA62A30DE541D2FB03
SHA1:	69E0207515E913243B94C2D3A116D232FF79AF5F
SHA-256:	5DCC1E0A197922907BCA2C4369F778BD07EE4B1BBBDF633E987A028A314D548E

SHA-512:	387BD07857B0DE67C04E0ABF89B754691683F30515726045FF382DA9B6B7F36570E38FAE9ECA5C4F0110CE9BB421D8045A5EC273C4C47B5831948564763ED144
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....|.....|.....|.....Rich.....PE..L.....%E..... ....@.....@.....I ..P....0..8..... ..D.....text..... ....`.rdata..... .....@..@.rsrc...8....0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_iscrypt.dll

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.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: 2% • Antivirus: Metadefender, Detection: 3%, Browse
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-6LIA6.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.203889009972449
Encrypted:	false
SSDEEP:	48:SvTmfWvPcXegCWUo1vlZwrAxoONfHFZONfH3d1xCWMBgW2p3SS4k+bkg6j0K:nfkcXegjJ/ZgYNzcld1xamW2pCSKv
MD5:	B4604F8CD050D7933012AE4AA98E1796
SHA1:	36B7D966C7F87860CD6C46096B397AA23933DF8E
SHA-256:	B50B7AC03EC6DA865BF4504C7AC1E52D9F5B67C7BCB3EC0DB59FAB24F1B471C5
SHA-512:	3057AA4810245DA0B340E1C70201E5CE528CFDC5A164915E7B11855E3A5B9BA0ED77FBC542F5E4EB296EA65AF88F263647B577151068636BA188D8C4FD44E43
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....E.....#.....@.....`.....<!.....P..8....@..0..... .....text..... ..`.rdata..|... .....@..@.data.....0.....@....pdata..0....@.....@..@.rsrc...8....P.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll

Process:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.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:	9908E573921D5DBC3454A1C0A6C969AB8A81CC2E8B5385391D46B1A738FB06A76AA3282E0E58D0D2FFA6F27C85668CD5178E1500B8A39B1BBAE04366AE6A86E3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Metadefender, Detection: 4%, Browse
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-VVS8D.tmp\is-SQE6E.tmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	673280
Entropy (8bit):	6.456966952098253
Encrypted:	false
SSDEEP:	12288:CkxzRCUn4rP/37YzHXA6/YUKsGjQNw4qpRRpDWowphIxz:ZFRCUn4rP/37YzHXA6QJsoPtlpqxz
MD5:	7CD12C54A9751CA6EEE6AB0C85FB68F5
SHA1:	76562E9B7888B6D20D67ADDB5A90B68B54A51987
SHA-256:	E82CABB027DB8846C3430BE760F137AFA164C36F9E1B93A6E34C96DE0B2C5A5F
SHA-512:	27BA5D2F719AAAC2EAD6FB42F23AF3AA866F75026BE897CD2F561F3E383904E89E6043BD22B4AE24F69787BD258A68FF696C09C03D656CBF7C79C2A52D8D82CC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 8% • Antivirus: Metadefender, Detection: 3%, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....@.....0.....@.....<%.....:.....P.....CODE..... ..`DATA....`.....@...BSS....`.....idata..<%.....&.....@....tls.....@.....rdata.....P.....@..P.reloc.....`.....@..P.rsrc....:.....:.....@..P.....0.....@..P.....

C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\0JzI2az.exe

Process:	C:\Program Files (x86)\fnSearcher\fnsearcher68.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: 38%
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
Entropy (8bit):	7.997057951465239
TrID:	• Win32 Executable (generic) a (10002005/4) 97.43% • Win32 Executable PowerBASIC/Win 9.x (148305/79) 1.44% • Inno Setup installer (109748/4) 1.07% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	file.exe

File size:	2881497
MD5:	9156fa044ec274f670095e43e205d137
SHA1:	62107d1bd3cb01d59924433f1c8a97c7096d5fb7
SHA256:	861751b8c762f3332f12c1f4ff45c3108357b1debbde2a07a5e9d44e806ce88d
SHA512:	5bbf3a2d3050cf7994e07cb0b6c5fd5605c095cf7ca2e0d46c5434a248a47f3f2dcf506a63d93efc97d7ce0f8aae8efb21f253cb1a5745da291765295ad0ad9e
SSDEEP:	49152:Z2cj4MkOZSuwjh/SfJe0jMgewii3AY6YlqQB14ZohSzyx60KS1UX/EqA5hq:Mc5kOnwjh/SfJe0Ygew+Yt8i14ahGB0I
TLSH:	F5D53372B5A1923AC7900B796CBEE72AFC337D3D112D9A54B6AC530D9C1308B914CB97
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x40991c
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:	TERMINAL_SERVER_AWARE
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:	884310b1928934402ea6fec1dbd3cf5e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFCCh
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-24h], eax
call 00007FBBA8AC4AFFh
call 00007FBBA8AC5D06h
call 00007FBBA8AC7F31h
call 00007FBBA8AC7FB8h
call 00007FBBA8ACA65Fh
call 00007FBBA8ACA7C6h
xor eax, eax
push ebp
push 00409FC6h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx

Instruction
push ebp
push 00409F7Ch
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [0040C014h]
call 00007FBBA8ACB1F0h
call 00007FBBA8ACAD7Bh
lea edx, dword ptr [ebp-10h]
xor eax, eax
call 00007FBBA8AC8435h
mov edx, dword ptr [ebp-10h]
mov eax, 0040CDD4h
call 00007FBBA8AC4BB0h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [0040CDD4h]
mov dl, 01h
mov eax, 0040719Ch
call 00007FBBA8AC8CA0h
mov dword ptr [0040CDD8h], eax
xor edx, edx
push ebp
push 00409F5Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007FBBA8ACB260h
mov dword ptr [0040CDE0h], eax
mov eax, dword ptr [0040CDE0h]
cmp dword ptr [eax+0Ch], 01h
jne 00007FBBA8ACB39Ah
mov eax, dword ptr [0040CDE0h]
mov edx, 00000028h
call 00007FBBA8AC90A1h
mov edx, dword ptr [0040CDE0h]
cmp eax, dword ptr [edx+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd000	0x950	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x2800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xf000	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	0x9040	0x9200	False	0.610980308219178	data	6.5386448278888665	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xb000	0x248	0x400	False	0.3046875	data	2.711035285634283	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xc000	0xe34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xd000	0x950	0xa00	False	0.414453125	data	4.430733069799036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xe000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xf000	0x18	0x200	False	0.052734375	data	0.2044881574398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x10000	0x8a4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x2800	0x2800	False	0.332421875	data	4.465850706524941	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x11354	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Dutch	Netherlands
RT_ICON	0x1147c	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	Dutch	Netherlands
RT_ICON	0x119e4	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	Dutch	Netherlands
RT_ICON	0x11ccc	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	Dutch	Netherlands
RT_STRING	0x12574	0x2f2	data		
RT_STRING	0x12868	0x30c	data		
RT_STRING	0x12b74	0x2ce	data		
RT_STRING	0x12e44	0x68	data		
RT_STRING	0x12eac	0xb4	data		
RT_STRING	0x12f60	0xae	data		
RT_RCDATA	0x13010	0x2c	data		
RT_GROUP_ICON	0x1303c	0x3e	data	English	United States
RT_VERSION	0x1307c	0x3cc	data	English	United States
RT_MANIFEST	0x13448	0x383	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, SizeofResource, SetLastError, SetFilePointer, SetErrorMode, SetEndOfFile, RemoveDirectoryA, ReadFile, LockResource, LoadResource, LoadLibraryA, IsDBCSLeadByte, GetWindowsDirectoryA, GetVersionExA, GetUserDefaultLangID, GetSystemInfo, GetSystemDefaultLCID, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetFileSize, GetFileAttributesA, GetExitCodeProcess, GetEnvironmentVariableA, GetCurrentProcess, GetCommandLineA, GetACP, InterlockedExchange, FormatMessageA, FindResourceA, 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**
Dutch	Netherlands	
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:33:53.535412073 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:53.562572956 CET	80	49699	45.139.105.171	192.168.2.3
Nov 3, 2022 12:33:53.562913895 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:53.563388109 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:53.590500116 CET	80	49699	45.139.105.171	192.168.2.3
Nov 3, 2022 12:33:55.095246077 CET	80	49699	45.139.105.171	192.168.2.3
Nov 3, 2022 12:33:55.095343113 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:55.523766994 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:55.551086903 CET	80	49699	45.139.105.171	192.168.2.3
Nov 3, 2022 12:33:57.073425055 CET	80	49699	45.139.105.171	192.168.2.3
Nov 3, 2022 12:33:57.073540926 CET	49699	80	192.168.2.3	45.139.105.171
Nov 3, 2022 12:33:57.121674061 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.149096012 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.149339914 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.150227070 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.178580046 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.179069996 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.179179907 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.207458019 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.234786034 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235316992 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235409021 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235416889 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235436916 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235454082 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235461950 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235471010 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235479116 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235487938 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235501051 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235503912 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235519886 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235526085 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235536098 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235552073 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.235574007 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.235599995 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.262746096 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262777090 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262794018 CET	80	49700	107.182.129.235	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:33:57.262810946 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262826920 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262842894 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262859106 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262885094 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262904882 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262922049 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262938023 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262949944 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.262955904 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262973070 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.262989044 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263000011 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.263005018 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263022900 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263031960 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.263045073 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263052940 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.263067961 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263088942 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.263089895 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263113022 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.263118982 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.263150930 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290268898 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290293932 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290309906 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290326118 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290342093 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290359974 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290375948 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290393114 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290409088 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290410042 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290425062 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290440083 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290446043 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290456057 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290469885 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290472031 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290487051 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290498972 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290503025 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290518999 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290522099 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290534973 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290539980 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290551901 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290565968 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290568113 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290585041 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290592909 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290600061 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290615082 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290621042 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290632010 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290648937 CET	80	49700	107.182.129.235	192.168.2.3
Nov 3, 2022 12:33:57.290652037 CET	49700	80	192.168.2.3	107.182.129.235
Nov 3, 2022 12:33:57.290664911 CET	80	49700	107.182.129.235	192.168.2.3

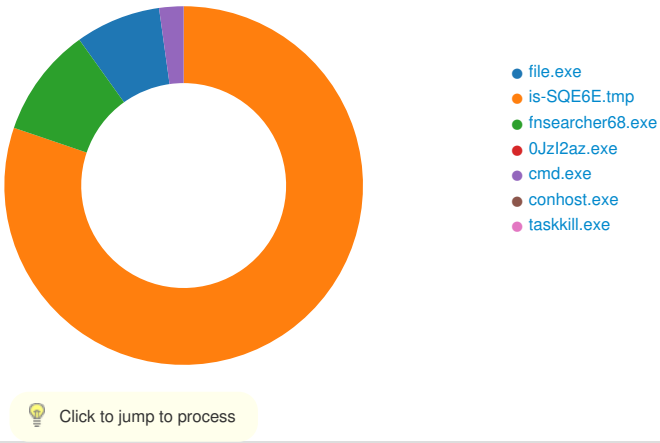
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:33:57.290679932 CET	49700	80	192.168.2.3	107.182.129.235

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: **5676**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:33:45
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	2881497 bytes
MD5 hash:	9156FA044EC274F670095E43E205D137
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: is-SQE6E.tmp PID: **5624**, Parent PID: **5676**

General

Target ID:	1
Start time:	12:33:46
Start date:	03/11/2022
Path:	C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp" /SL4 $30224 "C:\Users\user\Desktop\file.exe" 2630911 52736
Imagebase:	0x400000
File size:	673280 bytes
MD5 hash:	7CD12C54A9751CA6EEE6AB0C85FB68F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 8%, ReversingLabs • Detection: 3%, Metadefender, Browse
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-6LIA6.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	451DDF	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-6LIA6.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	473FFC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406E7A	CreateFileA
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406E7A	CreateFileA
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406E7A	CreateFileA
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_iscrypt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406E7A	CreateFileA
C:\Program Files (x86)\fnSearcher	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	450BF2	CreateDirectoryA
C:\Program Files (x86)\fnSearcher\unins000.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	46E58A	CreateFileA
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-51KLJ.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-OS12U.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-S6A9T.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-15O1T.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-8S345.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-DS22N.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-E8ARN.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA
C:\Program Files (x86)\fnSearcher\is-7C4Q3.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44F865	CreateFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	C:\Program Files (x86)\fnSearcher\unins000.exe	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-51KLJ.tmp	C:\Program Files (x86)\fnSearcher\fnsearcher68.exe	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-OS12U.tmp	C:\Program Files (x86)\fnSearcher\license_en.rtf	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-S6A9T.tmp	C:\Program Files (x86)\fnSearcher\license_ru.rtf	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-15O1T.tmp	C:\Program Files (x86)\fnSearcher\completed.wav	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-8S345.tmp	C:\Program Files (x86)\fnSearcher\reset.bat	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-DS22N.tmp	C:\Program Files (x86)\fnSearcher\unins.ico	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-E8ARN.tmp	C:\Program Files (x86)\fnSearcher\checksums.txt	success or wait	1	45110B	MoveFileA
C:\Program Files (x86)\fnSearcher\is-7C4Q3.tmp	C:\Program Files (x86)\fnSearcher\history.rtf	success or wait	1	45110B	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_RegDLL.tmp	0	3584	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 68 fa fd fd fd fd fd fd fd fd fd 48 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 7c fd fd fd fd fd fd 7c fd fd fd fd fd fd 7c fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 02 fd 25 45 00 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 02 00 00 00 08 00 00 00 00 00 00 fd 11 00 00 00 10 00 00 00 20 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$H|||RichPEL%E@	success or wait	1	406EC1	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_setup64.tmp	0	5632	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 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd 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 00 00 50 45 00 00 64 fd 05 00 fd 08 fd 45 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 10 02 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^I=\=\=\RichPEdE#	success or wait	1	406EC1	WriteFile
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_shfoldr.dll	0	23312	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 49 7a 4a 5e 0d 1b 24 0d 0d 1b 24 0d 0d 1b 24 0d 0d 1b 25 0d 22 1b 24 0d 54 38 37 0d 0b 1b 24 0d 5b 13 22 0d 0c 1b 24 0d 0d 1b 24 0d 0c 1b 24 0d 52 69 63 68 0d 1b 24 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 5c 3b 00 00 00 00 00 00 00 00 00 fd 00 06 23 0b 01 05 0c 00 20 00 00 00 34 00 00 00 00 00 00 fd 27 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$IzJ^$$$%"$T87$["$$$Rich$PEL\;# 4'	success or wait	1	406EC1	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-6LIA6.tmp_isetup_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>TcWb VcR<VcR? VcR9VcRichWcPELb@!	success or wait	1	406EC1	WriteFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.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	MZP@InUn!L!This program must be run under Win32$7	success or wait	11	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	48	4	49 6e 55 6e	InUn	success or wait	1	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	673021	21	72 65 71 75 69 72 65 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 22	requireAdministrator"	success or wait	1	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	673280	16	fd 50 fd 22 35 fd 21 fd 34 67 fd fd 7f 76 fd 1e	P"5!4gv	success or wait	2	44F9C0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	673296	10453	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 31 31 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 fd 00 00 00 fd 28 00 00 2a fd fd fd fd 65 6e 5e 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 (5.1.11)(*en^&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	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-51KLJ.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 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 fd 63 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 06 00 00 40 fd 00 00 00 00 00 40 fd 06 00 00 10 00 00 00 00 07 00 00 00 40 00 00 10 00 00 00 10 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 fd 23 01 00 10 00 00 00 00 00 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.$PELcc@@@#	success or wait	68	44F9C0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-OS12U.tmp	0	44011	7b 5c 72 74 66 31 5c 61 64 65 66 6c 61 6e 67 31 30 32 35 5c 61 6e 73 69 5c 61 6e 73 69 63 70 67 31 32 35 31 5c 75 63 31 5c 61 64 65 66 66 30 5c 64 65 66 66 30 5c 73 74 73 68 66 64 62 63 68 30 5c 73 74 73 68 66 6c 6f 63 68 30 5c 73 74 73 68 66 68 69 63 68 30 5c 73 74 73 68 66 62 69 30 5c 64 65 66 6c 61 6e 67 31 30 34 39 5c 64 65 66 6c 61 6e 67 66 65 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 66 65 30 5c 74 68 65 6d 65 6c 61 6e 67 63 73 30 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 62 69 64 69 20 5c 66 72 6f 6d 61 6e 5c 66 63 68 61 72 73 65 74 32 30 34 5c 66 70 72 71 32 7b 5c 2a 5c 70 61 6e 6f 73 65 20 30 32 30 32 30 36 30 33 30 35 30 34 30 35 30 32 30 33 30 34 7d 54 69 6d 65 73 20 4e 65 77 20 52 6f 6d 61 6e 3b 7d	{\rtf1\adeflang1025\ansi\ansic pg1251\uc1\adeff0\deff0\stshfd bch0\stshfloch0\stshfhich0\sts hfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\t hemelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}	success or wait	1	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-S6A9T.tmp	0	51922	7b 5c 72 74 66 31 5c 61 64 65 66 6c 61 6e 67 31 30 32 35 5c 61 6e 73 69 5c 61 6e 73 69 63 70 67 31 32 35 31 5c 75 63 31 5c 61 64 65 66 66 30 5c 64 65 66 66 30 5c 73 74 73 68 66 64 62 63 68 30 5c 73 74 73 68 66 6c 6f 63 68 30 5c 73 74 73 68 66 68 69 63 68 30 5c 73 74 73 68 66 62 69 30 5c 64 65 66 6c 61 6e 67 31 30 34 39 5c 64 65 66 6c 61 6e 67 66 65 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 66 65 30 5c 74 68 65 6d 65 6c 61 6e 67 63 73 30 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 62 69 64 69 20 5c 66 72 6f 6d 61 6e 5c 66 63 68 61 72 73 65 74 32 30 34 5c 66 70 72 71 32 7b 5c 2a 5c 70 61 6e 6f 73 65 20 30 32 30 32 30 36 30 33 30 35 30 34 30 35 30 32 30 33 30 34 7d 54 69 6d 65 73 20 4e 65 77 20 52 6f 6d 61 6e 3b 7d	{\rtf1\adeflang1025\ansi\ansic pg1251\uc1\adeff0\deff0\stshfd bch0\stshfloch0\stshfhich0\sts hfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\t hemelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}	success or wait	1	44F9C0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-15O1T.tmp	0	65536	52 49 46 46 fd 26 04 00 57 41 56 45 66 6d 74 20 12 00 00 00 01 00 02 00 44 fd 00 00 10 fd 02 00 04 00 10 00 00 00 4c 49 53 54 fd 00 00 00 49 4e 46 4f 49 41 52 54 1f 00 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 49 43 4d 54 1d 00 00 00 6d 70 33 63 75 74 2e 72 75 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 49 43 52 44 05 00 00 00 20 20 20 20 00 00 49 4e 41 4d 1f 00 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 49 50 52 44 1f 00 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 49 50 52 54 02 00 00 00 31 00 49 53 46 54 0e 00 00 00 4c 61 76 66 35 35 2e 32 32 2e 31 30 30 00 64	RIFF&WAVEfmt DLISTINFOIART ICMTmp3cut.ru ICRD INAM IPRD IPRT1ISFTLavf55. 22.100d	success or wait	5	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-8S345.tmp	0	20	6e 53 65 61 72 63 68 65 72 2e 65 78 65 20 2f 72 65 73 65 74	nSearcher.exe /reset	success or wait	1	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-DS22N.tmp	0	65536	00 00 01 00 07 00 30 30 00 00 01 00 20 00 fd 25 00 00 76 00 00 00 20 20 00 00 01 00 20 00 fd 10 00 00 1e 26 00 00 10 10 00 00 01 00 20 00 68 04 00 00 fd 36 00 00 00 00 00 00 01 00 20 00 03 fd 00 00 2e 3b 00 00 fd fd 00 00 01 00 20 00 28 08 01 00 31 fd 00 00 40 40 00 00 01 00 20 00 28 42 00 00 59 fd 01 00 18 18 00 00 01 00 20 00 fd 09 00 00 fd 05 02 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 00 00 00 00 00 fd 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd fd 00 fd fd fd 06 fd fd fd 07 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd	00 %v & h6 .; (1@@ (BY (0` %	success or wait	3	44F9C0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\is-E8ARN.tmp	0	356	41 6c 6c 20 63 68 65 63 6b 73 75 6d 20 69 6e 20 4d 44 35 0d 0a 0d 0a 63 6f 6d 70 6c 65 74 65 64 2e 77 61 76 09 09 38 65 34 36 62 65 35 61 34 31 35 35 37 31 30 33 36 31 31 38 31 65 33 62 36 37 33 37 33 34 30 34 0d 0a 68 69 73 74 6f 72 79 2e 72 74 66 09 09 31 62 66 63 64 65 32 62 33 64 35 35 37 63 66 62 38 62 39 30 30 34 30 35 35 64 33 61 39 30 66 35 0d 0a 6c 69 63 65 6e 73 65 5f 65 6e 2e 72 74 66 09 09 31 61 65 36 32 66 30 30 66 63 33 36 38 33 36 34 61 32 64 65 36 36 38 62 33 32 39 39 64 37 39 33 0d 0a 6c 69 63 65 6e 73 65 5f 72 75 2e 72 74 66 09 09 66 65 37 63 39 63 36 66 36 65 38 66 37 32 30 66 38 38 36 62 63 63 36 35 66 61 32 64 39 62 32 30 0d 0a 6e 73 65 61 72 63 68 65 72 2e 65 78 65 09 09 63 35 65 37 61 63 62 64 61 32 66 38 62 66 61 34 39 62 64 39 35	All checksum in MD5completed.wav8e46be5a4155710361181e3b67373404history.rtf1bfcde2b3d557cfb8b9004055d3a90f5license_en.rtf1ae62f00fc368364a2de668b3299d793license_ru.rtffe7c9c6f6e8f720f886bcc65fa2d9b20nsearcher.exec5e7acbda2f8bfa49bd95	success or wait	1	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\is-7C4Q3.tmp	0	44381	7b 5c 72 74 66 31 5c 61 64 65 66 6c 61 6e 67 31 30 32 35 5c 61 6e 73 69 5c 61 6e 73 69 63 70 67 31 32 35 31 5c 75 63 31 5c 61 64 65 66 66 30 5c 64 65 66 66 30 5c 73 74 73 68 66 64 62 63 68 30 5c 73 74 73 68 66 6c 6f 63 68 30 5c 73 74 73 68 66 68 69 63 68 30 5c 73 74 73 68 66 62 69 30 5c 64 65 66 6c 61 6e 67 31 30 34 39 5c 64 65 66 6c 61 6e 67 66 65 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 31 30 34 39 5c 74 68 65 6d 65 6c 61 6e 67 66 65 30 5c 74 68 65 6d 65 6c 61 6e 67 63 73 30 7b 5c 66 6f 6e 74 74 62 6c 7b 5c 66 30 5c 66 62 69 64 69 20 5c 66 72 6f 6d 61 6e 5c 66 63 68 61 72 73 65 74 32 30 34 5c 66 70 72 71 32 7b 5c 2a 5c 70 61 6e 6f 73 65 20 30 32 30 32 30 36 30 33 30 35 30 34 30 35 30 32 30 33 30 34 7d 54 69 6d 65 73 20 4e 65 77 20 52 6f 6d 61 6e 3b 7d	{\rtf1\adeflang1025\ansi\ansicpg1251\uc1\adeff0\deff0\stshfdbch0\stshfloch0\stshfhich0\stshfbi0\deflang1049\deflangfe1049\themelang1049\themelangfe0\themelangcs0{\fonttbl{\f0\fbidi \froman\fcharset204\fprq2{*\panose 02020603050405020304}Times New Roman;}	success or wait	1	44F9C0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\fnSearcher\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 62 32 36 34 61 31 38 45 2d 39 31 42 34 2d 34 39 31 30 2d 39 30 30 36 2d 38 62 66 33 37 31 32 34 62 36 39 35 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 46 4e 53 65 61 72 63 68 65 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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){b264a18E-91B4-4910-9006-8bf37124b695}FNSearcher	success or wait	2	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\unins000.dat	448	12	fd 0c 00 00 08 fd fd fd 5d fd fd 33	]3	success or wait	2	44F9C0	WriteFile
C:\Program Files (x86)\fnSearcher\fnsearcher68.exe	0	1	4d	M	success or wait	1	44092E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp	unknown	4	success or wait	1	44F8F0	ReadFile
C:\Users\user\Desktop\file.exe	unknown	64	success or wait	1	44F8F0	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	44F8F0	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	44F8F0	ReadFile
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp	unknown	65536	success or wait	1	44F8F0	ReadFile
C:\Users\user\AppData\Local\Temp\is-VVS8D.tmp\is-SQE6E.tmp	unknown	65536	success or wait	10	44F8F0	ReadFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	unknown	2	success or wait	13	44F8F0	ReadFile
C:\Program Files (x86)\fnSearcher\is-6KAKC.tmp	unknown	16	success or wait	10	44F8F0	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	8	44F8F0	ReadFile
C:\Users\user\Desktop\file.exe	unknown	5	success or wait	8	44F8F0	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	success or wait	1	42DC15	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	Inno Setup: Setup Version	unicode	5.1.11	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	Inno Setup: App Path	unicode	C:\Program Files (x86)\fnSearcher	success or wait	1	468C3C	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	InstallLocation	unicode	C:\Program Files (x86)\fnSearcher\	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	Inno Setup: Icon Group	unicode	fnSearcher	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	Inno Setup: User	unicode	hardz	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	DisplayName	unicode	fnSearcher 2.68	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	UninstallString	unicode	"C:\Program Files (x86)\fnSearcher\unins000.exe"	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	QuietUninstallString	unicode	"C:\Program Files (x86)\fnSearcher\unins000.exe" /SILENT	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	DisplayVersion	unicode	1.2.2.68	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	Publisher	unicode	FNSearcher	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	URLInfoAbout	unicode	http://www.fn-group.info/	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	HelpLink	unicode	http://www.fn-group.info/fnsearcher/help.html	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	URLUpdateInfo	unicode	http://www.fn-group.info/fnsearcher/download.html	success or wait	1	468C3C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	NoModify	dword	1	success or wait	1	468C9C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	NoRepair	dword	1	success or wait	1	468C9C	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b264a18E-91B4-4910-9006-8bf37124b695}_is1	InstallDate	unicode	20221103	success or wait	1	468C3C	RegSetValueExA

Analysis Process: fnsearcher68.exe PID: **3080**, Parent PID: **5624**

General

Target ID:	2
Start time:	12:33:49
Start date:	03/11/2022
Path:	C:\Program Files (x86)\fnSearcher\fnsearcher68.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\fnSearcher\fnsearcher68.exe"
Imagebase:	0x400000
File size:	4448253 bytes
MD5 hash:	3FCA96750E2F656A73FBC6A896F53209
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: 00000002.00000002.345115638.00000000037D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000002.00000002.343591826.0000000000400000.00000040.00000001.01000000.00000007.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}\0JzI2az.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	42874A	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\count[1].htm	0	1	30	0	success or wait	1	401BDA	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\0JzI2az.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 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 fd fd 1b fd fd fd fd fd fd fd fd 24 fd fd fd fd fd 24 fd fd fd 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 2e fd 39 fd fd fd fd 2e fd 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 00	MZ@!L!This program cannot be run in DOS mode.$..9.Rich	success or wait	1	421524	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\count[1].htm	0	1	30	0	success or wait	1	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\WJ8I2OL4\library[1].htm	0	1	30	0	success or wait	6	100010BA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\library[1].htm	0	1	30	0	success or wait	5	100010BA	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 0JzI2az.exe PID: **4556**, Parent PID: **3080**

General

Target ID:	3
Start time:	12:33:55
Start date:	03/11/2022
Path:	C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\0JzI2az.exe
Wow64 process (32bit):	true
Commandline:	

Imagebase:	0xa10000
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: 38%, ReversingLabs
Reputation:	moderate

Analysis Process: cmd.exe PID: **4392**, Parent PID: **3080**

General

Target ID:	13
Start time:	12:34:29
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "fnsearcher68.exe" /f & erase "C:\Program Files (x86)\fnSearcher\fnsearcher68.exe" & exit
Imagebase:	0xb0000
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)\fnSearcher\fnsearcher68.exe	cannot delete	1	D0374	DeleteFileW
C:\Program Files (x86)\fnSearcher\fnsearcher68.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: **3328**, Parent PID: **4392**

General

Target ID:	14
Start time:	12:34:29
Start date:	03/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4692**, Parent PID: **4392**

General

Target ID:	15
Start time:	12:34:29
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "fnsearcher68.exe" /f
Imagebase:	0x1070000
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