ID: 877011
Sample Name: 1ibwQtrqNy.exe
Cookbook: default.jbs
Time: 14:30:06
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

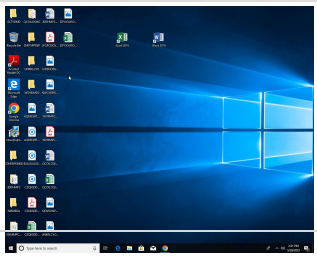
Windows Analysis Report

1ibwQtrqNy.exe

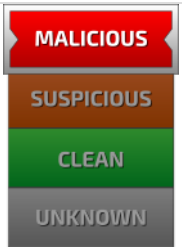
Overview

General Information

Sample Name:	1ibwQtrqNy.exe
Original Sample Name:	65dd3ed482f22..
Analysis ID:	877011
MD5:	65dd3ed482f22..
SHA1:	ffe8496a9d3f0a..
SHA256:	15f5d9cd2cb95..
Tags:	32 exe trojan
Infos:	



Detection



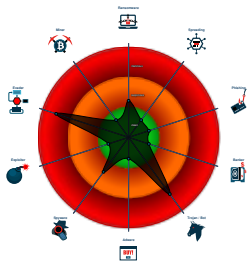
Nymaim

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

Signatures

- Found malware configuration
- 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
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- 1ibwQtrqNy.exe (PID: 4080 cmdline: C:\Users\user\Desktop\1ibwQtrqNy.exe MD5: 65DD3ED482F22906E70DD004A73E5CEF)
  - is-2H2P0.tmp (PID: 4944 cmdline: "C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp" /SL4 $2048E "C:\Users\user\Desktop\1ibwQtrqNy.exe" 1911253 52224 MD5: 1F2BC482C99F55A713CF6CA3C1FF04F8)
    - Rec528.exe (PID: 2576 cmdline: "C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe" MD5: 9D3532E4DB1BBBCCA78E0D2DC8AE2572)
      - IFLIjCfKSqd.exe (PID: 7052 cmdline: MD5: 3FB36CB0B7172E5298D2992D42984D06)
      - cmd.exe (PID: 5924 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "Rec528.exe" /f & erase "C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - taskkill.exe (PID: 2288 cmdline: taskkill /im "Rec528.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nymaim	Nymaim is a trojan downloader. It downloads (and runs) other malware on affected systems and was one of the primary malware families hosted on Avalanche. Nymaim is different in that it displays a localized lockscreen while it downloads additional malware. Nymaim is usually delivered by exploit kits and malvertising.	No Attribution	http://https://arielkoren.com/blog/2016/11/02/nymaim-deep-technical-dive-adventures-in-evasive-malware/https://bitbucket.org/daniel_plohmann/idapatchworkhttps://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/https://blog.talosintelligence.com/goznym/https://github.com/coldshell/Malware-Scripts/tree/master/Nymaim	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim

Malware Configuration

Threatname: Nymaim


```
{
  "C2 addresses": [
    "45.12.253.56",
    "45.12.253.72",
    "45.12.253.98",
    "45.12.253.75"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.443567321.0000000003260000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000002.00000002.442855707.0000000000400000.00000040.00000001.01000000.00000007.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Rec528.exe.400000.1.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.Rec528.exe.3260000.3.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.Rec528.exe.400000.1.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.Rec528.exe.3260000.3.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN GCleaner CnC Checkin M1 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.72

Timestamp:	192.168.2.345.12.253.7249698802044031 05/28/23-14:31:02.886782
SID:	2044031
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN GCleaner CnC Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 45.12.253.75

Timestamp:	192.168.2.345.12.253.7549699802044033 05/28/23-14:31:35.542564
SID:	2044033
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN GCleaner Payload Retrieval Attempt - Source IP: 192.168.2.3 - Destination IP: 45.12.253.72

Timestamp:	192.168.2.345.12.253.7249698802044032 05/28/23-14:31:02.924623

SID:	2044032
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN GCleaner Downloader - Payload Response - Source IP: 45.12.253.72 - Destination IP: 192.168.2.3	−
Timestamp:	45.12.253.72192.168.2.380496982044037 05/28/23-14:31:02.950793
SID:	2044037
Source Port:	80
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential GCleaner CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 45.12.253.56	−
Timestamp:	192.168.2.345.12.253.5649697802044034 05/28/23-14:31:02.810921
SID:	2044034
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Compliance

- Detected unpacking (overwrites its own PE header)

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected Nymaim

Data Obfuscation

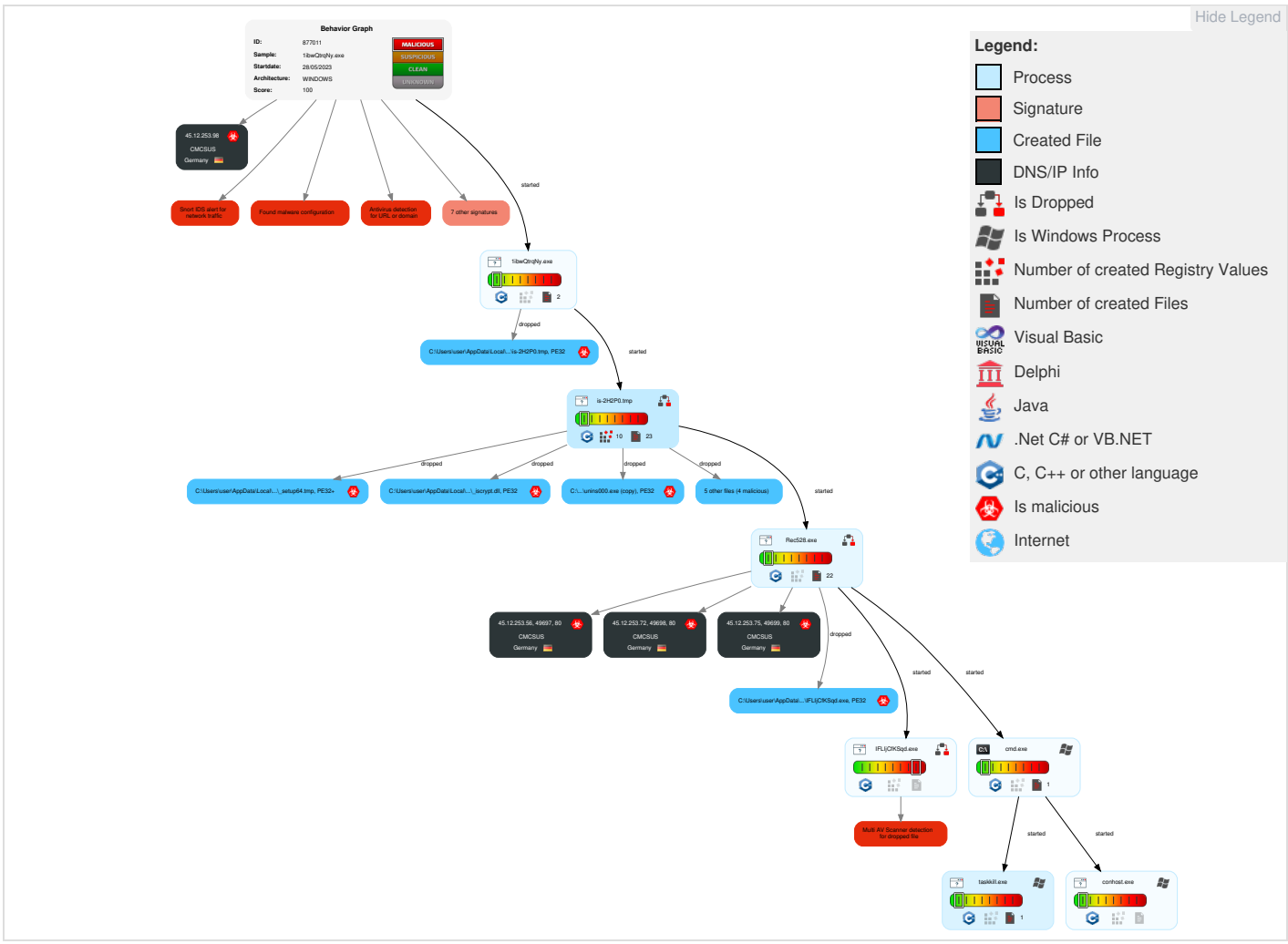
- Detected unpacking (overwrites its own PE header)
- Detected unpacking (changes PE section rights)

Stealing of Sensitive Information

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 3 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 4 1 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 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Process Injection	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

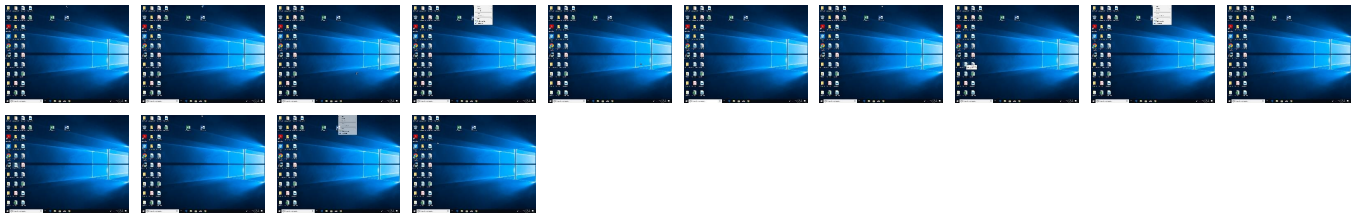
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1ibwQtrqNy.exe	20%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	100%	Avira	HEUR/AGEN.1314978	
C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\FLSCover\Rec528\Preview.exe (copy)	0%	ReversingLabs		
C:\Program Files (x86)\FLSCover\Rec528\is-Q8OGG.tmp	0%	ReversingLabs		
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	3%	ReversingLabs		
C:\Program Files (x86)\FLSCover\Rec528\unins000.exe (copy)	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_iscrypt.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_shfoldr.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\IFLIjCfKSqd.exe	62%	ReversingLabs	Win32.Trojan.GenusAgent	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://45.12.253.72/default/stuk.php	0%	URL Reputation	safe	
http://www.finalrecovery.com/buy.htm	0%	URL Reputation	safe	
http://www.remobjects.com/?ps	0%	URL Reputation	safe	
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixinte	0%	URL Reputation	safe	
http://45.12.253.72/default/puk.php	0%	URL Reputation	safe	
http://45.12.253.75/dll.php	0%	URL Reputation	safe	
http://www.innosetup.com	0%	URL Reputation	safe	
http://www.remobjects.com/?psU	0%	URL Reputation	safe	
http://45.12.253.75/dll.phpi	100%	Avira URL Cloud	malware	
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixintej	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phph	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phpd	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.php%	100%	Avira URL Cloud	malware	
http://45.12.253.72/del.php	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phpQ	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phpP	100%	Avira URL Cloud	malware	
http://45.12.253.72/default/stuk.phpi	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phpX	100%	Avira URL Cloud	malware	
http://www.innosetup.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://45.12.253.72/default/stuk.phpt	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phpL	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.phps	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.php4	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.php0	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.php9	100%	Avira URL Cloud	malware	
http://45.12.253.75/dll.php8	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.12.253.72/default/stuk.php	true	• URL Reputation: safe	unknown
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixinte	true	• URL Reputation: safe	unknown
http://45.12.253.72/default/puk.php	true	• URL Reputation: safe	unknown
http://45.12.253.75/dll.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	is-2H2P0.tmp, is-2H2P0.tmp, 00000001.000 00002.444700726.0000000000401000.0000002 0.00000001.01000000.00000004.sdmp, is-2H 2P0.tmp.0.dr, is-U3J98.tmp.1.dr	false	• URL Reputation: safe	unknown

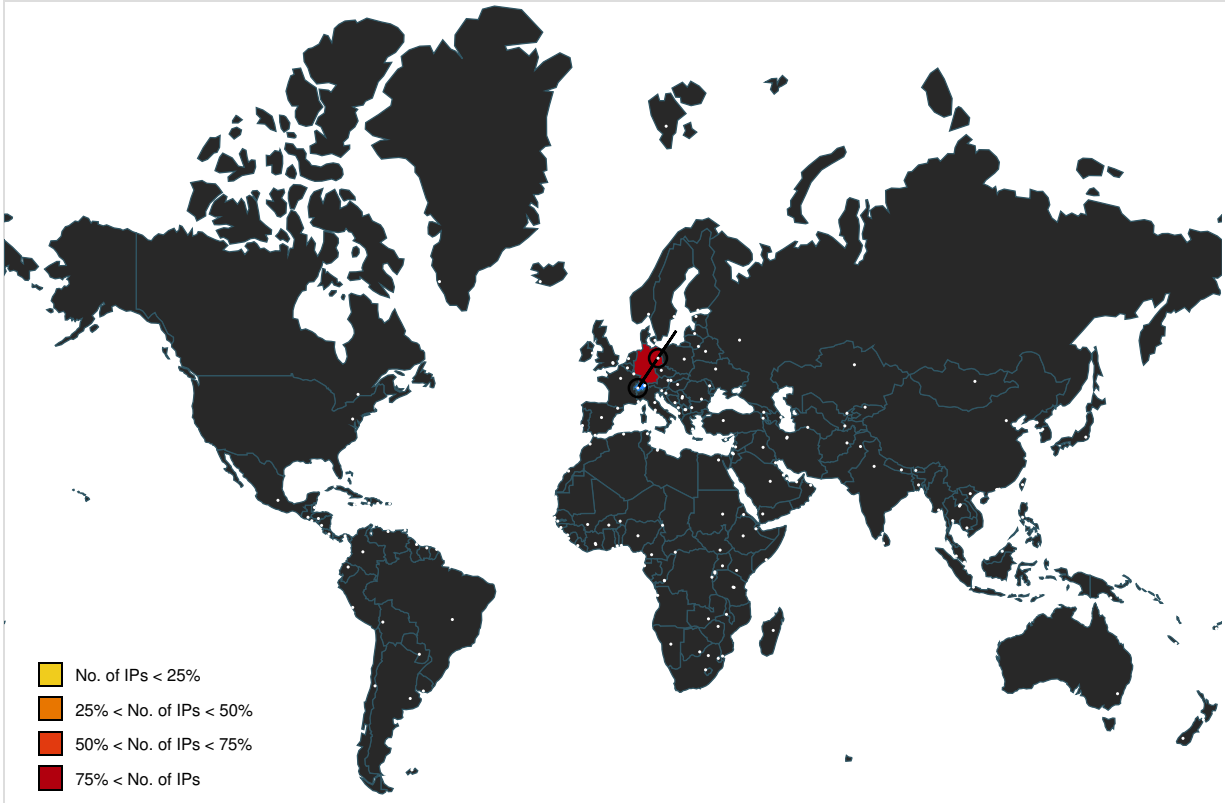
Name	Source	Malicious	Antivirus Detection	Reputation
http://45.12.253.75/dll.phpd	Rec528.exe, 00000002.00000003.367385976.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.373976623.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.imagemagick.org	is-EJ9G4.tmp.1.dr	false		high
http://https://macrorit.com/free-software.html	is-2H2P0.tmp, 00000001.00000002.445963159.0000000004BC0000.00000004.00001000.00020000.00000000.sdmp, Rec528.exe, 00000002.00000000.355680126.0000000001271000.00000002.00000001.01000000.00000007.sdmp, Rec528.exe.1.dr, is-EJ9G4.tmp.1.dr	false		high
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixintej	Rec528.exe, 00000002.00000002.443117659.000000000165A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phpi	Rec528.exe, 00000002.00000003.422045948.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phph	Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.php%	Rec528.exe, 00000002.00000003.422045948.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.72/del.php	Rec528.exe, 00000002.00000003.373976623.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430360645.000000001745000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.367385976.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phpQ	Rec528.exe, 00000002.00000003.415189342.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.finalrecovery.com/buy.htm	is-0I9HC.tmp.1.dr	false	• URL Reputation: safe	unknown
http://www.remobjects.com/?ps	1ibwQtrqNy.exe, 00000000.00000003.351264625.00000000021B0000.00000004.00001000.00020000.00000000.sdmp, 1ibwQtrqNy.exe, 00000000.00000003.351368763.0000000001FD8000.00000004.00001000.00020000.00000000.sdmp, is-2H2P0.tmp, is-2H2P0.tmp, 00000001.00000002.444700726.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-2H2P0.tmp.0.dr, is-U3J98.tmp.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.12.253.75/dll.phpP	Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.72/default/stuk.phpi	Rec528.exe, 00000002.00000002.443117659.0000000001700000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://macrorit.com/disk-wiper-commercial-license-upgrade.html	is-2H2P0.tmp, 00000001.00000002.445963159.0000000004BC0000.00000004.00001000.00020000.00000000.sdmp, Rec528.exe, 00000002.00000000.355680126.0000000001271000.00000002.00000001.01000000.00000007.sdmp, Rec528.exe.1.dr, is-EJ9G4.tmp.1.dr	false		high
http://45.12.253.75/dll.phpX	Rec528.exe, 00000002.00000003.380624834.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.innosetup.comDVarFileInfo$	1ibwQtrqNy.exe, 00000000.00000003.351264625.00000000021B0000.00000004.00001000.00020000.00000000.sdmp, 1ibwQtrqNy.exe, 00000000.00000003.351368763.0000000001FD8000.00000004.00001000.00020000.00000000.sdmp, is-2H2P0.tmp, 00000001.00000000.351821763.000000000004BC000.00000002.00000001.01000000.00000004.sdmp, is-2H2P0.tmp.0.dr, is-U3J98.tmp.1.dr	false	• Avira URL Cloud: safe	low
http://45.12.253.72/default/stuk.phpt	Rec528.exe, 00000002.00000002.443117659.0000000001700000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phpL	Rec528.exe, 00000002.00000003.395381822.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phpH	Rec528.exe, 00000002.00000003.380624834.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.12.253.75/dll.phps	Rec528.exe, 00000002.00000003.422045948.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.php4	Rec528.exe, 00000002.00000003.395381822.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.php0	Rec528.exe, 00000002.00000003.395381822.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.phpp	Rec528.exe, 00000002.00000003.373976623.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://www.innosetup.com	1ibwQtrqNy.exe	false	• URL Reputation: safe	unknown
http://45.12.253.75/dll.php9	Rec528.exe, 00000002.00000003.373976623.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://45.12.253.75/dll.php8	Rec528.exe, 00000002.00000002.443117659.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.373976623.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.0000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.0000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.415189342.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.367385976.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.401932962.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.408599172.000000000173B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.12.253.75/dll.phpx	Rec528.exe, 00000002.00000003.373976623.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.0000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.395381822.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.422045948.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.430338328.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.380624834.0000000001723000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.000000000173B000.00000004.00000020.00020000.00000000.sdmp, Rec528.exe, 00000002.00000003.388832564.0000000001723000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://www.remobjects.com/?psU	1ibwQtrqNy.exe, 00000000.00000003.351264625.00000000021B0000.00000004.00001000.00020000.00000000.sdmp, 1ibwQtrqNy.exe, 00000000.00000003.351368763.0000000001FD8000.00000004.00001000.00020000.00000000.sdmp, is-2H2P0.tmp, 00000001.00000002.444700726.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-2H2P0.tmp.0.dr, is-U3J98.tmp.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.12.253.72	unknown	Germany		33657	CMCSUS	true
45.12.253.75	unknown	Germany		33657	CMCSUS	true
45.12.253.98	unknown	Germany		33657	CMCSUS	true
45.12.253.56	unknown	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877011
Start date and time:	2023-05-28 14:30:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	9
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
Sample file name:	1ibwQtrqNy.exe
Original Sample Name:	65dd3ed482f22906e70dd004a73e5cef.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@12/23@0/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44.2% (good quality ratio 43.2%) • Quality average: 85.3% • Quality standard deviation: 23.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly 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
14:31:01	API Interceptor	1x Sleep call for process: IFLIjCfKSqd.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)\FLSCover\Rec528\Preview.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	791040
Entropy (8bit):	6.608982798504157
Encrypted:	false
SSDEEP:	24576:pvfBdvyjNf8cbMtMJjLKRfwaNSkxtkNkYzSYcj0oHyxdpVhNZFGv+56nBb/ExWyt:pBC4rTQnC1QaX4+I
MD5:	5C2FE7D4DDE65810152054F3C93C1815
SHA1:	2A19F3FAA78A5072068F7902DB19A248F11FA69B
SHA-256:	233D846FEB73A38141BDF6C813C7476FA3F66DCD3548338607F3B7CB61CAC730
SHA-512:	2C01AE918044829FC649F0775BF3FFDB417B1524B47CDABFF0C06B6382B6578A742D9C1D036090D7AD1FC3A8B7D563D28C0CDB94DE572BF883389825F73FD65
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....\|.....$.....@.....@.....@...,...0.....DH..... .....text...D{.....|..... ..`.itext..l..... ..`.data...l8.....:.....@....bss.....C.....idata...,...@.....@....tls....4....p.. .....rdata.....@..@.reloc.....@..B.rsrc.....0.....@..@.....@..@..... .....

C:\Program Files (x86)\FLSCover\Rec528\Readme.txt (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1949
Entropy (8bit):	4.915453283427292
Encrypted:	false
SSDEEP:	48:Sik3C0nGTAFE3blB/aMO0Mk2fLXVn7K+eq9hb6Suf:pkvGTAFELlB/A4GXVnWU9BNuf
MD5:	C0AE85DB30FE9027DBBF3BA758FA78BE
SHA1:	95E69DB95504A9F61D090690F32FB5D2F685C604
SHA-256:	CF63BBFD735C18757AC2AA6CB8A14C82745B6158F9FD299BD189D9CA3E7A2DE7
SHA-512:	DA53177074E79F96C1C7E477E0E7B63CD1D2B836DB9E8066F20B60897FC5770D2B16594A84A953A9CD56BD4C0DDB7D5EFBDDF881EEA840D6B106552C5AC685E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.. F i n a l R e c o v e r y v3.0.7.0325....Overview ..========....FinalRecovery is a powerful and easy-to-use file recovery software. It is suitable ..for various data recovery situations. Some of those situations are listed below. ....1 Recover accidentally deleted files (files were deleted by using windows explorer, .. command line, other software utilities; files which lost while empting recycle .. bin; file losses which caused by unknown reasons); ..2 Recover files from accidentally formatted disk volume; ..3 Recover files from lost partitions (the cases may be partition deletion, disk .. repartitioning, partition losses which caused by virus or other reasons) or .. corrupted partitions; ..4 Recover files from drive image files; ..5 Predict drive failures (doesn't support SCSI hard drives, removable hard drives). ....FinalRecovery supports FAT12, FAT16, FAT32, NTFS, NTFS5 and Raw file system. It can ..recover files from hard disks, floppies, U disks, PCMCIA-

C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	2491753
Entropy (8bit):	6.2535337137307625
Encrypted:	false
SSDEEP:	24576:TzyEzyqd/zyCzytzy3ozyikzy3DKzyH1cuu7hhyGW1G4dPApP8Xv+MysNKt19crT:PTIxvnu7byGx4Ff+MyOe19UuRDy
MD5:	9D3532E4DB1BBBCCA78E0D2DC8AE2572
SHA1:	E6F4EE6D2AEF36909CA0330BA03798AB76493CA8
SHA-256:	A9BAEFA9E8C28E5E028E19691EF04E5C85E94F0F81B4CF6844A9C63D9A22F3A1
SHA-512:	21B6265DF422B7F61D2FF8E5F87AFEBD4B0642806A3E88F50B39211AD4315349137C7CC2AD2441CE870CE09CF1A1790043C668BFF564C90C01775C04981ECBA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0,sd.....B.....@..... .....\.....\.....8.....$.....text..... ..`.rdata..z!.....0.....@..@.data...@..... .....@....tls.....@....rsrc....`.....`.....@..@.fls528.....p..i....p.....`..... ....

C:\Program Files (x86)\FLSCover\Rec528\data\Config.xml (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	XML 1.0 document, ASCII text, with very long lines (5978), with CRLF line terminators
Category:	dropped
Size (bytes):	6452
Entropy (8bit):	4.734154041089812
Encrypted:	false
SSDEEP:	96:EonMpdbxw/+9MjLKJ9+LsxS/wV2iderMRyLjQ1WsL+9w/SxEDz8bONAPujBUTjkv:E7nb
MD5:	247D3A0C3B0C53CA33D032A561619495
SHA1:	F30570C48749FE427FACCBDF925048B149D22460
SHA-256:	783AC8FBA1DD88291A4F331EC2459DDE4005CF70FAFB4F19F9061713FFD580EB
SHA-512:	9D18FDC8A32C86A0F8C2BB408A33A71645632289CA0D684B58B98862AA1A67E75258D39C621F4E647753A1480D50444756D125C273B16323A757270CD94B7BBD
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<Settings>...<Misc readyinform="True" showdlgonclick="True" adjustmentquery="True"/>...<Enhanced structu rematch="False"/>...<FileTypes expand="True">....<Type ext="rar"/><Type ext="zip"/><Type ext="doc"/><Type ext="xls"/><Type ext="ppt"/></FileTypes>...<RawRecover y>....<DefaultSize><Type major="0" minor="0" defaultsize="1" maxsize="20"/><Type major="0" minor="1" defaultsize="1" maxsize="20"/><Type major="0" minor="2" def aultsize="1" maxsize="20"/><Type major="0" minor="3" defaultsize="1" maxsize="20"/><Type major="0" minor="4" defaultsize="1" maxsize="20"/><Type major="0" minor ="5" defaultsize="1" maxsize="20"/><Type major="0" minor="6" defaultsize="1" maxsize="20"/><Type major="0" minor="7" defaultsize="1" maxsize="20"/><Type major=" 0" minor="8" defaultsize="1" maxsize="20"/><Type major="0" minor="9" defaultsize="1" maxsize="20"/><Type major="0" minor="10" defaultsize="1" maxsize="20"/><Type major="0" minor="11" defaultsize="1" m

C:\Program Files (x86)\FLSCover\Rec528\data\is-002RD.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	XML 1.0 document, ASCII text, with very long lines (5978), with CRLF line terminators
Category:	dropped
Size (bytes):	6452
Entropy (8bit):	4.734154041089812
Encrypted:	false
SSDEEP:	96:EonMpdbxw/+9MjLKJ9+LsxS/wV2iderMRyLjQ1WsL+9w/SxEDz8bONAPujBUTjkv:E7nb
MD5:	247D3A0C3B0C53CA33D032A561619495
SHA1:	F30570C48749FE427FACCBDF925048B149D22460
SHA-256:	783AC8FBA1DD88291A4F331EC2459DDE4005CF70FAFB4F19F9061713FFD580EB
SHA-512:	9D18FDC8A32C86A0F8C2BB408A33A71645632289CA0D684B58B98862AA1A67E75258D39C621F4E647753A1480D50444756D125C273B16323A757270CD94B7BBD
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>..<Settings>...<Misc readyinform="True" showdlgonclick="True" adjustmentquery="True"/>...<Enhanced structu rematch="False"/>...<FileTypes expand="True">....<Type ext="rar"/><Type ext="zip"/><Type ext="doc"/><Type ext="xls"/><Type ext="ppt"/></FileTypes>...<RawRecover y>....<DefaultSize><Type major="0" minor="0" defaultsize="1" maxsize="20"/><Type major="0" minor="1" defaultsize="1" maxsize="20"/><Type major="0" minor="2" def aultsize="1" maxsize="20"/><Type major="0" minor="3" defaultsize="1" maxsize="20"/><Type major="0" minor="4" defaultsize="1" maxsize="20"/><Type major="0" minor ="5" defaultsize="1" maxsize="20"/><Type major="0" minor="6" defaultsize="1" maxsize="20"/><Type major="0" minor="7" defaultsize="1" maxsize="20"/><Type major=" 0" minor="8" defaultsize="1" maxsize="20"/><Type major="0" minor="9" defaultsize="1" maxsize="20"/><Type major="0" minor="10" defaultsize="1" maxsize="20"/><Type major="0" minor="11" defaultsize="1" m

C:\Program Files (x86)\FLSCover\Rec528\finalrecovery.chm (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	553405
Entropy (8bit):	7.979175020825392
Encrypted:	false
SSDEEP:	12288:G8kCp81lkXlwDvsttKcoKRWqZPP4owP1G2uQeDyXwaWt:HJp3kXlDvKwRWg4owdGueDiwaWt
MD5:	37E6EEA8C4E469F6439F3790166815DD
SHA1:	E0A3768F291CC7FCE178A001F0356D4FBA29D81F
SHA-256:	606D66026DA226D1AA1C1A4CA6416F3B9F6C66791F4116EB3FFF9E8E28E6B113
SHA-512:	68D3DA77F272A382D800EBB07F02156957CB14C96728896BBB5F6A1E9AEA9A1A5DA4EFCCB09D49096E986A3FCE3F86685B5AFD790887DB28F8F9F5C76D9435A 9
Malicious:	false
Preview:	ITSF....`.....&..u.....|.{.....".....|.{.....".`.....x.....T.....q.....ITSP....T.....j..].!.....".T.....PMGL...../.... /#IDXHDR...Q.../#ITBITS..../#STRINGS.....<./#SYSTEM..F.9./#TOPICS...Q.../#URLSTR...-.a./#URLTBL...a.L./$FlftiMain..._..r./$OBJINST...D.../$WWAssociativeLinks/.. ../$WWAssociativeLinks/Property...@../$WWKeywordLinks/..../$WWKeywordLinks/Property...<../about.htm..v.../advscan.htm...T.../createimg.htm..m.../enhanced.htm... ..H./filetypes.htm...:.-./FinalRecovery.hhc...v./healthdiag.htm..._.[./licence.htm..u.../loadimg.htm..m.../misc.htm...c.m./new.htm..~.o./OptAdv.htm.....+./partiscan.htm.. ..+./quicktutorial.htm...P.8./quicktutorial.swf...3..../rawrecovery.htm...g.4./recover1.htm../.#./recover2.htm..R.../stdscan.htm..p...::DataSpace/NameList..<(::DataSpace/ Storage/MSCompressed/Content.....r,::DataSpace/Storage/MSCompressed/ControlData.j.)::DataSpace/Storage/MSCompr

C:\Program Files (x86)\FLSCover\Rec528\is-0I9HC.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1949
Entropy (8bit):	4.915453283427292
Encrypted:	false
SSDEEP:	48:Sik3C0nGTAFE3blB/aMO0Mk2fLXVn7K+eq9hb6Suf:pkvGTAFELlB/A4GXVnWU9BNuf
MD5:	C0AE85DB30FE9027DBBF3BA758FA78BE
SHA1:	95E69DB95504A9F61D090690F32FB5D2F685C604
SHA-256:	CF63BBFD735C18757AC2AA6CB8A14C82745B6158F9FD299BD189D9CA3E7A2DE7
SHA-512:	DA53177074E79F96C1C7E477E0E7B63CD1D2B836DB9E8066F20B60897FC5770D2B16594A84A953A9CD56BD4C0DDB7D5EFBDDF881EEA840D6B106552C5AC68 5E
Malicious:	false
Preview:	.. F i n a l R e c o v e r y v3.0.7.0325....Overview ..========....FinalRecovery is a powerful and easy-to-use file recovery software. It is suitable ..for various data recovery situations. Some of those situations are listed below. ....1 Recover accidentally deleted files (files were deleted by using windows explorer, .. command line, other software utilities; files which lost while empting recycle .. bin; file losses which caused by unknown reasons); ..2 Recover files from accidentally formatted disk vo lume; ..3 Recover files from lost partitions (the cases may be partition deletion, disk .. repartitioning, partition losses which caused by virus or other reasons) or .. corruptt ed partitions; ..4 Recover files from drive image files; ..5 Predict drive failures (doesn't support SCSI hard drives, removable hard drives). ....FinalRecovery supports FAT12, FAT16, FAT32, NTFS, NTFS5 and Raw file system. It can ..recover files from hard disks, floppies, U disks, PCMCIA-

C:\Program Files (x86)\FLSCover\Rec528\is-D912P.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	553405
Entropy (8bit):	7.979175020825392
Encrypted:	false
SSDEEP:	12288:G8kCp81lkXlwDvsttKcoKRWqZPP4owP1G2uQeDyXwaWt:HJp3kXlDvKwRWg4owdGueDiwaWt
MD5:	37E6EEA8C4E469F6439F3790166815DD
SHA1:	E0A3768F291CC7FCE178A001F0356D4FBA29D81F
SHA-256:	606D66026DA226D1AA1C1A4CA6416F3B9F6C66791F4116EB3FFF9E8E28E6B113
SHA-512:	68D3DA77F272A382D800EBB07F02156957CB14C96728896BBB5F6A1E9AEA9A1A5DA4EFCCB09D49096E986A3FCE3F86685B5AFD790887DB28F8F9F5C76D9435A 9
Malicious:	false
Preview:	ITSF....`.....&..u.....|.{.....".....|.{.....".`.....x.....T.....q.....ITSP....T.....j..].!.....".T.....PMGL...../.... /#IDXHDR...Q.../#ITBITS..../#STRINGS.....<./#SYSTEM..F.9./#TOPICS...Q.../#URLSTR...-.a./#URLTBL...a.L./$FlftiMain..._..r./$OBJINST...D.../$WWAssociativeLinks/.. ../$WWAssociativeLinks/Property...@../$WWKeywordLinks/..../$WWKeywordLinks/Property...<../about.htm..v.../advscan.htm...T.../createimg.htm..m.../enhanced.htm... ..H./filetypes.htm...:.-./FinalRecovery.hhc...v./healthdiag.htm..._.[./licence.htm..u.../loadimg.htm..m.../misc.htm...c.m./new.htm..~.o./OptAdv.htm.....+./partiscan.htm.. ..+./quicktutorial.htm...P.8./quicktutorial.swf...3..../rawrecovery.htm...g.4./recover1.htm../.#./recover2.htm..R.../stdscan.htm..p...::DataSpace/NameList..<(::DataSpace/ Storage/MSCompressed/Content.....r,::DataSpace/Storage/MSCompressed/ControlData.j.)::DataSpace/Storage/MSCompr

C:\Program Files (x86)\FLSCover\Rec528\is-EJ9G4.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	data
Category:	dropped
Size (bytes):	2491753
Entropy (8bit):	6.2535333299603195
Encrypted:	false
SSDEEP:	24576:mzyEzyqd/zyCzytzy3ozyikzy3DKzyH1cuu7hhyGW1G4dPApP8Xv+MysNKt19crT:wTIxvnu7byGx4Ff+MyOe19UuRDy
MD5:	AAE2F1475E852D41D371B6CB7F9813EF
SHA1:	E5C9DB852CA1268A076259E03E9C0DCF15EB22DA
SHA-256:	EAD63B2C168FC3984B0B8B8A948EB15062E2FDBB722BB974FCE8610D2D8EB50A
SHA-512:	C1DFABC1EE689C70FED3C825ABF86F9E3A76D8102B1EF3FBCFBDC87185E9640A875341ED1CAC31063005A0FB942623746A00E70DFE5E20B7A61202432AA663 12
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0,sd.....B.....@..... .....\.....\.....8.....$.....text..... ..`.rdata..z!.....0.....@..@.data...@..... .....@....tls.....@....rsrc...`.....`.....@..@.fls528.....p..i....p.....`..... ....

C:\Program Files (x86)\FLSCover\Rec528\is-Q8OGG.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	791040
Entropy (8bit):	6.608982798504157
Encrypted:	false
SSDEEP:	24576:pvfBdvyjNf8cbMtMJjLKRfwaNSkxtkNkYzSYcj0oHyxdpVhNZFGv+56nBb/ExWyt:pBC4rTQnC1QaX4+I
MD5:	5C2FE7D4DDE65810152054F3C93C1815
SHA1:	2A19F3FAA78A5072068F7902DB19A248F11FA69B
SHA-256:	233D846FEB73A38141BDF6C813C7476FA3F66DCD3548338607F3B7CB61CAC730
SHA-512:	2C01AE918044829FC649F0775BF3FFDB417B1524B47CDABFF0C06B6382B6578A742D9C1D036090D7AD1FC3A8B7D563D28C0CDB94DE572BF883389825F73FD65
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....\|.....$.....@.....@.....@...,...0.....DH..... .....text...D{.....|..... ..`.itext..l..... ..`.data...l8.....:.....@....bss.....C.....idata..,...@.....@....tls....4....p.. .....rdata.....@..@.reloc.....@..B.rsrc.....0.....@..@.....@..@..... .....

C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	670474
Entropy (8bit):	6.480362295801881
Encrypted:	false
SSDEEP:	12288:spmOmg1k2bfrP437QzH/A6A40lG77Nzkn9Gymxpp:mmt2bfrP437QzH/A6A7E7dmPmxpp
MD5:	9ED3858F4C066125A0A6B9FADCD95DCE
SHA1:	BEE9B47A0EF101F1784B65A0B3DB6C6518C7520F
SHA-256:	8EFE36858B9E1CDF3B5D901A4EC17E4EEC148707F526264F35A2BCDA5E139A13
SHA-512:	A460EF220E126D8406F7603ABF697379928E7983C8DAD8A070125E1C205F269702B173FC1B10E18B622B51C6FB081A3E30200E0A7F342FEA41147132C4D270E9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....@.....@.....%.....,.....0..... .....CODE....l..... ..`DATA.....@...BSS.....p.....idata...%.....&.....@....tls..... .....rdata .....0.....@..P.reloc..t....@.....@..P.rsrc....,.....,.....@..P.....@..P..... .....

C:\Program Files (x86)\FLSCover\Rec528\unins000.dat

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	InnoSetup Log Rec528, version 0x2a, 3674 bytes, 123716\user, "C:\Program Files (x86)\FLSCover\Rec528"
Category:	dropped

Size (bytes):	3674
Entropy (8bit):	4.378368790525658
Encrypted:	false
SSDEEP:	48:K4zyMuLBv8Ra0VpifrDWQNtahqqLVO3471N7nuRxWZv1rUczddv:72p8supAWQahqWOlhpnuqTv
MD5:	2FB7EF6747A75C8A0126D2B35C9A8254
SHA1:	3ADA72747D895F9F1AE603064C16830D91369846
SHA-256:	672A704DD5482DF3153A9DB796F784C83A8AD76F25364F4D652BE5AF5D7DE672
SHA-512:	66C6D7FDC8C49F8935929BCCE04F41729E194C6CB181C4B7A9BE352774EB0E05FF35770EDA90526C4BEFBF1CE2750CF7B05D094204250DF7F21D2FF96FF0CD6
Malicious:	false
Preview:	Inno Setup Uninstall Log (b).....Rec528.....Rec528.....*.....Z...%.....!.`\....q....1.....F....123716.user&C:\Program Files (x86)\FLSCover\Rec528.....9.).. .....D.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.GetSystem

C:\Program Files (x86)\FLSCover\Rec528\unins000.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	670474
Entropy (8bit):	6.480362295801881
Encrypted:	false
SSDEEP:	12288:spmOmg1k2bfrP437QzH/A6A40lG77Nzkn9Gymxpp:mmt2bfrP437QzH/A6A7E7dmPmxpp
MD5:	9ED3858F4C066125A0A6B9FADCD95DCE
SHA1:	BEE9B47A0EF101F1784B65A0B3DB6C6518C7520F
SHA-256:	8EFE36858B9E1CDF3B5D901A4EC17E4EEC148707F526264F35A2BCDA5E139A13
SHA-512:	A460EF220E126D8406F7603ABF697379928E7983C8DAD8A070125E1C205F269702B173FC1B10E18B622B51C6FB081A3E30200E0A7F342FEA41147132C4D270E9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....X.....@.....@.....%.....0.....CODE....I..... ..`DATA.....@...BSS.....p.....idata...%.....&.....@....tls..... .....rdata.....0.....@..P.reloc..t....@.....@..P.rsrc....,.....,.....@..P.....@..P.....

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

Process:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	21
Entropy (8bit):	3.975418017913833
Encrypted:	false
SSDEEP:	3:iIxcsJE:iyE
MD5:	C0236A8F8EB0411CC373CD432E252990
SHA1:	49CA519830FADD97FA7BFB7C3404ED2DB29DF4E0
SHA-256:	375CD2A305050C0ECDC8EF9A417194DB2955F3C99B04C76F1B2CD5A88369A242
SHA-512:	3EDFDF13D9AE53C3DC77B299137C7F318B689F4880D72E50CF037F5A4F5C2A6CBC24CB5FE557C10F458CD1658B65E27EF994794FAB2D8E1562694E7DE5039EE
Malicious:	false
Preview:	kvQoRqtcCyMtHmQyQXOUu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dll[1].htm

Process:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.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)\FLSCover\Rec528\Rec528.exe
File Type:	data
Category:	dropped
Size (bytes):	95248
Entropy (8bit):	**7.998277474001343**
Encrypted:	**true**
SSDEEP:	1536:1ajIVNDkCngyeaL3ZC7cjgn35QgjaeiPr6idOZAkOLfTRCaLQhAboaAkepTXnkY5:1vVpj3ZC72gnJQg2eikik4FC9/RX+f6
MD5:	636E3CA21F2541B5EE3AB9922A183C79
SHA1:	4B98C5432E534AF5FA17424C907E61CCFA6880D9
SHA-256:	9B97BF40465ACFBAB5D61EE45ECAC1E485A988ADC66E1A859F950605DC5677B9
SHA-512:	6AA99DFAB439063332383EBA737F34A5929353794245E8E4469EAEB2F7055889891D5A3F3CD3C9F20E37DCDEBFA78C5B5749F3BFDF40263970C880F047A0BDBB
Malicious:	false
Preview:	..'m..h.f{Q{..7_....I../....3`.p.$.....]....~@..Vt.%..eB.9a../_...G...\|.O..0HG`.....`... k..x#.).....W..n...;.vmN....T..:l.....37r.../..X.1,..)..^.Y....N.{8.....=..R..E.z.c..G.~X.0.}.b....rE ..d.....(...M`.O.Y....?....D...R....N...C.{..E.\i.....:.h...#..\...d...*O..".N.yw.2.$..L.{....[w\....v.....zm....9.|.q...p....j.WfQ.5h^rY.r.-..^}g.....]%...El.98Q..5F).F...).KBD..<0..I7...: ..!.....L..P.I..oV....h..~;.G..K....-..={.....U.%...~.(.DE..8..df./...n...FC....~#.`.a.....B.r..OJ^-...$.(`...N..*k....P..h.....+.o...W.m.0...&j...E...Sip..p...U..Qx...q.[.."......U..n|.Me_...PT.|c .wt....5l...'..f..6n..,.+....4*....J.\..+..\..C...:1.u..l.h...n.6..5P.-/.....m70D..D._....?..9.*V...M8..m.T.]4.i.IQN....BV..."h.....f.....V.(..W..H.`,.V`..l.;...}.@.....*..rD....6OP.OC#^..... =^7.R...tx..Q<..J..o.n..q.O..f.F....).Y2v..I...g.InV.X..sm.>....^eO.I.....EB...u.m.E.|.X...)b 7.K.ma."..%t..p.....U\.....L..A.:._.@...c3..[.m...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dll[1].htm

Process:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.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\plus[1].htm

Process:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.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-50VJD.tmp\is-2H2P0.tmp

Process:	C:\Users\user\Desktop\1ibwQtrqNy.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	659968
Entropy (8bit):	6.470646344307062
Encrypted:	false
SSDEEP:	12288:0pmOmg1k2bfrP437QzH/A6A40lG77Nzkn9Gymxp:umt2bfrP437QzH/A6A7E7dmPmxp
MD5:	1F2BC482C99F55A713CF6CA3C1FF04F8
SHA1:	852BACEF61B885AA31AFC7F615DE6C6AF0F715F4
SHA-256:	0A0D0B1916549CF997E2110A768D5BD088F5D1390960C22CB9609FE722779DCF
SHA-512:	A0ECE5740FADBDB08F8A9EFDB5E72B56198CFB35981835E03DAFD2AD09D61BC592E602887D7CF65C58FC19B26CAEA653C1B5E5D4F35A85EBDC784300AA694 8E9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....@.....@.....%.....0..... .....CODE....I..... ..`DATA.....@...BSS.....p.....idata...%.....&.....@....tls..... .....rdata .....0.....@..P.reloc..t....@.....@..P.rsrc....,.....,.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_iscrypt.dll

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.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:e1GSgDIX566lIB6SXvVmMPUjvhBrDsqZ:SgDKRlVImgUNBsG
MD5:	A69559718AB506675E907FE49DEB71E9
SHA1:	BC8F404FFDB1960B50C12FF9413C893B56F2E36F
SHA-256:	2F6294F9AA09F59A574B5DCD33BE54E16B39377984F3D5658CDA44950FA0F8FC
SHA-512:	E52E0AA7FE3F79E36330C455D944653D449BA05B2F9ABEE0914A0910C3452CFA679A40441F9AC696B3CCF9445CBB85095747E86153402FC362BB30AC08249A63
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.c.W.c.W.c...>.T.c.W.b.V.c.R.<.V.c.R.?.V.c.R.9.V.c.RichW. c.....PE..L....b.@.....!..... .....@.....p ..}.... ..(.....0..... ....text..... ..`.rdata..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.226829458093667
Encrypted:	false
SSDEEP:	48:6Q5EWGg69eR+Xl4SH8u09tmRJ/tE/wJI/tZ/P8sB1a:32Gel4NP9tK2/wGXhHa
MD5:	9E5BA8A0DB2AE3A955BEE397534D535D
SHA1:	EF08EF5FAC94F42C276E64765759F8BC71BF88CB
SHA-256:	08D2876741F4FD5EDFAE20054081CEF03E41C458AB1C5BBF095A288FA93627FA
SHA-512:	229A9C66080D59B7D2E1E651CFF9F00DB0CBDC08703E60D645651AF0664520CA143B088C71AD73813A500A33B48C63CA1795E2162B7620453935A4C26DB96B2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o4...g...g...g).zg...g...g...g.&lg...g.&yg...gRich...g.....PE..d... 9TTB.....#.....@.....P.....!..x.....@..H..... ....text..... ..`.rdata..... .....@..@.data...,....0.....@....pdata..H....@.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_shfoldr.dll

Process:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.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: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....IzJ^..$...$...$...%.".$.T87...$.[."...$...$...$.Rich..$.....PE..L.....\;.....#..... ...4.....'.....0.....q.....k...l)..<....@.../.....p..T.....text...{..... ....`.data...\....0.....&.....@....rsrc.../...@...0...(.....@..@.reloc.....p.....X.....@..B.....

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

Process:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.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: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.....Rich.....PE..L...,?c.....~.....@.....`.....@.....(....@.....P.....8.....@.....text..... ..`.rdata..dY.....Z.....@..@.data..... .....@....rsrc.....@.....@..@.reloc.....P.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, InnoSetup self-extracting archive
Entropy (8bit):	7.994995673189032
TrID:	• Win32 Executable (generic) a (10002005/4) 98.88% • Inno Setup installer (109748/4) 1.08% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	1ibwQtrqNy.exe
File size:	2146015
MD5:	65dd3ed482f22906e70dd004a73e5cef
SHA1:	ffe8496a9d3f0a2f5571e683b466d3f3d2092172
SHA256:	15f5d9cd2cb95efaecbf0bc1a455cd6cc301848a5ba71cc4788e4b68c327382d
SHA512:	762707faeacb8f9e17a2e084fa3345961325a7fd061f72a50e6136a890cf07f6832d514c2c30ff6538c31b98427c301b6fdbffdfcfd2d0290c3620627e3118e1
SSDEEP:	49152:Sii/UTUrr4aL/bmKCAnjHtY4pxw2XZs8wux:Si4W64aWKC6NYGnXmc
TLSH:	C1A5337192B54276E1C2C5BB6EB2CB705576FEB80660718C326DFC794E32242DC6A31A
File Content Preview:	MZP.....@.....Inno.. .HA.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	2d2e3797b32b2b99

Static PE Info

General

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

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFD4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-1Ch], eax
call 00007F3D6C693D7Bh
call 00007F3D6C695026h
call 00007F3D6C697229h
call 00007F3D6C697270h
call 00007F3D6C699867h
call 00007F3D6C6999CEh
mov esi, 0040BDE0h
xor eax, eax
push ebp
push 00409F05h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 00409EBBh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [0040B014h]
call 00007F3D6C69A3BFh
call 00007F3D6C699F7Eh
lea edx, dword ptr [ebp-10h]
xor eax, eax
call 00007F3D6C6976E4h
mov edx, dword ptr [ebp-10h]
mov eax, 0040BDD4h
call 00007F3D6C693E27h

Instruction
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [0040BDD4h]
mov dl, 01h
mov eax, 00407158h
call 00007F3D6C697DCBh
mov dword ptr [0040BDD8h], eax
xor edx, edx
push ebp
push 00409E99h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
lea edx, dword ptr [ebp-18h]
mov eax, dword ptr [0040BDD8h]
call 00007F3D6C697EC7h
mov ebx, dword ptr [ebp-18h]
mov edx, 00000030h
mov eax, dword ptr [0040BDD8h]
call 00007F3D6C698001h
mov edx, esi
mov ecx, 0000000Ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc000	0x8f0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	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	0xe000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xf000	0x884	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x2800	0x2800	False	0.32021484375	data	4.282044854754233	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1030c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Dutch	Netherlands
RT_ICON	0x10434	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	Dutch	Netherlands
RT_ICON	0x1099c	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	Dutch	Netherlands
RT_ICON	0x10c84	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	Dutch	Netherlands
RT_STRING	0x1152c	0x2f2	data		
RT_STRING	0x11820	0x30c	data		
RT_STRING	0x11b2c	0x2ce	data		
RT_STRING	0x11dfc	0x68	data		
RT_STRING	0x11e64	0xb4	data		
RT_STRING	0x11f18	0xae	data		
RT_GROUP_ICON	0x11fc8	0x3e	data	English	United States
RT_VERSION	0x12008	0x3a8	data	English	United States
RT_MANIFEST	0x123b0	0x289	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.12.253.724 9698802044031 05/28/23-14:31:02.886782	TCP	2044031	ET TROJAN GCleaner CnC Checkin M1	49698	80	192.168.2.3	45.12.253.72
192.168.2.345.12.253.754 9699802044033 05/28/23-14:31:35.542564	TCP	2044033	ET TROJAN GCleaner CnC Checkin M2	49699	80	192.168.2.3	45.12.253.75
192.168.2.345.12.253.724 9698802044032 05/28/23-14:31:02.924623	TCP	2044032	ET TROJAN GCleaner Payload Retrieval Attempt	49698	80	192.168.2.3	45.12.253.72
45.12.253.72192.168.2.38 0496982044037 05/28/23-14:31:02.950793	TCP	2044037	ET TROJAN GCleaner Downloader - Payload Response	80	49698	45.12.253.72	192.168.2.3
192.168.2.345.12.253.564 9697802044034 05/28/23-14:31:02.810921	TCP	2044034	ET TROJAN Potential GCleaner CnC Checkin	49697	80	192.168.2.3	45.12.253.56

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:31:02.783644915 CEST	49697	80	192.168.2.3	45.12.253.56
May 28, 2023 14:31:02.810148954 CEST	80	49697	45.12.253.56	192.168.2.3
May 28, 2023 14:31:02.810333967 CEST	49697	80	192.168.2.3	45.12.253.56
May 28, 2023 14:31:02.810920954 CEST	49697	80	192.168.2.3	45.12.253.56
May 28, 2023 14:31:02.836796045 CEST	80	49697	45.12.253.56	192.168.2.3
May 28, 2023 14:31:02.841438055 CEST	80	49697	45.12.253.56	192.168.2.3
May 28, 2023 14:31:02.841593027 CEST	49697	80	192.168.2.3	45.12.253.56
May 28, 2023 14:31:02.860186100 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.885916948 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.886037111 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.886781931 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.912609100 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.913141966 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.913265944 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.924623013 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.950473070 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.950793028 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.950850964 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.950901985 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.950948954 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.950980902 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.950980902 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.950995922 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951025963 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951025963 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951042891 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951090097 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951092005 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951121092 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951138973 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951155901 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951205969 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951215982 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951253891 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.951263905 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.951309919 CEST	49698	80	192.168.2.3	45.12.253.72

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:31:02.976932049 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977011919 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977057934 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977104902 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977150917 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977179050 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977205992 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977246046 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977253914 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977303028 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977307081 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977327108 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977356911 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977379084 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977404118 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977417946 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977449894 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977473021 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977510929 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977519035 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977559090 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977572918 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977606058 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977617979 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977652073 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977667093 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977699041 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977713108 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977746964 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977761030 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977794886 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977809906 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977840900 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977875948 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977889061 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:02.977914095 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:02.977956057 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.003834009 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.003909111 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.003957987 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004005909 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004053116 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004056931 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004100084 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004117012 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004148960 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004157066 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004195929 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004216909 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004244089 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004291058 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004317999 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004326105 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004383087 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004395962 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004442930 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004456043 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004491091 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004503965 CEST	49698	80	192.168.2.3	45.12.253.72

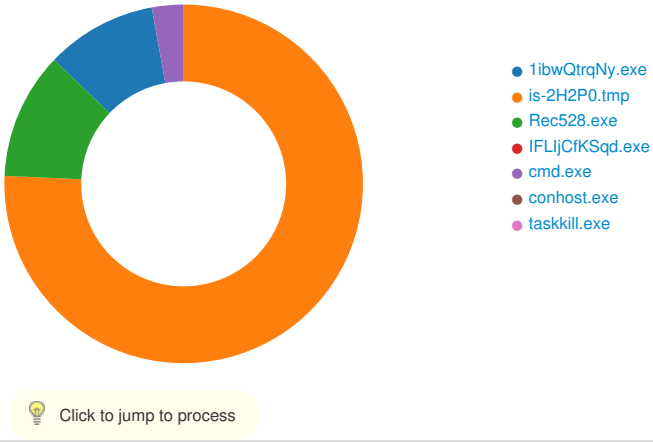
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:31:03.004539013 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004549980 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004585981 CEST	80	49698	45.12.253.72	192.168.2.3
May 28, 2023 14:31:03.004602909 CEST	49698	80	192.168.2.3	45.12.253.72
May 28, 2023 14:31:03.004652977 CEST	80	49698	45.12.253.72	192.168.2.3

HTTP Request Dependency Graph

- 45.12.253.56
- 45.12.253.72
- 45.12.253.75

Statistics

Behavior



System Behavior

Analysis Process: 1ibwQtrqNy.exe PID: **4080**, Parent PID: **3452**

General

Target ID:	0
Start time:	14:30:55
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\1ibwQtrqNy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1ibwQtrqNy.exe
Imagebase:	0x400000
File size:	2146015 bytes
MD5 hash:	65DD3ED482F22906E70DD004A73E5CEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: is-2H2P0.tmp PID: **4944**, Parent PID: **4080**

General

Target ID:	1
Start time:	14:30:56
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp" /SL4 $2048E "C:\Users\user\Desktop\1ibwQtrqNy.exe" 1911253 52224
Imagebase:	0x400000
File size:	659968 bytes
MD5 hash:	1F2BC482C99F55A713CF6CA3C1FF04F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	45244F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4722F4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_shfoldr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_iscrypt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406F76	CreateFileA
C:\Program Files (x86)\FLSCover	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451362	CreateDirectoryA
C:\Program Files (x86)\FLSCover\Rec528	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451362	CreateDirectoryA
C:\Program Files (x86)\FLSCover\Rec528\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451362	CreateDirectoryA
C:\Program Files (x86)\FLSCover\Rec528\unins000.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	46CD1E	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\FLSCover\Rec528\is-EJ9G4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\FLSCover\Rec528\is-D912P.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\FLSCover\Rec528\is-0I9HC.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\FLSCover\Rec528\is-Q8OGG.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA
C:\Program Files (x86)\FLSCover\Rec528\data\is-O02RD.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FEC1	CreateFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	C:\Program Files (x86)\FLSCover\Rec528\unins000.exe	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\FLSCover\Rec528\is-EJ9G4.tmp	C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\FLSCover\Rec528\is-D912P.tmp	C:\Program Files (x86)\FLSCover\Rec528\finalrecovery.chm	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\FLSCover\Rec528\is-0I9HC.tmp	C:\Program Files (x86)\FLSCover\Rec528\Readme.txt	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\FLSCover\Rec528\is-Q8OGG.tmp	C:\Program Files (x86)\FLSCover\Rec528\Preview.exe	success or wait	1	4517E3	MoveFileA
C:\Program Files (x86)\FLSCover\Rec528\data\is-O02RD.tmp	C:\Program Files (x86)\FLSCover\Rec528\data\Config.xml	success or wait	1	4517E3	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-5SERN.tmp_isetup_setup64.tmp	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 6f 34 fd fd 01 67 fd fd 01 67 fd fd 01 67 29 1a 7a 67 fd fd 01 67 fd fd 00 67 fd fd 01 67 0b 26 6c 67 fd fd 01 67 0b 26 79 67 fd fd 01 67 52 69 63 68 fd fd 01 67 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 04 00 39 54 54 42 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0c 02 00 00 00 00 00 fd 15 00 00 00 10 00 00 00 00 40 00 00 00 00 00 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$o4ggg)zgggg&lg g&yggRichgPEd9TTB#@	success or wait	1	406FBD	WriteFile

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.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	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	48	4	49 6e 55 6e	InUn	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	659968	10454	49 6e 6e 6f 20 53 65 74 75 70 20 4d 65 73 73 61 67 65 73 20 28 35 2e 31 2e 30 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 fd 28 00 00 29 fd fd fd fd 26 32 fd 26 41 62 6f 75 74 20 53 65 74 75 70 2e 2e 2e 00 25 31 20 76 65 72 73 69 6f 6e 20 25 32 0d 0a 25 33 0d 0a 0d 0a 25 31 20 68 6f 6d 65 20 70 61 67 65 3a 0d 0a 25 34 00 00 41 62 6f 75 74 20 53 65 74 75 70 00 59 6f 75 20 6d 75 73 74 20 62 65 20 6c 6f 67 67 65 64 20 69 6e 20 61 73 20 61 6e 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 77 68 65 6e 20 69 6e 73 74 61 6c 6c 69 6e 67 20 74 68 69 73 20 70 72 6f 67 72 61 6d 2e 00 46 6f 6c 64 65 72 20 6e 61 6d 65 73 20 63 61 6e 6e 6f 74 20 69 6e 63 6c 75 64 65 20 61 6e 79 20 6f 66 20	Inno Setup Messages (5.1.0)()&2&About Setup...%1 version %2%3%1 home page:%4About SetupYou must be logged in as an administrator when installing this program.Folder names cannot include any of	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\is-U3J98.tmp	670466	8	49 4d 73 67 00 12 0a 00	IMsg	success or wait	1	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\is-EJ9G4.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 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 30 2c 73 64 00 00 00 00 00 00 00 00 fd 00 42 01 0b 01 07 0d 00 fd 06 00 00 fd fd 00 00 00 00 00 fd fd 06 00 00 10 00 00 00 fd 06 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 01 00 00 00 00 00 04 00 01 00 00 00 00 00 00 10 06 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.$PEL0,sdB@	success or wait	39	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\is-D912P.tmp	0	65536	49 54 53 46 03 00 00 00 60 00 00 00 01 00 00 00 26 fd fd 75 04 08 00 00 10 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 11 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 60 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 78 00 00 00 00 00 00 00 54 10 00 00 00 00 00 00 fd 10 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 fd 71 08 00 00 00 00 00 00 00 00 00 00 00 00 00 49 54 53 50 01 00 00 00 54 00 00 00 0a 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 01 00 00 00 09 04 00 00 6a fd 02 5d 2e 21 fd 11 fd fd 00 fd fd 22 fd fd 54 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 50 4d 47 4c fd 0b 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 01 2f 00 00 00 08 2f 23 49 44 58 48 44 52 01 fd fd 51 fd 00 08 2f 23 49 54 42 49 54 53 00 00	ITSF`&u|{"|{"`xTqITSPTj].!"TPMGL//#IDXHDRQ/#ITBITS	success or wait	9	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\is-0I9HC.tmp	0	1949	0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 20 69 20 6e 20 61 20 6c 20 52 20 65 20 63 20 6f 20 76 20 65 20 72 20 79 20 20 20 20 76 33 2e 30 2e 37 2e 30 33 32 35 0d 0a 0d 0a 4f 76 65 72 76 69 65 77 20 0d 0a 3d 3d 3d 3d 3d 3d 3d 3d 0d 0a 0d 0a 46 69 6e 61 6c 52 65 63 6f 76 65 72 79 20 69 73 20 61 20 70 6f 77 65 72 66 75 6c 20 61 6e 64 20 65 61 73 79 2d 74 6f 2d 75 73 65 20 66 69 6c 65 20 72 65 63 6f 76 65 72 79 20 73 6f 66 74 77 61 72 65 2e 20 49 74 20 69 73 20 73 75 69 74 61 62 6c 65 20 0d 0a 66 6f 72 20 76 61 72 69 6f 75 73 20 64 61 74 61 20 72 65 63 6f 76 65 72 79 20 73 69 74 75 61 74 69 6f 6e 73 2e 20 53 6f 6d 65 20 6f 66 20 74 68 6f 73 65 20 73 69 74 75 61 74 69 6f 6e 73 20 61 72 65 20 6c 69 73 74 65 64 20 62 65 6c 6f 77 2e 20 0d 0a 0d 0a	F i n a l R e c o v e r y v3.0.7.0325Overview ========FinalRecovery is a powerful and easy-to-use file recovery software. It is suitable for various data recovery situations. Some of those situations are listed below.	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\is-Q8OGG.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	13	45013C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\FLSCover\Rec528\data\is-O02RD.tmp	0	6452	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0d 0a 3c 53 65 74 74 69 6e 67 73 3e 0d 0a 09 3c 4d 69 73 63 20 72 65 61 64 79 69 6e 66 6f 72 6d 3d 22 54 72 75 65 22 20 73 68 6f 77 64 6c 67 6f 6e 63 6c 69 63 6b 3d 22 54 72 75 65 22 20 61 64 6a 75 73 74 6d 65 6e 74 71 75 65 72 79 3d 22 54 72 75 65 22 2f 3e 0d 0a 09 3c 45 6e 68 61 6e 63 65 64 20 73 74 72 75 63 74 75 72 65 6d 61 74 63 68 3d 22 46 61 6c 73 65 22 2f 3e 0d 0a 09 3c 46 69 6c 65 54 79 70 65 73 20 65 78 70 61 6e 64 3d 22 54 72 75 65 22 3e 0d 0a 09 09 3c 54 79 70 65 20 65 78 74 3d 22 72 61 72 22 2f 3e 3c 54 79 70 65 20 65 78 74 3d 22 7a 69 70 22 2f 3e 3c 54 79 70 65 20 65 78 74 3d 22 64	<?xml version="1.0" encoding="UTF-8" standalone="no"?><Settings><Misc readyinform="True" showdlgonclick="True" adjustmentquery="True"/> <Enhanced structurematch="False"/> <FileTypes expand="True"><Type ext="rar"/><Type ext="zip"/><Type ext="d	success or wait	1	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\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 52 65 63 35 32 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 65 63 35 32 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)Rec528Rec528	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\unins000.dat	448	12	fd 0c 00 00 71 fd fd fd fd 31 fd	q1	success or wait	2	45013C	WriteFile
C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	0	1	4d	M	success or wait	1	44149E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp	unknown	4	success or wait	1	45002C	ReadFile
C:\Users\user\Desktop\1ibwQtrqNy.exe	unknown	64	success or wait	1	45002C	ReadFile
C:\Users\user\Desktop\1ibwQtrqNy.exe	unknown	4	success or wait	2	45002C	ReadFile
C:\Users\user\Desktop\1ibwQtrqNy.exe	unknown	4	success or wait	2	45002C	ReadFile
C:\Users\user\AppData\Local\Temp\is-50VJD.tmp\is-2H2P0.tmp	unknown	65536	success or wait	11	45002C	ReadFile
C:\Users\user\Desktop\1ibwQtrqNy.exe	unknown	4	success or wait	5	45002C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	success or wait	1	42DCAD	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	Inno Setup: Setup Version	unicode	5.1.3-beta	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	Inno Setup: App Path	unicode	C:\Program Files (x86)\FLSCover\Rec528	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	InstallLocation	unicode	C:\Program Files (x86)\FLSCover\Rec528\	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	Inno Setup: Icon Group	unicode	FLSCover\Rec528	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	Inno Setup: User	unicode	hardz	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	DisplayName	unicode	Cov 1.0.5.28	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	UninstallString	unicode	"C:\Program Files (x86)\FLSCover\Rec528\unins000.exe"	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	QuietUninstallString	unicode	"C:\Program Files (x86)\FLSCover\Rec528\unins000.exe" /SILENT	success or wait	1	4679F8	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	NoModify	dword	1	success or wait	1	467A58	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rec528_is1	NoRepair	dword	1	success or wait	1	467A58	RegSetValueExA

Analysis Process: Rec528.exe PID: **2576**, Parent PID: **4944**

General

Target ID:	2
Start time:	14:30:57
Start date:	28/05/2023
Path:	C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe"
Imagebase:	0x400000
File size:	2491753 bytes
MD5 hash:	9D3532E4DB1BBBCCA78E0D2DC8AE2572
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: 00000002.00000002.443567321.0000000003260000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000002.00000002.442855707.0000000000400000.00000040.00000001.01000000.00000007.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • 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}\IFLIjCfKSqd.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	42831A	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\IFLIjCfKSqd.exe	0	73728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b0 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b fd fd fd fd fd fd fd 24 fd fd fd fd 24 fd fd fd fd 24 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2e fd fd fd fd fd fd 2e fd 39 fd fd fd fd 2e fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$..9.Rich	success or wait	1	4210F4	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\plus[1].htm	0	1	30	0	success or wait	1	401BEA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\stuk[1].htm	0	21	6b 76 51 6f 52 71 74 63 43 79 4d 74 48 6d 51 79 51 58 4f 55 75	kvQoRqtcCyMtHmQyQXOUu	success or wait	1	401BEA	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fuckingdllENCR[1].dll	0	1000	fd 17 27 6d 74 fd 68 0d 66 7b 51 7b fd 1c 37 5f 16 01 fd fd 6c fd fd 2f 09 fd 14 fd 33 60 fd 70 fd 24 0a 1c fd 2e 05 5d fd fd fd 09 7e 40 fd fd 56 74 fd 25 0c 07 65 42 fd 39 61 fd fd 2f 5f fd fd fd 47 fd 02 0f 7c fd 4f fd fd 30 48 47 60 fd fd fd 11 fd fd 60 fd fd 06 20 6b 58 fd 78 23 fd 29 fd 1e aa fd fd 57 fd 91 6e 05 10 fd 3b 0b 76 6d 4e fd fd 14 fd 54 1b fd 3a 6c 7b 0c fd fd 07 ea fd fd 14 14 fd 33 37 72 fd 15 fd 2f fd fd 58 fd 31 2c fd fd 29 fd 05 5e 98 59 fd 0d fd fd 4e fd 7b 38 fd 7f fd 34 fd fd bb fd 3d fd a0 52 fd 06 45 09 7a fd 63 fd fd 47 fd 7e 58 fd 30 02 7d fd 62 61 04 00 fd 72 45 fd fd 64 fd fd 0a c8 1d fd fd fd fd fd 28 fd fd fd 4d 60 fd 4f fd 59 27 fd fd fd 3f 7f fd fd 15 44 fd 13 fd	'mhf{Q{7_!/3`p$.]~@Vt% eB9a/_G|O0HG`` kx#)Wn;vmNT:!37r/X1,)^ Y N{8=REzcG~X0}brEd(M` OY?D	success or wait	93	401BEA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dll[1].htm	0	1	30	0	success or wait	6	1000122D	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dll[1].htm	0	1	30	0	success or wait	5	1000122D	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: IFLljCfKSqd.exe PID: **7052**, Parent PID: **2576**

General

Target ID:	3
Start time:	14:31:01
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\IFLljCfKSqd.exe
Wow64 process (32bit):	true
Commandline:	
Imagebase:	0x90000
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: 62%, ReversingLabs
Reputation:	high

Analysis Process: cmd.exe PID: **5924**, Parent PID: **2576**

General

Target ID:	6
Start time:	14:31:38
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "Rec528.exe" /f & erase "C:\Program Files (x86)\FLSCover\Rec528\Rec528.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)\FLSCover\Rec528\Rec528.exe	cannot delete	1	D0374	DeleteFileW
C:\Program Files (x86)\FLSCover\Rec528\Rec528.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: **5972**, Parent PID: **5924**

General

Target ID:	7
Start time:	14:31:38
Start date:	28/05/2023
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: **2288**, Parent PID: **5924**

General

Target ID:	8
Start time:	14:31:38
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "Rec528.exe" /f
Imagebase:	0x930000
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