ID: 791301
Sample Name: file.exe
Cookbook: default.jbs
Time: 10:01:06
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2023

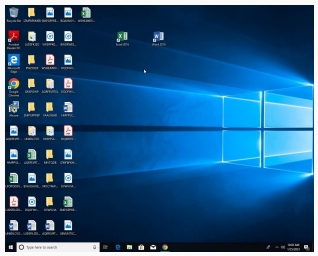
Windows Analysis Report

file.exe

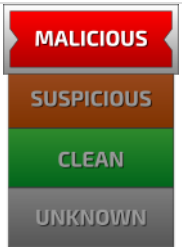
Overview

General Information

Sample Name:	file.exe
Analysis ID:	791301
MD5:	14e09c7a584268..
SHA1:	4c9e1cbcd93329..
SHA256:	a5ce2c21d3f920...
Tags:	exe
Infos:	



Detection



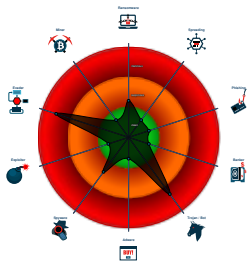
Nymaim

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5992 cmdline: C:\Users\user\Desktop\file.exe MD5: 14E09C7A5842688842F6C0BF61C17135)
  - file.tmp (PID: 6100 cmdline: "C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp" /SL5="$4023C,1536639,54272,C:\Users\user\Desktop\file.exe" MD5: D76329B30DB65F61D55B20F36B56DA26)
    - finalrecovery.exe (PID: 6076 cmdline: "C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe" MD5: 88A9155EB9D85157634ED38D128C877B)
      - 6tohc1clzbcir.exe (PID: 1756 cmdline: MD5: 3FB36CB0B7172E5298D2992D42984D06)
      - cmd.exe (PID: 4488 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "finalrecovery.exe" /f & erase "C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - taskkill.exe (PID: 5968 cmdline: taskkill /im "finalrecovery.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

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
00000002.00000002.323772698.0000000003250000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000002.00000002.323409231.0000000000400000.00000040.00000001.01000000.00000007.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.finalrecovery.exe.400000.1.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.finalrecovery.exe.3250000.2.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.finalrecovery.exe.3250000.2.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.finalrecovery.exe.400000.1.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN GCleaner Downloader - Payload Response - Source IP: 45.12.253.72 - Destination IP: 192.168.2.3

Timestamp:	45.12.253.72192.168.2.380497082852925 01/25/23-10:02:04.044834
SID:	2852925
Source Port:	80
Destination Port:	49708
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Copyright Joe Security LLC 2023

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Obfuscated command line found

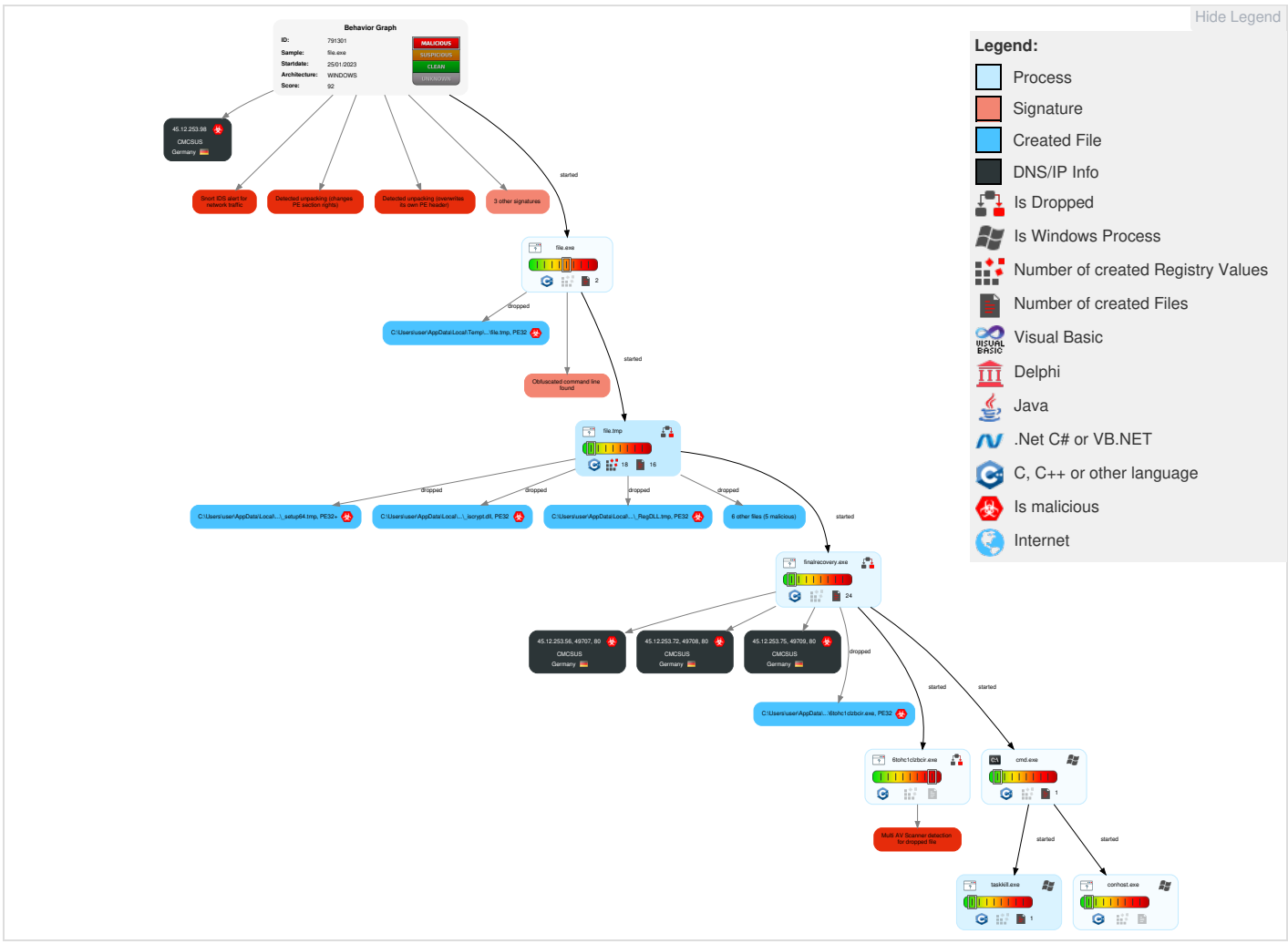
Stealing of Sensitive Information

Yara detected Nymaim

Mitre Att&ck Matrix

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

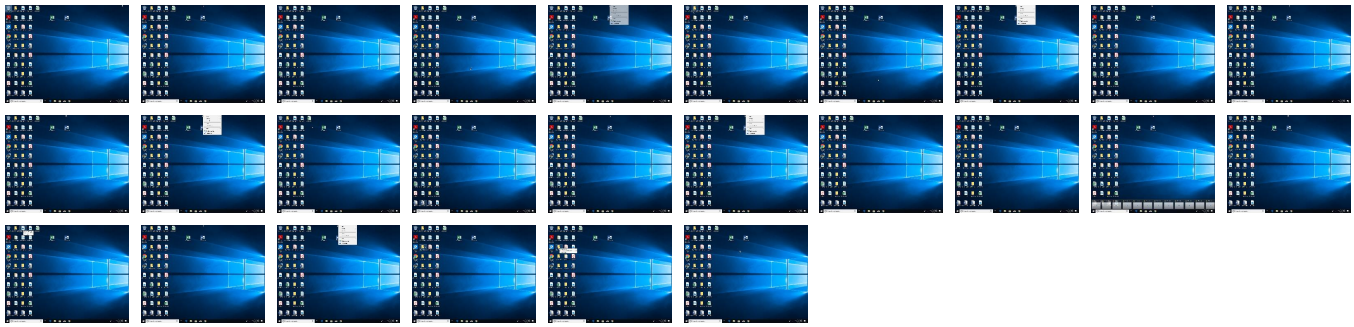
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\FgasoftFR\FinalRecovery\Preview.exe (copy)	0%	ReversingLabs		
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-RVFGU.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_RegDLL.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_iscrypt.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_shfoldr.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\6tohc1clzbcir.exe	60%	ReversingLabs	Win32.Trojan.GenusAgent	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.file.tmp.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link	Download
0.3.file.exe.23675c8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.file.tmp.4b375c.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.file.exe.218b608.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.finalrecovery.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
1.0.file.tmp.4b375c.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://www.innosetup.com/	0%	URL Reputation	safe	
http://45.12.253.72/default/stuk.php	0%	URL Reputation	safe	
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixinte	0%	URL Reputation	safe	
http://www.remobjects.com/psU	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.finalrecovery.com/buy.htm	0%	URL Reputation	safe	
http://www.remobjects.com/ps	0%	URL Reputation	safe	
http://nbafrog.com/b	0%	Avira URL Cloud	safe	
http://45.12.253.75/dll.phpI	0%	Avira URL Cloud	safe	
http://45.12.253.72/default/stuk.phpE	0%	Avira URL Cloud	safe	
http://nbafrog.com/.	0%	Avira URL Cloud	safe	
http://45.12.253.72/default/puk.phpk	0%	Avira URL Cloud	safe	
http://nbafrog.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

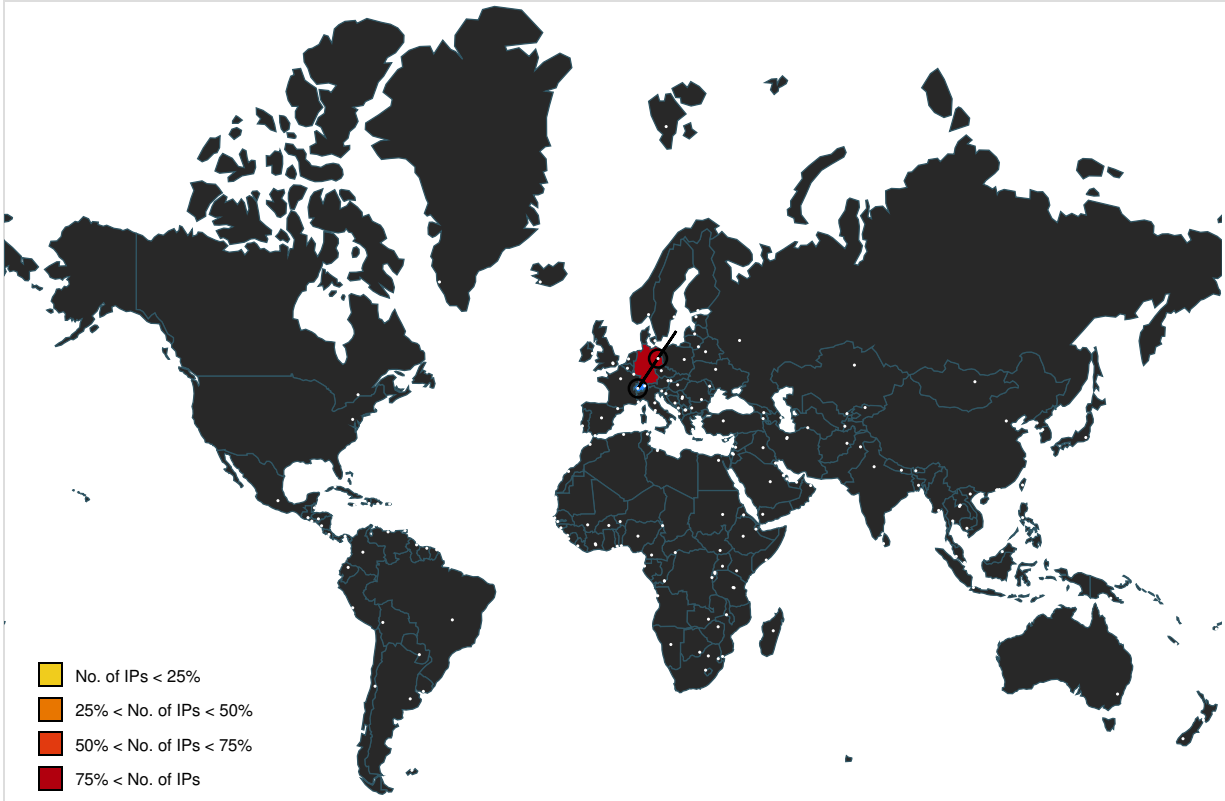
Name	Malicious	Antivirus Detection	Reputation
http://45.12.253.72/default/stuk.php	true	• URL Reputation: safe	unknown
http://45.12.253.56/advertisting/plus.php?s=NOSUB&str=mixtwo&substr=mixinte	true	• URL Reputation: safe	unknown
http://45.12.253.72/default/puk.php	true	• URL Reputation: safe	unknown
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/	file.tmp, file.tmp, 00000001.00000000.243074612.00000000401000.00000020.00000001.01000000.00000004.sdmp, file.tmp.0.dr, is-U89TP.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.remobjects.com/psU	file.exe, 00000000.00000003.242613252.000000022C0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.242766712.00000000020E8000.00000004.00001000.00020000.00000000.sdmp, file.tmp, 00000001.00000000.243074612.00000000401000.00000020.00000001.01000000.00000004.sdmp, file.tmp.0.dr, is-U89TP.tmp.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.12.253.75/dll.phpl	finalrecovery.exe, 00000002.00000002.323950124.000000000426A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.12.253.72/default/puk.phpk	finalrecovery.exe, 00000002.00000002.323596544.0000000001665000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nbafrog.com/b	file.tmp, 00000001.00000003.324143463.000000000782000.00000004.00000020.00020000.00000000.sdmp, file.tmp, 00000001.00000002.324394304.0000000000782000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.finalrecovery.com/buy.htm	is-587OJ.tmp.1.dr	false	• URL Reputation: safe	unknown
http://45.12.253.72/default/stuk.phpE	finalrecovery.exe, 00000002.00000002.323596544.0000000001665000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.remobjects.com/ps	file.exe, 00000000.00000003.242613252.000000022C0000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.242766712.00000000020E8000.00000004.00001000.00020000.00000000.sdmp, file.tmp, file.tmp, 00000001.00000000.243074612.0000000000401000.00000020.00000001.01000000.00000004.sdmp, file.tmp.0.dr, is-U89TP.tmp.1.dr	false	• URL Reputation: safe	unknown
http://nbafrog.com/	file.tmp, 00000001.00000003.243532631.000000002278000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nbafrog.com/.	file.exe, 00000000.00000003.324832803.000000020E1000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.242527892.00000000020E1000.00000004.00001000.00020000.00000000.sdmp, file.tmp, 00000001.00000002.324490677.0000000002267000.00000004.00001000.00020000.00000000.sdmp, file.tmp, 00000001.00000003.243532631.0000000002278000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: 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

Copyright Joe Security LLC 2023

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791301
Start date and time:	2023-01-25 10:01:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.evad.winEXE@12/24@0/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 38.5% (good quality ratio 37.4%) • Quality average: 81.2% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:02:03	API Interceptor	1x Sleep call for process: 6tohc1clzbcir.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)\FgasoftFR\FinalRecovery\Preview.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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:	moderate, 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)\FgasoftFR\FinalRecovery\Readme.txt (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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:	moderate, 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 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)\FgasoftFR\FinalRecovery\data\Config.xml (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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)\FgasoftFR\FinalRecovery\data\is-K2TAS.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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)\FgasoftFR\FinalRecovery\finalrecovery.chm (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	553405
Entropy (8bit):	7.979175020825392
Encrypted:	false
SSDEEP:	12288:G8kCp81IkXlwDvsttKcoKRWqZPP4owP1G2uQeDyXwaWt:HJp3kXIDvKwRWg4owdGueDiwaWt
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./$FIftiMain..._..r./$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)\FgasoftFR\FinalRecovery\finalrecovery.exe

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	modified
Size (bytes):	1327103
Entropy (8bit):	6.349641677377942
Encrypted:	false
SSDEEP:	24576:p8sn21M2uJJKYcbmuBm/GAihHJTo+M/FLUTTb2ghAfrZLya6p4ZyQzAp:CsroY6mGAugUlgIbn
MD5:	88A9155EB9D85157634ED38D128C877B
SHA1:	1ED44B28A6652EC52EE93DE9DD18065625938D0B
SHA-256:	919DBDEDBDF4312EF0EF97A94343DEC76EEBA35FD50CE0A8B3885029750FAD06
SHA-512:	4A04B85C7DF8ECCDCF7740EB5B451B0696D3C109308766D4A1BB7288B7A13891AC6023EF81BB1754A97157DDC265AF40660AAB6C0E468FC5A4366A92BFD54E 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..c.....@.....@..... ....`.....text..... ..`.rdata..:..... .....@..@.data... ....@....tls....!.....@....rsrc..... ....@..@.fga20..._....._.....`.7..... ....

C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-05LH6.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	553405
Entropy (8bit):	7.979175020825392
Encrypted:	false
SSDEEP:	12288:G8kCp81lkXlwDvsttKcoKRWqZPP4owP1G2uQeDyXwaWt:HJp3kXIDvKwRWg4owdGueDiwaWt
MD5:	37E6EEA8C4E469F6439F3790166815DD
SHA1:	E0A3768F291CC7FCE178A001F0356D4FBA29D81F
SHA-256:	606D66026DA226D1AA1C1A4CA6416F3B9F6C66791F4116EB3FFF9E8E28E6B113
SHA-512:	68D3DA77F272A382D800EBB07F02156957CB14C96728896BBB5F6A1E9AEA9A1A5DA4EFCCB09D49096E986A3FCE3F86685B5AFD790887DB28F8F9F5C76D9435/ 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./$FIftiMain..._..r./$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)\FgasoftFR\FinalRecovery\is-587OJ.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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)\FgasoftFR\FinalRecovery\is-8DP05.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	data
Category:	dropped
Size (bytes):	1327103
Entropy (8bit):	6.349642071497365
Encrypted:	false
SSDEEP:	24576:O8sn21M2uJJKYcbmuBm/GAihHJTo+M/FLUTTb2ghAfrZLya6p4ZyQzAp:dsroY6mGAugUlgIbn
MD5:	686E27330B438E55788EE0A132194478
SHA1:	19AB1A4D5724A647984EDBBDAC465E98F7093B2F
SHA-256:	5D07E971A265774EE4C2ACF51CC41C815D247284C1A69AD05298FD54A7285FCF
SHA-512:	B54D7258AFEB1243445A7E344655D6A050E8F5F44FEBAFF3C5D62D6CEFBC49F948CD35A549D0AFD654310CA3E50951C23863007F94BF944C0957496C4DE96AA 6
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..c.....@.....@..... ..`.....text..... ..`.rdata..:..... .....@..@.data... .....@....tls....!.....@....rsrc..... ....@..@.fga20..._....._.....`.7..... ....

C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-RVFGU.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.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:	2C01AE918044829FC649F0775BF3FFDB417B1524B47CDABFF0C06B6382B6578A742D9C1D036090D7AD1FC3A8B7D563D28C0CDB94DE572BF883389825F73FD6
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)\FgasoftFR\FinalRecovery\is-U89TP.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	723230
Entropy (8bit):	6.49191904892708
Encrypted:	false
SSDEEP:	12288:1QtLeYXPEv4arPEn37TzH7A6p3xxu9yz/eERMY1VLJrNufs9RZM2GHOQyD362kSW:WtCUA4arPEn37TzH7A6nw9yzeESUFWHF
MD5:	D0E4493CD1CEC1B97F24BAB12A942543
SHA1:	CEE352F43F982FCB36A337D2C15FFDD28B04B80D
SHA-256:	C5851530669107DF77FD7079EC7C6F0C668003D6094643D6E723FB74F1DEB5D9
SHA-512:	D2A02702AEDE0509AC81785DBECBA312CABD6D83E064DCAA7E95B43FF4E373D538327539290288CED6A6837F44819A6A7CCC912285E5E1407F9B79C086B6C5 F
Malicious:	**true**

Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....b.....n.....@.....@.....%.....@..... .....CODE.....`.....b..... ..`DATA.....f.....@...BSS.....x.....idata...%.....&...x.....@....tls.....rdata .....@..P.reloc.....@..P.rsrc....@.....@.....@..P.....j.....@..P..... .....

C:\Program Files (x86)\FgasoftFR\FinalRecovery\unins000.dat

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	InnoSetup Log FgasoftFR FinalRecovery, version 0x30, 4340 bytes, 585948\user, "C:\Program Files (x86)\FgasoftFR\FinalRecovery"
Category:	dropped
Size (bytes):	4340
Entropy (8bit):	4.712609745266559
Encrypted:	false
SSDEEP:	96:AyWx5pJU+oIahqwOIhdc87ICSss/LBtbgfj1:AyWx5pJU+KEIhZICSsATgfJ
MD5:	15CF1A53B3514856C721F859E721DCBD
SHA1:	9BC828AC64112060DB3059F8EEC43722BE1AB041
SHA-256:	87159F502A66551DA4E65C05DB04E132CBC46B1D4370EEC9022499FBEAD59A84
SHA-512:	C49D7B0D200BC65FA055302353FAC99BBD379D81EF0D220411A379006D4A6A3AA716D36F0E9E2B1BD2AFD699941F5547E371AFB277B99800CFB290A379C5DB9 9
Malicious:	false
Preview:	Inno Setup Uninstall Log (b).....FgasoftFR FinalRecovery.....FgasoftFR FinalRec overy.....0.....%.....Wc(.....y.s. .....N....585948.user.C:\Program Files (x86)\FgasoftFR\FinalRecovery.....:.Z.. .....b.IFPS..... ...BOOLEAN.....TWIZARDFORM....TWIZARDFORM.....TPASSWORDEDIT....TPASSWORDEDIT.....!MAIN....-1..(...dll:kernel32.dll.Crea teFileA.....$...dll:kernel32.dll.WriteFile....."...dll:kernel32.dll.CloseHandle....."...dll:kernel32.dll.ExitProcess.....%...dll:User32.d

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

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	723230
Entropy (8bit):	6.49191904892708
Encrypted:	false
SSDEEP:	12288:1QtLeYXPEv4arPEn37TzH7A6p3xxu9yz/eERMY1VLJrNufs9RZM2GHOQyD362kSW:WtCUA4arPEn37TzH7A6nw9yzeESUFWHF
MD5:	D0E4493CD1CEC1B97F24BAB12A942543
SHA1:	CEE352F43F982FCB36A337D2C15FFDD28B04B80D
SHA-256:	C5851530669107DF77FD7079EC7C6F0C668003D6094643D6E723FB74F1DEB5D9
SHA-512:	D2A02702AEDE0509AC81785DBECBA312CABD6D83E064DCAA7E95B43FF4E373D538327539290288CED6A6837F44819A6A7CCC912285E5E1407F9B79C086B6C5 F
Malicious:	**true**
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....b.....n.....@.....@.....%.....@..... .....CODE.....`.....b..... ..`DATA.....f.....@...BSS.....x.....idata...%.....&...x.....@....tls.....rdata .....@..P.reloc.....@..P.rsrc....@.....@.....@..P.....j.....@..P..... .....

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

Process:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.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:	6AA99DFAB439063332383EBA737F34A5929353794245E8E4469EAEB2F7055889891D5A3F3CD3C9F20E37DCDEBFA78C5B5749F3BFDF40263970C880F047A0BDB B
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\MEEXW4H4\stuk[1].htm	
Process:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	21
Entropy (8bit):	3.975418017913833
Encrypted:	false
SSDEEP:	3:ilxcsJE:iyE
MD5:	C0236A8F8EB0411CC373CD432E252990
SHA1:	49CA519830FADD97FA7BFB7C3404ED2DB29DF4E0
SHA-256:	375CD2A305050C0ECDC8EF9A417194DB2955F3C99B04C76F1B2CD5A88369A242
SHA-512:	3EDFDF13D9AE53C3DC77B299137C7F318B689F4880D72E50CF037F5A4F5C2A6CBC24CB5FE557C10F458CD1658B65E27EF994794FAB2D8E1562694E7DE5039EE
Malicious:	false
Preview:	kvQoRqtcCyMtHmQyQXOUu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dll[1].htm	
Process:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.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\dll[1].htm	
Process:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.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)\FgasoftFR\FinalRecovery\finalrecovery.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-EFH65.tmp_isetup_RegDLL.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.026670007889822
Encrypted:	false
SSDEEP:	48:ivuz1hEU3FR/pmqBl8/QMCBaquEMx5BC+SS4k+bkguj0KHc:bz1eEFNcqBC/Qrex5iSKDkc
MD5:	0EE914C6F0BB93996C75941E1AD629C6
SHA1:	12E2CB05506EE3E82046C41510F39A258A5E5549
SHA-256:	4DC09BAC0613590F1FAC8771D18AF5BE25A1E1CB8FDBF4031AA364F3057E74A2
SHA-512:	A899519E78125C69DC40F7E371310516CF8FAA69E3B3FF747E0DDF461F34E50A9FF331AB53B4D07BB45465039E8EBA2EE4684B3EE56987977AE8C7721751F5F9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....|.....|.....|.....Rich.....PE..L....M;J..... ....@.....@.....I ..P....0..@..... ..D.....text..... ....`.rdata..... .....@..@.rsrc...@....0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_iscrypt.dll

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

C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.215994423157539
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12pS5SKvkc:sfJEVYlvxaX12EF
MD5:	4FF75F505FDDCC6A9AE62216446205D9
SHA1:	EFE32D504CE72F32E92DCF01AA2752B04D81A342
SHA-256:	A4C86FC4836AC728D7BD96E7915090FD59521A9E74F1D06EF8E5A47C8695FD81
SHA-512:	BA0469851438212D19906D6DA8C4AE95FF1C0711A095D9F21F13530A6B8B21C3ACBB0FF55EDB8A35B41C1A9A342F5D3421C00BA395BC13BB1EF5902B979CE824
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d...XW:J.....#.....@.....`.....<!.....P..@....@..0..... .....text..... ..`.rdata..|... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...@....P.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_shfoldr.dll

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

C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	712704
Entropy (8bit):	6.4837542632664515
Encrypted:	false
SSDEEP:	12288:9QtLeYXPEv4arPEn37TzH7A6p3xxu9yz/eERMY1VLJrNufs9RZM2GHOQyD362kS0:+tCUA4arPEn37TzH7A6nw9yzeESUFWH/
MD5:	D76329B30DB65F61D55B20F36B56DA26
SHA1:	5E4C77B723AE8F05B3AE6AFEEE735A4355F00663
SHA-256:	229FBCB11EE7D1F082B6411610E95F726EEC4E6737E6B6392719DF4F0FE3FA1D
SHA-512:	A291AED0897315E88B6378B1DB10ADA05BDA8C1ECCAF73DE23F409FE61860EBD1DBB422063E00996584D3B4B100122931D5BBAB54A88951706D75EFCC660F7 0D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....b.....n.....@.....@.....%.....@..... .....CODE.....`.....b..... ..`DATA.....f.....@...BSS.....x.....idata...%.....&...x.....@....tls.....rdata .....@..P.reloc.....@..P.rsrc....@.....@.....@..P.....j.....@..P..... .....

C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\6tohc1clzbcir.exe

Process:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.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: 60%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.....Rich..... .....PE..L....,?c.....~....._.....@.....`.....@.....(....@.....P.....8.....@..... .....text..... ..`.rdata..dY.....Z.....@..@.data..... .....@....rsrc.....@.....@..@.reloc.....P.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.992737502830512
TrID:	• Win32 Executable (generic) a (10002005/4) 98.86% • Inno Setup installer (109748/4) 1.08% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	file.exe
File size:	1782938
MD5:	14e09c7a5842688842f6c0bf61c17135
SHA1:	4c9e1cbcd933293268c396b3c79f3836665059a8
SHA256:	a5ce2c21d3f92080a06e0aa7862303848b2661181b279a2db9b72b8f31a82702
SHA512:	291eba7114f626be1a02953267f4741adeb71593a75cbb8c65e74dc2783253fc94616ae73126dd2d7dd5eb273cebd6413d36a2a67fae66c1796e5b08c7344b15
SSDEEP:	49152:Zj8WUqIwpfvQvBkF9PPeaPhUMewEgjkdLCgv2MR:98WxIU+mzsv2MR
TLSH:	7885335282B1D4B9E293A77C3C33DD692ED3BA1961781024331E56CF1F277A2AC4E356
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x409c18
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	884310b1928934402ea6fec1dbd3cf5e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFC4h
push ebx

Instruction
push esi
push edi
xor eax, eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-24h], eax
call 00007EFFD44E77E3h
call 00007EFFD44E89EAh
call 00007EFFD44E8C79h
call 00007EFFD44EAC88h
call 00007EFFD44EACCFh
call 00007EFFD44ED5FEh
call 00007EFFD44ED765h
xor eax, eax
push ebp
push 0040A2D4h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 0040A29Dh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [0040C014h]
call 00007EFFD44EE1CBh
call 00007EFFD44EDDFEh
lea edx, dword ptr [ebp-10h]
xor eax, eax
call 00007EFFD44EB2B8h
mov edx, dword ptr [ebp-10h]
mov eax, 0040CDE8h
call 00007EFFD44E788Fh
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [0040CDE8h]
mov dl, 01h
mov eax, 00407364h
call 00007EFFD44EBB47h
mov dword ptr [0040CDECh], eax
xor edx, edx
push ebp
push 0040A255h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007EFFD44EE23Bh
mov dword ptr [0040CDF4h], eax
mov eax, dword ptr [0040CDF4h]
cmp dword ptr [eax+0Ch], 01h
jne 00007EFFD44EE37Ah
mov eax, dword ptr [0040CDF4h]
mov edx, 00000028h
call 00007EFFD44EBF48h
mov edx, dword ptr [000000F4h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd000	0x950	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x2c00	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xf000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x933c	0x9400	False	0.6138883023648649	data	6.557291120606636	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xb000	0x24c	0x400	False	0.3134765625	data	2.7679914923058866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xc000	0xe4c	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xd000	0x950	0xa00	False	0.414453125	data	4.430733069799036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xe000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xf000	0x18	0x200	False	0.052734375	data	0.2044881574398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x10000	0x8b4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x2c00	0x2c00	False	0.3243075284090909	data	4.467134664034375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x11354	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Dutch	Netherlands
RT_ICON	0x1147c	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	Dutch	Netherlands
RT_ICON	0x119e4	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	Dutch	Netherlands
RT_ICON	0x11ccc	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	Dutch	Netherlands
RT_STRING	0x12574	0x2f2	data		
RT_STRING	0x12868	0x30c	data		
RT_STRING	0x12b74	0x2ce	data		
RT_STRING	0x12e44	0x68	data		
RT_STRING	0x12eac	0xb4	data		
RT_STRING	0x12f60	0xae	data		
RT_RCDATA	0x13010	0x2c	data		
RT_GROUP_ICON	0x1303c	0x3e	data	English	United States
RT_VERSION	0x1307c	0x4b8	COM executable for DOS	English	United States
RT_MANIFEST	0x13534	0x560	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Copyright Joe Security LLC 2023

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.12.253.72192.168.2.38 0497082852925 01/25/23- 10:02:04.044834	TCP	2852925	ETPRO TROJAN GCleaner Downloader - Payload Response	80	49708	45.12.253.72	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:02:03.838169098 CET	49707	80	192.168.2.3	45.12.253.56
Jan 25, 2023 10:02:03.864574909 CET	80	49707	45.12.253.56	192.168.2.3
Jan 25, 2023 10:02:03.864726067 CET	49707	80	192.168.2.3	45.12.253.56
Jan 25, 2023 10:02:03.866645098 CET	49707	80	192.168.2.3	45.12.253.56
Jan 25, 2023 10:02:03.894937992 CET	80	49707	45.12.253.56	192.168.2.3
Jan 25, 2023 10:02:03.906924009 CET	80	49707	45.12.253.56	192.168.2.3
Jan 25, 2023 10:02:03.907047033 CET	49707	80	192.168.2.3	45.12.253.56
Jan 25, 2023 10:02:03.933878899 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:03.962369919 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:03.962474108 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:03.965511084 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:03.992350101 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:03.992405891 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:03.992479086 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.017834902 CET	49708	80	192.168.2.3	45.12.253.72

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:02:04.044780970 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.044833899 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.044881105 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.044903040 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.044934034 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.044971943 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045028925 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045042992 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045097113 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045144081 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045197964 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045212984 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045248032 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045277119 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045326948 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045353889 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045403004 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045423031 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045476913 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.045490980 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.045531988 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.072855949 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.072938919 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.072961092 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.072999001 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073029995 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073085070 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073100090 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073138952 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073163986 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073218107 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073234081 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073268890 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073296070 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073349953 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073364019 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073405027 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073425055 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073472023 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073508024 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073524952 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073553085 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073600054 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073626041 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073656082 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073683023 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073729992 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073750019 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073785067 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073812962 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073865891 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073879957 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073920012 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.073941946 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.073987961 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.074008942 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.074048042 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.074069977 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.074122906 CET	80	49708	45.12.253.72	192.168.2.3

Copyright Joe Security LLC 2023

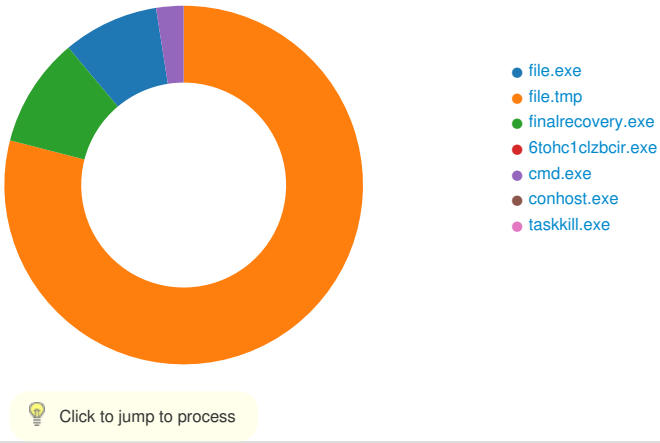
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:02:04.074136019 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.074170113 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.100656986 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.100718021 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.100743055 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.100780964 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.100815058 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.100871086 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.100887060 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.100938082 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.100951910 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.100985050 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101016998 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101146936 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101169109 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101198912 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101242065 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101289034 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101310968 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101342916 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101373911 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101442099 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101459026 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101506948 CET	80	49708	45.12.253.72	192.168.2.3
Jan 25, 2023 10:02:04.101553917 CET	49708	80	192.168.2.3	45.12.253.72
Jan 25, 2023 10:02:04.101569891 CET	49708	80	192.168.2.3	45.12.253.72

HTTP Request Dependency Graph

- 45.12.253.56
- 45.12.253.72
- 45.12.253.75

Statistics

Behavior



Copyright Joe Security LLC 2023

System Behavior

Analysis Process: file.exe PID: 5992, Parent PID: 3452

General

Target ID:	0
Start time:	10:01:58
Start date:	25/01/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	1782938 bytes
MD5 hash:	14E09C7A5842688842F6C0BF61C17135
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: file.tmp PID: 6100, Parent PID: 5992

General

Target ID:	1
Start time:	10:01:58
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp" /SL5="$4023C,1536639,54272,C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	712704 bytes
MD5 hash:	D76329B30DB65F61D55B20F36B56DA26
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 2%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-EFH65.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	452DCF	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-EFH65.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	47B20C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_RegDLL.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EC2	CreateFileA
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EC2	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_shfoldr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EC2	CreateFileA
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_iscrypt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EC2	CreateFileA
C:\Program Files (x86)\FgasoftFR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451B0E	CreateDirectoryA
C:\Program Files (x86)\FgasoftFR\FinalRecovery	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	451B0E	CreateDirectoryA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\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	451B0E	CreateDirectoryA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\unins000.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	473E6E	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-U89TP.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-8DPO5.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-05LH6.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-587OJ.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\is-RVFGU.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA
C:\Program Files (x86)\FgasoftFR\FinalRecovery\data\is-K2TAS.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44FB69	CreateFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-U89TP.tmp	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\unins000.exe	success or wait	1	452027	MoveFileA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-8DPO5.tmp	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\finalrecovery.exe	success or wait	1	452027	MoveFileA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-05LH6.tmp	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\finalrecovery.chm	success or wait	1	452027	MoveFileA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-587OJ.tmp	C:\Program Files (x86)\FgasoftFR\FinalRecovery\Readme.txt	success or wait	1	452027	MoveFileA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-RVFGU.tmp	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\Preview.exe	success or wait	1	452027	MoveFileA
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\data\is-K2TAS.tmp	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\data\Config.xml	success or wait	1	452027	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_RegDLL.tmp	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 68 fa fd fd fd fd fd fd fd fd fd 48 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 7c fd fd fd fd fd fd 7c fd fd fd fd fd fd fd 7c fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4d 3b 4a 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 08 00 00 02 00 00 00 0a 00 00 00 00 00 00 fd 11 00 00 00 10 00 00 00 20 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$H|||RichPELM;J@	success or wait	1	406F09	WriteFile
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_setup64.tmp	0	6144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 05 00 58 57 3a 4a 00 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 12 02 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^l=\=\=\RichPEdXW:J#	success or wait	1	406F09	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-EFH65.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$PEL\;# 4'	success or wait	1	406F09	WriteFile
C:\Users\user\AppData\Local\Temp\is-EFH65.tmp_isetup_iscrypt.dll	0	2560	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 13 fd 0d fd 57 fd 63 fd 57 fd 63 fd 57 fd 63 fd fd fd 3e fd 54 fd 63 fd 57 fd 62 fd 56 fd 63 fd 52 fd 3c fd 56 fd 63 fd 52 fd 3f fd 56 fd 63 fd 52 fd 39 fd 56 fd 63 fd 52 69 63 68 57 fd 63 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 62 fd 40 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 07 0a 00 02 00 00 00 04 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$WcWcWc>TcWbVcR<VcR?VcR9VcRichWcPELb@!	success or wait	1	406F09	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-U89TP.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	MZP@InUn!L!This program must be run under Win32$7	success or wait	11	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-U89TP.tmp	48	4	49 6e 55 6e	InUn	success or wait	1	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-U89TP.tmp	712704	20	fd 1e 1d fd 2c 5a fd fd 23 2a 33 fd 12 fd 7c 48 1d 01 42	Z#*3|HB	success or wait	2	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-U89TP.tmp	712724	10453	49 6e 6e 6f 20 53 65 74 75 70 20 4d 65 73 73 61 67 65 73 20 28 35 2e 31 2e 31 31 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 fd 28 00 00 2a fd fd fd fd 65 6e 5e 26 41 62 6f 75 74 20 53 65 74 75 70 2e 2e 2e 00 25 31 20 76 65 72 73 69 6f 6e 20 25 32 0d 0a 25 33 0d 0a 0d 0a 25 31 20 68 6f 6d 65 20 70 61 67 65 3a 0d 0a 25 34 00 00 41 62 6f 75 74 20 53 65 74 75 70 00 59 6f 75 20 6d 75 73 74 20 62 65 20 6c 6f 67 67 65 64 20 69 6e 20 61 73 20 61 6e 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 77 68 65 6e 20 69 6e 73 74 61 6c 6c 69 6e 67 20 74 68 69 73 20 70 72 6f 67 72 61 6d 2e 00 46 6f 6c 64 65 72 20 6e 61 6d 65 73 20 63 61 6e 6e 6f 74 20 69 6e 63 6c 75 64 65 20 61 6e 79 20 6f 66 20	Inno Setup Messages (5.1.11)(*en^&About Setup...%1 version %2%3%1 home page:%4About SetupYou must be logged in as an administrator when installing this program.Folder names cannot include any of	success or wait	2	44FCC4	WriteFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-8DPO5.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 35 fd fd 63 00 00 00 00 00 00 00 00 fd 00 0e 02 0b 01 07 0a 00 fd 06 00 00 00 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 40 fd 00 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.$PEL5c@@	success or wait	21	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-05LH6.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	44FCC4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-587OJ.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	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\is-RVFGU.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 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	MZP@!L!This program must be run under Win32$7	success or wait	13	44FCC4	WriteFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\data\is-K2TAS.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	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\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 46 67 61 73 6f 66 74 46 52 20 46 69 6e 61 6c 52 65 63 6f 76 65 72 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 67 61 73 6f 66 74 46 52 20 46 69 6e 61 6c 52 65 63 6f 76 65 72 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)FgasoftFR FinalRecoveryFgasoftFR FinalRecovery	success or wait	2	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\unins000.dat	448	12	28 0f 00 00 fd fd fd fd 79 fd 73 fd	(ys	success or wait	2	44FCC4	WriteFile
C:\Program Files (x86)\Fgasoft FR\FinalRecovery\finalrecovery.exe	0	1	4d	M	success or wait	1	4409E6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	unknown	64	success or wait	1	44FBF4	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	44FBF4	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	44FBF4	ReadFile
C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp	unknown	65536	success or wait	1	44FBF4	ReadFile
C:\Users\user\AppData\Local\Temp\is-HGAMR.tmp\file.tmp	unknown	65536	success or wait	10	44FBF4	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	5	44FBF4	ReadFile
C:\Users\user\Desktop\file.exe	unknown	5	success or wait	31	44FBF4	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	success or wait	1	42DD15	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Inno Setup: Setup Version	unicode	5.3.11 (a)	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Inno Setup: App Path	unicode	C:\Program Files (x86)\Fgasoft FR\FinalRecovery	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	InstallLocation	unicode	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Inno Setup: Icon Group	unicode	FgasoftFR\FinalRecovery	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Inno Setup: User	unicode	hardz	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Inno Setup: Language	unicode	default	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	DisplayName	unicode	FinalRecovery 1.25	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	DisplayIcon	unicode	C:\Program Files (x86)\Fgasoft FR\FinalRecovery\FinalRecovery.exe	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	UninstallString	unicode	"C:\Program Files (x86)\Fgasoft FR\FinalRecovery\unins000.exe"	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	QuietUninstallString	unicode	"C:\Program Files (x86)\Fgasoft FR\FinalRecovery\unins000.exe" /SILENT	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	Publisher	unicode	nbafrog.com	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	URLInfoAbout	unicode	http://nbafrog.com/	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	HelpLink	unicode	http://nbafrog.com/	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFR FinalRecovery_is1	URLUpdateInfo	unicode	http://nbafrog.com/	success or wait	1	46DB0C	RegSetValueExA

Copyright Joe Security LLC 2023

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFRFinalRecovery_is1	NoModify	dword	1	success or wait	1	46DB6C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFRFinalRecovery_is1	NoRepair	dword	1	success or wait	1	46DB6C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFRFinalRecovery_is1	InstallDate	unicode	20230125	success or wait	1	46DB0C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FgasoftFRFinalRecovery_is1	EstimatedSize	dword	3313	success or wait	1	46DB6C	RegSetValueExA

Analysis Process: finalrecovery.exe PID: **6076**, Parent PID: **6100**

General

Target ID:	2
Start time:	10:01:59
Start date:	25/01/2023
Path:	C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe"
Imagebase:	0x400000
File size:	1327103 bytes
MD5 hash:	88A9155EB9D85157634ED38D128C877B
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: 00000002.00000002.323772698.0000000003250000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000002.00000002.323409231.0000000000400000.00000040.00000001.01000000.00000007.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	406855	CreateDirectoryA
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\6tohc1clzbcir.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\6tohc1clzbcir.exe	0	73728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b0 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b fd fd fd fd fd fd fd fd 24 fd fd fd fd fd 24 fd fd fd fd fd fd fd fd 24 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2e fd fd fd fd fd 2e fd 39 fd fd fd fd 2e fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$..9.Rich	success or wait	1	4210F4	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\plus[1].htm	0	1	30	0	success or wait	1	401BEA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\stuk[1].htm	0	21	6b 76 51 6f 52 71 74 63 43 79 4d 74 48 6d 51 79 51 58 4f 55 75	kvQoRqtcCyMtHmQyQXOUu	success or wait	1	401BEA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fuckingdllENCR[1].dll	0	1000	fd 17 27 6d 74 fd 68 0d 66 7b 51 7b fd 1c 37 5f 16 01 fd fd 6c fd fd 2f 09 fd 14 fd 33 60 fd 70 fd 24 0a 1c fd 2e 05 5d fd fd fd 09 7e 40 fd fd 56 74 fd 25 0c 07 65 42 fd 39 61 fd fd 2f 5f fd fd fd 47 fd 02 0f 7c fd 4f fd fd 30 48 47 60 fd fd fd 11 fd fd 60 fd fd 06 20 6b 58 fd 78 23 fd 29 fd 1e aa fd fd 57 fd 91 6e 05 10 fd 3b 0b 76 6d 4e fd fd 14 fd 54 1b fd 3a 6c 7b 0c fd fd 07 ea fd fd 14 14 fd 33 37 72 fd 15 fd 2f fd fd 58 fd 31 2c fd fd 29 fd 05 5e 98 59 fd 0d fd fd 4e fd 7b 38 fd 7f fd 34 fd fd bb fd 3d fd a0 52 fd 06 45 09 7a fd 63 fd fd 47 fd 7e 58 fd 30 02 7d fd 62 61 04 00 fd 72 45 fd fd 64 fd fd 0a c8 1d fd fd fd fd fd 28 fd fd fd 4d 60 fd 4f fd 59 27 fd fd fd 3f 7f fd fd 15 44 fd 13 fd	'mhf{Q{7_I/3`p$.]~@Vt%eB9a/_G|O0HG``kx#)Wn;vmNT:l37r/X1,)^YN{8=REzcG~X0}brEd(M`OY?D	success or wait	92	401BEA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dll[1].htm	0	1	30	0	success or wait	6	1000122D	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dll[1].htm	0	1	30	0	success or wait	5	1000122D	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 6tohc1clzbcir.exe PID: **1756**, Parent PID: **6076**

General

Target ID:	3
Start time:	10:02:03
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\6tohc1clzbcir.exe
Wow64 process (32bit):	true
Commandline:	

Imagebase:	0x170000
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: 60%, ReversingLabs
Reputation:	high

Analysis Process: cmd.exe PID: **4488**, Parent PID: **6076**

General

Target ID:	15
Start time:	10:02:35
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "finalrecovery.exe" /f & erase "C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.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)\FgasoftFR\FinalRecovery\finalrecovery.exe	cannot delete	1	D0374	DeleteFileW
C:\Program Files (x86)\FgasoftFR\FinalRecovery\finalrecovery.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: **5040**, Parent PID: **4488**

General

Target ID:	16
Start time:	10:02:35
Start date:	25/01/2023
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: **5968**, Parent PID: **4488**

General

Target ID:	17
Start time:	10:02:35
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "finalrecovery.exe" /f
Imagebase:	0x850000
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