

JoeSandbox Cloud BASIC



ID: 753425

Sample Name: file.exe

Cookbook: default.jbs

Time: 20:03:09

Date: 24/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report file.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Nymaim	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Compliance	5
Networking	5
E-Banking Fraud	5
Data Obfuscation	5
Stealing of Sensitive Information	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	10
Public IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\Program Files (x86)\PrintFolders\Guide.chm (copy)	12
C:\Program Files (x86)\PrintFolders\History.txt (copy)	13
C:\Program Files (x86)\PrintFolders\License.txt (copy)	13
C:\Program Files (x86)\PrintFolders\PrintFolders.exe	13
C:\Program Files (x86)\PrintFolders\Russian.dll (copy)	14
C:\Program Files (x86)\PrintFolders\is-0E5GB.tmp	14
C:\Program Files (x86)\PrintFolders\is-2632S.tmp	14
C:\Program Files (x86)\PrintFolders\is-48N1K.tmp	15
C:\Program Files (x86)\PrintFolders\is-5F7BS.tmp	15
C:\Program Files (x86)\PrintFolders\is-60UNK.tmp	15
C:\Program Files (x86)\PrintFolders\is-OK1CQ.tmp	16
C:\Program Files (x86)\PrintFolders\unins000.dat	16
C:\Program Files (x86)\PrintFolders\unins000.exe (copy)	16
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\fuckngdll\ENCR[1].dll	17
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEEXW4H4\ping[1].htm	17
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\library[1].htm	17
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\count[1].htm	17
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\library[1].htm	18
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_iscrypt.dll	18
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetup_setup64.tmp	18
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetup_shfoldr.dll	19

C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp	19
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\uywwtiNQ.exe	19
Static File Info	20
General	20
File Icon	20
Static PE Info	20
General	20
Entrypoint Preview	20
Data Directories	21
Sections	22
Resources	22
Imports	23
Possible Origin	23
Network Behavior	23
TCP Packets	23
HTTP Request Dependency Graph	25
Statistics	25
Behavior	25
System Behavior	25
Analysis Process: file.exePID: 6084, Parent PID: 3452	25
General	25
File Activities	26
Analysis Process: is-QPTG8.tmpPID: 6080, Parent PID: 6084	26
General	26
File Activities	26
File Created	26
File Moved	27
File Written	27
File Read	32
Registry Activities	32
Key Created	33
Key Value Created	33
Analysis Process: PrintFolders.exePID: 4532, Parent PID: 6080	34
General	34
File Activities	34
File Created	34
File Written	34
Analysis Process: uywwtiNQ.exePID: 6120, Parent PID: 4532	35
General	35
Analysis Process: cmd.exePID: 1336, Parent PID: 4532	36
General	36
File Activities	36
File Deleted	36
Analysis Process: conhost.exePID: 1760, Parent PID: 1336	36
General	36
Analysis Process: taskkill.exePID: 3416, Parent PID: 1336	36
General	36
File Activities	37
Disassembly	37

Windows Analysis Report

file.exe

Overview

General Information

Sample Name:

file.exe

Analysis ID:

753425

MD5:

2ed741014b8cda..

SHA1:

3d65ac9a3d0950..

SHA256:

fc33189d3c1463...

Tags:

exe

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nymaim

Score:

88

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Detected unpacking (overwrites its o...

Yara detected Nymaim

Detected unpacking (changes PE se...

Antivirus detection for URL or domain

Multi AV Scanner detection for drop...

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...

Uses code obfuscation techniques (...)

Classification

Process Tree

System is w10x64

file.exe (PID: 6084 cmdline: C:\Users\user\Desktop\file.exe MD5: 2ED741014B8CDAFD91A740432A3CFFA1)

is-QPTG8.tmp (PID: 6080 cmdline: "C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp" /SL4 \$40228 "C:\Users\user\Desktop\file.exe" 1252960 51712 MD5: 85B94E72C3F2D2B5464E2AAF3C9E242A)

PrintFolders.exe (PID: 4532 cmdline: "C:\Program Files (x86)\PrintFolders\PrintFolders.exe" MD5: 2ABBE052537A4C836AFE8DBAC888F131)

uywwtiNQ.exe (PID: 6120 cmdline: MD5: 3FB36CB0B7172E5298D2992D42984D06)

cmd.exe (PID: 1336 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "PrintFolders.exe" /f & erase "C:\Program Files (x86)\PrintFolders\PrintFolders.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe (PID: 1760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

taskkill.exe (PID: 3416 cmdline: taskkill /im "PrintFolders.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)

cleanup

Malware Configuration

Threatname: Nymaim

```
{
  "C2_addresses": [
    "45.139.185.1",
    "85.31.46.167",
    "107.182.129.235",
    "171.22.30.106"
  ]
}
```

Yara Signatures

Memory Dumps

Copyright Joe Security LLC 2022

Page 4 of 37

Source	Rule	Description	Author	Strings
00000002.00000002.325696039.0000000001660000.0000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000002.00000002.326103420.00000000033A0000.0000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000002.00000002.325006522.0000000000400000.00000040.00000001.01000000.00000006.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.PrintFolders.exe.400000.1.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.PrintFolders.exe.400000.1.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.PrintFolders.exe.33a0000.3.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
2.2.PrintFolders.exe.33a0000.3.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Sigma Signatures

 No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nymaim

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

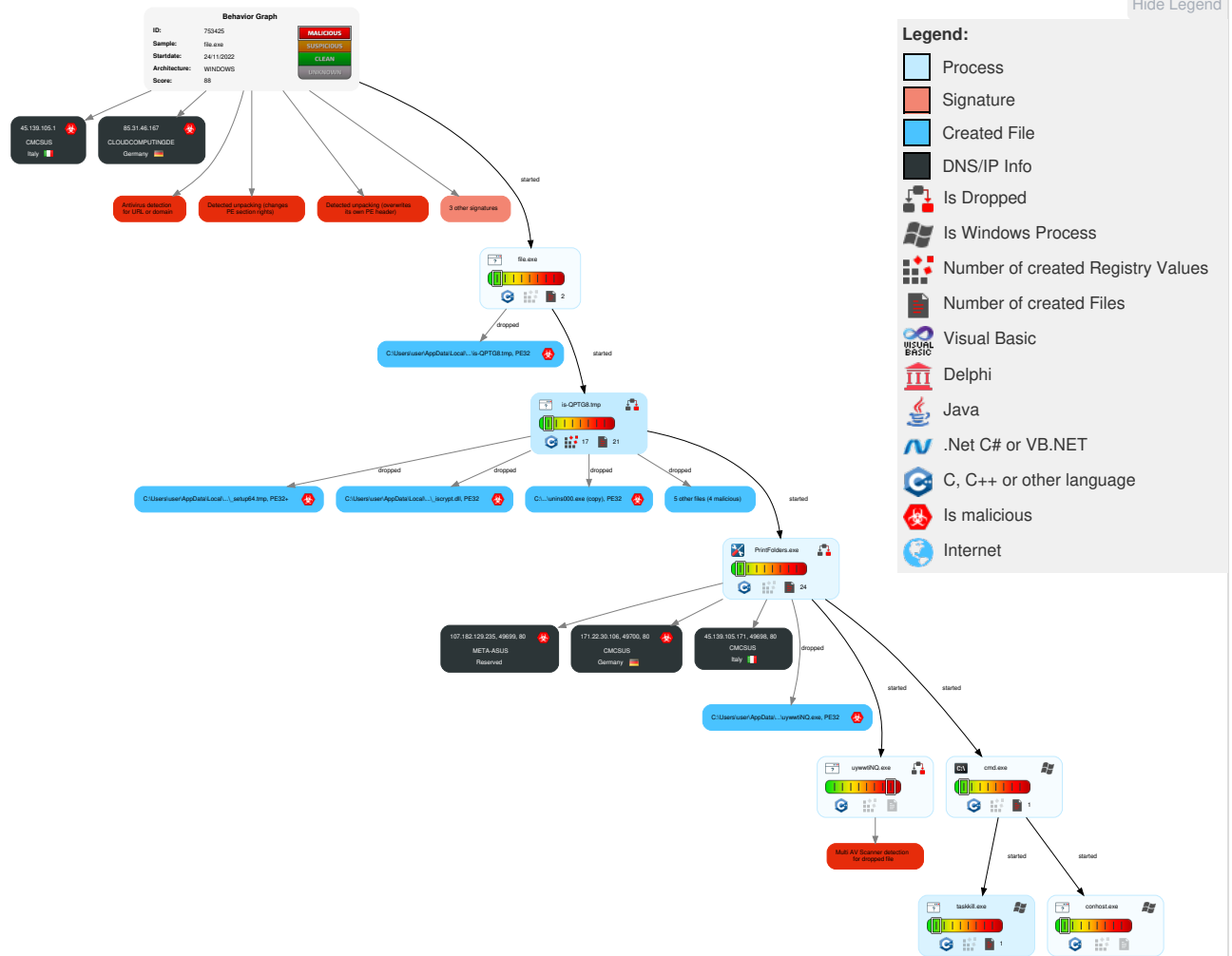


Yara detected Nymaim

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	2 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 3 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 4 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	3 Process 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)	1 3 Process Injection	NTDS	1 1 Application Window 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	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Account 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	3 Obfuscated Files or Information	Cached Domain Credentials	1 System Owner/User 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	2 3 Software Packing	DCSync	3 File and Directory 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	2 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

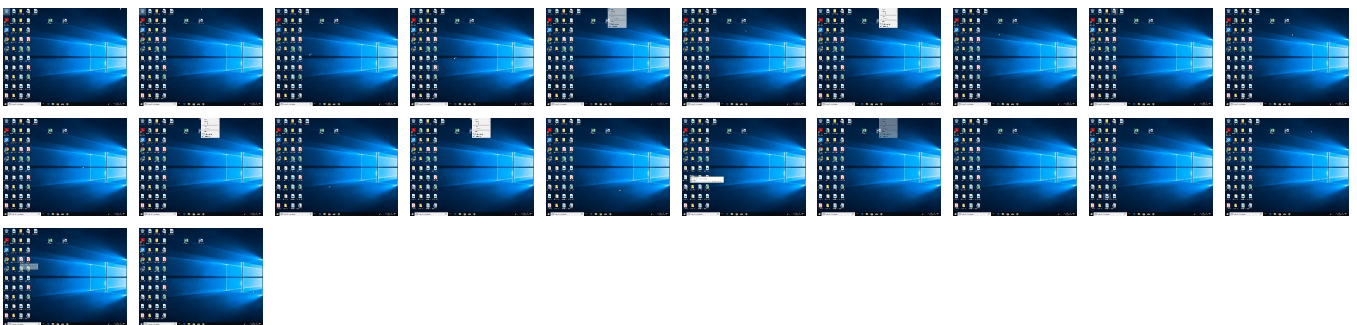
Behavior Graph



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)\PrintFolders\PrintFolders.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\PrintFolders\Russian.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\PrintFolders\is-2632S.tmp	0%	ReversingLabs		
C:\Program Files (x86)\PrintFolders\is-48N1K.tmp	2%	ReversingLabs		
C:\Program Files (x86)\PrintFolders\unins000.exe (copy)	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_iscrypt.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetup_shfolder.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp	4%	ReversingLabs		
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\uywwtiNQ.exe	46%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
--------	-----------	---------	-------	------	----------

Source	Detection	Scanner	Label	Link	Download
2.2.PrintFolders.exe.10000000.6.unpack	100%	Avira	TR/Crypt.XPAC K.Gen8		Download File
1.2.is-QPTG8.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.12 32832		Download File
2.2.PrintFolders.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.12 50671		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.12 48792		Download File
0.3.file.exe.20b8000.6.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File

Domains
 No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://45.139.105.171/itsnotmalware/count.php?sub=NOSUB&stream=mixtwo&substream=mixinte	0%	URL Reputation	safe	
http://107.182.129.235/storage/extension.php	0%	URL Reputation	safe	
http://www.remobjects.com/?ps	0%	URL Reputation	safe	
http://www.innosetup.com	0%	URL Reputation	safe	
http://107.182.129.235/storage/ping.php	0%	URL Reputation	safe	
http://107.182.129.235/storage/ping.php	0%	URL Reputation	safe	
http://171.22.30.106/library.php	100%	URL Reputation	malware	
http://www.remobjects.com/?psU	0%	URL Reputation	safe	
http://171.22.30.106/library.phpXZ	100%	Avira URL Cloud	malware	
http://107.182.129.235/storage/extension.phpum	0%	Avira URL Cloud	safe	
http://www.atopoint.com	0%	Virustotal		Browse
http://pfolders.atopoint.com.	0%	Avira URL Cloud	safe	
http://www.atopoint.com	0%	Avira URL Cloud	safe	
http://pfolders.atopoint.com	0%	Avira URL Cloud	safe	
http://www.atopoint.com.	0%	Avira URL Cloud	safe	
http://171.22.30.106/library.phpBZ	100%	Avira URL Cloud	malware	
http://www.innosetup.comDVarFileInfo\$	0%	Avira URL Cloud	safe	

Domains and IPs
Contacted Domains
 No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://pfolders.atopoint.com.	file.exe, 00000000.00000003.327202532.00 000000020B1000.00000004.00001000.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.239393272.000000000020B1000.00000004 .00001000.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	is-QPTG8.tmp, is-QPTG8.tmp, 00000001.0000000.240048151.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-48N1K.tmp.1.dr, is-QPTG8.tmp.0.dr	false	URL Reputation: safe	unknown
http://171.22.30.106/library.phpXZ	PrintFolders.exe, 00000002.00000002.325942100.0000000001762000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://www.atopoint.com	file.exe, 00000000.00000003.239322832.0000000021A0000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000003.327202532.00000000020B1000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000003.239393272.00000000020B1000.00000004.00001000.00020000.00000000.sdmp, is-QPTG8.tmp, 00000001.00000000.240048151.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-48N1K.tmp.1.dr, is-QPTG8.tmp.0.dr	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://www.remobjects.com/?ps	file.exe, 00000000.00000003.239484290.000000021A0000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000003.239653432.00000000020B8000.00000004.00001000.00020000.00000000.sdmp, is-QPTG8.tmp, is-QPTG8.tmp, 00000001.00000000.240048151.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-48N1K.tmp.1.dr, is-QPTG8.tmp.0.dr	false	URL Reputation: safe	unknown
http://pfolders.atopoint.com	file.exe, 00000000.00000003.239393272.000000020B1000.00000004.00001000.00020000.0.00000000.sdmp, is-QPTG8.tmp, 00000001.00000003.240607544.0000000002750000.0000004.00001000.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.innosetup.com	file.exe	false	URL Reputation: safe	unknown
http://107.182.129.235/storage/extension.phpum	PrintFolders.exe, 00000002.00000002.325958183.0000000001773000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.atopoint.com.	file.exe, 00000000.00000003.327202532.000000020B1000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000003.239393272.00000000020B1000.00000004.00001000.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://171.22.30.106/library.phpBZ	PrintFolders.exe, 00000002.00000002.325942100.0000000001762000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://www.innosetup.comDVarFileInfo\$	file.exe, 00000000.00000003.239484290.000000021A0000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000003.239653432.00000000020B8000.00000004.00001000.00020000.00000000.sdmp, is-QPTG8.tmp, 00000001.00000002.326821048.00000000004BC000.00000002.00000001.01000000.00000004.sdmp, is-48N1K.tmp.1.dr, is-QPTG8.tmp.0.dr	false	Avira URL Cloud: safe	low
http://www.remobjects.com/?psU	file.exe, 00000000.00000003.239484290.000000021A0000.00000004.00001000.00020000.0.00000000.sdmp, file.exe, 00000000.00000003.239653432.00000000020B8000.00000004.00001000.00020000.00000000.sdmp, is-QPTG8.tmp, 00000001.00000000.240048151.0000000000401000.00000020.00000001.01000000.00000004.sdmp, is-48N1K.tmp.1.dr, is-QPTG8.tmp.0.dr	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753425
Start date and time:	2022-11-24 20:03:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@12/23@0/5

EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 39.1% (good quality ratio 37.9%) - Quality average: 80.9% - Quality standard deviation: 24.7%
HCA Information:	- Successful, ratio: 96% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	Found application associated with file extension: .exe

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
20:04:06	API Interceptor	1x Sleep call for process: uywwtiNQ.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)\PrintFolders\Guide.chm (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	118869
Entropy (8bit):	7.933172616287708
Encrypted:	false

SSDEEP:	1536:a8+b7UxViBmVQVxSHmlKruCGFkw8dctBJclFEvSrT3eoxNjT+YL/fe3iWP7:Z+b76wV3hCb86tBJc7SffxNjqO/qiWT
MD5:	204A5BF160646F9A55ED70AB6E1A07A6
SHA1:	5404AB219FA01C270ADC36303D447109503C4A4D
SHA-256:	CACDD2C8BFA4BAE33A16A10ED609F4841AC5C4C2FE481ED0FD8CB04BC8016BBDD
SHA-512:	6AAFBFAF8565BF57BF4CC9E8D5EEF947E32E0D1A962C0BB619A25C35C68B7AA24599C60CB1C1B108FC9F58A1F13FF80B66E1A4DA506BE2FFD2DD05331865DA A15
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	ITSF.....[.....".....".{.....".....".`.....x.....T.....U.....ITSP....T.....j.....".T.....PMGL...../...../.....#IDXHDR.. ...../ITBITS.....#STRINGS...>.../SYSTEM..V.../TOPICS...`/URLSTR...Gw./URLTBL...H./#WINDOWS....D/\$FfItiMain...g..8/\$OBJINST...T.../author.htm...m.</c mdline.htm...O.../ctxmenu.jpg...3..B./index.htm...y./interface.htm...^./logo.jpg...P..4./main.css...u.../PrintDir.hhc...).'/screenshot.jpg....././shell.htm...~.Q...:DataSpace/Na meList..<(:DataSpace/Storage/MSCCompressed/Content..[.....:DataSpace/Storage/MSCCompressed/ControlData.j.)::DataSpace/Storage/MSCCompressed/SpanInfo.b./ ::DataSpace/Storage/MSCCompressed/Transform/List.<&_::DataSpace/Storage/MSCCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C)/Instanc eData/...i::DataSpace/Storage/MSCCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C)/InstanceData/ResetTable...P.....

C:\Program Files (x86)\PrintFolders\History.txt (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5403
Entropy (8bit):	4.918324842676727
Encrypted:	false
SSDEEP:	96:uUzxQ0Bz664UbxDcqEVFUz1BDzeRGH+QanjY3ZLBxdfC4INXM/gr53F8EPeHI9j4:uU1QyZ4e9cqEfUz1BD0GH+QGjYJBxdY
MD5:	C8B211D81EB7D4F9EBB071A117444D51
SHA1:	43BF57BB0931EBED953FE17F937C1C7FF58A027C
SHA-256:	AFD6FEA6A792B722E45A6587F70334F30051798017F4A278508C7ED3FEEA80CC
SHA-512:	C7C558EB66B570A0B03D1E8941217673677A6AF1F7CE4C43BE77D1AA859AD8DF7B212CF778B03678DD451535C7A7B02FEB65F20B744A8E9C969DF633F79A2A B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	=====.. History of Releases..=====...Legend.....[+] - added..[*] - modified..[-] - bug fixed.....Version 2.51b.....[-] The output file path wasn't updated in certain circumstances..[-] Added the workaround for the modal message boxes bug in Wine....Version 2.51a.....[+] Focus rectangle added for the "Go!" button..[+] Added program version to the setup info..[*] A couple of interface optimizations..[-] "Check for updates" now should work under Wine....Version 2.51.....[+] The "Help" buttons now present in each dialog..[+] Russian user interface..[*] Improved Wine compatibility..[-] One very elusive bug inherited from the early versions finally fixed..[-] Improved the "Check for updates" behavior..[-] Fixed several regressions and smaller bugs....Version 2.5.....[+] C hecking for updates on startup (registered users only)..[*] Faster processing of large numbers of files..[*] Folders containing no files acc

C:\Program Files (x86)\PrintFolders\License.txt (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	RAGE Package Format (RPF),
Category:	dropped
Size (bytes):	3391
Entropy (8bit):	4.812121234949207
Encrypted:	false
SSDEEP:	96:FjjD9Grzqpptlaj6JGcnRH7aamJL4zUtWAbakj:FYrrawhbaVFtTuk
MD5:	A5E8094B0CBADE929AEE07F5DA5E9429
SHA1:	60BB56A380CD9126AC067AE39B262E28A22532CD
SHA-256:	F3AC2009C96EB3A42AFAEC7FA67D3A14E5E9C30819B543D572C9BEA790CFCAD1
SHA-512:	018D1963A0B45A731687C5811E6447911E9BC7285B25EE3BBAD95D4D9C23718EF4E9714714C8A68617EAE4F840FB3D76BC77B0C49A64346D9605CCF70592356C
Malicious:	false
Preview:	PRINTFOLDERS version 2.51b..Copyright (C) 2009-2012 Andrey Pivovarov. All rights reserved.....END USER LICENSE AGREEMENT....This license describes the conditions under which you may use version 2.51b of ..PrintFolders ("the program"). If you are unable or unwilling to accept these ..conditions in full, then, notwithstanding the conditions in the remainder of ..this license, you may not use the program at all.....The program is a full-functional software. The program never expires and may be ..used for any period of time. The program has no exclusive limitations and does ..not require registration, though you may register your copy of the program to ..support the authors and remove the nag screens.....You may copy and distribute verbatim copies of the program executable, in any ..medium, provided that you conspicuously and appropriately publish on each copy ..an appropriate copyright notice and disclaimer of warranty; keep intact all the ..notices that refer to this license and to the a

C:\Program Files (x86)\PrintFolders\PrintFolders.exe  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	modified
Size (bytes):	1990648
Entropy (8bit):	6.135022664098298
Encrypted:	false

SSDEEP:	49152:G0e7jkeRVgTU1Sw1pUfsWFQVNiTneoDsQ:gE2kYpUfs0QCe9Q
MD5:	2ABBE052537A4C836AFE8DBAC888F131
SHA1:	A0629A6130B7B7107681B033C0AFEE0C4EEB6CDB
SHA-256:	70717E7EE9E2A9EE5EF3804E3571B0DF6A1C2ABAF63179410A414C99705F9A47
SHA-512:	CD0361EF97CF7EB1CF248875FCBA471A2D5A9F82FA38EA15825EE60159B16465904116C1244D0CA21ED3B49895C2647653FF836B7A114FE5EC384C4E28962E01
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....PE..L....c.....'.....0.....@.....`..... .....4.....0...c.....text.....`..rdata..n.....@..@.data...@.....@...tIs.....@....rsrc...p...0...p...0.....@..@.rgw89.....`.....

C:\Program Files (x86)\PrintFolders\Russian.dll (copy)  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	4.508743257769972
Encrypted:	false
SSDEEP:	192:kxsrC3rSQgvlS7pEeHPmIOBaVeFSiLW70ygWr:csvGmIOBa5f
MD5:	4FB606EDBDE8EFB6D34E6E1BC5F677F1
SHA1:	F8F094064D107384E619DED1139932AA38476272
SHA-256:	A960C9DCD1D5C7B79F4FDD38D6F25299F4F7925555E381EA4AB6217681482F62
SHA-512:	5B34ECB87582FFC210CA4EED06C729979D7197191CF74EB3CDB59D0F629603C171D50B6D9351DEB7DD13F6FCBBDD79F8A23ED0114BBD991520CA9BFA4EF10A4D
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....u.....5.....5.....Rich.....PE..L....SwO.....P.....p.....@.....`..M.....rdata..m..... .....@..@.rsrc...`M... ..N.....@..@.....

C:\Program Files (x86)\PrintFolders\is-0E5GB.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	RAGE Package Format (RPF),
Category:	dropped
Size (bytes):	3391
Entropy (8bit):	4.812121234949207
Encrypted:	false
SSDEEP:	96:FijD9GrzqpptIaj6JGcnRH7aamJL4zUtWAbakj:FYrrawhbaVFiTuk
MD5:	A5E8094B0CBADE929AEE07F5DA5E9429
SHA1:	60BB56A380CD9126AC067AE39B262E28A22532CD
SHA-256:	F3AC2009C96EB3A42AFAEC7FA67D3A14E5E9E30819B543D572C9BEA790CFCAD1
SHA-512:	018D1963A0B45A731687C5811E6447911E9BC7285B25EE3BBAD95D4D9C23718EF4E9714714C8A68617EAE4F840FB3D76BC77B0C49A64346D9605CCF70592356C
Malicious:	false
Preview:	PRINTFOLDERS version 2.51b..Copyright (C) 2009-2012 Andrey Pivovarov. All rights reserved.....END USER LICENSE AGREEMENT.....This license describes the conditions under which you may use version 2.51b of ..PrintFolders ("the program"). If you are unable or unwilling to accept these ..conditions in full, then, notwithstanding the conditions in the remainder of ..this license, you may not use the program at all.....The program is a full-functional software. The program never expires and may be ..used for any period of time. The program has no exclusive limitations and does ..not require registration, though you may register your copy of the program to ..support the authors and remove the nag screens.....You may copy and distribute verbatim copies of the program executable, in any ..medium, provided that you conspicuously and appropriately publish on each copy ..an appropriate copyright notice and disclaimer of warranty; keep intact all the ..notices that refer to this license and to the a

C:\Program Files (x86)\PrintFolders\is-2632S.tmp  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	4.508743257769972
Encrypted:	false
SSDEEP:	192:kxsrC3rSQgvlS7pEeHPmIOBaVeFSiLW70ygWr:csvGmIOBa5f
MD5:	4FB606EDBDE8EFB6D34E6E1BC5F677F1

SHA1:	F8F094064D107384E619DED1139932AA38476272
SHA-256:	A960C9DCD1D5C7B79F4FDD38D6F25299F4F7925555E381EA4AB6217681482F62
SHA-512:	5B34ECB87582FFC210CA4EED06C729979D7197191CF74EB3CDB59D0F629603C171D50B6D9351DEB7DD13F6FCBBDD79F8A23ED0114BBD991520CA9BFA4EF10A4D
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....u.....5.....5.....Rich.....PE..L....SwO.....P.....p.....@.....M.....rdata..m.....@..@.rsrc...`M... ..N.....@..@.....

C:\Program Files (x86)\PrintFolders\is-48N1K.tmp  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	669450
Entropy (8bit):	6.478399502986981
Encrypted:	false
SSDEEP:	12288:2h5UooqWolrP837JzHvA6izJgnnyFNmayiAZrvJxOx:M5NoqWolrP837JzHvA6yknyWFxvJxOx
MD5:	CF680B53729F6E3059183D51F91D337D
SHA1:	4D6EB765BB4837F09283101490375DF5F68C8E37
SHA-256:	A3F8C832C69388A88E47DD8B612382F74D5131E8C710741EFB2410EC450BDF2D
SHA-512:	1F59A9A03485DFDB9E232F0D8B52CD864993FC25734E16DD2160190045626531685E81BDBCf0636EBA9F7CEDA9DA082A9AAD2DD4C5BFE165110731B7F89FCA1
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 2%
Preview:	MZP.....@.....InUn.....!..L!..This program must be run under Win32..\$7.....PE..L....`B*.....d.....t.....@.....@.....\$%....P+.....@.....0..... .....CODE.....`DATA.....@..BSS...x.....idata..\$%.....&.....@...tls.....rdata.....0.....@..P.reloc.....@.....@..P.rsrc...P+.....@..P.....@..P.....

C:\Program Files (x86)\PrintFolders\is-5F7BS.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5403
Entropy (8bit):	4.918324842676727
Encrypted:	false
SSDEEP:	96:uUzxQ0Bz664UbxDcqEVFUz1BDzeRGH+QanjY3ZLBxdfC4INXM/gr53F8EPeHI9j4:uU1QyZ4e9cqEfUz1BD0GH+QGjYJBxdY
MD5:	C8B211D81EB7D4F9EBB071A117444D51
SHA1:	43BF57BB0931EBED953FE17F937C1C7FF58A027C
SHA-256:	AFD6FEA6A792B722E45A6587F70334F30051798017F4A278508C7ED3FEEA80CC
SHA-512:	C7C558EB666B570A0B03D1E8941217673677A6AF1F7CE4C43BE77D1AA859AD8DF7B212CF778B03678DD451535C7A7B02FEB65F20B744A8E9C969DF633F79A2AB
Malicious:	false
Preview:	=====.. History of Releases.=====...Legend.....[+] - added..[*] - modified..[-] - bug fixed.....Version 2.51b.....[-] The output file path wasn't updated in certain circumstances..[-] Added the workaround for the modal message boxes bug in Wine....Version 2.51a.....[+] Focus rectangle added for the "Go!" button..[+] Added program version to the setup info..[*] A couple of interface optimizations..[-] "Check for updates" now should work under Wine....Version 2.51.....[+] The "Help" buttons now present in each dialog..[+] Russian user interface..[*] Improved Wine compatibility..[-] One very elusive bug inherited from the early versions finally fixed..[-] Improved the "Check for updates" behavior..[-] Fixed several regressions and smaller bugs....Version 2.5.....[+] C hecking for updates on startup (registered users only)..[*] Faster processing of large numbers of files..[*] Folders containing no files acc

C:\Program Files (x86)\PrintFolders\is-60UNK.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	118869
Entropy (8bit):	7.933172616287708
Encrypted:	false
SSDEEP:	1536:a8+b7UxVIBmVQVxSHmlKruCGFkw8dctBJcIFEvSrT3eoxNjT+YL/fe3iWP7:Z+b76wV3hCb86tBJc7SffxNjqO/qiWT
MD5:	204A5BF160646F9A55ED70AB6E1A07A6
SHA1:	5404AB219FA01C270ADC36303D447109503C4A4D

SHA-256:	CACDD2C8BFA4BAE33A16A10ED609F4841AC5C4C2FE481ED0FD8CB04BC8016BBD
SHA-512:	6AAFBFAF8565BF57BF4CC9E8D5EEF947E32E0D1A962C0BB619A25C35C68B7AA24599C60CB1C1B108FC9F58A1F13FF80B66E1A4DA506BE2FFD2DD05331865DA A15
Malicious:	false
Preview:	ITSF.....[.....".....][.....".....x.....T.....U.....ITSP...T.....j.....l.....".....T.....PMGL...../...../.....#IDXHDR../#ITBITS.../#STRINGS...>.../#SYSTEM..V.../#TOPICS...`../URLSTR...Gw./#URLTBL...H./#WINDOWS.....D./\$FItiMain...g..8./\$OBJINST...T.../author.htm...m.<./c mdline.htm...O.../ctxmenu.jpg...3..B./index.htm...'.y./interface.htm...^./logo.jpg...P..4./main.css...u.../PrintDir.hhc...).'/screenshot.jpg....././shell.htm...~.Q::DataSpace/Na meList..<(:DataSpace/Storage/MSCompressed/Content..[...::DataSpace/Storage/MSCompressed/ControlData.j)::DataSpace/Storage/MSCompressed/SpanInfo.b./ ::DataSpace/Storage/MSCompressed/Transform/List.<&_::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/Instanc eData/...i::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/InstanceData/ResetTable...P.....

C:\Program Files (x86)\PrintFolders\is-OK1CQ.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	data
Category:	dropped
Size (bytes):	1990648
Entropy (8bit):	6.13502190347102
Encrypted:	false
SSDEEP:	49152:v0e7jkeRVgTU1Sw1pUfsWfQVNiTneoDsQ:zE2kYpUfs0QCe9Q
MD5:	DE99B1E8819F3E7BD2265CDB39050B9C
SHA1:	FC3C8DDE6D6D01983B1888C3139AD37DED4ED2FE
SHA-256:	37343E82AD7BE281C2CB98A3B97DE2E5AD31BDFEB7850E5A54F07D124B96D4D6
SHA-512:	04B99842B2DD22AFCF5399B71915D0EEF0036581050AC6DE4320AEBFE81A0EA7FD1EC9ED79D98B4FD2D4704DD006D12F1B47869DAFC51EAC10096CF328F54 BC
Malicious:	false
Preview:	.Z.....@.....!..!This program cannot be run in DOS mode....\$.PE..L...c.....'.....0.....@.....`..... 4.....0...c.....text.....`..rdata..n.....@..@.data..@.....@...tls.....@....rsrc....p..0..p..0.....@..@.rgw89.....`.....

C:\Program Files (x86)\PrintFolders\unins000.dat	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	InnoSetup Log PrintFolders {73D78C7A-78F2-476F-86FF-9025EA410908}, version 0x2a, 3813 bytes, 609290\user, "C:\Program Files (x86)\PrintFolders"
Category:	dropped
Size (bytes):	3813
Entropy (8bit):	4.504029461113114
Encrypted:	false
SSDEEP:	48:weNyMHLBv8ID86plmE6FoIN0hqkLVO3471qV/LD0zA47brL1XLk:hrp8ID86p45olyhqYOIh0No
MD5:	5CA9A255015A4BEF13CC4C4CB36429CA
SHA1:	C26147239E8EB7D5E47FF10808E94D91DACB2C1D
SHA-256:	E6A32D37F4C0E10502BD5D726A310B9AC7D7DB52E79F87728AD30110F580CED5
SHA-512:	070DA32A80D5C79807BE4579CEB958CCD33CE07080D35EFAC817A9DC5B4BC42FD2008A12764D774AB999834968F1F9206C5094685FE889B4DEE01671837E59C
Malicious:	false
Preview:	Inno Setup Uninstall Log (b).....{73D78C7A-78F2-476F-86FF-9025EA410908}}.....PrintFolders.....*.....%.....<.....y.....C....6 09290.user#C:\Program Files (x86)\PrintFolders.....Q.IFPS.....BOOLEAN......TWIZARDFORM.....TWIZARDFORM.....TPASSWORDEDIT.....TPASSWORDEDIT.....!MAIN....-1...'..dll:kernel32.dll.CreateFileA.....#. .dll:kernel32.dll.WriteFile.....!...dll:kernel32.dll.CloseHandle.....!...dll:kernel32.dll.ExitProcess.....\$...dll:User32.dll.GetSystemMet

C:\Program Files (x86)\PrintFolders\unins000.exe (copy)  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	669450
Entropy (8bit):	6.478399502986981
Encrypted:	false
SSDEEP:	12288:2h5UooqWolrP837JzHvA6izJgnnyFNmayiAZrvJxOx:M5NoqWolrP837JzHvA6yknyWFxvJxOx
MD5:	CF680B53729F6E3059183D51F91D337D
SHA1:	4D6EB765BB4837F09283101490375DF5F68C8E37
SHA-256:	A3F8C832C69388A88E47DD8B612382F74D5131E8C710741EFB2410EC450BDF2D
SHA-512:	1F59A9A03485DFDB9E232F0D8B52CD864993FC25734E16DD2160190045626531685E81BDBCF0636EBA9F7CEDA9DA082A9AAD2DD4C5BFE165110731B7F89FCA 1
Malicious:	true

Antivirus:	Antivirus: ReversingLabs, Detection: 2%
Preview:	MZP.....@.....InUn.....I..L.I..This program must be run under Win32..\$7.....PE..L...^B*.....d.....t.....@.....@.....\$%...P+.....@.....0.....CODE.....`DATA.....@...BSS...x.....idata.\$%.....&.....@...tls.....rdata.....0.....@..P.reloc.....@.....@..P.rsrc...P+.....@..P.....@..P.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OW10PBUV\fuckngdllENCr[1].dll 	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.exe
File Type:	data
Category:	dropped
Size (bytes):	94224
Entropy (8bit):	7.998072640845361
Encrypted:	true
SSDEEP:	1536:Nsbl9W6dHdtnEXOxZpZlUcETzNtXofjmgGTeJduLLt+YBPoJTMrmNXg30:KWW6TZVz9PNtXo8M5OR0
MD5:	418619EA97671304AF80EC60F5A50B62
SHA1:	F11DCD709BDE2FC86EBBCD66E1CE68A8A3F9CB6
SHA-256:	EB7ECE66C14849064F462DF4987D6D59073D812C44D81568429614581106E0F4
SHA-512:	F2E1AE47B5B0A5D3DD22DD6339E15FEE3D7F04EF03917AE2A7686E73E9F06FB95C8008038C018939BB9925F395D765C9690BF7874DC5E90BC2F77C1E730D3AC0
Malicious:	false
Preview:	...mi...};...F").T..K;...O.Y0:....3j\..lj.2R.P...C...q .2....iR2W.F.C=MU.....H6...A....@...O.c...M.x8...L.-.b.. C...Z}.w...l.a.aT...br,...6w#.j.P.li.=.....o.....S.{.R.....5...#;...- ...b+...G(>...Q.....iN{+y...ZC.z3sE...T..2.J...3.9U.4&..P....."wl....@...x%>..D..'z.^....^(....NC.[[k.....V]G..)e.....`.....K/L.Ul..F..".8\$.Ad....i.g..0.d...[...T"!U.M.=0.....,ku. W,...7.Q.Fi=w...u....Q-.R.)0...L....n...tnv....z....e..l.C.....9.V.~1+[].7...xQ.....\$L..o.eQ./b.Z.....p;.*)...#b...%1.....@...G..[...../c.Z.....G...:n..E.i.O..o.U.B.Px...1{.a. ...#k.dj..L4...}.d<....llyy.J.f.W...^vV.Ao.K."+OX8IF...YP...u.-.Bik.[u...&Wt..P..m....^..k~....l..o.zMV.l.s..h...{.n2;z...K.?S...eW...c.....-V.bg..9.l.g.x.g...}'..5..(*P...J#...: IS..D).v.....jk9.LQF...oOhV...)h.v^~..F...<....Vh.1....!...!...BYc..C?..D2.....2.K(.6...B...D..ay..= ...'....[1.~.YB:/...A'...=.F..K.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ping[1].htm	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	17
Entropy (8bit):	3.1751231351134614
Encrypted:	false
SSDEEP:	3:nCmxEl:Cmc
MD5:	064DB2A4C3D31A4DC6AA2538F3FE7377
SHA1:	8F877AE1873C88076D854425221E352CA4178DFA
SHA-256:	0A3EC2C4FC062D561F0DC989C6699E06FFF850BBD47923F14F26135EF42107C0
SHA-512:	CA94BC1338FC283C3E5C427065C29BA32C5A12170782E18AA0292722826C5CB4C3B29A5134464FFEB67A77CD85D8E15715C17A049B7AD4E2C890E97385751BE
Malicious:	false
Preview:	UwUooollrwgh24uuU

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUE05ZZ\library[1].htm	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.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:	5FCEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\count[1].htm	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.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:	5FECB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\library[1].htm	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.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:	5FECB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Temp\is-385TG.tmp_iscrypt.dll  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.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:SGDKRiVImgUNBsG
MD5:	A69559718AB506675E907FE49DEB71E9
SHA1:	BC8F404FFDB1960B50C12FF9413C893B56F2E36F
SHA-256:	2F6294F9AA09F59A574B5DCD33BE54E16B39377984F3D5658CDA44950FA0F8FC
SHA-512:	E52E0AA7FE3F79E36330C455D944653D449BA05B2F9ABEE0914A0910C3452CFA679A40441F9AC696B3CCF9445CBB85095747E86153402FC362BB30AC08249A6C
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 2%
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-385TG.tmp_isetup_setup64.tmp  	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.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+XI4SH8u09tmRJ/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-385TG.tmp_isetup_shfoldr.dll 	
Process:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.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:	9908E573921D5DBC3454A1C0A6C969AB8A81CC2E8B5385391D46B1A738FB06A76AA3282E0E58D0D2FFA6F27C85668CD5178E1500B8A39B1BBAE04366AE6A8613
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....lzJ^..\$...\$...%".\$.T87..\$.["...\$...\$.Rich..\$......PE ..L...;.....#.....4.....'.....0.....q.....k..!)..<...@../.....p..T.....text... {.....`..data...`..0.....&.....@...rsrc.../...@...0...(.....@..@.reloc.....p.....X.....@..B.....

C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp  	
Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	658944
Entropy (8bit):	6.468629759056718
Encrypted:	false
SSDEEP:	12288:Oh5UooqWolrP837JzHvA6izJgnyFNmayiAZrvJxO0:05NoqWolrP837JzHvA6yknyWFxvJxO0
MD5:	85B94E72C3F2D2B5464E2AAF3C9E242A
SHA1:	CE7CCAE5F50A990D059D59292D4A332979E162BA
SHA-256:	1441464FEEEF365573AF18802C464769B7D3107624FDE24604F57E386F97F1A7
SHA-512:	C0C27189989DB482BE9BDA5B6B8B1441BDC5E9B0F3A41CCAB4C4BE516E7F99E25717845361A5B196114502FAAAF21BEC7ACA91B497ACD2E2396F49C31850880
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 4%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..\$7.....PE..L...^B*.....d.....t.....@.....@.....\$%...P+.....@.....0.....CODE.....`DATA.....@...BSS....x.....idata..\$%...&.....@...tls.....rdata.....0.....@...P.reloc.....@.....@...P.rsrc...P+.....@...P.....@...P.....

C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\uywwtiNQ.exe  	
Process:	C:\Program Files (x86)\PrintFolders\PrintFolders.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+XfHAgbqmE8MpKdhuasZLUM7DsWIXcdyZgfmI:WDLZKa/MiXfHAgbqmEtxsfmyZgfmI
MD5:	3FB36CB0B7172E5298D2992D42984D06
SHA1:	439827777DF4A337CBB9FA4A4640D0D3FA1738B7
SHA-256:	27AE813CEFF8AA56E9FA68C8E50BB1C6C4A01636015EAC4BD8BF444AFB7020D6
SHA-512:	6B39CB32D77200209A25080AC92BC71B1F468E2946B651023793F3585EE6034ADC70924DBD751CF4A51B5E71377854F1AB43C2DD287D4837E7B544FF886F470C

Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 46%
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):	7.991071631974842
TrID:	- Win32 Executable (generic) a (10002005/4) 98.88% - Inno Setup installer (109748/4) 1.08% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	1488975
MD5:	2ed741014b8cdfd91a740432a3cfa1
SHA1:	3d65ac9a3d0950a55d4c7e4cb5a6bfeab180cab
SHA256:	fc33189d3c146375f5742bbb0e82277e2b8ed3789d8feae27939e834b07ee8dc
SHA512:	a309386146699f4cfd48872f705cce681266c63af93d9e9347a79e940a6221ce6a3606e52f7afa8a4ca91e259c31f600bad43c851eca387941b4154fe69c6d3c
SSDEEP:	24576:hizo5TdlqnGpid2DCDeCSxDQrOAE/1MA5sLsplYj85itlqSdgZIY7eCLxYi5:KSjiQeef2E/1MDQLJjHlqDNeVi5
TLSH:	2D65330EE623297CE08340B25F7A59584766BE240D782162FAF0A4F58D7FB85690F7D3
File Content Preview:	MZP.....@.....Inno'....G.....!..L!..This program must be run under Win32..\$7.....

File Icon

	
Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x40968c
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	da86ff6d22d7419ae7f10724a403dffd

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
add esp, FFFFFFFD4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-1Ch], eax
call 00007FB90D3609BFh
call 00007FB90D361C6Ah
call 00007FB90D363E5Dh
call 00007FB90D363EA4h
call 00007FB90D3663F3h
call 00007FB90D3664E2h
mov esi, 0040BDE0h
xor eax, eax
push ebp
push 00409D71h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 00409D27h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [0040B014h]
call 00007FB90D366E6Fh
call 00007FB90D366A2Eh
lea edx, dword ptr [ebp-10h]
xor eax, eax
call 00007FB90D364318h
mov edx, dword ptr [ebp-10h]
mov eax, 0040BDD4h
call 00007FB90D360A6Bh
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [0040BDD4h]
mov dl, 01h
mov eax, 004070C4h
call 00007FB90D36497Bh
mov dword ptr [0040BDD8h], eax
xor edx, edx
push ebp
push 00409D05h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
lea edx, dword ptr [ebp-18h]
mov eax, dword ptr [0040BDD8h]
call 00007FB90D364A53h
mov ebx, dword ptr [ebp-18h]
mov edx, 00000030h
mov eax, dword ptr [0040BDD8h]
call 00007FB90D364B8Dh
mov edx, esi
mov ecx, 0000000Ch

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc000	0x8c8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x263c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf000	0x0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xe000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x8e00	0x8e00	False	0.6218364876760564	data	6.600437911517656	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xa000	0x248	0x400	False	0.3115234375	data	2.7204325510923035	IMAGE_SCN_CNT_INITIALIZE D_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	0x8c8	0xa00	False	0.389453125	data	4.2507970587946735	IMAGE_SCN_CNT_INITIALIZE D_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_INITIALIZE D_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xf000	0x86c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x263c	0x2800	False	0.322265625	data	4.568719834340923	IMAGE_SCN_CNT_INITIALIZE D_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	English	United States
RT_ICON	0x10434	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	English	United States
RT_ICON	0x1099c	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_ICON	0x10c84	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	English	United States
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, SetEndOfFile, RemoveDirectoryA, ReadFile, IsDBCSLeadByte, GetWindowsDirectoryA, GetVersionExA, GetUserDefaultLangID, GetSystemInfo, GetSystemDefaultLCID, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetFileSize, GetFileAttributesA, GetExitCodeProcess, GetEnvironmentVariableA, GetCurrentProcess, GetCommandLineA, InterlockedExchange, FormatMessageA, DeleteFileA, CreateProcessA, CreateFileA, CreateDirectoryA, CloseHandle
user32.dll	TranslateMessage, SetWindowLongA, PeekMessageA, MsgWaitForMultipleObjects, MessageBoxA, LoadStringA, ExitWindowsEx, DispatchMessageA, DestroyWindow, CreateWindowExA, CallWindowProcA, CharPrevA
comctl32.dll	InitCommonControls
advapi32.dll	AdjustTokenPrivileges

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

Network Behavior				
TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:04:06.946058989 CET	49698	80	192.168.2.3	45.139.105.171
Nov 24, 2022 20:04:06.974109888 CET	80	49698	45.139.105.171	192.168.2.3
Nov 24, 2022 20:04:06.974369049 CET	49698	80	192.168.2.3	45.139.105.171
Nov 24, 2022 20:04:06.975188017 CET	49698	80	192.168.2.3	45.139.105.171
Nov 24, 2022 20:04:07.002732992 CET	80	49698	45.139.105.171	192.168.2.3
Nov 24, 2022 20:04:07.008284092 CET	80	49698	45.139.105.171	192.168.2.3
Nov 24, 2022 20:04:07.008407116 CET	49698	80	192.168.2.3	45.139.105.171
Nov 24, 2022 20:04:07.070561886 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.098324060 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.098479033 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.099627018 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.129308939 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.129746914 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.129908085 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.167032003 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.195297956 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195595026 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195625067 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195647955 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195672035 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195697069 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195724964 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195734978 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.195753098 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195776939 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.195781946 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195808887 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.195836067 CET	80	49699	107.182.129.235	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:04:07.195873022 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.195914030 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.223795891 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223831892 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223859072 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223885059 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223911047 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223913908 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.223938942 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223963976 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.223965883 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.223993063 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.224016905 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.224037886 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.224055052 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.224085093 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.224133015 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251636028 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251678944 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251702070 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251724005 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251743078 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251748085 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251773119 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251797915 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251797915 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251797915 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251820087 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251822948 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251847982 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251859903 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251873016 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251887083 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251902103 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.251909971 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251938105 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.251966000 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281215906 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281248093 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281270981 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281295061 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281317949 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281327963 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281347990 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281378031 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281383991 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281383991 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281399012 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281409979 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281419992 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281443119 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281457901 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281459093 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281481028 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.281492949 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281510115 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.281532049 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309762955 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309798956 CET	80	49699	107.182.129.235	192.168.2.3

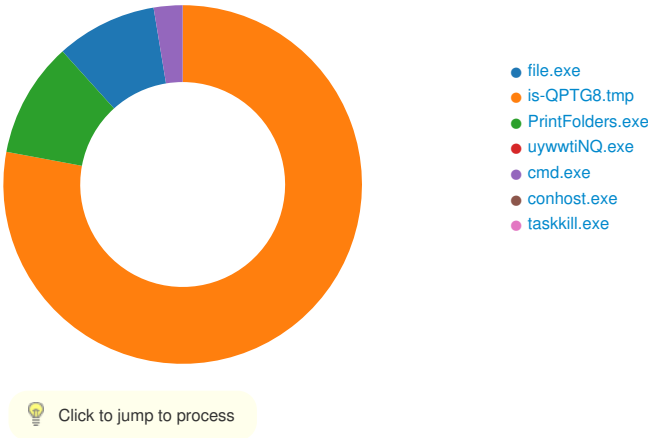
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:04:07.309824944 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309849977 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309875965 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309887886 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309889078 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309889078 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309900999 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309926033 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309950113 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309973001 CET	80	49699	107.182.129.235	192.168.2.3
Nov 24, 2022 20:04:07.309973001 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309973001 CET	49699	80	192.168.2.3	107.182.129.235
Nov 24, 2022 20:04:07.309973955 CET	49699	80	192.168.2.3	107.182.129.235

HTTP Request Dependency Graph

- 45.139.105.171
- 107.182.129.235
- 171.22.30.106

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 6084, Parent PID: 3452

General

Target ID:	0
Start time:	20:03:59
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	1488975 bytes
MD5 hash:	2ED741014B8CDAFD91A740432A3CFFA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: is-QPTG8.tmp PID: 6080, Parent PID: 6084

General	
Target ID:	1
Start time:	20:04:00
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp" /SL4 \$40228 "C:\Users\user\Desktop\file.exe" 1252960 51712
Imagebase:	0x400000
File size:	658944 bytes
MD5 hash:	85B94E72C3F2D2B5464E2AAF3C9E242A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	Detection: 4%, ReversingLabs
Reputation:	moderate

File Activities

File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\is-385TG.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	452163	CreateDirectoryA	
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetaup	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	471FF4	CreateDirectoryA	
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetaup_setup64.tmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	406F7E	CreateFileA	
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_isetaup_shfoldr.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	406F7E	CreateFileA	
C:\Users\user\AppData\Local\Temp\is-385TG.tmp_iscrypt.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	406F7E	CreateFileA	
C:\Program Files (x86)\PrintFolders	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4513C2	CreateDirectoryA	
C:\Program Files (x86)\PrintFolders\unins000.dat	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	46CA26	CreateFileA	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-385TG.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 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 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.\$!zJ^\$\$\$%"\$T87\$ ["\$\$\$Rich\$PEL\;# 4'	success or wait	1	406FC5	WriteFile
C:\Users\user\AppData\Local\Temp\is-385TG.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 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 50 45 00 00 4c 01 03 00 fd 62 fd 40 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 07 0a 00 02 00 00 00 04 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$WcWcWc>TcWb VcR<VcR? VcR9VcRichWcPELb@!	success or wait	1	406FC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\PrintFolders\is-60UNK.tmp	0	65536	49 54 53 46 03 00 00 00 60 00 00 00 01 00 00 00 fd fd fd fd 19 04 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 55 fd 01 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 0c 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 1f fd 00 08 2f 23 49 54 42 49 54 53 00 00	ITSF'["] {"xTUITSPtj].!TPMGL //#IDXHDR/#ITBITS	success or wait	2	450258	WriteFile
C:\Program Files (x86)\PrintFolders\is-5F7BS.tmp	0	5403	3d 0d 0a 20 48 69 73 74 6f 72 79 20 6f 66 20 52 65 6c 65 61 73 65 73 0d 0a 3d 0d 0a 0d 0a 4c 65 67 65 6e 64 0d 0a 2d 2d 2d 2d 2d 2d 0d 0a 5b 2b 5d 20 2d 20 61 64 64 65 64 0d 0a 5b 2a 5d 20 2d 20 6d 6f 64 69 66 69 65 64 0d 0a 5b 2d 5d 20 2d 20 62 75 67 20 66 69 78 65 64 0d 0a 0d 0a 0d 0a 56 65 72 73 69 6f 6e 20 32 2e 35 31 62 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 5b 2d 5d 20 54 68 65 20 6f 75 74 70 75 74 20 66 69 6c 65 20 70 61 74 68 20 77 61 73 6e 27 74 20 75 70 64 61 74 65 64 20 69 6e 20 63 65 72 74 61 69 6e 20 63 69 72 63 75 6d 73 74 61 6e 63 65 73 0d 0a 5b 2d 5d 20 41 64 64 65 64 20 74 68 65 20 77 6f 72 6b 61 72 6f 75 6e	===== == History of Releases===== =====Legend----- [+] - added[+] - modified[-] - bug fixedVersion 2.51b-- -----[-] The output file path wasn't updated in certain circumstances[-] Added the workaroun	success or wait	1	450258	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\PrintFolders\is-0E5GB.tmp	0	3391	50 52 49 4e 54 46 4f 4c 44 45 52 53 20 76 65 72 73 69 6f 6e 20 32 2e 35 31 62 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 32 30 30 39 2d 32 30 31 32 20 41 6e 64 72 65 79 20 50 69 76 6f 76 61 72 6f 76 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a 45 4e 44 20 55 53 45 52 20 4c 49 43 45 4e 53 45 20 41 47 52 45 45 4d 45 4e 54 0d 0a 0d 0a 54 68 69 73 20 6c 69 63 65 6e 73 65 20 64 65 73 63 72 69 62 65 73 20 74 68 65 20 63 6f 6e 64 69 74 69 6f 6e 73 20 75 6e 64 65 72 20 77 68 69 63 68 20 79 6f 75 20 6d 61 79 20 75 73 65 20 76 65 72 73 69 6f 6e 20 32 2e 35 31 62 20 6f 66 20 0d 0a 50 72 69 6e 74 46 6f 6c 64 65 72 73 20 28 22 74 68 65 20 70 72 6f 67 72 61 6d 22 29 2e 20 49 66 20 79 6f 75 20 61 72 65 20 75 6e 61 62 6c 65 20 6f 72	PRINTFOLDERS version 2.51bCopyright (C) 2009- 2012 Andrey Pivovarov. All rights reserved.END USER LICENSE AGREEMENTThis l icense describes the conditions under which you may use version 2.51b of PrintFolders ("th e program"). If you are unable or	success or wait	1	450258	WriteFile
C:\Program Files (x86)\PrintFolders\is-2632S.tmp	0	21504	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 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 75 8d fd 1b fd fd fd 1b fd fd fd 1b fd fd 35 fd fd fd 1b fd fd fd fd fd fd 1b fd fd 35 fd fd fd fd 1b fd 52 69 63 68 fd fd 1b fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 53 77 4f 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0a 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.\$u55RichPELSwO! P	success or wait	1	450258	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\PrintFolders\is-OK1CQ.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 40 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 7e 7f 63 00 00 00 00 00 00 00 00 fd 00 27 02 0b 01 02 05 00 fd 06 00 00 fd fd 00 00 00 00 00 30 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 60 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@! This program cannot be run in DOS mode.\$PELc'0@`	success or wait	31	450258	WriteFile
C:\Program Files (x86)\PrintFolders\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 7b 37 33 44 37 38 43 37 41 2d 37 38 46 32 2d 34 37 36 46 2d 38 36 46 46 2d 39 30 32 35 45 41 34 31 30 39 30 38 7d 7d 00 50 72 69 6e 74 46 6f 6c 64 65 72 73 00	Inno Setup Uninstall Log (b){73D78C7A-78F2-476F-86FF-9025EA410908}}PrintFolders	success or wait	2	450258	WriteFile
C:\Program Files (x86)\PrintFolders\unins000.dat	448	12	19 0d 00 00 fd fd fd fd 79 fd 8a	y	success or wait	2	450258	WriteFile
C:\Program Files (x86)\PrintFolders\PrintFolders.exe	0	1	4d	M	success or wait	1	4415CE	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp	unknown	4	success or wait	1	450148	ReadFile	
C:\Users\user\Desktop\file.exe	unknown	64	success or wait	1	450148	ReadFile	
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	450148	ReadFile	
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	450148	ReadFile	
C:\Users\user\AppData\Local\Temp\is-KU6HQ.tmp\is-QPTG8.tmp	unknown	65536	success or wait	11	450148	ReadFile	
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	5	450148	ReadFile	

Registry Activities

Key Created				
Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Atopoint Software	success or wait	1	42DD81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Atopoint Software\PrintFolders	success or wait	1	42DD81	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	success or wait	1	42DD81	RegCreateKeyExA

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Atopoint Software\PrintFolders	Language	unicode	eng	success or wait	1	46B611	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	Inno Setup: Setup Version	unicode	5.1.2-beta	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	Inno Setup: App Path	unicode	C:\Program Files (x86)\PrintFolders	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	InstallLocation	unicode	C:\Program Files (x86)\PrintFolders\	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	Inno Setup: Icon Group	unicode	PrintFolders	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	Inno Setup: User	unicode	hardz	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	DisplayName	unicode	PrintFolders 2.89	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	DisplayIcon	unicode	C:\Program Files (x86)\PrintFolders\PrintFolders.exe	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	UninstallString	unicode	"C:\Program Files (x86)\PrintFolders\unins000.exe"	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	QuietUninstallString	unicode	"C:\Program Files (x86)\PrintFolders\unins000.exe" /SILENT	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	DisplayVersion	unicode	2.89	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	Publisher	unicode	Atopoint Software	success or wait	1	4676A0	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	URLInfoAbout	unicode	http://www.atopoint.com	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	HelpLink	unicode	http://pfolders.atopoint.com	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	URLUpdateInfo	unicode	http://pfolders.atopoint.com	success or wait	1	4676A0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	NoModify	dword	1	success or wait	1	467700	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{73D78C7A-78F2-476F-86FF-9025EA410908}_is1	NoRepair	dword	1	success or wait	1	467700	RegSetValueExA

Analysis Process: PrintFolders.exe PID: 4532, Parent PID: 6080	
General	
Target ID:	2
Start time:	20:04:02
Start date:	24/11/2022
Path:	C:\Program Files (x86)\PrintFolders\PrintFolders.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\PrintFolders\PrintFolders.exe"
Imagebase:	0x400000
File size:	1990648 bytes
MD5 hash:	2ABBE052537A4C836AFE8DBAC888F131
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: 00000002.00000002.325696039.0000000001660000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000002.00000002.326103420.00000000033A0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000002.00000002.325006522.0000000000400000.00000040.00000001.01000000.00000006.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}\uywwtiNQ.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	42839A	CreateFileW	

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\uywwtiNQ.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 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 24 fd 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$..9.Rich	success or wait	1	421174	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\count[1].htm	0	1	30	0	success or wait	1	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEEXW4H4\ping[1].htm	0	17	55 77 55 6f 6f 6f 49 49 72 77 67 68 32 34 75 75 55	UwUooollrwgh24uuU	success or wait	1	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\fuckindll\ENCR[1].dll	0	1000	fd 67 0b 6d 69 fd 02 fd 7d 3b fd 18 fd 46 22 fd 29 fd 54 fd 11 27 4b 3b 1b fd fd fd 4f fd 59 30 3a fd fd fd fd 19 33 6a fd 5c 17 49 6a fd 32 52 49 50 17 fd 06 fd 43 07 19 fd 71 fd 7c fd 32 fd 0e fd fd fd 69 52 32 57 fd 46 2b 43 3d 4d 55 fd fd 16 cb fd fd 48 36 fd fd fd 41 fd 1a fd fd fd 40 7f fd 4f fd 63 1a fd fd 4d fd 78 38 94 fd fd 4c fd fd 2d 20 48 fd 62 fd fd 7c 12 43 fd fd a4 5a 7d fd 77 d4 2e fd 6c 1a 61 fd 61 54 fd fd a5 62 72 2c 19 fd 18 36 77 23 06 6a fd 50 4c 6c 69 fd 3d fd fd fd 1b 0e fd 6f fd 1e fd fd fd fd 53 fd 7b fd fd 52 fd fd fd fd 2e fd fd fd 35 60 15 fd fd 23 3b fd 14 fd 04 2d fd fd fd fd 62 2b 19 fd 47 28 fd 3e fd 02 51 05 fd fd fd fd 69 4e 7b fd 2b 79 0c 1d fd 5a 43	mij;F")T'K;OY0:3j\lj2RPCq 2iR2WFC=MUH6A@OcMx8L-b CZ}w.laaTbr,6w#jPlI=oS{R.5#;-b+G(>QiN{+yZC	success or wait	89	401BDA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\P SUEOSZZ\library[1].htm	0	1	30	0	success or wait	6	100010BA	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\library[1].htm	0	1	30	0	success or wait	5	100010BA	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: uywwtiNO.exe PID: 6120, Parent PID: 4532

General	
Target ID:	3
Start time:	20:04:06
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Roaming\{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}\uywwtiNQ.exe
Wow64 process (32bit):	true
Commandline:	

Imagebase:	0xbc0000
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: 46%, ReversingLabs
Reputation:	high

Analysis Process: cmd.exe PID: 1336, Parent PID: 4532

General

Target ID:	13
Start time:	20:04:39
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "PrintFolders.exe" /f & erase "C:\Program Files (x86)\PrintFolders\PrintFolders.exe" & exit
Imagebase:	0xbc0000
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)\PrintFolders\PrintFolders.exe	cannot delete	1	D0374	DeleteFileW
C:\Program Files (x86)\PrintFolders\PrintFolders.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: 1760, Parent PID: 1336

General

Target ID:	14
Start time:	20:04:39
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 3416, Parent PID: 1336

General

Target ID:	15
Start time:	20:04:39
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "PrintFolders.exe" /f
Imagebase:	0xd80000
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