ID: 552998
Sample Name: O53TFikPkp
Cookbook: default.jbs
Time: 03:36:24
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

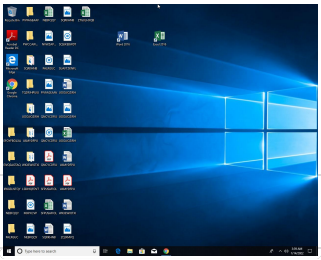
Windows Analysis Report O53TFikPkp

Overview

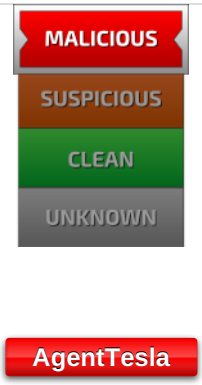
General Information

Sample Name:	O53TFikPkp (renamed file extension from none to exe)
Analysis ID:	552998
MD5:	be56d049ee926fb.
SHA1:	1fa7ea2d0e348b7.
SHA256:	626213dec6f5f7c..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



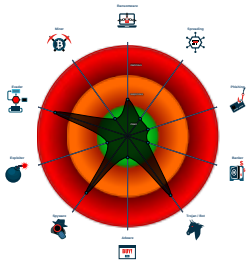
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for dropp…
- Detected unpacking (creates a PE fi…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Moves itself to temp directory
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- O53TFikPkp.exe (PID: 6712 cmdline: "C:\Users\user\Desktop\O53TFikPkp.exe" MD5: BE56D049EE926FBCCEC623695D12A5C6)
  - O53TFikPkp.exe (PID: 6892 cmdline: "C:\Users\user\Desktop\O53TFikPkp.exe" MD5: BE56D049EE926FBCCEC623695D12A5C6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "mailfilter247@yandex.com",
  "Password": "daddyhandsome@1234",
  "Host": "smtp.yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.665781318.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.665781318.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.924721394.000000000361000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.924721394.000000000361000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.923015296.000000000549000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.O53TFikPkp.exe.25e0000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.O53TFikPkp.exe.25e0000.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.1.O53TFikPkp.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.1.O53TFikPkp.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.O53TFikPkp.exe.415058.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 53 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

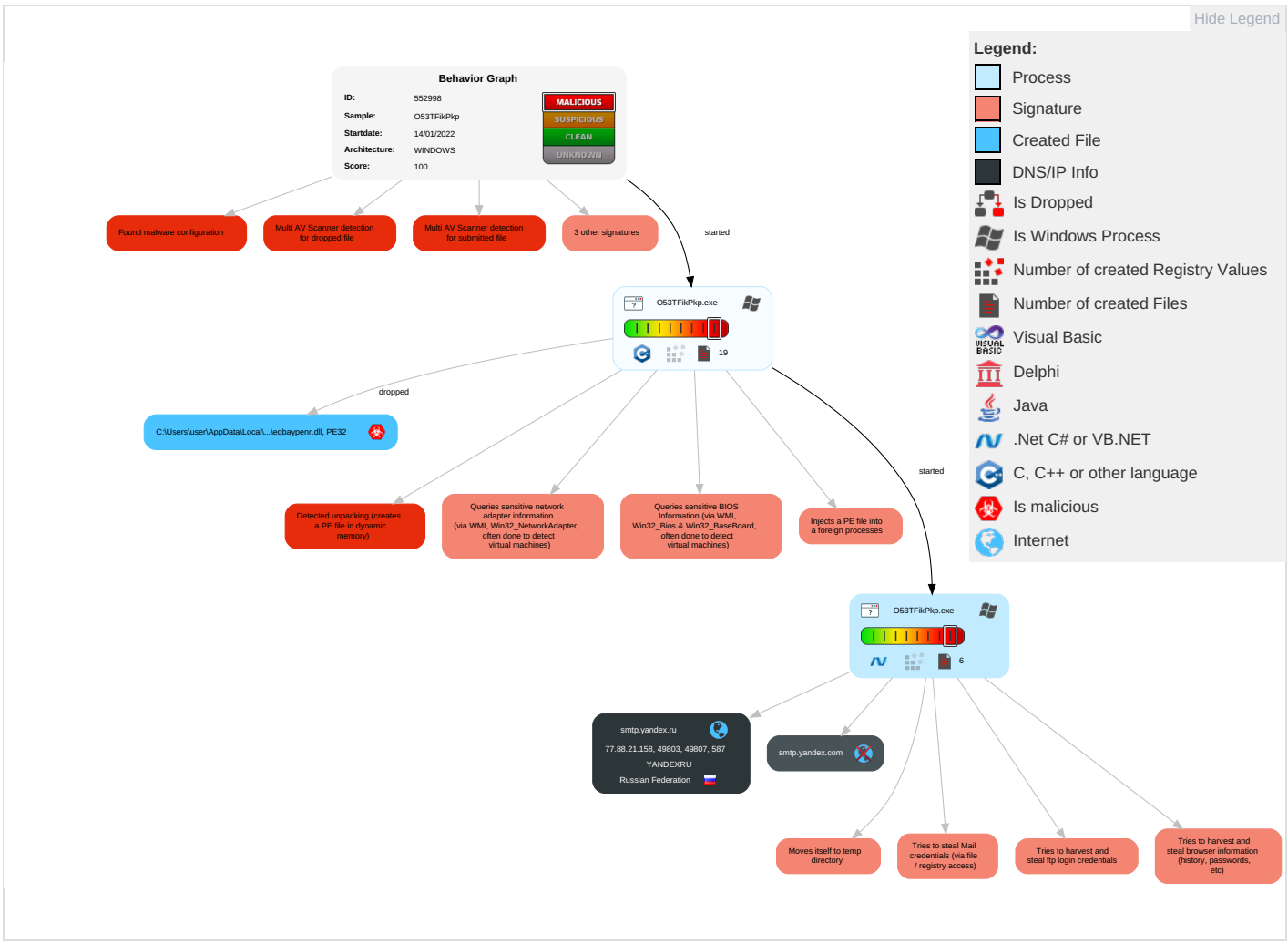
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 2 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Security Software Discovery 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
O53TFikPkp.exe	51%	Virustotal		Browse
O53TFikPkp.exe	53%	ReversingLabs	Win32.Worm.SpyBot	
O53TFikPkp.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsr28EF.tmp\eqbaypenr.dll	41%	ReversingLabs	Win32.Trojan.SpyNoon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.O53TFikPkp.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.O53TFikPkp.exe.4970000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.O53TFikPkp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.O53TFikPkp.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.O53TFikPkp.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.O53TFikPkp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.O53TFikPkp.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.O53TFikPkp.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.O53TFikPkp.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.O53TFikPkp.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://subca.ocsp-certu	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://UbQjJM.com	0%	Avira URL Cloud	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://https://bbTPeNUsMvT4JktW3MN.com	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://crl.certum	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552998
Start date:	14.01.2022
Start time:	03:36:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	O53TFikPkp (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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:	mal100.troj.spyw.evad.winEXE@3/5@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.1% (good quality ratio 14.2%) • Quality average: 80.2% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:37:30	API Interceptor	733x Sleep call for process: O53TFikPkp.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\di4dp15wu7r4o4e8	
Process:	C:\Users\user\Desktop\O53TFikPkp.exe
File Type:	data
Category:	dropped
Size (bytes):	292863

C:\Users\user\AppData\Local\Temp\di4dp15wu7r4o4e8	
Entropy (8bit):	7.960756321339627
Encrypted:	false
SSDEEP:	6144:nG5d30duZbuUYgGsFxZZLt2lGPSgQF5P+tauUASi2/WNhBR20fJtq:Gr3WuZbuUYXsF7dklTNv6N7Rvfe
MD5:	836F7E06923775EBB7DA041B320352E7
SHA1:	BAA947AC30331C0E38F17FD42E45D485E2BF1B93
SHA-256:	432EE7145FF38C9BA1538CD1B9A06B9C724623CEECF1EB55BDB32D2F5D3383D7
SHA-512:	92C969F43B9994CAC1F88FFF0E155A509D0D6B38F59AAD6F63BB23E0BC30901D8940B3B6A2ECDB15BDE8ECD91FB2FB09D4C1286E4950B808B5B3DB0DBF203 DD
Malicious:	false
Reputation:	low
Preview:	.0..Kg.K`..h...m.D....A.K.....C.....!.I.x..A.._.<)....*,c<..r..v..1.~.~..8H...\<...s.j..P.z.hy...r.i~MSw...P..:.5.....F{X.n...3+..!b...#0.)..!..]...J..2.e.L.!.V-.....2{'/...&[b(2....._...B.>..... {...E;6..i!..3:.G.]....'Z3U&c0s.L.7a...;...N}..sg.K...h..m}..]...A.K..q.9d.....D..!...x..A.-_..<).?....i<.u/....#~P69..f.#....+a-.@PS...1. .....?/..Da% ....{{X.Q&1.....Y.gU..<.N4..E. .B.6..\.to..n...+.+...S$...Zh...4".}.^$.....s..;...1r....}.....=,...FY..5Zi.....<<'...Q.k...;....QU.Rg.K.".h.n.mr...B.A.K.....C..'.....A..A.;_.s<).....Lc<../..J..7#.P+9..OI.D..!.a-%.PS/...0... a..^..?/....%..a!.a@X.i&1.....u.g.N<....=. .B.....n.....+..S.6...h..4".}.^$....s.J;...1r....}.....=,...F....i.....<<'...Q.k...;...N}..sg.K...h...mrD....A.K.....C.....!.I.x..A.._.<).....c<../..J..7#. P69..f.#...P.a- @PS..... ..a..^..?/..D.% ....F{X.Q&1.....].g..<....=. .B.6..\.to..n...+.+...S....h...4".}.^$.....s..;...1r....}.....=,...F.....i.

C:\Users\user\AppData\Local\Temp\nsr28EE.tmp	
Process:	C:\Users\user\Desktop\O53TFikPkp.exe
File Type:	data
Category:	dropped
Size (bytes):	326482
Entropy (8bit):	7.78664277552046
Encrypted:	false
SSDEEP:	6144:XCrqG5d30duZbuUYgGsFxZZLt2lGPSgQF5P+tauUASi2/WNhBR20fJt:SNr3WuZbuUYXsF7dklTNv6N7Rvf
MD5:	97A7BA9AF50642C7397AA0533D53206E
SHA1:	67B6E642A98AD4E8BE87568EC0D7D3B3581D2EAA
SHA-256:	DBFAC0266262C8ADB6BDB311E4FCC3EFC41DA69AE0F8E07DA261022AB80214D9
SHA-512:	CE1C41E77024A5DF6A01E7A1E0C9BB716354B51BAE874166159FB76ED9E4B3AD5E59859FB9E43DDBEBA34E192CD5F9A9D953332BE9539D39A8A3357F7F97A7 F6
Malicious:	false
Reputation:	low
Preview:	.\.....,.....&....F.....[.....s\..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsr28EF.tmp\eqbaypenr.dll	
Process:	C:\Users\user\Desktop\O53TFikPkp.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7803683556919934
Encrypted:	false
SSDEEP:	48:CnGI9I+Li4RxYtY8qxpnFbfGFN1RuqSd:iGyW4RxY2xpF49x
MD5:	24E8067B956182DDEE35AB317DE624C6
SHA1:	37E4431822CA95FD5B26248A36C39FDF9F6B7A9D
SHA-256:	BA259C3BF51AE2B5CEAF843DD2E5CAE3865ACBA2F5E81115FA6D3F4BB1D3F392
SHA-512:	31CE4162321577E54FC48BE48131305F361C2CCFFAB2B5542DAF88B6F1D3ED66C75ADBFA60E758462A450E5DC1D0CF883B3B868F52577087C69DABF1B1A0D6 2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L...3..a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text...O..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\okjdlpklcx	
Process:	C:\Users\user\Desktop\O53TFikPkp.exe
File Type:	data
Category:	dropped
Size (bytes):	5304
Entropy (8bit):	6.087454449151516
Encrypted:	false
SSDEEP:	96:g6P9SMp73nKbDsHM8u7ni6F4RI+3ZqYHRdML4O9xl12yq160N2D3PDz:g6P9NTnDs8ue6alhH3MkqYpJN2b

C:\Users\user\AppData\Local\Temp\okjdlpklcx	
MD5:	D3D435ACB4C52B21856675D898614EF0
SHA1:	498FA98468A240DDF040804A4F952517B27EAF3A
SHA-256:	7282D29AE2D2BBF420B65E435651A86778BD6F3170C34BBCE183D756FA7D4B31
SHA-512:	7E126163569E8921580B47D6015E324263737FE74E734398F15A4B4272A666E0DD0F8D116D08926ED31472098030FB189FDEB09EA5E998A50DC861EED57C7B96
Malicious:	false
Reputation:	low
Preview:	"/.....G.....8..8tF'8..8tF.....F._.....;..7.F.w.....F/..+..;..7.F.w.....F...3..;..7.F.w.4....F.....;..7.F.w.....F....7..Q...\...F;.F'..#.F7...T.F..~.F..~....T..7...F.....F.....F.....#.T.....c..... ./.....J....J...'.....7.?.;..?.{.g...../J..F.8..F.....Cc.d.....c>.....F....&..;....zz8..8tF..F...LF;.g.F....~7.s....C...F..F...G.~....F.....&..;..u.....]....s....(.....>.....A....._8.. 8tF..F.7....F/.F.....u.F.....F.G.F..F.?.F..#.s.....E.F....\...C>/..>+.F.....*..C>/..>+.....\...C./w...(.....w.....F..8.F.w....A....F.....F.....F.&.....G8..8tF..F._....F.F.....u.F..... F.G.F..F.?.F..#.....8.....F....\...C>..>.F;....*..C>..>.F7....*.C>..>.FsT...\...Cv.{v.F.....*..C>..>.....\...C..w.u...%...w.$....F...o....F..~o...p..o..s..7..;....P....F.....F.....F.&..s. ....k.F.7....F#.F.....u.F.....F.G.F..F.?.F..#.....E.F....\...C>#..>..F;....*..C>#..>.....\...C.#w.>...`...w.c....F..=..

C:\Users\user\AppData\Roaming\yf3kqygs.3ju\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\O53TFikPkp.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C 7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.937396375196458
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	O53TFikPkp.exe
File size:	271485
MD5:	be56d049ee926fbccec623695d12a5c6
SHA1:	1fa7ea2d0e348b7e1d79a7e6426e6f10376238e4
SHA256:	626213dec6f5f7c552974fc4d9fe954cb70b94f03588aa4550cd545789034167
SHA512:	571bf9c0c0ca1c70a71ff1c92bf8e0da04a27ee013097a770ad319165bab274f483adea5fc00dc78b4e1e88f10c3eb70eb64c338593360294cf4b8664eceb0f3
SSDEEP:	6144:owsJm3jpsSbMcpJxUNhZfbn5Svf7AkjdOFIP6:B3lTbvpJqNj5af7DjAFIi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 03:39:12.476604939 CET	192.168.2.4	8.8.8.8	0x95e0	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:12.521090031 CET	192.168.2.4	8.8.8.8	0xbd24	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:15.646847010 CET	192.168.2.4	8.8.8.8	0x9b97	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:15.674953938 CET	192.168.2.4	8.8.8.8	0x548e	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 03:39:12.493963957 CET	8.8.8.8	192.168.2.4	0x95e0	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:39:12.493963957 CET	8.8.8.8	192.168.2.4	0x95e0	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:12.540709019 CET	8.8.8.8	192.168.2.4	0xbd24	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:39:12.540709019 CET	8.8.8.8	192.168.2.4	0xbd24	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:15.666949987 CET	8.8.8.8	192.168.2.4	0x9b97	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:39:15.666949987 CET	8.8.8.8	192.168.2.4	0x9b97	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:15.695369959 CET	8.8.8.8	192.168.2.4	0x548e	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:39:15.695369959 CET	8.8.8.8	192.168.2.4	0x548e	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 03:39:12.969264984 CET	587	49803	77.88.21.158	192.168.2.4	220 vla5-047c0c0d12a6.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1642127952-QQ7GqpzHRI-dCPe5Bo9
Jan 14, 2022 03:39:12.969578981 CET	49803	587	192.168.2.4	77.88.21.158	EHLO 088753
Jan 14, 2022 03:39:13.031784058 CET	587	49803	77.88.21.158	192.168.2.4	250-vla5-047c0c0d12a6.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 14, 2022 03:39:13.032092094 CET	49803	587	192.168.2.4	77.88.21.158	STARTTLS
Jan 14, 2022 03:39:13.094244957 CET	587	49803	77.88.21.158	192.168.2.4	220 Go ahead
Jan 14, 2022 03:39:16.042094946 CET	587	49807	77.88.21.158	192.168.2.4	220 myt5-cceafa914410.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1642127956-YBrbW5xT92-dFPq8SOr
Jan 14, 2022 03:39:16.042336941 CET	49807	587	192.168.2.4	77.88.21.158	EHLO 088753

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 03:39:16.096930027 CET	587	49807	77.88.21.158	192.168.2.4	250-myt5-cceafa914410.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 14, 2022 03:39:16.097151041 CET	49807	587	192.168.2.4	77.88.21.158	STARTTLS
Jan 14, 2022 03:39:16.149956942 CET	587	49807	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: O53TFikPkp.exe PID: 6712 Parent PID: 5616

General

Start time:	03:37:17
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\O53TFikPkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\O53TFikPkp.exe"
Imagebase:	0x400000
File size:	271485 bytes
MD5 hash:	BE56D049EE926FBCCEC623695D12A5C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.667167111.00000000022B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.667167111.00000000022B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: O53TFikPkp.exe PID: 6892 Parent PID: 6712

General

Start time:	03:37:18
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\O53TFikPkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\O53TFikPkp.exe"
Imagebase:	0x400000
File size:	271485 bytes
MD5 hash:	BE56D049EE926FBCCEC623695D12A5C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.665781318.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.665781318.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.924721394.0000000003631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.924721394.0000000003631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.923015296.0000000000549000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.923015296.0000000000549000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.923951407.0000000002631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.923951407.0000000002631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.666315289.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000001.666315289.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.665066940.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.665066940.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.924840687.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.924840687.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.923912577.00000000025E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.923912577.00000000025E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.922818649.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.922818649.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis