ID: 830908
Sample Name: file.exe
Cookbook: default.jbs
Time: 19:42:10
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

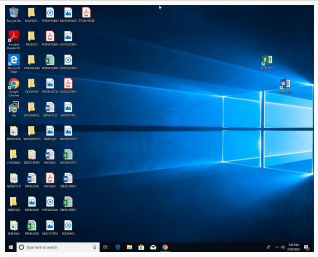
Windows Analysis Report

file.exe

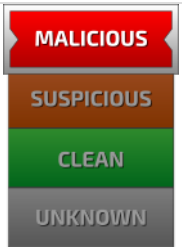
Overview

General Information

Sample Name:	file.exe
Analysis ID:	830908
MD5:	856572778608…
SHA1:	ef79e01019b95..
SHA256:	be316d90b0e5…
Tags:	exe
Infos:	



Detection



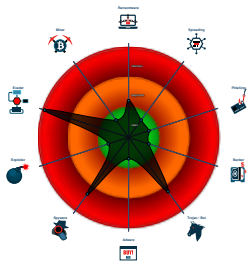
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected AgentTesla
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for drop…
- Detected unpacking (creates a PE f…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to harvest and steal Putty / W…
- Machine Learning detection for sam…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 1544 cmdline: C:\Users\user\Desktop\file.exe MD5: 8565727786082426567 95BD15CC3683C)
  - zjlxnt.exe (PID: 5320 cmdline: "C:\Users\user\AppData\Local\Temp\zjlxnt.exe" C:\Users\user\AppData\Local\Temp\anaictjg.cte MD5: A22E128E1C66E8E76F2F05CA2D81A8F1)
    - conhost.exe (PID: 4496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - zjlxnt.exe (PID: 6076 cmdline: C:\Users\user\AppData\Local\Temp\zjlxnt.exe MD5: A22E128E1C66E8E76F2F05CA2D81A8F1)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Host": "us2.smtp.mailhostbox.com",
  "Username": "log3@forrwel.net",
  "Password": "HNnNLPY3          "
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.575938781.0000000002391000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.575938781.0000000002391000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: zjlxnt.exe PID: 6076	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: zjlxnt.exe PID: 6076	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

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

Maps a DLL or memory area into another process

Stealing of Sensitive Information

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

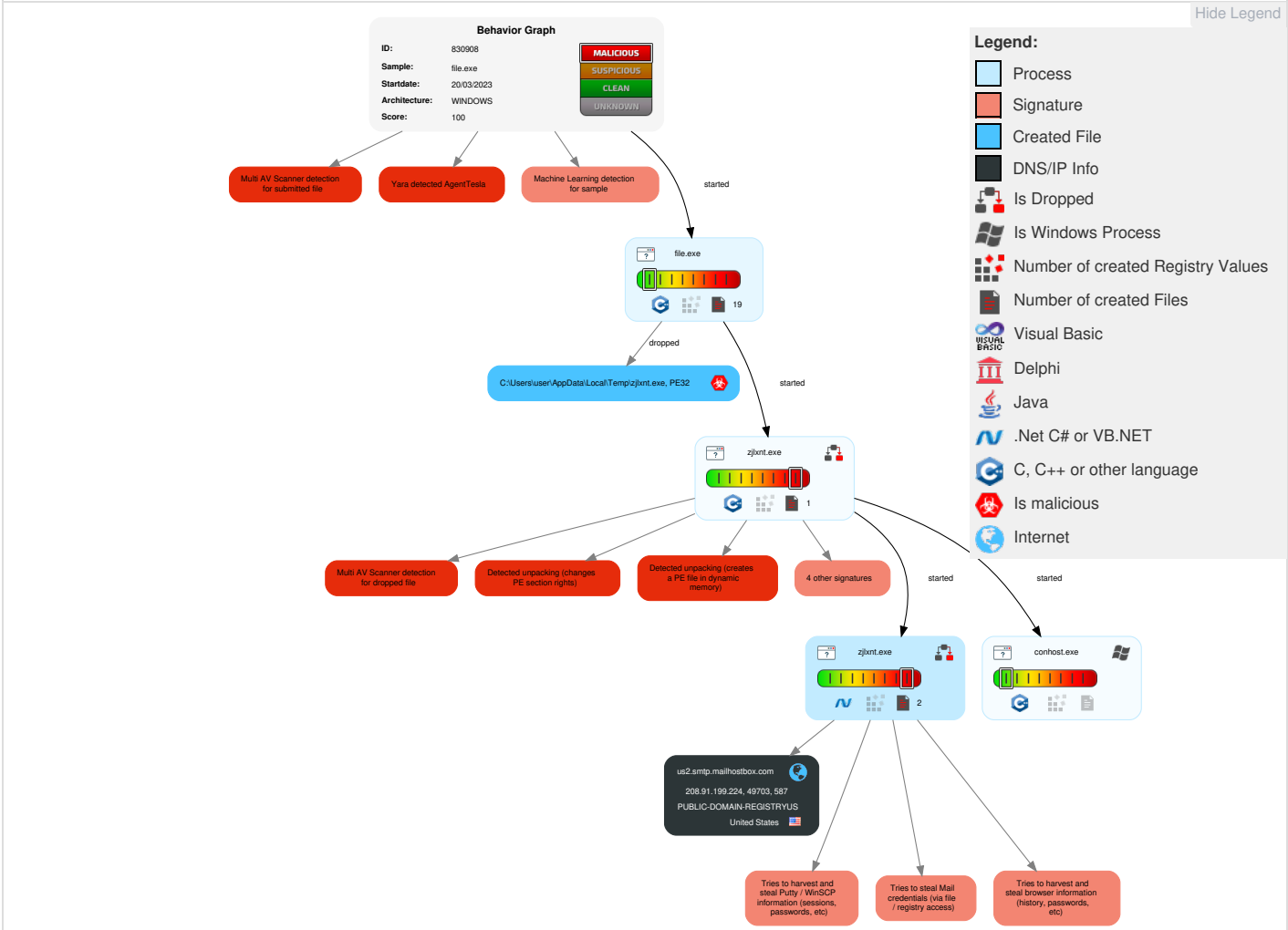
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Email Collection	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)	3 1 Software Packing	NTDS	1 2 7 System Information Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	2 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	49%	ReversingLabs	Win32.Trojan.Nemesis	
file.exe	48%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\zjlxnt.exe	42%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\zjlxnt.exe	35%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.zjlxnt.exe.4800000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.zjlxnt.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo?	0%	Avira URL Cloud	safe	
http://crl.usertru	0%	Avira URL Cloud	safe	

Domains and IPs

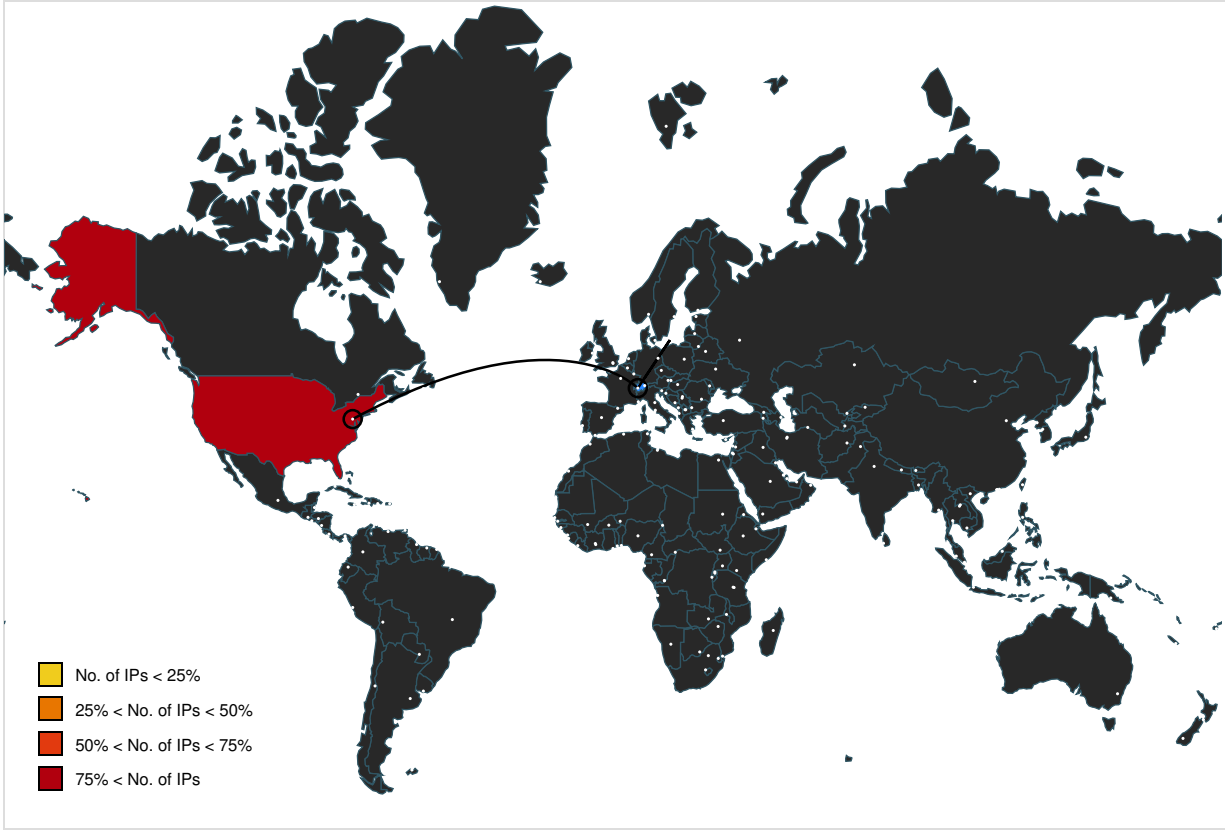
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	zjlxnt.exe, 00000003.00000002.575938781.00000000023E9000.00000004.00000800.00020000.00000000.sdmp, zjlxnt.exe, 00000003.00000002.577003560.0000000005458000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0A	zjlxnt.exe, 00000003.00000002.575938781.00000000023E9000.00000004.00000800.00020000.00000000.sdmp, zjlxnt.exe, 00000003.00000002.577003560.0000000005458000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	zjlxnt.exe, 00000003.00000002.575938781.00000000023E9000.00000004.00000800.00020000.00000000.sdmp, zjlxnt.exe, 00000003.00000002.577003560.0000000005458000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	file.exe	false		high
http://us2.smtp.mailhostbox.com	zjlxnt.exe, 00000003.00000002.575938781.00000000023E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crt.sectigo?	zjlxnt.exe, 00000003.00000002.577003560.0000000005458000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.usertru	zjlxnt.exe, 00000003.00000002.577003560.0000000005458000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830908
Start date and time:	2023-03-20 19:42:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/4@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.4% (good quality ratio 19%) • Quality average: 79.3% • Quality standard deviation: 29.7%

HCA Information:	• Successful, ratio: 100% • 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, WMIADAP.exe, conhost.exe
- 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 NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:43:17	API Interceptor	30x Sleep call for process: zjlxnt.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:\Users\user\AppData\Local\Temp\anaictjg.cte

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	6061
Entropy (8bit):	7.152729915217053
Encrypted:	false
SSDEEP:	96:Farc6oYBg/DrYuvk2XO5oSwsnP+ZjVe9LWKdUdAAU0HJsUV7scbvbz4LUtnnIgAf:FarcRZ3hX1ShnP2jE9LXdEAARpP1rbvy
MD5:	8009F662B5AB8050A4F5AEEAE94BA722
SHA1:	FE55E206DB001BF178AD87DF2BC4A6A899482D2A
SHA-256:	3A5D1645A4DAB4AEF75FA65EC4B7585917C1527C0B913287179168B5EF18147A
SHA-512:	6CB0A5BBE859263A2D97745F06AC33952C783314F6B49B7CD387B4276C947BD51EF9ADE02CEC2F0D5E38561B9895CF6DB1262F2790E1530A9FCC33879C139E2

Malicious:	false
Reputation:	low
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.:,q%..5M%.}.:,qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	381886
Entropy (8bit):	7.672264691913513
Encrypted:	false
SSDEEP:	6144:Ntm1Z1J8zN5MoAqIIGXyCk4642/VGan7ZhhlqbK88SII5NX1GKGsGZExocCp:NI1ix5lAmxd4P27VKlGNX1GKGsHG
MD5:	BD05EB6029978E8A69332B07B4334349
SHA1:	990D883D1827493EB50825719F585D1ABC1113FB
SHA-256:	02D5CDB8D67E1003EA4A6134F8C935F7EABAEF5761AB25362353400F7892483A
SHA-512:	E6DB920547761D9E66448305DFE1984AE553DDC4DD52C50526854146C2E052604A11F4A048EA03CABB257900A1175B681AE300EA653B2D463B7CCBE026D95A1
Malicious:	false
Reputation:	low
Preview:	.+.....,.....n.....+.....+.....+.....F..... ....

C:\Users\user\AppData\Local\Temp\pqknsgems.bq

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	268841
Entropy (8bit):	7.971116927383392
Encrypted:	false
SSDEEP:	6144:Stm1Z1J8zN5MoAqIIGXyCk4642/VGan7ZhhlqbK88SII5NF:SI1ix5lAmxd4P27VKlGNF
MD5:	3D14489C8EE3D764649F70D1A27542F9
SHA1:	59E98B00E554B4E30DEF17AEBF731571F88CBFCE
SHA-256:	0645F4AF22D167E907F2C7CEA114D05CB45CF3CE639CECD67E66DE9D0E190701
SHA-512:	65457B732E118EFA58971F670D3E6D335983914603BA84F0C774786A777C5778BD3506C76393585E55B6D7790167E2A5DECC745015452BF229FC38ED71126076
Malicious:	false
Reputation:	low
Preview:	R.".z.....D....1....f..%.J..,.L.M.@..-.....FU.h:..:....0.(H.TU%e...dhh.A....^F'...h.U.....q+B....NY:...f..S. ...O..'I.7.5...|..T.R.WWI5Px....mVE..10VZ.....9,._.H.A9@-.7..z.>.. zg.K.2....c0...fM..?n....):Bipo..wsH.3#.(],.....%.I..<..z.u"..T...<..,.....v...._f...._...v...@..]-....^.U.h...:..'..()...%...(",...9k...2...@.s...F...V ..h.m...M.W.....8O...I.7i.v..G.....HX,.o _.&...._...n..m..0.....}..2..4I....a.F.....N.,"$@s~0.....o.....`%<....(.h.bD.....Ma-s....D...<..z..{_.u.....H..1...._f..%.J...,L.M.....H.U.h...:V..'..()...%....",,...W..FF\.....^.....J y..h$m...M.W..eq.R..R$/I.7.;..C....6.\..X,.4_..F..._...V..m..0.....}..E..I....a.F.....N.,"$@s~0...QLc.]...`%<....(.2.bW.....Ma-s....D...<..z.u"..T...4.....H..1...._f..%.J..,.L.M.@..-.. ...FU.h:..:...'..()...%....",,..9....2...@....gF....V ..h$m...M.W...q..8O..'I.7i.v..G...y>.\.HX,.4_..F..._...n..m..0.....}..E..I....a.F.....N.,"$@s~0...QLc.]...`%<....(.2.bW...

C:\Users\user\AppData\Local\Temp\zjlxnt.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	6.226201646790148
Encrypted:	false
SSDEEP:	1536:+0ZlV4KXc4OxQEsGZDmS+jtBaK/eRuZocSZUpxwkyBp+NnFsSW81kxgsWJjcdvwk:Ld4KALsGZDN+x/yuZocSTkyBw9y8eASd
MD5:	A22E128E1C66E8E76F2F05CA2D81A8F1
SHA1:	589A59B124FACC5A045FA99B334E476415E57CA2
SHA-256:	EE05F69606802B01D1FA5BB8BC43885F7F5F66C53893DE380F9026CD3AFAA79D
SHA-512:	C646ED13AA87FC2345AAE5AC640CD6E3A4B46B780045C86F4A384F4AFFD7E9FD510D7F50ECF2AFBFB12F34734997077E4DC7DC46B1222A8EDE0D0D793F774 8B
Malicious:	**true**

Antivirus:	• Antivirus: ReversingLabs, Detection: 42% • Antivirus: Virustotal, Detection: 35%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7...s...s...s...8...y...8.....8...g.....U.....b.....`...8...j...s.....r.....r.. .Richs.....PE..L...V..d.....!....|.....".....@.....|k.....^.....]..@..... .....text..... ..`.rdata...f.....h.....@..@.data...l.....l.....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.932397161868976
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	316557
MD5:	8565727786082426567 95bd15cc3683c
SHA1:	ef79e01019b9518fa82e8dc628d416cd9ccd7817
SHA256:	be316d90b0e5c1f88f32fa6dc7cf5b2c760c8ea63e7ddec3e2303cccf8ae25f9
SHA512:	df6e4621f566ba7f067e44f87fec3b0f7350a45b71d8401e3c1eeae0c82b24594bdc54e68787e61fd53193afbc31a85c0f5c90accf606fddf0fa59f6b591f077
SSDEEP:	6144:vYa6mUhRSVGVVj8vjpxMegWObBb3vztdsPTtH2vkcikg5JjzPw4312:vYYC0VGHWjpxTgDbBdebl2vkciksA
TLSH:	B964122427E4C593C4E342317C3A9AE5A8F9FA2B1560E70F276033587935AA1E70E323
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F413CC5844Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F413CC5841Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xcd8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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
.text	0x1000	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0xcd8	0xe00	False	0.4224330357142857	data	4.220947409031048	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b1d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x3b4c0	0x100	data	English	United States
RT_DIALOG	0x3b5c0	0x11c	data	English	United States
RT_DIALOG	0x3b6e0	0x60	data	English	United States
RT_GROUP_ICON	0x3b740	0x14	data	English	United States
RT_VERSION	0x3b758	0x23c	data	English	United States
RT_MANIFEST	0x3b998	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu

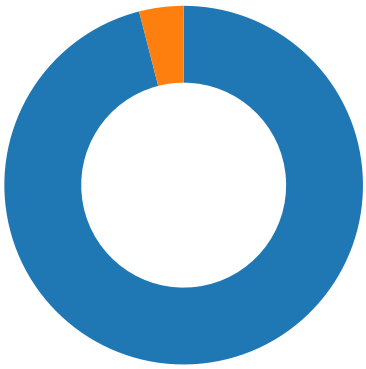
DLL	Import
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 25

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 19:43:18.322552919 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:18.508263111 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:18.508500099 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.077830076 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.079662085 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.264877081 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.265360117 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.265678883 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.451806068 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.501507044 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.687264919 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.687323093 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.687382936 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.687422037 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.687428951 CET	49703	587	192.168.2.5	208.91.199.224

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 19:43:19.687489986 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.690313101 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.872652054 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:19.872816086 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:19.936322927 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:20.122263908 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:20.190968990 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:20.376351118 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:20.377393007 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:20.566237926 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:20.566880941 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:20.757528067 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:20.757951021 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:20.946297884 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:20.947021961 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.157416105 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:21.157855034 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.344383001 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:21.346679926 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.346805096 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.346874952 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.346931934 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:21.532103062 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:21.532279968 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:21.666341066 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:21.906209946 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:43:22.080671072 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:43:22.080802917 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:44:58.259578943 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:44:58.445679903 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:44:58.446547985 CET	587	49703	208.91.199.224	192.168.2.5
Mar 20, 2023 19:44:58.446655989 CET	49703	587	192.168.2.5	208.91.199.224
Mar 20, 2023 19:44:58.459429979 CET	49703	587	192.168.2.5	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 19:43:18.274879932 CET	61893	53	192.168.2.5	8.8.8.8
Mar 20, 2023 19:43:18.297280073 CET	53	61893	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 19:43:18.274879932 CET	192.168.2.5	8.8.8.8	0x9af3	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)	false

DNS Answers

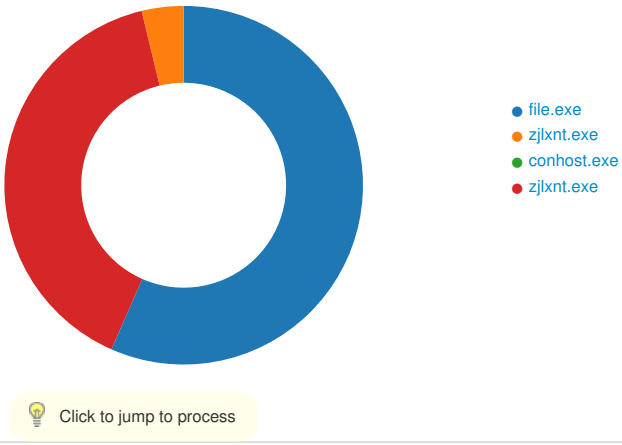
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 19:43:18.297280073 CET	8.8.8.8	192.168.2.5	0x9af3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 19:43:18.297280073 CET	8.8.8.8	192.168.2.5	0x9af3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 19:43:18.297280073 CET	8.8.8.8	192.168.2.5	0x9af3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 19:43:18.297280073 CET	8.8.8.8	192.168.2.5	0x9af3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 19:43:19.077830076 CET	587	49703	208.91.199.224	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 19:43:19.079662085 CET	49703	587	192.168.2.5	208.91.199.224	EHLO 035347
Mar 20, 2023 19:43:19.265360117 CET	587	49703	208.91.199.224	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 19:43:19.265678883 CET	49703	587	192.168.2.5	208.91.199.224	STARTTLS
Mar 20, 2023 19:43:19.451806068 CET	587	49703	208.91.199.224	192.168.2.5	220 2.0.0 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **1544**, Parent PID: **3324**

General

Target ID:	0
Start time:	19:43:07
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	316557 bytes
MD5 hash:	856572778608242656795BD15CC3683C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsi8BD6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsd8C07.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsd8C07.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	405BE2	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\pqknsgems.bq	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\anaictjg.cte	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\zjlxnt.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi8BD6.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsd8C07.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	0	26276	fd 2b 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 6e 00 00 00 fd 1d 00 00 00 00 00 00 0e 2b 00 00 01 00 00 00 fd 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	+,n+++	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\pqknsgems.bq	0	16384	52 12 22 fd 7a fd fd fd 76 fd fd fd 44 fd de 7f fd 31 00 fd 02 fd fd 66 03 fd 25 fd 4a fd fd 2c fd 4c fd 4d fd 40 fd fd 2d fd 2e fd 04 fd 46 55 fd 68 3a fd fd 3a 03 1b fd fd 30 fd 28 48 fd 54 55 25 65 13 fd fd 64 68 68 fd 41 fd fd 00 00 5e 46 27 fd fd fd 68 1a 55 fd fd fd fd fd 16 71 2b 42 0a 08 12 fd 4e 59 3a fd fd fd 66 1d fd 53 fd 20 16 fd fd 4f fd 1a 27 49 fd 37 08 35 fd fd e5 7c fd fd 54 fd 52 fd 57 57 49 35 50 78 fd fd 1c 01 6d 56 45 fd fd 31 30 56 5a fd fd fd fd fd 39 2c 0f 5f fd 48 fd 41 39 40 2d fd 37 fd 1c 7a fd 3e 7f fd 7a 67 5a 4b fd 32 fd fd cd fd 63 30 08 0f fd 66 4d 0b fd 3f 6e fd 30 b6 fd 29 3a 42 69 70 6f 08 fd 77 73 48 fd 33 23 fd 28 5d 2c fd fd fd 18 fd fd fd 91 25 fd 6c fd fd 3c fd 0a 7a	R"zD1f%J,LM@-.FUh::0(HTU%edhhA^F'hUq+BNY:fSO'I75|TRWWI5PxmVE10VZ9,_HA9@-7z>zgK2c0fM?n):BipowsH3#(],%l<z	success or wait	17	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\anaictjg.cte	0	6061	c6 30 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	005mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\zjlxnt.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 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 37 fd fd fd 73 fd fd fd 73 fd fd fd 73 fd fd fd 38 fd fd fd 79 fd fd fd 38 fd fd fd fd fd fd 38 fd fd fd 67 fd fd fd fd fd 55 fd fd fd fd fd 62 fd fd fd fd fd 60 fd fd fd 38 fd fd fd 6a fd fd fd 73 fd fd fd fd fd fd fd fd fd fd 72 fd fd fd fd fd fd 72 fd fd fd 52 69 63 68 73 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 56 fd 17 64 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7sss8y88gUb`8j srrRichsPELVd	success or wait	6	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	unknown	512	success or wait	75	4061F5	ReadFile
C:\Users\user\Desktop\file.exe	unknown	16384	success or wait	18	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	unknown	11224	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsi8BD7.tmp	unknown	16384	success or wait	24	4061F5	ReadFile

Analysis Process: zjlxnt.exe PID: **5320**, Parent PID: **1544**

General

Target ID:	1
Start time:	19:43:08
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\zjlxnt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\zjlxnt.exe" C:\Users\user\AppData\Local\Temp\anaictjg.cte

Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	A22E128E1C66E8E76F2F05CA2D81A8F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 42%, ReversingLabs • Detection: 35%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\anaictjg.cte	unknown	4096	success or wait	1	407824	ReadFile
C:\Users\user\AppData\Local\Temp\anaictjg.cte	unknown	4096	success or wait	1	407824	ReadFile

Analysis Process: conhost.exe PID: 4496, Parent PID: 5320

General

Target ID:	2
Start time:	19:43:08
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: zjlxnt.exe PID: 6076, Parent PID: 5320

General

Target ID:	3
Start time:	19:43:09
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\zjlxnt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\zjlxnt.exe
Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	A22E128E1C66E8E76F2F05CA2D81A8F1
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: 00000003.00000002.575938781.0000000002391000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.575938781.0000000002391000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7226CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7226CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7224CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\5e83f775-9011-4959-a70e-e42b96ed319f	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\5e83f775-9011-4959-a70e-e42b96ed319f	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	71071B4F	ReadFile

Disassembly

No disassembly