ID: 764029
Sample Name: file.exe
Cookbook: default.jbs
Time: 10:31:05
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

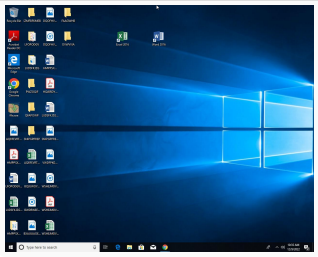
Windows Analysis Report

file.exe

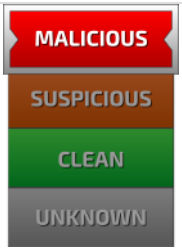
Overview

General Information

Sample Name:	file.exe
Analysis ID:	764029
MD5:	2396925cc38be4..
SHA1:	8884e5383b3601..
SHA256:	e91bb1f7c2b2ffd..
Tags:	exe
Infos:	



Detection



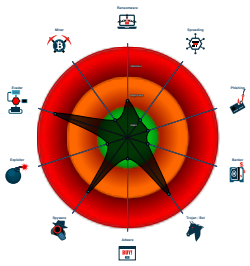
Amadey

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

Signatures

- Yara detected Amadeys stealer DLL
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Amadey bot
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Machine Learning detection for sam…
- Contains functionality to inject code…
- Creates an undocumented autostart…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3520 cmdline: C:\Users\user\Desktop\file.exe MD5: 2396925CC38BE4F07BD426CF080256CE)
  - gntuud.exe (PID: 2016 cmdline: "C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe" MD5: 2396925CC38BE4F07BD426CF080256CE)
    - schtasks.exe (PID: 5144 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gntuud.exe (PID: 5292 cmdline: C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe MD5: 2396925CC38BE4F07BD426CF080256CE)
- **cleanup**

Malware Configuration

Threatname: Amadey

```
{
  "C2 url": "77.73.133.72/hfk3vK9/index.php",
  "Version": "3.50"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	INDICATOR_TOOL_PWS_Amady	Detects password stealer DLL. Dropped by Amadey	ditekSHen	• 0xd868:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15604:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x16074:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15158:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0x151bc:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0xdd0c:$s3: \Mikrotik\Winbox\Addresses.cdb • 0x190d8:$s4: \HostName • 0x19100:$s5: \Password • 0x17c04:$s6: SOFTWARE\RealVNC\ • 0x17c30:$s6: SOFTWARE\RealVNC\ • 0x17c5c:$s6: SOFTWARE\RealVNC\ • 0x17ca4:$s6: SOFTWARE\RealVNC\ • 0x17cd0:$s6: SOFTWARE\RealVNC\ • 0x18008:$s7: SOFTWARE\TightVNC\ • 0x18034:$s7: SOFTWARE\TightVNC\ • 0x18060:$s7: SOFTWARE\TightVNC\ • 0x180ac:$s7: SOFTWARE\TightVNC\ • 0x1c43c:$s8: cred.dll

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.259666135.00000000005D3000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1640:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000003.293480849.00000000007CB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000001.00000003.271178795.0000000000680000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000000.00000002.259530025.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000004.00000003.312159954.0000000000940000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.gntuud.exe.400000.0.raw.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
4.2.gntuud.exe.6e0e67.1.raw.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
4.3.gntuud.exe.940000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.2.file.exe.900e67.1.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.2.file.exe.400000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
Click to see the 9 entries				

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 domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Yara detected Amadey bot

Boot Survival

Creates an undocumented autostart registry key

Uses schtasks.exe or at.exe to add and modify task schedules

HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

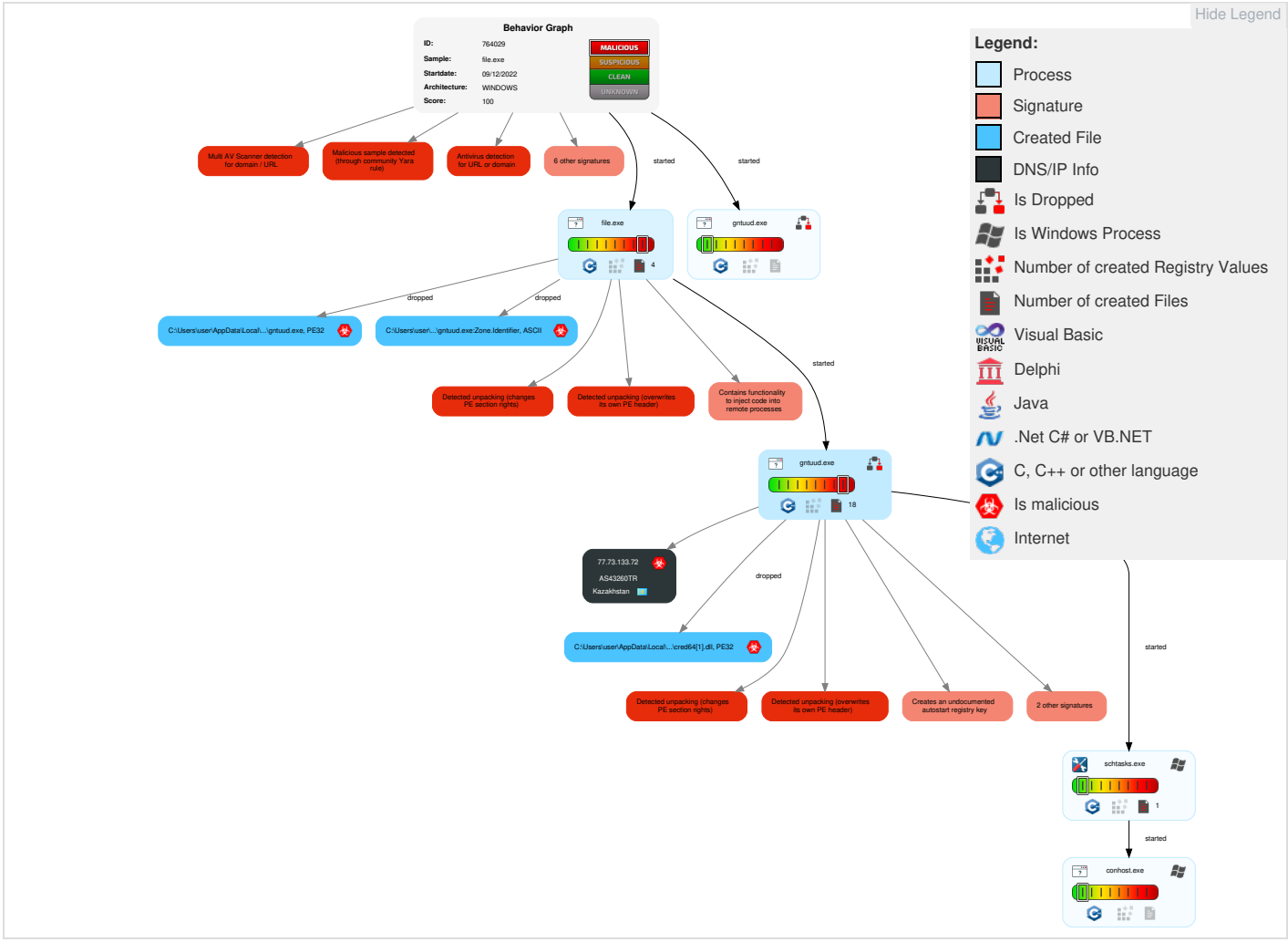
Yara detected Amadeys stealer DLL

Yara detected Amadey bot

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 Scheduled Task/Job	1 Scheduled Task/Job	1 Exploitation for Privilege Escalation	1 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	1 1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated 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	2 Software Packing	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	Compile After Delivery	DCSync	2 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 4 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

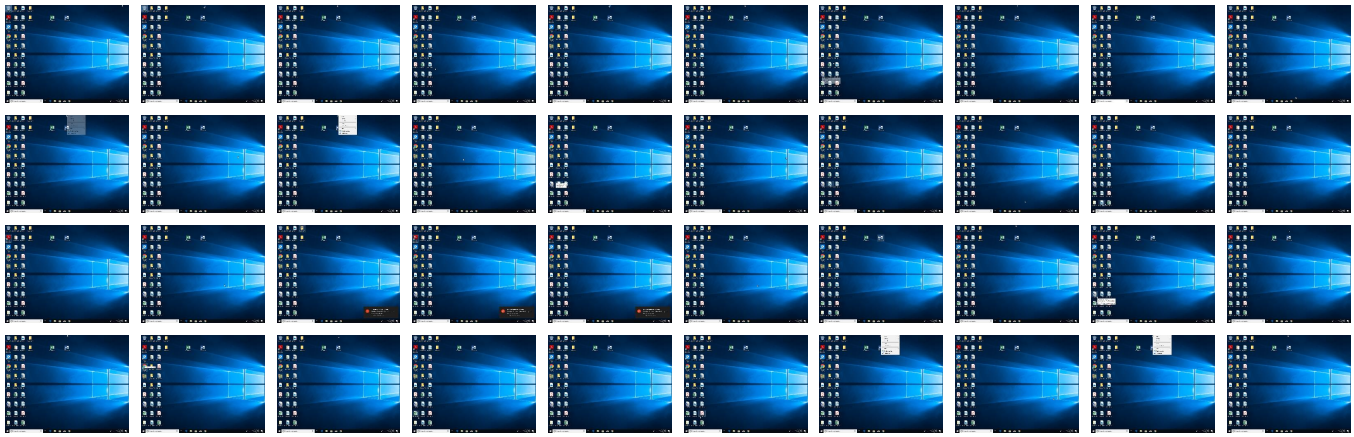
Behavior Graph



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

Source	Detection	Scanner	Label	Link
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	88%	ReversingLabs	Win32.Infostealer.Decred	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
77.73.133.72/hfk3vK9/index.php	0%	URL Reputation	safe	
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll_	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll=	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll	19%	Virustotal		Browse
http://77.73.133.72/hfk3vK9/index.php	10%	Virustotal		Browse
http://77.73.133.72/hfk3vK9/index.php	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/index.php8	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll)	100%	Avira URL Cloud	malware	
http://77.73.133.72/hfk3vK9/index.phpplay	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

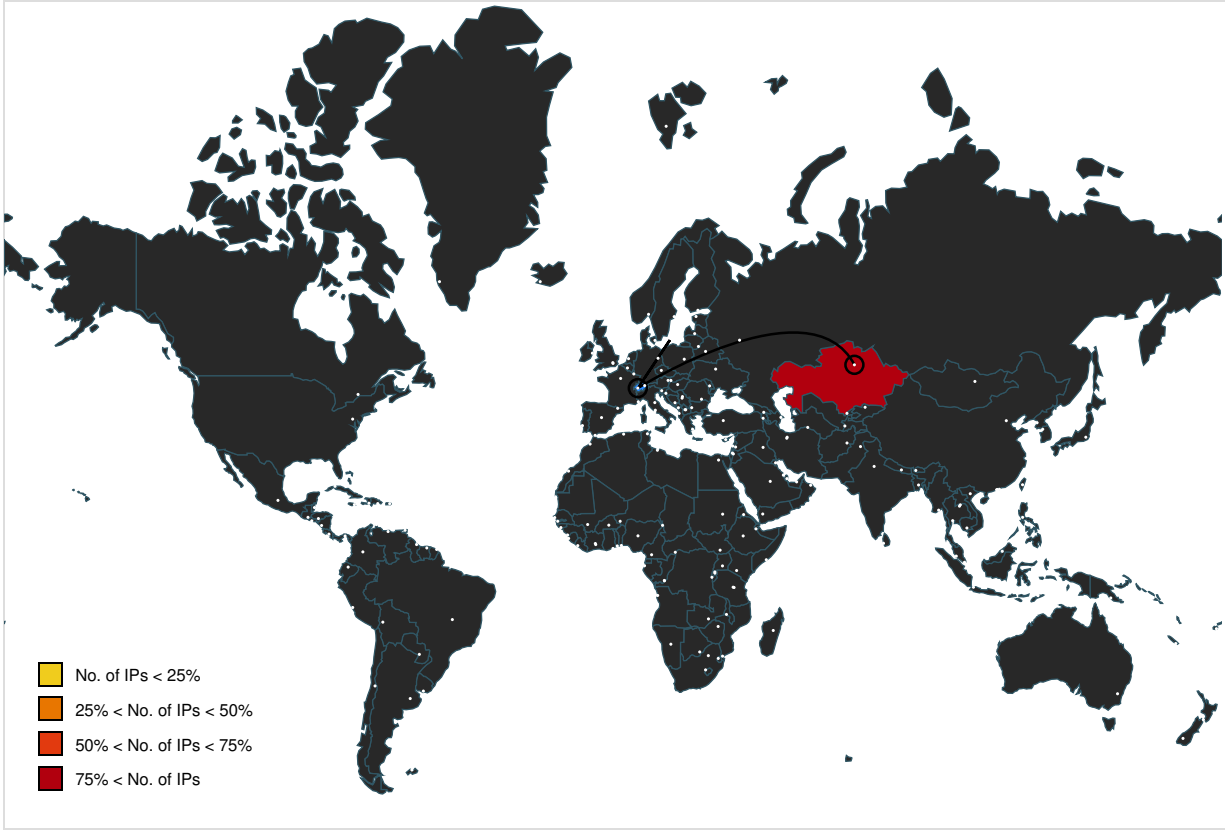
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
77.73.133.72/hfk3vK9/index.php	true	• URL Reputation: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll_	gntuud.exe, 00000001.00000003.293433328.00000000007AF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll	gntuud.exe, 00000001.00000003.293294453.000000000079B000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000001.00000003.293433328.00000000007AF000.00000004.00000020.00020000.00000000.sdmp	false	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll=	gntuud.exe, 00000001.00000003.293294453.000000000079B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/index.php	gntuud.exe, 00000001.00000003.293349447.00000000007A7000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000001.00000003.293294453.000000000079B000.00000004.00000020.00020000.00000000.sdmp	false	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/index.php8	gntuud.exe, 00000001.00000003.293294453.000000000079B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/Plugins/cred64.dll)	gntuud.exe, 00000001.00000003.293433328.00000000007AF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://77.73.133.72/hfk3vK9/index.phpplay	gntuud.exe, 00000001.00000003.293294453.000000000079B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.73.133.72	unknown	Kazakhstan		43260	AS43260TR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764029
Start date and time:	2022-12-09 10:31:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
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:	19
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@7/4@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.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 NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:32:10	API Interceptor	2664x Sleep call for process: gntuud.exe modified
10:32:12	Task Scheduler	Run new task: gntuud.exe path: C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe

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\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.512109370826634
Encrypted:	false
SSDEEP:	3072:ox7pOYzBekTRmWDWCMq6As523HeS9FAiZ87vO2rlL3RnG9:ox7ZNhTR/dMq6AO0a7vVIT
MD5:	349B2B47FEF50FA6A1FC19D0EE4B2DB8
SHA1:	077F4328B3F060A9F010B1A63D9E127D24DDAFD4
SHA-256:	5CD41F164DE6F783B7DA82B5F6DBD49413ECCD87CC7470F2004D58CA081FB0E0

SHA-512:	83FD58BE4C0051ED05B7A03443D256D52F09206D2F433BD302C9E9E3780B9D472E823AED1DB01B5052DC8FDC63A4352BEAC9E399858A8252C057F11CF2BD173
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Reputation:	moderate, very likely benign file
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....x.....@.....@.....O.....&.... ....CODE..... ..`DATA.....@...BSS.....idata..&.....@....edata..O.....@..P.reloc .....@..P.rsrc..... .....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Temp\853321935212	
Process:	C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	95068
Entropy (8bit):	7.918851174293143
Encrypted:	false
SSDEEP:	1536:CmbM4iTkYMKsGHObkbXmBRn052EGdH/LaAD5Y9xe4dHEdI2uhiVxp669M6bpt:hiI5GubLR+GhWr7bddpKhN
MD5:	6F8C496BA629E10E2BBF21C5BB00EA7B
SHA1:	3C6C25B7C07632F85DF4E651F68FB849852D354A
SHA-256:	00012D0BE6FC61DFF5851A32B162F2FDBBD13E1289213DEF91DCD25AF1C57B4B
SHA-512:	58F718FCB6A4D3B53024B9CC00502641259825705562472FDA199C8856C9EB5C258072AC616C06F5849BDA077B0F5B88F4EBDD2638AF179627D4AC623F7AEE06
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/I.1./...C...W.....,1....R.0.W.M.!.I7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....I.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe	
Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	430592
Entropy (8bit):	6.163540154379331
Encrypted:	false
SSDEEP:	6144:YecLXGqxxoij2Fjzp5/bCgXhh6K9W9n6ded89kTt:Y1LGq3NA5/bvIK9W9nbac
MD5:	2396925CC38BE4F07BD426CF080256CE
SHA1:	8884E5383B3601E59089F0D287ACAD1EFF20C676
SHA-256:	E91BB1F7C2B2FFD094D3915F1FFFBFE929EFD49E1D732B51D60E8A378A8A066B
SHA-512:	D0622E928CAD41C185244CED7E0AC587B256B9A773F85D8ADEC807B4CDCBB73E55AB03AF3C8A8EA4A67BA347F9FE21A30515CB9A5AC871189B4AADC9442432A9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.m....C...C...C...C(..C...C...C...C...C$%xC...C...C}..C...C.. .C...C...C...C...CRich...C.....PE..L.....a.....n...P.....p.....@.....;e.....s..<.... .....0I..@.. .....text...Vm.....n..... ..`.data...${.....L..r.....@....wuve.....@..@.bedicarp.....@..@.rsrc..... ....@..@.reloc..I.....t.....@..B.....

C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621

Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.163540154379331
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:	430592
MD5:	2396925cc38be4f07bd426cf080256ce
SHA1:	8884e5383b3601e59089f0d287acad1eff20c676
SHA256:	e91bb1f7c2b2ffd094d3915f1fffbfe929efd49e1d732b51d60e8a378a8a066b
SHA512:	d0622e928cad41c185244ced7e0ac587b256b9a773f85d8adec807b4cdcbb73e55ab03af3c8a8ea4a67ba347f9fe21a30515cb9a5ac871189b4aadc9442432a9
SSDEEP:	6144:YecLXGqxxoij2Fjzp5/bCgXhh6K9W9n6ded89kTt:Y1LGq3NA5/bvIK9W9nbac
TLSH:	F194D0003299C6F1E3A21D375819DBE1E93BB82BF7245537F3582B6F6E3328157A2215
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.m....C...C...C...C(..C...C...C...C...C$%xC...C...C}..C...C...C...C...C...C...CRich...C.....PE..L.....a.....n.

File Icon

Icon Hash:	8286dccea68c9ca4

Static PE Info

General

Entrypoint:	0x407096
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6190B3DA [Sun Nov 14 06:59:38 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	eeffe9860bc9c6507e24465b9b5239be

Entrypoint Preview

Instruction
call 00007FD0B4BE489Ch
jmp 00007FD0B4BDEBFEh
mov edi, edi
push ebp
mov ebp, esp
sub esp, 28h
xor eax, eax
push ebx
mov ebx, dword ptr [ebp+0Ch]
push esi
mov esi, dword ptr [ebp+10h]
push edi
mov edi, dword ptr [ebp+08h]
mov byte ptr [ebp-08h], al
mov byte ptr [ebp-07h], al
mov byte ptr [ebp-06h], al
mov byte ptr [ebp-05h], al
mov byte ptr [ebp-04h], al
mov byte ptr [ebp-03h], al
mov byte ptr [ebp-02h], al
mov byte ptr [ebp-01h], al
cmp dword ptr [0044CB64h], eax
je 00007FD0B4BDED90h
push dword ptr [0044FB08h]
call 00007FD0B4BE37C8h
pop ecx
jmp 00007FD0B4BDED87h
mov eax, 0040CC48h
mov ecx, dword ptr [ebp+14h]
mov edx, 000000A6h
cmp ecx, edx
jg 00007FD0B4BDEEFAh
je 00007FD0B4BDEEE1h
cmp ecx, 19h
jg 00007FD0B4BDEE7Eh
je 00007FD0B4BDEE6Fh
mov edx, ecx
push 00000002h
pop ecx
sub edx, ecx
je 00007FD0B4BDEE53h
dec edx
je 00007FD0B4BDEE43h
sub edx, 05h
je 00007FD0B4BDEE2Bh
dec edx
je 00007FD0B4BDEE0Ch
sub edx, 05h
je 00007FD0B4BDEDF3h
dec edx
je 00007FD0B4BDEDC7h
sub edx, 09h
jne 00007FD0B4BDEF5Ah
mov dword ptr [ebp-28h], 00000003h
mov dword ptr [ebp-24h], 00401348h
fld qword ptr [edi]
lea ecx, dword ptr [ebp-28h]
fstp qword ptr [ebp-20h]
push ecx

Instruction
fld qword ptr [ebx]
fstp qword ptr [ebp+00h]

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x173c4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x1a510	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6d000	0xda4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11f0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4930	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x19c	.text
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	0x16d56	0x16e00	False	0.5955110143442623	data	6.70284422084366	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x18000	0x37b24	0x34c00	False	0.5779074718601895	data	5.56923108020657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.wuve	0x50000	0xbb8	0xc00	False	0.008138020833333334	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bedicar	0x51000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x1a510	0x1a600	False	0.6376073755924171	data	6.234348410854522	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6d000	0x1c6c	0x1e00	False	0.38958333333333334	data	3.8825877184339204	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x6a450	0x2	data	Slovak	Slovakia
AFX_DIALOG_LAYOUT	0x6a438	0x2	data	Slovak	Slovakia
AFX_DIALOG_LAYOUT	0x6a440	0xc	data	Slovak	Slovakia
SUXUMOWUDAKOLA	0x682d0	0x2107	ASCII text, with very long lines (8455), with no line terminators	Slovak	Slovakia
RT_CURSOR	0x6a458	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_CURSOR	0x6b300	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x6bbd0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0	Slovak	Slovakia
RT_CURSOR	0x6bd00	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0	Slovak	Slovakia
RT_ICON	0x52990	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x53058	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x55600	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x55a98	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x56940	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x571e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x57750	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x59cf8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x5ada0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x5b728	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x5bbf8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x5caa0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x5d348	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x5da10	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x5df78	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x60520	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x615c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x61a98	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Slovak	Slovakia
RT_ICON	0x62940	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Slovak	Slovakia
RT_ICON	0x631e8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Slovak	Slovakia
RT_ICON	0x638b0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Slovak	Slovakia
RT_ICON	0x63e18	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Slovak	Slovakia
RT_ICON	0x663c0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Slovak	Slovakia
RT_ICON	0x67468	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Slovak	Slovakia
RT_ICON	0x67df0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Slovak	Slovakia
RT_STRING	0x6bfc8	0x546	data	Slovak	Slovakia
RT_ACCELERATOR	0x6a3d8	0x40	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x6bba8	0x22	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x6bdb0	0x22	data	Slovak	Slovakia
RT_GROUP_ICON	0x61a30	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x55a68	0x30	data	Slovak	Slovakia
RT_GROUP_ICON	0x5bb90	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x68258	0x76	data	Slovak	Slovakia
RT_VERSION	0x6bdd8	0x1f0	MS Windows COFF PowerPC object file	Slovak	Slovakia
None	0x6a418	0xa	data	Slovak	Slovakia
None	0x6a428	0xa	data	Slovak	Slovakia

Imports

DLL	Import
KERNEL32.dll	FillConsoleOutputCharacterA, GetCPInfo, GetProfileIntW, GetSystemDefaultLCID, GetModuleHandleW, WaitNamedPipeW, TlsSetValue, GetPriorityClass, GetVolumeInformationA, LoadLibraryW, IsProcessInJob, AssignProcessToJobObject, GetCalendarInfoW, GetFileAttributesA, TransactNamedPipe, WriteConsoleW, GetVolumePathNameA, CreateJobObjectA, GetVolumeNameForVolumeMountPointA, FillConsoleOutputCharacterW, GetLastError, GetProcAddress, VirtualAlloc, EnumSystemCodePagesW, SetFileAttributesA, LoadLibraryA, WriteConsoleA, GetProcessWorkingSetSize, LocalAlloc, OpenJobObjectW, FoldStringW, FoldStringA, FindFirstChangeNotificationA, GetFileInformationByHandle, FindActCtxSectionStringW, LCMapStringW, GetConsoleAliasesW, GetFullPathNameW, HeapFree, HeapAlloc, Sleep, ExitProcess, GetStartupInfoW, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapReAlloc, WriteFile, GetStdHandle, GetModuleFileNameA, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlUnwind, SetHandleCount, GetFileType, GetStartupInfoA, SetFilePointer, TlsGetValue, TlsAlloc, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, InitializeCriticalSectionAndSpinCount, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, RaiseException, GetConsoleOutputCP, MultiByteToWideChar, SetStdHandle, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, CreateFileA, GetModuleHandleA, HeapSize, GetLocaleInfoA, LCMapStringA, GetStringTypeA, GetStringTypeW, SetEndOfFile, GetProcessHeap, ReadFile
ADVAPI32.dll	BackupEventLogW

Possible Origin

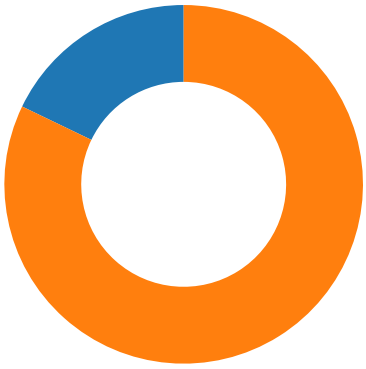
Language of compilation system	Country where language is spoken	Map
Slovak	Slovakia	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: file.exe PID: 3520, Parent PID: 3452

General

Target ID:	0

Start time:	10:31:56
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	430592 bytes
MD5 hash:	2396925CC38BE4F07BD426CF080256CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.259666135.00000000005D3000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000002.259530025.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000003.256458471.0000000000940000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000002.259872011.0000000000900000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.259872011.0000000000900000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: gntuud.exe PID: **2016**, Parent PID: **3520**

General

Target ID:	1
Start time:	10:32:03
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe"
Imagebase:	0x400000
File size:	430592 bytes
MD5 hash:	2396925CC38BE4F07BD426CF080256CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000001.00000003.293480849.00000000007CB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000001.00000003.271178795.0000000000680000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000001.00000003.293433328.00000000007AF000.00000004.00000020.00020000.00000000.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\f49dfc5e4e2508	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41190C	CreateDirectoryA
C:\Users\user\AppData\Roaming\f49dfc5e4e2508\cred64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	408BB2	CreateFileA
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	409D80	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	409D80	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409D80	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\f49dfc5e4e2508\cred64.dll	success or wait	1	41F5F3	DeleteFileW
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	13	41F5F3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	408BF9	InternetReadFile
unknown	unknown	16384			invalid handle	16	408C17	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	99707	409747	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	unknown	16384	success or wait	1	408BF9	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	unknown	16384	success or wait	7	408C26	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	unknown	14336	end of file	1	408C26	InternetReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	expand unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Local\Temp\ecaac49691\	success or wait	1	402F97	RegSetValueExA

Analysis Process: schtasks.exe PID: **5144**, Parent PID: **2016**

General

Target ID:	2
Start time:	10:32:10
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe" /F
Imagebase:	0x1050000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

Analysis Process: conhost.exe PID: **5300**, Parent PID: **5144**

General

Target ID:	3
Start time:	10:32:10
Start date:	09/12/2022
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: gntuud.exe PID: **5292**, Parent PID: **1080**

General

Target ID:	4
Start time:	10:32:12
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ecaac49691\gntuud.exe
Imagebase:	0x400000
File size:	430592 bytes
MD5 hash:	2396925CC38BE4F07BD426CF080256CE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000004.00000003.312159954.0000000000940000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000004.00000002.312844293.0000000000400000.00000040.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000004.00000002.313317695.00000000006E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000004.00000002.313317695.00000000006E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.313412358.0000000000745000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly