



ID: 756293
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:08:06
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Amadey 4
Yara Signatures 4
Dropped Files 4
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Compliance 6
Networking 6
System Summary 6
Data Obfuscation 6
Persistence and Installation Behavior 6
Boot Survival 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
World Map of Contacted IPs 10
Public IPs 10
Private 10
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll 12
C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe 12
C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe:Zone.Identifier 13
C:\Users\user\AppData\Local\Temp\853321935212 13
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 17
Possible Origin 17
Network Behavior 17
Statistics 17
Behavior 17

Copyright Joe Security LLC 2022

System Behavior 18
Analysis Process: file.exePID: 5520, Parent PID: 3324 18
General 18
File Activities 18
Analysis Process: rovwer.exePID: 4360, Parent PID: 5520 18
General 18
File Activities 19
File Created 19
File Deleted 20
File Written 20
File Read 21
Registry Activities 21
Key Value Modified 21
Analysis Process: schtasks.exePID: 5492, Parent PID: 4360 21
General 21
File Activities 21
Analysis Process: conhost.exePID: 5456, Parent PID: 5492 21
General 22
Analysis Process: rovwer.exePID: 1248, Parent PID: 1084 22
General 22
Analysis Process: rundll32.exePID: 3972, Parent PID: 4360 22
General 22
Disassembly 22

Copyright Joe Security LLC 2022

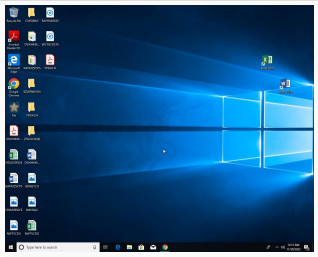
Windows Analysis Report

file.exe

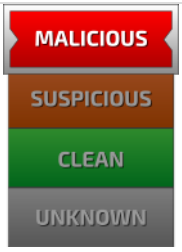
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756293
MD5:	efbdd62a08b28e..
SHA1:	ee2037450f52a6..
SHA256:	3c96f5e66f70af3..
Tags:	Amadey exe
Infos:	



Detection



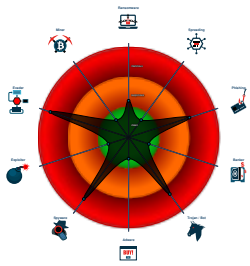
Amadey

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

Signatures

- Yara detected Amadeys stealer DLL
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Amadey bot
- System process connects to networ…
- 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…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5520 cmdline: C:\Users\user\Desktop\file.exe MD5: EFBDD62A08B28E63464F97D0600EAEF8)
  - rovwer.exe (PID: 4360 cmdline: "C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe" MD5: EFBDD62A08B28E63464F97D0600EAEF8)
    - schtasks.exe (PID: 5492 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN rovwer.exe /TR "C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 3972 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- rovwer.exe (PID: 1248 cmdline: C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe MD5: EFBDD62A08B28E63464F97D0600EAEF8)
- **cleanup**

Malware Configuration

Threatname: Amadey

```
{
  "C2 url": "193.56.146.194/h49vlBP/index.php",
  "Version": "3.50"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.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
00000008.00000002.315094938.000000000069E000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1220:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000002.00000002.298616677.00000000006E0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000008.00000002.315045334.00000000005E0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000002.00000002.299234828.0000000000739000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1170:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000005.00000003.343604843.0000000000674000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	

Click to see the 1 entries

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

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



System process connects to network (likely due to code injection or exploit)

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



System process connects to network (likely due to code injection or exploit)

Contains functionality to inject code into remote processes

Stealing of Sensitive Information



Yara detected Amadeys stealer DLL

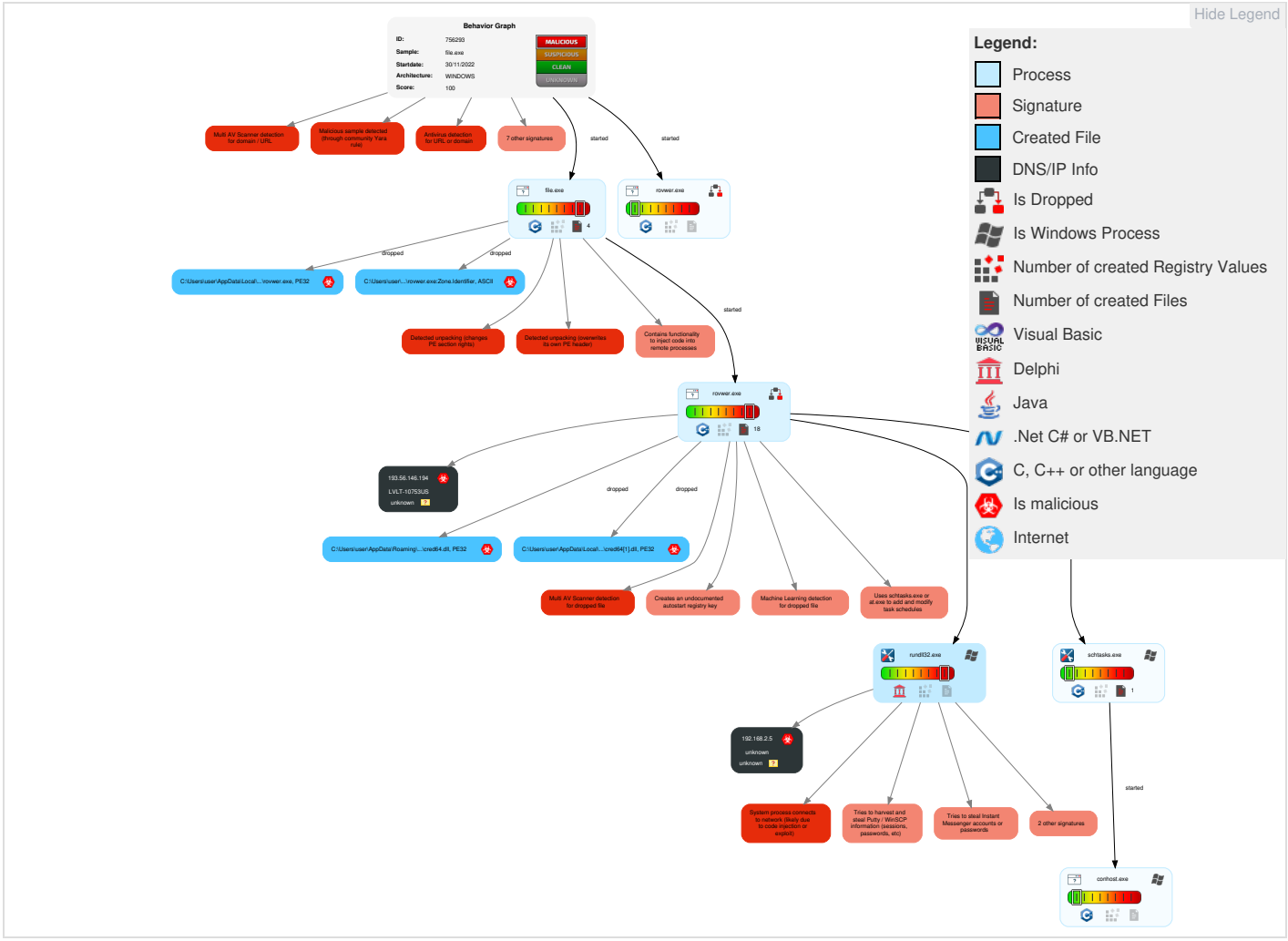
Copyright Joe Security LLC 2022

Yara detected Amadey bot
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 ftp login credentials
Tries to steal Instant Messenger accounts or passwords

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 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	2 1 1 Process Injection	2 Obfuscated Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	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	2 Software Packing	2 Credentials in Registry	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	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 Masquerading	1 Credentials In Files	2 4 System Information Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 2 1 Security Software Discovery	SSH	1 Input Capture	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 1 1 Process Injection	Cached Domain Credentials	2 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 Rundll32	DCSync	1 Process 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

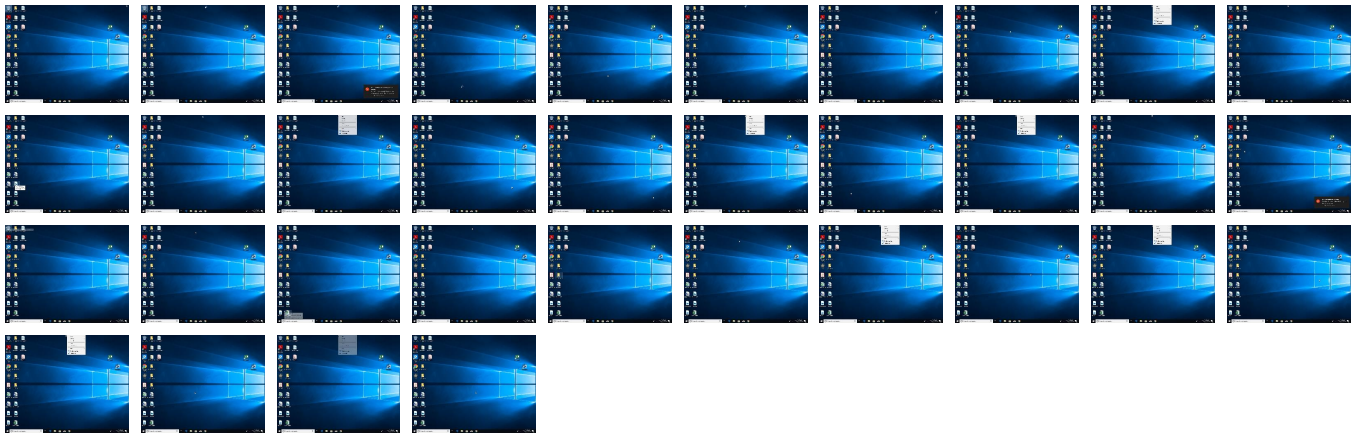
Behavior Graph



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	38%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	88%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	83%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe	41%	ReversingLabs	Win32.Ransomware.LockbitCrypt	
C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe	38%	Virustotal		Browse
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	88%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	83%	Virustotal		Browse

Copyright Joe Security LLC 2022

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
193.56.146.194/h49vlBP/index.php	12%	Virustotal		Browse
193.56.146.194/h49vlBP/index.php	100%	Avira URL Cloud	malware	

Domains and IPs

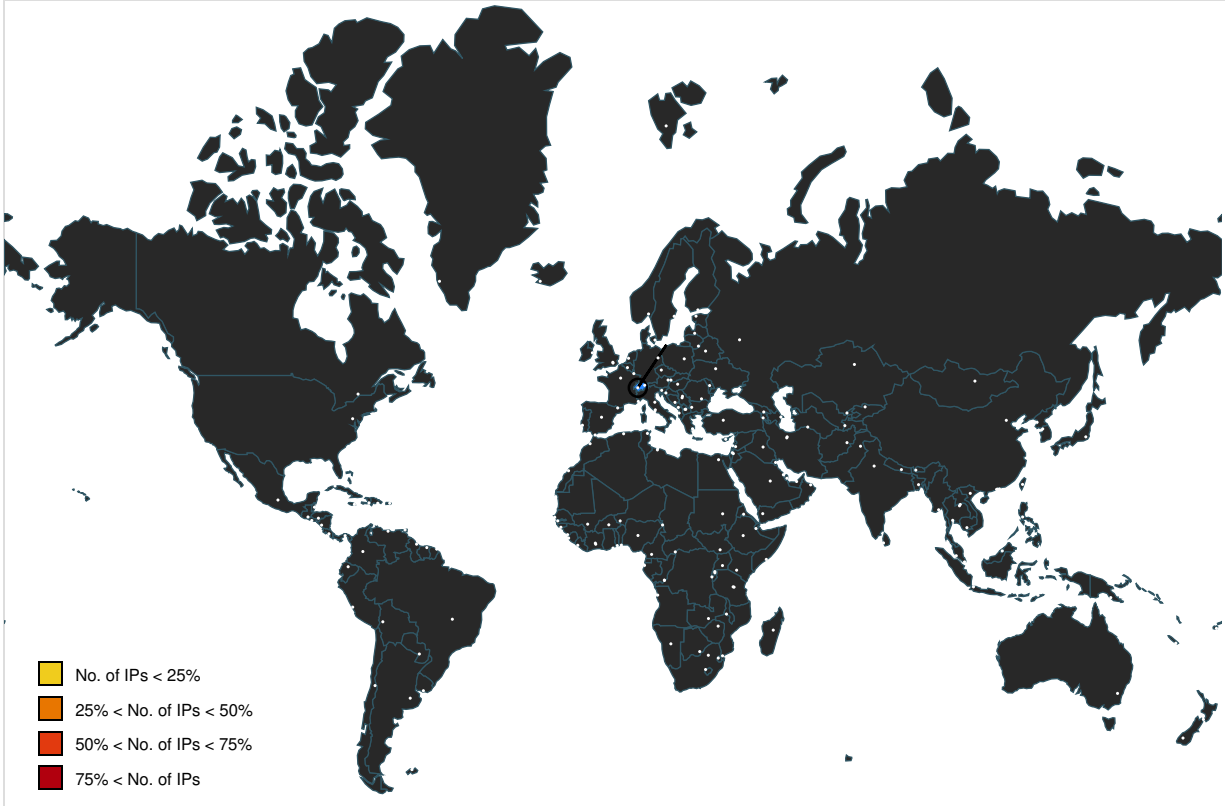
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
193.56.146.194/h49vlBP/index.php	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.56.146.194	unknown	unknown		10753	LVLT-10753US	true

Private

IP
192.168.2.5

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756293
Start date and time:	2022-11-30 00:08:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 0s
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:	13
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.phis.troj.spyw.evad.winEXE@9/5@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
00:09:03	API Interceptor	2722x Sleep call for process: rovwer.exe modified
00:09:04	Task Scheduler	Run new task: rovwer.exe path: C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.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\B87Z87FM\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.5119837978161605
Encrypted:	false
SSDEEP:	3072:ox7pOYzBektmWDWCMq6As523HeS9FAiZ87vO2rlL3Rne9:ox7ZNht/dMq6AO0a7vVlT
MD5:	674CEC24E36E0DFAEC6290DB96DDA86E
SHA1:	581E3A7A541CC04641E751FC850D92E07236681F
SHA-256:	DE81531468982B689451E85D249214D0AA484E2FFEDFD32C58D43CF879F29DED
SHA-512:	6D9898169073C240FE454BD45065FD7DC8458F1D323925B57EB58FA4305BB0D5631BBCEB61835593B225E887E0867186EF637C440460279378CB29E832066029
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\B87Z87FM\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\B87Z87FM\cred64[1].dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Virustotal, Detection: 83%, Browse
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\50c1695437\rovwer.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	209408
Entropy (8bit):	7.448890595749396
Encrypted:	false
SSDEEP:	3072:VDiatiyRJG2AUp508sUPHK5dsLIZ7WDvACjOm35PiYj+ZH1CagcZPakhYG/1qOl+:Y2i0G2P6SACD35PTjoCago9713+
MD5:	EFBDD62A08B28E63464F97D0600EAEF8
SHA1:	EE2037450F52A6095CD4365B0035072EE52BD7C2
SHA-256:	3C96F5E66F70AF3B7340F1D26163A6F299F6E48E53915F3E5A2D0D8402C15B15

SHA-512:	31C0A4E522865BC0AA653ACF25C83C82A997C1DFE04E1D9B0398857B4B26D4C83F5790773663DD4980F8BD807E88273D3CD23258D1FB1CB60BA51FF3A7514C7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41% • Antivirus: Virustotal, Detection: 38%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I....4.I.+...$.I.+...].I..]2.2.I.5.H.I.+.....I.+...4.I.+...4.I.Rich5 .I.....PE..L...Z_\a.....v.....L..... ....@.....P....P..P0.....@.....<..... .....text..... ..`.data...,... .....@....rsrc...P0...P...2.....@..@.....

C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\853321935212

Process:	C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.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):	83613
Entropy (8bit):	7.897756904424589
Encrypted:	false
SSDEEP:	1536:C14NsHjQAGVnUHzSstBBJ7NTz0E0dv1sgjGrGAEKHq+B8yvPvcq1sO6jEroWovg7:JNsHO10G4BBP/Ol1s51HqTykad2gd5
MD5:	F2357E4625FC12EC7807839B65552967
SHA1:	89BBC84D860AFE303E6D0CFEFBF69FA29127488B
SHA-256:	52369366F2308265D6FBD929364EF3C3A4E20B73B172E0C8945F1E0323ECF090
SHA-512:	468FA4033C588AD697D1A34E7A1D01BF89DB02246D41BE45D029EE1288DDC924B3B93E9F380F68C2E2DFE607C1F6164462C5B6963E18D87B4624AEA6D3D87C 0
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222

Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Virustotal, Detection: 83%, Browse
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..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.448890595749396
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:	209408
MD5:	efbdd62a08b28e63464f97d0600eaef8
SHA1:	ee2037450f52a6095cd4365b0035072ee52bd7c2
SHA256:	3c96f5e66f70af3b7340f1d26163a6f299f6e48e53915f3e5a2d0d8402c15b15
SHA512:	31c0a4e522865bc0aa653acf25c83c82a997c1dfe04e1d9b0398857b4b26d4c83f5790773663dd4980f8bd807e88273d3cd23258d1fb1cb60ba51ff3a7514c77
SSDEEP:	3072:VDiatiyRJG2AUp508sUPHK5dsLIZ7WDvACjOm35PiYj+ZH1CagcZPakhYG/1qOl+:Y2i0G2P6SACD35PTjoCago9713+
TLSH:	3B24F115B6A0E032D5A2F874193583E17E7FB9332DB549473B180B6E8F622C1B66E347
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I.....4.I.+...$.I.+...].I..]2.2.I.5.H...I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L...Z_\a.....

File Icon



Icon Hash:	d4b4b0e0e0eaf0d0

Static PE Info

General

Entrypoint:	0x404c97
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x615C5F5A [Tue Oct 5 14:21:14 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:	2ac0f7085258eff31142b9f87cb0f218

Entrypoint Preview

Instruction
call 00007FEBD4D948ECh
jmp 00007FEBD4D8EACDh
sub eax, 000003A4h
je 00007FEBD4D8EC74h
sub eax, 04h
je 00007FEBD4D8EC69h
sub eax, 0Dh
je 00007FEBD4D8EC5Eh
dec eax
je 00007FEBD4D8EC55h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007FEBD4D8FE5Eh
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 004303D8h
add esp, 0Ch
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl
inc eax
dec edi
jne 00007FEBD4D8EC49h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]
mov byte ptr [eax], dl
inc eax
dec esi
jne 00007FEBD4D8EC49h

Copyright Joe Security LLC 2022

Instruction
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [00430FE0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [00401170h]
mov edi, 00000100h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [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	0x10a9c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x65000	0x3050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	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	0x2cd8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x23c	.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	0x107d4	0x10800	False	0.5121182528409091	data	6.098303458795212	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x12000	0x52c88	0x1f400	False	0.970609375	data	7.937108707403602	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x65000	0x3050	0x3200	False	0.6284375	data	5.640049212553214	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
JEBOPOZUSUHARAFA	0x67430	0x55f	ASCII text, with very long lines (1375), with no line terminators	Raeto-Romance	Switzerland

Name	RVA	Size	Type	Language	Country
RT_ICON	0x652b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x65978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x65ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x66f88	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0x67b78	0x2d8	data	Raeto-Romance	Switzerland
RT_STRING	0x67e50	0x1fc	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x67990	0xa0	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x673f0	0x3e	data	Raeto-Romance	Switzerland
RT_VERSION	0x67a30	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	OpenMutexW, GetConsoleAliasExesLengthA, CopyFileExA, ReadConsoleOutputCharacterW, CompareStringW, SetVolumeLabelA, FillConsoleOutputAttribute, GetConsoleTitleA, QueryDosDeviceW, EnumCalendarInfoExA, GetProcessPriorityBoost, IsProcessInJob, AddConsoleAliasW, CreateFileW, SetMailslotInfo, GetWindowsDirectoryW, GetModuleHandleA, GlobalLock, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerA, GetVersionExA, SearchPathA, MoveFileExW, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, LocalAlloc, GetBinaryTypeA, GetCPInfoExW, WriteConsoleOutputA, GetCommandLineA, EnumDateFormatsW, CancelTimerQueueTimer, GetHandleInformation, FindResourceA, CreateJobObjectA, FindFirstVolumeA, GlobalFlags, CreateNamedPipeW, InterlockedIncrement, CloseHandle, CopyFileW, GetComputerNameExA, GetShortPathNameA, FlushFileBuffers, GetLogicalDriveStringsW, InterlockedCompareExchange, EnumCalendarInfoW, GetConsoleAliasExesLengthW, InterlockedExchange, GetNamedPipeHandleStateW, GetModuleHandleW, GetCurrentActCtx, GenerateConsoleCtrlEvent, MoveFileW, AddAtomA, SetThreadPriority, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointW, VirtualAlloc, _hread, EnumResourceLanguagesW, ClearCommBreak, QueryMemoryResourceNotification, GlobalFindAtomA, HeapWalk, SetFilePointer, GetTickCount, EnumSystemCodePagesW, VerifyVersionInfoA, LoadLibraryW, CreateFileA, GetLastError, WideCharToMultiByte, HeapReAlloc, HeapAlloc, HeapFree, UnhandledExceptionFilter, SetUnhandledExceptionFilter, DeleteFileA, GetStartupInfoA, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, HeapCreate, VirtualFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, GetConsoleCP, GetConsoleMode, RtlUnwind, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, HeapSize, ReadFile
GDI32.dll	GetCharWidthA, GetCharABCWidthsA
WINHTTP.dll	WinHttpSetOption

Possible Origin

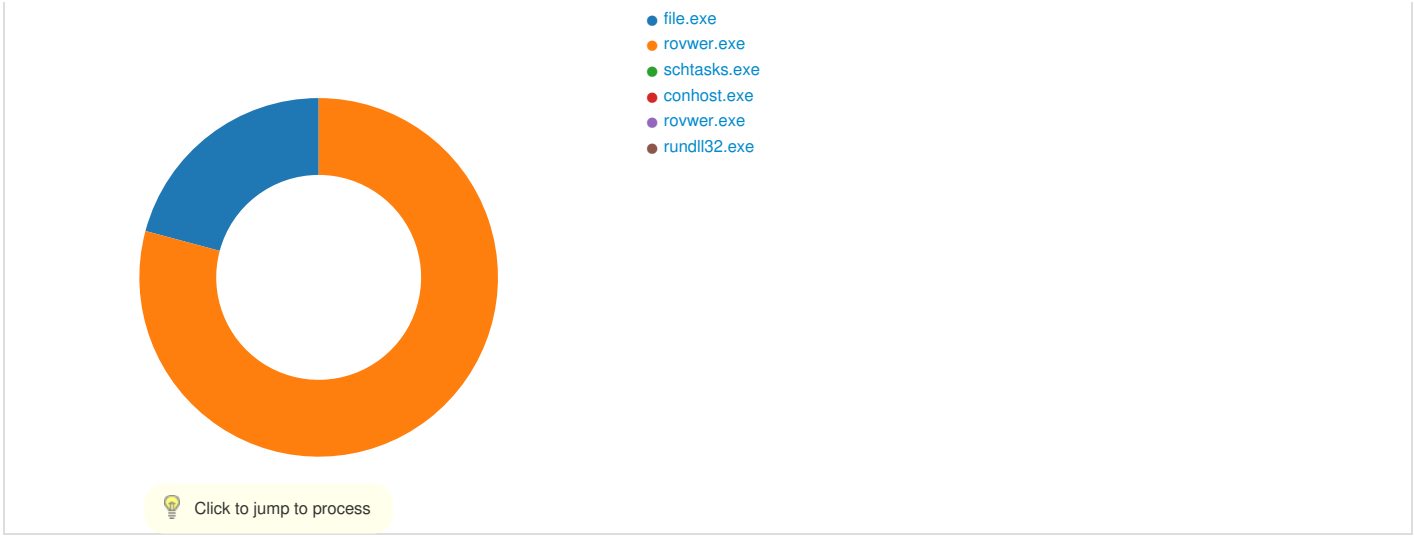
Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 5520, Parent PID: 3324

General

Target ID:	2
Start time:	00:08:56
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	209408 bytes
MD5 hash:	EFBDD62A08B28E63464F97D0600EAEF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000002.00000002.298616677.00000000006E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000002.00000002.299234828.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: rovwer.exe PID: 4360, Parent PID: 5520

General

Target ID:	5
Start time:	00:09:00
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe"
Imagebase:	0x400000
File size:	209408 bytes
MD5 hash:	EFBDD62A08B28E63464F97D0600EAEF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000005.00000003.343604843.0000000000674000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000005.00000003.343786461.0000000000674000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs • Detection: 38%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bf045808586a24	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\bf045808586a24\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
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

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	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\Local\Temp\853321935212	success or wait	16	41F5F3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.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 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	99571	409747	ReadFile

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\50c1695437\	success or wait	1	402F97	RegSetValueExA

Analysis Process: schtasks.exe PID: **5492**, Parent PID: **4360**

General

Target ID:	6
Start time:	00:09:02
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN rovwer.exe /TR "C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe" /F
Imagebase:	0xe30000
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: **5456**, Parent PID: **5492**

General	
Target ID:	7
Start time:	00:09:03
Start date:	30/11/2022
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: rovwer.exe PID: **1248**, Parent PID: **1084**

General	
Target ID:	8
Start time:	00:09:04
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\50c1695437\rovwer.exe
Imagebase:	0x7ff6ffff0000
File size:	209408 bytes
MD5 hash:	EFBDD62A08B28E63464F97D0600EAEF8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000008.00000002.315094938.000000000069E000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000008.00000002.315045334.00000000005E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: rundll32.exe PID: **3972**, Parent PID: **4360**

General	
Target ID:	9
Start time:	00:09:04
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Main
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	high

Disassembly

Copyright Joe Security LLC 2022

No disassembly