ID: 764034
Sample Name:
5GPueTFF2S.exe
Cookbook: default.jbs
Time: 10:38:07
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 5GPueTFF2S.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Amadey 4
Threatname: Vidar 5
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
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
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 12
Public IPs 12
Private 12
General Information 13
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\ProgramData\398664070279004990265593 52 14
C:\ProgramData\427400630576927468119676 90 14
C:\ProgramData\457077454726762573405296 48 15
C:\ProgramData\669749108561484176828778 49 15
C:\ProgramData\703426734006626601488074 53 15
C:\ProgramData\736474307208412306119856 31 15
C:\ProgramData\75873290272674793137.exe 16
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cred64[1].dll 16
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nppshell[1].exe 16
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe 17
C:\Users\user\AppData\Local\Temp\853321935212 17
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll 17

\Device\ConDrv 18
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Authenticode Signature 19
Entrypoint Preview 19
Rich Headers 20
Data Directories 20
Sections 21
Resources 21
Imports 22
Possible Origin 22
Network Behavior 22
Statistics 22
Behavior 22
System Behavior 23
Analysis Process: 5GPueTFF2S.exePID: 5848, Parent PID: 3528 23
General 23
File Activities 23
Analysis Process: 75873290272674793137.exePID: 6132, Parent PID: 5848 23
General 23
File Activities 24
File Created 24
File Written 24
Analysis Process: cmd.exePID: 5576, Parent PID: 5848 24
General 24
File Activities 25
File Deleted 25
Analysis Process: conhost.exePID: 5652, Parent PID: 5576 25
General 25
Analysis Process: timeout.exePID: 3216, Parent PID: 5576 25
General 25
File Activities 25
Analysis Process: gntuud.exePID: 5292, Parent PID: 6132 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
File Read 28
Registry Activities 28
Key Value Modified 28
Analysis Process: schtasks.exePID: 5724, Parent PID: 5292 28
General 28
File Activities 28
Analysis Process: conhost.exePID: 5768, Parent PID: 5724 28
General 29
Analysis Process: cmd.exePID: 3644, Parent PID: 5292 29
General 29
File Activities 29
Analysis Process: conhost.exePID: 2160, Parent PID: 3644 29
General 29
Analysis Process: cmd.exePID: 4628, Parent PID: 3644 30
General 30
File Activities 30
Analysis Process: cacls.exePID: 3856, Parent PID: 3644 30
General 30
File Activities 30
File Written 30
Analysis Process: cacls.exePID: 4760, Parent PID: 3644 30
General 30
File Activities 31
File Written 31
Analysis Process: cmd.exePID: 4384, Parent PID: 3644 31
General 31
Analysis Process: cacls.exePID: 5932, Parent PID: 3644 31
General 31
File Activities 31
File Written 31
Analysis Process: cacls.exePID: 4532, Parent PID: 3644 32
General 32
File Activities 32
File Written 32
Analysis Process: gntuud.exePID: 5956, Parent PID: 1088 32
General 32
Analysis Process: rundll32.exePID: 5968, Parent PID: 5292 32
General 32
Disassembly 33

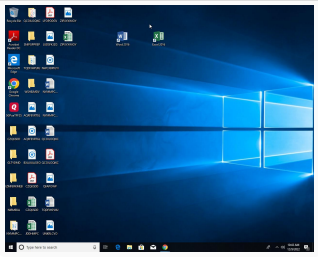
Windows Analysis Report

5GPueTFF2S.exe

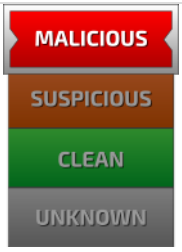
Overview

General Information

Sample Name:	5GPueTFF2S.exe
Analysis ID:	764034
MD5:	7d124bc23be85d..
SHA1:	09633b90a0b993.
SHA256:	04805512d670fb..
Tags:	32 exe trojan
Infos:	



Detection



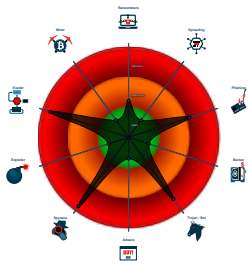
Amadey, Vidar

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

Signatures

- Yara detected Amadeys stealer DLL
- Malicious sample detected (through…
- Yara detected Amadey bot
- System process connects to networ…
- Yara detected Vidar stealer
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Detected unpacking (creates a PE f…
- Hides threads from debuggers
- Tries to steal Mail credentials (via fi…
- Overwrites code with unconditional j…
- Overwrites code with function prolog…

Classification



Process Tree

- **System is w10x64**
- 5GPueTFF2S.exe (PID: 5848 cmdline: C:\Users\user\Desktop\5GPueTFF2S.exe MD5: 7D124BC23BE85D73B1177143F41B5E72)
  - 75873290272674793137.exe (PID: 6132 cmdline: "C:\ProgramData\75873290272674793137.exe" MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
    - gntuud.exe (PID: 5292 cmdline: "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
      - schtasks.exe (PID: 5724 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 3644 cmdline: "C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\03bd543fce" /P "user:N"&&CACLS "..\03bd543fce" /P "user:R" /E&&Exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 2160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4628 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cacls.exe (PID: 3856 cmdline: CACLS "gntuud.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cacls.exe (PID: 4760 cmdline: CACLS "gntuud.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cmd.exe (PID: 4384 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cacls.exe (PID: 5932 cmdline: CACLS "..\03bd543fce" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cacls.exe (PID: 4532 cmdline: CACLS "..\03bd543fce" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
      - rundll32.exe (PID: 5968 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - cmd.exe (PID: 5576 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\5GPueTFF2S.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 3216 cmdline: timeout /t 6 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- gntuud.exe (PID: 5956 cmdline: C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
- **cleanup**

Malware Configuration

Threatname: Amadey

```
{
  "C2 url": "85.209.135.109/jg94cVd30f/index.php",
  "Version": "3.50"
}
```


Threatname: Vidar


```
{
  "C2 url": [
    "http://135.181.10.220:80",
    "https://t.me/vmt001"
  ],
  "Botnet": "1760",
  "Version": "56.1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000003.483002099.0000000001165000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
00000012.00000002.518241260.00000000000A1000.00000020.00000001.01000000.00000007.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000001.00000002.445175041.0000000000F71000.00000020.00000001.01000000.00000006.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.5GPueTFF2S.exe.a3f900.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.3.5GPueTFF2S.exe.b070000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.3.5GPueTFF2S.exe.a3f900.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.5GPueTFF2S.exe.b070000.2.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.3.5GPueTFF2S.exe.b070000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 8 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 dropped file

Machine Learning detection for sample

Compliance

Detected unpacking (creates a PE file in dynamic memory)

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)

PE file contains section with special chars

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

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

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Overwrites code with function prologues

Self deletion via cmd or bat file

Malware Analysis System Evasion

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Amadeys stealer DLL

Yara detected Amadey bot

Yara detected Vidar stealer

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

Tries to steal Crypto Currency Wallets

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

Tries to harvest and steal ftp login credentials

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to steal Instant Messenger accounts or passwords

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

Remote Access Functionality

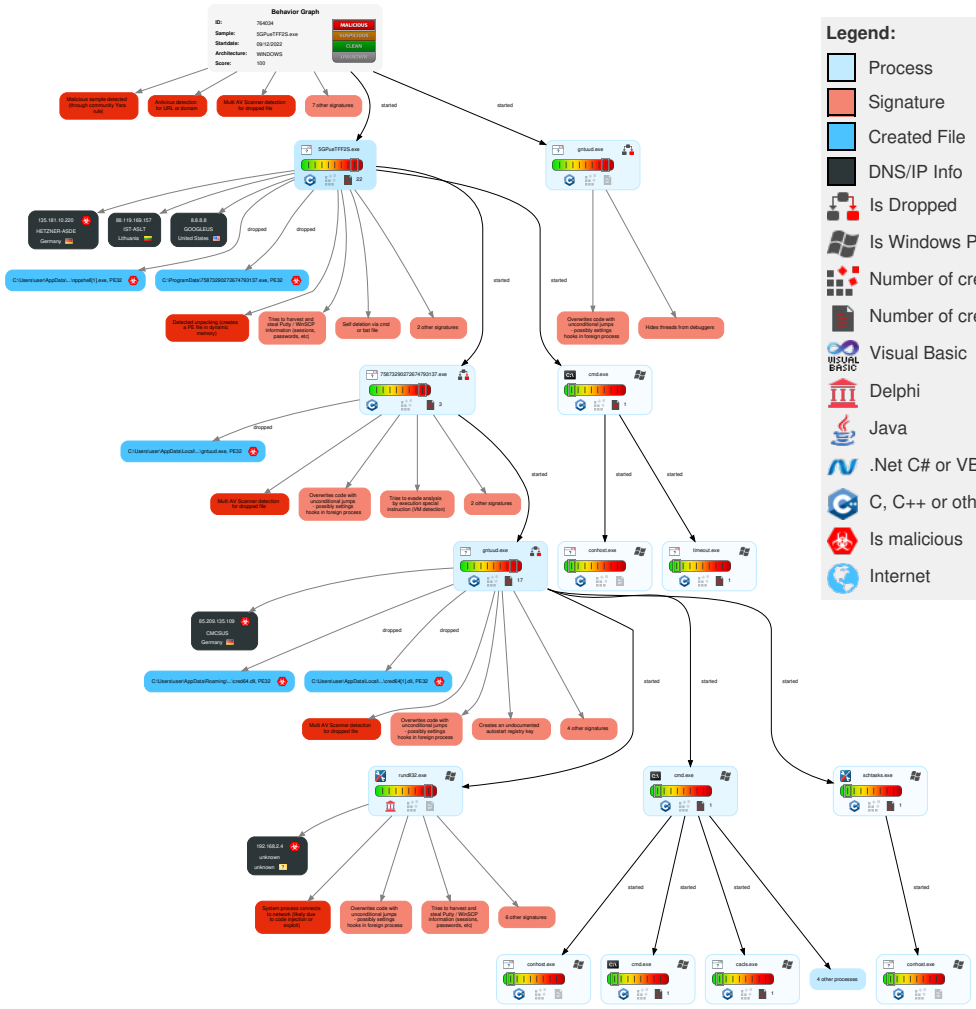
Yara detected Vidar stealer

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 Native API	1 Scheduled Task/Job	1 1 1 Process Injection	2 Obfuscated Files or Information	2 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	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 2 Software Packing	1 Credential API Hooking	2 File and Directory Discovery	Remote Desktop Protocol	4 Data from Local System	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Services File Permissions Weakness	1 Registry Run Keys / Startup Folder	1 File Deletion	1 Input Capture	2 4 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Services File Permissions Weakness	1 Masquerading	2 Credentials in Registry	4 3 1 Security Software Discovery	Distributed Component Object Model	1 Credential API Hooking	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	1 Credentials In Files	1 1 Process 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	1 1 1 Process Injection	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 Services File Permissions Weakness	DCSync	1 Remote System 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	1 Rundll32	Proc Filesystem	Network Service Scanning	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

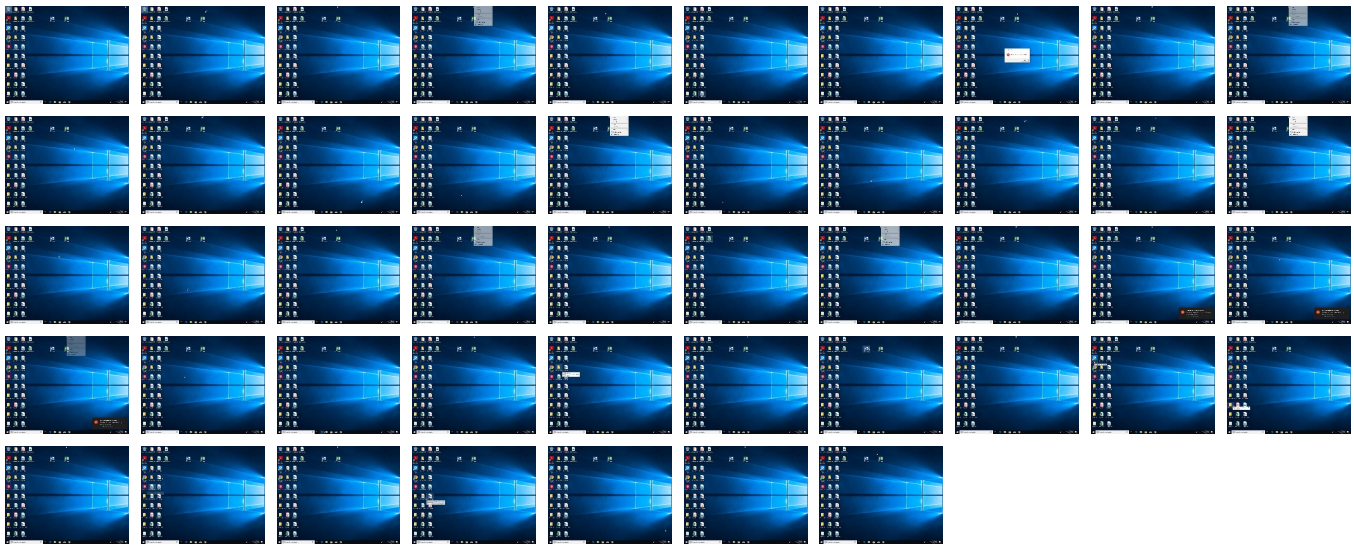
Hide Legend



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
5GPueTFF2S.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\75873290272674793137.exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cred64[1].dll	12%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nppshell[1].exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll	12%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.5GPueTFF2S.exe.b070000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.5GPueTFF2S.exe.a3f900.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.5GPueTFF2S.exe.a3f900.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://135.181.10.220/update.zip	0%	Avira URL Cloud	safe	
http://135.181.10.220:801760	0%	Avira URL Cloud	safe	
http://135ple-wells-2022.net/yzoyoebw6fqrey/nppshell.exe	0%	Avira URL Cloud	safe	
85.209.135.109/jg94cVd30f/index.php	0%	Avira URL Cloud	safe	
http://135.181.10.220/1760	0%	Avira URL Cloud	safe	
http://ripple-wells-2022.net/yzoyoebw6fqrey/nppshell.exe	100%	Avira URL Cloud	malware	
http://135.181.10.220:80/update.zip	0%	Avira URL Cloud	safe	
http://mikub7zdt5qfxou902vyke64v30mcoy.lnrmxftsk2pynk6vwbpg5s/	0%	Avira URL Cloud	safe	
http://135.181.10.220:8	0%	Avira URL Cloud	safe	
http://135.181.10.220:80https://t.me/vmt001hello2092;open_open	0%	Avira URL Cloud	safe	
http://ripple-wells-2022.net/yzoyoebw6fqrey/nppshell.exerO	0%	Avira URL Cloud	safe	
http://135.181.10.220:80/update.zipb1ef1c57276c118008692-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6963	0%	Avira URL Cloud	safe	
http://135.181.10.220:80	0%	Avira URL Cloud	safe	
http://mIkUB7ZDt5qfxou902VyKe64v30McOy.LnrmXFtSK2Pynk6VWBPG5Sf1w0AavRp1BVjmQQUkh2vmJkxEZO5UQQZNHAms9	0%	Avira URL Cloud	safe	
http://135.181.10.220/	0%	Avira URL Cloud	safe	
http://135.181.10.220/1760jf.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
85.209.135.109/jg94cVd30f/index.php	true	• Avira URL Cloud: safe	low
http://https://t.me/vmt001	false		high
http://135.181.10.220:80	true	• Avira URL Cloud: safe	unknown

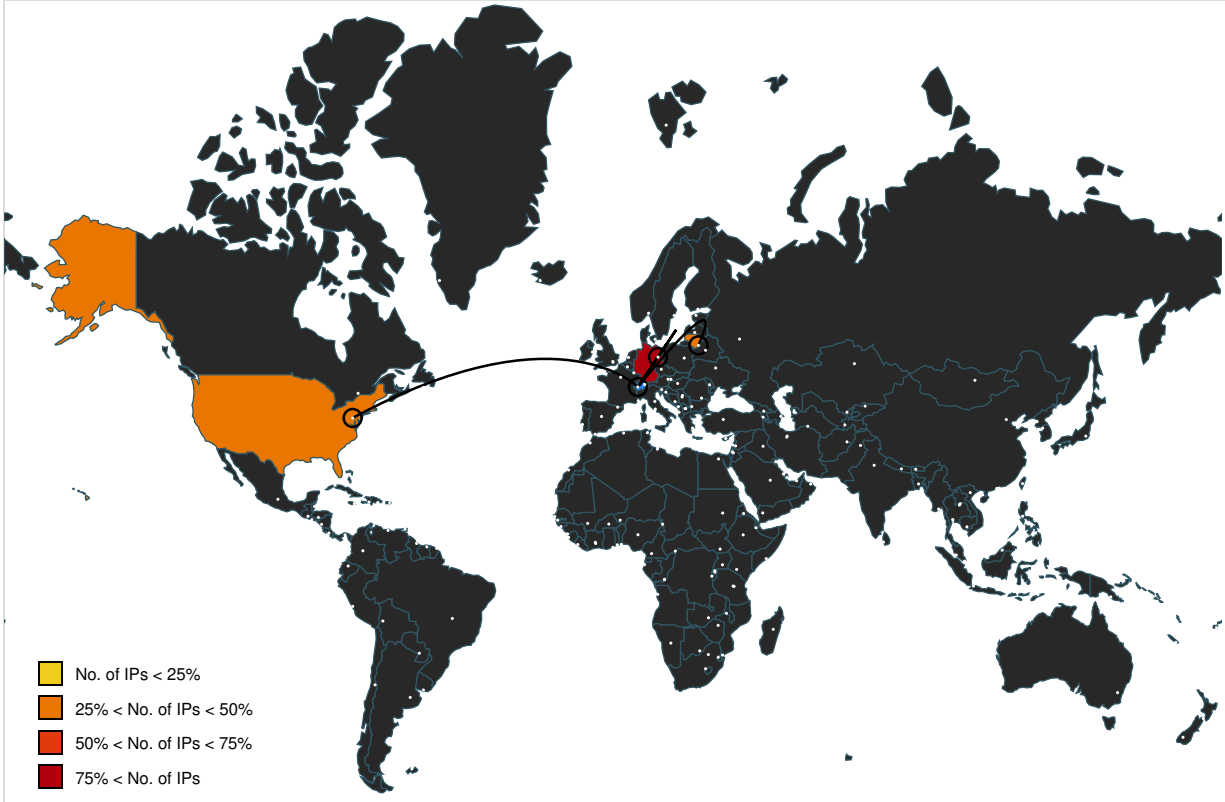
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://135.181.10.220/1760	5GPueTFF2S.exe, 00000000.00000003.420608823.00000000009F7000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423133875.00000000009F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mikub7zdt5qfxou902vyke64v30mcoy.lnrmxftsk2pynk6vwbpg5s/	5GPueTFF2S.exe, 00000000.00000003.420608823.00000000009F7000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423133875.00000000009F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://135ple-wells-2022.net/yzoyoebw6fqrey/nppshell.exe	5GPueTFF2S.exe, 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	39866407027900499026559352.0.dr	false		high
http://https://sectigo.com/CPS0	75873290272674793137.exe, 00000001.00000003.430764953.0000000002F01000.00000004.00000800.00020000.00000000.sdmp, cred64[1].dll.7.dr, 75873290272674793137.exe.0.dr, gntuud.exe.1.dr	false	• URL Reputation: safe	unknown
http://135.181.10.220:80/update.zip	5GPueTFF2S.exe, 00000000.00000002.422509988.00000000005AC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://ocsp.sectigo.com0	75873290272674793137.exe, 00000001.00000003.430764953.0000000002F01000.00000004.00000800.00020000.00000000.sdmp, cred64[1].dll.7.dr, 75873290272674793137.exe.0.dr, gntuud.exe.1.dr	false	• URL Reputation: safe	unknown
http://135.181.10.220:801760	5GPueTFF2S.exe, 00000000.00000002.425200801.0000000002A90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ripple-wells-2022.net/yzoyoebw6fqrey/nppshell.exe	5GPueTFF2S.exe, 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	39866407027900499026559352.0.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://135.181.10.220:80https://t.me/vmt001hello2092;open_open	5GPueTFF2S.exe, 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.432090196.000000000B0A5000.00000002.00000800.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000003.387953405.000000000B070000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://ac.ecosia.org/autocomplete?q=	39866407027900499026559352.0.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	5GPueTFF2S.exe, 00000000.00000003.395141799.0000000008DF0000.00000004.00000800.00020000.00000000.sdmp, 39866407027900499026559352.0.dr	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	75873290272674793137.exe, 00000001.00000003.430764953.0000000002F01000.00000004.00000800.00020000.00000000.sdmp, cred64[1].dll.7.dr, 75873290272674793137.exe.0.dr, gntuud.exe.1.dr	false	• URL Reputation: safe	unknown
http://135.181.10.220/update.zip	5GPueTFF2S.exe, 00000000.00000002.423133875.00000000009F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	75873290272674793137.exe, 00000001.00000003.430764953.0000000002F01000.00000004.00000800.00020000.00000000.sdmp, cred64[1].dll.7.dr, 75873290272674793137.exe.0.dr, gntuud.exe.1.dr	false	• URL Reputation: safe	unknown
http://135.181.10.220:8	5GPueTFF2S.exe, 00000000.00000003.385525417.000000000CCC0000.00000040.00000800.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.431582702.000000000B030000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://135.181.10.220:80/update.zipb1ef1c57276c118008692-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6963	5GPueTFF2S.exe, 00000000.00000002.422509988.00000000005AC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mIkUB7ZDt5qfxou902VyKe64v30McOy.LnrmXFtSK2Pynk6VWBPG5Sf1w0AavRp1BVjmQQUkh2vmJkxEZO5UQQZNHAms9	5GPueTFF2S.exe, 00000000.00000002.424393747.00000000028CA000.00000040.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	39866407027900499026559352.0.dr	false		high
http://ripple-wells-2022.net/yzoyoebw6fqrey/nppshell.exerO	5GPueTFF2S.exe, 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://135.181.10.220/1760jf.	5GPueTFF2S.exe, 00000000.00000003.420608823.00000000009F7000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423133875.00000000009F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://135.181.10.220/	5GPueTFF2S.exe, 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, 5GPueTFF2S.exe, 00000000.00000002.430008393.0000000008E30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
135.181.10.220	unknown	Germany		24940	HETZNER-ASDE	true
88.119.169.157	unknown	Lithuania		61272	IST-ASLT	false
85.209.135.109	unknown	Germany		33657	CMCSUS	true

Private

IP
192.168.2.4

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764034
Start date and time:	2022-12-09 10:38:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5GPueTFF2S.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:	23
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@31/16@0/5
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 49.3% (good quality ratio 47.2%) • Quality average: 82.3% • Quality standard deviation: 22.5%
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 • 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, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenFile 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: 5GPueTFF2S.exe

Simulations

Behavior and APIs

Time	Type	Description
10:40:18	API Interceptor	1804x Sleep call for process: gntuud.exe modified
10:40:20	Task Scheduler	Run new task: gntuud.exe path: C:\Users\user\AppData\Local\Temp\03bd543fce\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:\ProgramData\39866407027900499026559352

Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\42740063057692746811967690

Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\457077454726762573405296 48	
Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 4, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.47889536469736377
Encrypted:	false
SSDEEP:	96:MHVdU+bb3HDsX0ctSOaDN6tOVjN9DLjGQLBE3u:YVK+H3HDi9GN6IVj3XBBE3u
MD5:	D6648BE90F0B2A39C26D60D499E5EB03
SHA1:	69D2F56BBA9264621C0779F5D74B356C3794AFF0
SHA-256:	E26A78FA6C8A1C60B67536CCB9A620F69FF4588F50F7F3956E14E438C6E5F9D6
SHA-512:	BEF8A8D7391D16444B6347C1F2E07037EE1DF67652910551133919EF59F44C94636971BF602D93087D628A6E38DDF0929CF4C824994B35E6C2376B0B55AD4974
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\669749108561484176828778 49	
Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.43613063485556663
Encrypted:	false
SSDEEP:	12:TLqlUlFnGP6Gkwtwhg4FdbXGwvfhowcFOaOmzdOtssh+bgc4Jp+FxOUwa5q0u9z3:TLqlj1czkwubXYFpFNYcw+6UwcYzHr
MD5:	46076967A4692D6323BCBDAD8532DA6A
SHA1:	A2C61F0EAECF8C2D126FCF82828808B78291E582
SHA-256:	BFA77719DCA9C4C92B38BD8A23C9DD751B82DB0F21620E6937C4F97AECC5536B
SHA-512:	B4C03F075B2E4DC527AD25B5D5788BE55D4CBCCA66002884CC75528FC57AF54C494B2219C726999E9A29C5AB05C789DB1412F4A01A8AC61726E2F7B785E776 1
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\703426734006626601488074 53	
Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 4, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.47889536469736377
Encrypted:	false
SSDEEP:	96:MHVdU+bb3HDsX0ctSOaDN6tOVjN9DLjGQLBE3u:YVK+H3HDi9GN6IVj3XBBE3u
MD5:	D6648BE90F0B2A39C26D60D499E5EB03
SHA1:	69D2F56BBA9264621C0779F5D74B356C3794AFF0
SHA-256:	E26A78FA6C8A1C60B67536CCB9A620F69FF4588F50F7F3956E14E438C6E5F9D6
SHA-512:	BEF8A8D7391D16444B6347C1F2E07037EE1DF67652910551133919EF59F44C94636971BF602D93087D628A6E38DDF0929CF4C824994B35E6C2376B0B55AD4974
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\736474307208412306119856 31	
Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped

Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\75873290272674793137.exe

Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f.?...6.f.....6.f.4...6.Rich..6.....PE..L....6.c.....r.....FU.....@.....~.v...@.....p.....`..`c.....u.....P.....0E..p.....A..@.....A.h.....lB@dO\ih..... ..`Fh?jG[OJL.....@..@qNR5:WbSLD.....@...z?fd8ijJh.=..... ..`CV?7x>JO.....A.....@...EVjKc_MI.wo...A..xo..... ..`dT<:EHzj.....P.....o.....@..@@]topACL`c...`...\....o.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7705824
Entropy (8bit):	7.9708080300718365
Encrypted:	false
SSDEEP:	196608:ZQoqS56OZEssxxpKIIue41Cf7sgZz6kmAZQ/9RWB0:dMOevKiB1CfQgplmz/9a0
MD5:	2B62E02B3581980EE5A1DDA42FA4F3FE
SHA1:	5C36BFA4A4973E8F694D5C077E7312B1C991AEDF
SHA-256:	8C46C2AF1CB25BFA8FBBF9D683D72D30DDB2E5D0ECC6BBA997B24714CF2B8C91
SHA-512:	255E1B1D51D52872C5E0C54F7807ADC3581D36B3DFB8220C818AC38AC7FCEA91DD42999EE6CCAEF3B9836CD59FCFE19C2669A5B697D627DE4C1D9B8BA563B3D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....X.....@.....*.u. .....O...X>..@.....~u.....F.....f5g\gWe7..... ..`zDthL)*@.....@...nb"h!m#Y.....$^+<%+dU&.....@...Z-).j99tO.....@..P8"ikKHD[b.C..... ..`k&l<0?<6.....F.....@...n[uZh3ex.lu...F..nu..... ..`Uh%r6i!H.....xu.....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nppshell[1].exe

Process:	C:\Users\user\Desktop\5GPueTFF2S.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false

SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f. ?...6.f.....6.f.4...6.Rich..6.........PE..L....6.c.....................r.......FU...........@................................~.v...@...................................p......`..`c............u......P......0E..p.......................... A..@.............A.h...........................lB@dO\ih............................ ..`Fh?jG[OJL............................@..@qNR5:WbSLD..........................@...z?fd8ijJh.=.......................... ..`CV?7x >JO......A.....................@...EVjKc_MI.wo...A..xo................. ..`dT<:EHzj.....P........o............@..@@]topACL`c...`...\....o............@..@... ....

C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe

Process:	C:\ProgramData\75873290272674793137.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f. ?...6.f.....6.f.4...6.Rich..6.........PE..L....6.c.....................r.......FU...........@................................~.v...@...................................p......`..`c............u......P......0E..p.......................... A..@.............A.h...........................lB@dO\ih............................ ..`Fh?jG[OJL............................@..@qNR5:WbSLD..........................@...z?fd8ijJh.=.......................... ..`CV?7x >JO......A.....................@...EVjKc_MI.wo...A..xo................. ..`dT<:EHzj.....P........o............@..@@]topACL`c...`...\....o............@..@... ....

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

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\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):	96208
Entropy (8bit):	7.920718791075791
Encrypted:	false
SSDEEP:	1536:C66YpZSvaEuegY9ArFi7deYA070yjPTv6SUv9bMzXQoHID3WlgDnqc1uhDO6KgrO:YYnSvbtgsArFi3Y+yVFWAoHQWlep1u1S
MD5:	864C73BCC733D275D7A8B0AC455F09CF
SHA1:	D885D54A9AEED3B4D4F097218747629E59A83582
SHA-256:	D376E89252A2E21635744857EA02E60105545A58D6E75CEFF0F7D3FC4B07A2BF
SHA-512:	A6BF03A348371A7E38B24F51777195EDC995B3FC09A44D874942A85C123B9BEA041176C80BC5CF72088AB9C5D1D854607C82A2C9F12E78083703B5CC47E5657
Malicious:	false
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222..........."..................... ....}.........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w........!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5............\|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23....._....m.....'.........S.. ..W....'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(....Q..R...`2.`....j.$.....+..];$....F...K.1...3.)k...@<1..@.../...G. .....g.G.....~.W.W.......

C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7705824
Entropy (8bit):	7.9708080300718365
Encrypted:	false
SSDEEP:	196608:ZQoqS56OZEssxxpKIlue41Cf7sgZz6kmAZQ/9RWB0:dMOevKiB1CfQgplmz/9a0
MD5:	2B62E02B3581980EE5A1DDA42FA4F3FE
SHA1:	5C36BFA4A4973E8F694D5C077E7312B1C991AEDF

SHA-256:	8C46C2AF1CB25BFA8FBBF9D683D72D30DDB2E5D0ECC6BBA997B24714CF2B8C91
SHA-512:	255E1B1D51D52872C5E0C54F7807ADC3581D36B3DFB8220C818AC38AC7FCEA91DD42999EE6CCAEF3B9836CD59FCFE19C2669A5B697D627DE4C1D9B8BA563B3D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....X.....@.....*.u.....O...X>..@.....~u.....F.....f5g\gWe7..... ..`zDthL)*@.....@...nb"h!m#Y.....$^+<%+dU&.....@...Z-),j99tO.....@..P8"ikKHD[b.C..... ..`k&l<0?<6.....F.....@...n[uZh3ex.lu...F..nu..... ..`Uh%r6i!H.....xu.....@..P.....@.....@..P.....

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\cacls.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.240223928941852
Encrypted:	false
SSDEEP:	3:o3F:o1
MD5:	509B054634B6DE74F111C3E646BC80FD
SHA1:	99B4C0F39144A92FE42E22473A2A2552FB16BD13
SHA-256:	07C7C151ADD6D955F3C876359C0E2A3A3FB0C519DD1E574413F0B68B345D8C36
SHA-512:	A9C2D23947DBE09D5ECFBF6B3109F3CF8409E43176AE10C18083446EDE006E60E41C3EA2D2765036A967FC81B085D5F271686606AED4154AE45287D412CF6D4
Malicious:	false
Preview:	processed dir:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.937705906500799
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:	5GPueTFF2S.exe
File size:	1493440
MD5:	7d124bc23be85d73b1177143f41b5e72
SHA1:	09633b90a0b993fd4dec6d522a1243433fc3ab10
SHA256:	04805512d670fb5f37bdf17bf00aae6976650f82c0b4bd342f3506d204f7aea2
SHA512:	f4d318361bcccd7a3a77cdb243fa27e46abb6831cc315a4d8c4df9c37f30d11d2a0cd8a0ab9c8567f2c584dbcca1a9c336677216b8e31495c20061b287c29ebe
SSDEEP:	24576:jEiV++MCUfiiF5CYElcxGvvJq89F85NURwfCULmNQpBAXFVw/5xbpY0Y8vNcup:jEiV++MCxiF0tJ25NK2mapBA1uxYSlcG
TLSH:	BA65236E93951032DAC617342CF7CF9BB739EF2516A897472A869D2A7C31BD0D930306
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#c..g...g...g...yPb.~...yPs.v...yPe.+...@..`...g...9...yPl.e...yPr.f...g.q.b...yPw.f...Richg.....PE..L....#.c.....

File Icon

Icon Hash:	c8d4f2e8e8b2e4d8

Static PE Info

General

Entrypoint:	0x40901d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63922306 [Thu Dec 8 17:46:46 2022 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:	bb2af1988009d4b4491115f62e2f94ab

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US
Signature Validation Error:	**A certificate chain could not be built to a trusted root authority**
Error Number:	-2146762486
Not Before, Not After	• 10/25/2022 2:00:00 AM 11/23/2023 12:59:59 AM
Subject Chain	• CN=vcoins.com
Version:	3
Thumbprint MD5:	7353B8C793C943D5CF2DE1715C892554
Thumbprint SHA-1:	D2516DC5680485D69BC68CCCCA5E2D61A43D345F
Thumbprint SHA-256:	C831B8A2466C3A56F5AA15E9C540B5A2B3359C94386EE03D349C975F08DE1C03
Serial:	050A012C9D98C6D640D2D7F67E016985

Entrypoint Preview
Instruction
call 00007F70A8E0920Fh
jmp 00007F70A8E07A6Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [00540008h+ecx*8]
je 00007F70A8E07C05h
inc ecx
cmp ecx, 2Dh
jc 00007F70A8E07BE3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F70A8E07C00h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0054000Ch+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F70A8E08C5Ch

Instruction
test eax, eax
jne 00007F70A8E07BF8h
mov eax, 00540170h
ret
add eax, 08h
ret
push 0000000Ch
push 0053F408h
call 00007F70A8E08FC1h
mov ecx, dword ptr [ebp+08h]
xor edi, edi
cmp ecx, edi
jbe 00007F70A8E07C20h
push FFFFFFE0h
pop eax
xor edx, edx
div ecx
cmp eax, dword ptr [ebp+0Ch]
sbb eax, eax
inc eax
jne 00007F70A8E07C11h
call 00007F70A8E07BB9h
mov dword ptr [eax], 0000000Ch
push edi
push edi
push edi
push edi
push edi
call 00007F70A8E09349h
add esp, 14h
xor eax, eax
jmp 00007F70A8E07CCAh
imul ecx, dword ptr [ebp+0Ch]
mov esi, ecx
mov dword ptr [ebp+08h], esi
cmp esi, edi
jne 00007F70A8E07BF5h
xor esi, esi
inc esi
xor ebx, ebx
mov dword ptr [ebp-1Ch], ebx
cmp esi, FFFFFFE0h
jnbe 00007F70A8E07C5Bh
cmp dword ptr [00755448h], 03h
jne 00007F70A8E07C3Dh
add esi, 0Fh

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	0x13f674	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x356000	0x28330	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x16b600	0x13c0	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x37f000	0x14d4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x13e170	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x13f338	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x13e000	0x134	.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	0x13c331	0x13c400	False	0.9838724370059289	data	7.993775932964981	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x13e000	0x1d66	0x1e00	False	0.36627604166666666	data	5.590565779983959	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x140000	0x21557c	0xe00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x356000	0x28330	0x28400	False	0.8145805027173914	data	7.416644005362062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x37f000	0x3cc8	0x3e00	False	0.28616431451612906	data	3.1400595377335185	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x356508	0x1b278	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Polish	Poland
RT_ICON	0x371780	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	Polish	Poland
RT_ICON	0x3759a8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Polish	Poland
RT_ICON	0x377f50	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	Polish	Poland
RT_ICON	0x378df8	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	Polish	Poland
RT_ICON	0x379460	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Polish	Poland
RT_ICON	0x37a508	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	Polish	Poland
RT_ICON	0x37adb0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	Polish	Poland
RT_ICON	0x37b098	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Polish	Poland
RT_ICON	0x37ba20	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576	Polish	Poland
RT_ICON	0x37c0e8	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	Polish	Poland
RT_ICON	0x37c2d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Polish	Poland
RT_ICON	0x37c738	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	Polish	Poland
RT_ICON	0x37cca0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	Polish	Poland
RT_DIALOG	0x37cdc8	0x108	data	Polish	Poland
RT_DIALOG	0x37ced0	0x15c	data	Polish	Poland

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x37d02c	0x13c	data	Polish	Poland
RT_DIALOG	0x37d168	0x19c	data	Polish	Poland
RT_STRING	0x37d304	0x14c	data	Polish	Poland
RT_STRING	0x37d450	0x5ac	data	Polish	Poland
RT_STRING	0x37d9fc	0x540	data	Polish	Poland
RT_STRING	0x37df3c	0x1cc	data	Polish	Poland
RT_GROUP_ICON	0x37e108	0xca	Targa image data - Map 32 x 45688 x 1 +1	Polish	Poland
RT_MANIFEST	0x37e1d4	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetSystemDefaultLangID, lstrlenA, TlsGetValue, HeapAlloc, InterlockedIncrement, OutputDebugStringW, IsBadReadPtr, GetConsoleCP, Sleep, HeapCreate, GetACP, GetLastError, GetCurrentDirectoryW, SetLastError, GetProcAddress, FoldStringW, GetCurrentProcessId, GetThreadUILanguage, LCMapStringW, LCMapStringA, GetStringTypeW, MultiByteToWideChar, GetStringTypeA, GetStartupInfoW, SetUnhandledExceptionFilter, GetModuleHandleW, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, InterlockedDecrement, VirtualFree, HeapFree, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, IsDebuggerPresent, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, LoadLibraryA, InitializeCriticalSectionAndSpinCount, GetCPInfo, GetOEMCP, IsValidCodePage, RtlUnwind, HeapSize, GetLocaleInfoA, WideCharToMultiByte
USER32.dll	GetMessagePos, MessageBoxW, IsIconic, GetMessageExtraInfo, IsZoomed, GetWindowTextLengthA, GetForegroundWindow
ole32.dll	CoInitialize, CoUninitialize

Possible Origin

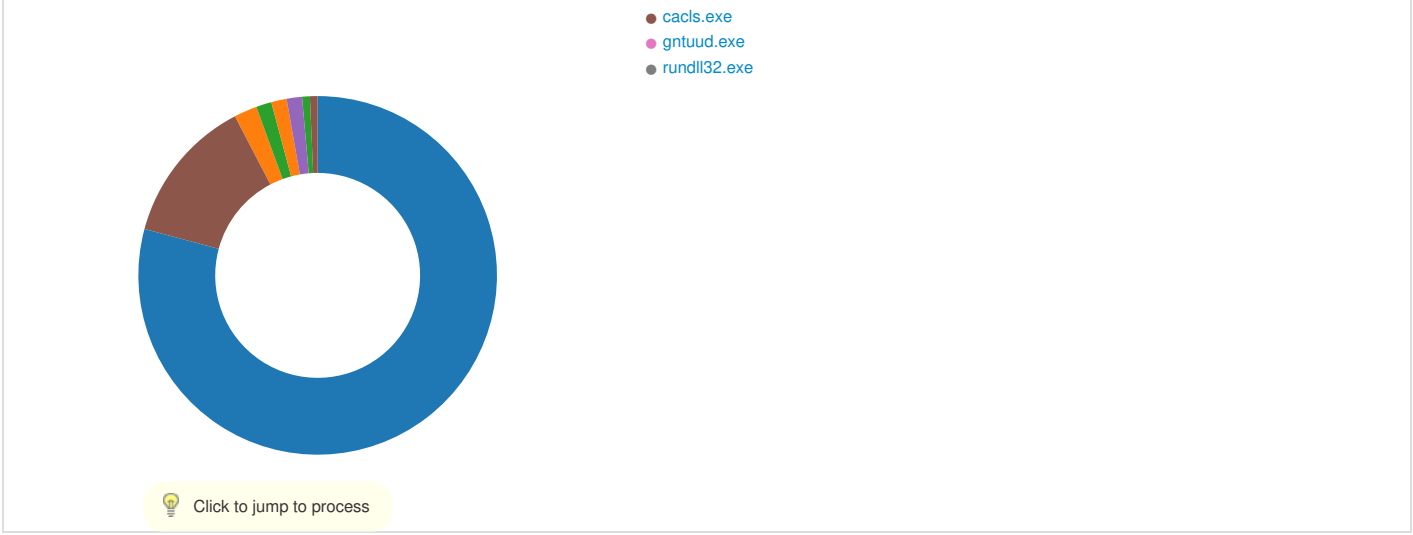
Language of compilation system	Country where language is spoken	Map
Polish	Poland	
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: 5GPueTFF2S.exe PID: 5848, Parent PID: 3528

General

Target ID:	0
Start time:	10:39:00
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\5GPueTFF2S.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\5GPueTFF2S.exe
Imagebase:	0xec0000
File size:	1493440 bytes
MD5 hash:	7D124BC23BE85D73B1177143F41B5E72
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000000.00000003.420692753.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.432090196.000000000B0A5000.00000002.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000000.00000002.423403008.0000000000A31000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000003.387953405.000000000B070000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: 75873290272674793137.exe PID: 6132, Parent PID: 5848

General

Target ID:	1
Start time:	10:39:50
Start date:	09/12/2022
Path:	C:\ProgramData\75873290272674793137.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\75873290272674793137.exe"

Imagebase:	0xf70000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
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: 00000001.00000002.445175041.0000000000F71000.00000020.00000001.01000000.00000006.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\03bd543fce	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F7B6F6	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	F7B852	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe	0	524288	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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 58 48 fd fd 36 1b fd fd 36 1b fd fd 36 1b fd fd 35 1a fd fd 36 1b fd fd 33 1a 61 fd 36 1b fd fd 32 1a fd fd 36 1b 28 fd 32 1a fd fd 36 1b 28 fd 35 1a fd fd 36 1b 28 fd 33 1a fd fd 36 1b fd fd 37 1a fd fd 36 1b fd fd 37 1b 5c fd 36 1b 66 fd 3f 1a fd fd 36 1b 66 fd fd 1b fd fd 36 1b 66 fd 34 1a fd fd 36 1b 52 69 63 68 fd fd 36 1b 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08	MZ@!L!This program cannot be run in DOS mode.$XH666563a626(26(56(36767\6f?6f6f46Rich6PEL	success or wait	15	F7B852	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5576**, Parent PID: **5848**

General

Target ID:	4
Start time:	10:39:56
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\5GPueTFF2S.exe" & exit
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\5GPueTFF2S.exe	cannot delete	1	DB0374	DeleteFileW
C:\Users\user\Desktop\5GPueTFF2S.exe	cannot delete	1	DB0374	DeleteFileW

Analysis Process: conhost.exe PID: **5652**, Parent PID: **5576**

General

Target ID:	5
Start time:	10:39:56
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: timeout.exe PID: **3216**, Parent PID: **5576**

General

Target ID:	6
Start time:	10:39:56
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0x1140000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: gntuud.exe PID: **5292**, Parent PID: **6132**

General

Target ID:	7
Start time:	10:40:04
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe"
Imagebase:	0xa0000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000007.00000003.483002099.0000000001165000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\c33e9ad058e5d3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	B199C	CreateDirectoryA
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A8BC2	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	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	A9D90	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	14	BF6D5	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\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 fd 00 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 50 45 00 00 4c 01 09 00 19 5e 42 2a 00 00 00 00 00 00 00 00 fd 00 fd fd 0b 01 02 19 00 fd 01 00 00 58 00 00 00 00 00 00 fd fd fd 00 00 10 00 00 00 fd 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 fd fd 00 00 04 00 00 2a fd 75 00 02 00 01 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 2c fd 00 4f 00 00	MZP@!L!This program must be run under Win32$7PEL^B*X@*u,O	success or wait	471	A8C27	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cred64[1].dll	16384	16384	fd fd fd 02 fd fd 40 7a 6c fd fd 00 37 20 3d fd 6d fd 78 fd 00 fd 15 0c 11 fd 6d 69 fd 2c fd fd fd 9d 22 23 7e 7f fd fd 1c 00 64 58 1e fd fd fd 70 09 7d 7f fd 47 ce 00 0e fd 1e 7c fd 6f fd 7e fd fd 78 fd fd fd 27 13 fd fd fd fd 23 76 51 7f fd 39 54 63 fd 32 fd 1b 74 7f fd 4f fd 00 0e fd 26 fd fd 0b 3a 31 77 7f 01 75 fd 00 04 fd 26 76 fd 77 15 fd 74 fd 1f fd fd 74 fd fd 1c 3a fd 77 fd fd fd 8b fd 35 57 47 c9 fd fd 2c 64 17 fd 41 23 43 0c fd 5d 33 fd 2d fd fd 24 33 fd 5c fd fd fd f6 fd 2b fd fd 15 10 3c fd 76 77 fd 36 fd fd 03 fd 11 fd 50 fd 6c fd 2b fd 22 7a 09 4d fd 25 6e 33 fd 44 fd fd fd 75 fd fd 30 fd 49 34 fd fd 29 5f 75 fd fd 5c fd 48 61 33 0e d0 fd fd 4a fd fd 4d 73 fd 34 fd 7c 33 27 fd 49 fd fd 61 5d 5d	@zl7=mxmi,#~dXp}G|~x' #vQ9Tc2tO &:1wu&vwtt:w5WG,dA#C]3-$3\+<vw 6PI+"zM%n3D0I4)_u\Ha3 JMs4|3'a]]	success or wait	464	A8C36	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	99484	A9757	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\03bd543fce\	success or wait	1	A2F97	RegSetValueExA

Analysis Process: schtasks.exe PID: **5724**, Parent PID: **5292**

General

Target ID:	8
Start time:	10:40:17
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\03bd543fce\gntuud.exe" /F
Imagebase:	0x11e0000
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: **5768**, Parent PID: **5724**

General	
Target ID:	9
Start time:	10:40:17
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: cmd.exe PID: **3644**, Parent PID: **5292**

General	
Target ID:	10
Start time:	10:40:17
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\03bd543fce" /P "user:N"&&CACLS "..\03bd543fce" /P "user:R" /E&&Exit
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: **2160**, Parent PID: **3644**

General	
Target ID:	11
Start time:	10:40:17
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61e220000
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: cmd.exe PID: **4628**, Parent PID: **3644**

General	
Target ID:	12
Start time:	10:40:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: cacls.exe PID: **3856**, Parent PID: **3644**

General	
Target ID:	13
Start time:	10:40:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:N"
Imagebase:	0x1200000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	12049CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	16	12049CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **4760**, Parent PID: **3644**

General	
Target ID:	14
Start time:	10:40:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true

Commandline:	CACLS "gntuud.exe" /P "user:R" /E
Imagebase:	0x1200000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	16	12049CC	fprintf

Analysis Process: cmd.exe PID: **4384**, Parent PID: **3644**

General

Target ID:	15
Start time:	10:40:19
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cacls.exe PID: **5932**, Parent PID: **3644**

General

Target ID:	16
Start time:	10:40:19
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:N"
Imagebase:	0x1200000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	12049CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	15	12049CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: 4532, Parent PID: 3644

General

Target ID:	17
Start time:	10:40:19
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:R" /E
Imagebase:	0x1200000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	15	12049CC	fprintf

Analysis Process: gntuud.exe PID: 5956, Parent PID: 1088

General

Target ID:	18
Start time:	10:40:20
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Imagebase:	0xa0000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
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: 00000012.00000002.518241260.00000000000A1000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5968, Parent PID: 5292

General

Target ID:	19
Start time:	10:40:22
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll, Main
Imagebase:	0xf10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Disassembly

No disassembly