

ID: 764037
Sample Name: q3oUuJIXkc.exe
Cookbook: default.jbs
Time: 10:52:09
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report q3oUuJIXkc.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Amadey 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 5
Persistence and Installation Behavior 5
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 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
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\2WF3MMUU\cred64[1].dll 12
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe 12
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe:Zone.Identifier 13
C:\Users\user\AppData\Local\Temp\853321935212 13
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll 13
\Device\ConDrv 14
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Authenticode Signature 15
Entrypoint Preview 15
Data Directories 16
Sections 17
Resources 17
Imports 18
Possible Origin 18

Network Behavior 18
Statistics 18
Behavior 18
System Behavior 19
Analysis Process: q3oUuJlXkc.exePID: 1780, Parent PID: 3528 19
General 19
File Activities 19
Analysis Process: gntuud.exePID: 5280, Parent PID: 1780 19
General 19
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: 1128, Parent PID: 5280 21
General 21
File Activities 22
Analysis Process: conhost.exePID: 1592, Parent PID: 1128 22
General 22
Analysis Process: cmd.exePID: 2188, Parent PID: 5280 22
General 22
File Activities 22
Analysis Process: conhost.exePID: 5164, Parent PID: 2188 23
General 23
Analysis Process: cmd.exePID: 4216, Parent PID: 2188 23
General 23
File Activities 23
Analysis Process: cacls.exePID: 1844, Parent PID: 2188 23
General 23
File Activities 24
File Written 24
Analysis Process: cacls.exePID: 5132, Parent PID: 2188 24
General 24
File Activities 24
File Written 24
Analysis Process: cmd.exePID: 4768, Parent PID: 2188 24
General 24
Analysis Process: cacls.exePID: 5412, Parent PID: 2188 24
General 24
File Activities 25
File Written 25
Analysis Process: cacls.exePID: 5344, Parent PID: 2188 25
General 25
File Activities 25
File Written 25
Analysis Process: gntuud.exePID: 2468, Parent PID: 1088 25
General 25
Analysis Process: rundll32.exePID: 4828, Parent PID: 5280 26
General 26
Disassembly 26

Copyright Joe Security LLC 2022

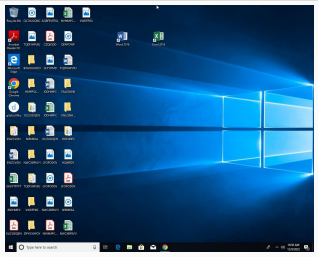
Windows Analysis Report

q3oUuJIXkc.exe

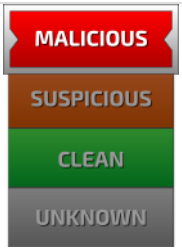
Overview

General Information

Sample Name:	q3oUuJIXkc.exe
Analysis ID:	764037
MD5:	2239a58cc93fd9…
SHA1:	f09eb7d69bc744..
SHA256:	682abd62b6e3c0..
Tags:	32 exe trojan
Infos:	



Detection



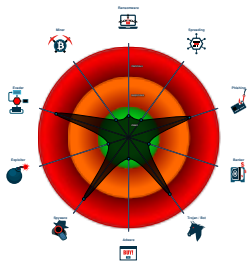
Amadey

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

Signatures

- Yara detected Amadeys stealer DLL
- Multi AV Scanner detection for subm…
- Yara detected Amadey bot
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Hides threads from debuggers
- Tries to steal Mail credentials (via fi…
- Overwrites code with unconditional j…
- Overwrites code with function prolog…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- q3oUuJIXkc.exe (PID: 1780 cmdline: C:\Users\user\Desktop\q3oUuJIXkc.exe MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
  - gntuud.exe (PID: 5280 cmdline: "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
    - schtasks.exe (PID: 1128 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: 1592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 2188 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: 5164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 4216 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cacls.exe (PID: 1844 cmdline: CACLS "gntuud.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
      - cacls.exe (PID: 5132 cmdline: CACLS "gntuud.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
      - cmd.exe (PID: 4768 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cacls.exe (PID: 5412 cmdline: CACLS "..\03bd543fce" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
      - cacls.exe (PID: 5344 cmdline: CACLS "..\03bd543fce" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
    - rundll32.exe (PID: 4828 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- gntuud.exe (PID: 2468 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"
}
```

Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.315315946.0000000000071000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0000000C.00000002.379083563.0000000001281000.00000020.00000001.01000000.00000004.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000001.00000003.350752206.0000000000EAD000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
Process Memory Space: gntuud.exe PID: 5280	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.gntuud.exe.1280000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.2.q3oUuJlXkc.exe.70000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking



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

C2 URLs / IPs found in malware configuration

System Summary



PE file contains section with special chars

Persistence and Installation Behavior



Yara detected Amadey bot

Copyright Joe Security LLC 2022

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

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

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

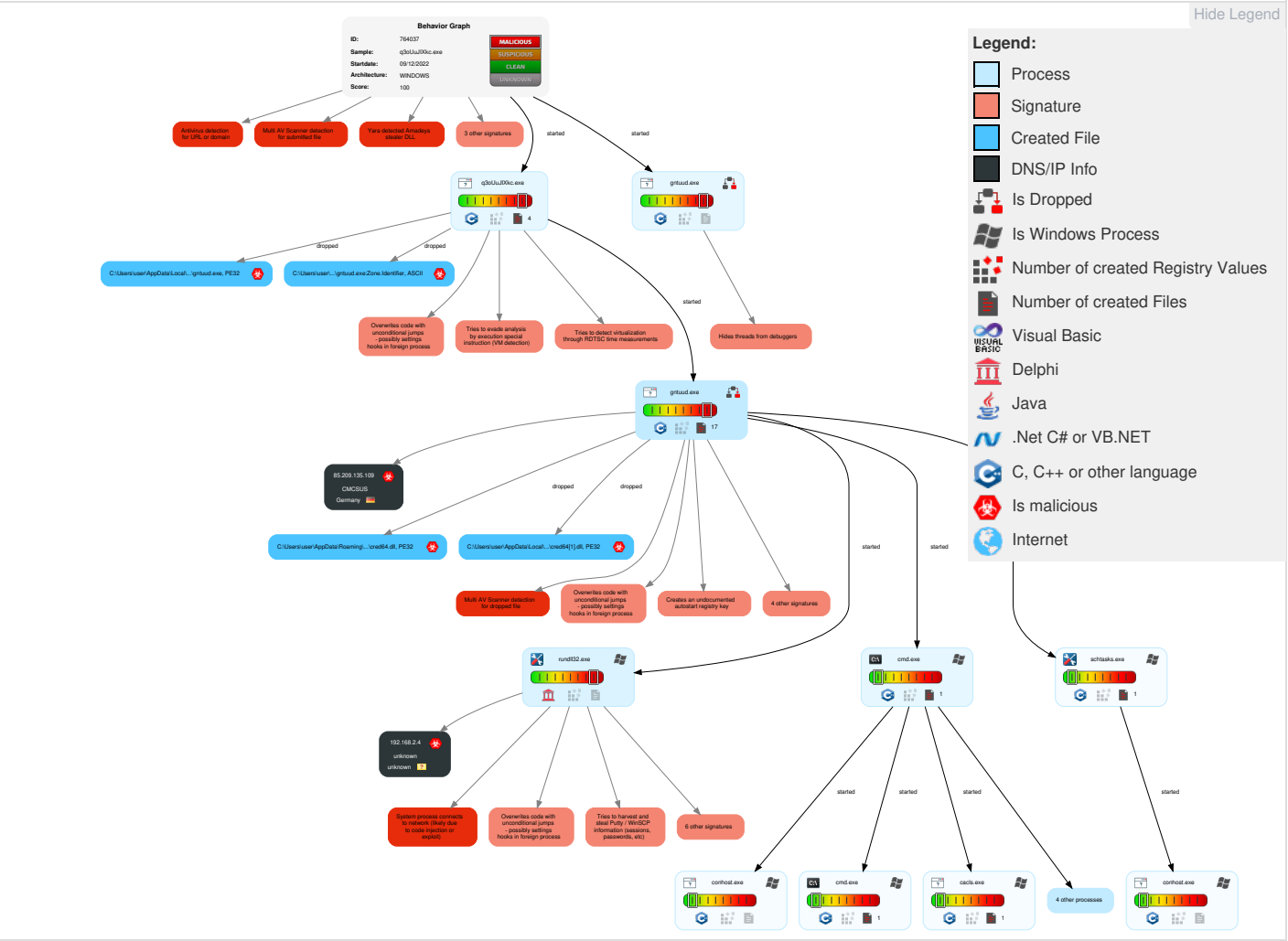
Tries to steal Instant Messenger accounts or passwords

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 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	4 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 3 1 Virtualization/Sandbox Evasion	1 Credential API Hooking	1 Process Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Services File Permissions Weakness	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Input Capture	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Input Capture	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 Obfuscated Files or Information	2 Credentials in Registry	1 File and Directory Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Services File Permissions Weakness	1 Credentials In Files	2 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Behavior Graph

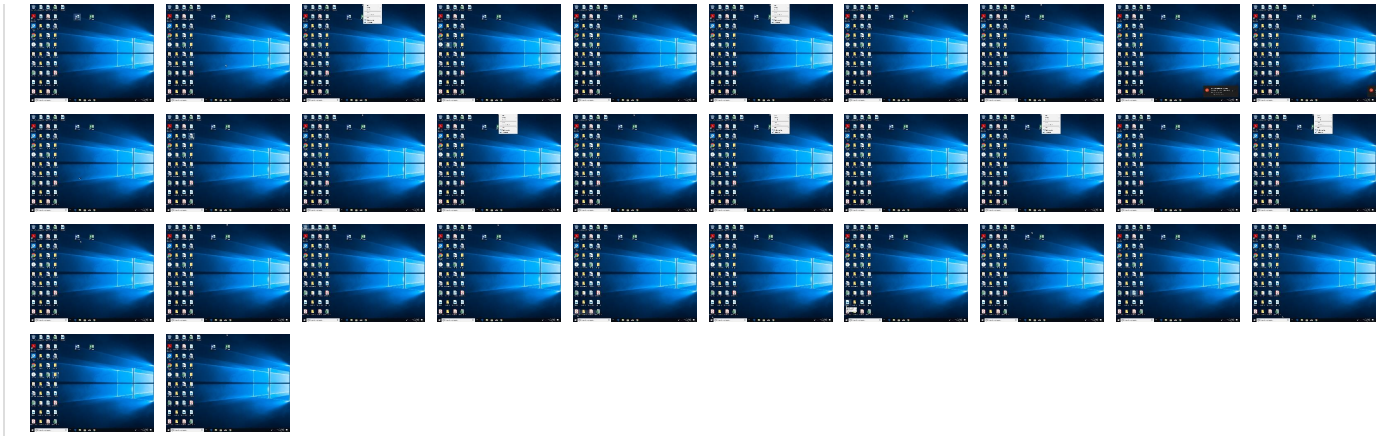


Screenshots

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
q3oUuJIXkc.exe	15%	Virustotal		Browse
q3oUuJIXkc.exe	35%	ReversingLabs	Win32.Trojan.Amadey	

Copyright Joe Security LLC 2022

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cred64[1].dll	12%	ReversingLabs		
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

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://85.209.135.109/jg94cVd30f/index.phpj	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.phpF	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.php	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.php?scr=1	100%	Avira URL Cloud	malware	
http://85.209.135.109/jg94cVd30f/index.phpb	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.phpd3	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.php58e5d3	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.phpz	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.phpv	0%	Avira URL Cloud	safe	
85.209.135.109/jg94cVd30f/index.php	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.php0	0%	Avira URL Cloud	safe	
http://85.209.135.109/jg94cVd30f/index.phpR	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

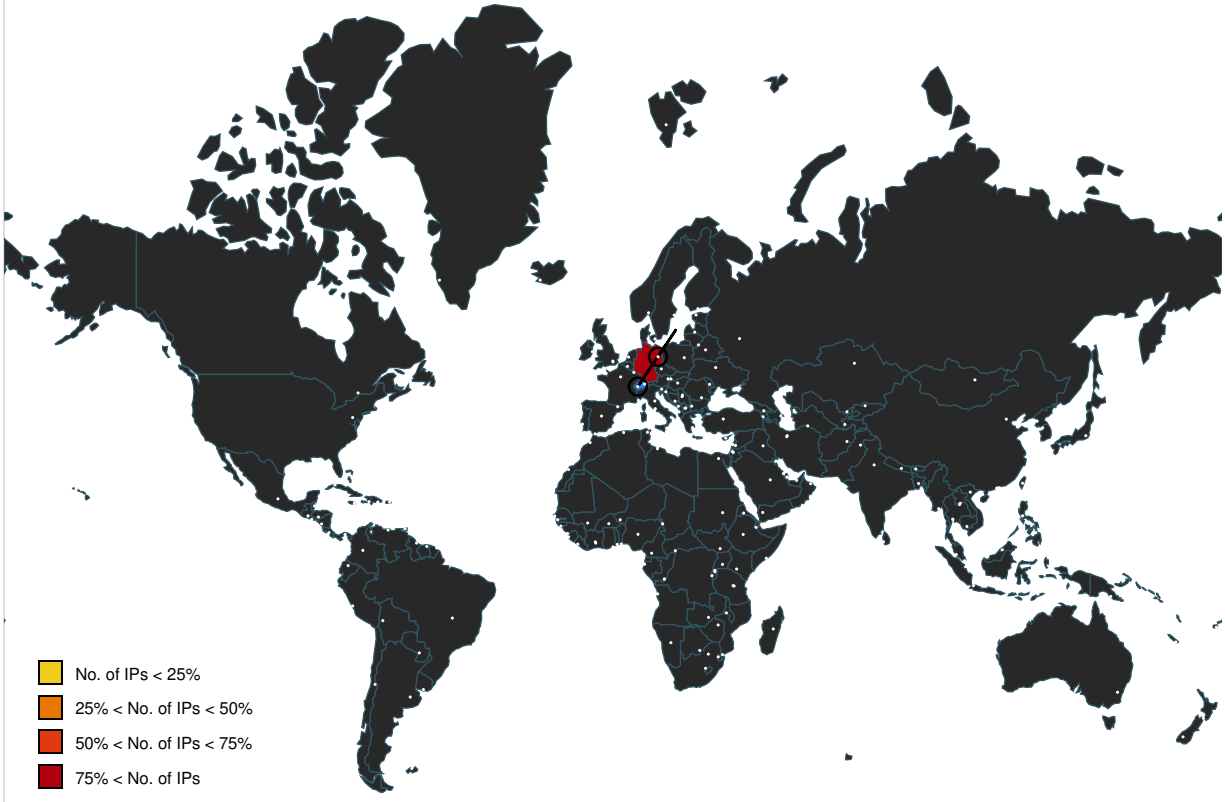
Name	Malicious	Antivirus Detection	Reputation
85.209.135.109/jg94cVd30f/index.php	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	q3oUuJlXkc.exe, gntuud.exe.0.dr, cred64[1].dll.1.dr, cred64.dll.1.dr	false	• URL Reputation: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpj	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	q3oUuJlXkc.exe, gntuud.exe.0.dr, cred64[1].dll.1.dr, cred64.dll.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://85.209.135.109/jg94cVd30f/index.php	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000001.00000003.350805710.0000000000EC8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	q3oUuJIXkc.exe, gntuud.exe.0.dr, cred64[1].dll.1.dr, cred64.dll.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpF	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.php?scr=1	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	q3oUuJIXkc.exe, gntuud.exe.0.dr, cred64[1].dll.1.dr, cred64.dll.1.dr	false	• URL Reputation: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpb	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.php58e5d3	gntuud.exe, 00000001.00000003.350805710.0000000000EC8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpd3	gntuud.exe, 00000001.00000003.350805710.0000000000EC8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpz	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpv	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.phpR	gntuud.exe, 00000001.00000003.350729543.0000000000EE6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://85.209.135.109/jg94cVd30f/index.php0	gntuud.exe, 00000001.00000003.350805710.0000000000EC8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.209.135.109	unknown	Germany		33657	CMCSUS	true

Copyright Joe Security LLC 2022

Private

IP
192.168.2.4

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764037
Start date and time:	2022-12-09 10:52:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	q3oUuJIXkc.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@24/9@0/2
EGA Information:	Failed
HDC Information:	Failed
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
- Execution Graph export aborted for target rundll32.exe, PID 4828 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:53:18	API Interceptor	2546x Sleep call for process: gntuud.exe modified
10:53:19	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:\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\Temp\03bd543fce\gntuud.exe

Process:	C:\Users\user\Desktop\q3oUuJIXkc.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:Zone.Identifier

Process:	C:\Users\user\Desktop\q3oUuJIXkc.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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):	106755
Entropy (8bit):	7.930938749687084
Encrypted:	false
SSDEEP:	1536:C+HaFexHpq4LV97q5wQq23vv5C4bndDT4vSxJu0VdNjEfYcnF4MXRWNt9bsdjogU:xt/q4xlnQqF0VrX5XrMXWAksu6rGu01
MD5:	BC1FA342F0AE360EA815BF64C71D503E
SHA1:	929ACB54CBF1E6B6C495A8768F694804FA0ECED1
SHA-256:	5722B2526976E9C37277C435D09080C9CEBA052922B306A694D4EA0CCB1ABDFA
SHA-512:	1F1065173E96BCEF16F0E40FE90A8B35372C15CB59453CB3DBF130A9E20B7DEF1CAAF741146643D6ADF8F662566D9120284F1D2BB19420B8DFA32A67A489847
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222

\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):	7.8779499305543865
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:	q3oUuJIXkc.exe
File size:	7732440
MD5:	2239a58cc93fd94dc2806ce7f6af0a0b
SHA1:	f09eb7d69bc7440d3d45e14267236a78ac789fcb
SHA256:	682abd62b6e3c0e8ca57f079cd96f2d3848752eaf7002bdf57bfb512bd242811
SHA512:	f77c16626a0e17ff79b95f9fded6a365f913896c89baf76d16bcc8706f3ad10a9476c7cbd3f235250b936171c6e958e145c402952506dc0e434a4f911c99fe02
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
TLSH:	C57623B3A3B41145C1D0CD3D9537AFA473F18FA7CB422A36658DB9C618721F4E622A87
File Content 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..

File Icon



Icon Hash:	78c09ace96cee071

Static PE Info

General

Entrypoint:	0x9546db
Entrypoint Section:	EVjKc_MI
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:	0x639036D5 [Wed Dec 7 06:46:45 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0

Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	a09599f99e4c72911ae32fe016ed9145

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=luminous company
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/8/2022 1:47:11 AM 12/8/2023 2:07:11 AM
Subject Chain	• CN=luminous company
Version:	3
Thumbprint MD5:	48B0126BEA96E72E0ACAF9BF22EFD655
Thumbprint SHA-1:	9CC7CA44B6A43D98C0CFE0845AB97B6AB08694BA
Thumbprint SHA-256:	5E29C591440A557F3A7B7CAB7BA338B2C19D4BC16CFC917BFAAAC0804627E3EE
Serial:	4E9D6FD78307E6AD4C5583A2D9753AE2

Entrypoint Preview
Instruction
push edx
mov edx, 006C25E2h
push ecx
call 00007F02DD1E4FEEh
stc
rol al, 1
neg al
cmovnl edx, ebx
mov edx, ebp
not al
rol al, 1
xor bl, al
mov word ptr [esp+eax], cx
stc
lea edi, dword ptr [edi-00000004h]
sal dx, cl
mov edx, dword ptr [edi]
cmp ah, 00000053h
xor edx, ebx
stc
cmc
clc
not edx
cmc
clc
rol edx, 1
test bp, 1AA8h
cmp esi, eax
test ebx, ebp
neg edx
jmp 00007F02DCFA5223h
inc ecx
rol ecx, 1
cmp ebx, esp
test dh, dh
add ecx, 32723618h
clc
cmc
test esp, 3E02325Eh
xor ebx, ecx
cmp ecx, ecx

Instruction
jmp 00007F02DD0474D4h
dec ebp
mov ebx, dword ptr [edx]
dec eax
movzx ecx, bp
inc ecx
mov edi, dword ptr [edx+08h]
dec eax
cmp ebx, esi
inc cx
sub ecx, ebp
clc
dec ecx
add edx, 0000000Ch
inc ecx
mov dword ptr [ebx], edi
jmp 00007F02DD1C6408h
inc cx
movzx edi, byte ptr [edx]
inc ebp
mov cl, byte ptr [edx+02h]
cmp ch, 00000015h
jmp 00007F02DD1BF94Eh
jne 00007F02DD0914E6h
pop ebx
not edx
btc eax, 51h
dec al
mov dword ptr [esi], edx
lea ebp, dword ptr [ebp-00000004h]
mov eax, dword ptr [ebp+00h]
stc
cmc
xor eax, ebx
neg eax
dec eax
jmp 00007F02DD1F6924h
xor al, bl
clc
jmp 00007F02DD0583F4h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x70adbc	0xdc	EVjKc_MI
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb16000	0x66360	@]topACL
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x75e600	0x16d8	EVjKc_MI
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb15000	0x610	dT<:EHzj
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb14530	0x70	EVjKc_MI
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb14120	0x40	EVjKc_MI
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x41c000	0x68	CV?7x>JO
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Copyright Joe Security LLC 2022

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
lB@dO\ih	0x1000	0x2df16	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
Fh?jG[OJ	0x2f000	0x9c4c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
qNR5:WbS	0x39000	0x444c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
z?fd8ijJ	0x3e000	0x3ddf68	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
CV?7x>JO	0x41c000	0x5cc	0x600	False	0.057291666666666664	data	0.36065717947425463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
EVjKc_MI	0x41d000	0x6f77a0	0x6f7800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
dT<:EHzj	0xb15000	0x610	0x800	False	0.40869140625	data	3.500908726389375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
@]topACL	0xb16000	0x66360	0x65c00	False	0.2412133369164619	data	3.398442344823821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb165c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_ICON	0xb16a30	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0xb173b8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0xb18460	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0xb1aa08	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0xb1ec30	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0xb240b8	0x67e8	Device independent bitmap graphic, 80 x 160 x 32, image size 25600	English	United States
RT_ICON	0xb2a8a0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0xb33d48	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0xb44570	0x47e5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0xb48d58	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_ICON	0xb491c0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0xb49b48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0xb4abf0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0xb4d198	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0xb513c0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0xb56848	0x67e8	Device independent bitmap graphic, 80 x 160 x 32, image size 25600	English	United States
RT_ICON	0xb5d030	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0xb664d8	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0xb76d00	0x47e5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xb7ba5c	0x7e	data	English	United States
RT_DIALOG	0xb7badc	0xa8	data	English	United States
RT_DIALOG	0xb7bb84	0x114	data	English	United States
RT_DIALOG	0xb7bc98	0x6c8	empty	English	United States
RT_GROUP_ICON	0xb7b4e8	0x92	data	English	United States
RT_GROUP_ICON	0xb7b57c	0x92	data	English	United States
RT_VERSION	0xb7b610	0x2cc	data	English	United States
RT_MANIFEST	0xb7b8dc	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetVersionExW
USER32.dll	GetSystemMetrics
GDI32.dll	CreateCompatibleBitmap
ADVAPI32.dll	RegCloseKey
SHELL32.dll	ShellExecuteA
WININET.dll	HttpOpenRequestA
gdiplus.dll	GdipSaveImageToFile
KERNEL32.dll	GetSystemTimeAsFileTime
USER32.dll	CharUpperBuffW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress

Possible Origin

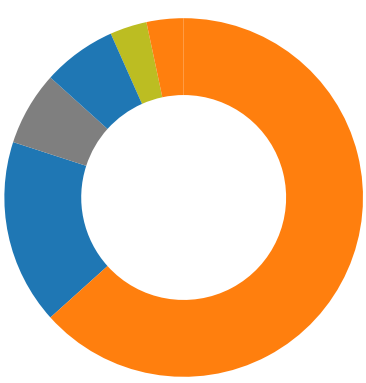
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- q3oUuJIXkc.exe
- gntuud.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- conhost.exe
- cmd.exe
- cacls.exe
- cacls.exe
- cmd.exe
- cacls.exe
- cacls.exe
- gntuud.exe
- rundll32.exe

Click to jump to process

System Behavior

Analysis Process: q3oUuJIXkc.exe PID: 1780, Parent PID: 3528

General

Target ID:	0
Start time:	10:52:59
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\q3oUuJIXkc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\q3oUuJIXkc.exe
Imagebase:	0x70000
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: 00000000.00000002.315315946.0000000000071000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: gntuud.exe PID: 5280, Parent PID: 1780

General

Target ID:	1
Start time:	10:53:07
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:	0x1280000
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: 00000001.00000003.350752206.0000000000EAD000.00000004.00000020.00020000.00000000.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	129199C	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	1288BC2	CreateFileA

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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	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	1289D90	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	12	129F6D5	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

Target ID:	2
Start time:	10:53:17
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:	0x1340000
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: 1592, Parent PID: 1128

General

Target ID:	3
Start time:	10:53:17
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: 2188, Parent PID: 5280

General

Target ID:	4
Start time:	10:53:17
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: 5164, Parent PID: 2188

General

Target ID:	5
Start time:	10:53:17
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: 4216, Parent PID: 2188

General

Target ID:	6
Start time:	10:53:17
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: 1844, Parent PID: 2188

General

Target ID:	7
Start time:	10:53:17
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:N"
Imagebase:	0x1270000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

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	12749CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	16	12749CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **5132**, Parent PID: **2188**

General

Target ID:	8
Start time:	10:53:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:R" /E
Imagebase:	0x1270000
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	12749CC	fprintf

Analysis Process: cmd.exe PID: **4768**, Parent PID: **2188**

General

Target ID:	9
Start time:	10:53:18
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

Analysis Process: cacls.exe PID: **5412**, Parent PID: **2188**

General

Target ID:	10
Start time:	10:53:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:N"
Imagebase:	0x1270000
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	12749CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	15	12749CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **5344**, Parent PID: **2188**

General

Target ID:	11
Start time:	10:53:18
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:R" /E
Imagebase:	0x1270000
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	12749CC	fprintf

Analysis Process: gntuud.exe PID: **2468**, Parent PID: **1088**

General

Target ID:	12
Start time:	10:53:19
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

Copyright Joe Security LLC 2022

Imagebase:	0x1280000
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: 0000000C.00000002.379083563.0000000001281000.00000020.00000001.01000000.00000004.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **4828**, Parent PID: **5280**

General	
Target ID:	13
Start time:	10:53:22
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:	0xd30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Disassembly

No disassembly