CrackedCantil: Malware Work Together

By Lena aka LambdaMamba

Archived: 2026-04-05 18:29:01 UTC

Lena aka LambdaMamba

I am a Chief Research Officer at a cybersecurity company. My passions include investigations, experimentations, gaming, writing, and drawing. I also like playing around with hardware, operating systems, and FPGAs. I enjoy assembling things as well as disassembling things! In my spare time, I do CTFs, threat hunting, and write about them. I am fascinated by snakes, which includes the Snake Malware!

Check out:

- My website
- My LinkedIn profile

Malware is constantly evolving to become more evasive, destructive, efficient, and infectious. There are numerous families of malware, each with its own unique characteristics. These different families of malware can work together in a symphonious manner to deliver a powerful infection. For instance, the stealer malware can exfiltrate data before the ransomware encrypts the files.

In this blog post, we're diving into a recent case of something I started calling a "malware symphony." It's a way to describe how different types of malware can work together, sort of like instruments in an orchestra. And just like how each instrument adds to the harmony, these malware parts work together in a coordinated way — we'll explore the behavior of each malware involved in this symphony in detail.

Let's dive right into it!

Overview of CrackedCantil

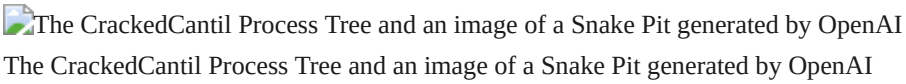
The author (of this article, not the malware), Lena (aka LambdaMamba) has decided to name this type of malware the "**CrackedCantil**".

The "Cracked" part comes from cracked software meaning a common vector of infection. The "Cantil" part comes from the Cantil Viper, which is a species of highly venomous viper. This viper uses its bright yellow tail to lure in prey, just like how this malware uses cracked software to lure in victims.

And just like viper venom, which uses a complex cocktail of chemicals that work together to wreak havoc in the victim's body, numerous malware work together in the CrackedCantil to wreak havoc in the victim's system. The CrackedCantil examined in this article includes the following:

- Loaders: Includes the PrivateLoader and Smoke, which drops more malware onto the system
- Infostealers: Includes the Lumma, RedLine, RisePro, Amadey, Stealc, which steals sensitive information
- Crytominers: Turns the infected system into a cryptominer, which drains system resources
- Proxy Bot Malware: Includes the Socks5Systemz, which turns the infected system into a proxy bot
- Ransomware: Includes the STOP, which encrypts the files and disrupts the system

Also, the process tree is long, packed, and intertwined like a snake pit.

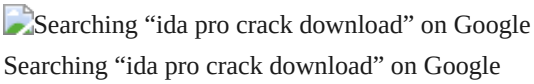

The CrackedCantil Process Tree and an image of a Snake Pit generated by OpenAI

Analyzing the behavior in a sandbox

The CrackedCantil ANY.RUN sample examined in this article can be found here. Additionally, the analysis techniques introduced in my blog Analyzing Snake Keylogger in ANY.RUN: a Full Walkthrough will be used here.

Searching for the Cracked software

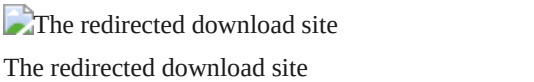
The query "ida pro crack download" was searched on Google on a Windows 11 Google Chrome using a United States Residential Proxy. There was a peculiar Google Groups result "CRACK IDA Pro V6 8 150423 And HEX-Rays Decompiler …" within the first search result page:


Searching "ida pro crack download" on Google

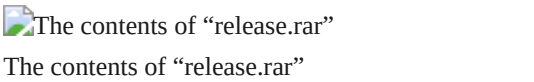
Visiting the Google Groups search result showed a Google Groups conversation with the subject "CRACK IDA Pro V6 8 150423 And HEX-Rays Decompiler ARM X86 X64-iDAPROl". A shortened link is included in the body:


A Google Groups conversation with a download link

Clicking on the shortened link redirects to *hxxps://airfiltersing[.]com.…* , and Clicking on the "Download" button will download "release.rar" from *hxxps://afashionstudio[.]com*:

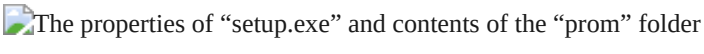

The redirected download site

The archive file is password-protected and can be opened with the password provided on the download site, which was "1234". A folder called "prom" and an application called "setup.exe" are inside the archive. These were extracted onto the Desktop:


The contents of "release.rar"

The details of "setup.exe" can be seen in the Properties. The file description was "Logitech PlugIn Installer Utility (UNICODE)", and the original filename was "PlugInInstallerUtility.exe". The folder "prom" contains various files with

unique extensions, such as “.dllqqq”, “.dllew”, “.dllw”, “.dlww”:


The properties of “setup.exe” and contents of the “prom” folder

Running the Cracked Software

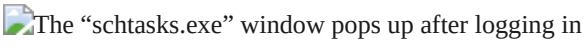
Double-clicking on “setup.exe” will execute the application. Around a minute after executing “setup.exe”, a bunch of processes is spawned, and “cmd.exe” and “schtasks.exe” windows pop up:


The “cmd.exe” and “schtasks.exe” windows pop up after executing “setup.exe”

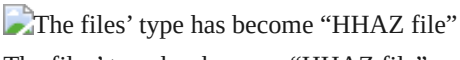
After “cmd.exe” and “schtasks.exe” closes, nothing alarming happens from the user’s perspective. The system is manually restarted for experimentation. The system restarts normally from the user’s perspective, and logins to “admin”.


Logging into “admin” after manual system reboot

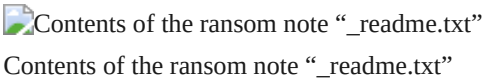
After the login, everything on the Desktop looks normal from the user’s perspective. Approximately 15 seconds later, a “schtasks.exe” window pops up and a bunch of processes are spawned:


The “schtasks.exe” window pops up after logging in

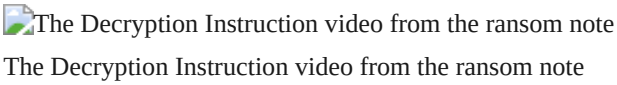
A few seconds later, the files’ icons change to a white file icon, and the “.hhaz” extension is added to the files, indicating they were encrypted:


The files’ type has become “HHAZ file”

The ransom note is located in “C:\Users\admin_readme.txt”. The ransom note includes a link to download the decryption instruction video, the contact email, and a personal ID:


Contents of the ransom note “_readme.txt”

In a different ANY.RUN task, the WeTransfer link was opened in a browser, and the”Decrypt Software.avi” was downloaded and opened in a Video player. It showed a decryption instruction video with a “.djvuu” example:


The Decryption Instruction video from the ransom note

Analyzing the Processes based on Malware Family

The process tree is complex, and numerous notorious malware families were involved. This section will break down the different malware families involved and explore each one in detail. They include PrivateLoader, Smoke, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, and STOP.

PrivateLoader

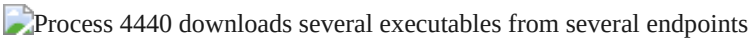
PrivateLoader is a malicious loader family first identified in 2021 and is known for distributing many kinds of malware including stealers, rootkits, spyware, and more. It is written in C++, and cracked software is a common source of infection. Additionally, it drops payloads depending on the configuration of the victim's system. More information on PrivateLoader can be found in ANY.RUN's PrivateLoader Malware Trends.

Process 4440: setup.exe

The process "setup.exe" (process 1952) starts when the "setup.exe" executable is double-clicked from the Desktop. Almost immediately after, another process called "setup.exe" (process 4440) spawns, and is detected as a PrivateLoader. From Process 4440, numerous malicious processes spawn, which includes more PrivateLoader instances, Smoke, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, and STOP.


The "setup.exe" (process 4440) is detected as a PrivateLoader

Numerous executables are downloaded by "setup.exe" (process 4440) from several endpoints. Detonating these executables independently inside the ANY.RUN Sandbox revealed that they are Stealc (timeSync.exe ANY.RUN task), Redline (autorun.exe ANY.RUN task), Risepro (good.exe ANY.RUN task), and Sock5Systemz (adobe.exe ANY.RUN task).


Process 4440 downloads several executables from several endpoints

Process 4440 is also seen communicating with its C2 server, 185[.]216.70.235 and 195.20.16[.]45 via port 80 (T1071 – Application Layer Protocol). HTTP requests *"/api/tracemap.php"* and *"/api/firegate.php"* were made to the host 185[.]216.70.235 and 195.20.16[.]45 by Process 4440:


The HTTP requests by Process 4440

An example network stream between 195.20.16[.]45:80 and VM:52634 can be seen below:


The *Network Stream* for Process 4440 between 195.20.16[.]45:80 and VM:52634

The contents include Base64-encoded strings, like "*Q0uWGgHyOK1yWQK-BXHkM-HySJVrM-bkDRjaZRMVle11OCvYaPf2WzR9nGuLpCPzAv8ibLyhynT0DqT5CPejzN_j4vkuL4Rmafqdqg7q29RNzn9VOTArbMt6Jrq5lsZ3*", but decoding these strings did not reveal human-readable results. These strings are encrypted, and decrypting may reveal the C2 server and other crucial information as shown in PrivateLoader: Analyzing the Encryption and Decryption of a Modern Loader.

Process 5088: vRNddZqIkwaYVpHLFkGcr1Tk.exe

The initial PrivateLoader "setup.exe" (process 4440) spawns "vRNddZqIkwaYVpHLFkGcr1Tk.exe" (process 5088), which is also detected as PrivateLoader.


The "setup.exe" (process 4440) > "vRNddZqIkwaYVpHLFkGcr1Tk.exe" (process 5088) is detected as a PrivateLoader.
The "setup.exe" (process 4440)

The “vRNddZqIkwaYVpHLFkGcr1Tk.exe” (process 5088) was seen modifying files in the Chrome extension folder. Browser extensions can be abused to establish persistent access to systems (T1176 – Browser Extensions).


Process 5088 is seen modifying files in the Chrome extension folder

The extension “difpelfbkngealhghppkgcpkgbgohhph” is associated with K Searches. According to the K Searches description, “The extension will update your search settings and will change your new tab search provider to Microsoft Bing”. Opening Google Chrome on a different ANY.RUN task after detonating “setup.exe” showed the K Searches extension being added to the browser:


The K Searches extension on a Chrome Browser

Process 5088 also communicates with its C2, 195.20.16[.]45 via port 80 (T1071 – Application Layer Protocol), and the HTTP POST requests also contain Base64 encoded and encrypted strings just like Process 4440:


The *Network Stream* for Process 5088 between 195.20.16[.]45:80 and VM:53329

Process 1916: wlC578T8hWfvZ2yJxLzrF38Y.exe

The initial PrivateLoader “setup.exe” (process 4440) spawns “wlC578T8hWfvZ2yJxLzrF38Y.exe” (process 1916), which is also detected as PrivateLoader.

The “setup.exe” (process 4440)

Process 1916 was seen dropping executables “C:\Users\admin\Pictures\Minor Policy\5RfuRxo3fpxiWkD42DRCixRe[.]exe” and “C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\J0KBFYBW\build2[1].exe”. These two executables have the same hash, and “5RfuRxo3fpxiWkD42DRCixRe[.]exe” is examined in a later section, which is detected as Amadey.


Process 1916 drops executable files immediately after the start

Process 5088 also communicates with its C2, 45.15.156[.]229 via port 80 (T1071 – Application Layer Protocol). Similar to Process 4440 and Process 5088, the HTTP POST requests also contain Base64 encoded and encrypted strings:


The *Network Stream* for Process 1916 between 45.15.156[.]229:80 and VM:52754

Smoke

Smoke is a modular malware first identified in 2011, and is known to download other malware as well as steal information. The Smoke Loader can load several files, execute them, mimic legitimate processes, and more. It injects malicious code into system processes like “explorer.exe”, and conducts malicious activities while evading detection. More information on the Smoke Loader can be found in ANY.RUN’s Smoke Loader Malware Trends.

Process 4192: explorer.exe

The initial PrivateLoader “setup.exe” (process 4440) spawns “vvlbVE_a1T9mi81qLqDvAjYH.exe” (process 2648), which runs injected code in “explorer.exe” (process 4192). This is detected as Smoke.


The “setup.exe” (process 4440)

The “C:\Users\admin\Pictures\Minor Policy\vvlbVE_a1T9mi81qLqDvAjYH.exe” is responsible for injecting malicious code into “explorer.exe”:


The “vvlbVE_a1T9mi81qLqDvAjYH.exe” (process 2648) runs injected code in another process

The “explorer.exe” (process 4192) conducts several malicious activities after being injected with malicious code. Process 4192 is seen communicating with the C2 servers, 34.94.245[.]237, 91.215.85[.]17, 34.168.225[.]46 via port 80 (T1071 – Application Layer Protocol).

HTTP POST requests “/” to the host *sumagulituyo[.]org*, *stualialuyastrelia[.]net*, *criogetikfenbut[.]org* were observed for 34.94.245[.]237, 91.215.85[.]17, 34.168.225[.]46 respectively for Process 4192. The response to the POST requests contained references to *https://myattwg.att[.]com/UverseAccount.html*, and opening this URL in a browser in ANY.RUN sandbox shows a site that asks for AT&T credentials. This is known to be a browser hijacker according to OSINT.


The Network Stream comparison

Process 4192 runs a command that uses PowerShell to tell the Windows Defender to ignore the current user’s profile folder (“C:\Users\admin” in this case), and the Program Files folder (“C:\Program Files” in this case) during scans. This allows more malware into the system without being detected by Windows Defender (T1562.001 – Impair Defenses: Disable or Modify Tools).


Process 4192 adds a path to the Windows Defender exclusion list with the line surrounded by green

Process 4192 runs a command that will start a scheduled task called “*GoogleUpdateTaskMachineQC*” using *schtasks* (Task Scheduler). The purpose is to evade analysis environments with time-based methods, and the Windows Task

Scheduler can be abused for the initial or recurring execution of malicious code (T1497.003 – Virtualization/Sandbox Evasion: Time Based Evasion, and T1053.005 – Scheduled Task/Job: Scheduled Task).


CrackedCantil malware analysis
Process 4192 uses the Task Scheduler to run other applications with the line surrounded by green

The “GoogleUpdateTaskMachineQC” is an XML file that is modified by “svchost.exe” (process 1272). The “svchost.exe” is located under “C:\Windows\system32\”. This is a system file in Windows, and acts as a host process for services running from DLLs.


CrackedCantil malware analysis
Process 1272 modifies the file “GoogleUpdateTaskMachineQC”

“GoogleUpdateTaskMachineQC” is an XML configuration file for a scheduled task. It configures a scheduled task called “GoogleUpdateTaskMachineQC”, which will be triggered at every system boot. It runs using the highest available privilege, and will execute “C:\Program Files\Google\Chrome\updater.exe”.


CrackedCantil malware analysis
The URI is “GoogleUpdateTaskMachineQC”


CrackedCantil malware analysis
The RunLevel is “HighestAvailable”


CrackedCantil malware analysis
The Exec location is “C:\Program Files\Google\Chrome\updater.exe”

The “t4vXjCz8dD8LVP0hkcsFvzr1.exe” (process 6320) spawns from the PrivateLoader “wlC578T8hWfvZ2yJxLzrF38Y.exe” (process 1916), and modifies “C:\Program Files\Google\Chrome\updater.exe”:


CrackedCantil malware analysis
Process 6320 modifies “C:\Program Files\Google\Chrome\updater.exe”

Detonating “updater.exe” in this sample, independently in ANY.RUN sandbox revealed that it is a Miner malware.


CrackedCantil malware analysis
The attributes of “updater.exe” in *Static Discovering*

After the system reboot, “updater.exe” (process 1632) starts via Task Scheduler:


CrackedCantil malware analysis
System Reboot > “updater.exe” (process 1632)

Process 1632 drops executable files “C:\Program Files\Google\Libs\WR64.sys”, and “C:\Windows\TEMP\cwpxsctaqxko.tmp”.


CrackedCantil malware analysis
Process 1632 drops executable files immediately after reboot

In the “WR64.sys” and “cwpxsctaqxko.tmp” EXIF information, the MachineType mentioned “AMD AMD64”. According to OSINT, these files are Miner malware for AMD64.


CrackedCantil malware analysis

The attributes of “WR64.sys” and “cwpxsctaqxko.tmp” in *Static Discovering*

Process 1436: explorer.exe

After the system reboot, “bdutbcd” (process 3984) injects “explorer.exe” (process 1436), and this is detected as Smoke.


CrackedCantil malware analysis
System reboot > “bdutbcd” (process 3984) ↦ “explorer.exe” (process 1436) is detected as Smoke

Process 3984 originates from the initial Smoke instance before reboot, “explorer.exe” (process 4192). “bdutbcd” has the exact same hash as “vvlbVE_a1T9mi81qLqDvAjYH.exe”, which injected “explorer.exe” (process 4192):


CrackedCantil malware analysis
“C:\Users\admin\AppData\Roaming\bdutbcd” originates from Process 4192

Numerous HTTP POST requests to several hosts and IPs were observed for Process 1436:


CrackedCantil malware analysis
The HTTP POST requests and the *Network Stream* for Process 1436

Lumma

Lumma is an information stealer first identified in 2022. It is developed using the C programming language and is known to steal sensitive information such as cryptocurrency wallets, credentials, and more. Lumma can target a wide range of systems, ranging from Windows 7 up to 11, and has been actively evolving since its discovery. More information on Lumma can be found in ANY.RUN’s Lumma Malware Trends.

Process 1588: T6OBqC4lLuNgq7EqPk6LjxrX.exe

The initial PrivateLoader “setup.exe” (process 4440) spawns “T6OBqC4lLuNgq7EqPk6LjxrX.exe” (process 2344), which also spawns “T6OBqC4lLuNgq7EqPk6LjxrX.exe” (process 1588). This is detected as Lumma.


CrackedCantil malware analysis
The “setup.exe” (process 4440)

Process 1588 was also seen connecting to its C2 via port 80 (T1071 – Application Layer Protocol), and HTTP POST requests *“/api”* to the host *cinemaretailermkw[.]fun* were observed.


CrackedCantil malware analysis
The HTTP POST requests made by Process 1588

In one of the POST requests to the host *cinemaretailermkw[.]fun*, the string “*Content-Disposition: form-data; name=”file”; filename=”file””* and “*Content-Type: attachment/x-object*” were observed (in green). This indicates that the content underneath is a file. Strings like “*System.txt*”, “*Software.txt*”, and “*Screen.png*” (in red) were observed within the content, which suggests that this file is an archive file.


CrackedCantil malware analysis
The *Network Stream* for Process 1588 between 188.114.97[.]3:80 and VM:56670

The PCAP was downloaded, and the file contents were extracted from “*MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: “be85de5ipdocierre1”* > “*Media Type*” > “*Export Packet Bytes…*” with Wireshark. The

file was named “file.zip”.


CrackedCantil malware analysis
Extracting “file.zip” from the PCAP using Wireshark

This “file.zip” was opened inside a new ANY.RUN sandbox’s sample. This archive file contains “System.txt”, “Software.txt”, and “Screen.png”. Opening “Screen.png” shows a screenshot of the original CrackedCantil task at 6:31 AM:


CrackedCantil malware analysis
Opening “file.zip” with WinRAR, and “Screen.png in Photos

Opening “Software.txt” and “System.txt” in Notepad showed a bunch of interesting information. “Software.txt” contained the information of installed software in the ANY.RUN sandbox system. “System.txt” contained the Lumma ID, the Telegram (@lummanowork), and system information like the PC name, user, OS Version, HWID, Screen Resolution, Language, CPU Name, GPU, Physical Installed Memory.


CrackedCantil malware analysis

In another POST request to the host *cinemaretailermkw[.]fun*, something similar was observed. Strings like “*Edge/BrowserVersion.txt*”, “*Edge/dp.txt*”, and “*Edge/Default/History*” (in red) were observed within the content, which suggests that this file is also an archive file.


CrackedCantil malware analysis
The *Network Stream* for Process 1588 between 188.114.96[.]3:80 and VM:53676

The PCAP was downloaded, and the file contents were extracted with the method highlighted previously. This file was named “file2.zip”, and was opened inside a new sample, which contained a folder “Edge”. The contents of “Edge” can be viewed with the command “tree /F”, and contain various Edge-related information:


CrackedCantil malware analysis
The contents of “file2.zip”

“History” contained the Edge Browser history, “Login Data” contained the Edge Browser login data, “Cookies” contained the Edge browser cookies, and more:


CrackedCantil malware analysis
A section of “Edge/Default/Login Data”, “Edge/Default/History”

In another POST request to the host *cinemaretailermkw[.]fun*, something similar was observed. Strings like “*Mozilla Firefox/8o2qovza.default-release/key4.db*” (in red) were observed within the content.


CrackedCantil malware analysis
The *Network Stream* for Process 1588 between 188.114.97[.]3:80 and VM:54018

The file contents were extracted, and named “file3.zip”. It was opened inside an ANY.RUN sample, which contained a folder “Mozilla Firefox”:


CrackedCantil malware analysis
The contents of “file3.zip”

It contained .db, .sqlite, and .json files with various Firefox related information, like the Firefox Browser history, meta data, bookmarks, and credentials:

Sections of the database files containing sensitive Firefox information


CrackedCantil malware analysis
The contents of “logins.json” in *Static Discovering*, which contains the encrypted username and password

The information in the archive files are exfiltrated via HTTP by Process 1588.

Process 4360: RegSvcs.exe

The initial PrivateLoader “setup.exe” (process 4440) spawns “cuS4AGoWkhss2UsAPWfpvGrK.exe” (process 2452), which spawns “RegSvcs.exe” (process 4360). This is also detected as Lumma.


CrackedCantil malware analysis
Lumma is detected

“RegSvcs.exe” (process 4360) is located in “C:\Windows\Microsoft.NET\Framework\v4.0.30319\”. This is a part of the Microsoft .NET Framework for version 4.0.30319, and is mostly used for setting up applications that require COM interop. However, “RegSvcs.exe” is known to be abused for registering and executing malicious .NET assemblies by malware. More details can be found in Perception Point’s Lumma Analysis.

Process 4360 is seen connecting to its C2, 104.21.88[.]119 via port 80 (T1071 – Application Layer Protocol). HTTP POST requests *“/api”* to the host *ensurerecommendedd[.]pw* were observed.


CrackedCantil malware analysis
The HTTP POST requests made by Process 4360

In the HTTP POST requests, behavior nearly identical to “T6OBqC4lLuNgq7EqPk6LjxrX.exe” (process 1588) were observed, where various archive files containing Browser (Edge, Firefox) information, system information, and screenshots were exfiltrated via HTTP. Additionally, an archive file containing Chrome Browser information was observed for Process 4360, and this was opened in a this sample.


CrackedCantil malware analysis
The *Network Stream* comparison

Unarchiving “file4.zip” reveals various files containing sensitive information related to Chrome. For example, the “Chrome/Default/History” contained the Chrome Browser history, which included the Google search query “ida pro crack download”. It also included the URL of sites we have previously visited in Analyzing the Behavior in a Sandbox section.

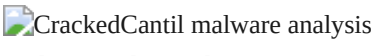

CrackedCantil malware analysis
A section of “Chrome/Default/History”

RedLine

RedLine is a .NET malware written in C#, and was first identified in 2020. RedLine is known to act as an infostealer that collects information like passwords, credit cards, cookies, location, and more. Additionally, RedLine can be used to deliver more malware, like ransomware, RATs, trojans, miners, and more. More information on RedLine can be found in ANY.RUN's RedLine Malware Trends.

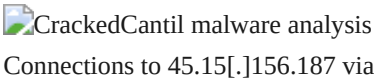
Process 6280: AppLaunch.exe

The initial PrivateLoader "setup.exe" (process 4440) spawns "nNjCpnjCODqx6RJUBNXhaAHF.exe" (process 5764). This spawns "AppLaunch.exe" (process 6280), and is detected as RedLine.

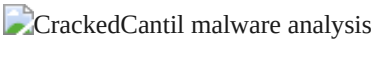

CrackedCantil malware analysis
RedLine is detected

The "AppLaunch.exe" (process 6280) is located in "C:\Windows\Microsoft.NET\Framework\v4.0.30319\". This is a part of the Microsoft .NET Framework for version 4.0.30319, and is usually used for launching applications based on the .NET Framework. However, the RedLine payload is known to be injected into "AppLaunch.exe" and other legitimate processes to conduct malicious activities while evading detection. More details can be found in Netskope's RedLine Stealer Analysis.

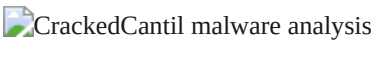
Process 6280 was seen repeatedly connecting to 45.15[.]156.187 over port 23929 (T1571 – Non-Standard Port):


CrackedCantil malware analysis
Connections to 45.15[.]156.187 via port 23929 by Process 6280

The contents of the uploaded data were identical, which contained "*net.tcp://45.15.156[.]187:23929/*":


CrackedCantil malware analysis

The malware configuration for RedLine reveals the C2, Botnet and Keys. The Botnet is "LogsDiller Cloud (Telegram: @logsdillabot)", according to OSINT this account sells various logs.

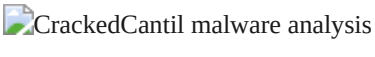

CrackedCantil malware analysis
The *Malware Configuration* for "AppLaunch.exe"

RisePro

RisePro is an information-stealing malware first identified in 2022. It is known to steal credit card, password, and crypto-wallet information. RisePro is written in C++, and employs a system of embedded DLL dependencies. More information on RisePro can be found in ANY.RUN's RisePro Malware Analysis: Exploring C2 Communication of a New Version.

Process 3004: 3Pvvg68HWOfBwJ9BdOsWgpEz.exe

The initial PrivateLoader "setup.exe" (process 4440) spawns "3Pvvg68HWOfBwJ9BdOsWgpEz.exe" (process 3004), which is detected as RisePro.


CrackedCantil malware analysis
RisePro is detected

Process 3004 runs a command that creates a scheduled task called “OfficeTrackerNMP131 HR” and “OfficeTrackerNMP131 LG”. This runs “C:\ProgramData\OfficeTrackerNMP131\OfficeTrackerNMP131.exe” on an hourly basis and at user logon with the highest privilege, namely “admin” (T1497.003 – Virtualization/Sandbox, and T1053.005 – Scheduled Task/Job: Scheduled Task).


CrackedCantil malware analysis
Process 3004 runs the lines surrounded in green.

This executable is dropped by Process 3004:


CrackedCantil malware analysis
Process 3004 drops “C:\ProgramData\OfficeTrackerNMP131\OfficeTrackerNMP131.exe”

The “OfficeTrackerNMP131.exe” (process 3940) is run from the Task Scheduler after the system reboot (T1497.003, and T1053.005). Detonating “OfficeTrackerNMP131.exe” independently inside a the sample reveals that it’s a RisePro malware.

The “3Pvvg68HWOfBwJ9BdOsWgpEz.exe” (process 3004) creates a file in the startup directory, namely “C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FANBooster131.lnk”. Persistence may be achieved by adding a program to a startup folder, which causes the referenced program to be executed upon log-in (T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder).


CrackedCantil malware analysis
Process 3004 creates files in the Startup directory

The “FANBooster131.lnk” is a LNK file, which is a shortcut that points to “C:\Users\admin\AppData\Local\Temp\FANBooster131\FANBooster131.exe”:


CrackedCantil malware analysis
“FANBooster131.lnk” points to “FANBooster131.exe”

“FANBooster131.exe” is dropped by Process 3004, and has the exact same hash as “OfficeTrackerNMP131.exe”. The “FANBooster131.exe” (process 7056) starts upon user login. Detonating “FANBooster131.exe” independently inside this example reveals that it’s also a RisePro malware.


CrackedCantil malware analysis
Process 3004 drops “C:\Users\admin\AppData\Local\Temp\FANBooster131\FANBooster131.exe”

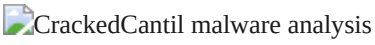
Process 5076: Iq4tpcuftnMe73YjwlKR3YVy.exe

The initial PrivateLoader “setup.exe” (process 4440) spawns “Iq4tpcuftnMe73YjwlKR3YVy.exe” (process 5076), which is detected as RisePro.

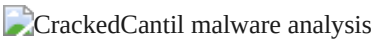

CrackedCantil malware analysis

Similar to “3Pvvg68HWOfBwJ9BdOsWgpEz.exe” (process 3004), the “Iq4tpcuftnMe73YjwlKR3YVy.exe” (process 5076) creates a scheduled task called “OfficeTrackerNMP1 LG” and “OfficeTrackerNMP1 HR“. This runs “C:\ProgramData\OfficeTrackerNMP1\OfficeTrackerNMP1.exe” at user logon and on an hourly basis with the highest

privilege, namely “admin”. Detonating “OfficeTrackerNMP1.exe” independently inside a sample reveals that it’s also a RisePro malware.


CrackedCantil malware analysis
Process 5076 runs the lines surrounded in green

The *Malware Configuration* contained the C2 IP addresses, which was 193[.]223.132.51 and 195[.]20.16.45.

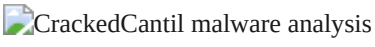

CrackedCantil malware analysis

Amadey

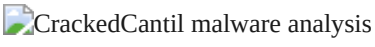
Amadey is a very versatile malware first identified in 2018, and can act as a loader or an infostealer. It can perform a wide range of malicious activities, including reconnaissance, data exfiltration, and loading more payloads. More information on Amadey can be found in ANY.RUN’s Amadey Malware Trends.

Process 4124: 5RfuRxo3fpxiWkD42DRCixRe.exe

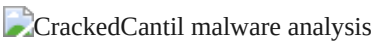
The initial PrivateLoader “setup.exe” (process 4440) spawns another PrivateLoader “wlC578T8hWfvZ2yJxLzrF38Y.exe” (process 1916). This spawns “5RfuRxo3fpxiWkD42DRCixRe.exe” (process 4124), which is detected as Amadey.


CrackedCantil malware analysis
Amadey is detected

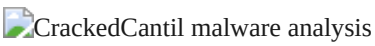
Process 4124 creates a scheduled task called “5RfuRxo3fpxiWkD42DRCixRe.exe” that runs “C:\Users\admin\Pictures\Minor Policy\5RfuRxo3fpxiWkD42DRCixRe.exe“ every minute.


CrackedCantil malware analysis
Process 4124 uses the Task Scheduler to run other applications,

Process 4124 also changes the autorun value in the registry. The Registry key “HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\USER SHELL FOLDERS” stores the paths to important system folders for the current user, which includes the Desktop, Startup, etc. For “STARTUP”, the value is now “%USERPROFILE%\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP”. This means that the path to the Startup folder has been changed by Process 4124, and whatever that is in “AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup” will now execute every time upon login (T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder).


CrackedCantil malware analysis
Process 4124 creates autorun value in the registry

These are the files in the “AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup” directory, and include LNK files that point to RisePro malware (FANBooster131.exe ANY.RUN task, PowerExpertNT.exe ANY.RUN task):

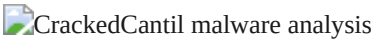

CrackedCantil malware analysis
The files under the “AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup” directory

Stealc

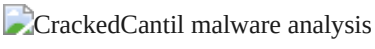
Stealc is an information-stealing malware first identified in 2023. It is written in C and utilizes WinAPI functions, and is known to steal sensitive information from browsers and exfiltrate the information to the C2 using HTTP POST requests. The development of Stealc relies on other stealers such as Vidar, Racoon, Redline, and Mars. More information on Stealc can be found in Malpedia's Stealc.

Process 2412: hzQj407t3pAeMkmtH8lxdDg1.exe

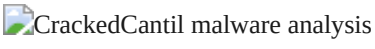
The initial PrivateLoader "setup.exe" (process 4440) spawns "hzQj407t3pAeMkmtH8lxdDg1.exe" (process 2412), which is detected as Stealc.


CrackedCantil malware analysis
Stealc is detected

"hzQj407t3pAeMkmtH8lxdDg1.exe" (process 2412) is located in "C:\Users\admin\Pictures\Minor Policy\", and is seen connecting to its C2, 5.42.64[.]41 via port 80. HTTP POST request "*/40d570f44e84a454.php*" to the host 5.42.64[.]41 was observed:


CrackedCantil malware analysis
The *Network Stream* for Process 2412 between 5.42.64[.]41:80 and VM:52705

However, Process 2412 crashes after a while. Detonating "hzQj407t3pAeMkmtH8lxdDg1.exe" independently in the task reveals the malware configuration, which includes the C2, Keys, and Strings:

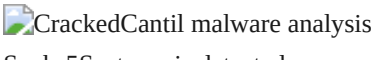

CrackedCantil malware analysis
The *Malware Configuration* for "hzQj407t3pAeMkmtH8lxdDg1.exe"

Socks5Systemz

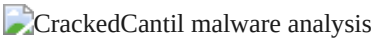
Socks5Systemz is a proxy bot malware that is known to infect devices through PrivateLoader and Amadey. Socks5Systemz turns infected devices into traffic-forwarding proxies for malicious traffic and connects to its C2 server with a DGA. More information on Socks5Systemz can be found in BleepingComputer's Socks5Systemz proxy service infects 10,000 systems worldwide.

Process 6364: DTPanelQT.exe

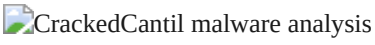
The initial PrivateLoader "setup.exe" (process 4440) spawns "69wM7sx_H1qc_If9hwYqEhWr.exe" (process 4960), which spawns "69wM7sx_H1qc_If9hwYqEhWr.tmp" (process 5560). This spawns "DTPanelQT.exe" (process 6364), which is detected as Socks5Systemz.


CrackedCantil malware analysis
Socks5Systemz is detected

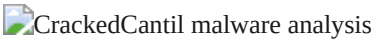
Process 6364 was seen connecting to its C2, 185.196.8[.]22 via port 80 (T1071 – Application Layer Protocol). Numerous GET requests to the host *ercwwol[.]ua* were observed:


CrackedCantil malware analysis
The HTTP GET requests and the *Network Stream* for Process 6364

It is also seen connecting to 176.9.47[.]240 via port 2023, which is a non-typical protocol and port pairing (T1571 – Non-Standard Port):

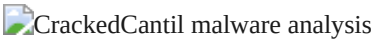

CrackedCantil malware analysis
Connections to 176.9.47[.]240 via port 2023 by Process 6364

The data sent to 176.9.47[.]240 via port 2023 appears to be a bunch of IP addresses and the port in the syntax "*[IP ADDRESS]:[PORT];*", and all the contents were identical:

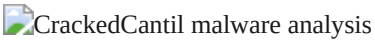

CrackedCantil malware analysis
The *Network Stream*

Process 4120: TacDecoLIB.exe

The initial PrivateLoader "setup.exe" (process 4440) spawns "H0jrwuNM7IG2q266V2EfAiVo.exe" (process 4548), which spawns "rjcJoThBdrYU.exe" (process 6880), which also spawns "rjcJoThBdrYU.tmp" (process 4900). This spawns "TacDecoLIB.exe" (process 4120), which is also detected as Socks5Systemz.


CrackedCantil malware analysis
Socks5Systemz process tree

Process 4120 was also seen connecting to its C2, 185.196.8[.]22 via port 80, and 176.9.47[.]240 via port 2023. This is the same as "DTPanelQT.exe" (process 6364), except to the host *aitmrzn[.]ru* instead of *ercwwol[.]ua*. The data sent to 176.9.47[.]240 via port 2023 appears to be a bunch of IP addresses and the port, which was identical to Process 6364.

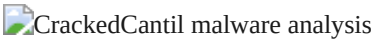

CrackedCantil malware analysis
The HTTP GET requests by Process 4120

STOP

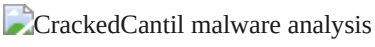
STOP is ransomware that encrypts user data, and the encrypted file extensions include .hhaz, .djvuu, .ljaz, and more. DJVU is a variant of the STOP ransomware and can include several layers of obfuscation which makes analysis more difficult. STOP/DJVU was first seen in 2018, and known to use AES-256, and Salsa20 for encryption. DJVU is known to collaborate with other malware, for example, it works with infostealer malware to steal sensitive information before the files are encrypted. More information on STOP/DJVU can be found in BlackBerry's DJVU: The Ransomware That Seems Strangely Familiar.

Process 6412: TzjwSXczmD2hOVANbz7L7Roc.exe

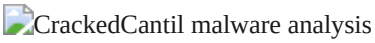
The initial PrivateLoader "setup[.]exe" (process 4440) spawns "TzjwSXczmD2hOVANbz7L7Roc[.]exe" (process 4944), which spawns "TzjwSXczmD2hOVANbz7L7Roc[.]exe" (process 6380), which spawns "TzjwSXczmD2hOVANbz7L7Roc[.]exe" (process 6808). This finally spawns "TzjwSXczmD2hOVANbz7L7Roc[.]exe" (process 6412). This is detected as STOP.


CrackedCantil malware analysis
STOP is detected

It uses the line *"–Admin IsNotAutoStart IsNotTask"*, meaning that it runs using admin privileges, and specifies to not automatically start or run as a task. The purpose is likely to allow the infostealers (Lumma, RedLine, RisePro, Amadey, Stealc) to steal sensitive information before the ransomware encrypts the files.

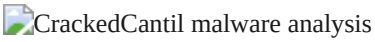

CrackedCantil malware analysis
The *Network Stream*

It was seen making HTTP GET requests "*/test2/get.php?pid=47DCC01E8C1FE7754757A5DC66C0F42F&first=true*" to the host *zexeq[.]com*, and the response contained a public key (in green). The MAC address for the system is 52:54:00:4a:ad:11, and converting this to Upper Case and generating the MD5 hash reveals that it is identical to the string in the GET request (in red):

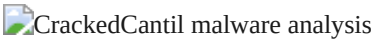

CrackedCantil malware analysis

Process 6328: TzjwSXczmD2hOVANbz7L7Roc.exe

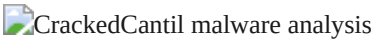
After the system reboot, the process "TzjwSXczmD2hOVANbz7L7Roc.exe" (process 2404) spawns "TzjwSXczmD2hOVANbz7L7Roc.exe" (process 6328), which is detected as STOP.


CrackedCantil malware analysis
STOP process tree

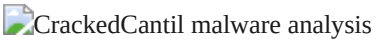
This time, it uses the line "*–AutoStart*" to automatically start:


CrackedCantil malware analysis
The lines surrounded in green are used to specify the task options

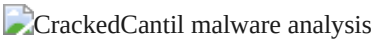
Process 6328 creates a file "geo[1].json" under "C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\J0KBFYBW\". This JSON file contains EXIF, which includes location information such as the City, Country, Ip, Latitude, Longitude, Region, etc.


CrackedCantil malware analysis
The attributes and contents of "geo[1].json" in *Static Discovering*

A few seconds after reboot and login, it starts encrypting files and appends the ".hhaz" extension (T1486 – Data Encrypted for Impact).


CrackedCantil malware analysis
Process 6328 encrypts various files

The files with the .hhaz extension contained the string "*{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}*" at the very end. This is a mutex, and is used by ransomware to avoid double-encrypting files.


CrackedCantil malware analysis
The contents of a .hhaz file, including the mutex

Conclusion

This deep dive explored the dangers of cracked software, traits and behaviors of several notorious malware families, and how they can work together to deliver a powerful infection in a symphonious manner.

The malware symphony in this CrackedCantil included Loaders, Infostealers, Cryptominers, Proxy Bot malware, and Ransomware. The Loaders (PrivateLoader, Smoke) dropped several notorious malware onto the system, the Infostealers (Lumma, RedLine, RisePro, Amadey, Stealc) stole various sensitive information before the ransomware encrypted the files, the Proxy Bot malware (Socks5Systemz) turned the system into a proxy bot, and the Ransomware (STOP) encrypted the files and demanded ransom for recovery.

This malware was named "CrackedCantil" by the author (of the article, not the malware), Lena (aka LambdaMamba).

About ANY.RUN

ANY.RUN is an interactive malware analysis sandbox that streamlines the work of SOC and DFIR teams. Our service is trusted by 300,000 professionals worldwide who use it to investigate both emerging and persistent threats.

Request a free trial of ANY.RUN for 14 days to explore all the features we offer.

Request demo →

Appendix 1: IOCs

Google Groups URL: hxxps://groups.google[.]com/g/exhibitor-users/c/eQTt-Z_Bnbw

Shortened URL: hxxps://byltly[.]com/2wIwtU

Redirect URL: hxxps://airfiltersing[.]com/CRACK+IDA+Pro+V6+8+150423+And+HEX-Rays+Decompiler+ARM+X86+X64-iDAPROl.zip

File Hosting URL: hxxps://afashionstudio[.]com/b/release.rar

Google Groups URL: hxxps://groups.google[.]com/g/exhibitor-users/c/eQTt-Z_Bnbw

Shortened URL: hxxps://byltly[.]com/2wIwtU

Redirect URL: hxxps://airfiltersing[.]com/CRACK+IDA+Pro+V6+8+150423+And+HEX-Rays+Decompiler+ARM+X86+X64-iDAPROl.zip

File Hosting URL: hxxps://afashionstudio[.]com/b/release.rar

Filename	MD5
release.rar	57AB5E01E6E92D13AE33E587004AD918

PrivateLoader

Filename	IP
C:\Users\admin\Desktop\setup.exe	185[.]216.70.235, 195[.]20.16.45, 172[.]67.75.163, 34[.]117.59.81, 87[.]240.129.133, 5[.]42.64.35, 109[.]107.182.3, 176[.]113.115.84, 194[.]33.191.102, 91[.]215.85.209, 104[.]192.141.1, 188[.]114.97.3, 188[.]114.96.3, 54[.]231.234.241, 23[.]37.62.128, 18[.]66.142.79
C:\Users\admin\Pictures\Minor Policy\vRNddZqIkwaYVpHLFkGcr1Tk.exe	195[.]20.16.45, 172[.]67.75.163, 34[.]117.59.81, 195[.]20.16.45, 195[.]20.16.46, 87[.]240.129.133, 172[.]67.147.32, 104[.]21.4.208
C:\Users\admin\Pictures\Minor Policy\wlC578T8hWfvZ2yJxLzrF38Y.exe	45[.]15.156.229, 172[.]67.75.163, 34[.]117.59.81, 87[.]240.129.133, 185[.]172.128.19, 87[.]240.137.140

Smoke

Filename	MD5
C:\Users\admin\Pictures\Minor Policy\vvlbVE_a1T9mi81qLqDvAjYH.exe	DF1CA8FEDCF81BC2A5E456465E56FCEF
C:\Users\admin\AppData\Roaming\bdutbcd	DF1CA8FEDCF81BC2A5E456465E56FCEF

Lumma

Filename	MD5
C:\Users\admin\Pictures\Minor Policy\T6OBqC4lLuNgq7EqPk6LjxrX.exe	188[.]114.97.3
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	104[.]21.88.119
Filename	MD5
C:\Users\admin\Pictures\Minor Policy\T6OBqC4lLuNgq7EqPk6LjxrX.exe	188[.]114.97.3

RedLine

Filename	IP
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	45[.]15.156.187

RisePro

Filename	MD5	IP
C:\Users\admin\Pictures\Minor Policy\3Pvvg68HWOfBwJ9BdOsWgpEz.exe	EF5C1EC128AC1822358D9281DCF3B710	193[.]233.132.51
C:\Users\admin\Pictures\Minor Policy\Iq4tpcuftnMe73YjwlKR3YVy.exe	E8EB594C3BB064E91514C6A9C93B22FF	195[.]20.16.45

Amadey

Filename	MD5	IP
C:\Users\admin\Pictures\Minor Policy\5RfuRxo3fpxiWkD42DRCixRe.exe	0099A99F5FFB3C3AE78AF0084136FAB3	185[.]172.128.19, 13[.]32.121.85, 18[.]66.142.79

Stealc

Filename	MD5	IP
C:\Users\admin\Pictures\Minor Policy\hzQj407t3pAeMkmtH8lxdDg1.exe	C6570BB5720D82B807160D350D83EE07	5[.]42.64.41

Socks5Systemz

Filename	IP
C:\Program Files (x86)\DTPanelQT\DTPanelQT.exe	172[.]67.148.28, 185[.]196.8.22, 176[.]9.47.240
C:\Program Files (x86)\TacDecoLIB\TacDecoLIB.exe	172[.]67.148.28, 185[.]196.8.22, 176[.]9.47.240

STOP

Filename	MD5	IP
C:\Users\admin\Pictures\Minor Policy\TzjwSXczmD2hOVANbz7L7Roc.exe	89F6A0761EB024C46520A74ABB7868A9	188[.]114.97.3, 190[.]224.203.37
C:\Users\admin\AppData\Local\9fd99086-6e14-4786-92b0-465dc82ad88d\TzjwSXczmD2hOVANbz7L7Roc.exe	89F6A0761EB024C46520A74ABB7868A9	188[.]114.97.3

Appendix 2: MITRE MATRIX

TA0002: Execution	T1204: User Execution	Rely upon specific actions by a user in order to gain execution.
	T1053: Scheduled Task	Task scheduling functionality may be abused to facilitate initial or recurring execution of malicious code.
TA0003: Persistence	T1053: Scheduled Task	Task scheduling functionality may be abused to facilitate initial or recurring execution of malicious code.
	T1547: Boot or Logon Autostart Execution	System settings may be configured to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges.
	T1176: Browser Extensions	Internet browser extensions may be abused to
TA0004: Privilege Escalation	T1053: Scheduled Task	Task scheduling functionality may be abused to facilitate initial or recurring execution of malicious code.
	T1547: Boot or Logon Autostart Execution	System settings may be configured to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges.
TA0005: Defense Evasion	T1497: Virtualization/Sandbox Evasion	Various methods may be employed to detect and avoid virtualization and analysis environments.

	T1562: Impair Defenses	Components of a victim environment may be maliciously modified in order to hinder or disable defensive mechanisms.
	T1070: Indicator Removal	Artifacts generated within systems may be deleted or modified to remove evidence of their presence or hinder defenses.
TA0006: Credential Access	T1552: Unsecured Credentials	Search compromised systems to find and obtain insecurely stored credentials.
	T1555: Credentials from Password Stores	Search for common password storage locations to obtain user credentials.
TA0007: Discovery	T1497: Virtualization/Sandbox Evasion	Various methods may be employed to detect and avoid virtualization and analysis environments.
	T1518: Software Discovery	Get a listing of software and software versions that are installed.
	T1012: Query Registry	Interact with the Windows Registry to gather information.
	T1082: System Information Discovery	Get detailed information about the operating system and hardware.
TA0011: Command and Control	T1071: Application Layer Protocol	Communicate using OSI application layer protocols to avoid detection.
	T1571: Non-Standard Port	Communicate using a protocol and port pairing that are typically not associated.
TA0040: Impact	T1486: Data Encrypted for Impact	Encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.

*Not every tactics and techniques involved are included due to the complexity

I am a Chief Research Officer at a cybersecurity company. My passions include investigations, experimentations, gaming, writing, and drawing. I also like playing around with hardware, operating systems, and FPGAs. I enjoy assembling things as well as disassembling things! In my spare time, I do CTFs, threat hunting, and write about them. I am fascinated by snakes, which includes the Snake Malware! Check out:

- My website
- My LinkedIn profile
