CrackedCantil Dropper Delivers Numerous Malware

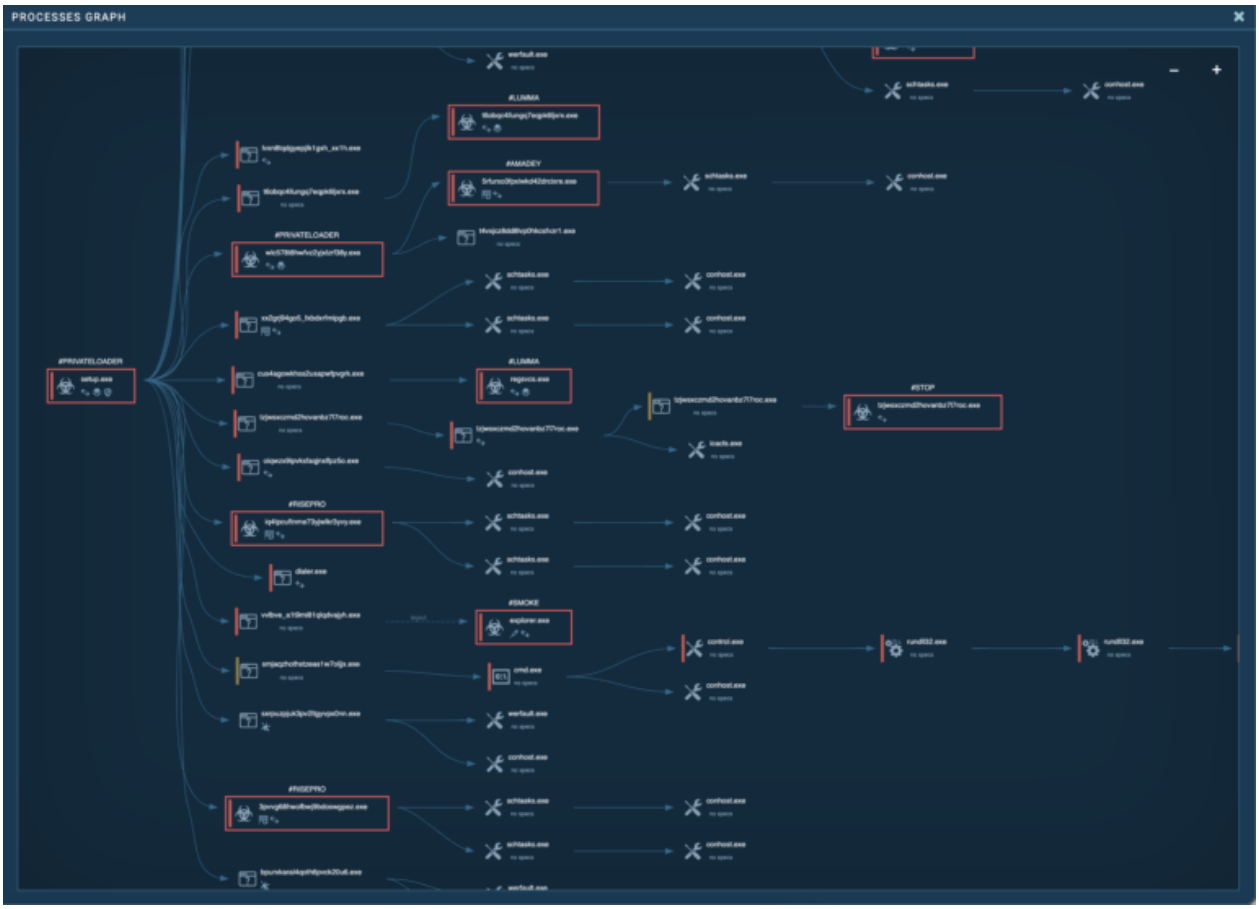
gridinsoft.com/blogs/crackedcantil-dropper-malware/

View all of Stephanie Adlam's posts. February 2, 2024

CrackedCantil is a unique dropper malware sample that operates with a wide variety of malware families. Infecting with one may effectively mean up to five other malware types running in the system. Let’s break down on what it is, how it spreads, and why it is so dangerous.

What is CrackedCantil?

CrackedCantil is a dropper malware discovered and described by the malware analyst LambdaMamba. The name of this malware derives from two parts. “Cracked” for software cracks, is the primary spreading vector, and “Cantil” for the Cantil viper, a species of highly venomous viper, suggesting the malware’s harmful potential. By its nature, **CrackedCantil is a loader/dropper** malware that targets at delivering a lot of different malware samples, including stealers, ransomware, spyware and backdoors.



The CrackedCantil process tree (source: ANY.RUN)

Overview of distribution ways

The main way to spread such malware is through the use of cracked software. People looking for free versions of paid software often resort to downloading “cracked” versions. These versions are often legitimate software modified to bypass licensing mechanisms. However, attackers use this demand for cracked software as a means to spread malware.

The process begins on questionable websites or forums. After downloading and running what looks like an installer, malware is **installed on the user’s computer**. This may be disguised as useful files or integrated into the installation executables. Once activated, the malware begins infecting the system, a process that may include several actions. Then it can install additional malware, steal data, encrypt files for ransom, and turn the infected device into part of a botnet.

CrackedCantil Delivers Droppers, Spyware and Ransomware

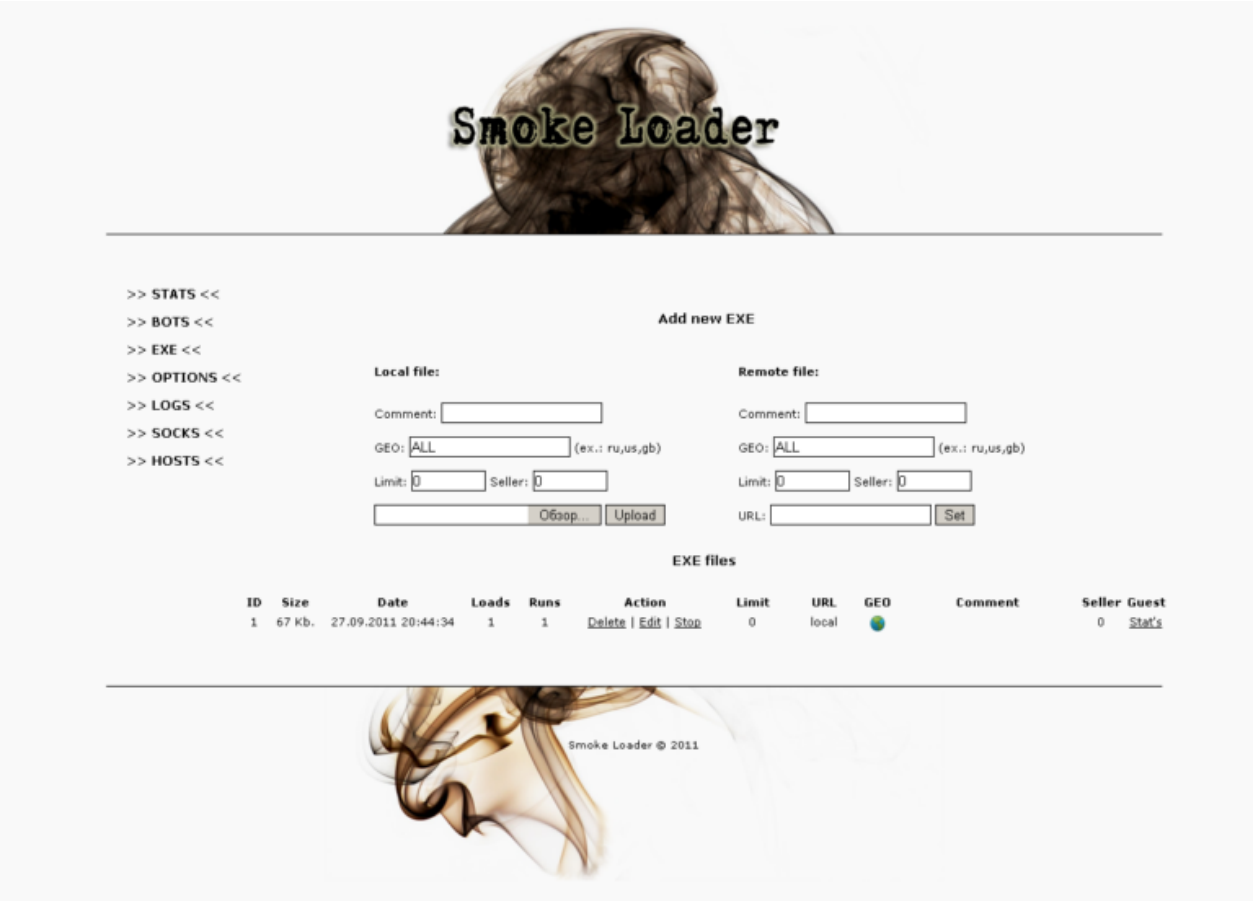
The tree of processes involved in the incident is quite complicated, and several infamous malware families were found to be involved. Let’s look at these families in the overall threat picture, focusing on the role of each in the symphony of cyberattacks.

PrivateLoader

PrivateLoader works as a polymorphic downloader that uses various obfuscation and packaging techniques to evade detection by antivirus programs. It is written in C++ and is often **distributed with cracked software**. It is also capable of downloading and executing additional malicious modules from remote control servers. Also, PrivateLoader often includes features to check the execution environment to avoid running in virtual machines or analysis environments, making it difficult for security researchers to investigate and analyze.

SmokeLoader

SmokeLoader, also known as Dofoil, is a “loader” type malware used to spread additional malware such as backdoors, keyloggers, and Trojans. It is also capable of stealing information. SmokeLoader can inject malicious code into system processes, thereby evading detection.



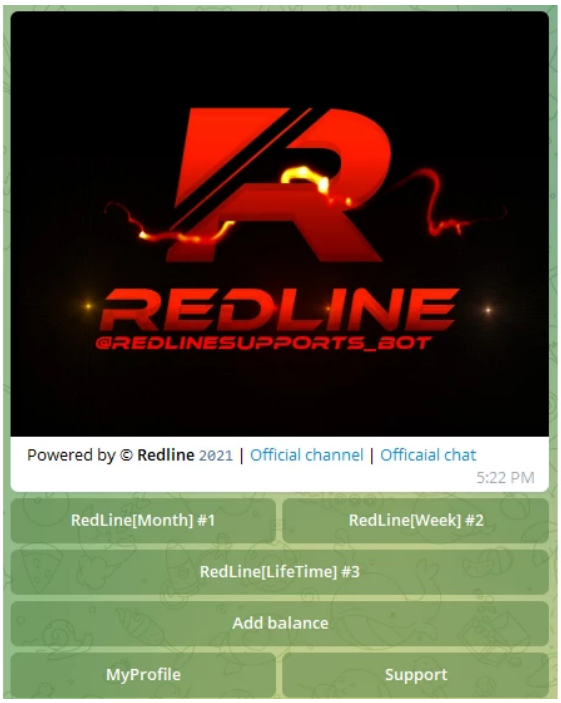
C2 panel of Smokeloader backdoor

Lumma

Lumma is an infostealer that received quite a bit of attention over the last few months. It can extract personal and financial data from a variety of **sources on infected computers**, including web browsers, email clients, and cryptocurrency wallet files. Most commonly, Lumma Stealer propagates through social engineering and phishing attacks. It can also evade antivirus detection and transmit collected data to a remote command and control (C&C) server.

RedLine

RedLine Stealer is a malicious program designed to steal various types of sensitive information from infected computers. It is capable of **extracting browser credentials**, credit card data, e-wallet passwords, and system information. Appeared back in 2020, it has quickly become one of the most popular stealers on the malware market.



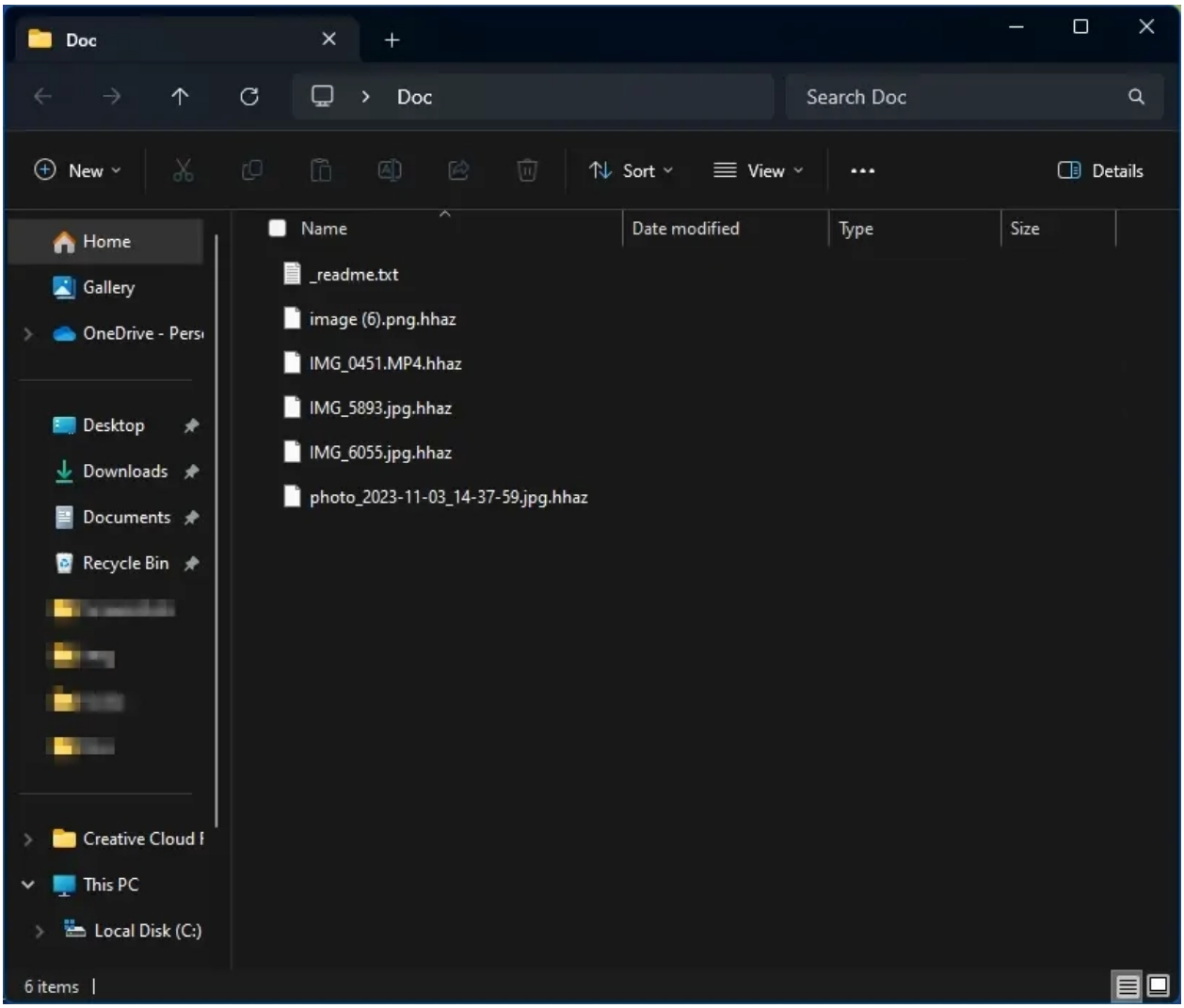
Telegram bot that malware devs use to promote RedLine

Socks5Systemz

Socks5Systemz is a malware that infects devices through PrivateLoader and Amadey. Infected devices are turned into traffic-forwarding proxies for malicious traffic, and the malware connects to its C2 server with a DGA.

STOP/Djvu Ransomware

STOP Ransomware is an encryptor characterized by adding unique extensions to encrypted files and creating ransom text files that contain instructions for the victim on how to make the payment and obtain the decryptor. Also, it encrypts files and adds its extensions to their ends – .hhaz, .cdaz, cdcc, and the like. DJVU is also a variant of the STOP ransomware that can include **multiple levels of stealth**, making it harder to analyze. STOP/DJVU encrypts files using AES-256 and Salsa20. It is known to collaborate with other malware, such as infostealer malware, to steal sensitive information before encryption.



The outcome of Djvu ransomware – encrypted files

How dangerous is CrackedCantil?

CrackedCantil is another player on the dropper malware market, but its unique ability to coordinate different types of malware sets it apart from the crowd. It makes a so-called “symphony of malware” where each element is carefully tuned for maximum impact. The **growing popularity** of CrackedCantil points to its effectiveness, in both detection evasion and malware delivery. Huge distribution through users’ desire to access paid software for free.

To avoid infection through cracked programs, the following precautions are recommended:

- Always purchase software from official vendors or directly from the developers. This not only ensures the legitimacy of your software, but also ensures that you receive all necessary security updates.
- Regularly update all installed programs and the operating system. This helps protect your system from vulnerabilities that can be exploited by malware.

- Use a reliable antivirus solution and scan your system regularly. Modern antivirus programs frequently update their databases to recognize new threats.
- Increase your and your employees' knowledge of cyber threats and social engineering techniques. Knowing how threats spread can significantly reduce the risk of exposure.