Saint Stealer Malware

(an intelligent malware)

Description

Cybersecurity researchers have dissected the inner workings of an information-stealing malware called Saintstealer that's designed to siphon credentials and system information.

 These forms of malware also steal information from a litany of locations throughout the entirety of the targeted system, compressing the data into a ZIP file that is protected by a password.

This malware was found on last week of April and officially published on may 10 2022.

What is Saint Stealer and its Details

Its a .NET-based information stealer developed by the Saint gang. After execution, the stealer extracts username, passwords, credit card details, etc

The Saintstealer malware uses a NET-based 32-bit C# executable dubbed “saintgang.exe” to steal information. The malware is designed with checks for anti-analysis so that it can delete itself if operating in a virtual space or a sandbox.

Saintstealer steals a plethora of data, including cookies, autofill information, screen captures, passwords, and more. The malware steals information within [Chromium browsers](https://www.zdnet.com/pictures/all-the-chromium-based-browsers/), including the likes of Brave, Edge, Opera, Chrome, Yandex, and Vivaldi. Additionally, the malware is advanced to the point that it can pluck tokens for multi-factor authentication directly from the popular Discord chat platform. Saintstealer can also steal files with .docx, .doc, and .txt extensions and extract data from Open VPN, Nord VPN, Telegram, VimeWorld, and more.

Data Tranfer to Attacker

The metadata related to the exfiltrated information is sent to a Command and Control (C&C) server – hxxp://f0591243.xsph[.]ru.

The C&C server initially refused the connection, but upon checking the IP (141.8.197[.]42) associated with the domain, we found multiple similar sub-domains hosted on this IP.

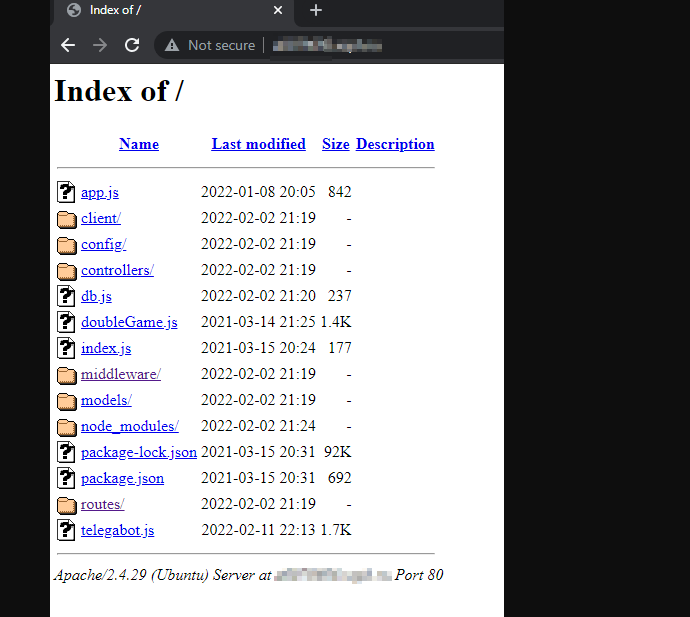


Figure 1 – Files Hosted on C&C

Apart from the C&C, i investigated two other malicious domains

hxxp://notste[redacted].com.xsph[.]ru/

 hxxp://ilov[redacted].ru.xsph[.]ru/.

These domains show the possible login panel for the TAs and the link to the Telegram channel t.me/[redacted]team, possibly affiliated with the TAs

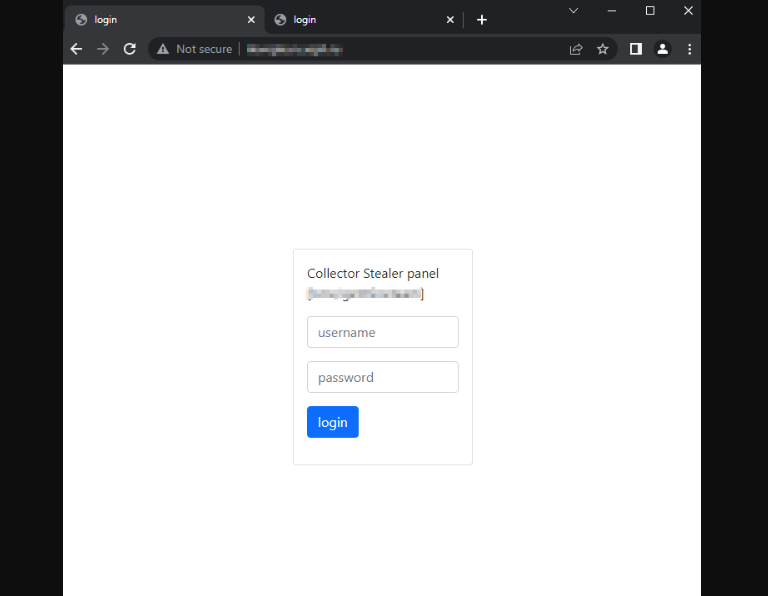


Figure 2 – TAs Login Panel

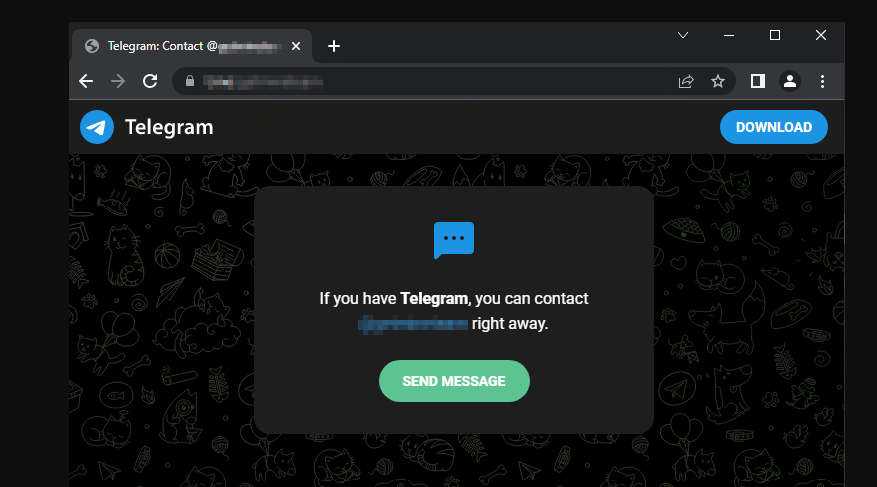


Figure 3 – TA’s Telegram Channel

For Detail Analysis :- <https://thecybersecurity.news/general-cyber-security-news/experts-detail-saintstealer-and-prynt-stealer-info-stealing-malware-families-18799/>

<https://blog.cyble.com/2022/04/27/dissecting-saintstealer/>

Finding the malware is packed or not

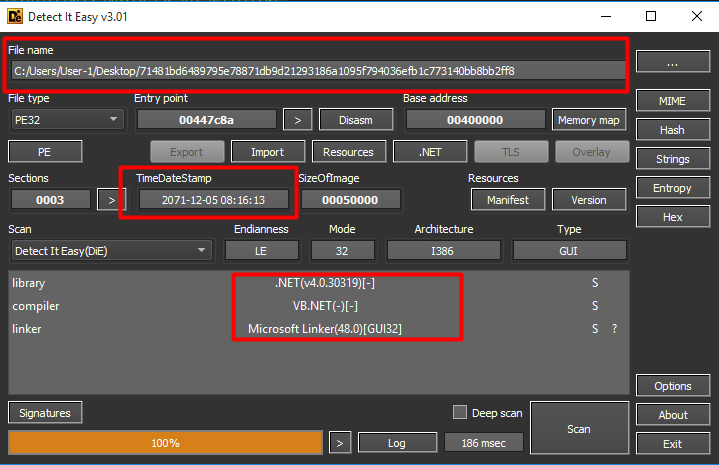
I used ExeinfoPE tool to check whether that file is packed or not.

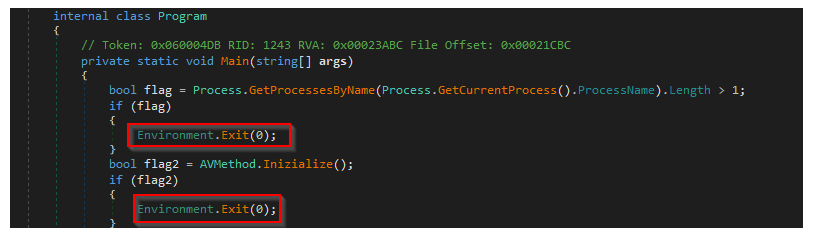
The ExeInfo utility shows general information about executable files, dynamic-link libraries (.dll) and drivers files. It can recognize all major types of executables like MS-DOS files and Portable Executable files (PE).

Its find the difference between the IMAGE SECTION HEADER RAW SIZE and VIRTUAL SIZE

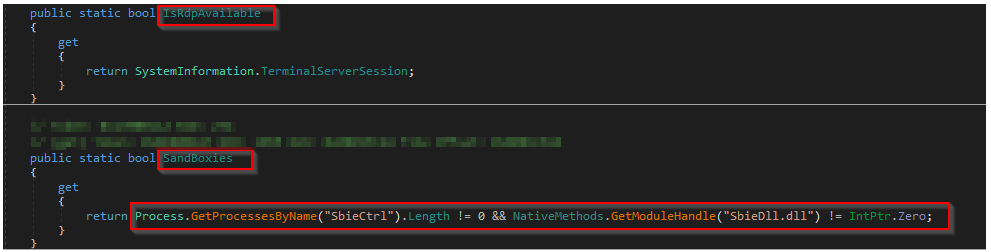
After analysing the I got to know that the file is not packed.

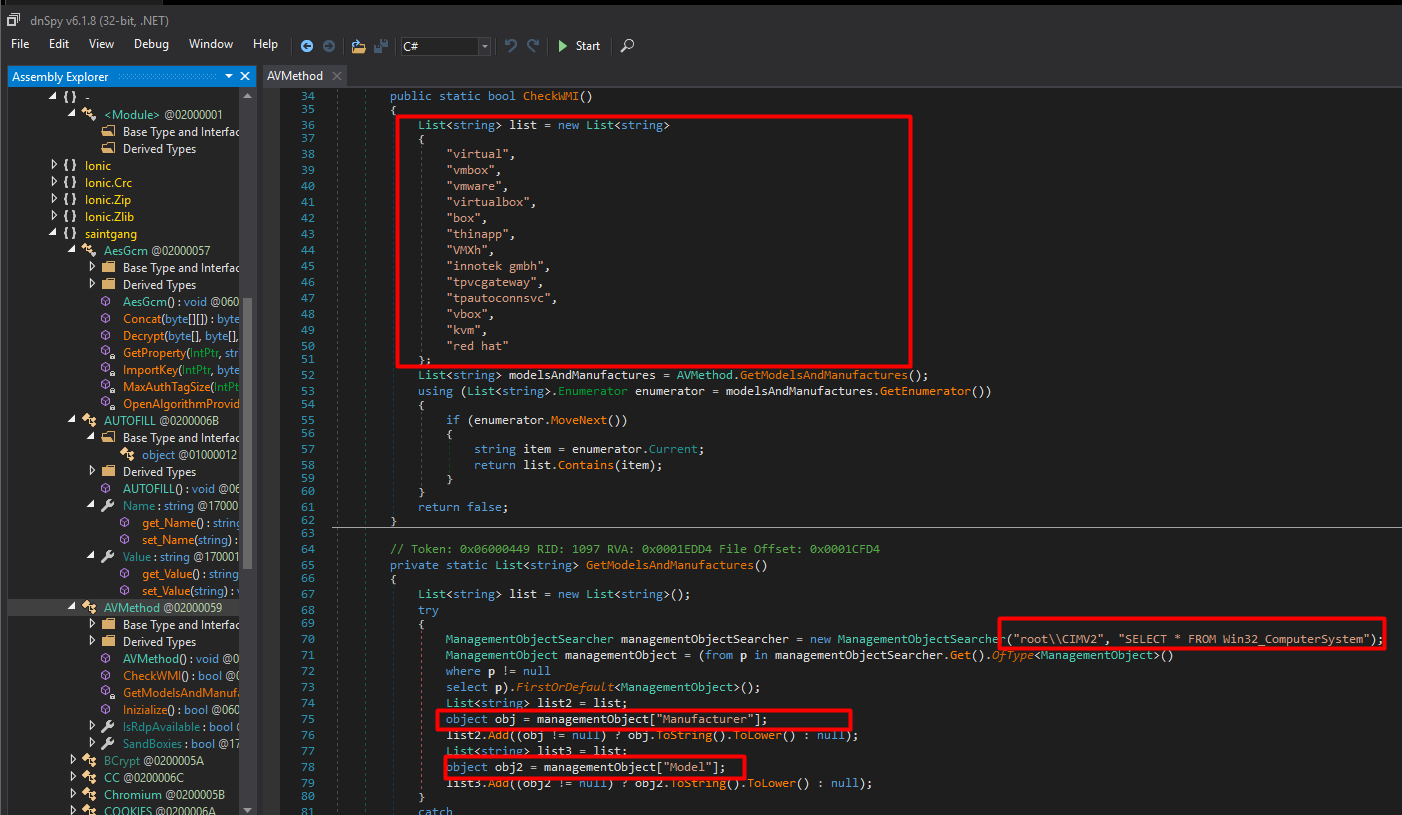
Malware Working Mechanism Using Dnspy Tool

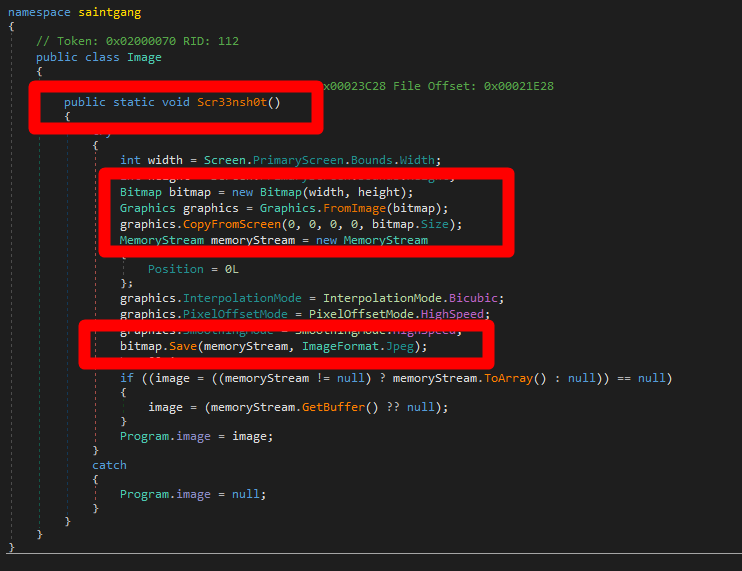
1. Stealer Checking Environment
2. Anti-Reversing Technique Used by the Stealer



1. Stealer Checking for Rdp and Sandboxie

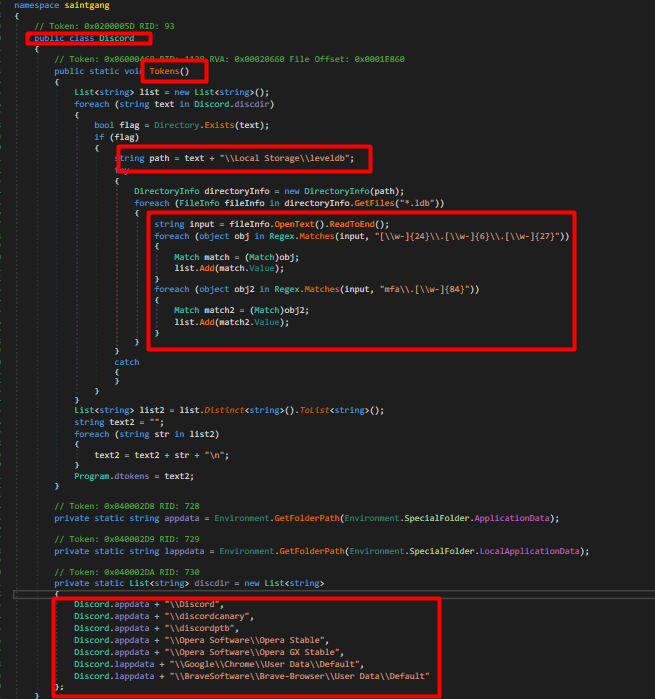


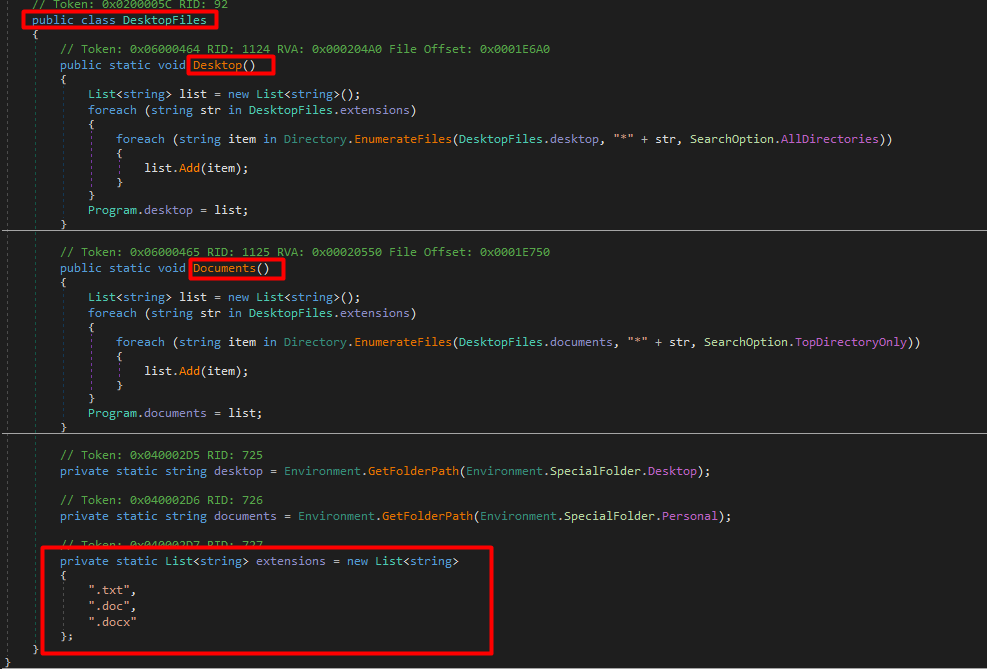
1.  Stealer Checking Virtual Environment

 5 Stealer Routine for Capturing Screenshots

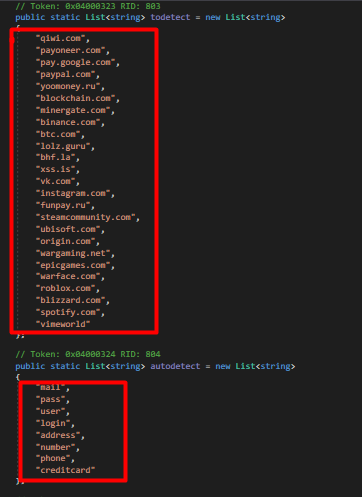
5 Stealer Extracting System Information



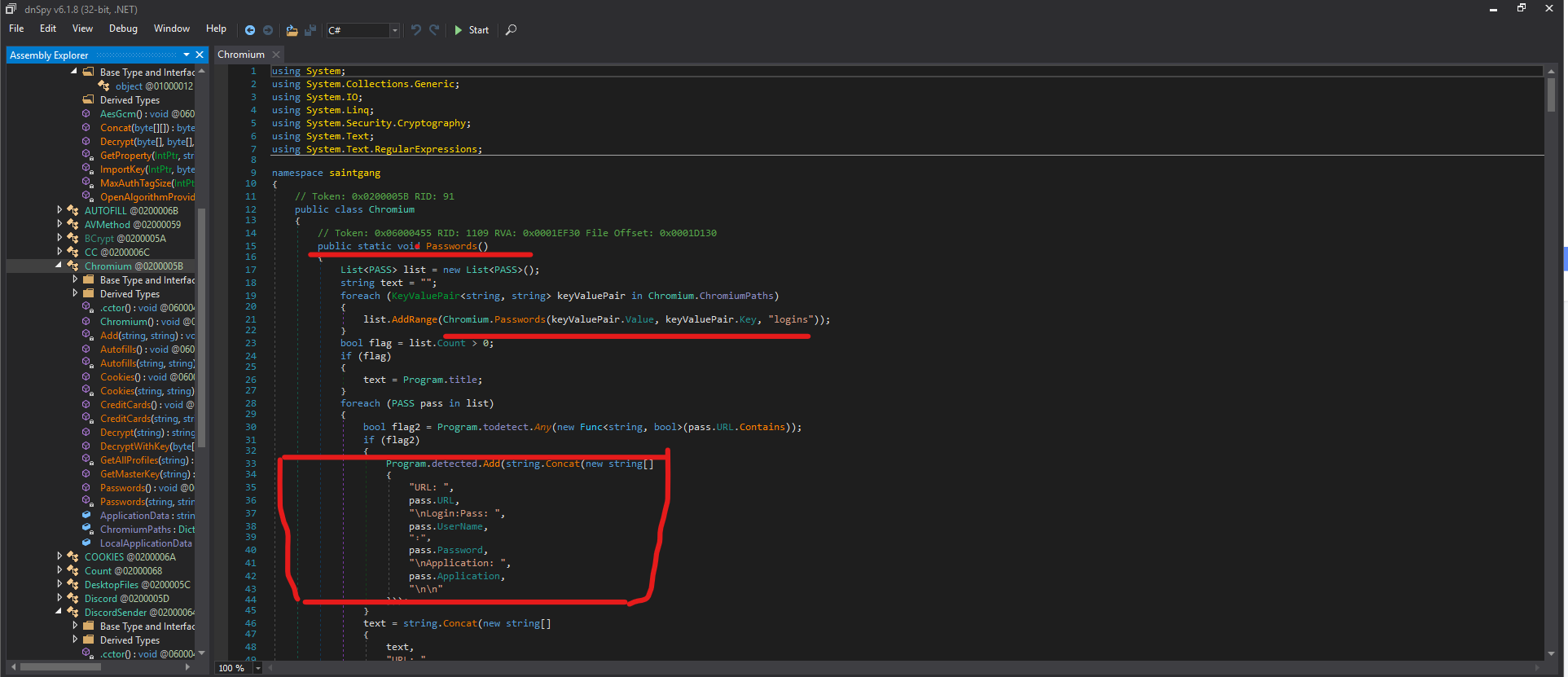
1. Stealer Routine for Discord Data Exfiltration
2. Stealer Extracting Desktop and Document Files



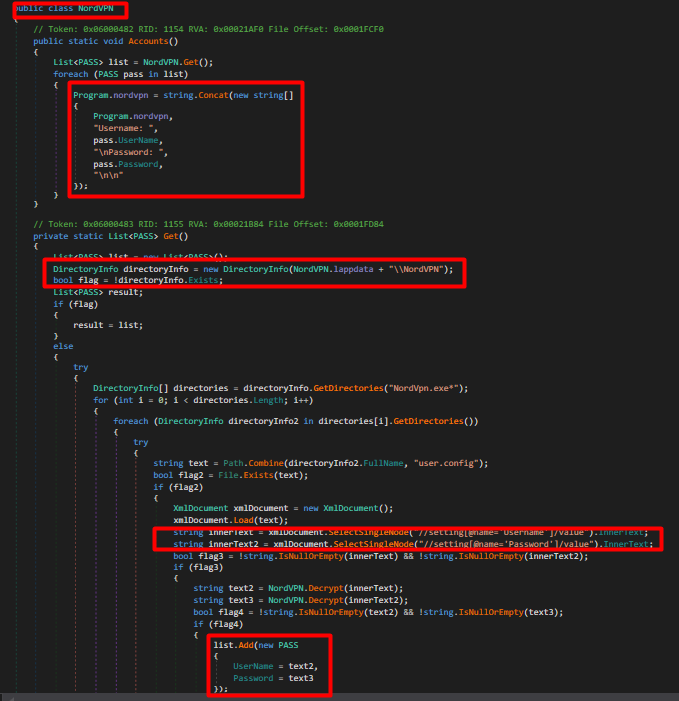
7 Targeted Websites and Data



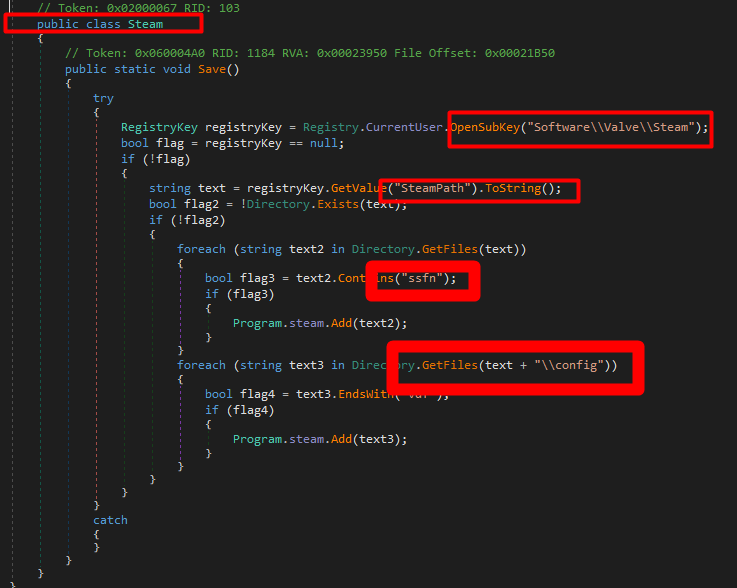
1. Stealer Routine for Browser Data Extraction



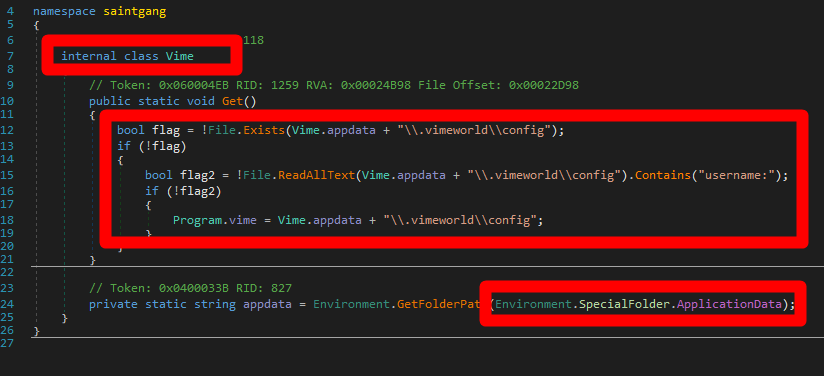
1. Stealer Routine for NordVPN Data Extraction



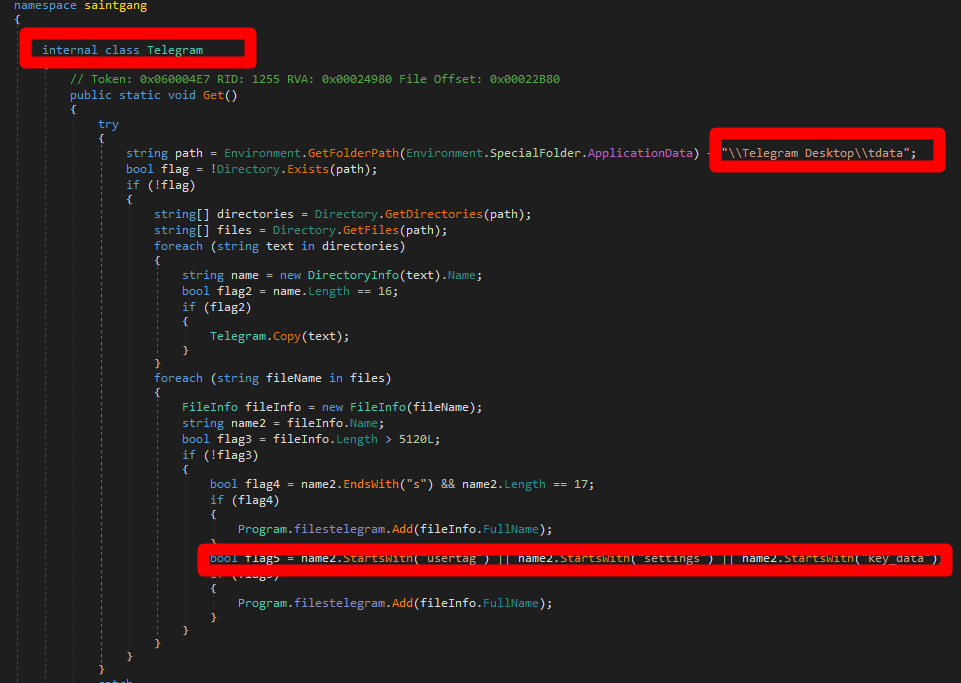
1. Stealer Routine for Steam Data Extraction



1. Stealer Routine for VimeWorld Data Extraction



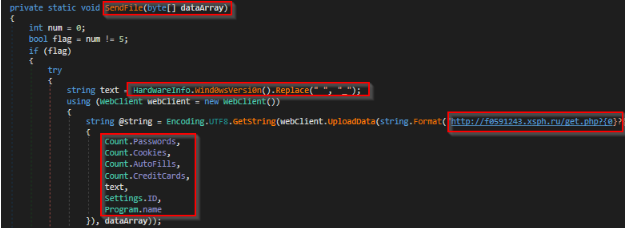
1. Stealer Routine for Telegram Data Extraction



1. Stealer Routine for Sending Stolen Data to the Telegram Chat



1. Stealer Routine for Sending Metadata to C&C



References:

<https://thehackernews.com/2022/05/experts-detail-saintstealer-and-prynt.html>

<https://thecybersecurity.news/general-cyber-security-news/experts-detail-saintstealer-and-prynt-stealer-info-stealing-malware-families-18799/>

<https://blog.cyble.com/2022/04/27/dissecting-saintstealer/>