

Approaching stealers devs : a brief interview with StealC

By g0njxa

Published: 2023-12-05 · Archived: 2026-04-05 17:56:11 UTC



To completely understand what's going on in a market that has been growing in the last years I found mandatory to know which players are dominating it. Always remember that behind every user of the Internet there is another human like you, so if you can be kind enough to reach them and they agree, you can have a little talk. Asking things is not a crime.

Please note everything that stated on this blog has only an informational purpose. I will never promote the use of these products.

Let's see, StealC: [@plymOuth](#)

Get g0njxa's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The interview was made in Russian. Since a translator was used, questions will be shown in original english, and answers will be given both in original Russian (in case translation is misled) and translations to english.

g0njxa

How would you describe StealC?

Plymouth Support

Our software is something like a technical demo, we came to the market from Private and Stealc is one of our main tools for attacks, which was originally developed to work on point targets, but has also shown itself well in mass attacks (installs, advertising, etc.)

The version of Stealc that is on public sale is the public version with which customers start working with us – in the future, many regular customers already take the so-called private – we We finalize and/or add functionality to meet the needs of customers

How would you describe StealC?

наш софт это что-то вроде технического демо, мы пришли на рынок из привата и stealc это один из основных наших инструментов для атак, который изначально разрабатывался для работы по точечным целям, но неплохо себя показал и в массовых атаках (инсталлы, реклама и тому подобное)

та версия stealc, что находится в открытой продаже это публичная версия, с которой клиенты начинают работу с нами — в дальнейшем многие постоянные клиенты уже берут так называемый приват — мы дорабатываем и/или добавляем функционал под нужды клиентов

g0njxa

What does the name STEALC means? is there a history behind the name?

Plymouth Support

The name is trivial – Steal (Stealer) C (C Language), Stiller written in C

What does the name STEALC means? is there a history behind the name?

название банальное — steal (stealer) c (c language), стиллер написанный на c

g0njxa

What makes StealC different from other products?

Plymouth Support

we are now almost the only ones who provide the ability to keep all your data under control – our admin panel is written in PHP and does not contain any code obfuscation, and you can (and should) install it on your server

almost everyone has long switched to the MaaS (malware as a service) model, in which there is no guarantee that the collected data is available only to the client – if you, as a client, have the opportunity to conveniently sort logs in the admin panel, which is not installed on your server, then be sure that the owners of this software have the same convenient functionality for sorting logs

What makes StealC different from other products?

мы сейчас чуть ли не единственные, кто предоставляет возможность держать под контролем все свои данные — наша админ-панель написана на php и не содержит какой-либо обфускации кода, а поставить её можно (и нужно) на свой сервер

практически все уже давно перешли на модель MaaS (malware as a service), при которой нет никакой гарантии, что собираемые данные доступны только клиенту — если у вас как у клиента есть возможность удобно сортировать логи в админ-панели, которая не установлена на вашем сервере, то будьте уверены — такой же удобный функционал сортировки логов есть и у владельцев этого софта

Let's point out this, have you ever seen a StealC panel? Maybe is something that we need to take a look...

g0njxa

Since when has StealC been operating?

Plymouth Support

Our software went on sale in January 2023, but closed tests began in the summer of 2022

Since when has StealC been operating?

в продажу наш софт вышел в январе 2023 года, но закрытые тесты начались еще летом 2022

g0njxa

How many people do you think have tested the product? Approximately

Plymouth Support

Before the sale, our software was issued to several teams, a total of about 40 people took part in the tests (we can count by the number of unique builds issued by each of the closed test versions) Now

we do not disclose the number of our clients, we can name an approximate number – several hundred

How many people do you think have tested the product? Approximately

до продажи наш софт был выдан нескольким командам, в общей сложности около 40 человек приняли участие в тестах (можем посчитать по количеству выданных уникальных билдов каждой из закрытых тестовых версий)

сейчас количество наших клиентов мы не раскрываем, можем назвать примерное число — несколько сотен

g0njxa

STEALC uses a unique log exfiltration by parts on exe builds. This type of communication between build and server panel has been imitated by other products, what is your opinion?

Plymouth Support

As far as we know, Vidar has only recently switched to the scheme of transferring files by individual requests, rather than building ZIP on the client side

when we started development, there was no software on the market with such a system for transferring data to the server – everyone relied on the ZIP build on the client

side closer to our public release Raccoon introduced a similar technique

STEALC uses a unique log exfiltration by parts on exe builds. This type of communication between build and server panel has been imitated by other products, what is your opinion?

насколько нам известно, vidar только недавно перешел на схему передачи файлов отдельными запросами а не сборкой zip на стороне клиента

когда мы начинали разработку, на рынке не было софтов с подобной системой передачи данных на сервер — все полагались на сборку zip на стороне клиента

ближе к нашему публичному релизу похожую технику ввел у себя raccoon

g0njxa

you said your administration panel is written in php, is always like that? Some "expert" people confuses StealC with other products because of the similarities with the scheme for transferring files

Plymouth Support

Our panel was originally in PHP and we didn't have any other options, but there is an internal version of Stealc that accesses a server written on C#

sockets via TCP, but it has not been made public and is used by several clients in targeted attacks

On the reverse side behind the socket server there is still a PHP admin panel, the only difference is in the scheme of data transfer from build to server

This version is still in test form and is needed to decrypt all data on the server side (reading the database of Firefox browsers, Chrome browsers and decrypting them using a pre-assembled key from the local state)

We find it convenient, and there is no way to protect ourselves from reverse and further use of our developments, so we take it simply

You said your administration panel is written in php, is always like that? Some "expert" people confuses StealC with other products because of the similarities with the scheme for transferring files

наша панель изначально была на php и других вариантов у нас не предусматривалось, но есть внутренняя версия stealc которая обращается по tcp к серверу написанном на сокетах с# но она не вышла в паблик и используется несколькими клиентами в точечных атаках

на обратной стороне за сокет сервером находится все равно php админ-панель, отличия только в схеме передачи данных от билда к серверу

эта версия все еще находится в тестовом виде и нужна для расшифровки всех данных на стороне сервера (чтение бд firefox браузеров, chrome браузеров и их расшифровка с помощью заранее собранного ключа из local state)

мы находим ее удобной, а от реверса и дальнейшего использования наших наработок никак не защититься поэтому мы относимся к этому просто

Have you ever heard of the private StealC variant written in C#?

g0njxa

Does StealC allows working on CIS countries? What is your opinion of people working with russians with other product?

Plymouth Support

Our software does not work in the CIS countries and will never be for those who allow their clients to work in the CIS, everything is clear – mainly now they are natives of Ukraine (who do not consider themselves to be

in the CIS), but personally we are still faithful to the rules and even despite the current problems, we prohibit work in Ukraine as well

Does StealC allows working on CIS countries? What is your opinion of people working with russians with other product?

наш софт не работает по странам СНГ и никогда не будет

к тем, кто позволяет своим клиентам работать по СНГ все понятно — в основном сейчас это выходы из Украины (которые себя за СНГ не считают), но лично мы все еще верны правилам и даже не смотря на нынешние проблемы запрещаем работу по Украине в том числе

g0njxa

stealc is not usually used by teams, more likely an option for individuals. Do you think your product can be used by these people and replace other products in the future?

Plymouth Support

I would argue – we have a lot of teams among the clients, for some teams we have a special version of the admin panel with the configuration of users and their rights
, in the future this functionality will go to the public version

Stealc is not usually used by teams, more likely an option for individuals. Do you think your product can be used by these people and replace other products in the future?

*я бы поспорил — у нас много команд в числе клиентов, для некоторых команд у нас есть специальная версия админ панели с настройкой пользователей и их прав
в дальнейшем этот функционал перейдет и в публичную версию*

g0njxa

Speaking about the market, how do you see it? Is a good time to work?

Plymouth Support

There is no such thing as a good time – in the moment everything looks like an inconvenient time)

g0njxa

why man? some people says is good other that there is a shortage of products? what you think

Plymouth Support

Such statements have always existed, perhaps now they have become louder due to the arrival of too many poorly trained and not particularly eager to

learn people in the topic

There have always been those who lacked something – there was an Azorult Everyone missed a pony, an Azorult closed A mole appeared – everyone lacks an Azorult already, a Mole has closed, someone else has appeared – everyone lacks a Mole and an Azorult, "But in general, there was once a pony, this is yes it was convenient"

you need to whine less and work more, learn – and then there will be no problems)

Speaking about the market, how do you see it? Is a good time to work?

хорошего времени не существует — в моменте все выглядит как неудобное время)

why man? some people says is good other that there is a shortage of products? what you think

подобные высказывания всегда были, возможно сейчас они стали громче за счет прихода в тематику слишком большого количества плохо обученных и не особо горящих желанием обучаться людей

всегда были те, кому чего то не хватало — был азорульт всем не хватало пони, закрылся азорульт появился крот — всем не хватает уже азорульта, закрылся крот появился еще кто-то — всем не хватает крота и азорульта, “а вот вообще пони был когда то вот это да удобно былооо”

нужно меньше ныть и больше работать, обучаться — и тогда проблем не будет)

g0njxa

what are your plans on the future of StealC?

Plymouth Support

continue to improve our product and release new ones – we have had our resident bot in development and testing for a long time

What are your plans on the future of StealC?

продолжать улучшать наш продукт и выпускать новые — у нас уже долго находится в разработке и тестах наш резидентный бот к примеру

g0njxa

and last question :)

What would you say to those “information security experts” who are trying to track StealC?

Plymouth Support

We can wish you good luck, finally understand that viruses are almost always "encrypted" in the wild, and if you come across a 5 megabyte Stealc sample, it does not mean that it weighs 5 megabytes in the original) Very often attribute various anti-emulation techniques that are used by cryptors to our and other software, although this is wrong on their part

What would you say to those “information security experts” who are trying to track StealC?

можем пожелать удачи, наконец понять что вирусы практически всегда в дикой среде “закриптованы” и если вам попался образец stealc весом в 5 мегабайт, это не значит, что в оригинале он весит 5 мегабайт) очень часто приписывают различные техники антиэмуляции, которые используются крипторами к нашему и другим софтам, хотя это неверно с их стороны

The end?

Remember to check the other interviews at: [g0njxa — Medium](#)

Expect more content,

Best regards.

[@g0njxa](#)

Source: <https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-stealc-cbe5c94b84af>