Approaching stealers devs : a brief interview with StealC

g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-stealc-cbe5c94b84af

g0njxa December 5, 2023

g0njxa

--

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.

Let's see, StealC: @plym0uth

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.

> **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*

> **What does the name STEALC means? is there a history behind the name?**
>
> *название банальное — steal (stealer) c (c language), стиллер написанный на си*

> **What makes StealC different from other products?**
>
> *мы сейчас чуть ли не единственные, кто предоставляет возможность держать под контролем все свои данные — наша admin-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 admin-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…

> **Since when has StealC been operating?**
>
> *в продажу наш софт вышел в январе 2023 года, но закрытые тесты начались еще летом 2022*

> **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*

> **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*

> **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 c#но она не вышла в паблик и используется несколькими клиентами в точечных атаках*
>
> *на обратной стороне за сокет сервером находится все равно php admin-панель, отличия только в схеме передачи данных от билда к серверуэта 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#?

> **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 выходцы 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*

> **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 правв дальнейшем этот функционал перейдет и в паблик версию*

> **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)*

> **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*

> **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