Approaching stealers devs : a brief interview with Vidar

g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-vidar-2c0a62a73087

g0njxa November 30, 2023


FatefulSigns.com

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, Vidar: (As requested, identity can't be disclosed)

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 VIDAR to someone who has never used it?**
>
> *VIDAR — это Stealer, который используется для получения данных с компьютера, на котором был запущен наш продукт.Если человек знает, для чего создано это приложение, но не когда не был нашим клиентом, мы можем посоветовать написать нашей службе поддержки, которая всегда подскажет все преимущества нашего продукта.О продукте можно говорить много, но ключевые качества это*
>
> ** Быстрая и оперативная техническая поддержка* Стабильные и постоянные обновления* Прогрессивный и удобный WEB интерфейс* Огромный функционал продукта.* Опытная команда, где каждый человек занят своим делом* Хорошая Инфраструктура проекта*

> **What is the history of the name VIDAR? I can read the full description on your site, but I would like a summary)**
>
> *Название Vidar пришло совершенно случайно, долго о нём не задумывались и оно запало нашим клиентам в душу!*
>
> *Vidar — бог молчания, большая масса наших клиентов является именно профессионалами своего дела и не рассказывают о своей работе :)Так же мы выбирали созвучное звучание, которое легко звучит и читается, что позволило бы клиентам запомнить нас.*

Regarding the Vidar text shown at their sites:

Who is Vidar

Hail to the Silent One!
Hail to Leathershod!
Hail to the Wolf Ripper!
Hail to the Far-Seer!
Hail to the Survivor of Old Times!
Hail to the Son of Odin!
Hail to Fenrir's Bane!

Vidar is a god from the Aesir family of gods. He is the son of the chief of those gods, Odin. Vidar was born to avenge his father.

In the Voluspa, it tells of a coming final battle where the gods will fight their enemies, the giants. One of the enemies is a wolf called Fenrir. This wolf will, according to the prediction, swallow Odin.

Odin is a clever fellow. Knowing his fate, he conspired to make some changes in the way things work in the future. He sought out the correct mother for this purpose, and created Vidar. It would be Vidar's job to destroy Fenrir.

Vidar grew quickly. His strength became as great as the strongest of the Aesir. He was a skilled warrior and learned his trade fast. But there is more to him.

Because he was born for the future, he had the gift of foresight. That is why he is called Vidar the Far-Seer. He knew the nature of the future, but he did not tell the things he saw. It is for this reason that he is called Vidar the Silent. He knows the patterns of the future and the likely outcome of things.

He knows that in the last battle, the wolf will swallow his father and that Vidar will but his great boot on the lower jaw of the wolf and use his hands to hold the upper jaw. From this position, he will tear the wolf apart, releasing a great wind from the beast's belly. There is speculation that this great wind is actually Odin making his escape.

This act of rending the wolf is why Vidar is called Wolf Ripper and Fenrir's Bane. His reinforced boot, for standing on the wolf's lower jaw, is why he is called Vidar Leathershod.

When the last battle is over, and the worlds are renewed, Vidar will be one of the surviving gods. He will be a Survivor of Old Times.

Vidar is not an idle god while waiting for the wolf to die. He is an active part of even this noisy world. You can often find his presence in the silent places of nature. You can find him nudging mankind into the future as we explore science and space. He is a god of patience and foresight. He is a god of inspired thought and hope for better days. He is a god of seeing the patterns and estimating where they are likely to go.

Most importantly, Vidar is a sympathetic and caring god. He knows that humans plan the best they can despite their limitations. He knows we race to our future without really knowing where we will go. If he seems silent and grim, it is because he does know where we are going and he sometimes feels bad for us.

Vidar may not answer your questions directly; he has earned the name Silent One. However, if you can find the silent places and still the noise in your mind, he may help you see the patterns the way he does. That may be all the answer you need.

> **What makes Vidar different from other products?**
>
> *Конкурентов у нас мало, трудно говорить о различиях, так как общий основной функционал у всех один.*
>
> *Тем не менее, я уже выше описывал наши преимущества перед другими продуктами.Самое главное наше отличие — это*
>
> ** Молниеносная техническая поддержка наших клиентов* Стабильность* Мы первые были на рынке по системе MAS (Аренды) и нас начали копировать*

Pioneers in the MaaS market

> **When did the Vidar project started?**
>
> *В конце 2018 года 19.11.2018г*

That makes Vidar one of the oldest projects still active as for now. 5 years of operations without cease.

> **How many people have tested Vidar? Approximately**
>
> *Мы не можем разглашать нашу информацию, клиентов у нас не мало. Наш продукт считается достаточно солидным и даже те кто уходили к конкурентам, обычно возвращаются к нам*

> **What do you think about those who say that Vidar is a copy of ARKEI?**
>
> *Мы не Arkei, но первые версии были построены на исходниках этого продукта, которые были куплены у бывших разработчиков. За это время продукт полностью был изменен.У нас только один продукт.*

> **I saw that updates are coming out every week since 07/01/2022. It's a lot of work, does it really guarantee a clean and correct product? What do you think was the biggest update to VIDAR?**
>
> *Каждую неделю мы выпускаем обновление продукта, порой выпускаем 2 или даже 3 раза в неделю. Это позволяет поддерживать наш продукт в чистоте со всех направлений.Этот процесс обязательный, так как нам нужно менять сервера, прокладки, а так же чистить сам код и запутывать следы.*
>
> *У нас нет самых больших обновлений, мы всё делаем постепенно и развиваем наш продукт с конца 2018 года.*

The January 7th, 2022 date was mentioned because this is the first upgrade statement that can be found now at their site:
"1.3 — Второе тестовое обновление Проверяем систему уведомлений" | 1.3 — Second test update Checking the notification system.
Since this day a weekly update statement is released, most of them cleaning Vidar for AV detections.

Vidar was asked about this situation:
07/01/2022 — We have been releasing updates every week since 2018.
2022 — we changed the server and moved the old data to the archive.

At the time of publishing this article, Vidar is on version 6.7

At November 6th, 2023, a major update was released, changing Vidar C2 communications:

```
Переписана полностью вся кодовая часть софта.
Теперь отправка лога осуществляется частями(пофайлово).
За счёт пофайловой отправки улучшили отстук порядка +15-20 процентов.
Улучшили рантайм. Улучшили валидность гугла.
Улучшили определение дубликатов (добавили новый формат hwid, учитывающий не только
железо, но и учетную запись системы).
Улучшили граббер файлов, так же добавили новые настройки сбора файлов. Полностью
переработали поддерживаемые браузеры, кошельки и плагины - теперь мы можем добавлять
их без ребилда (если мы добавили кошелек в обнове, то и на старом билде начиная с
этой обновы он будет собираться).
Улучшили сбор информации о системе. Версии билда - формат .dll и dll внутри билда -
временно не доступны они будут доработаны в самое ближайшее время.
В ближайшее время перейдем полностью на отправку через https протокол.

The entire code part of the software has been completely rewritten.Now the log is
sent in parts (by file).Due to file-by-file sending, the response rate was improved
by about +15-20 percent.Improved runtime. Improved Google validity.Improved detection
of duplicates (added a new hwid format that takes into account not only the hardware,
but also the system account).The file grabber has been improved and new file
collection settings have been added. We have completely redesigned supported
browsers, wallets and plugins - now we can add them without rebuilding (if we added a
wallet in an update, then it will be built on the old build starting with this
update).Improved collection of information about the system. Build versions - .dll
format and dll inside the build - are temporarily not available; they will be
finalized in the very near future.In the near future we will switch completely to
sending via the https protocol.
```

> **VIDAR uses Telegram and Steam for exfiltration, have you ever thought about using other methods?**
>
> *Мы использовали множество способов, но на текущий момент самым стабильным и успешным является Steam + Telegram (Так же у нас есть возможность использовать другие сервисы для наших клиентов)*

I was talking about the **dead drop resolvers** used by Vidar builds. The most common example is:

Source: Cert AgID on X: ()
I could never find any other example on any other domain.

> **Vidar is not usually used in teams or large groups. Is this your goal or am I wrong?**
>
> *У нас работают большие команды, у нас есть для этого специальный функционал. На базе нашего продукта , вы можете создать свой Stealer, где сможете разграничивать права своим пользователям и выдавать им индивидуальные сборки продукта.*

I was speaking about the fact that I can't find any source of a group using Vidar as their main source of goods, indeed, Vidar is one of the top 5 stealers in the market but their users are doing a good job hiding their activity. *Vidar, the god of silence*Activity, not their builds ;)

> **I want to ask if VIDAR can work in CIS. What do you think about the people working with Russians?**
>
> *Мы не работаем в таких странах как Беларусь, Россия и Казахстан (Это наши личные принципы, которые важны для нашего сообщества). Продукт в данных странах не будет работать.*

> **How do you see the market, is now a good time to work?**
>
> *Время всегда хорошее, всегда удачное — сейчас намного сложнее чем раньше, поддерживать такой продукт, но мы справляемся*

> **Do you have anything to say to the "information security specialists" who are actively hunting for VIDAR?**
>
> *Хотим сказать, что не нужно держать на нас зла. Мы думаем, что наши данные уже известны таким структурам как ЦРУ, ФБР и прочим структурам, так же как и нам известны их данные, ведь они тоже запускают наш продукт, порой совершенно случайно! :)Каждый делает свою работу.*

Are LEA's often targeted with Vidar? No way that office guy is downloading the *Microsoft 2023 Crack Free* from an untrusted source :p

Be wary of suspicious downloads, links or attachments. Protect yourself of threats, I expect we will have Vidar for a long time.

The end?

Remember to check the other interviews at: g0njxa — Medium

Expect more content,
Best regards.

@g0njxa