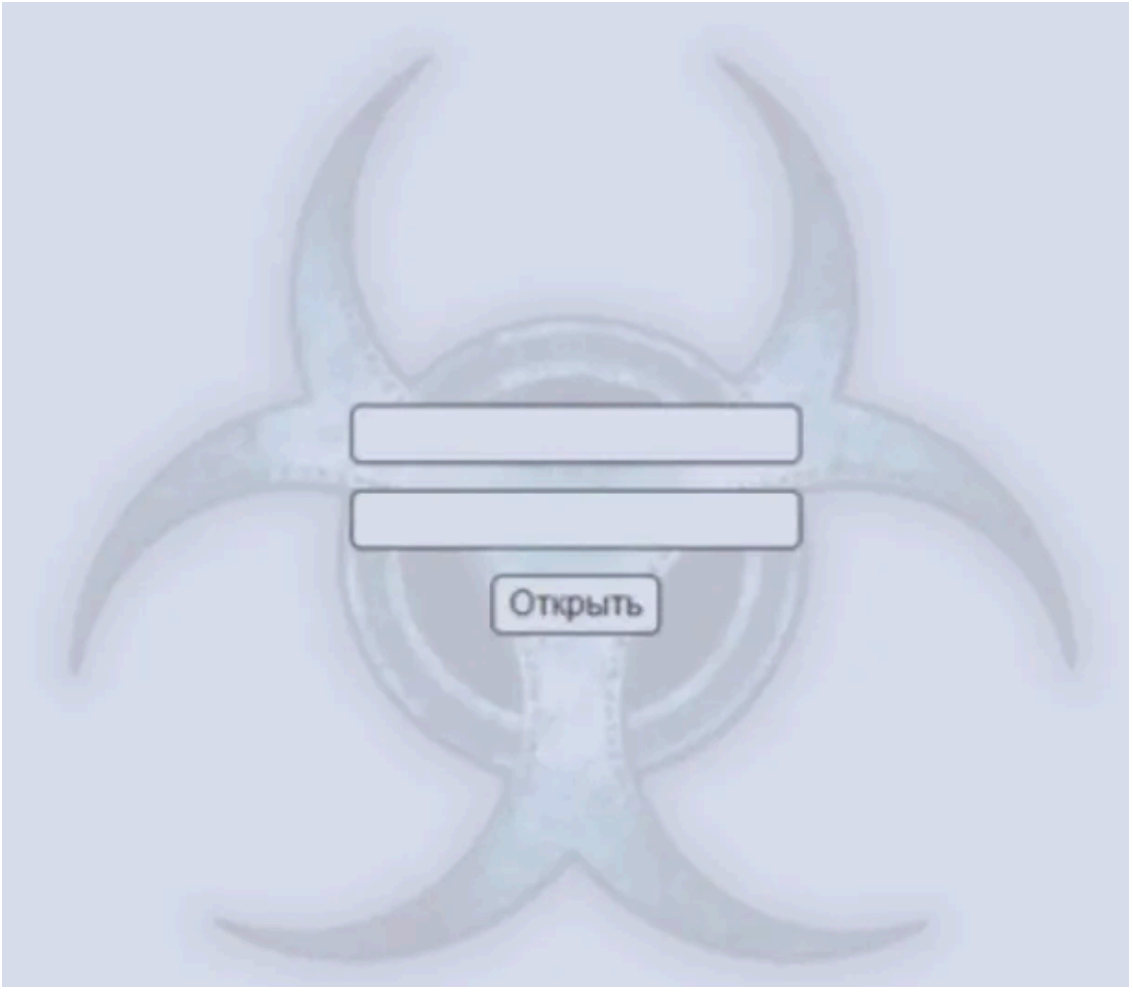
Approaching stealers devs : a brief interview with Amadey

By g0njxa

Published: 2023-12-02 · Archived: 2026-05-05 02:17:21 UTC

5 min read

Dec 2, 2023



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, Amadey Loader: a talk with **InCrease**, owner of Amadey.

The interview was made in English, everything shown here is the original text of the interview.

g0njxa

How would you describe Amadey?

InCrease

At the development stage, it was supposed to be perfect. Smoke Loader was outdated at that time (2018) and did not suit me anymore. In the short term – still perfect

Amadey is a malware known as a "loader": *its main functionality is to load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.* In this case, he says that another famous "loader" (Smoke Loader) didn't meet the requirements of his work and developed his own tool. That's why Amadey was created.

g0njxa

What does the name "Amadey" means? Is there a history behind the name?

InCrease

There were big problems with the name, until the release, the investor and I could not decide on the name. The working title of the project was a1

Then he suggested the Amadey name, and I approved it because it was sonorous and could cause problems with google searches.

Amadey was (and is) developed by his owner, InCrease. As I understood, the project is only managed by him, and the initial budget was raised by an unknown investor.
Was "a1" a better name than Amadey? The argument about search engine indexation was outdated a long time ago.

g0njxa

What makes Amadey different from other products?

InCrease

At first glance, a loader seems to be a simple program, but as soon as it gets all the necessary functions, it becomes very buggy. At the stage of development and constant cleaning, errors constantly occur. You can't just write a loader, you need a lot of tests and preparation to identify and fix errors.

My code differs from others because it works without errors, or with a minimum of errors due to the fault of the testers. This is what makes it different from others. I have seen the sources of other loaders – there are a lot of "human errors", even the parameters of function calls are mixed up.

Amadey works perfectly without errors, and if some error is found, it is the “tester’s” fault. We can consider the tester as the customer.

g0njxa

Since when has Amadey been working?

InCrease

8 of October 2018

writed and tested in summer 2018

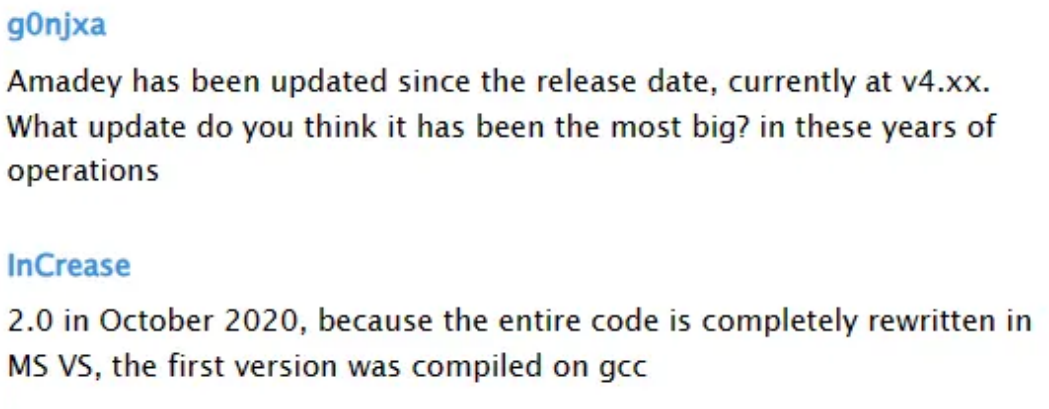
Recently Amadey was at its 5th anniversary:
https://x.com/g0njxa/status/1713264658747166799

g0njxa

How many people do you think have used your product? Approximately

InCrease

I know it, but I can't say anything because this is not public information. Quite a lot.



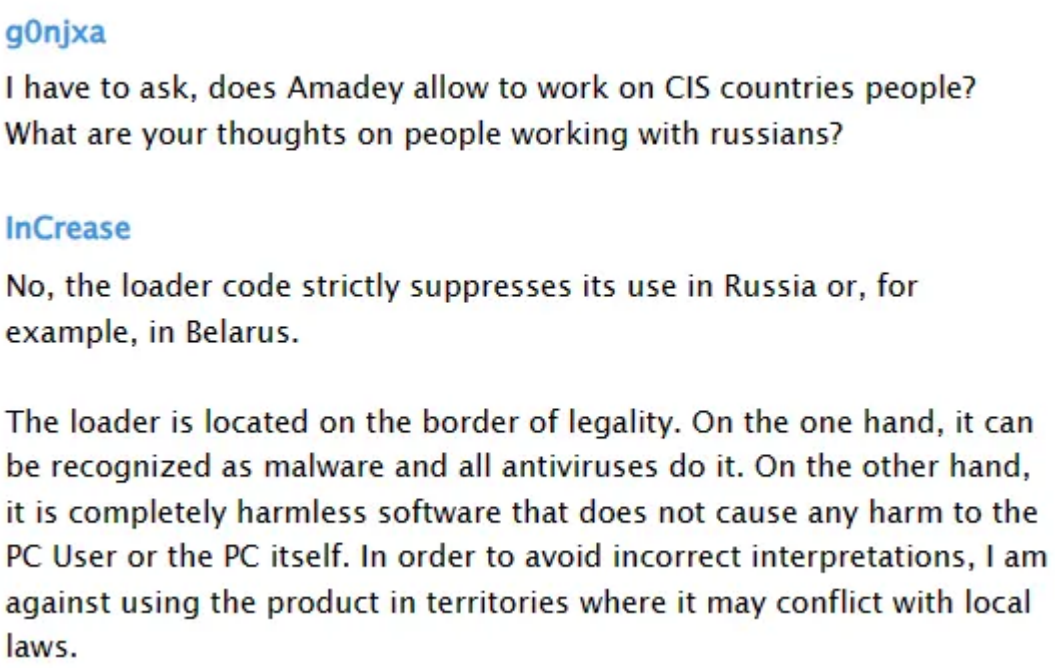
A big update was released at the 5th anniversary (Amadey V4). Find the release statement here: https://x.com/g0njxa/status/1715089181071016073

```
gcc Amadey.c -o Amadey
```

Please find the original release statement where he talks about the v2.00 updates:

```
AUGUST 24, 2020

Немного новостей - полным ходом идет закрытое альфа тестирование версии 2.00

[!] Так как за два года текущий код всем прилично примелькался.... Полностью новый EXE, др

[!] По вышеуказаной причине - без проблем x64 версия.

[+] Правильный (!) запуск вашего шеллкода в памяти (fileless | bodyless | безфайловый)! + Пр

      Долгое время не удавалось правильно реализовать этот момент в связи с его сложностью

[+] Новый автозапуск! Абсолютно без реестра.

[+] Улучшена система скачивания, в случае неудачи лоадер будет пытаться еще несколько раз, н

[+] Система контроля за исполнением загруженных и запущенных файлов - перезапуск в случае

[+] Система контроля за основным файлом - если процесс кем-то или чем-то снят, то он будет

[?] Система контроля за основным файлом, автоматическое скачивание с СС в случае его удале

[+] Новая система обфускации - уже  более месяца удачно применяется на версиях 1.99.x и усп

[+] Улучшена логика потоков, как и в сегодняшнем обновлении 1.99.5

[+] Улучшена Панель Управления | Command Center, расширена статистика по заданим для юнита,

[?] Тестируются новые решения выхода из Low Mode

[+] Убраны моменты, за которые очень цеплясь АВ, такие как получение ИД например.

[+] Новая система плагинов, в основном нацеленная на определение разрядности ОС и использо
```

```
[+] Улучшена и без того отличная стабильность(!) Альфа версия - 500 тысяч синхронизаций с CC

[*] Еще много major/minor фишек/плюшек/нововведений/красивых решений и т.д. о которых буд

[*] Релиз запланирован на октябрь-ноябрь 2020.

P/S После релиза скидки точно будут отменены на ближайшие пол-года/год.
```



Amadey follow its own Anti-CIS policies.

Get g0njxa’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Amadey owner says that his product is completely harmless and he is against the use of it, if it is used against local laws.

g0njxa

Amadey has been an object of study by some "security experts" because of his high activity as seen in the wild. These people sometimes find the way to get into the Panel and then they share the findings. How do you prevent that people can do this and how do you identify the vulnerabilities that are being exploited?

InCrease

Yes, they often end up in control panels. But the hacking was recorded only once, all other penetrations were the fault of another software. I get information about possible vulnerabilities from numerous enthusiasts on the forum, clients, testers. Also, sometimes an independent audit is conducted by specialists.

The information received is not valuable in terms of statistics, even if someone gets access to a dozen of panels, it will not give him any information about the whole picture.

g0njxa

you said "But the hacking was recorded only once, all other penetrations were the fault of another software." Can you explain?

InCrease

many clients put a lot of different software on one server, as well they leave vulnerabilities like open remote access to SQL and so on.

there are also problems with our hosters from the forum, there have been cases that the IP of the server belonging to my client was transferred by the hoster by mistake to another client of mine. With all the botnets on it.

As said before, he states that if there is any issue with Amadey, is the fault of the client, “tester”, customer as a result of misconfigurations.

g0njxa

I want to dive a little bit about this issue, there was a vulnerability on Amadey that let researchers to get a reverse shell, being exploited until june 2023

people says 1000 amadey panels were exploited and 7 million devices were found

InCrease

yes, but the main problem is to find the panels, there are a lot of them

100% not true =)

g0njxa

this findings were shared on DEFCON this year, how do you specifically found this issue and you fixed it?

InCrease

the parts of the code that had the problem were rewritten for version 4

the entire panel-bot dialog is encrypted in both directions using a unique rc4 key for each client. The parts of the code that had the problem were rewritten for version 4

g0njxa

okay but this were fixed in june 2023

InCrease

Yes, but 1000 panels just didn't exist this year

g0njxa

1000 panels since december 2022

InCrease

I didn't have so many clients and builds in either 2022 or 2023

Amadey was asked about these issues based on the findings of an amazing security researcher: @evstykas

In his DEFCON 31 (2023) presentation: *The Art of Compromising C2 Servers: A Web Application Vulnerabilities Perspective*, Vangelis Stykas exposed how he was able to find multiple vulnerabilities ON the Amadey's code.

Please if you still didn't watched this presentation, I found mandatory to watch it:

As exposed, starting at December 2022 until the patch at June 2023, more than a thousand Amadey instances were accessed with over 7 million devices compromised. Amadey owner denies these statements.

> **g0njxa**
>
> what are your plans for Amadey in the future?
>
> **InCrease**
>
> hVNC is the most anticipated and expected plugin. There won't be more big updates, just the evolution of what Amadey is

hVNC is a common feature on Remote Access Tools, and soon will be a feature of Amadey.

> **g0njxa**
>
> What would you say to those "information security experts" who are trying to track Amadey?
>
> **InCrease**
>
> Well, like any loader, it's just a tool
>
> It can be a weapon in some sense. But by itself, it is harmless and is used by many system administrators completely legally and voluntarily. Then Mikhail Kalashnikov must be recognized as a criminal, because he invented something that killed thousands of people – the Kalashnikov assault rifle.

What should be considered a "criminal"?

The end?

Remember to check the other interviews at: g0njxa — Medium

Expect more content,
Best regards.

@g0njxa
