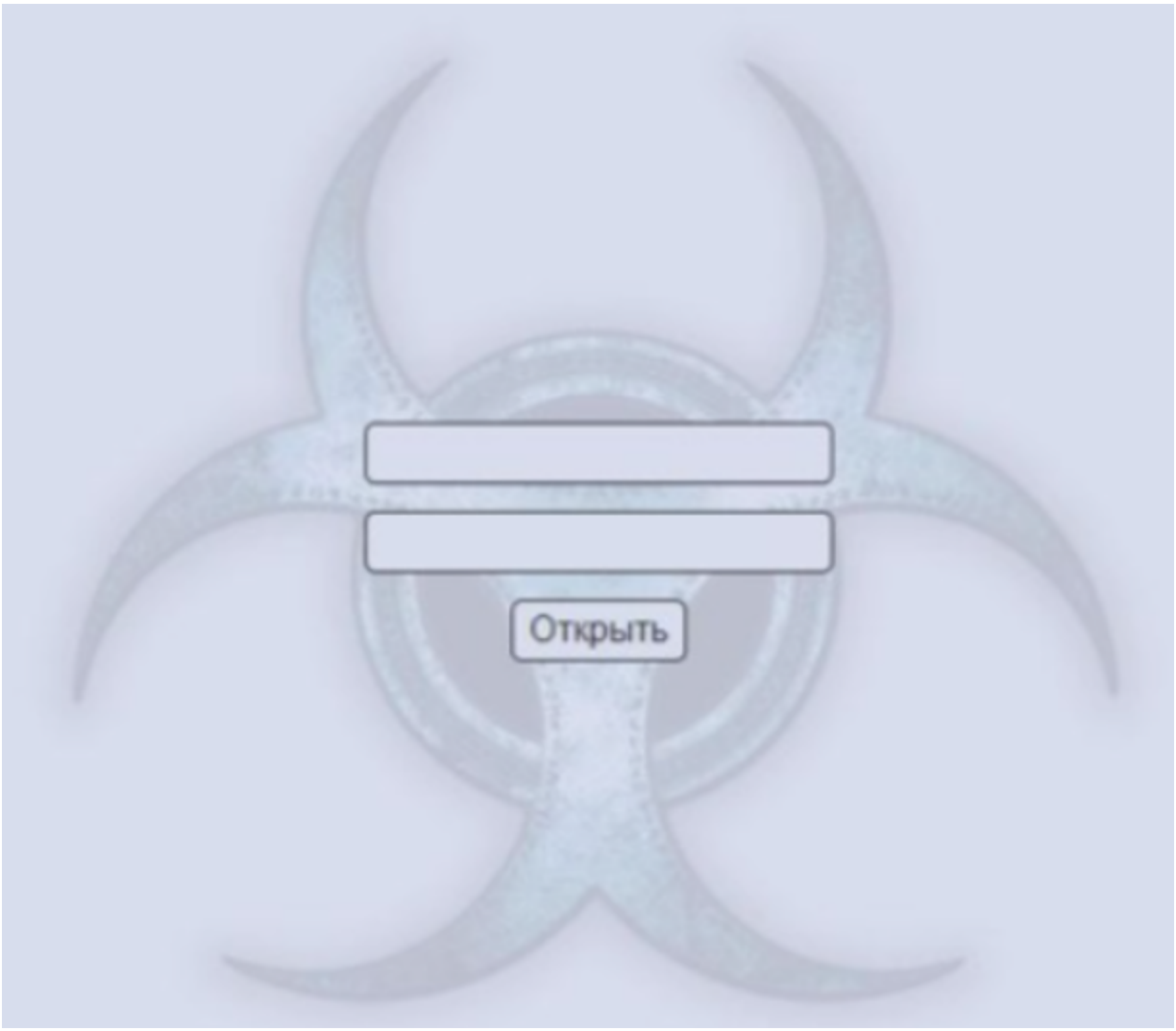
Approaching stealers devs : a brief interview with Amadey

g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-amadey-56c8c6ea0ad6

g0njxa December 2, 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, 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.

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.

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 The argument about search engine indexation was outdated a long time ago.

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.

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

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, другой код, другой компилятор (Visual Studio C++ 2019 в новой, вместо gcc в текущей)

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

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

Долгое время не удавалось правильно реализовать этот момент в связи с его сложностью и нестабильностью полуприват/паблик решений - мне не хотелось использовать вариант RunPE с GitHub (как это сделано в некоторых других лоадерах) по причине его глючности - шеллкод то не запускается, то вылетает с ошибкой, то вовсе крашит сам лоадер. И большинство решений все-таки дропают файл на диск, а потом считывают fread, это я не могу назвать безфайловым.

[+] Новый автозапуск! Абсолютно без реестра.

[+] Улучшена система скачивания, в случае неудачи лоадер будет пытаться еще несколько раз, не подвешивая целевой поток.

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

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

[?] Система контроля за основным файлом, автоматическое скачивание с CC в случае его удаления. Тестируется.

```
[+] Новая система обфускации - уже  более месяца удачно применяется на версиях 1.99.x
и успешна против Windows Defender


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


[+] Улучшена Панель Управления | Command Center, расширена статистика по заданим для
юнита, добавлены опции отображения, расширена БД, много мелких изменений. Скорость
работы сохранена.


[?] Тестируются новые решения выхода из Low Mode


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


[+] Новая система плагинов, в основном нацеленная на определение разрядности ОС и
использования нужной версии плагина, в будущем это поможет стилеру в работе с x64
браузерами, такими как FF и еще много плюшек станут доступны.


[+] Улучшена и без того отличная стабильность(!) Альфа версия - 500 тысяч
синхронизаций с CC в рабочих условиях, полет нормальный :)


[*] Еще много major/minor фишек/плюшек/нововведений/красивых решений и т.д. о которых
будет (возможно) объявлено при релизе...


[*] 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.

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

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.

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.

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

What should be considered a "criminal"?

The end?

Remember to check the other interviews at: g0njxa — Medium

Expect more content,
Best regards.

@g0njxa