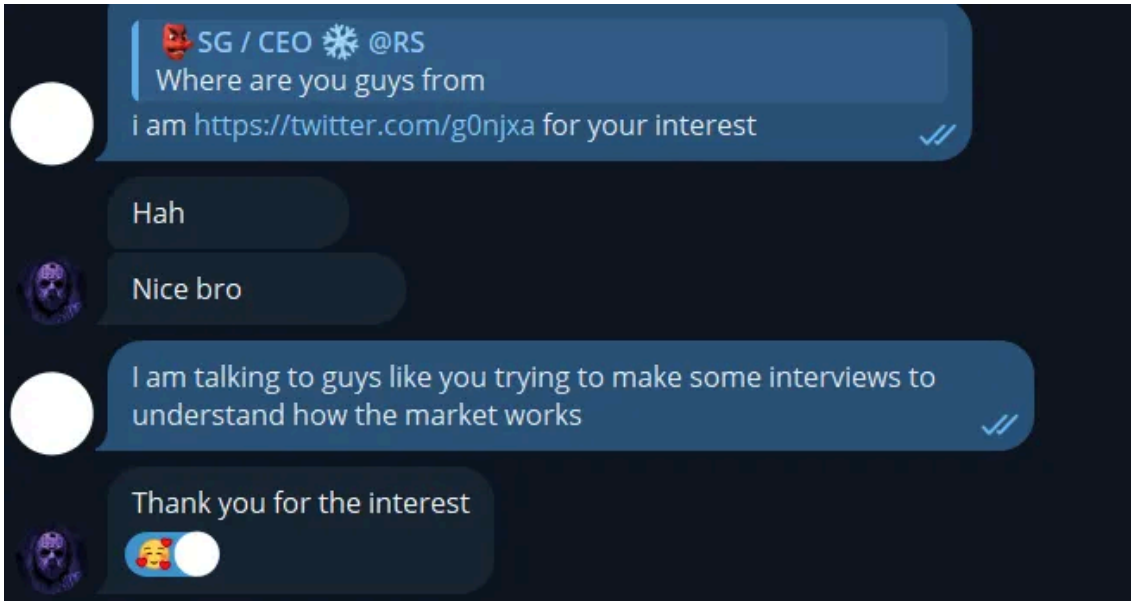
Approaching stealers devs : a brief interview with Recordbreaker

By g0njxa

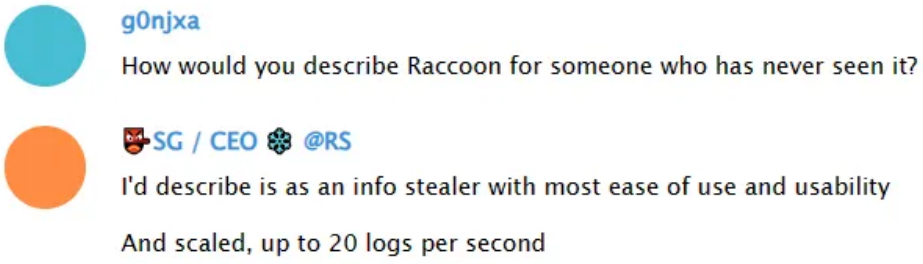
Published: 2023-11-30 · Archived: 2026-04-05 17:20:39 UTC

Let’s see, *Recordbreaker* aka the OG Raccoon but v2: @slaughter_team

The interview was made in English, this was a surprise to me. So everything shown here is the original text of the interview.



Press enter or click to view image in full size



If you are looking a further description, you can always check the sales post on Russian forums: (?)

```
RACCOON STEALER 2.0 We are Back!

Для нас, как и для многих, это были нелёгкие несколько месяцев. Мы были вынуждены закрыть

Но нет худа без добра и мы рады вернуться обратно!

Проект был полностью переписан с нуля. Билд, фронт и бекенд. Мы учли ошибки прошлого и с
```

Билд стал в 10 раз меньше, полностью сохранив все свои старые функции, а также приобрёл но

Помимо качества работы нашего софта, как и прежде, мы уделили большое внимание внешнему

Панель полностью переписана на самых современных библиотеках. Мы сохранили наш мощный г

На бекенде также произошли изменения в лучшую сторону. Мы решили запустить проект, отказа

Также в планах добавить старую систему общих прокси для самых «ленивых» клиентов, кто пред

Всё та же надёжность бекенда, система логирования и алертов, децентрализованная схема и рег

Добавлен бот для Telegram, позволяющий отправлять логи на ваш аккаунт, а также возможность

Прежде чем начать открытую продажу, мы тестировали проект более двух месяцев, как бета ве

Software:

• стилер полностью переписан с чистого листа (также на C++);
• убраны зависимости от CRT, размер исполнительного 55 кб (раньше 580 кб);
• динамический импорт всех функций;
• раньше стилер стучал 2мя запросами - сначала забирал данные, а вторым запросом отправлял
• поддержка SSL. Скоро: поддержка кастомных портов для отстука;
• в стилере больше нет списка поддерживаемых браузеров – весь поиск производится рекурсивно
• расшифровка паролей, куки-файлов, сохранённых карт (CC) хрома (AES GCM) теперь происходи
• на серверной части автоматически определяются адреса кошельков (вы можете настроить block

Поддерживаемые кошельки:
Coinbase
MetaMask
Brave
Ronin

Скоро:
Phantom

• Loader: EXE/DLL/CMD/POWERSHELL.
Вы можете использовать команды POWERSHELL для различных целей (например, фейк-ошибки, или

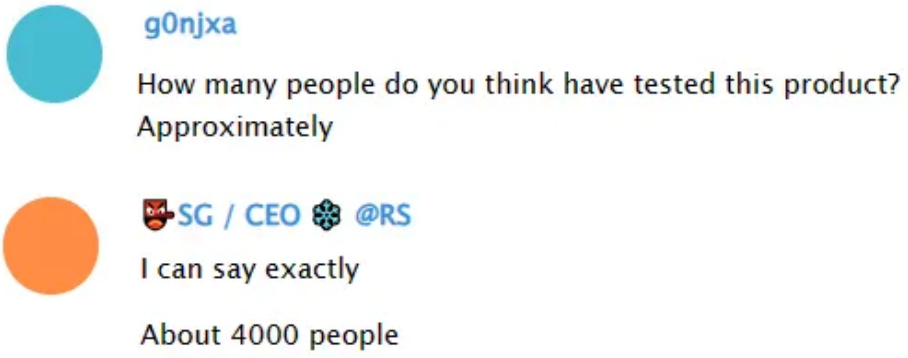
• Grabber: Поддержка ярлыков, рекурсивный поиск, %DSK_235% или %DSK23% для поиска по всем дис

Front-end сохранил свои основные моменты, такие как:

• лаконичность и современность;
• стиль и внимание к деталям;
• гибкую систему поиска с неограниченными возможностями;
• скрытие ненужных элементов;
• копирование информации в 1 клик;
• статусы логов NEW, OPEN или DOUBLE;
• теги и маски поиска;
• смена конфига граббера и дроппера на лету, без перегенерации;
• массовое удаление и скачка;
• комментарии;

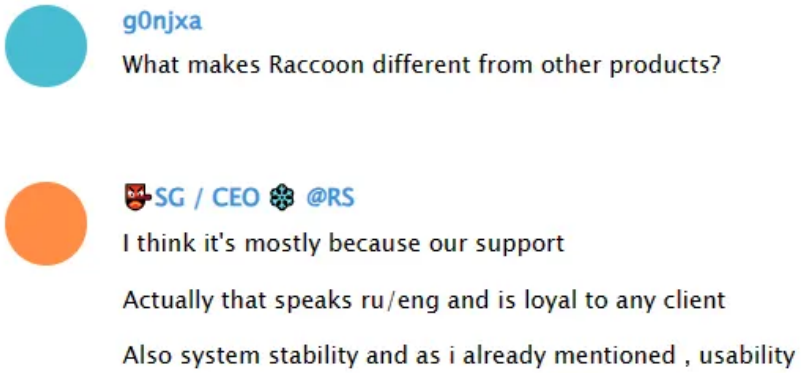
```
• новости;
• информативный FAQ;
• статистика.

Новые функции:

• динамическая таблица логов, позволяющая настроить собственный вид;
• настройка телеграм бота;
• обозреватель блоков кошельков;
• перевод на китайский язык.

 Теперь Вам не нужно вскрывать кошелек, чтобы посмотреть баланс адресов для MetaMask, Brave,
```

I always expect some history behind any name, seems like “Raccoon” is something that vanished over time…

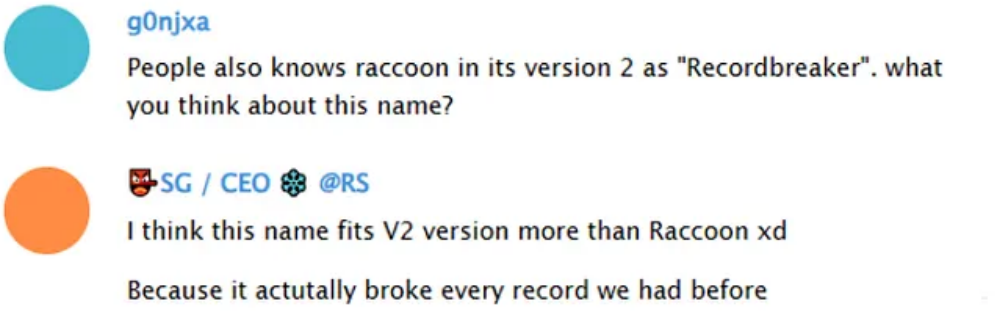


Indeed, a lot. That’s why Raccoon is an infamous project.

Press enter or click to view image in full size

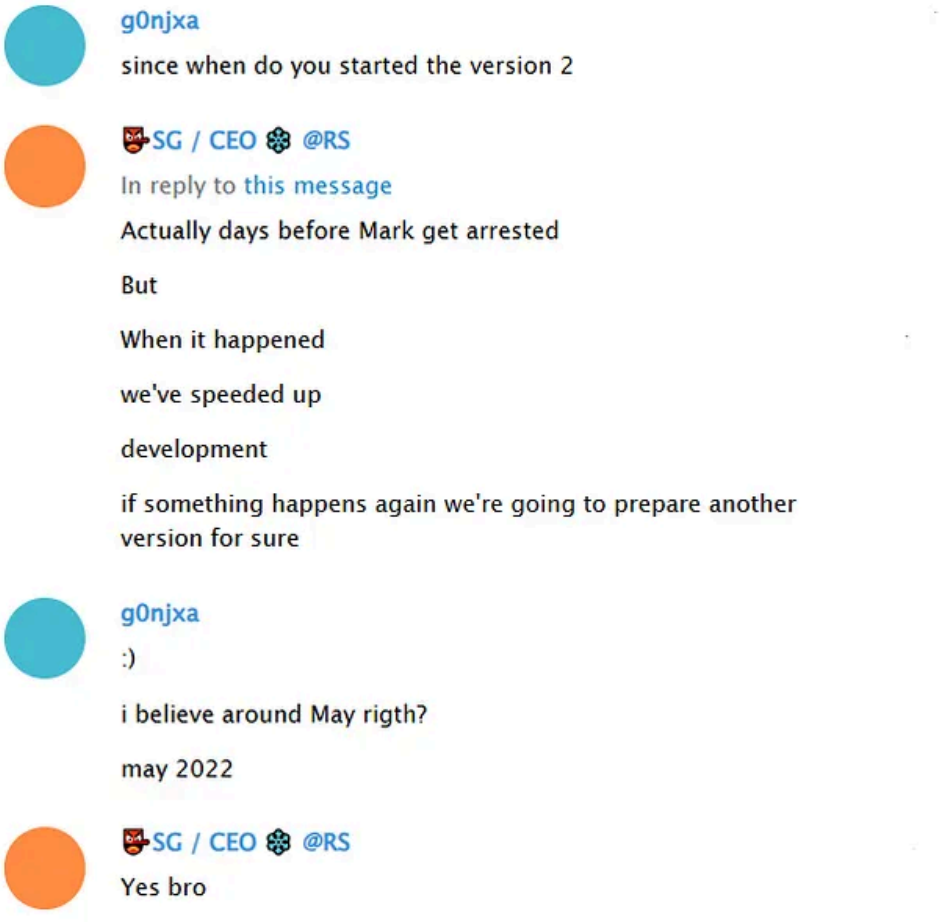


Press enter or click to view image in full size



Recordbreaker is also the first User Agent found on Raccoon V2 builds in order to communicate to C2 servers. Is it also truly a “record breaker” product, one of the most used over time.

Press enter or click to view image in full size

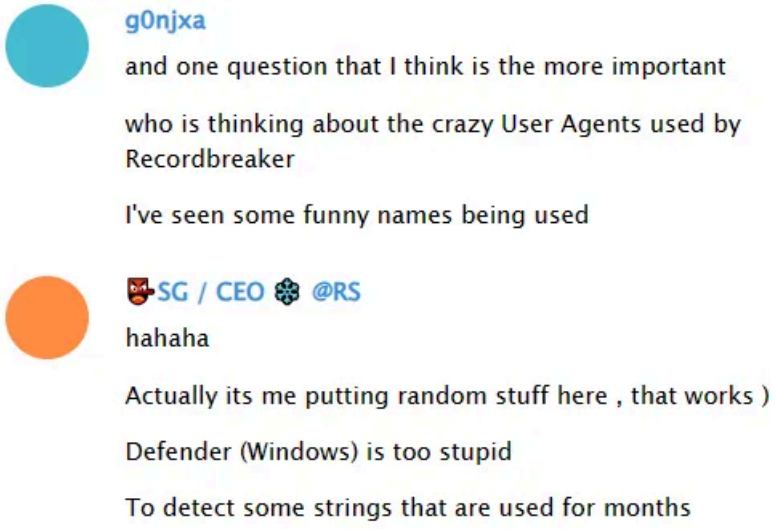


I said May because this is the time when the first v2 statement release was announced, although we know that prior this date there was some “beta testing”, that would correspond with the “speeded-up development” of the product. “Mark” arrestment was produced in March 2023, so that would make a gap of <2 months to finish a new product that I believe it was not at an early stage of development. Indeed, there was a rush to get everything back asap.

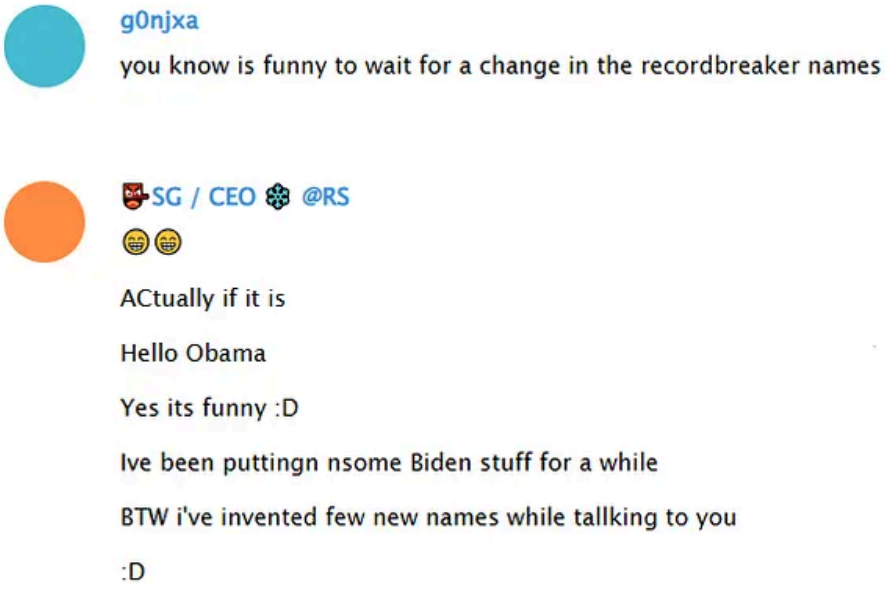
Get g0njxa’s stories in your inbox

As stated, if “Recordbreaker” gets terminated like its predecessor, allegedly, we must expect a **Raccoon V3**!

Press enter or click to view image in full size

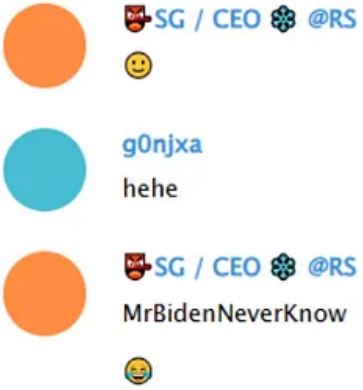


Press enter or click to view image in full size

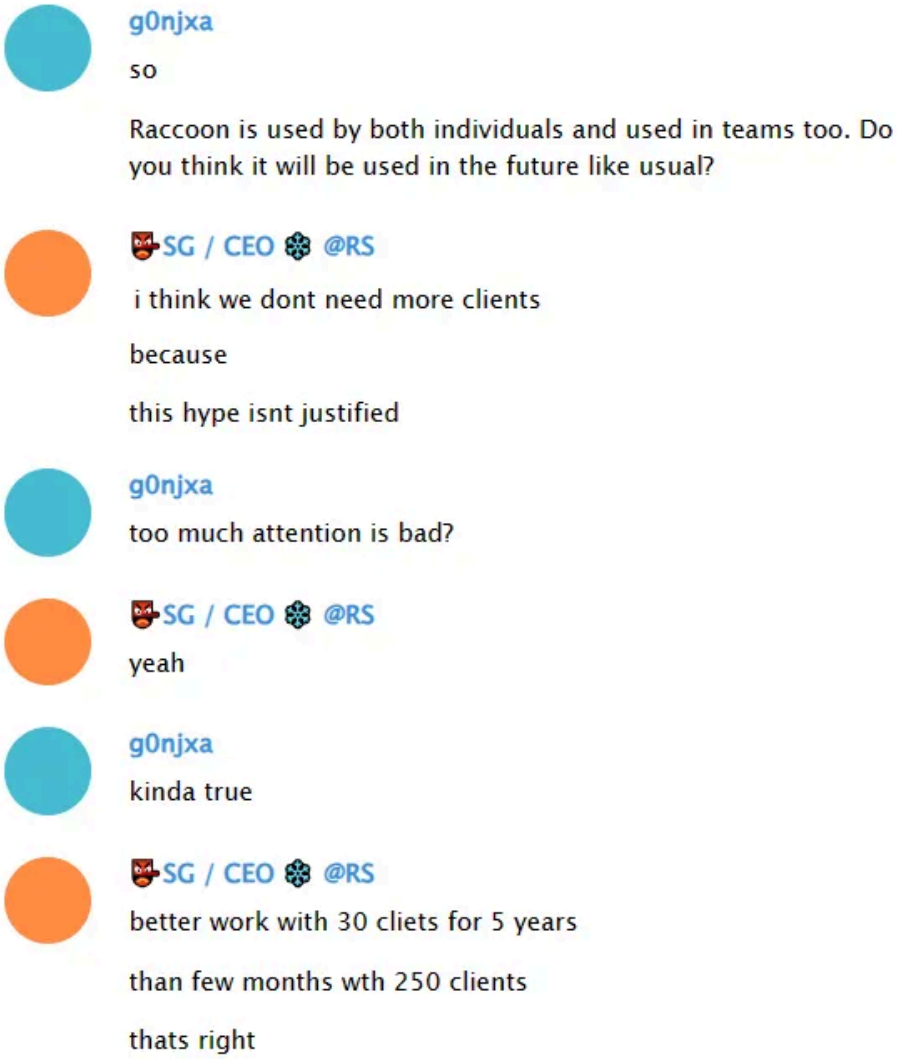


One of the most interesting things I found in Recordbreaker is the custom User Agents being used at builds to reach C2 servers while exfiltrating information from the infected host. One of the best Threat Analysts in the malware hunting community has been making an amazing and persistent tracking on these custom UAs since the release of Raccoon V2, so please find at the bottom of these interview a full diagram of Recordbreaker’s User Agents over time.

Press enter or click to view image in full size



Will "***MrBidenNeverKnow***" the next custom User-Agent? we will see :)



This is an important thought in order to understand the malware market, every project needs to have a different vision for the future. I totally agree that too much attention can be annoying and disturbing for a product team,

especially if there's a point where is possible that you can't handle that much attention.

I don't know how much time we will see Recordbreaker around, but I expect long years of activity. Keep watching!

The end?

Special thanks to @crep1x for his work on Recordbreaker's UA hunt (and a lot more) and also to @suyog41 for his findings on new Recordbreaker builds on the wild. I've also made my contribution to the User-Agents findings, my little grain of sand.
