Approaching stealers devs : a brief interview with Recordbreaker

g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-recordbreaker-f6400c11d58b

g0njxa November 30, 2023

g0njxa

--

Easter egg
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.

Prologue

The original Raccoon Stealer operations were stopped in2022 by law enforcement agencies in a cybercrime operation involving the arrest of a 26-year-old Ukrainian national suspected of his alleged involvement in the Raccoon Stealer campaign and the consequent dismantling of the entire infrastructure behind this malware product.

You can read the news Ukrainian charged for operating Raccoon Stealer malware service (bleepingcomputer.com)

Western District of Texas | Newly Unsealed Indictment Charges Ukrainian National with International Cybercrime Operation | United States Department of Justice

Raccoon Stealer was reborn in a short period of time after these events happened, in a newly created product that was named as the V2 of the original Raccoon.

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.

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 наш весьма успешный проект из-за независящих от нас обстоятельств.

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 сохранили все хорошие идеи, которые пришлись нашим постоянникам по вкусу.

Билд стал в 10 раз меньше, полностью сохранив все свои старые функции, а также приобрёл новые фишки, что сделало логи ещё более информативными! Динамическая отправка информации лога позволила увеличить отстук.

Помимо качества работы нашего софта, как и прежде, мы уделили большое внимание внешнему виду и функционалу панели управления.

Панель полностью переписана на самых современных библиотеках. Мы сохранили наш мощный поиск, теги, маски поиска, теги билдов и многие другие функции (например, обозреватель блоков кошельков и многие другие).

На бекенде также произошли изменения в лучшую сторону. Мы решили запустить проект, отказавшись от общих прокси. Теперь пользователь может пропатчить билд 5-ю IP-адресами и отследить их из панели. Это позволило улучшить отстук, так как пользователи больше не влияют друг на друга.

Также в планах добавить старую систему общих прокси для самых «ленивых» клиентов, кто предпочитает получить стилер «под ключ».

Всё та же надёжность бекенда, система логирования и алертов, децентрализованная схема и регулярные бэкапы.

Добавлен бот для Telegram, позволяющий отправлять логи на ваш аккаунт, а также возможность настроить гибкую отправку по тегам.

Прежде чем начать открытую продажу, мы тестировали проект более двух месяцев, как бета версию, и минимальные ошибки были устранены. Пользователи бета-версии полностью удовлетворены результатом и остаются нашими постоянными клиентами по сей день.

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 полный лог после сбора всех данных. Сейчас данные отправляются частями в течение сбора: каждый профиль браузера отдельно, систем инфо, скриншот. Когда АВ палит файл в рантайме, часть данных, скорее всего, уже у вас в панели;
• поддержка SSL. Скоро: поддержка кастомных портов для отстука;
• в стилере больше нет списка поддерживаемых браузеров — весь поиск производится рекурсивно, поддерживаются почти все браузеры, в том числе, YandexBrowser (кроме стран RU, UA, BY, UZ, AM, KZ, KG);
• расшифровка паролей, куки-файлов, сохранённых карт (CC) хрома (AES GCM) теперь происходит на серверной части, как и форматирование всех .txt файлов и их названий;
• на серверной части автоматически определяются адреса кошельков (вы можете настроить block explorer в панели для проверки баланса кошельков).

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 уведомления MessageBox, отстука в iplogger, и т.п.). Теперь можно выбрать кастомную локацию дропа файла, если вы работаете от LowIL уровня и др.

• Grabber: Поддержка ярлыков, рекурсивный поиск, %DSK_235% или %DSK23% для поиска по всем дискам. Поиск очень оптимизирован и обыщет весь ваш ПК быстрее, чем вы ожидали!

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, Ronin, TronLink. Вы можете сами выбрать block explorer для Eth, Ronin, Tron!

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.

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.

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.

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

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.

Will "" 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.

Author: @Crep1x
Remember to check the other interviews at: g0njxa — Medium

Expect more content,
Best regards.

@g0njxa