Что изощрённый вредонос пытается найти на скомпрометированных устройствах?

Исследователи в области кибербезопасности обнаружили новое вредоносное ПО под названием Fickle Stealer, разработанное на языке программирования Rust – это язык программирования, разработанный компанией Mozilla. Он сочетает в себе производительность и безопасность, позволяя создавать быстрые и надёжные программы.

 Основные особенности Rust включают в себя строгую систему типов, которая позволяет избежать большинства ошибок времени выполнения, а также возможность эффективной работы с памятью и безопасное управление потоками данных. Rust также обладает многопоточностью, что позволяет создавать параллельные приложения.

 Данный язык может быть использован для различных целей, включая создание операционных систем, драйверов, веб-серверов, игр и многих других приложений.

 Rust постоянно развивается и улучшается благодаря активной разработке сообщества, что делает его всё более популярным среди разработчиков." data-html="true" data-original-title="Rust" >Rust. Эта программа направлена на кражу конфиденциальной информации с заражённых устройств.

Эксперты из компании Fortinet – это компания, которая занимается разработкой и производством оборудования и программного обеспечения для информационной безопасности. Она была основана в 2000 году в Калифорнии, а в настоящий момент имеет офисы в более чем 100 странах мира.
 Продукты Fortinet включают в себя решения для сетевой безопасности, такие как фаерволы, VPN, антивирусное и антималварное программное обеспечение." data-html="true" data-original-title="Fortinet" >Fortinet выявили четыре метода распространения Fickle Stealer: VBA dropper, VBA downloader, link downloader и executable downloader. Некоторые из них используют PowerShell-скрипт для обхода контроля учётных записей пользователей (UAC) и запуска вредоносной программы.

PowerShell-скрипт, известный как «bypass.ps1» или «u.ps1», также предназначен для периодической отправки информации о жертве, включая страну, город, IP-адрес, версию операционной системы, имя компьютера и пользователя, в Telegram-бот, управляемый злоумышленниками.

Вредоносная нагрузка Fickle Stealer, защищённая с помощью упаковщика, выполняет серию проверок для обнаружения песочницы или виртуальной машины, после чего отправляет данные на удалённый сервер в формате JSON.

Fickle Stealer собирает информацию из криптокошельков, веб-браузеров на основе Chromium и Gecko (Google Chrome, Microsoft Edge, Brave, Vivaldi и Mozilla Firefox), а также из приложений AnyDesk, Discord, FileZilla, Signal, Skype, Steam и Telegram. Программа также экспортирует файлы с расширениями txt, kdbx, pdf, doc, docx, xls, xlsx, ppt, pptx, odt, odp и wallet.dat.

«Помимо популярных приложений, этот инфовор ищет конфиденциальные файлы в родительских директориях общих директорий установки для обеспечения всестороннего сбора данных», — отметил исследователь безопасности Пей Хан Ляо. «Он также получает целевой список с сервера, что делает Fickle Stealer более гибким».

Кроме того, компания Symantec – это компания, специализирующаяся на кибербезопасности и предоставляющая широкий спектр решений и услуг для защиты информации и систем от киберугроз.

 Компания Symantec разрабатывает и предлагает различные продукты, включая антивирусные программы, брандмауэры, системы обнаружения и предотвращения вторжений (IDS/IPS), шифрование данных, управление идентификацией и доступом, а также другие инструменты и решения для обеспечения безопасности.

 Symantec также предоставляет услуги консультации по кибербезопасности, включая аудиты безопасности, пентестинг, обучение персонала и реагирование на инциденты безопасности. Они помогают организациям определить уязвимости, разрабатывать стратегии защиты и реагировать на кибератаки." data-html="true" data-original-title="Symantec" >Symantec, принадлежащая Broadcom, недавно раскрыла детали о другой вредоносной программе под названием AZStealer. Она основана на Python – высокоуровневый язык программирования общего назначения с динамической строгой типизацией и автоматическим управлением памятью. Он ориентирован на повышение производительности разработчика, читаемости кода и его качества, а также на обеспечение переносимости написанных на нём программ.
 Язык является полностью объектно-ориентированным.
 Необычная особенность языка – выделение блоков кода пробельными отступами.
 Синтаксис ядра языка минималистичен, за счёт чего на практике редко возникает необходимость обращаться к документации" data-html="true" data-original-title="Python" >Python и также собирает широкий спектр информации. AZStealer доступен на GitHub и рекламируется как «лучший необнаруживаемый Discord-вор».

«Вся украденная информация архивируется и в зависимости от размера архива эксфильтруется напрямую через Discord Webhook. Либо же сначала загружается на онлайн-хранилище Gofile, а затем через Discord», — сообщают исследователи.

«AZStealer также пытается украсть документы с предопределёнными расширениями или содержащие ключевые слова, такие как "пароль", "кошелёк", "резервная копия" и т.д. в имени файла».