viettel
security

Leaking Critical Personal Information Due to Various Types of Information-stealing Malware

Redline Stealer

TABLE OF **CONTENTS**

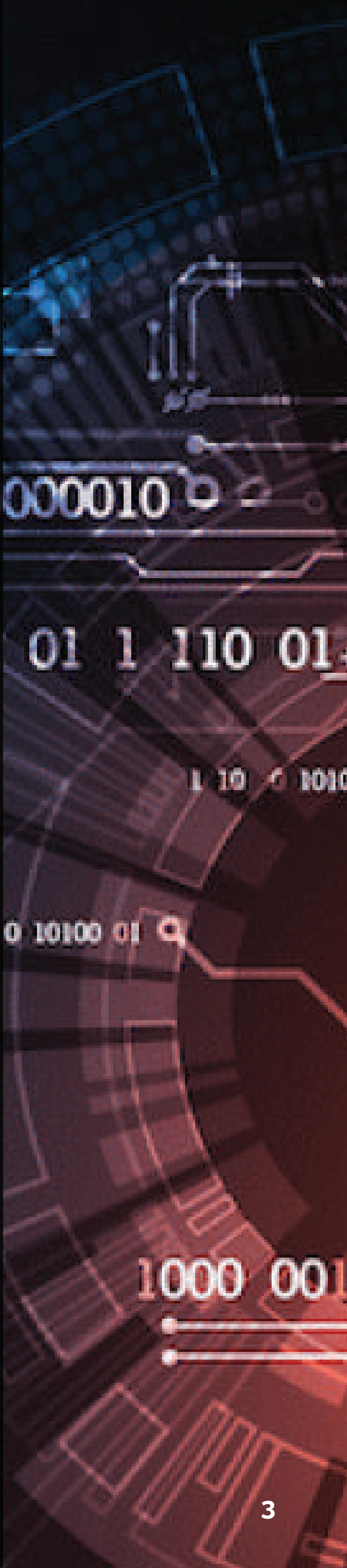
SECTION 01

Introduction

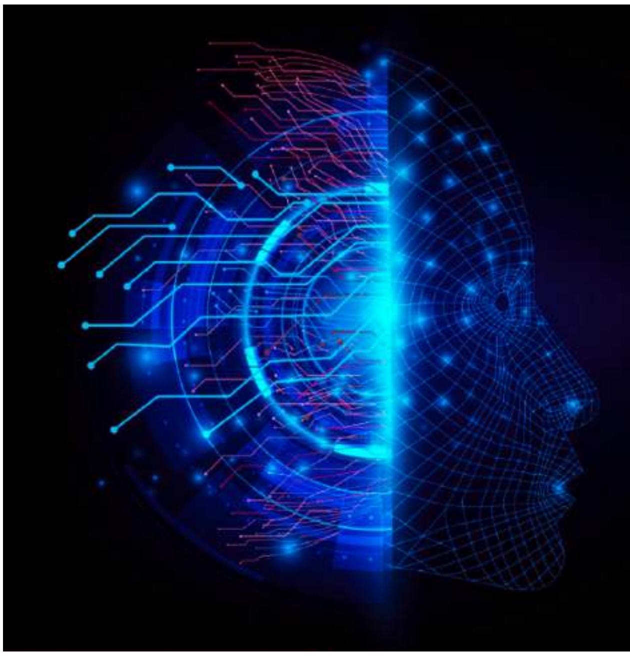
During the cyber monitoring process, **Viettel Threat Intelligence** has detected and collected a large amount of information-stealing malware's log data.

More seriously, the information of Vietnamese users who logged into the critical infrastructure, especially including national banking, government and media systems, has continuously appeared in this data set and occupied a large number. Therefore, Viettel Threat Intelligence experts have issued alerts for the critical threat of leaking personal information, raised awareness for users to minimize the impact and made recommendations on the prevention of these dangerous malwares.

In this article, Viettel Threat Intelligence will monitor the cyber behavior of Redline Stealer and its affects on users and customers, and then make recommendations from experts to handle these malwares.
The article is only for the purpose of researching and sharing knowledge about cybersecurity. Viettel Threat Intelligence is not responsible for any misuse of this knowledge for attack or demage purposes.



Executive Summary



VIETTEL THREAT INTELLIGENCE has detected many campaigns spreading the Redline Stealer malwares. This is considered a critical threat due to the large number of identified victims and the great impact of leaking sensitive data sets on not only national but also international critical infrastructure.

Adversary

Redline Stealer, an information-stealing malware, is a Malware-as-a-Service (MaaS) which provides Adversary Operator and Adversary Customer, diffusely distributes and makes individual profits regardless of the suppliers.

Victims

The affected victims could be anyone who downloads an unknown software with the Redline malware installed. They will be infected if they are accidentally targeted by a certain campaign or simply execute some crack files floating around in Cyberspace. Here are some of the victims targeted in the Redline malware campaigns:

- Ordinary users who accidentally download cracked software containing Redline malware, including a large number of Vietnamese users.
- 3D Digital Artists* who own coins and NFT tokens.
- Users who believe in the US's Folding@home campaign against COVID-19 (a distributed computing project to build Protein structure models for COVID-19 preven,.8n tion research models) and are encouraged to download the Simulator app to accompany the project. At that time, the attacker will take advantage of this app to trick users into downloading a fake Simulator one containing Redline malware.

**Digital Artists: Artistic content creators using digital technologies in the form of NFT.*

Capabilities

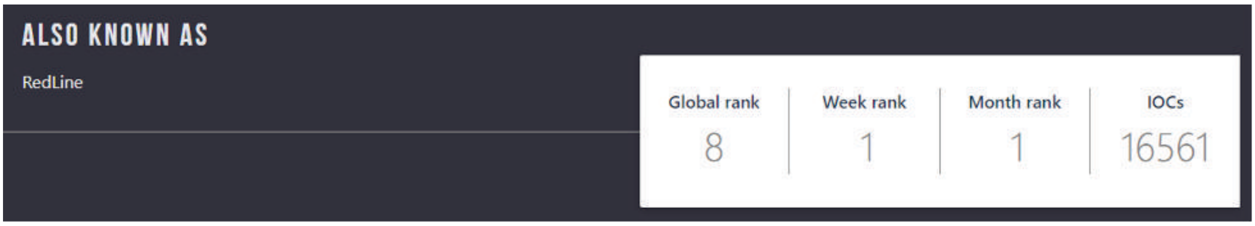
This Redline malware can collect information from the users' system, browser, e-wallet and other valuable information with various infection methods and the ability to remotely execute code to download many malicious tools.

Infrastructure

- HTTP-SOAP connection to extract data and remotely download & execute code.
- Different C&C for each customer due to the characteristics of MaaS malware.
- Infrastructure that can be mapped from download links and C&C (Details in IOCs section)

Redline Stealer

This information-stealing malware is extremely popular recently with the number of malicious samples uploaded always on the top of the Any Run chart.



ALSO KNOWN AS

RedLine

Global rank	Week rank	Month rank	IOCs
8	1	1	16561

Figure 1.1. Redline Stealer is strongly spreading on Cyberspace.

The number of malicious files uploaded to Public Sandbox services every day continues to grow and remains monthly, with a total of more than 16,561 IOCs at Any.Run from launch to date.

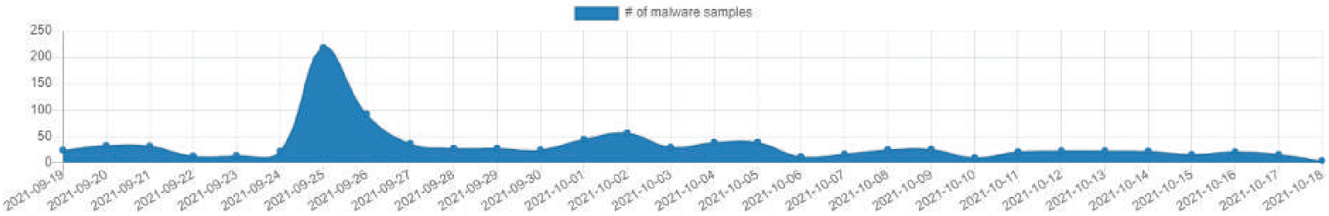
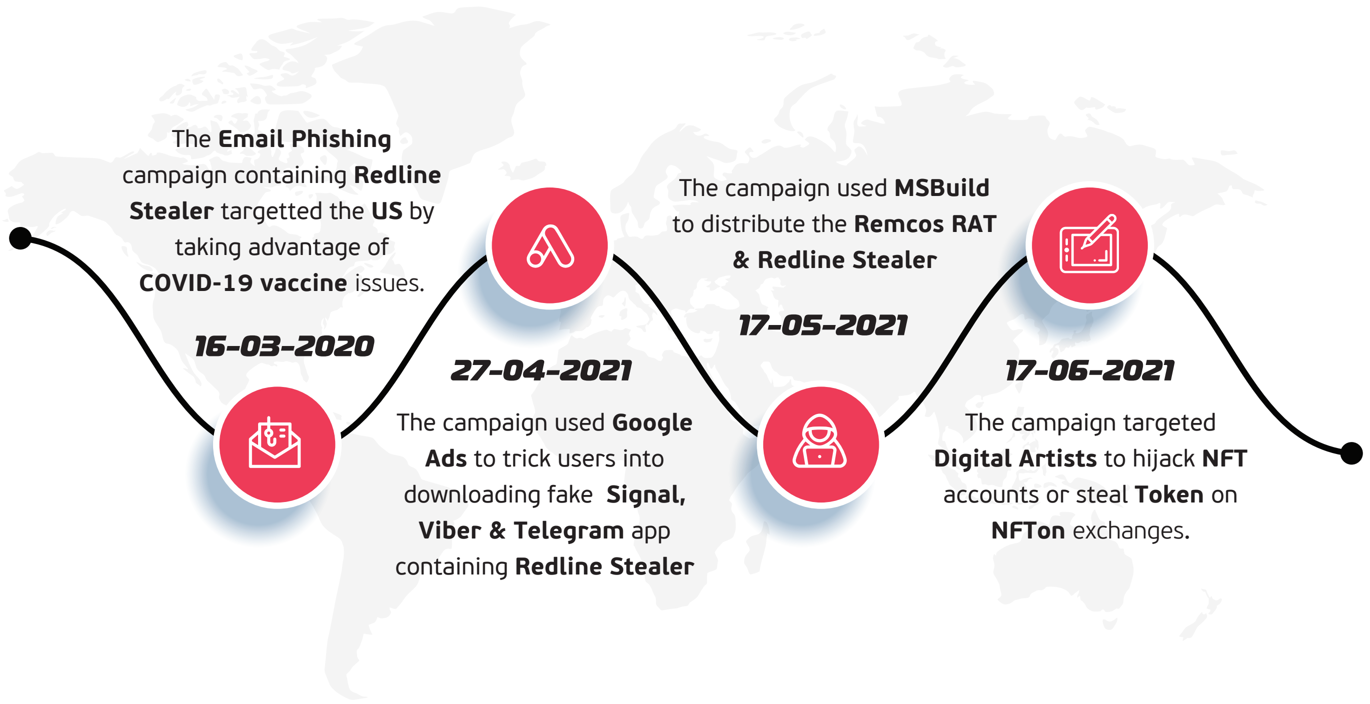


Figure 1.2. Number of malicious samples uploaded to the Public Sandbox.



16-03-2020

The **Email Phishing** campaign containing **Redline Stealer** targetted the **US** by taking advantage of **COVID-19 vaccine** issues.

27-04-2021

The campaign used **Google Ads** to trick users into downloading fake **Signal, Viber & Telegram** app containing **Redline Stealer**

17-05-2021

The campaign used **MSBuild** to distribute the **Remcos RAT & Redline Stealer**

17-06-2021

The campaign targeted **Digital Artists** to hijack **NFT** accounts or steal **Token** on **NFTon** exchanges.

Figure 1.3. Timeline of major attack campaigns using Redline Stealer.

Compared to the Oski malware described in part 1 by Viettel Threat Intelligence, Redline has a more complex structure and operation by expanding some key functions and directly targeting sensitive information, including:

- System information
- Browser credentials
- Crypto wallet information
- Screenshot
- Files
- [New] FTP information
- [New] VPN credentials
- [New] Information from Instant Messengers software such as Discord, Telegram
- [New] Steam player information

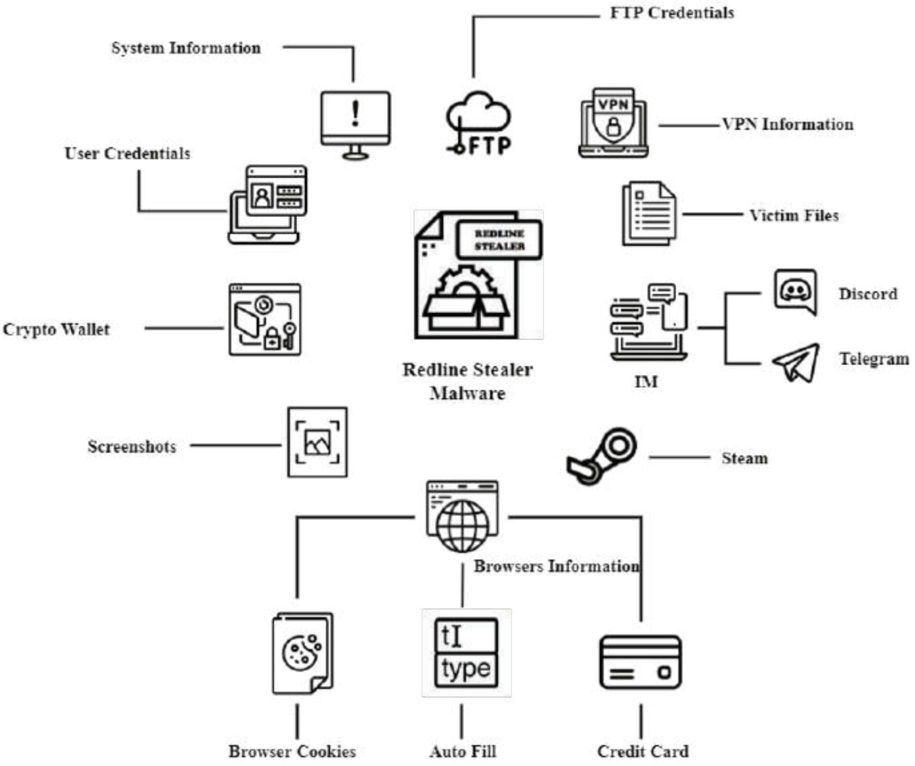
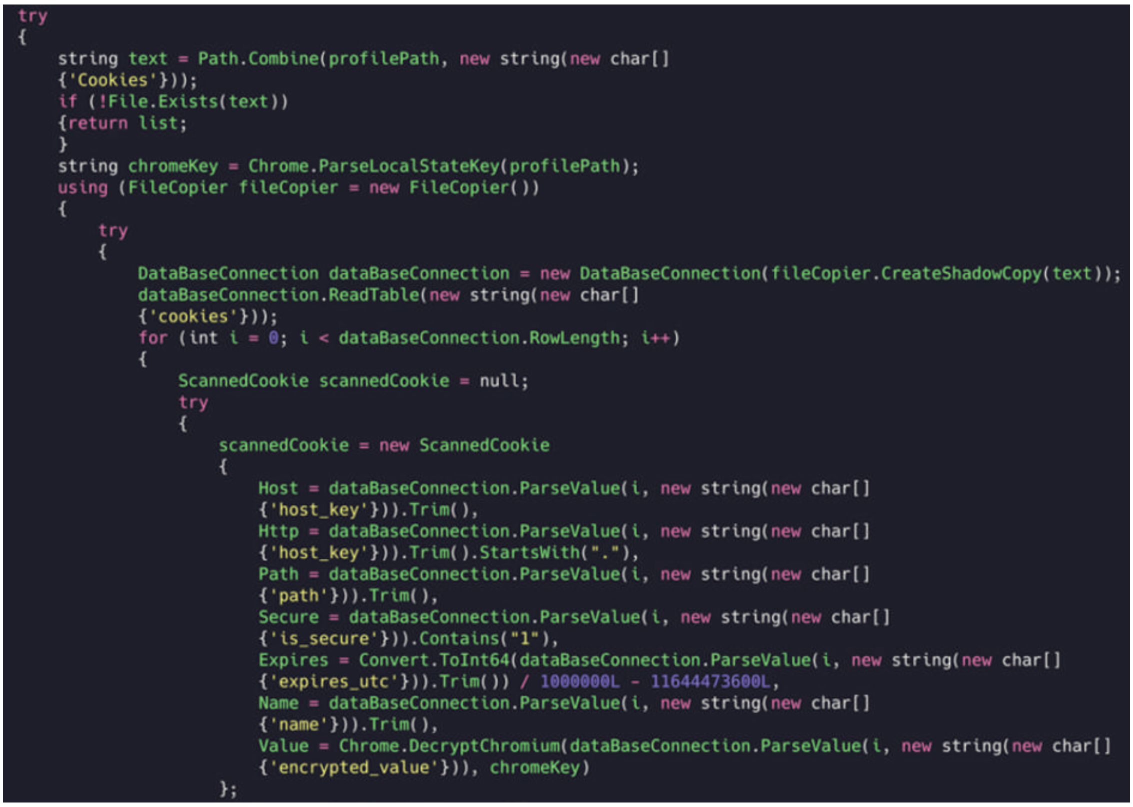


Figure 1.4. Details of the targets' data collected by Redline malware.



```
try
{
    string text = Path.Combine(profilePath, new string(new char[]
    {'Cookies'}));
    if (!File.Exists(text))
    {return list;
    }
    string chromeKey = Chrome.ParseLocalStateKey(profilePath);
    using (FileCopier fileCopier = new FileCopier())
    {
        try
        {
            DataBaseConnection dataBaseConnection = new DataBaseConnection(fileCopier.CreateShadowCopy(text));
            dataBaseConnection.ReadTable(new string(new char[]
            {'cookies'}));
            for (int i = 0; i < dataBaseConnection.RowLength; i++)
            {
                ScannedCookie scannedCookie = null;
                try
                {
                    scannedCookie = new ScannedCookie
                    {
                        Host = dataBaseConnection.ParseValue(i, new string(new char[]
                        {'host_key'})).Trim(),
                        Http = dataBaseConnection.ParseValue(i, new string(new char[]
                        {'host_key'})).Trim().StartsWith("."),
                        Path = dataBaseConnection.ParseValue(i, new string(new char[]
                        {'path'})).Trim(),
                        Secure = dataBaseConnection.ParseValue(i, new string(new char[]
                        {'is_secure'})).Contains("1"),
                        Expires = Convert.ToInt64(dataBaseConnection.ParseValue(i, new string(new char[]
                        {'expires_utc'})).Trim()) / 1000000L - 11644473600L,
                        Name = dataBaseConnection.ParseValue(i, new string(new char[]
                        {'name'})).Trim(),
                        Value = Chrome.DecryptChromium(dataBaseConnection.ParseValue(i, new string(new char[]
                        {'encrypted_value'})), chromeKey)
                    };
```

Figure 1.5. The feature of stealing information stored in the browser.

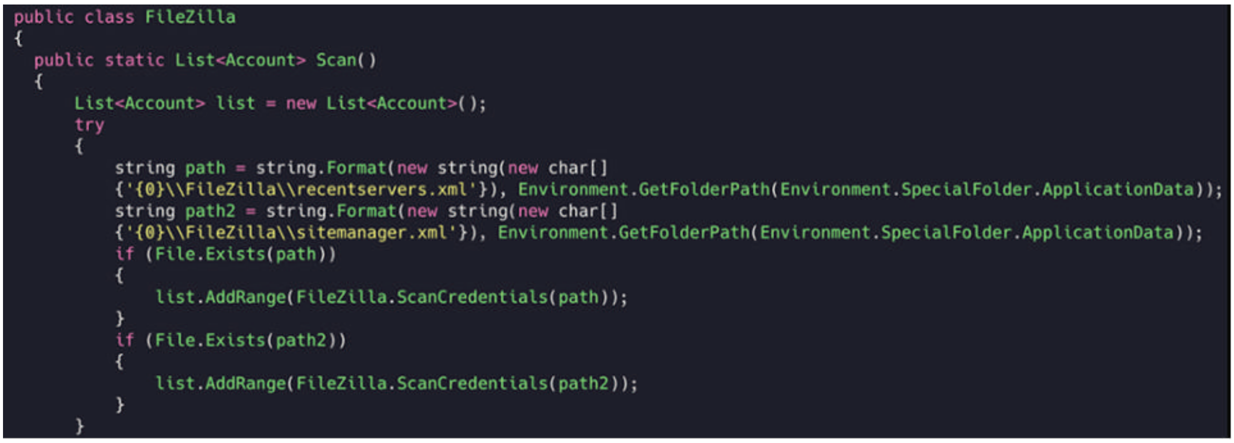
According to Viettel Threat Intelligence analysis, the first 5 features of Redline are also created with the same function as the Oski malware. Besides, there are some new features as follows.

[New] Stealing FTP Credential

The Redline malware targets two popular open source FTP applications, FileZilla and WinSCP. After determining these two applications have been installed on the devices, the malware will get data including:

- ***With FileZilla***
  - Connections
  - Login/authentication information
  - Recently used information such as host, port, account, password

- ***With WinSCP***
  - Password
  - Connections

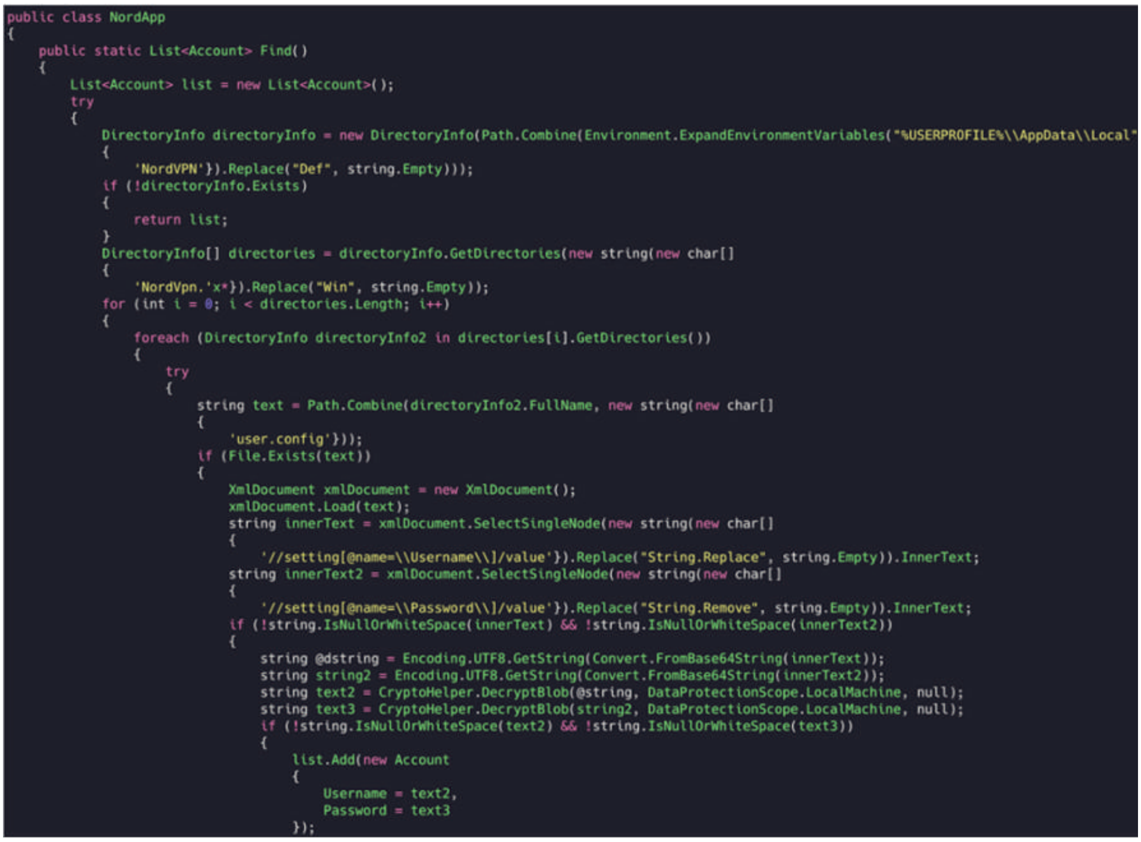


```
public class FileZilla
{
  public static List<Account> Scan()
  {
      List<Account> list = new List<Account>();
      try
      {
          string path = string.Format(new string(new char[]
          {'{0}\\FileZilla\\recentservers.xml'}), Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
          string path2 = string.Format(new string(new char[]
          {'{0}\\FileZilla\\sitemanager.xml'}), Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
          if (File.Exists(path))
          {
              list.AddRange(FileZilla.ScanCredentials(path));
          }
          if (File.Exists(path2))
          {
              list.AddRange(FileZilla.ScanCredentials(path2));
          }
      }
```

Figure 1.6. Stealing FileZilla software credentials.

[New] Stealing VPN Credential

Given the popularity of VPN apps these days, the malware targets a number of VPN apps like NordVPN, ProtonVPN, and OpenVPN.
It will read the config files of each application and output the account and password of each profile.



```
public class NordApp
{
    public static List<Account> Find()
    {
        List<Account> list = new List<Account>();
        try
        {
            DirectoryInfo directoryInfo = new DirectoryInfo(Path.Combine(Environment.ExpandEnvironmentVariables("%USERPROFILE%\\AppData\\Local"
            {
                'NordVPN'}).Replace("Def", string.Empty)));
            if (!directoryInfo.Exists)
            {
                return list;
            }
            DirectoryInfo[] directories = directoryInfo.GetDirectories(new string(new char[]
            {
                'NordVpn.'x*}).Replace("Win", string.Empty));
            for (int i = 0; i < directories.Length; i++)
            {
                foreach (DirectoryInfo directoryInfo2 in directories[i].GetDirectories())
                {
                    try
                    {
                        string text = Path.Combine(directoryInfo2.FullName, new string(new char[]
                        {
                            'user.config'}));
                        if (File.Exists(text))
                        {
                            XmlDocument xmlDocument = new XmlDocument();
                            xmlDocument.Load(text);
                            string innerText = xmlDocument.SelectSingleNode(new string(new char[]
                            {
                                '//setting[@name=\\Username\\]/value'}).Replace("String.Replace", string.Empty)).InnerText;
                            string innerText2 = xmlDocument.SelectSingleNode(new string(new char[]
                            {
                                '//setting[@name=\\Password\\]/value'}).Replace("String.Remove", string.Empty)).InnerText;
                            if (!string.IsNullOrWhiteSpace(innerText) && !string.IsNullOrWhiteSpace(innerText2))
                            {
                                string @dstring = Encoding.UTF8.GetString(Convert.FromBase64String(innerText));
                                string string2 = Encoding.UTF8.GetString(Convert.FromBase64String(innerText2));
                                string text2 = CryptoHelper.DecryptBlob(@string, DataProtectionScope.LocalMachine, null);
                                string text3 = CryptoHelper.DecryptBlob(string2, DataProtectionScope.LocalMachine, null);
                                if (!string.IsNullOrWhiteSpace(text2) && !string.IsNullOrWhiteSpace(text3))
                                {
                                    list.Add(new Account
                                    {
                                        Username = text2,
                                        Password = text3
                                    });
```

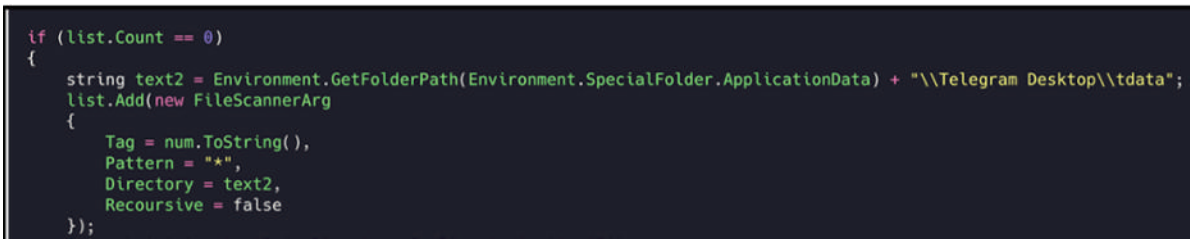
Figure 1.7. Stealing information from VPN software.

[NEW] Stealing Login Credentials in Instant Messenger apps (Telegram, Discord)

Instant Messenger (IM) is the services used for text-based communication. The malware targets two highly popular IM applications, Discord and Telegram.

- ***With Telegram***

  - Locate the tdata folder at %AppData\Roaming\Telegram Desktop\tdata% containing data about cache, sessions, images and conversations.

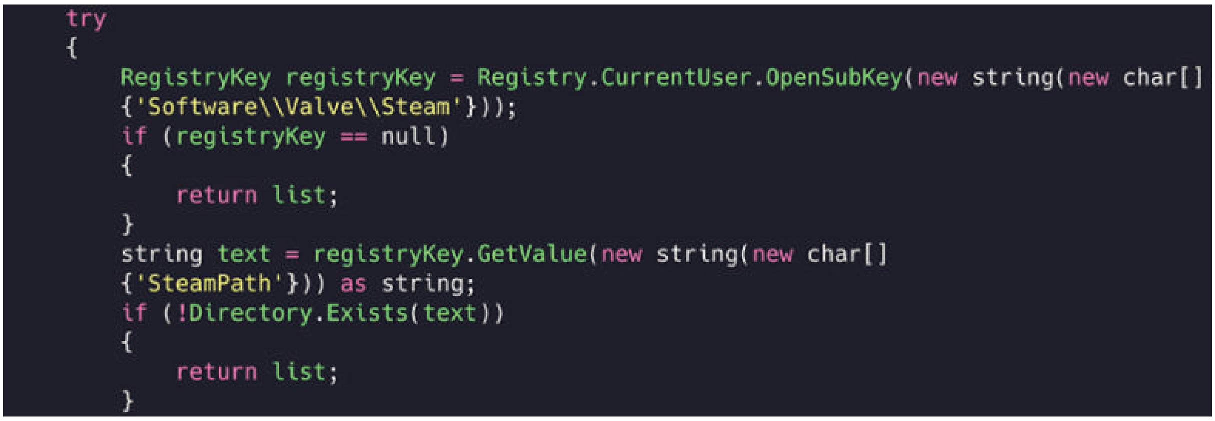


```
if (list.Count == 0)
{
    string text2 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Telegram Desktop\\tdata";
    list.Add(new FileScannerArg
    {
        Tag = num.ToString(),
        Pattern = "*",
        Directory = text2,
        Recoursive = false
    });
```

Figure 1.8. Stealing data of Telegram users.

[NEW] Stealing Steam Login Credentials

Steam is a fairly popular online gaming platform today with more than 100 million users. The malware will steal player profiles at Steam Sentry File (.SSFN) containing account password and associated credit card information to perform transactions on Steam.



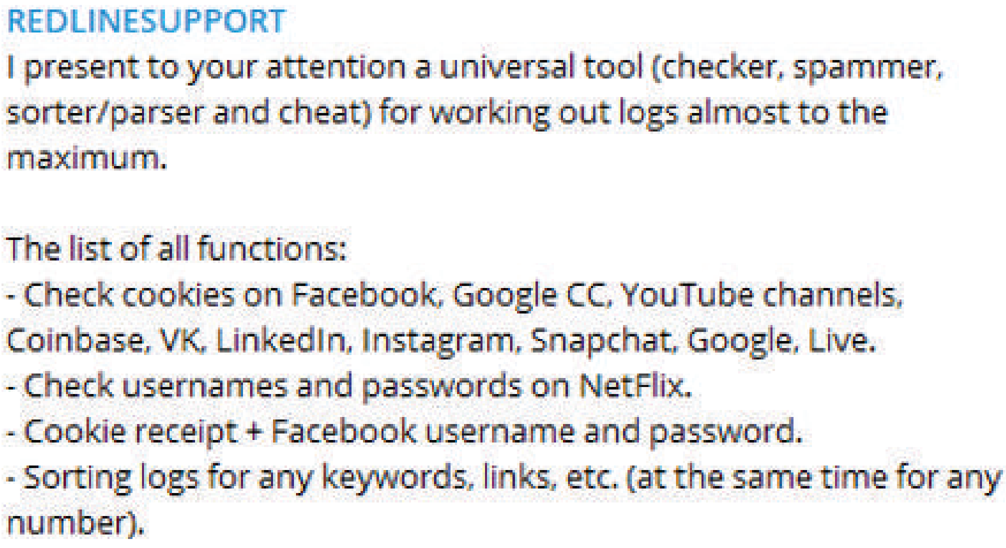
```
    try
    {
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(new string(new char[]
        {'Software\\Valve\\Steam'}));
        if (registryKey == null)
        {
            return list;
        }
        string text = registryKey.GetValue(new string(new char[]
        {'SteamPath'})) as string;
        if (!Directory.Exists(text))
        {
            return list;
        }
```

Figure 1.9. Stealing Steam credentials.

In addition to the main features to steal information, Redline also provides remote access features to serve multiple purposes such as:

- Download and execute arbitrary files
- Open arbitrary links
- Download and execute new Redline updates
- Execute commands via CMD

In addition, the attacker can buy some additional plugins called Universal Tool to serve multiple purposes (checker, spammer, sorter/parser, and cheat) including checking
whether the collected data such as cookies, account passwords on some platforms are valid or not.



REDLINESUPPORT

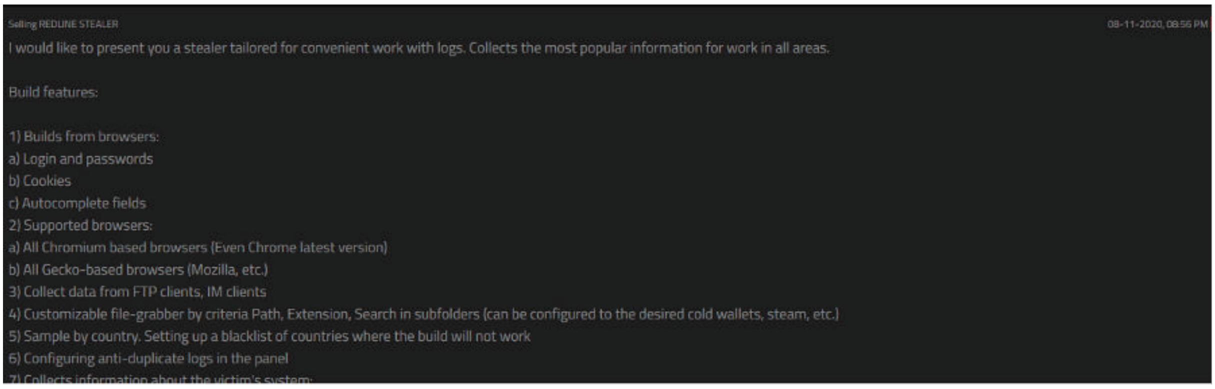
I present to your attention a universal tool (checker, spammer, sorter/parser and cheat) for working out logs almost to the maximum.

The list of all functions:
- Check cookies on Facebook, Google CC, YouTube channels, Coinbase, VK, LinkedIn, Instagram, Snapchat, Google, Live.
- Check usernames and passwords on NetFlix.
- Cookie receipt + Facebook username and password.
- Sorting logs for any keywords, links, etc. (at the same time for any number).

Figure 1.2.1. The tool used to classify collected data.

Tracking Redline's Behaviour on Cyber Space

This information-stealing malware is extremely popular recently with the number of malicious samples uploaded always on the top of the Any Run chart.



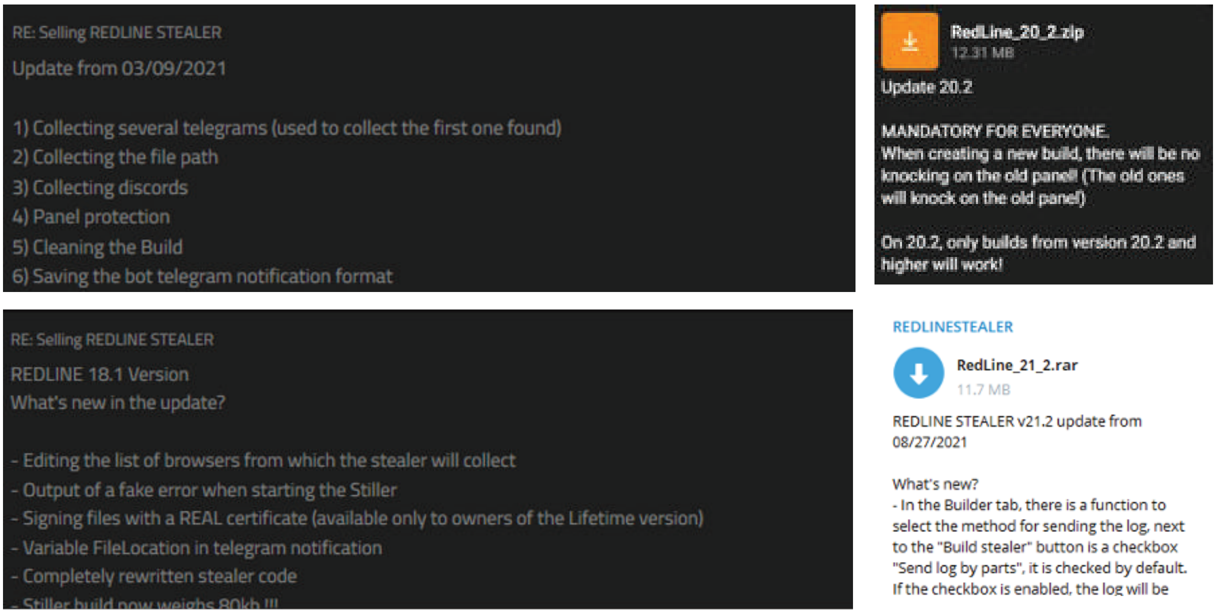
Selling REDLINE STEALER 08-11-2020, 08:56 PM

I would like to present you a stealer tailored for convenient work with logs. Collects the most popular information for work in all areas.

Build features:

1) Builds from browsers:
a) Login and passwords
b) Cookies
c) Autocomplete fields
2) Supported browsers:
a) All Chromium based browsers (Even Chrome latest version)
b) All Gecko-based browsers (Mozilla, etc.)
3) Collect data from FTP clients, IM clients
4) Customizable file-grabber by criteria Path, Extension, Search in subfolders (can be configured to the desired cold wallets, steam, etc.)
5) Sample by country. Setting up a blacklist of countries where the build will not work
6) Configuring anti-duplicate logs in the panel
7) Collects information about the victim's system:

Figure 2.1. About information stealing features



RE: Selling REDLINE STEALER

Update from 03/09/2021

1) Collecting several telegrams (used to collect the first one found)
2) Collecting the file path
3) Collecting discords
4) Panel protection
5) Cleaning the Build
6) Saving the bot telegram notification format

RedLine_20_2.zip
12.31 MB

Update 20.2

MANDATORY FOR EVERYONE.
When creating a new build, there will be no knocking on the old panel! (The old ones will knock on the old panel)

On 20.2, only builds from version 20.2 and higher will work!

RE: Selling REDLINE STEALER

REDLINE 18.1 Version
What's new in the update?

- Editing the list of browsers from which the stealer will collect
- Output of a fake error when starting the Stiller
- Signing files with a REAL certificate (available only to owners of the Lifetime version)
- Variable FileLocation in telegram notification
- Completely rewritten stealer code
- Stiller build now weighs 80kb !!!

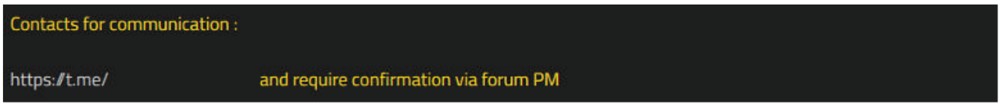
REDLINESTEALER

RedLine_21_2.rar
11.7 MB

REDLINE STEALER v21.2 update from 08/27/2021

What's new?
- In the Builder tab, there is a function to select the method for sending the log, next to the "Build stealer" button is a checkbox "Send log by parts", it is checked by default. If the checkbox is enabled, the log will be

Figure 2.2. Updates are continuously given on the group's channel.



Contacts for communication :

https://t.me/ and require confirmation via forum PM

Figure 2.3. Main trading channel on Telegram.

Viettel Threat Intelligence monitored closed groups that buy, sell, exchange and distribute Redline malware. These groups are divided into different purposes:

- The [Support] channel only for transaction of malware.
- The [Members] channel for providing installation instructions, user guide and updates.

Malware Transactions

Specifically, the installation that was publicly available for sale on Telegram with the latest version 22.4.5 (December 13, 2021) had the following options:

- Regular version: **$100/week** or **$150/month**
- Premium/Lifetime version: **$800**, unlimited expansion with some features. Especially with the **PRO version**, users can also use the signing real certificate feature.

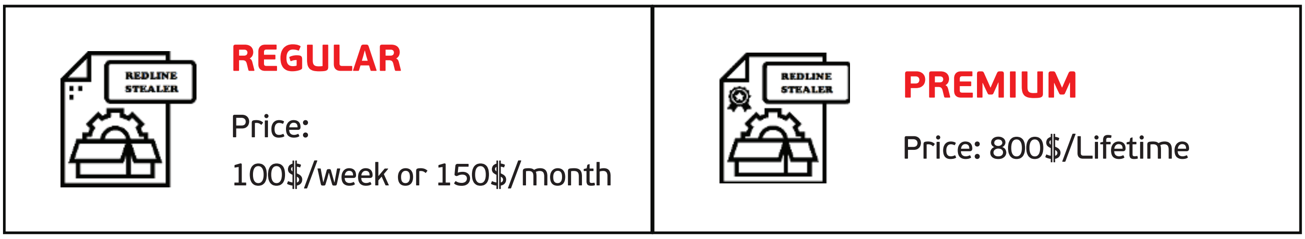
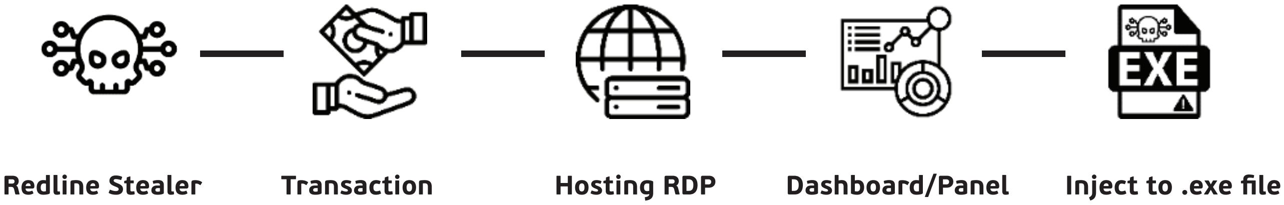


Figure 2.4. Redline Stealer trading options from the official channel.

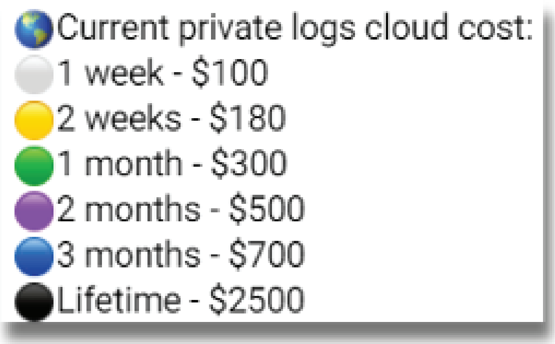
Malware Deployments

After successfully trading the Redline malware with the Threat Actor (TA), the attacker built a Panel on an RDP hosting and distributed the malware via .exe files. Information was collected and sent to the Panel, receiving notifications through arbitrary channels.



Channel of buying, selling and exchanging LOGs

User LOGS data stolen by the malware will be here for sale. Transaction fees typically ranged from $150-200$ to $2500 with a commitment of 1-3GB of Fresh Logs* data per week.



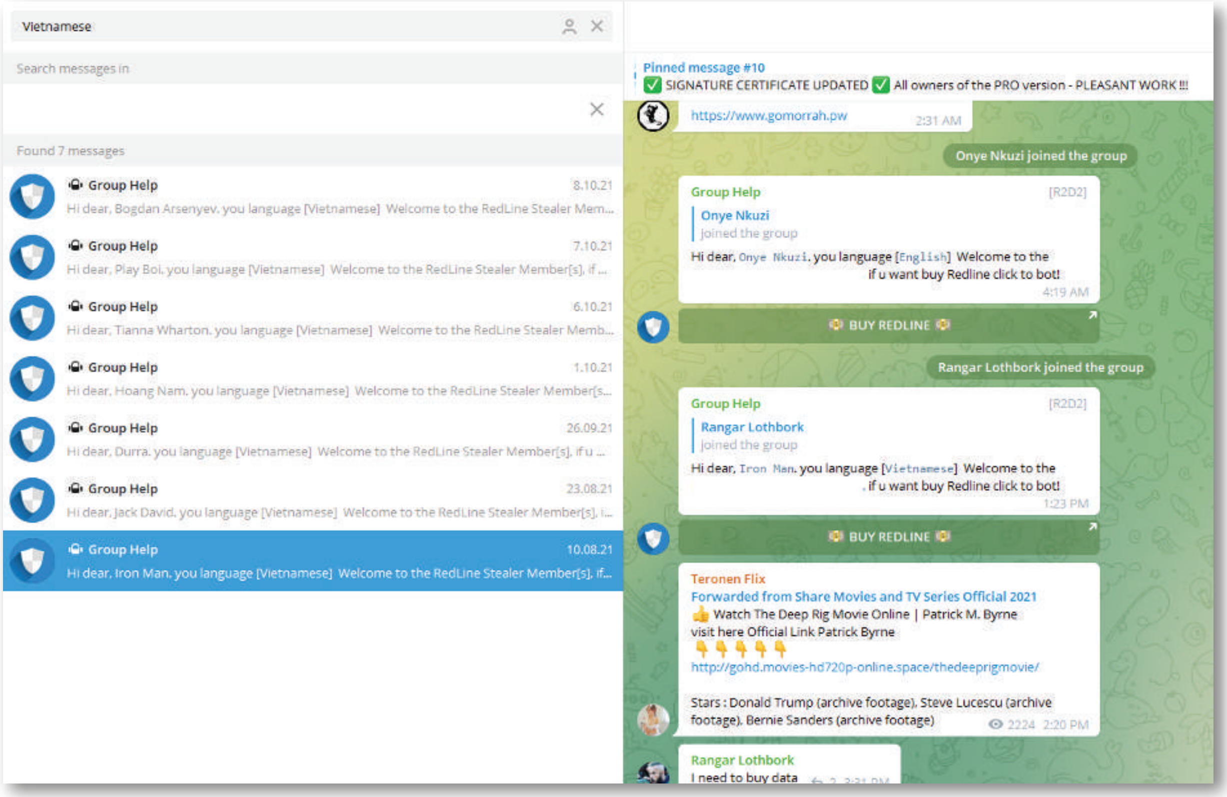
🌎Current private logs cloud cost:
⚪1 week - $100
🟡2 weeks - $180
🟢1 month - $300
🟣2 months - $500
🔵3 months - $700
⚫Lifetime - $2500

Figure 2.5. Redline Stealer trading options from the official channel.

**Fresh Logs: Clean logs, newly collected within 1 week, includes accounts never been used after being stolen and unexpired cookies.*

Vietnamese Users in the Malware Trading Market

The number of Vietnamese users participating in the malware trading market has been gradually growing. Some users are said to focuse on stolen Facebook accounts for some personal purpose.



Vietnamese

Search messages in

Found 7 messages

Group Help 8.10.21
Hi dear, Bogdan Arsenyev. you language [Vietnamese] Welcome to the RedLine Stealer Mem...

Group Help 7.10.21
Hi dear, Play Boi. you language [Vietnamese] Welcome to the RedLine Stealer Member[s], if ...

Group Help 6.10.21
Hi dear, Tianna Wharton. you language [Vietnamese] Welcome to the RedLine Stealer Memb...

Group Help 1.10.21
Hi dear, Hoang Nam. you language [Vietnamese] Welcome to the RedLine Stealer Member[s...

Group Help 26.09.21
Hi dear, Durra. you language [Vietnamese] Welcome to the RedLine Stealer Member[s], if u ...

Group Help 23.08.21
Hi dear, Jack David. you language [Vietnamese] Welcome to the RedLine Stealer Member[s], i...

Group Help 10.08.21
Hi dear, Iron Man. you language [Vietnamese] Welcome to the RedLine Stealer Member[s], if...

Pinned message #10
✅ SIGNATURE CERTIFICATE UPDATED ✅ All owners of the PRO version - PLEASANT WORK !!!

https://www.gomorrah.pw 2:31 AM

Onye Nkuzi joined the group

Group Help [R2D2]
Onye Nkuzi
joined the group
Hi dear, Onye Nkuzi. you language [English] Welcome to the
if u want buy Redline click to bot!
4:19 AM

Rangar Lothbork joined the group

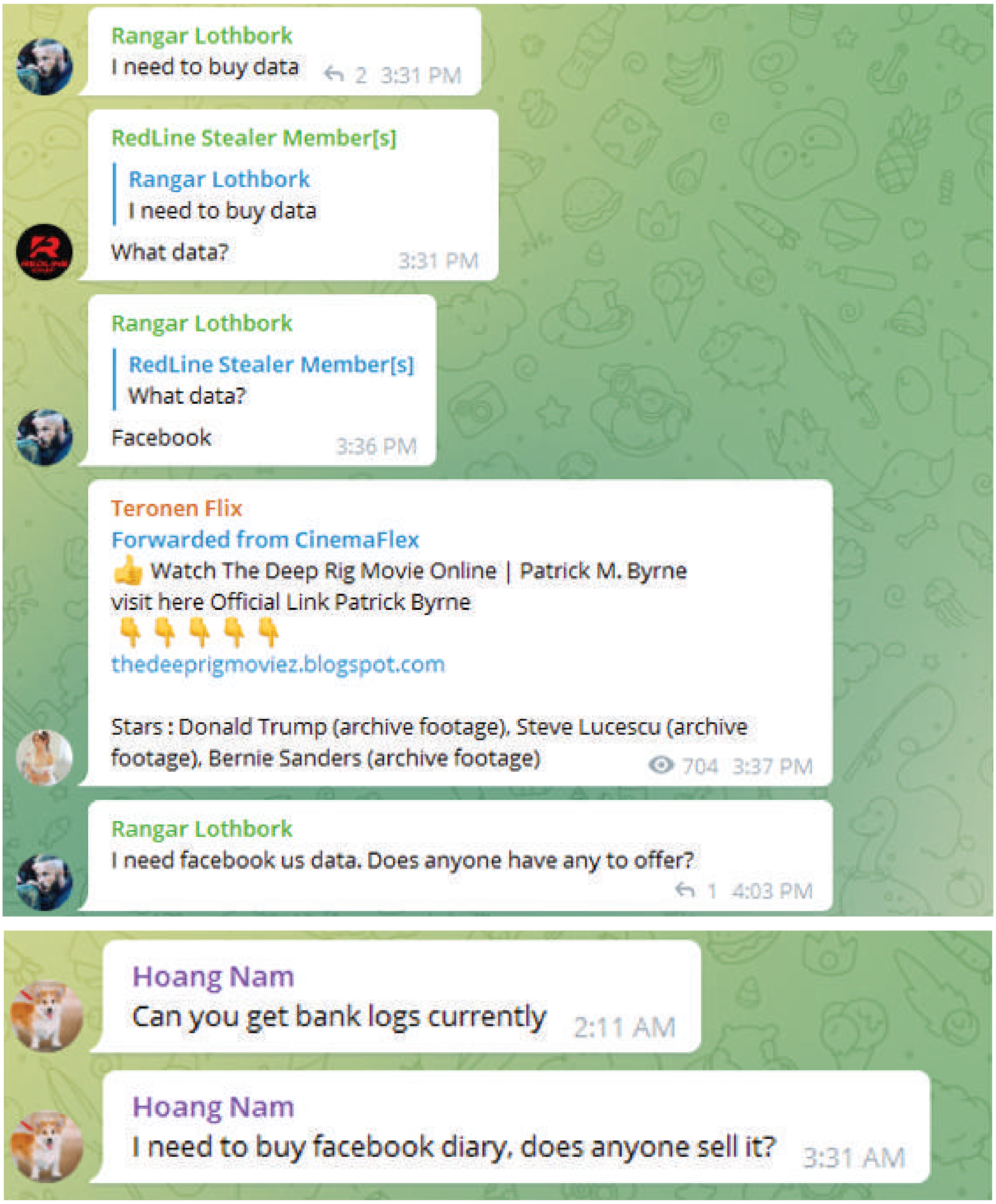
Group Help [R2D2]
Rangar Lothbork
joined the group
Hi dear, Iron Man. you language [Vietnamese] Welcome to the
. if u want buy Redline click to bot!
1:23 PM

Teronen Flix
Forwarded from Share Movies and TV Series Official 2021
👍 Watch The Deep Rig Movie Online | Patrick M. Byrne
visit here Official Link Patrick Byrne
👇👇👇👇👇
http://gohd.movies-hd720p-online.space/thedeeprigmovie/

Stars : Donald Trump (archive footage), Steve Lucescu (archive footage), Bernie Sanders (archive footage)
2224 2:20 PM

Rangar Lothbork
I need to buy data

Figure 2.6. Filter out a small number of users with Vietnamese language.
(Source: VIETTEL THREAT INTELLIGENCE)



Rangar Lothbork
I need to buy data ↩ 2 3:31 PM

RedLine Stealer Member[s]
> Rangar Lothbork
> I need to buy data

What data? 3:31 PM

Rangar Lothbork
> RedLine Stealer Member[s]
> What data?

Facebook 3:36 PM

Teronen Flix
Forwarded from CinemaFlex
👍 Watch The Deep Rig Movie Online | Patrick M. Byrne
visit here Official Link Patrick Byrne
👇👇👇👇👇
thedeeprigmoviez.blogspot.com

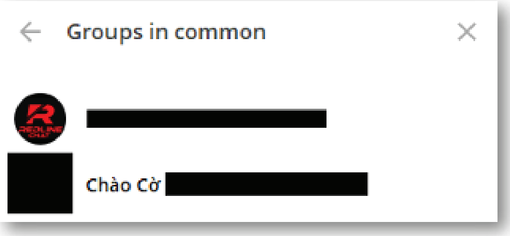
Stars : Donald Trump (archive footage), Steve Lucescu (archive footage), Bernie Sanders (archive footage) 704 3:37 PM

Rangar Lothbork
I need facebook us data. Does anyone have any to offer? ↩ 1 4:03 PM

Hoang Nam
Can you get bank logs currently 2:11 AM

Hoang Nam
I need to buy facebook diary, does anyone sell it? 3:31 AM

Figure 2.7. Some users are said to be interested in Facebook-related data. (Source: VIETTEL THREAT INTELLIGENCE)



Groups in common

[redacted]

Chào Cờ [redacted]

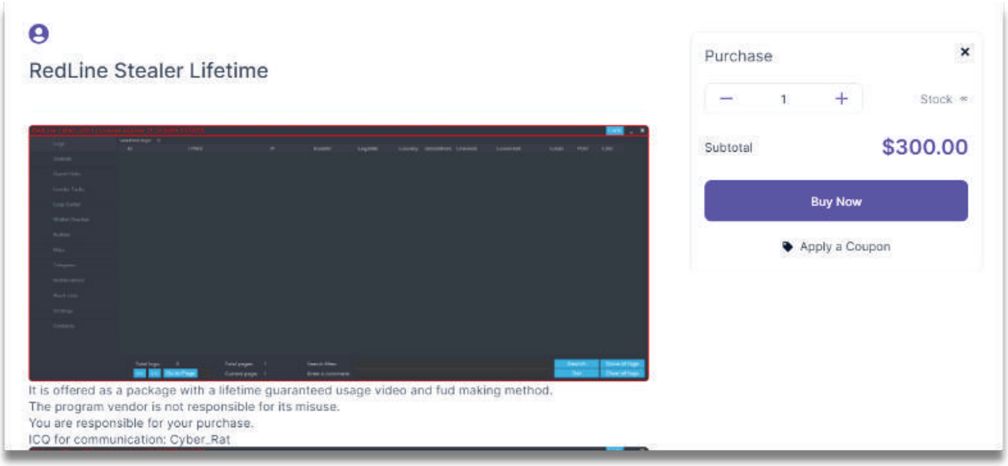
Figure 2.8. Identify some Vietnamese users by participating in some common groups. (Source: VIETTEL THREAT INTELLIGENCE)

SECTION

02

Analysis Working Flows Through Some Redline’s Cracked Versions

In addition to being sold with the official version, the Panel Crack of the malware is also distributed strongly on some Underground forums. These versions are widely shared, with very detailed instructions from setting up the host, logging into the Panel to building your own malware at will, leading to dramatically increase the threat of Redline's spread and distribution.



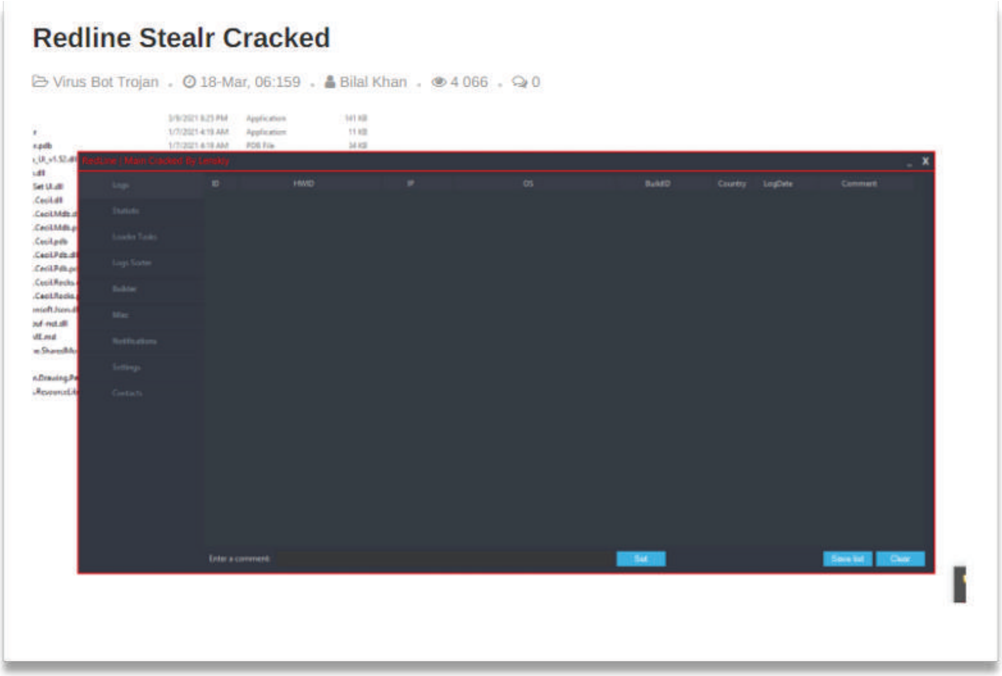
RedLine Stealer Lifetime

It is offered as a package with a lifetime guaranteed usage video and fud making method.
The program vendor is not responsible for its misuse.
You are responsible for your purchase.
ICQ for communication: Cyber_Rat

Purchase

Stock ∞

Subtotal $300.00



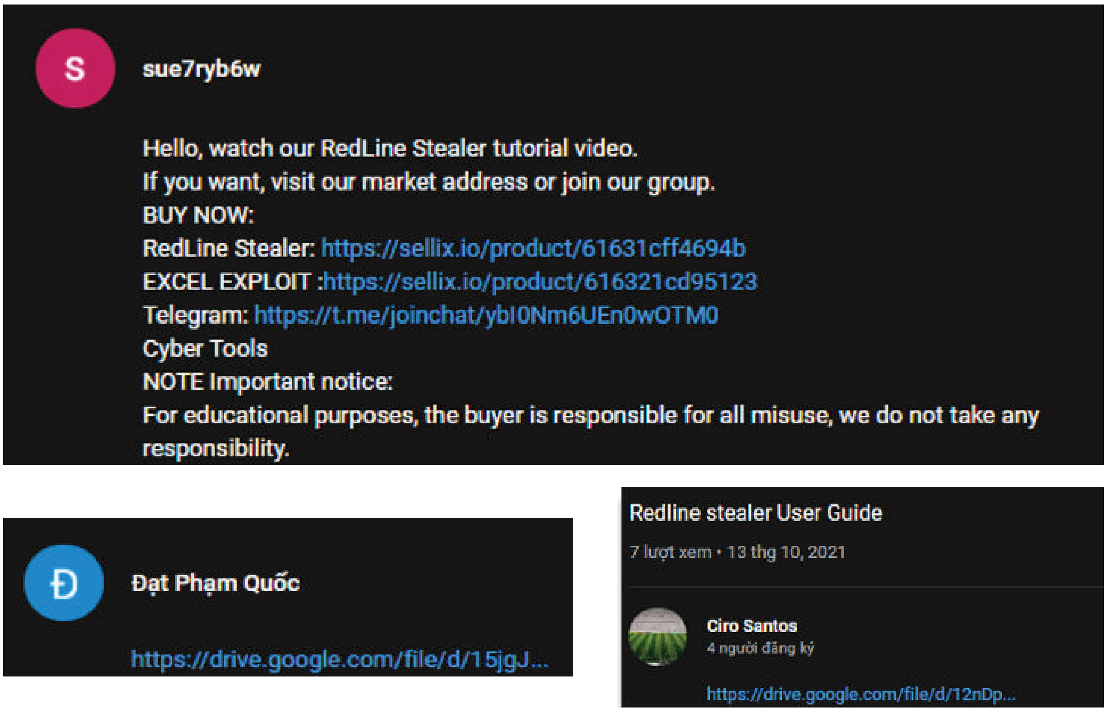
Redline Stealr Cracked

Virus Bot Trojan . 18-Mar, 06:159 . Bilal Khan . 4 066 . 0

RedLine | Main Cracked By Lensky

ID	HWID	IP	OS	BuildID	Country	LogDate	Comment

Figure 3.1. Redline Crack software is shared publicly on Cyberspace. (Source: VIETTEL THREAT INTELLIGENCE)



sue7ryb6w

Hello, watch our RedLine Stealer tutorial video.
If you want, visit our market address or join our group.
BUY NOW:
RedLine Stealer: https://sellix.io/product/61631cff4694b
EXCEL EXPLOIT :https://sellix.io/product/616321cd95123
Telegram: https://t.me/joinchat/ybI0Nm6UEn0wOTM0
Cyber Tools
NOTE Important notice:
For educational purposes, the buyer is responsible for all misuse, we do not take any responsibility.

Đạt Phạm Quốc

https://drive.google.com/file/d/15jgJ...

Redline stealer User Guide
7 lượt xem • 13 thg 10, 2021

Ciro Santos
4 người đăng ký

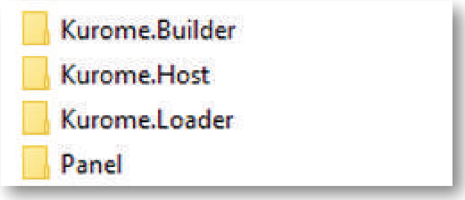
https://drive.google.com/file/d/12nDp...

Figure 3.2. Instructions for using this software are publicly posted on the Youtube platform (Source: VIETTEL THREAT INTELLIGENCE)

Analysis of the Main Activity Flow

After making a transaction or downloading the Crack version, users will receive a software with 3 main components:

- Original dashboard of the malware (Must pay to use)
- (*) The Control Panel of the malware that has been Cracked
- (*) Builder to create executable files (.exe) for distribution



Kurome.Builder
Kurome.Host
Kurome.Loader
Panel

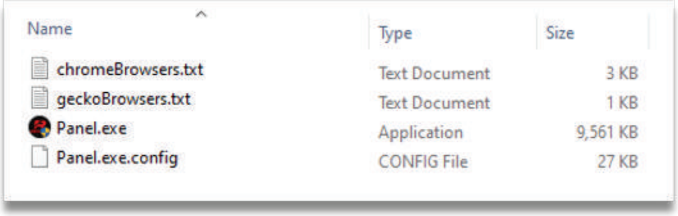
Figure 3.3. The main components of the Crack version. (Source: VIETTEL THREAT INTELLIGENCE)

To configure malware distribution, follow these steps:

1. Initialize Host to connect to Server Crack..

Stolen data will be aggregated and brought here. Therefore, there were many campaigns to distribute Crack software on a large scale to increase the number of Threat Actors and the number of logs aggregated for the Host.

2. Log in to the Cracked Panel using the provided account. Here are “ims0rry” and “dr-***.com”



Name	Type	Size
chromeBrowsers.txt	Text Document	3 KB
geckoBrowsers.txt	Text Document	1 KB
Panel.exe	Application	9,561 KB
Panel.exe.config	CONFIG File	27 KB

Figure 3.4. Panel of the Redline Stealer malware.
(Source: VIETTEL THREAT INTELLIGENCE)

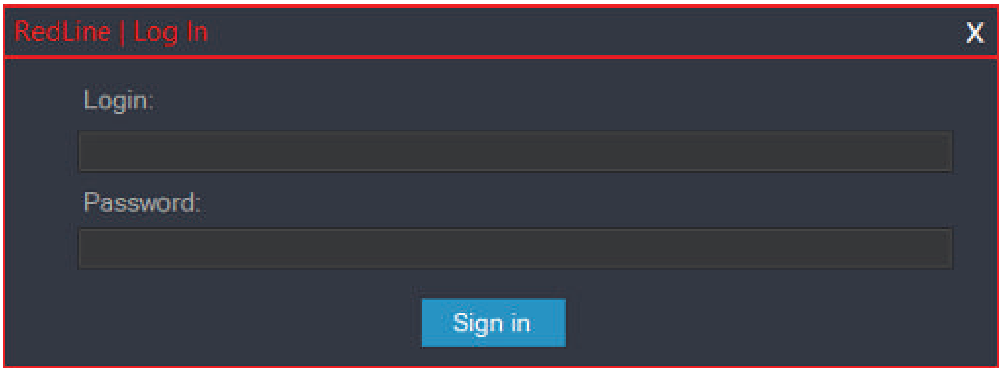
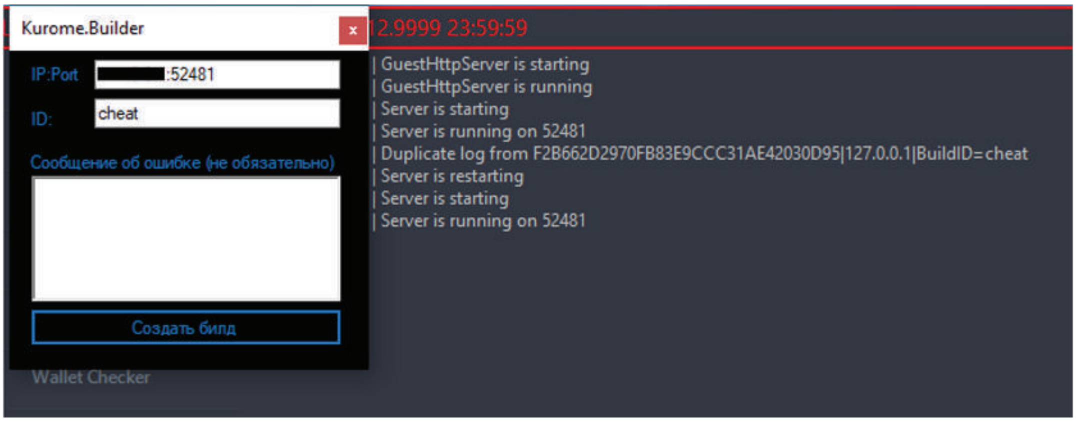


Figure 3.5. Login form to Panel. (Source: VIETTEL THREAT INTELLIGENCE)

3. Use the Builder to create the build.exe used for distribution, with the Destination as the IP:Port of the Panel build environment.



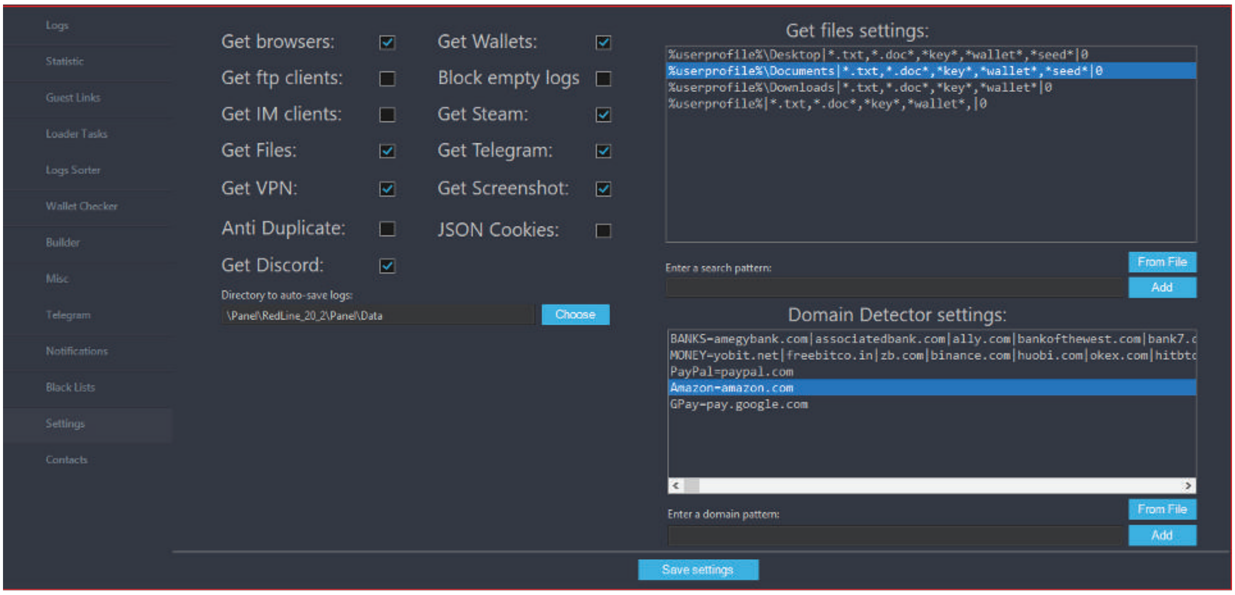
IP:Port [redacted]:52481

ID: cheat

```
12.9999 23:59:59
| GuestHttpServer is starting
| GuestHttpServer is running
| Server is starting
| Server is running on 52481
| Duplicate log from F2B662D2970FB83E9CCC31AE42030D95|127.0.0.1|BuildID=cheat
| Server is restarting
| Server is starting
| Server is running on 52481
```

Figure 3.6. Builder Clone generates malware (or third software does if it is the Crack version).
(Source: VIETTEL THREAT INTELLIGENCE)

4. Configure and customize before building malware at the Settings tab: Get files settings: configure the malware to steal files according to the desired wildcard path. For example: %userprofile%\Desktop|*.txt,*doc*,*key*,*wallet*,*seed*|0: steal all files with format *.txt, .*doc*, .* key*,.. in the victim's Desktop folder.



Get browsers: ☑
Get ftp clients: □
Get IM clients: □
Get Files: ☑
Get VPN: ☑
Anti Duplicate: □
Get Discord: ☑

Get Wallets: ☑
Block empty logs □
Get Steam: ☑
Get Telegram: ☑
Get Screenshot: ☑
JSON Cookies: □

Directory to auto-save logs: \Panel\RedLine_20_2\Panel\Data

Get files settings:

```
%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0
%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*|0
%userprofile%\Downloads|*.txt,*.doc*,*key*,*wallet*|0
%userprofile%|*.txt,*.doc*,*key*,*wallet*,|0
```

Enter a search pattern:

Domain Detector settings:

```
BANKS-amegybank.com|associatedbank.com|ally.com|bankofthewest.com|bank7.c
MONEY-yobit.net|freebitco.in|zb.com|binance.com|huobi.com|okex.com|hitbtc
PayPal=paypal.com
Amazon-amazon.com
GPay-pay.google.com
```

Enter a domain pattern:

Figure 3.7. Customize to steal information before you build malware.
(Source: VIETTEL THREAT INTELLIGENCE)

Go to the Builder tab, where the attacker packages the malware along with the customized settings above. In addition, for the Premium version of the owner at Redline Support, users will be provided with an additional Certificate.

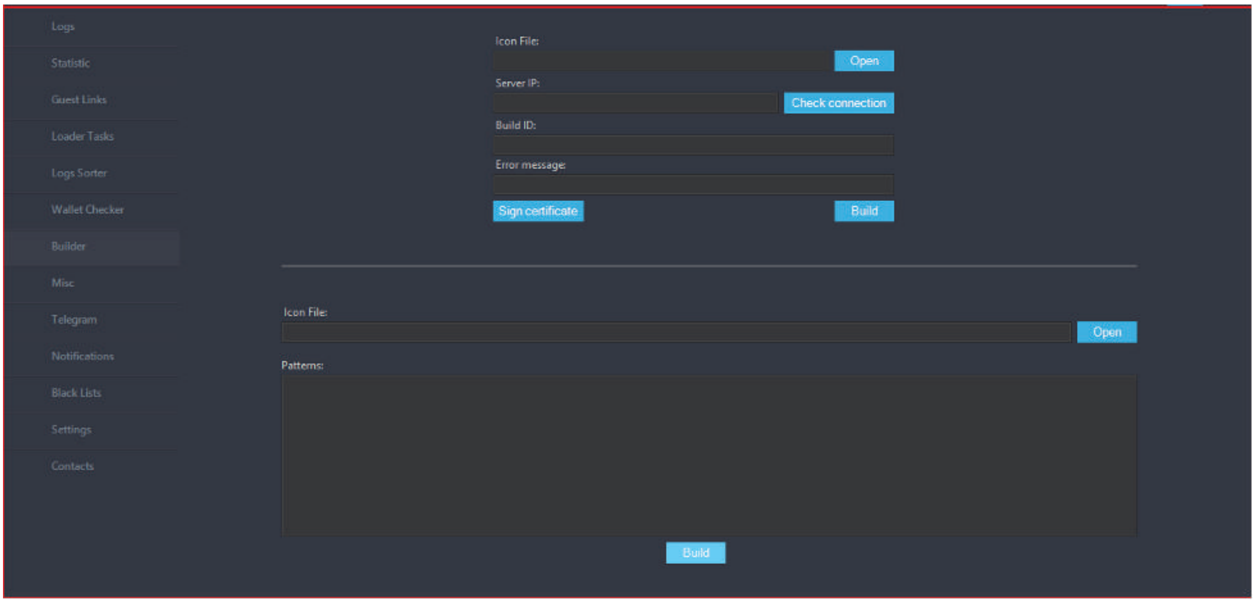
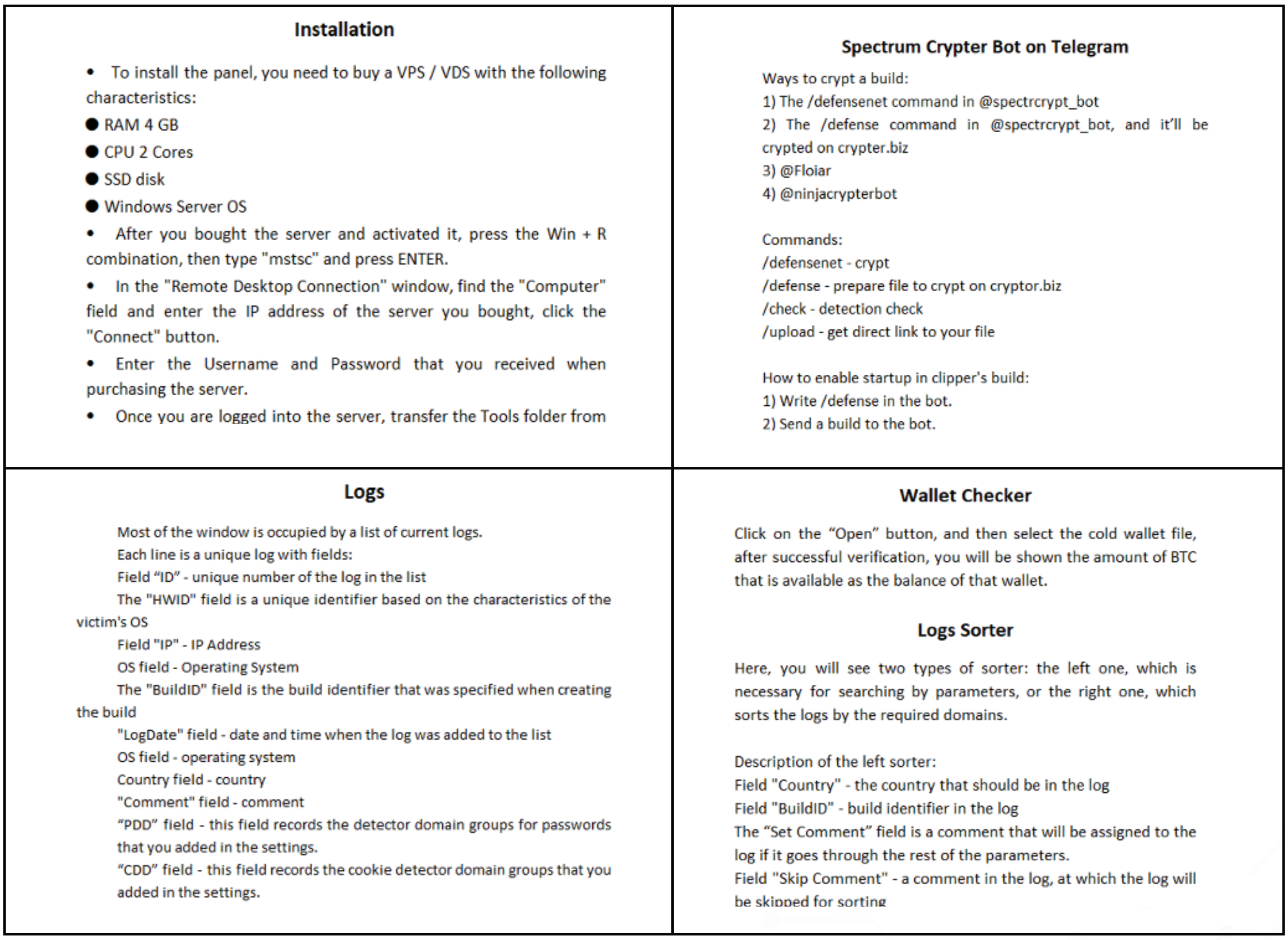


Figure 3.8. Builder generates malware (Original version will generate in Panel)
(Source: VIETTEL THREAT INTELLIGENCE)

Figure 3.9. File after packing is complete.
(Source: VIETTEL THREAT INTELLIGENCE)

In addition, the software also provides a separate FAQ to guide how to install & build Redline, explain the indexes in the software and even guide how to use Spectrum Crypter to avoid AV detection.



Installation

- To install the panel, you need to buy a VPS / VDS with the following characteristics:
- ● RAM 4 GB
- ● CPU 2 Cores
- ● SSD disk
- ● Windows Server OS
- After you bought the server and activated it, press the Win + R combination, then type "mstsc" and press ENTER.
- In the "Remote Desktop Connection" window, find the "Computer" field and enter the IP address of the server you bought, click the "Connect" button.
- Enter the Username and Password that you received when purchasing the server.
- Once you are logged into the server, transfer the Tools folder from

Spectrum Crypter Bot on Telegram

Ways to crypt a build:
1) The /defensenet command in @spectrcrypt_bot
2) The /defense command in @spectrcrypt_bot, and it'll be crypted on crypter.biz
3) @Floiar
4) @ninjacrypterbot

Commands:
/defensenet - crypt
/defense - prepare file to crypt on cryptor.biz
/check - detection check
/upload - get direct link to your file

How to enable startup in clipper's build:
1) Write /defense in the bot.
2) Send a build to the bot.

Logs

Most of the window is occupied by a list of current logs.
Each line is a unique log with fields:
Field "ID" - unique number of the log in the list
The "HWID" field is a unique identifier based on the characteristics of the victim's OS
Field "IP" - IP Address
OS field - Operating System
The "BuildID" field is the build identifier that was specified when creating the build
"LogDate" field - date and time when the log was added to the list
OS field - operating system
Country field - country
"Comment" field - comment
"PDD" field - this field records the detector domain groups for passwords that you added in the settings.
"CDD" field - this field records the cookie detector domain groups that you added in the settings.

Wallet Checker

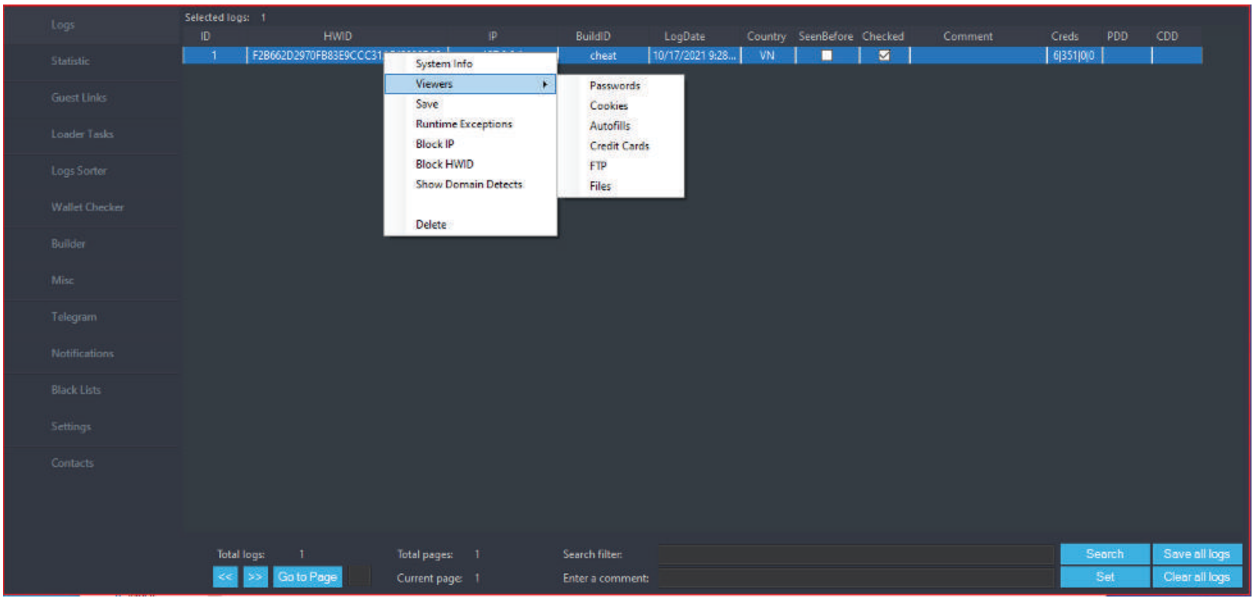
Click on the "Open" button, and then select the cold wallet file, after successful verification, you will be shown the amount of BTC that is available as the balance of that wallet.

Logs Sorter

Here, you will see two types of sorter: the left one, which is necessary for searching by parameters, or the right one, which sorts the logs by the required domains.

Description of the left sorter:
Field "Country" - the country that should be in the log
Field "BuildID" - build identifier in the log
The "Set Comment" field is a comment that will be assigned to the log if it goes through the rest of the parameters.
Field "Skip Comment" - a comment in the log, at which the log will be skipped for sorting

Figure 3.1.1. FAQ is provided by the owner. (Source: VIETTEL THREAT INTELLIGENCE)



Selected logs: 1

ID	HWID	IP	BuildID	LogDate	Country	SeenBefore	Checked	Comment	Creds	PDD	CDD
1	F2B662D2970FB83E9CCC31		cheat	10/17/2021 9:28...	VN	□	☑		6|351|0|0		

Total logs: 1
Total pages: 1
Current page: 1
Search filter:
Enter a comment:

Figure 3.1.2. The main display panel of information on infected machines.
(Source: VIETTEL THREAT INTELLIGENCE)

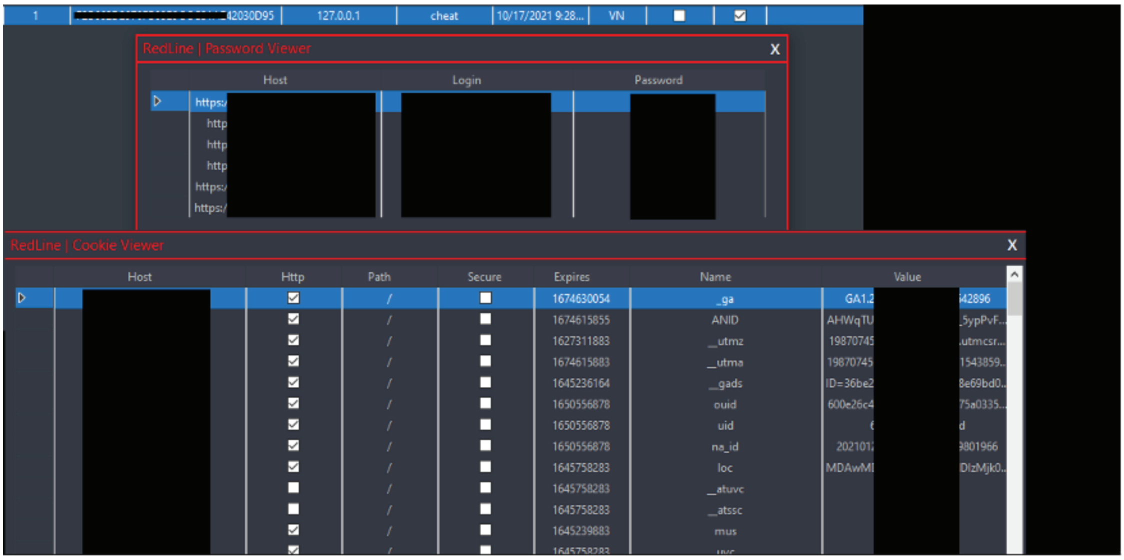
Additional tables such as Password Viewer and Cookie Viewer to display detailed values include basic information fields such as:

- Password Viewer: Host, Login, Password

After being stolen, this information can be used for malicious purposes, illegally logging into affected systems, etc.

- Cookie Viewer: Host, Http, Path, Secure, Expires, Name, Value

Stolen cookies are used by attackers to perform session stealing or spoofing, unauthorized intrusions without requiring authentication.



1	[redacted]42030D95	127.0.0.1	cheat	10/17/2021 9:28...	VN	□	☑

RedLine | Password Viewer

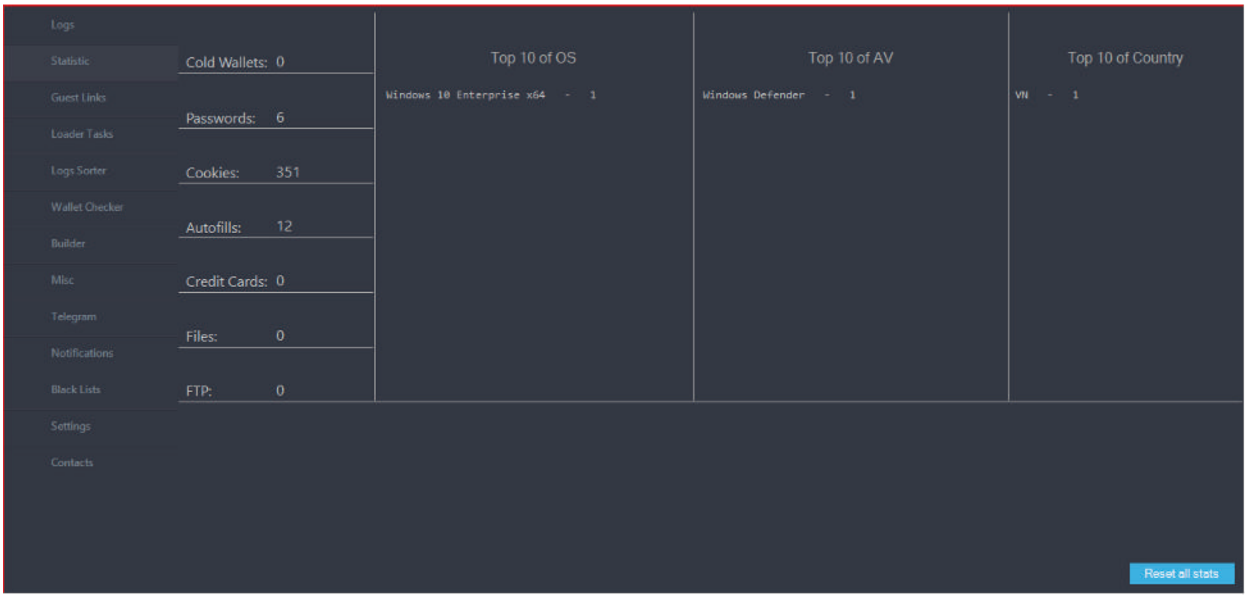
Host	Login	Password
https:/[redacted]	[redacted]	[redacted]
http[redacted]		
http[redacted]		
http[redacted]		
https:/[redacted]		
https:/[redacted]		

RedLine | Cookie Viewer

Host	Http	Path	Secure	Expires	Name	Value
[redacted]	☑	/	□	1674630054	_ga	GA1.2[redacted]42896
[redacted]	☑	/	□	1674615855	ANID	AHWqTU[redacted]_5ypPvF...
[redacted]	☑	/	□	1627311883	__utmz	19870745[redacted].utmcsr...
[redacted]	☑	/	□	1674615883	__utma	19870745[redacted]1543859...
[redacted]	☑	/	□	1645236164	__gads	ID=36be2[redacted]8e69bd0...
[redacted]	☑	/	□	1650556878	ouid	600e26c4[redacted]75a0335...
[redacted]	☑	/	□	1650556878	uid	6[redacted]d
[redacted]	☑	/	□	1650556878	na_id	2021012[redacted]9801966
[redacted]	☑	/	□	1645758283	loc	MDAwMI[redacted]DlzMjk0...
[redacted]	□	/	□	1645758283	__atuvc	[redacted]
[redacted]	□	/	□	1645758283	__atssc	[redacted]
[redacted]	☑	/	□	1645239883	mus	[redacted]

Figure 3.1.3. Detailed information about the fields of the collected record.
(Source: VIETTEL THREAT INTELLIGENCE)

To get the number of machines that have been successfully infected, the Statistic table shows the number of values in an overview as follows:

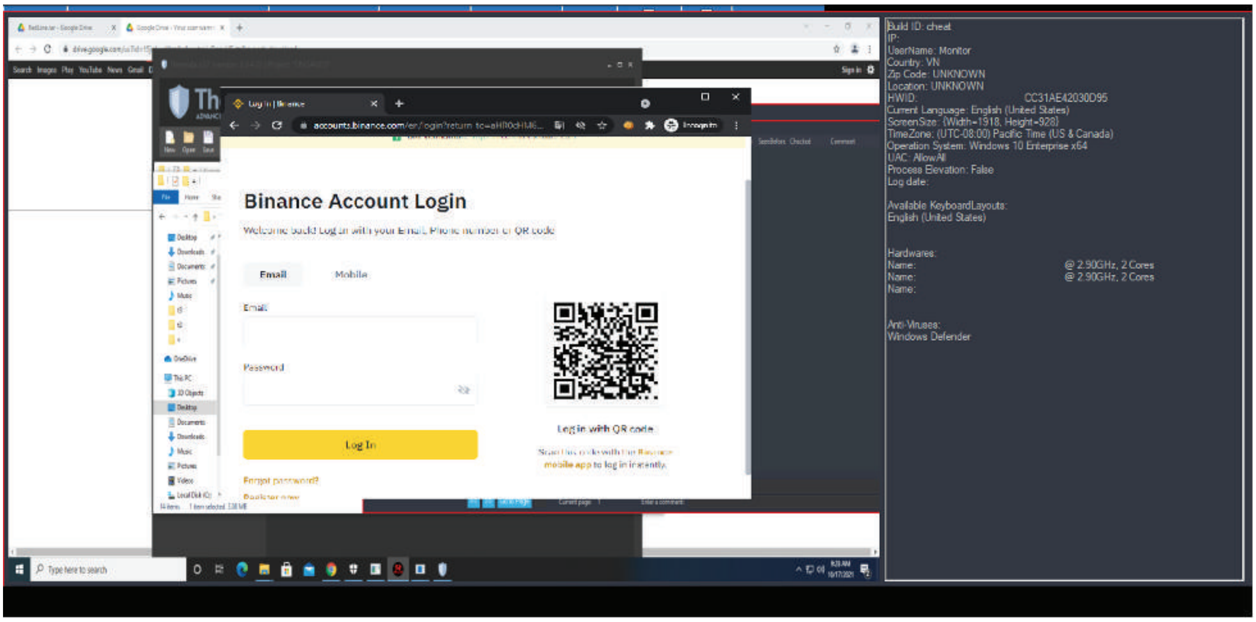


Cold Wallets: 0
Passwords: 6
Cookies: 351
Autofills: 12
Credit Cards: 0
Files: 0
FTP: 0

Top 10 of OS	Top 10 of AV	Top 10 of Country
Windows 10 Enterprise x64 - 1	Windows Defender - 1	VN - 1

Figure 3.1.4. The number of infected machines is detailed in the Statistic table.
(Source: VIETTEL THREAT INTELLIGENCE)

The System Viewer sub-panel is used to display system information and screenshots as soon as the victim executes malware on the machine.


Binance Account Login
Welcome back! Log in with your Email, Phone number or QR code
Email
Mobile
Email
Password
Log In
Forgot password?
Register now
Log in with QR code
Scan this code with the Binance mobile app to log in instantly.

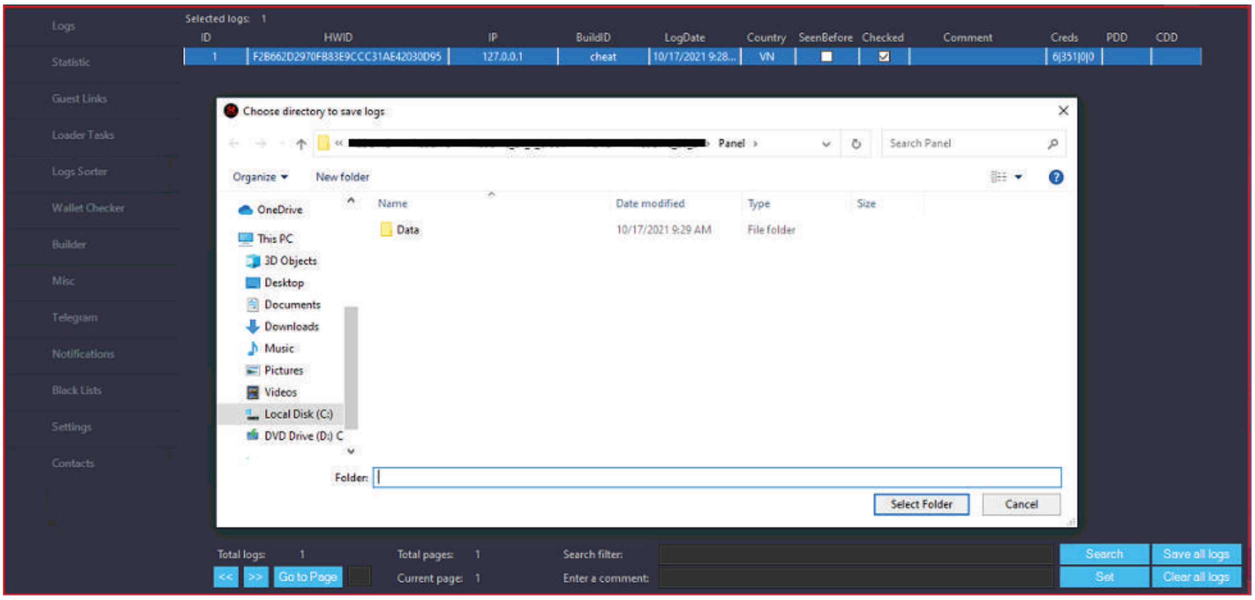
```
Build ID: cheat
IP:
UserName: Monitor
Country: VN
Zip Code: UNKNOWN
Location: UNKNOWN
HWID:                    CC31AE42030D95
Current Language: English (United States)
ScreenSize: {Width=1918, Height=928}
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
Operation System: Windows 10 Enterprise x64
UAC: AllowAll
Process Elevation: False
Log date:

Available KeyboardLayouts:
English (United States)


Hardwares:
Name:                          @ 2.90GHz, 2 Cores
Name:                          @ 2.90GHz, 2 Cores
Name:


Anti-Viruses:
Windows Defender
```

Figure 3.1.5. Screenshots and system information.
(Source: VIETTEL THREAT INTELLIGENCE)



Selected logs: 1

ID	HWID	IP	BuildID	LogDate	Country	SeenBefore	Checked	Comment	Creds	PDD	CDD
1	F2B662D2970FB83E9CCC31AE42030D95	127.0.0.1	cheat	10/17/2021 9:28...	VN	□	☑		6|351|0|0		

Choose directory to save logs

« [redacted] › Panel ›

Name	Date modified	Type	Size
Data	10/17/2021 9:29 AM	File folder	

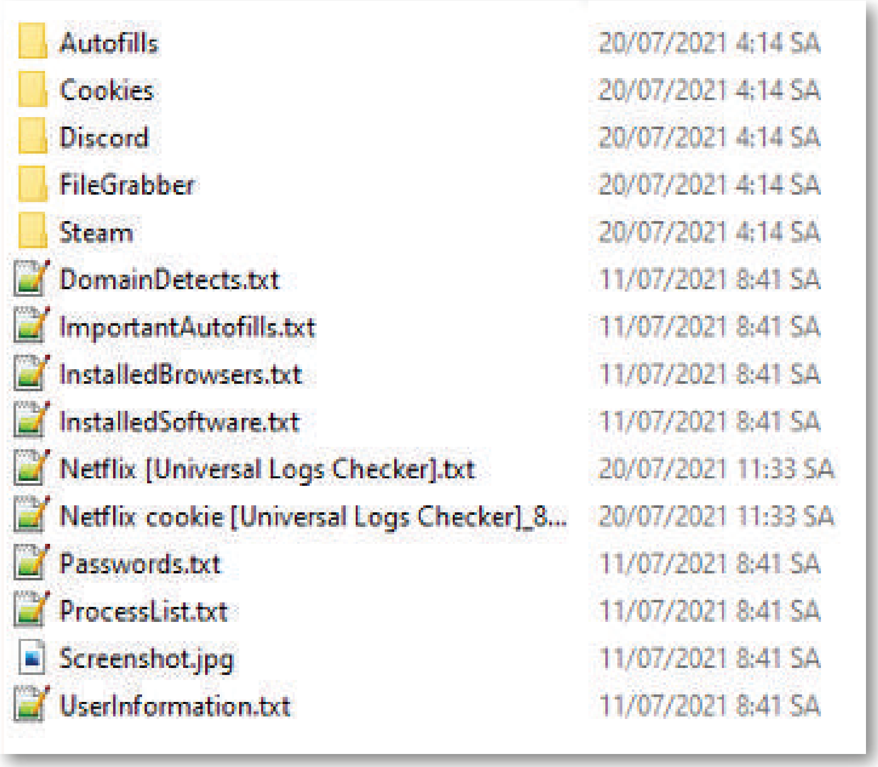
Folder:

Total logs: 1 Total pages: 1 Search filter:

Current page: 1 Enter a comment:

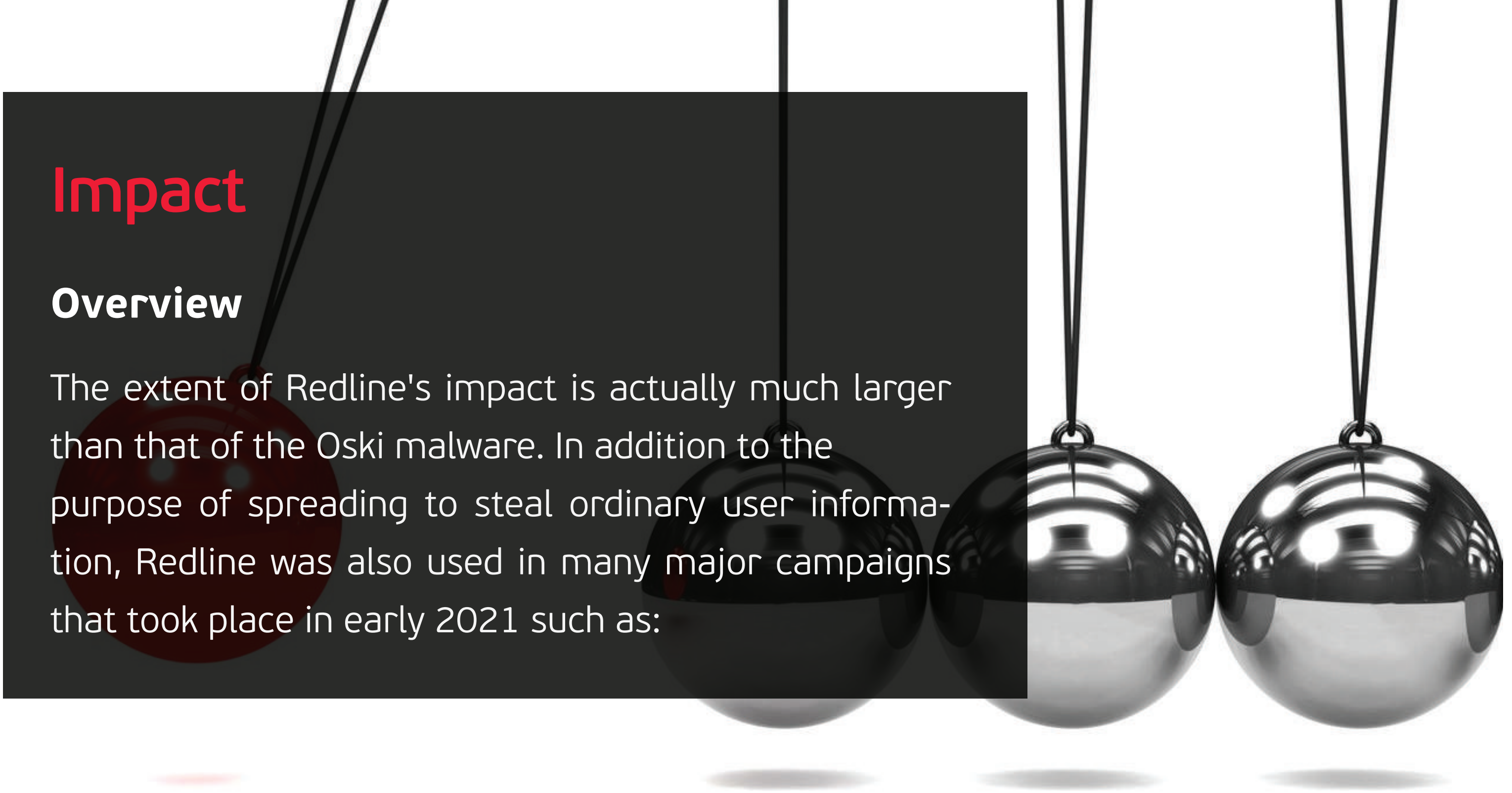
Figure 3.1.6. Attacker saves Logs data to execute next Phase.
(Source: VIETTEL THREAT INTELLIGENCE)

After completing the information stealing, the folder will be compressed with a name as the format:
CountryCode (ISO-3166-1-a-2)[HWID][Date_Time].zip
(eg:AM[F6B6356DD68E3FD59A56680E6BEDD5F7]
[2021-07-29T20_39_03.8503625].zip) and send it back via C&C.



Autofills	20/07/2021 4:14 SA
Cookies	20/07/2021 4:14 SA
Discord	20/07/2021 4:14 SA
FileGrabber	20/07/2021 4:14 SA
Steam	20/07/2021 4:14 SA
DomainDetects.txt	11/07/2021 8:41 SA
ImportantAutofills.txt	11/07/2021 8:41 SA
InstalledBrowsers.txt	11/07/2021 8:41 SA
InstalledSoftware.txt	11/07/2021 8:41 SA
Netflix [Universal Logs Checker].txt	20/07/2021 11:33 SA
Netflix cookie [Universal Logs Checker]_8...	20/07/2021 11:33 SA
Passwords.txt	11/07/2021 8:41 SA
ProcessList.txt	11/07/2021 8:41 SA
Screenshot.jpg	11/07/2021 8:41 SA
UserInformation.txt	11/07/2021 8:41 SA

Figure 3.1.7. The information after being collected and extracted will have the form above.
(Source: VIETTEL THREAT INTELLIGENCE)



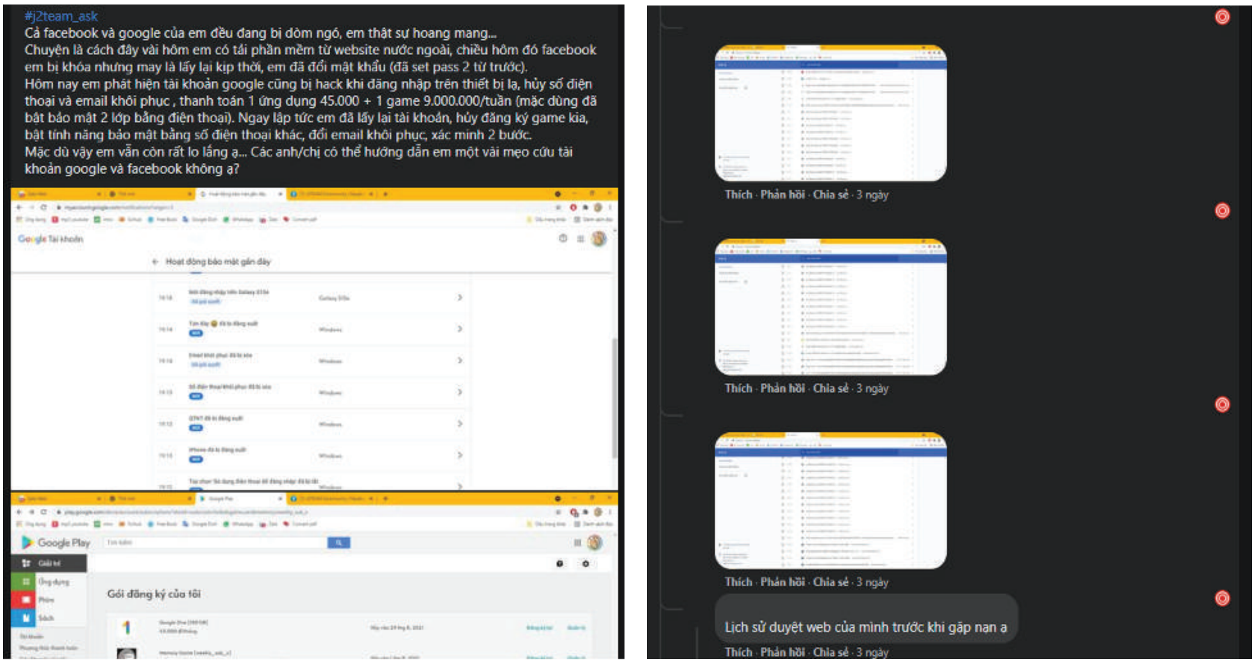
Impact

Overview

The extent of Redline's impact is actually much larger than that of the Oski malware. In addition to the purpose of spreading to steal ordinary user information, Redline was also used in many major campaigns that took place in early 2021 such as:

Time	Campaign	Key Information
2021-06-17	Digital artists targeted in RedLine infostealer campaign	The campaign targeted Digital Artists to hijack NFT accounts or steal Tokens on NFT exchanges.
2021-05-17	Threat Actors Use MSBuild to Deliver RATs Filelessly	The campaign used MSBuild to distribute the Remcos RAT and Redline Stealer.
2021-04-27	RedLine Stealer Masquerades as Telegram Installer Become A VIP Victim With New Discord Distributed Malware	The campaign used Google Ads to trick users into downloading fake Signal, Viber and Telegram apps containing Redline Stealer.
2020-03-16	New Redline Password Stealer Malware	The Email Phishing campaign containing Redline Stealer targeted the US by taking advantage of COVID-19 vaccine issues.

Being in the one of the target groups of this malware, many ordinary users in Vietnam have also become victims of this malware’s campaigns to steal information, due to downloading some rampant cr@ck software on the sites that were warned in the previous section.



#j2team_ask
Cả facebook và google của em đều đang bị dòm ngó, em thật sự hoang mang...
Chuyện là cách đây vài hôm em có tải phần mềm từ website nước ngoài, chiều hôm đó facebook em bị khóa nhưng may là lấy lại kịp thời, em đã đổi mật khẩu (đã set pass 2 từ trước).
Hôm nay em phát hiện tài khoản google cũng bị hack khi đăng nhập trên thiết bị lạ, hủy số điện thoại và email khôi phục , thanh toán 1 ứng dụng 45.000 + 1 game 9.000.000/tuần (mặc dùng đã bật bảo mật 2 lớp bằng điện thoại). Ngay lập tức em đã lấy lại tài khoản, hủy đăng ký game kia, bật tính năng bảo mật bằng số điện thoại khác, đổi email khôi phục, xác minh 2 bước.
Mặc dù vậy em vẫn còn rất lo lắng ạ... Các anh/chị có thể hướng dẫn em một vài mẹo cứu tài khoản google và facebook không ạ?

Thích · Phản hồi · Chia sẻ · 3 ngày

Thích · Phản hồi · Chia sẻ · 3 ngày

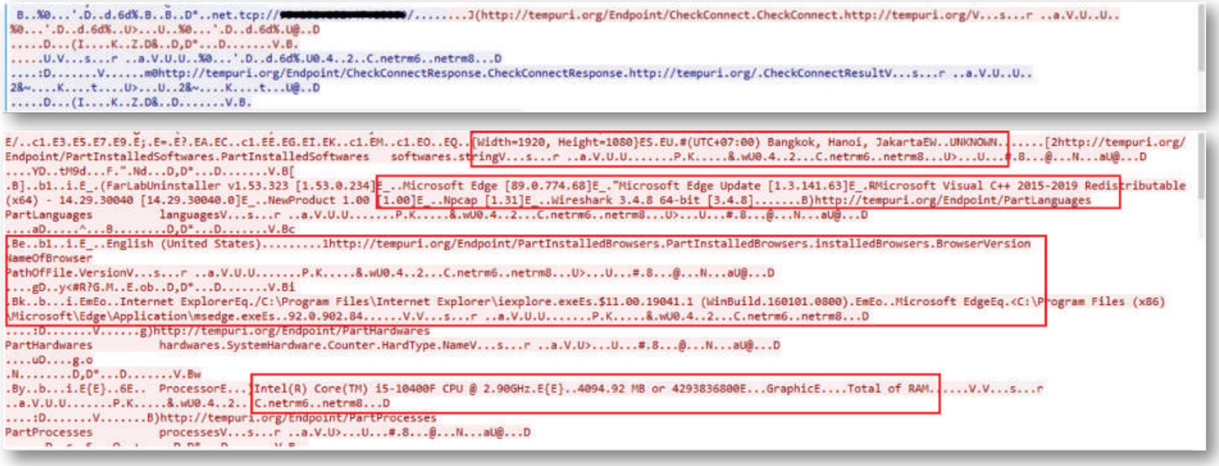
Thích · Phản hồi · Chia sẻ · 3 ngày

Lịch sử duyệt web của mình trước khi gặp nan a

Thích · Phản hồi · Chia sẻ · 3 ngày

Figure 4.1.Infected users ask for help in some groups on Facebook.
(Source: VIETTEL THREAT INTELLIGENCE)

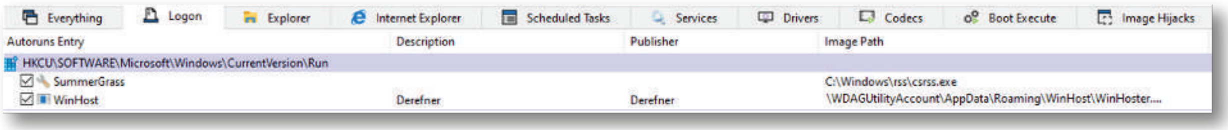
After collecting information, analyzing and reviewing, VIETTEL THREAT INTELLIGENCE identified the type of malware as Redline Stealer with typically conspicuous characteristics.



```
B..%0...'.D..d.6d%.B..B..D*..net.tcp://[redacted]/........J(http://tempuri.org/Endpoint/CheckConnect.CheckConnect.http://tempuri.org/V...s...r ..a.V.U..U..
%0...'.D..d.6d%..U>...U..%0...'.D..d.6d%.U@..D
.....D...(I....K..Z.D&..D,D*...D.......V.B.
.....U.V...s...r ..a.V.U.U..%0...'.D..d.6d%.U0.4..2..C.netrm6..netrm8...D
....:D.......V......m0http://tempuri.org/Endpoint/CheckConnectResponse.CheckConnectResponse.http://tempuri.org/.CheckConnectResultV...s...r ..a.V.U..U..
2&~....K....t....U>...U..2&~....K....t...U@..D
.....D...(I....K..Z.D&..D.......V.B.
```

```
E/..c1.E3.E5.E7.E9.Ë;.E=.E?.EA.EC..c1.EE.EG.EI.EK..c1.EM..c1.EO..EQ..{Width=1920, Height=1080}ES.EU.#(UTC+07:00) Bangkok, Hanoi, JakartaEW..UNKNOWN.......[2http://tempuri.org/
Endpoint/PartInstalledSoftwares.PartInstalledSoftwares   softwares.stringV...s...r ..a.V.U.U.......P.K.....&.wU0.4..2...C.netrm6..netrm8...U>...U...#.8...@...N...aU@...D
....YD..tM9d...F.".Nd...D,D*...D.......V.B[
.B]..b1..i.E_.(FarLabUninstaller v1.53.323 [1.53.0.234]E_..Microsoft Edge [89.0.774.68]E_."Microsoft Edge Update [1.3.141.63]E_.RMicrosoft Visual C++ 2015-2019 Redistributable
(x64) - 14.29.30040 [14.29.30040.0]E_..NewProduct 1.00 [1.00]E_..Npcap [1.31]E_..Wireshark 3.4.8 64-bit [3.4.8].......B)http://tempuri.org/Endpoint/PartLanguages
PartLanguages          languagesV...s...r ..a.V.U.U.......P.K.....&.wU0.4..2...C.netrm6..netrm8...U>...U...#.8...@...N...aU@...D
....aD....^...B........D,D*...D.......V.Bc
.Be..b1..i.E_..English (United States).........1http://tempuri.org/Endpoint/PartInstalledBrowsers.PartInstalledBrowsers.installedBrowsers.BrowserVersion
NameOfBrowser
PathOfFile.VersionV...s...r ..a.V.U.U.......P.K.....&.wU0.4..2...C.netrm6..netrm8...U>...U...#.8...@...N...aU@...D
....gD..y<#R?G.M..E.ob..D,D*...D.......V.Bi
.Bk..b...i.EmEo..Internet ExplorerEq./C:\Program Files\Internet Explorer\iexplore.exeEs.$11.00.19041.1 (WinBuild.160101.0800).EmEo..Microsoft EdgeEq.<C:\Program Files (x86)
\Microsoft\Edge\Application\msedge.exeEs..92.0.902.84......V.V...s...r ..a.V.U.U.......P.K.....&.wU0.4..2...C.netrm6..netrm8...D
....:D.......V......g)http://tempuri.org/Endpoint/PartHardwares
PartHardwares          hardwares.SystemHardware.Counter.HardType.NameV...s...r ..a.V.U>...U...#.8...@...N...aU@...D
....uD....g.o
.N........D,D*...D.......V.Bw
.By..b...i.E{E}..6E..  ProcessorE...Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz.E{E}..4094.92 MB or 4293836800E...GraphicE....Total of RAM......V.V...s...r
..a.V.U.U.......P.K.....&.wU0.4..2...C.netrm6..netrm8...D
....:D.......V.......B)http://tempuri.org/Endpoint/PartProcesses
PartProcesses          processesV...s...r ..a.V.U>...U...#.8...@...N...aU@...D
```

Figure 4.2. The malware uses SOAP HTTP to make connections and communicate with C&C.
(Source: VIETTEL THREAT INTELLIGENCE)



Autoruns Entry	Description	Publisher	Image Path
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ SummerGrass			C:\Windows\rss\csrss.exe
☑ WinHost	Derefner	Derefner	\WDAGUtilityAccount\AppData\Roaming\WinHost\WinHoster....

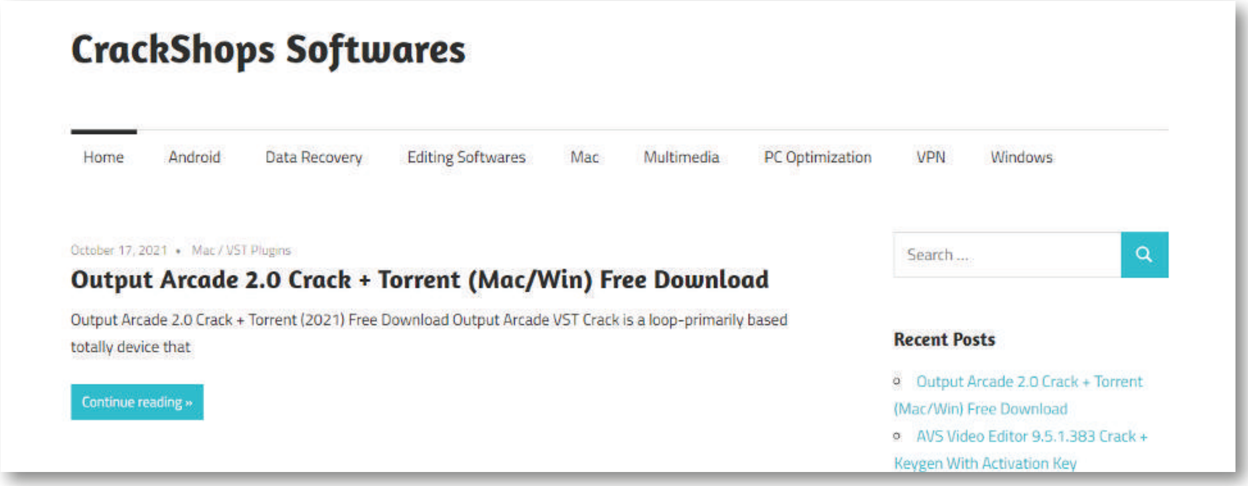
Figure 4.3. The malware executes Persistence using Autologon

Method of Infection

Through campaigns related to the Redline Stealer malware, the infection methods used are very diverse such as:

Time	Campaign	Content	Attack Method
2021-06-17	Digital artists targeted in RedLine infostealer campaign	The campaign targets Digital Artists to hijack NFT accounts or steal Tokens on NFT exchanges.	Directly contacting with the victim via social media.
2021-05-17	Threat Actors Use MSBuild to Deliver RATs Filelessly	The campaign uses MSBuild to distribute the Remcos RAT and Redline Stealer.	Phishing
2021-04-27	RedLine Stealer Masquerades as Telegram Installer Become A VIP Victim With New Discord Distributed Malware	The campaign uses Google Ads to trick users into downloading fake Signal, Viber and Telegram apps containing Redline Stealer.	Taking advantage of the cover of many software like Telegram, Whatsapp or legitimate websites like Pastebin to trick users into downloading.
2020-03-16	New Redline Password Stealer Malware	The Email Phishing campaign containing Redline Stealer targets the US by taking advantage of COVID-19 vaccine issues.	Phishing

In addition, with the same infection method as Part I, the attacker prepares a large number of the above websites to download software containing Redline malware. These websites are created with SEO standards by supporting plugins to be in the top of search results on Google in many countries.



CrackShops Softwares

Home | Android | Data Recovery | Editing Softwares | Mac | Multimedia | PC Optimization | VPN | Windows

October 17, 2021 • Mac / VST Plugins

Output Arcade 2.0 Crack + Torrent (Mac/Win) Free Download

Output Arcade 2.0 Crack + Torrent (2021) Free Download Output Arcade VST Crack is a loop-primarily based totally device that

Continue reading »

Search …

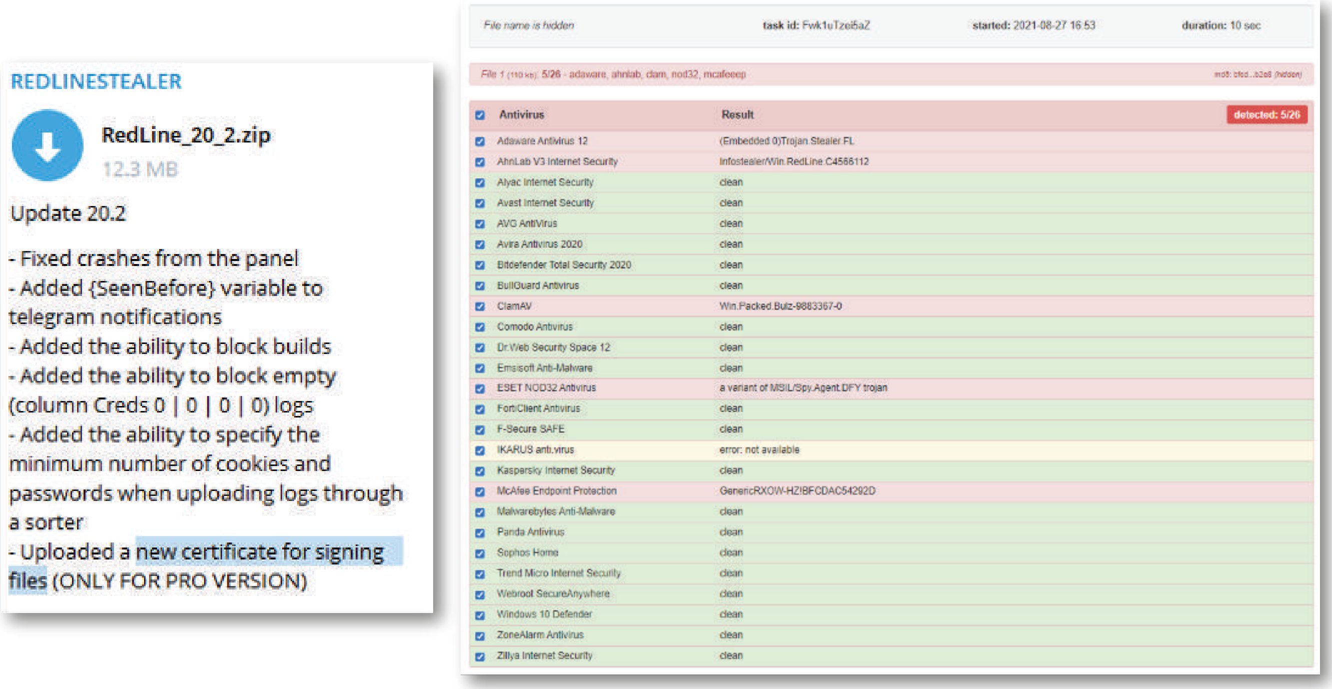
Recent Posts

- Output Arcade 2.0 Crack + Torrent (Mac/Win) Free Download
- AVS Video Editor 9.5.1.383 Crack + Keygen With Activation Key

Figure 4.4. Websites containing Redline Stealer malware trick users into downloading

Cause of Infection

With the development and upgrade, TA advertised that if users use the upgraded version, the malware would be provided with a signing file cert to bypass current AV software.



REDLINESTEALER

RedLine_20_2.zip

12.3 MB

Update 20.2

- Fixed crashes from the panel
- Added {SeenBefore} variable to telegram notifications
- Added the ability to block builds
- Added the ability to block empty (column Creds 0 | 0 | 0 | 0) logs
- Added the ability to specify the minimum number of cookies and passwords when uploading logs through a sorter
- Uploaded a new certificate for signing files (ONLY FOR PRO VERSION)

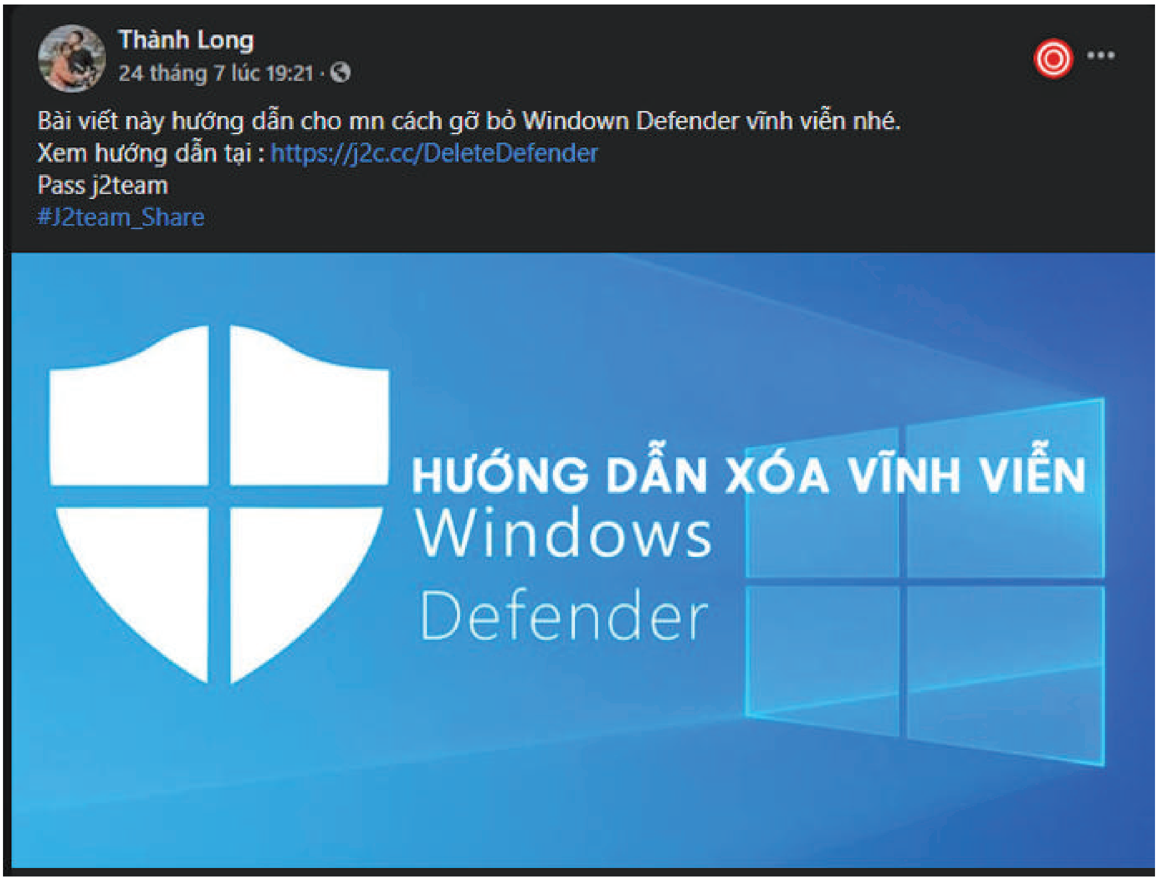
File name is hidden | task id: Fwk1uTzei5aZ | started: 2021-08-27 16:53 | duration: 10 sec

File 1 (110 kb): 5/26 - adaware, ahnlab, clam, nod32, mcafeeep | md5: cfcd...b2a8 (hidden)

☑	Antivirus	Result	detected: 5/26
☑	Adaware Antivirus 12	(Embedded 0)Trojan.Stealer.FL	
☑	AhnLab V3 Internet Security	Infostealer/Win.RedLine.C4566112	
☑	Alyac Internet Security	clean	
☑	Avast Internet Security	clean	
☑	AVG AntiVirus	clean	
☑	Avira Antivirus 2020	clean	
☑	Bitdefender Total Security 2020	clean	
☑	BullGuard Antivirus	clean	
☑	ClamAV	Win.Packed.Bulz-9883367-0	
☑	Comodo Antivirus	clean	
☑	Dr.Web Security Space 12	clean	
☑	Emsisoft Anti-Malware	clean	
☑	ESET NOD32 Antivirus	a variant of MSIL/Spy.Agent.DFY trojan	
☑	FortiClient Antivirus	clean	
☑	F-Secure SAFE	clean	
☑	IKARUS anti.virus	error: not available	
☑	Kaspersky Internet Security	clean	
☑	McAfee Endpoint Protection	GenericRXOW-HZ!BFCDAC54292D	
☑	Malwarebytes Anti-Malware	clean	
☑	Panda Antivirus	clean	
☑	Sophos Home	clean	
☑	Trend Micro Internet Security	clean	
☑	Webroot SecureAnywhere	clean	
☑	Windows 10 Defender	clean	
☑	ZoneAlarm Antivirus	clean	
☑	Zillya Internet Security	clean	

Figure 4.5. Few AVs detect this as malware. (Source: VIETTEL THREAT INTELLIGENCE)

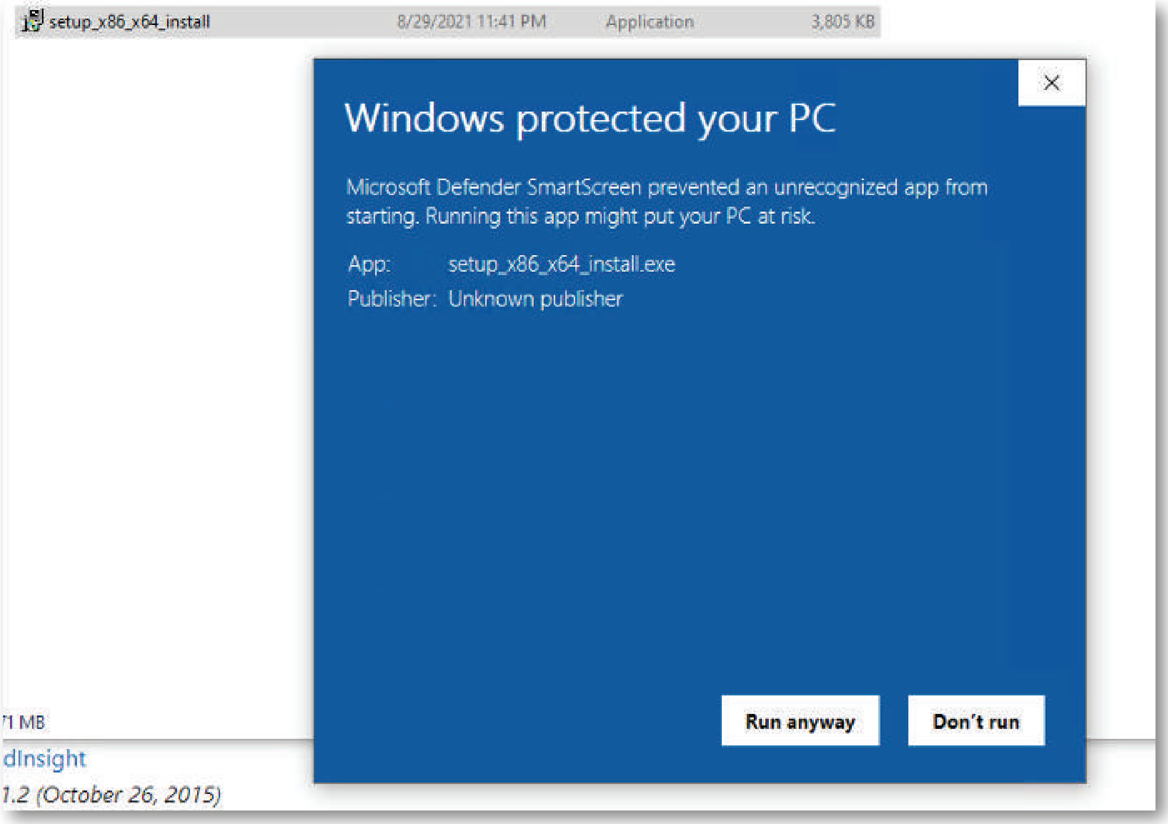
In addition, a more common cause of being affected by information-stealing malware is the frequent use of cracked software, not using anti-virus software or even removing Windows Defender on the machine for more convenient use.



Thành Long
24 tháng 7 lúc 19:21 ·

Bài viết này hướng dẫn cho mn cách gỡ bỏ Windown Defender vĩnh viễn nhé.
Xem hướng dẫn tại : https://j2c.cc/DeleteDefender
Pass j2team
#J2team_Share

Figure 4.6. The article guides you to completely remove Windows Defender.
(Source: VIETTEL THREAT INTELLIGENCE)



setup_x86_x64_install 8/29/2021 11:41 PM Application 3,805 KB

Windows protected your PC

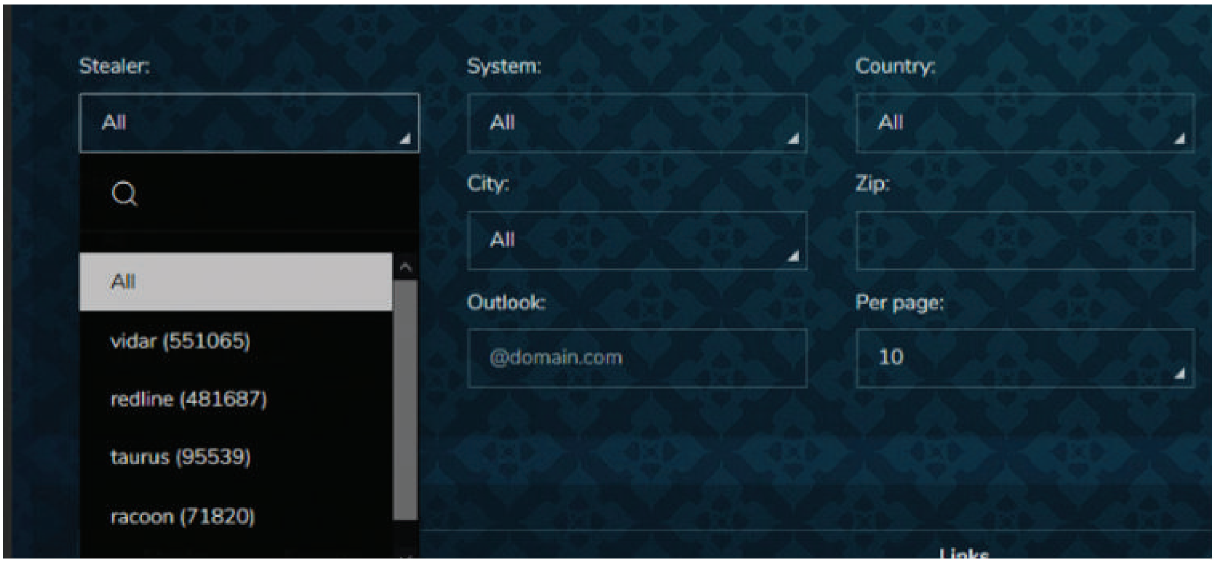
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: setup_x86_x64_install.exe
Publisher: Unknown publisher

Figure 4.7. Windows always warns applications of unknown origin, but users often ignore it.
(Source: VIETTEL THREAT INTELLIGENCE)

Trading Stolen Data on Dark Web

The stolen data will be for sale on Underground forums or group channels at Telegram. Typically at Russian Market, one of the largest illegal transactions of stolen data in the Dark Web is as follows:



Stealer: All

All
vidar (551065)
redline (481687)
taurus (95539)
racoon (71820)

System: All

Country: All

City: All

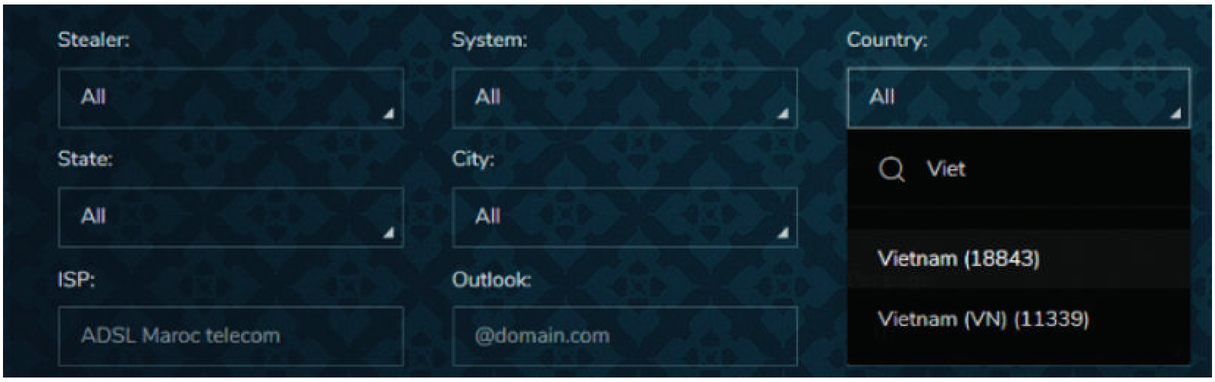
Zip:

Outlook: @domain.com

Per page: 10

Links

Figure 4.8. User information stolen by Redline amounts to 481,687 computers. (Image: VIETTEL THREAT INTELLIGENCE)



Stealer: All

System: All

Country: All

Viet
Vietnam (18843)
Vietnam (VN) (11339)

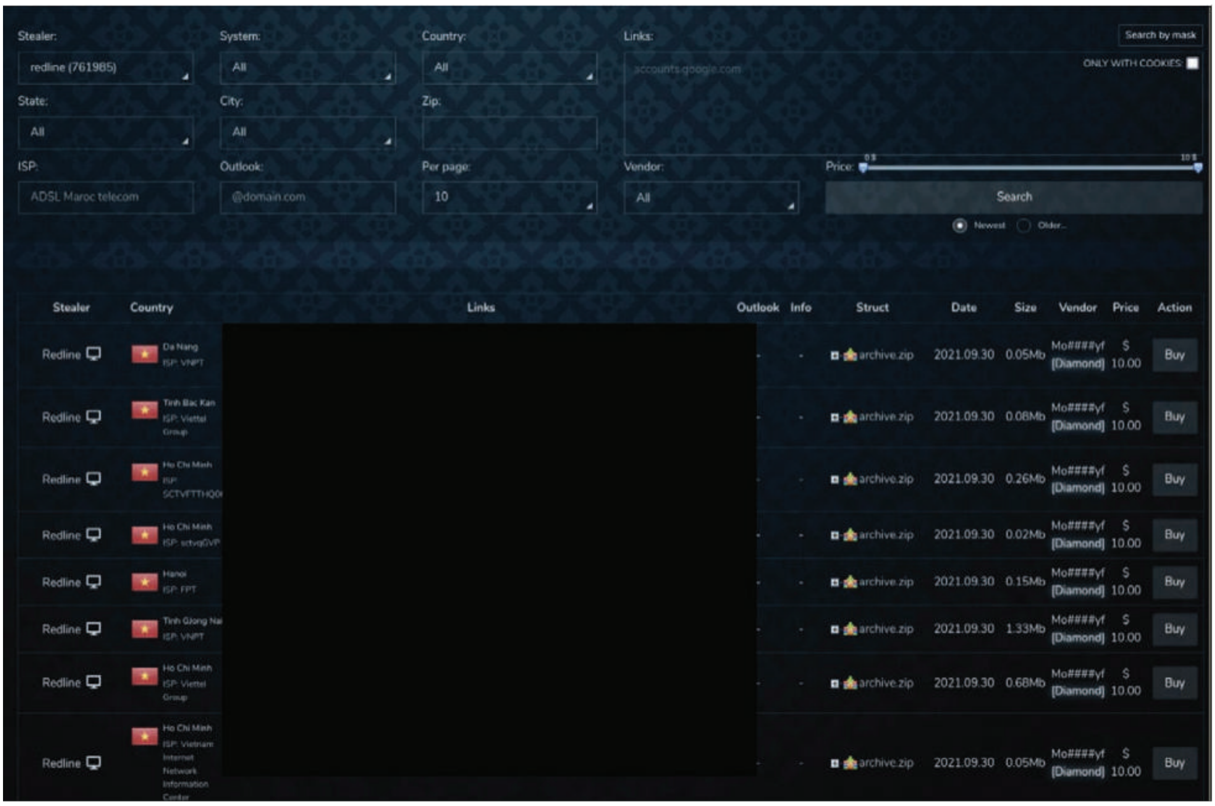
State: All

City: All

ISP: ADSL Maroc telecom

Outlook: @domain.com

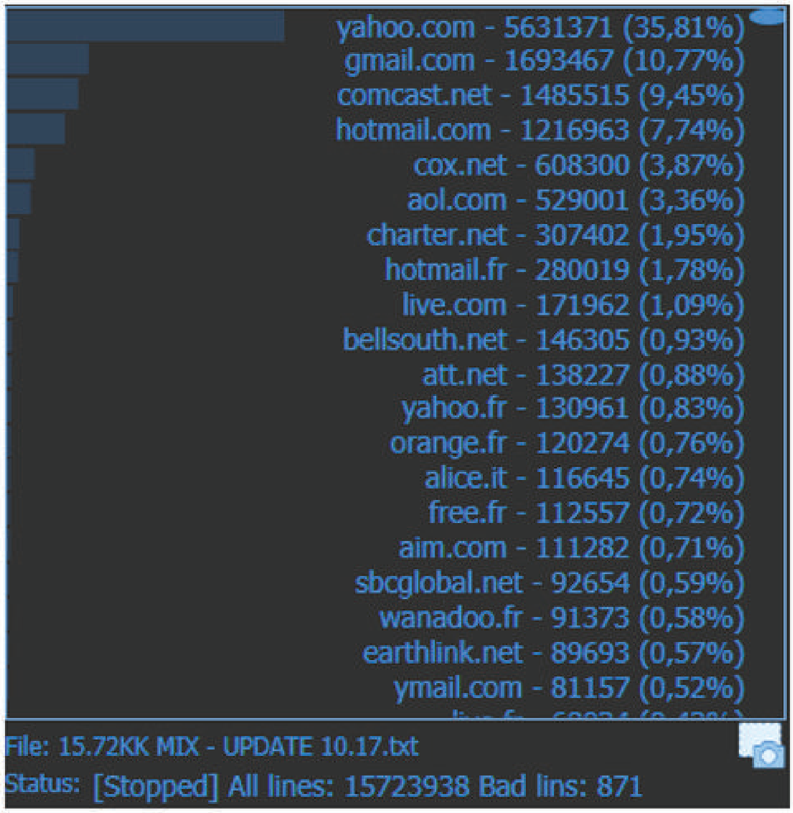
Figure 4.9. Vietnam contains more than 30,000 computers for sale with stolen information. (Image: VIETTEL THREAT INTELLIGENCE)



Stealer: redline (761985)
System: All
Country: All
Links: accounts.google.com
Search by mask
ONLY WITH COOKIES: □
State: All
City: All
Zip:
ISP: ADSL Maroc telecom
Outlook: @domain.com
Per page: 10
Vendor: All
Price: 0 $ – 10 $
Search
● Newest ○ Older...

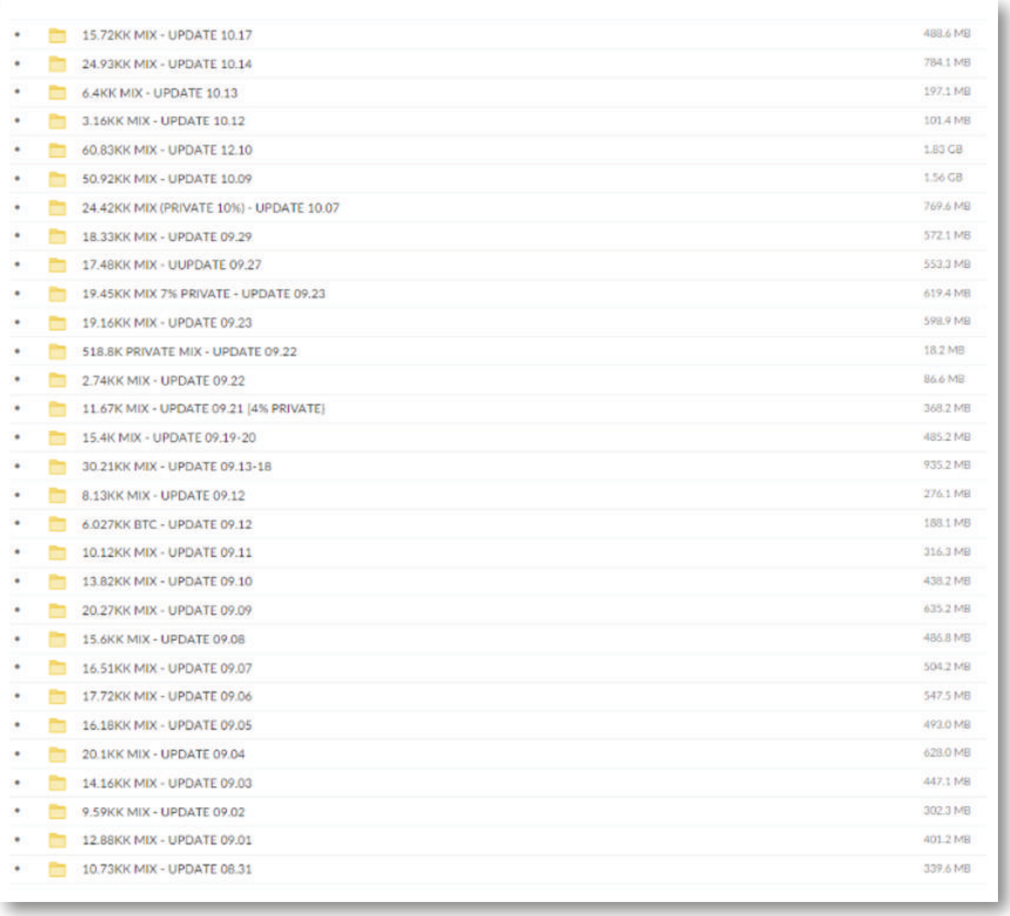
Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Redline	Da Nang ISP: VNPT	[redacted]	-	-	archive.zip	2021.09.30	0.05Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Tinh Bac Kan ISP: Viettel Group	[redacted]	-	-	archive.zip	2021.09.30	0.08Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Ho Chi Minh ISP: SCTVFTTHQ0	[redacted]	-	-	archive.zip	2021.09.30	0.26Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Ho Chi Minh ISP: sctvqGVP	[redacted]	-	-	archive.zip	2021.09.30	0.02Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Hanoi ISP: FPT	[redacted]	-	-	archive.zip	2021.09.30	0.15Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Tinh Giong Nai ISP: VNPT	[redacted]	-	-	archive.zip	2021.09.30	1.33Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Ho Chi Minh ISP: Viettel Group	[redacted]	-	-	archive.zip	2021.09.30	0.68Mb	Mo####yf [Diamond]	$ 10.00	Buy
Redline	Ho Chi Minh ISP: Vietnam Internet Network Information Center	[redacted]	-	-	archive.zip	2021.09.30	0.05Mb	Mo####yf [Diamond]	$ 10.00	Buy

Figure 4.1.1. Data related to Vietnam is for sale at Russian Market (Photo: Recorded Future)



```
yahoo.com - 5631371 (35,81%)
gmail.com - 1693467 (10,77%)
comcast.net - 1485515 (9,45%)
hotmail.com - 1216963 (7,74%)
cox.net - 608300 (3,87%)
aol.com - 529001 (3,36%)
charter.net - 307402 (1,95%)
hotmail.fr - 280019 (1,78%)
live.com - 171962 (1,09%)
bellsouth.net - 146305 (0,93%)
att.net - 138227 (0,88%)
yahoo.fr - 130961 (0,83%)
orange.fr - 120274 (0,76%)
alice.it - 116645 (0,74%)
free.fr - 112557 (0,72%)
aim.com - 111282 (0,71%)
sbcglobal.net - 92654 (0,59%)
wanadoo.fr - 91373 (0,58%)
earthlink.net - 89693 (0,57%)
ymail.com - 81157 (0,52%)
File: 15.72KK MIX - UPDATE 10.17.txt
Status: [Stopped] All lines: 15723938 Bad lins: 871
```

Figure 4.1.2. Number of stolen records for sale classified by domain. (Source: Telegram)

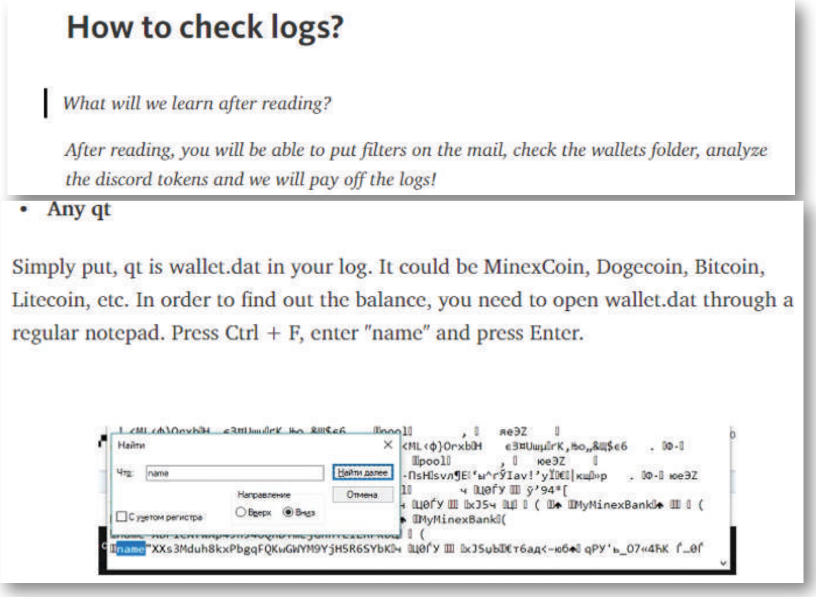


15.72KK MIX - UPDATE 10.17	488.6 MB
24.93KK MIX - UPDATE 10.14	784.1 MB
6.4KK MIX - UPDATE 10.13	197.1 MB
3.16KK MIX - UPDATE 10.12	101.4 MB
60.83KK MIX - UPDATE 12.10	1.83 GB
50.92KK MIX - UPDATE 10.09	1.56 GB
24.42KK MIX (PRIVATE 10%) - UPDATE 10.07	769.6 MB
18.33KK MIX - UPDATE 09.29	572.1 MB
17.48KK MIX - UUPDATE 09.27	553.3 MB
19.45KK MIX 7% PRIVATE - UPDATE 09.23	619.4 MB
19.16KK MIX - UPDATE 09.23	598.9 MB
518.8K PRIVATE MIX - UPDATE 09.22	18.2 MB
2.74KK MIX - UPDATE 09.22	86.6 MB
11.67K MIX - UPDATE 09.21 (4% PRIVATE)	368.2 MB
15.4K MIX - UPDATE 09.19-20	485.2 MB
30.21KK MIX - UPDATE 09.13-18	935.2 MB
8.13KK MIX - UPDATE 09.12	276.1 MB
6.027KK BTC - UPDATE 09.12	188.1 MB
10.12KK MIX - UPDATE 09.11	316.3 MB
13.82KK MIX - UPDATE 09.10	438.2 MB
20.27KK MIX - UPDATE 09.09	635.2 MB
15.6KK MIX - UPDATE 09.08	486.8 MB
16.51KK MIX - UPDATE 09.07	504.2 MB
17.72KK MIX - UPDATE 09.06	547.5 MB
16.18KK MIX - UPDATE 09.05	493.0 MB
20.1KK MIX - UPDATE 09.04	628.0 MB
14.16KK MIX - UPDATE 09.03	447.1 MB
9.59KK MIX - UPDATE 09.02	302.3 MB
12.88KK MIX - UPDATE 09.01	401.2 MB
10.73KK MIX - UPDATE 08.31	339.6 MB

Figure 4.1.3. The amount of data for sale publicly on Cyberspace. (Source: Telegram)

Processing Data After the Transaction

VIETTEL THREAT INTELLIGENCE discovered many documents at the Dark Web instructing to check information such as handling cookies or balances in stolen e-wallets after the transaction. When these documents are released to the public, victims can be put at extremely serious risk.



How to check logs?

> *What will we learn after reading?*

After reading, you will be able to put filters on the mail, check the wallets folder, analyze the discord tokens and we will pay off the logs!

- **Any qt**

Simply put, qt is wallet.dat in your log. It could be MinexCoin, Dogecoin, Bitcoin, Litecoin, etc. In order to find out the balance, you need to open wallet.dat through a regular notepad. Press Ctrl + F, enter "name" and press Enter.

```
<ML<ф}OrxbH    є3¤UшџrK,Њо„&$є6   . Ф-
 pool       ,   юеЭZ
-ПsHsvл¶E'ы^rЎIav!'yЇ€|кш»p   . Ф- юеЭZ
         ч Џ0ґУ  ў'94*[
 Џ0ґУ  хJ5ч   (   MyMinexBank   (
 MyMinexBank(
name"XXs3Mduh8kxPbgqFQKwGWYM9YjH5R6SYbKч Џ0ґУ  хJ5џЬ€т6ад<-юб qPY'ь_07«4ЋК ґ_0ґ
```

Figure 4.1.4. Detailed instructions on how to extract data from raw data (Source: VIETTEL THREAT INTELLIGENCE)

SECTION

03

Data Analysis

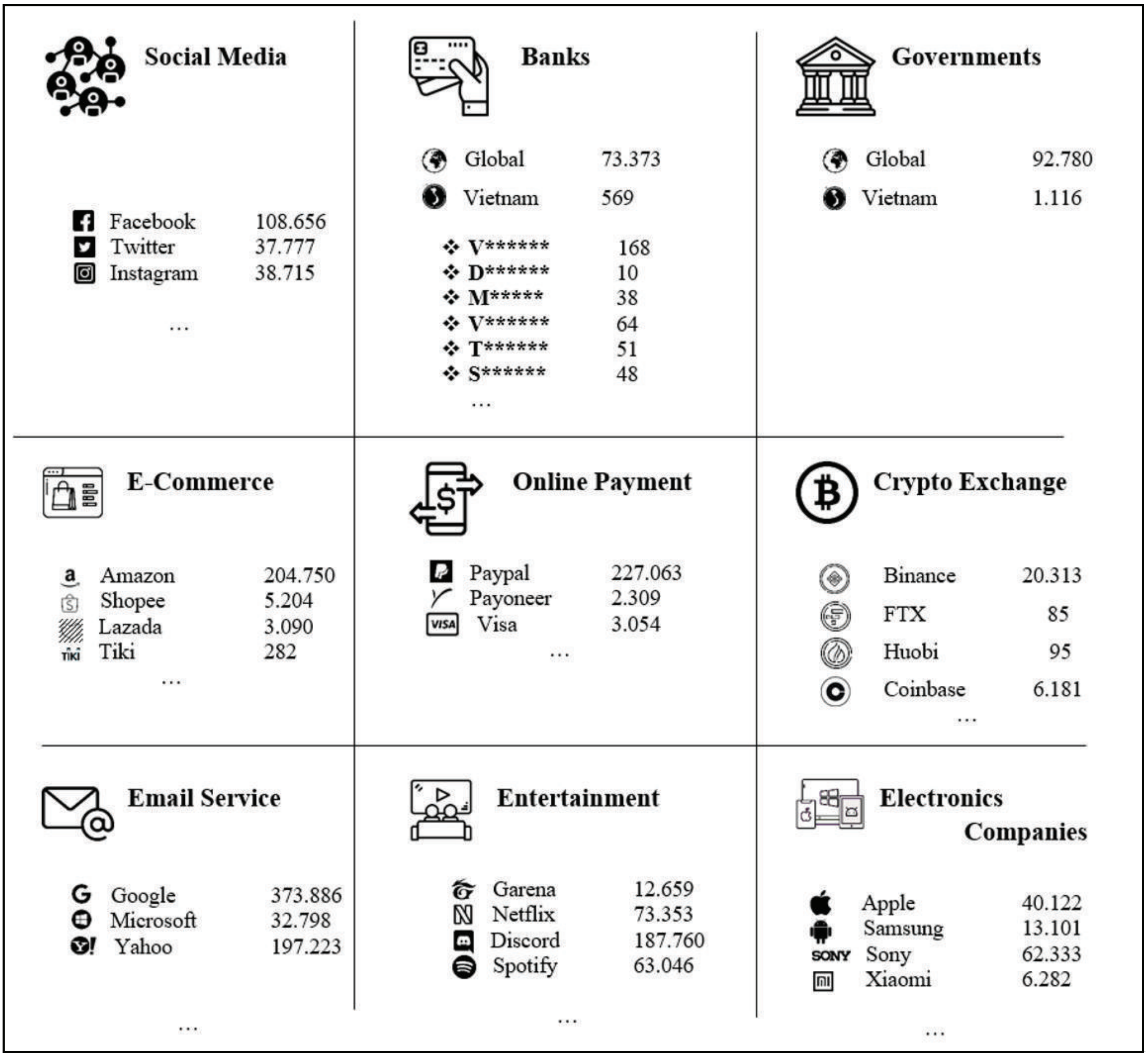
To have a better understanding about the threat of Redline Malware impacting on users, VIETTEL THREAT INTELLIGENCE will analyze the collected data set from the last two months on Deep/Dark Web:

Country:

- 188/206 countries are affected
- Over 40,432 devices are infected

Data

- Login accounts 3,450.958
- Cookies: 17,441,456
- Files: 30,140



Social Media

Facebook	108.656
Twitter	37.777
Instagram	38.715

…

Banks

Global	73.373
Vietnam	569
❖ V******	168
❖ D******	10
❖ M*****	38
❖ V******	64
❖ T******	51
❖ S******	48

…

Governments

Global	92.780
Vietnam	1.116

E-Commerce

Amazon	204.750
Shopee	5.204
Lazada	3.090
Tiki	282

…

Online Payment

Paypal	227.063
Payoneer	2.309
Visa	3.054

…

Crypto Exchange

Binance	20.313
FTX	85
Huobi	95
Coinbase	6.181

…

Email Service

Google	373.886
Microsoft	32.798
Yahoo	197.223

…

Entertainment

Garena	12.659
Netflix	73.353
Discord	187.760
Spotify	63.046

…

Electronics Companies

Apple	40.122
Samsung	13.101
Sony	62.333
Xiaomi	6.282

…

The leaked data, collected by VIETTEL THREAT INTELLIGENCE, has alerted customers using Threat Intelligence Service. For detailed information, please visit Viettel Threat Intelligence’s homepage: cyberintel.io

Identification/Malware Infrastructure

1. Review folders or processes that have paths to the following directories:

2. Review events to investigate the behaviors of malwares:

Startup folder:

C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\IntelRapid.lnk

Task schedule:

C:\Users\<user>\AppData\Roaming\services64.exe

C:\Program Files\PowerControl\PowerControl_Svc.exe

%temp%\dQmOBORtOOmVIQYxa\XOLcDlHHxqomGEP\DGsBsDU.exe

c:\users\<user>\appdata\roaming\**.exe

Insert root certificate:

• Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E

• HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\E1C950E6EF22F84C5645728B922060D7D5A7A3E8

• HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\6252DC40F71143A22FDE9EF7348E064251B18118

•HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\CABD2A79A1076A31F21D253635CB039D4329A5E8

Turn off Windows defender:

- HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS DEFENDER\REAL-TIME PROTECTION
- After executing, a log file should be created at:
- C:\Users\<user>\AppData\Local\Microsoft\CLR_v4.0
- C:\Users\<user>\AppData\Local\Microsoft\CLR_v4.0_32

Create a new folder and drop malicious files into it:

- C:\Users\<user>\AppData\Local\Temp\7zS88D38CD4
- C:\Users\<user>\AppData\Local\Temp\7zS368A.tmp
- C:\Users\<user>\AppData\Local\Temp\bengal
- C:\Users\<user>\AppData\Local\Temp\cghjgasaaz99
- C:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files\-Content.IE5\HTA0MJH8
- C:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files\-Content.IE5\ULMDHA1D
- C:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files\-Content.IE5\7ZCR29RO
- C:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files\-Content.IE5\4RT59HOG
- C:\Users\<user>\AppData\Local\Temp\{kGhO-bmno0-as2g-9etC8}
- C:\Program Files (x86)\Company\NewProduct

Review dropped files at folder %TEMP% and %APPDATA% (Possibly with fake icons of reputable applications)

List of the several sites that host malwares based on the article:

- Omnisphere 2.6 Crack + Keygen With Torrent For Mac [VST] (crackshops.com)
- YouTube By Click 2.3.12 Crack + Activation Code Free Download! (optimal-cracks.com)
- Voicemod Pro 2.16.0.1 Crack With License Key (2021) Latest Download (mix-cracked.net)
- Voicemod Pro 2.6.0.7 Crack With License Key [Latest] (freedownloadfiles.org)
- Voicemod Pro 2.17.0.2 Crack + License Code [32bit/64bit] Download (pcsoftstore.com)
- VoiceMod Pro 2.15 Crack + License Key With Torrent [Free Voices] (crack-shops.com)

- Voicemod Pro 2.14.0.10 Crack With License Key Full Download (zeemalcrack.com)
- Voicemod Pro 2.16.0.1 Crack With License Key Free Download 2021 (crackspro.co)
- Voicemod Pro 2.17.0.2 Crack + License Key [MAC] Download (zrootcracked.com)
- Voicemod Pro 2.16.0.1 Crack License Key (32/64-Bit) Free Download 2021 (scracked.com)
- Voicemod Pro 2.17 Crack + License Key (2021) Free Download (crackkits.com)
- Voicemod Pro 2.11.0.5 Crack + License Key [Latest] 2021 Free (ezcrack.info)

List of Domains that redirects to IP spreading Redline Malware:

- hokumala[.]xyz
- zencomo[.]xyz
- lasbella[.]xyz
- nahrerhost[.]xyz

Example:

- https://hokumala[.]xyz/?s=47
- http://zencomo[.]xyz/?s=298

List of IPs spreading Redline Malwares (Not C&C):

- 52.26.28[.]19
- 52.13.172[.]43
- 34.209.155[.]151
- 34.209.250[.]165
- 34.214.252[.]214
- 52.41.248[.]44
- 54.213.232[.]221
- 13.56.165[.]39
- 35.160.145[.]230
- 34.217.79[.]62
- 3.101.85[.]107
- 54.71.47[.]168
- 34.220.236[.]233

IOCs

Due to the nature of Redline, IOCs will vary from model to model:

Sample of C&C included in the article:

IOCs:	Description	Type
FC0CE6A2471E5145519920CDCFCC24C09F1A0D3449C235FA71DCD27FAC9C5F60	SHA256	Hash
8018D2E6459F8CFFA3383B5E9599C74DFEDAEF7D6BB37247740350B70861A317	SHA256	Hash
95.181.152[.]47	IP	C&C

Yara Rule

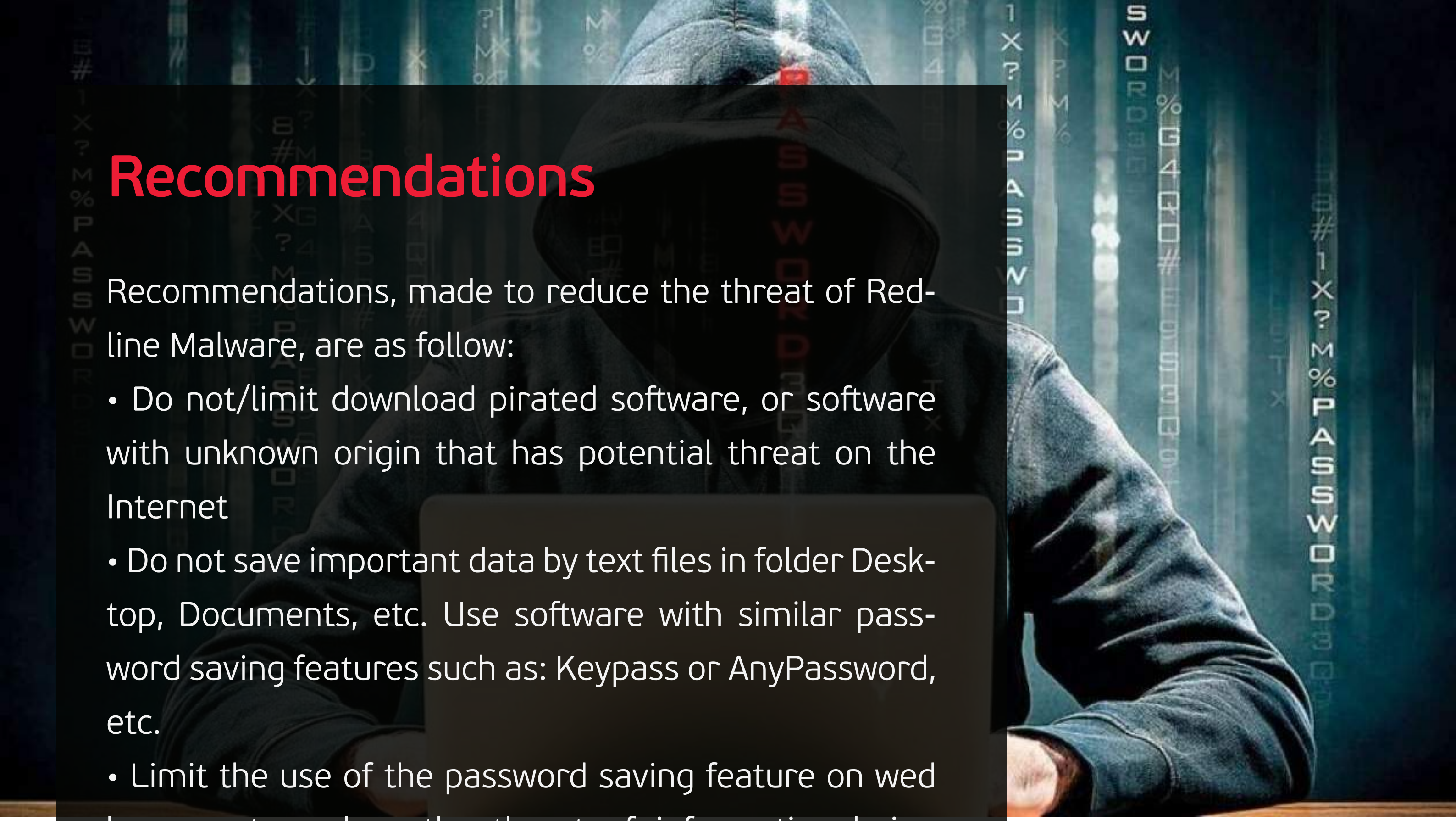
Update Yara Rule for solution based on the following rules:

Malwares have been obfuscated:

```
import "pe"
import "time"
rule Mal_InfoStealer_Win32_RedLine_Obfuscated_2021
{
    meta:
        description = "Detects Obfuscated RedLine Infostealer Executables (.NET)"
        date = "2021-07"
    strings:
        // The file name appears to use a ramdom word and never contains numbers
        $x1 = /[a-zA-z]+.exe/
        $x2 = "Signature"
        $x3 = "callback"
        $x4 = "Protect"
        $x5 = "Replace"
        $x6 = "Sleep"
        $x7 = "GetProcAddress"
        $x8 = "LoadLibrary"
        $x9 = "FreeLibrary"
        $x10 = "FromBase64String"
    condition:
        //PE File
        uint16(0) == 0x5a4d and
        // Must have exactly 3 sections
        pe.number_of_sections == 3 and
        // DotNet Imports
        pe.imports("mscoree.dll", "_CorExeMain") and
        // DotNet Imphash
        pe.imphash() == "f34d5f2d4577ed6d9ceec516c1f5a744" and
        // Timestamp at least 20 years in the future (Unix Time)
        pe.timestamp > time.now() + (31556926*20) and
        // File Version 0.0.0.0
        pe.version_info["FileVersion"] == "0.0.0.0" and
        //All Strings
        all of ($x*) and
}
```

Malwares have not been obfuscated (Un-Obfuscate)

```
import "pe"
import "time"
rule Mal_InfoStealer_Win32_RedLine_Unobfuscated_2021
{
    meta:
        description = "Detects Unobfuscated RedLine Infostealer Executables (.NET)"
        date = "2021-07"
    strings:
        $x1 = "Account"
        $x2 = "AllWalletsRule"
        $x3 = "Autofill"
        $x4 = "BrowserExtensionsRule"
        $x5 = "BrowserVersion"
        $x6 = "CommandLineUpdate”
        $x7 = "DiscordRule"
        $x8 = "DownloadAndExecuteUpdate"
        $x9 = "FileCopier"
        $x10 = "FileScanner"
        $x11 = "Gecko"
        $x12 = "GeoInfo"
        $x13 = "RecoursiveFileGrabber"
        $x14 = "ResultFactory"
        $x15 = "ScannedBrowser"
        $x16 = "ScannedCookie"
        $x17 = "ScannedFile"
        $x18 = "StringDecrypt"
        $x19 = "SystemInfoHelper"
        $x20 = "UpdateTask"
condition:
        //PE File
        uint16(0) == 0x5a4d and
        // DotNet Imports
        pe.imports("mscoree.dll", "_CorExeMain") and
        // DotNet Imphash
        pe.imphash() == "f34d5f2d4577ed6d9ceec516c1f5a744" and
        //All Strings
        all of ($x*)
}
```



Recommendations

Recommendations, made to reduce the threat of Redline Malware, are as follow:

- Do not/limit download pirated software, or software with unknown origin that has potential threat on the Internet
- Do not save important data by text files in folder Desktop, Documents, etc. Use software with similar password saving features such as: Keypass or AnyPassword, etc.
- Limit the use of the password saving feature on wed browser to reduce the threat of information being leaked. Change your password regularly to prevent mishaps. Enable multi-factor authentication for login accounts.
- Limit reuse passwords on different platforms. Attackers could easily scan for other services used by other users and attack Brute Force with leaked passwords.

In the event of (or suspect of) infected with malwares:

- Update and install the latest definition updates for security (Ex: Antivirus, EDR, etc.)
- Base on the sign to recognize malwares to spread and search for infected devices

Appendix

Appendix 1: Example for leaked file:

1. File name: UserInformation.txt

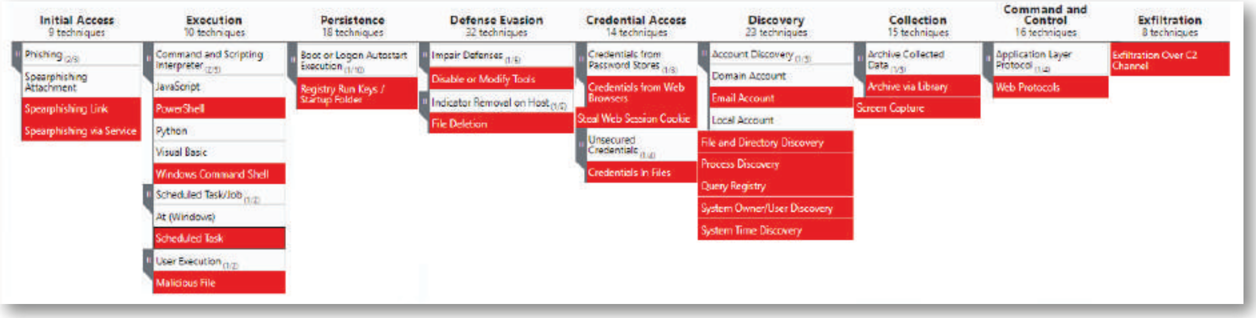
```
******************************************** ***
*   Telegram: https://t.me/REDLINESUPPORT    *
***********************************************
```

Build ID: @radviq IP: 14.226.***.24 FileLocation: C:\Users\**** UserName: Lu Thien Country: VN Zip Code: UNKNOWN Location: UNKNOWN HWID: E1255EB800175****7D79590EF748 OEM ID: 76a910f0-****-****-bf23-79f916c40356 Current Language: English (United States)	ScreenSize: 1920x1080 TimeZone: (UTC+07:00) Bangkok, Hanoi, Jakarta Operation System: Windows 10 Enterprise x64 UAC: AllowAll Process Elevation: False Log date: 7/24/2021 10:04:23 AM Available KeyboardLayouts: English (United States) Vietnamese (Vietnam)

2. File name: Passwords.txt

URL: https://idmsa.apple.com/apple-auth/auth/ Username: luhthien***@icloud.com Password: *********@47 Application: Google_[Chrome]_Default	URL: https://id.cisco.com/signin Username: khoa*****@gmail.com Password: *******00 Application: Google_[Chrome]_Default

Appendix 2: MITRE ATT&CK



Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Defense Evasion 32 techniques	Credential Access 14 techniques	Discovery 23 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques
Phishing (2/3)	Command and Scripting Interpreter (2/5)	Boot or Logon Autostart Execution (1/10)	Impair Defenses (1/6)	Credentials from Password Stores (1/3)	Account Discovery (1/3)	Archive Collected Data (1/3)	Application Layer Protocol (1/4)	Exfiltration Over C2 Channel
Spearphishing Attachment	JavaScript	Registry Run Keys / Startup Folder	Disable or Modify Tools	Credentials from Web Browsers	Domain Account	Archive via Library	Web Protocols	
Spearphishing Link	PowerShell		Indicator Removal on Host (1/6)	Steal Web Session Cookie	Email Account	Screen Capture		
Spearphishing via Service	Python		File Deletion	Unsecured Credentials (1/4)	Local Account			
	Visual Basic			Credentials In Files	File and Directory Discovery			
	Windows Command Shell				Process Discovery			
	Scheduled Task/Job (1/2)				Query Registry			
	At (Windows)				System Owner/User Discovery			
	Scheduled Task				System Time Discovery			
	User Execution (1/2)							
	Malicious File							

Figure 5.1. Techniques used in the article

VIETTEL THREAT INTELLIGENCE

Automated gather, detect and analyze cyber threat intelligence

📍 41st Floor, Keangnam Landmark 72, Pham Hung Rd., Nam Tu Liem Dist., Hanoi, Vietnam.

🌐 https://cyberintel.io

✉ cyberthreat@viettel.com.vn

☎ (+84) 971 360 360