MALWARE/
TOOLS
PROFILE

Recorded Future®

By Insikt Group®

October 14, 2021

RedLine Stealer Is Key Source of Identity Data for Criminal Shops

Recorded Future®

Insikt Group used the Recorded Future® Platform, dark web analysis, and proprietary and open sources to assess the RedLine infostealer malware and its use as a source of stolen information for Russian Market and Amigos Market. This report will interest threat intelligence analysts, security operations centers (SOC), and incident response teams who defend against data theft attacks.

Note: This report was updated on October 19, 2021 with additional insight on the relationship between Russian Market and Amigos Market provided by contacts at the KELA Group. We thank the KELA team for their contributions to this research.

Executive Summary

RedLine Stealer is an infostealer malware marketed and sold on several online criminal forums by the Russian-speaking cybercriminal "REDGlade", also known as "Glade". RedLine Stealer is used to steal credentials and other information such as cryptocurrency wallet files that are easily monetized by direct use or sale to other criminals. The sale of this stolen data is often conducted through underground markets that provide one-stop shopping for criminals involved in identity theft or who simply wish to cash out what they can based on the stolen credentials available.

The infostealer has seen broad distribution since its initial release in early 2020. Insikt Group identified and analyzed multiple samples of RedLine Stealer, along with a cracked builder for the malware, and concluded that the advertised capabilities of the malware are accurate.

RedLine Stealer has been actively in use since the first quarter of 2020 but has become more widely adopted in 2021. The infostealer is competently written and maintained, and due to the variety of threat actors operating it, RedLine Stealer can be associated with a wide array of tactics, techniques, and procedures (TTPs). However, despite this diversity of TTPs, Recorded Future was able to create network and endpoint signatures for defenders to detect the use of RedLine Stealer.

Key Judgments

- RedLine Stealer malware steals information that can be easily monetized, including usernames, passwords, cookies, payment card information, and cryptocurrency wallet information.
- The infostealer is marketed by the threat actor REDGlade on Telegram and several criminal forums; a cracked version has also become available.
- RedLine Stealer has been widely adopted by criminals over the past year.
- RedLine Stealer is a primary source of the stolen information sold on multiple criminal shops, including Amigos Market and Russian Market.
- The volume of advertisements for stolen log information harvested by RedLine Stealer has increased over the past year, aligning with the increased attention RedLine Stealer has gotten across entry-level and top-tier criminal sources.

Background

RedLine Stealer is sold by the actor REDGlade on various forums and on Telegram beginning in February 2020. The infostealer is offered as malware-as-a-service with a subscription of varying lengths available.

Online discussions, reporting, and activities involving RedLine Stealer increased in March 2021 and have since been relatively constant. This increase is also a reflection of reporting and sharing of information about RedLine Stealer as it has become more broadly recognized as a threat by the security community.

RedLine Stealer collects usernames, passwords, cookies, saved credentials, and credit card information from browsers. It also collects data from FTP clients and IM clients. The malware also provides file collection functionality, and the user can specify collection from certain file folders to gather files from cryptocurrency cold wallets and other file locations.

RedLine Stealer is also capable of performing basic download and execute functions. The malware can download files from specified links, run executable programs, and open links via a browser. It is therefore capable of loading additional malware onto the victim system. The RedLine Stealer malware can be used purely for credential and data theft or as a loader and installer for other malware. Although in most RedLine Stealer incidents that have been observed the malware was used primarily as an infostealer, incident responders discovering a system with RedLine Stealer installed should presume that other malware may also be installed on the system.

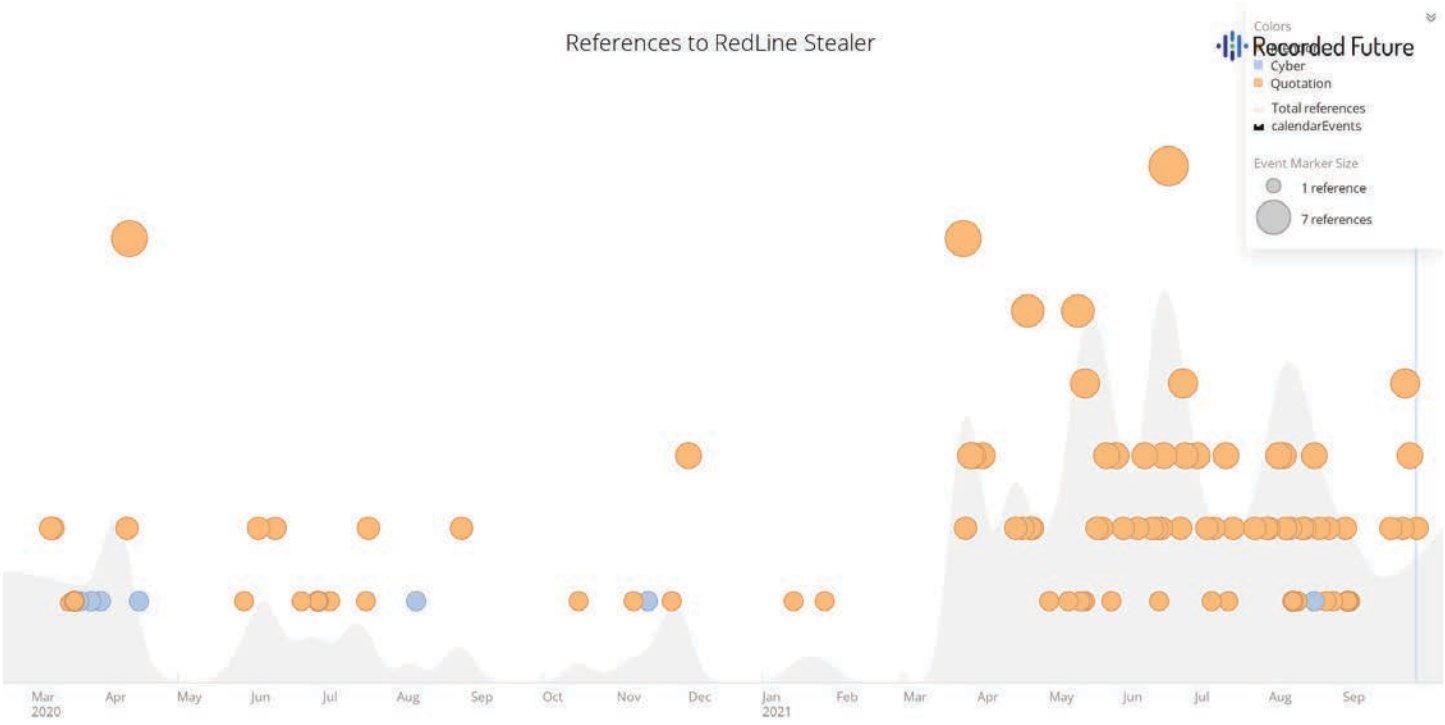

Figure 1: Timeline of RedLine Stealer events 2020 to 2021 (Source: Recorded Future)

Methods of Distribution

RedLine Stealer is commonly distributed by phishing email, as well as messaging on social media. The phishing email lures are often topical, concerning current events such as COVID-19 information. RedLine Stealer has also been found disguised as legitimate applications, including as an installer for Telegram, and has been installed via SmokeLoader masquerading as privacy software. Legitimate websites may be used as part of the infection chain for RedLine Stealer distribution. As a commodity malware that has been available since early 2020, and for which a cracked version has been released, the malware is used by disparate operators; thus, initial RedLine Stealer installation vectors may include many different methods and techniques.

Threat Analysis

RedLine Stealer is one of the most notorious infostealer brands being sold on the dark web for the last year and a half. The stealer is associated with several threat actors primarily operating on low-tier Russian-speaking forums and Telegram channels.

RedLine Stealer was first advertised on February 18, 2020, on the low-tier Best Hack Forum (BHF) by the threat actor REDGlade. Similar advertisements were observed several days later on other Russian-language low-tier forums WWH Club by the threat actor Glade. All advertisements listed the Telegram channel @REDLINESUPPORT as a primary point of contact for the interested parties, a contact which is still active at the time of this publication. REDGlade also originally registered on Best Hack Forum on February 13, 2020, and has a positive reputation among other cybercriminals on the forum. Analysis of the content published by REDGlade indicates that they are primarily involved in the sales and support of RedLine Stealer. REDGlade was also active on other Russian-speaking dark web forums posting about RedLine Stealer. The threat actor Glade registered on WWH Club forum on February 13, 2020, the same date REDGlade registered on BHF. Considering identical product listings, dates of registration, and the Telegram handle @REDLINESUPPORT, Insikt Group believes that the usernames REDGlade and Glade are very likely operated by the same individual or threat actor group.

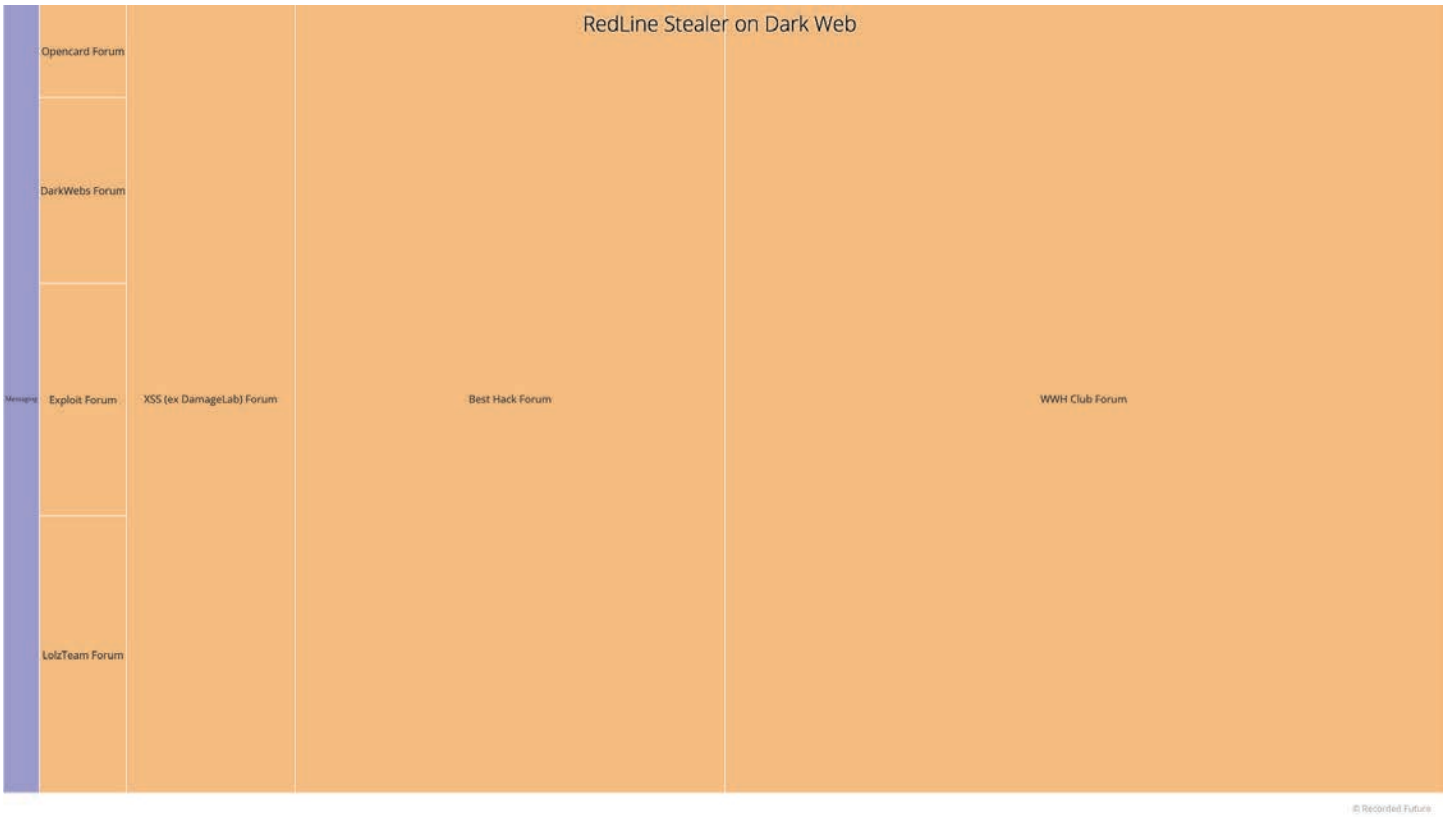

Figure 2: List of sources with RedLine Stealer advertisements (Source: Recorded Future)

Examination of dark web discussions indicates that the primary sources supporting the sale of RedLine Stealer are BHF and WWH Club forums. The seller encourages threat actors to use personal messages and forum escrow for conducting purchases and provides a 20% discount for all types of goods and services that meet the requirements. Open-source references toward the Telegram handle @REDLINESUPPORT indicate that it was allegedly registered in Denmark.

According to the threat actor, RedLine Stealer is an infostealer with an admin panel developed in C# and steals login data from multiple sources, including:

- All Chromium and Mozilla Gecko-based web browsers
- Cookies
- Account credentials
- Payment card data
- Autofill forms
- FTP and Instant messenger client data

RedLine Stealer is advertised as having the following technical functionality:

- A customizable file-grabber
- Filters for country and operating system (capable of setting up a blocklist of countries where the build will not work)
- Create and edit tasks
- Panel configuration that enables actors to remove duplicate logs
- Collect information about the victim's system based on the following indicators. Information can be viewed directly from the panel without opening the log:
    - IP address
    - Country
    - City
    - Current username
    - HWID
    - Keyboard layouts
    - Screenshot
    - Screen resolution
    - Operating system

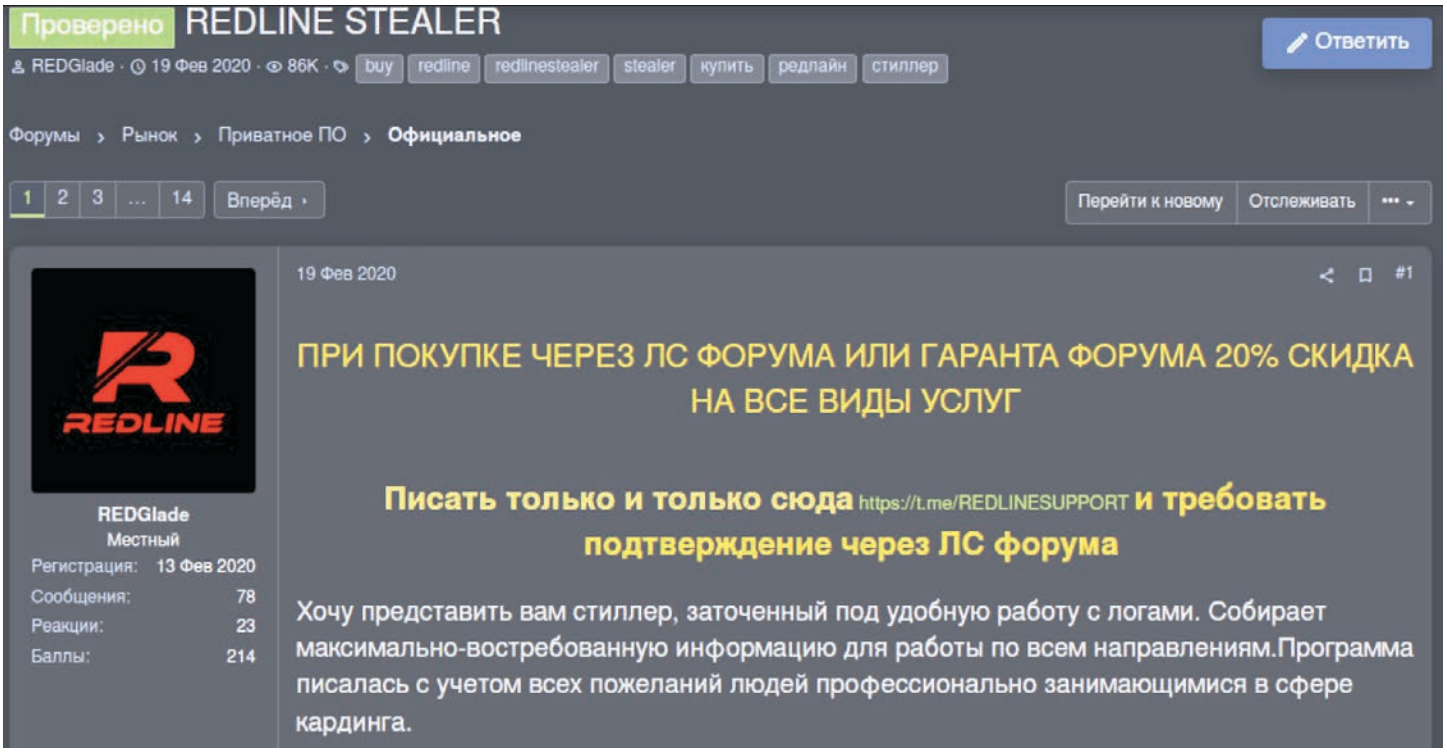

Figure 3: RedLine Stealer sales thread on the dark web (Source: BHF Forum)

- UAC settings
- Types of privileges
- User-Agent
- Information about the components of the infected machine (video cards and processors)
- Installed antiviruses

Initial advertisements for RedLine Stealer detailed several secondary tasks or functions it supports, such as:

- RunPE — injection of a 32-bit file downloaded from a direct link into another user-specified file
- DownloadAndEx — download a file via a direct link to the specified path from subsequent launch
- OpenLink — open the link in the default browser
- Downloading files via a direct link to a specified path

"Cracked" Versions of RedLine Stealer

Threat actors continue to distribute "cracked" versions of RedLine Stealer in 2021. The distribution of cracked versions of RedLine Stealer is not a new phenomenon and has been reported as far back as 2020. While the validity of these cracked versions of the stealer from over a year ago is less certain, actors in 2021 attempting to gain access to the malware are more likely to rely on recent iterations of RedLine Stealer that were reportedly leaked across multiple sources within the past two months.

- On August 26, 2021, the threat actor "alfy1331" publicly shared on XSS Forum a cracked version of RedLine Stealer v. 20.2. According to the threat actor, the infostealer was cracked by another threat actor with the Telegram account @kurome_sup. A search for this Telegram handle on dark web sources found the threat actor "Kurome", a member of the low-tier Russian-speaking forum, who uses it as a primary point of contact. This upload likely had a cascading effect as other forums, including Best Hack Forum, where REDGlade initially operated, had members sharing cracked versions of RedLine Stealer with the same version as the sample uploaded to XSS Forum: Version 20.2.

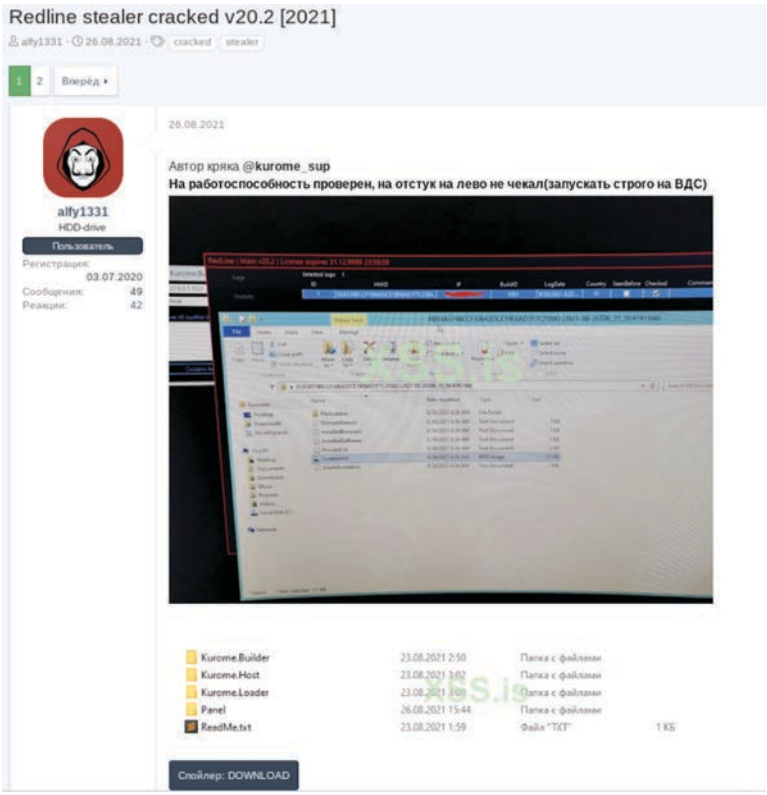

Figure 4: alfy1331 shared cracked version of RedLine Stealer v.20.2 builder (Source: XSS Forum)

As of this writing, the latest version of RedLine Stealer, version 21.2, was released on September 3, 2021. alfy1331 stated that the admin panel of the malware was updated and old RedLine Stealer builds would not work in the updated admin panel.

According to REDGLade, there are 2 types of subscription licenses for the latest malware variants:

- "PRO", a lifetime license available for $800 with 3 months of free crypt service and antivirus scan check
- "Lite", a 1-month license with 1 month of free crypt service available for $150

REDGLade previously provided discounts to buyers, and the subscription costs have varied since the product's launch in February 2020. RedLine Stealer is advertised as accepting payments in the following cryptocurrencies: Bitcoin, Litecoin, Ethereum, Monero, and Tether. Additionally, RedLine Stealer's Telegram support channel has continued to provide updates regarding new features available to Lite and PRO users throughout 2021. In February 2021, the channel stated that future builds would be signed by default with Code Signing digital certificates.

Since its initial appearance, RedLine Stealer has continued to be adopted by top-tier cybercriminals. A thread launched on June 27, 2021, on the top-tier Russian-speaking forum Exploit called "Raccoon VS Redline VS Smoke" detailed how cybercriminals discussed the positives and negatives of various infostealers that currently operate on the dark web market. Participants stated that RedLine Stealer has good technical functionality and provides compromised credentials and other relevant data as stated in the specs. Also, they stated that one of the primary advantages of RedLine Stealer is its crypt service, "Spectrum Crypt Service" @spectrcrypt_bot. For example, the threat actor "_pra9ma" added that its functionality is similar to that of AZORult stealer.

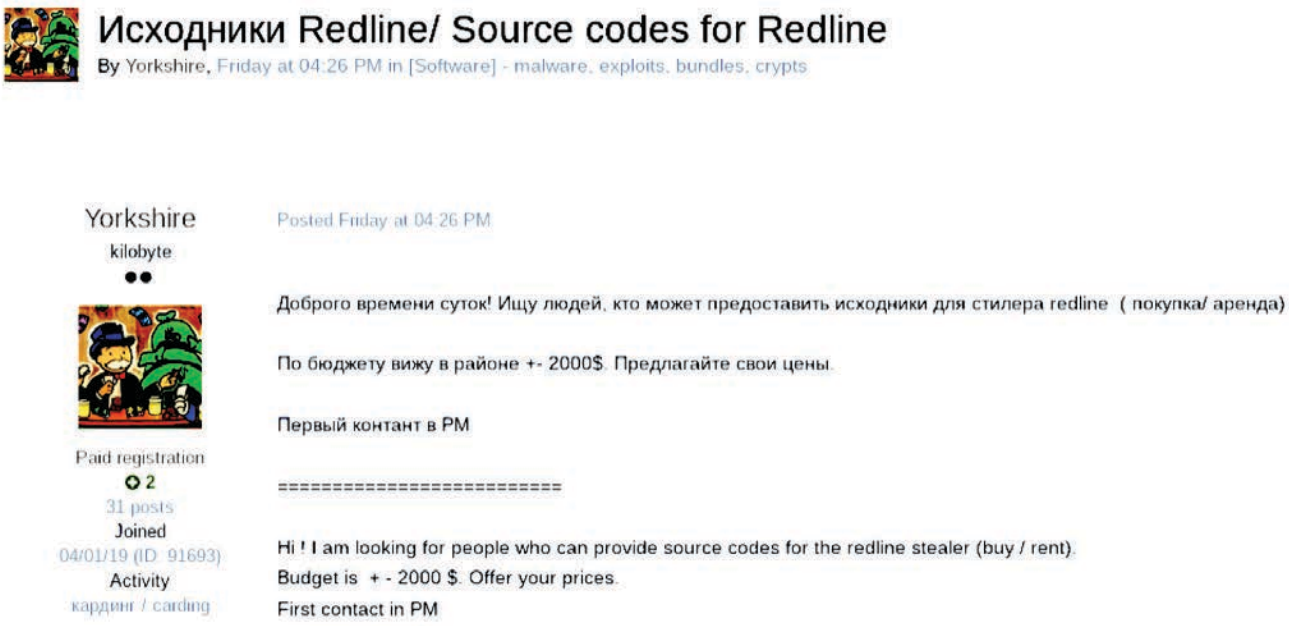

Figure 5: Yorkshire looking for RedLine Stealer source code (Source: Exploit Forum)

Given its positive feedback among cybercriminals, the source code of RedLine Stealer is sought after by many threat actors, who are ready to pay a price significantly higher than its lifetime license cost. On September 17, 2021, the threat actor "Yorkshire" on Exploit Forum was going to buy RedLine Stealer's source code for $2,000.

Role of RedL ine Stealer in Underground Shops

Analysis of the dark web shops involved in the sales of the stolen account credentials indicates that RedLine Stealer continues to supply several prominent underground shops, including Russian Market and Amigos Market, with the largest number of compromised accounts as of this writing in comparison to 4 to 5 other stealers often leveraged by its administrators. Typically, the prices for RedLine Stealer-compromised accounts are higher than other infostealers. Recently compromised accounts by RedLine Stealer cost $10.

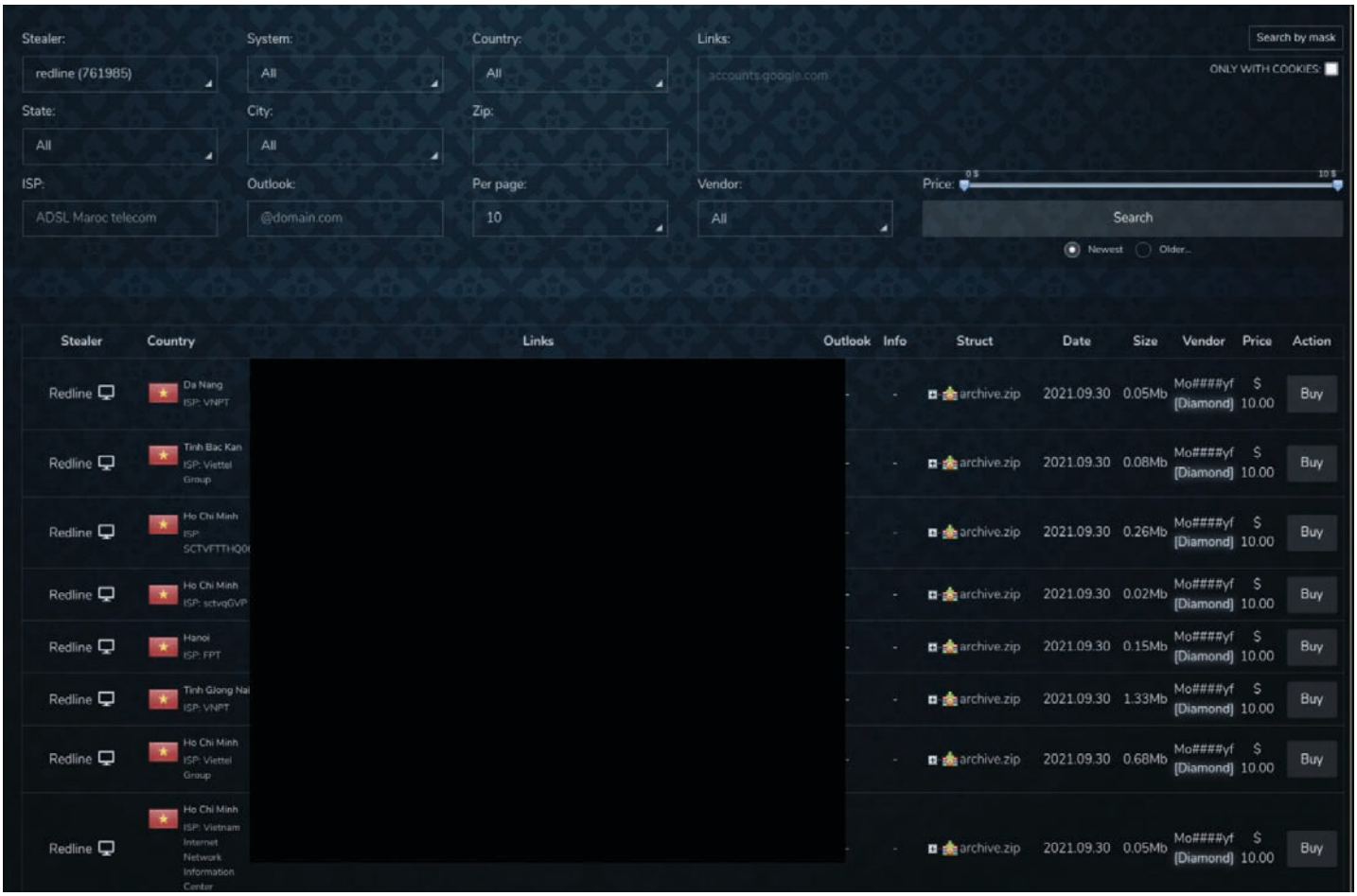

Figure 6: RedLine Stealer listings for sale on the dark web (Source: Russian Market)

Stealer	Russian Market Listings	Amigos Market Listings
RedLine	**761,985**	**765,217**
Vidar	645,078	645,078
Taurus	95,417	95,417
Racoon	85,951	87,720
AZORult	48,663	48,663
Ficker	Does not supply credentials	1,561

Table 1: Compromised account listings by infostealer brand on Amigos Market and Russian Market (Source: Recorded Future Data)

Despite the volume of RedLine Stealer infections appearing across Russian Market and Amigos Market listings, both Amigos Market and Russian Market were identified by Insikt Group (June 2021) posting identical listings regularly that contained the same timestamps, infostealer variants used, geographical locations of affected machines, and ISPs. This also means that the figures in Table 1, above, tabulating the true number of listings across the 2 shops is inflated by nearly double, as there are a large number of listings on both shops which are identical.

KELA Group shared research with Insikt Group to further corroborate the relationship between the 2 shops. Their research highlights unique identifiers, viewable by inspecting the HTML page content, that are identical between Russian Market and Amigos Market. Bot data being advertised on Amigos Market that has been scraped from Russian Market uses the identifier that was assigned to this data set on Russian Market and prepends it with the letter "v". In some instances, the same stolen data is re-listed on Amigos Market for a 50% markup over its price on Russian Market. KELA's analysis shows that of the 1.5 million bots being advertised on Amigos Market, the number of identifiers that do not have the prepended "v" designation is a small fraction of what is being advertised overall, suggesting a large portion of Amigos Market is almost entirely a mirror of Russian Market.

Technical Analysis

Insikt Group analyzed the 3 main RedLine Stealer components: the legitimate admin panel, which contains an integrated builder that requires purchasing the software to use, the cracked version, which allows free access to the admin panel but does not allow builds to be created from within the panel, and a cracked builder that generates RedLine Stealer builds outside of the admin panel without needing to pay for the software.

RedLine Stealer Admin Panel Analysis

On August 26th, 2021, alfy1331 shared a cracked version of the admin panel used to build RedLine Stealer and explore data stolen from infected machines on XSS Forum, giving other threat actors free access to RedLine Stealer. The cracked version shared on XSS is version 20.2; as of this writing the official RedLine Stealer is up to version 21.2. Insikt Group acquired this cracked version for in-depth analysis.

There are only 4 steps involved to configure the cracked version. These steps can be completed in under 10 minutes by an experienced threat actor. This includes running 2 executables as an administrative user, logging in to the panel using the supplied username ("ims0rry") and password ("racoon"), and filling out a few fields in a panel that generates a functioning build of RedLine Stealer. The cracked distribution also contains an FAQ, a 12-page PDF included when RedLine Stealer is purchased from the original developer. The FAQ has detailed installation, building, crypting, and general configuration and customization instructions, making RedLine Stealer more accessible and easy to use for any threat actor on the dark web.

Before generating a build for RedLine Stealer, threat actors can customize the build settings using the panel seen in Figure 7 below. Threat actors can choose to collect data from browsers, VPN clients, Steam, Telegram, and more. They can also specify which files they want to retrieve, including the use of wildcard filtering, and also which domains to filter for, including sensitive passwords and cookies.

The cracked version of RedLine Stealer also includes a standalone builder configured with the default parameters seen above. Threat actors can use the cracked standalone builder (Kurome.Builder) to specify their server IP address, port, build ID, and error message, as seen in Figure 8 below. Insikt Group developed a script to extract the configuration information from an executable that was built using the cracked builder. The script and extracted configuration details are available to Recorded Future clients.

Insikt Group used the cracked builder to create a malware sample that exfiltrated the collected data to an admin panel running in our lab. This gave us access to the data exfiltrated from the infostealer and allowed us to interact with the data using the admin panel. The panel view labeled "Logs" contains a list of machines infected with RedLine Stealer that have finished exfiltrating stolen data. This can be seen below in Figure 9, along with the options available to the threat actor to explore the stolen data.

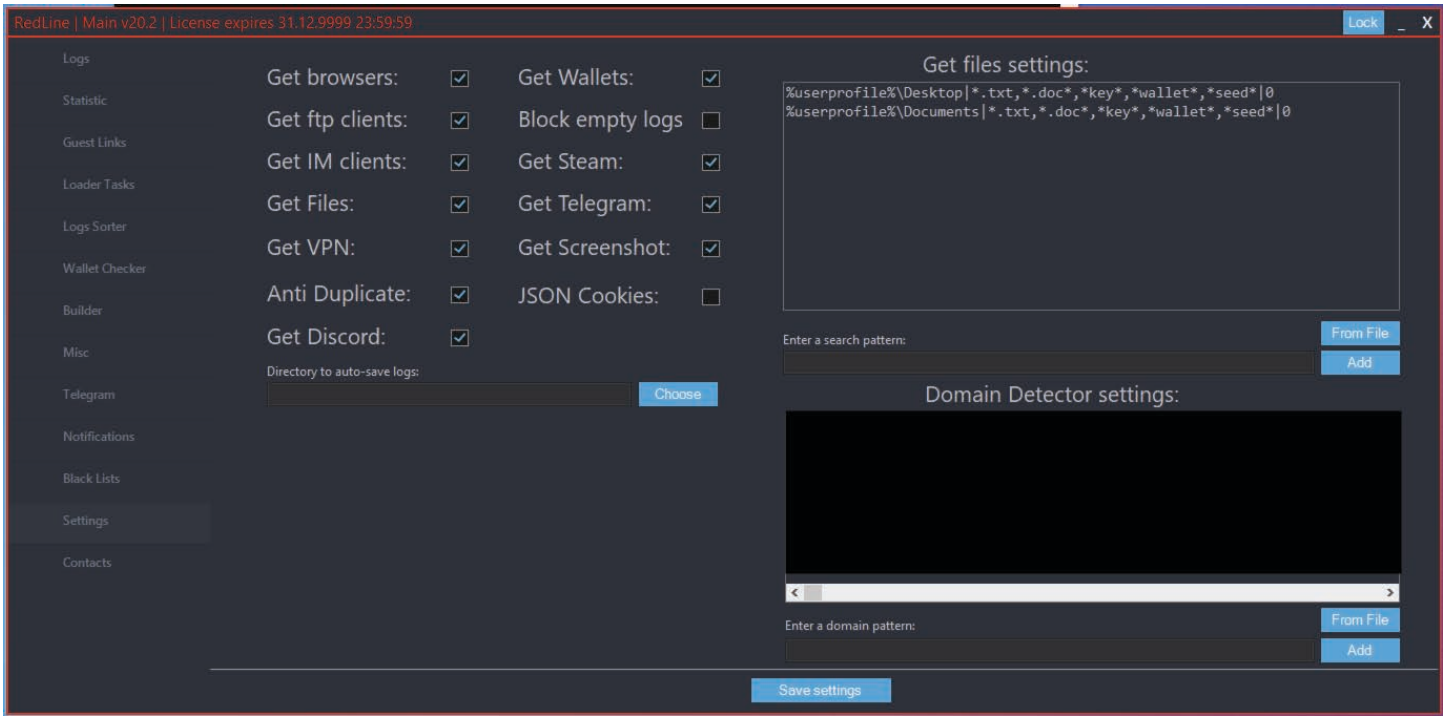

Figure 7: RedLine Stealer build settings panel (Source: Recorded Future)

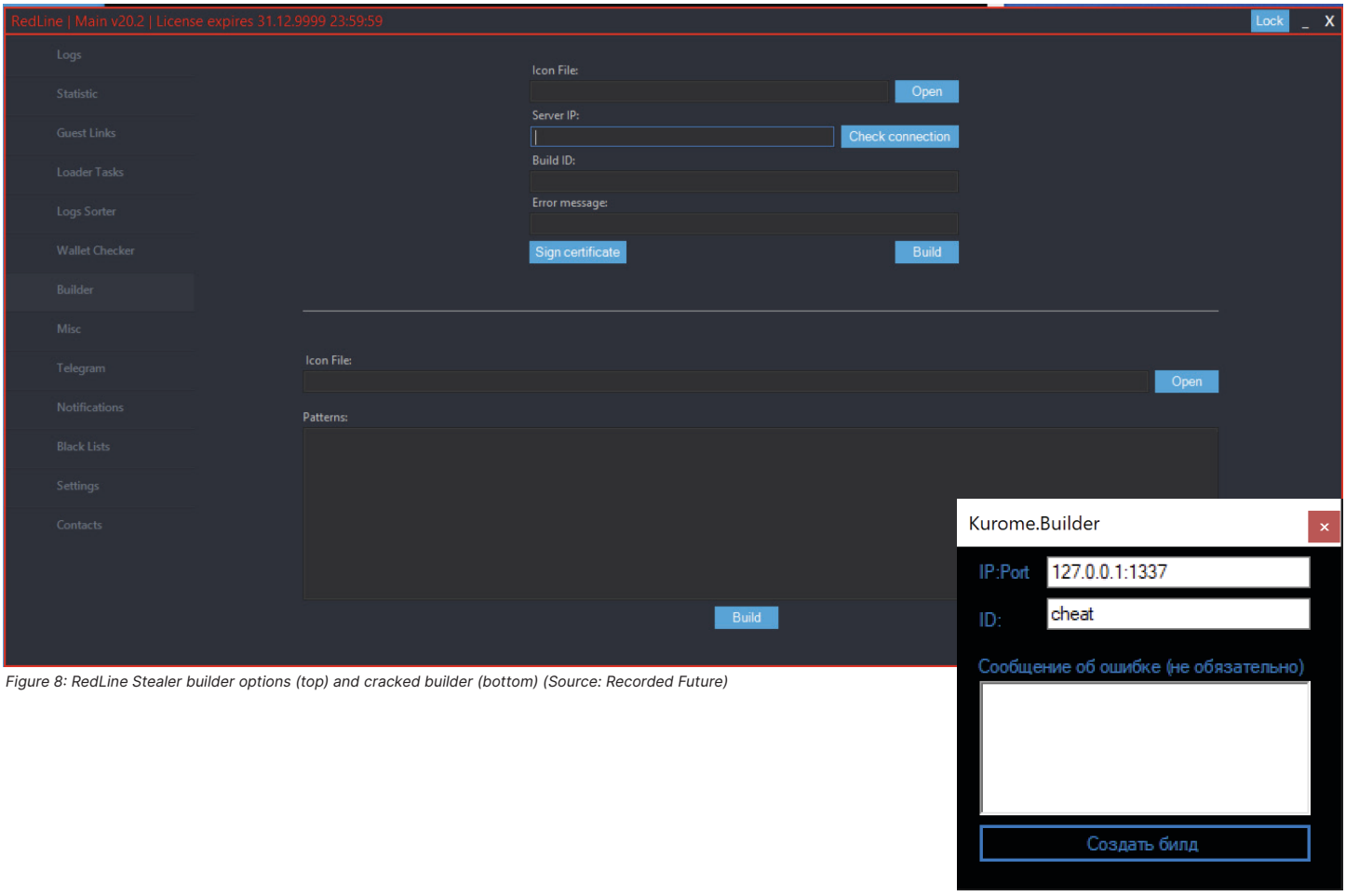

Figure 8: RedLine Stealer builder options (top) and cracked builder (bottom) (Source: Recorded Future)

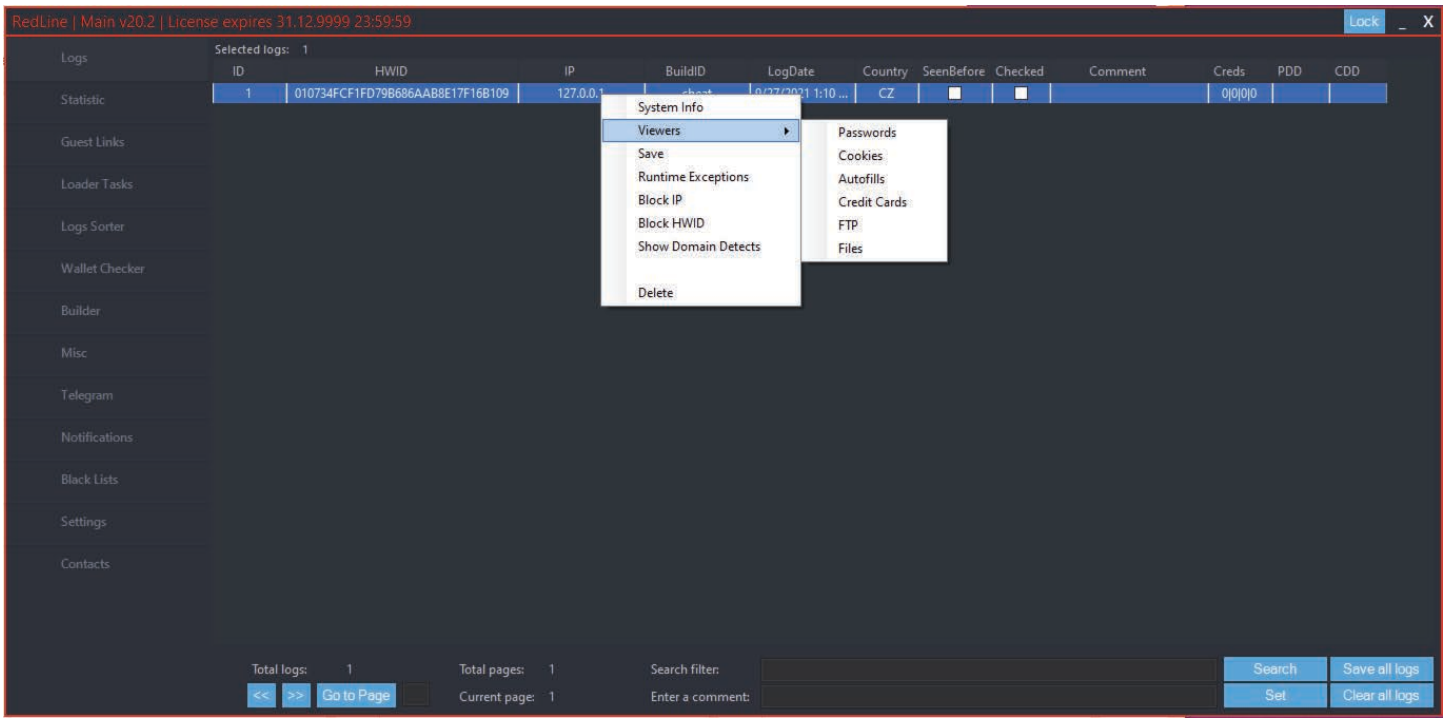

Figure 9: RedLine Stealer panel showing exfiltrated logs from infected machine (Source: Recorded Future)

One of the menu options, "System Info", gives the threat actor a detailed view into the infected machine, such as the installed operating system, hardware details, a screenshot, installed antivirus, the country code, IP address, and other useful information, which can be seen in Figure 10 below.

Threat actors can access specific logs to gain information to support further operations. An example, seen below in Figure 11, shows the detailed view giving the threat actor access to the cookies stolen from the infected machine. Theft of cookies can lead to session hijacking and session spoofing, which can allow an attacker to impersonate the infected user and access websites they frequent.

Information exfiltrated from an infected machine can be saved locally to be accessed outside of the dedicated admin panel. Additional information outside of what is displayed in the panel can be found in the saved logs, including a list of installed software, a process list, and more detailed user information.

Threat actors that manage multiple deployments of RedLine Stealer can use the "Statistics" tab in the panel to get an overview of the data they've successfully stolen. The statistics include the number of wallets, passwords, credit cards, and cookies, as well as statistics about the top 10 operating systems, antivirus systems, and countries where they've deployed RedLine Stealer.

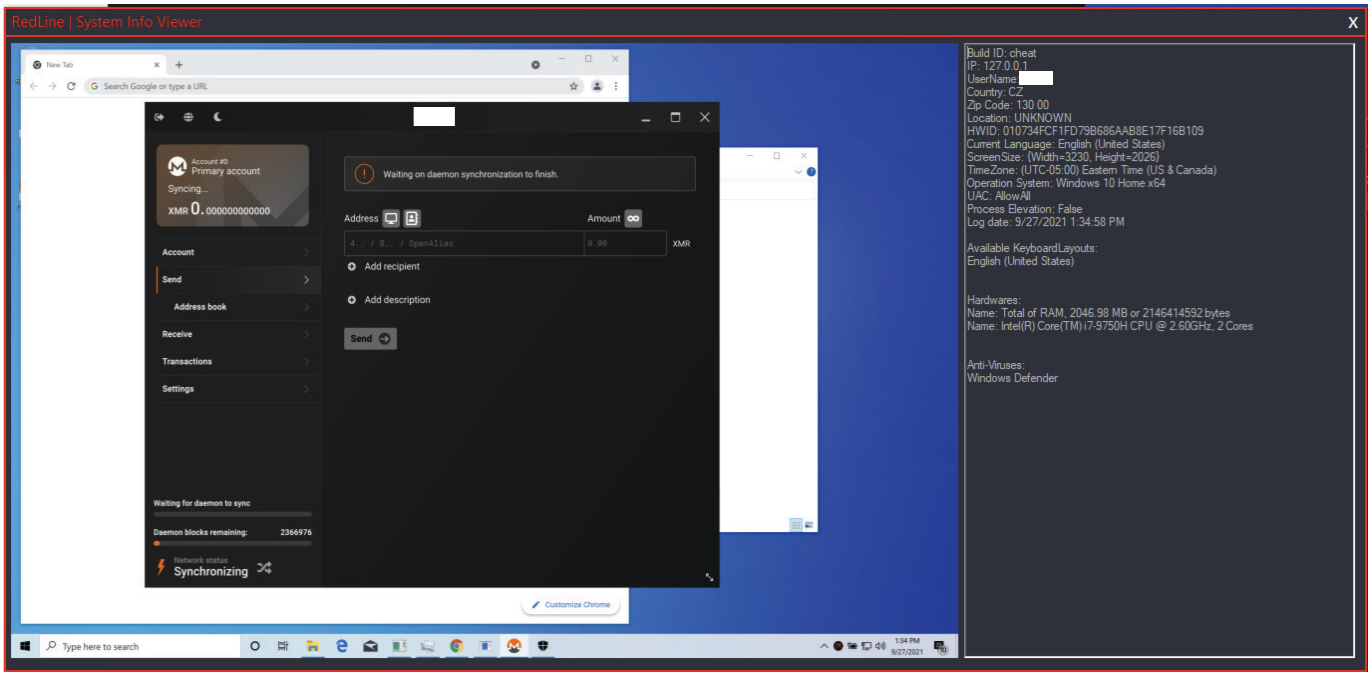

Figure 10: System information and screenshot exfiltrated from an infected machine to RedLine Stealer admin panel (Source: Recorded Future)

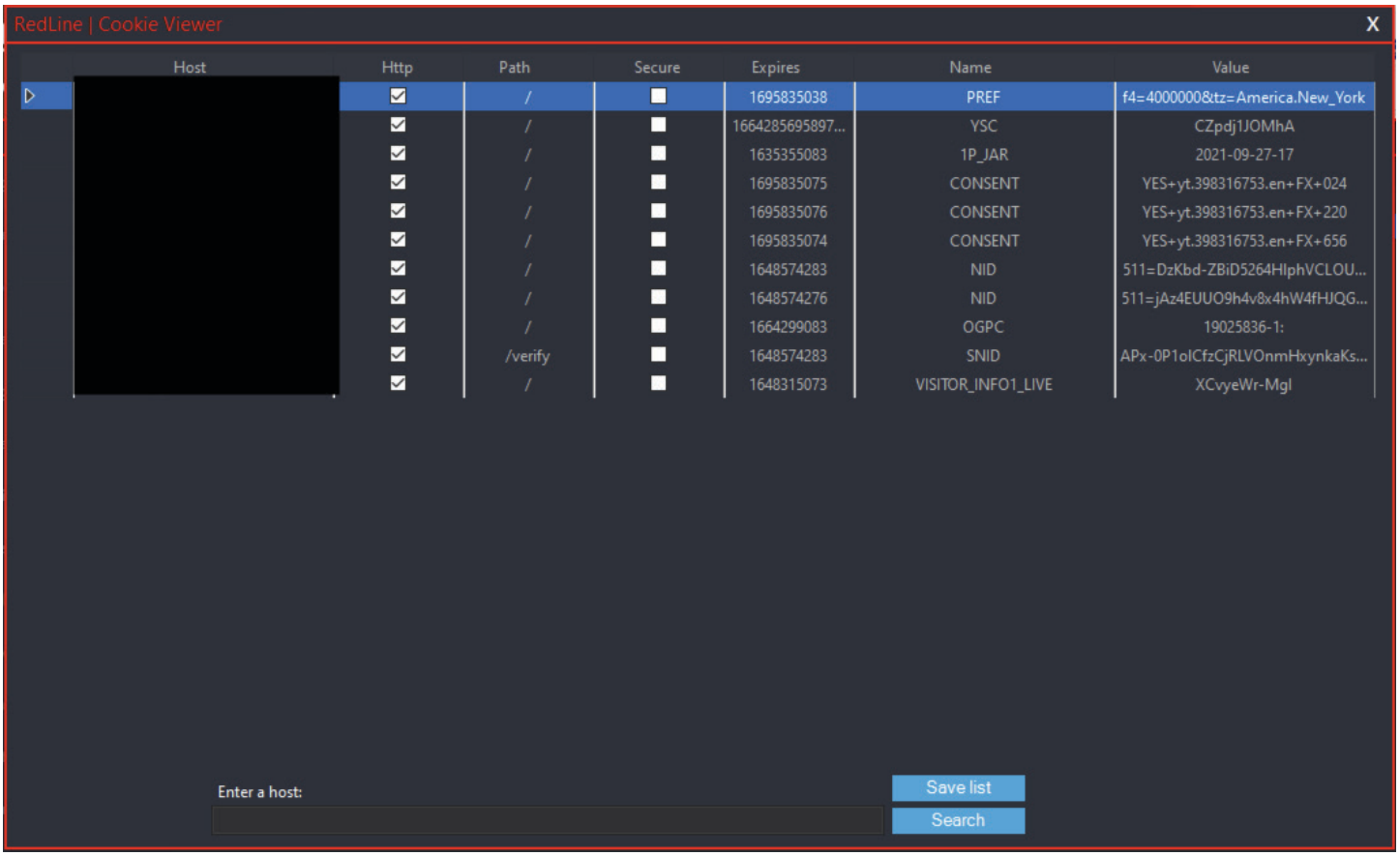

Figure 11: Cookies exfiltrated from an infected machine to RedLine Stealer panel (Source: Recorded Future)

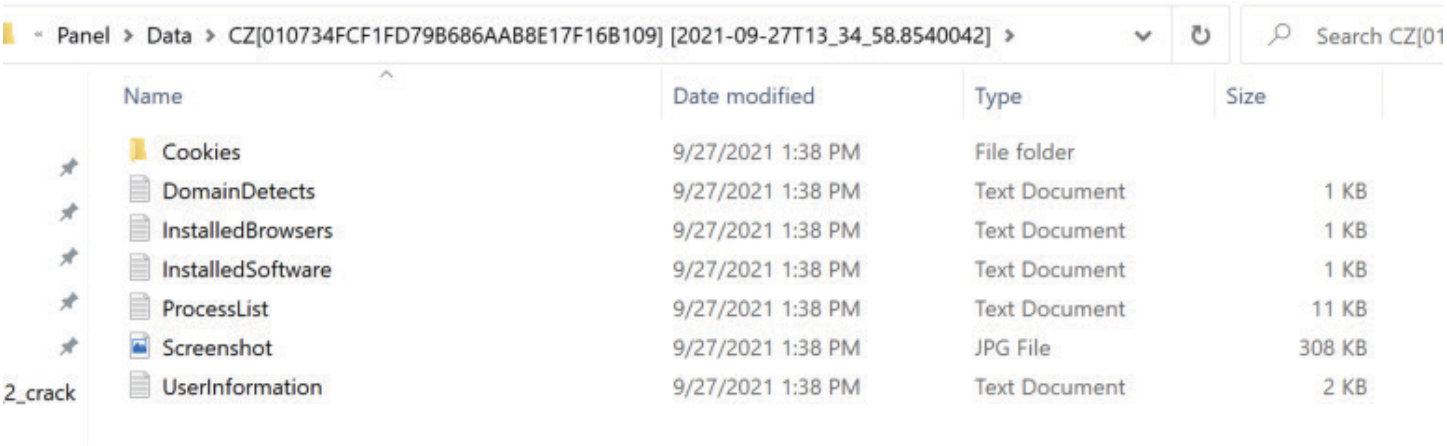

Figure 12: Saving a "log" from an infected machine results in these files being saved to the specified folder (Source: Recorded Future)

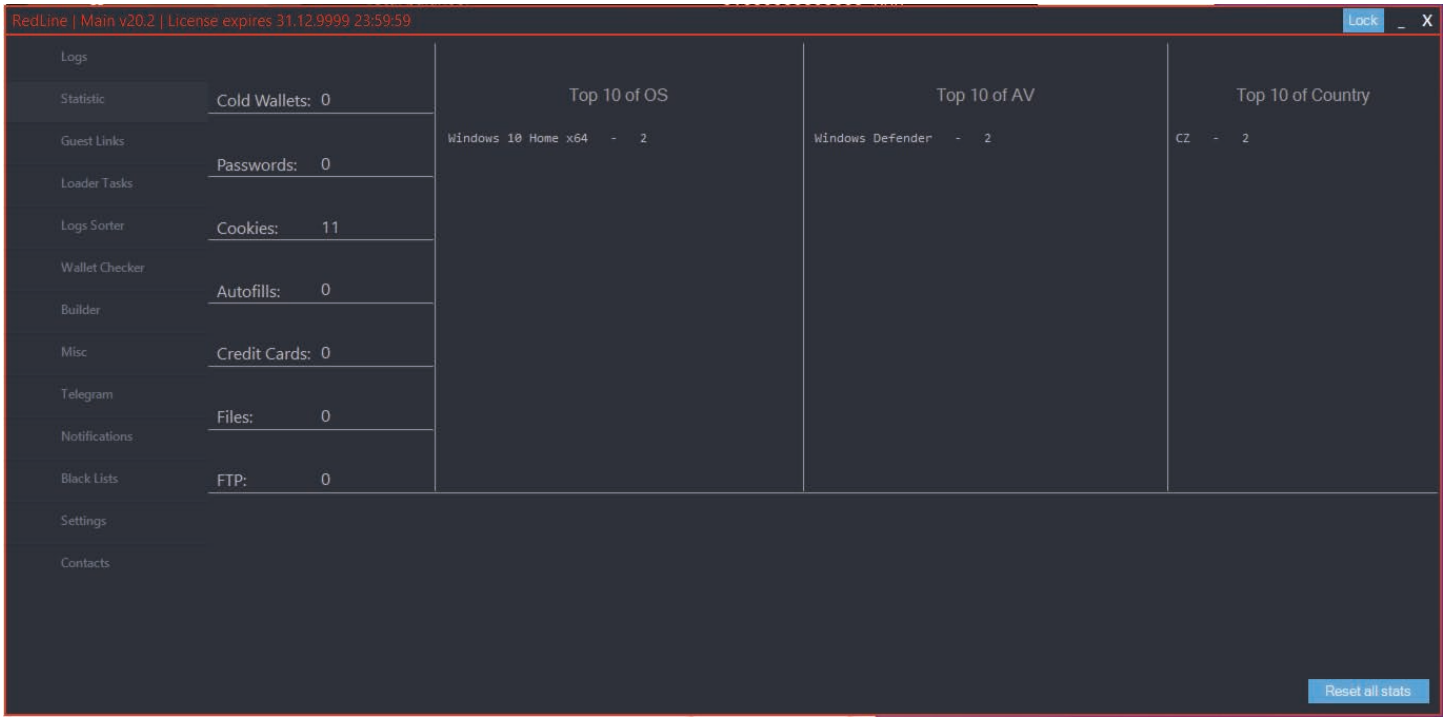

Figure 13: RedLine Stealer panel showing statistics about infected machines that communicate with this command and control server(Source: Recorded Future)

RedLine Stealer Analysis

The Redilne Stealer is written in C#, and based on Insikt Group's analysis, the code appears to be written by an experienced C# developer. The malware has a modular design with classes dedicated to each task or module, seen below in Figure 14. This allows new components to be written and integrated with minimal overhead. The icon file associated with the executable can vary from build to build as it can be specified by the threat actor using the RedLine Stealer admin panel. Builds created using the cracked builder have an original filename "Implosions.exe", the assembly name "Happy.exe", and are 96 KB; however, this can change depending on the layers of obfuscation applied by each threat actor after building RedLine Stealer. The threat actor who developed RedLine Stealer included recommendations in the FAQ on crypting services available via Telegram that can be used with RedLine Stealer, one of which is the @spectrcrypt_bot. The recommended services are:

- Using the /defensenet command in @spectrcrypt_bot, which is operated by the threat actor
- Using the /defense command in @spectrcrypt_bot, and the executable will be crypted on crypter[.]biz
- @Floiar
- @ninjacrypterbot

```
// Types:
//
// <Module>
// <PrivateImplementationDetails>
// Account
// AllWalletsRule
// ArmoryRule
// AtomicRule
// Autofill
// BCRYPT_AUTHENTICATED_CIPHER_MODE_INFO
// BCRYPT_KEY_LENGTHS_STRUCT
// BCRYPT_OAEP_PADDING_INFO
// BCRYPT_PSS_PADDING_INFO
// BrowserExtensionsRule
// BrowserVersion
// CC
// CoinomiRule
// CommandLineUpdate
// CryptoHelper
// CryptoProvider
// C_h_r_o_m_e
// DataBaseConnection
// DesktopMessangerRule
// DiscordRule
// DownloadAndExecuteUpdate
// DownloadUpdate
// ElectrumRule
// EndpointConnection
// EntryPoint
// EthRule
// ExodusRule
// Extensions
// FileCopier
// FileScanner
// FileScannerArg
// FileScannerRule
// FileZilla
// GameLauncherRule
// Gecko
// GeoHelper
// GeoInfo
// GeoPlugin
// GuardaRule
// HardwareType
// IpSb
// IRemoteEndpoint
// ITaskProcessor
// Json
// Jx
// LocalState
// MonitorHelper
// NativeHelper
// NordApp
// OpenUpdate
// OpenVPNRule
// OsCrypt
// Program
// ProtonVPNRule
// RecordHeaderField
// RecoursiveFileGrabber
// ResultFactory
// ScanDetails
// ScannedBrowser
// ScannedCookie
// ScannedFile
// ScanningArgs
// ScanResult
// SqliteMasterEntry
// StringDecrypt
// SystemHardware
// SystemInfoHelper
// TableEntry
// TaskResolver
// UpdateAction
// UpdateTask
```

Figure 14: Modules included in RedLine Stealer version 20.2 (Source: Recorded Future)

```
// ProtonVPNRule
// Token: 0x06000087 RID: 135 RVA: 0x00006248 File Offset: 0x00004448
public override IEnumerable<FileScannerArg> GetScanArgs()
{
    List<FileScannerArg> list = new List<FileScannerArg>();
    try
    {
        list.Add(new FileScannerArg
        {
            Directory = Path.Combine(Environment.ExpandEnvironmentVariables("%USERPstring.ReplaceROFILE%\\Apstring.ReplacepData\\Locastring.Replacel").Replace
              ("string.Replace", string.Empty), new string(new char[]
            {
                'P',
                'r',
                'o',
                't',
                'o',
                'n',
                'V',
                'P',
                'N'
            })),
            Pattern = new string("npvo*".Reverse<char>().ToArray<char>()),
            Recoursive = false
        });
    }
    catch
    {
    }
    return list;
}
```

Figure 15: Example of the ProtonVPNRule class highlighting developer tendencies (Source: Recorded Future)

Figure 15 highlights the following trends used by the developer throughout the RedLine Stealer code:

1. The code obfuscates path strings and uses string replacement functions to determine the real file path, helping the malware evade static string detection.
2. It uses arrays for strings instead of string variables and stores strings in reverse order to avoid string detection.
3. Continuous misspellings of words can be found within the code.

The bulk of the collection can be seen in the module labeled "ResultFactory", specifically in the function called directly from the application's Program.Execute main function named "sl9HSDF234". Interestingly, the names of the functions in ResultFactory are obfuscated, while all other function names in the binary are unobfuscated.

RedLine Stealer will terminate its own process and delete itself from disk in an attempt to remain undetected after collecting and exfiltrating the stolen data.

Since the release of the cracked builder, the original developer has continued to add functionality to RedLine Stealer. Some researchers report the addition of more types of crypto wallets being collected from newer samples including TerraStation, HarmonyWallet, Coin98Wallet, TonCrystal, and KardiaChain.

Host-Based Detection

```
// Token: 0x0600008A RID: 138 RVA: 0x00006480 File Offset: 0x00004680
public static bool sl9HSDF234(ScanningArgs settings, ref ScanResult result)
{
    bool result2;
    try
    {
        result.ScanDetails = new ScanDetails
        {
            AvailableLanguages = new List<string>(),
            Browsers = new List<ScannedBrowser>(),
            FtpConnections = new List<Account>(),
            GameChatFiles = new List<ScannedFile>(),
            GameLauncherFiles = new List<ScannedFile>(),
            InstalledBrowsers = new List<BrowserVersion>(),
            MessageClientFiles = new List<ScannedFile>(),
            NordAccounts = new List<Account>(),
            Open = new List<ScannedFile>(),
            Processes = new List<string>(),
            Proton = new List<ScannedFile>(),
            ScannedFiles = new List<ScannedFile>(),
            ScannedWallets = new List<ScannedFile>(),
            SecurityUtils = new List<string>(),
            Softwares = new List<string>(),
            SystemHardwares = new List<SystemHardware>()
        };
        ResultFactory.AKSFD8H23(settings, ref result);
        foreach (ResultFactory.ParsingStep parsingStep in ResultFactory.Actions)
        {
            try
            {
                parsingStep(settings, ref result);
            }
            catch
            {
            }
        }
        result2 = true;
    }
    catch
    {
        result2 = false;
    }
    return result2;
}
```

```
// ResultFactory
// Token: 0x0600009E RID: 158 RVA: 0x00006A08 File Offset: 0x00004C08
public static void ашы9p34(ScanningArgs settings, ref ScanResult result)
{
    if (settings.ScanWallets)
    {
        result.ScanDetails.ScannedWallets = new List<ScannedFile>();
        BrowserExtensionsRule browserExtensionsRule = new BrowserExtensionsRule();
        browserExtensionsRule.SetPaths(settings.ScanChromeBrowsersPaths);
        result.ScanDetails.ScannedWallets.AddRange(FileScanner.Scan(new FileScannerRule[]
        {
            new ArmoryRule(),
            new AtomicRule(),
            new CoinomiRule(),
            new ElectrumRule(),
            new EthRule(),
            new ExodusRule(),
            new GuardaRule(),
            new Jx(),
            new AllWalletsRule(),
            browserExtensionsRule
        }));
    }
}
```

Figure 16: ResultFactory class showing the list of collected data (left), and a detailed view of the scanned wallets (right) (Source: Recorded Future)

RedLine Stealer samples execute various commands that can be keyed on for detection. Although the PID and the path of the executable will change depending on the environment this instance of RedLine Stealer is running in, these commands and subsequent actions can be used for detection. We have created a Sigma rule to detect the use of commands and this rule has been shared on the Recorded Future Platform.

Insikt Group has also created a YARA rule for RedLine Stealer. The YARA rule is based upon uncommon strings found in the code as well as the misspellings described in the RedLine Stealer Analysis section. The YARA rule is available to Recorded Future clients.

Network-Based Detection

Network detection logic can be developed by making use of several key elements in the communications between the RedLine Stealer implant and the command and control (C2) server:

- RedLine Stealer communicates using the Microsoft Simple Object Access Protocol (SOAP), which allows applications to transfer data over HTTP. Tempuri[.]org is the default domain used by Microsoft development products including SOAP, and this and other SOAP artifacts are observed in the RedLine Stealer C2 traffic.
- Specific communications from the server are visible in the traffic, including commands from the C2 to gather information. There are some uncommon strings used.
- Specific communications from the infected system are visible in the traffic, such as system enumeration and responses to commands. Some uncommon strings are used.

Figure 17: RedLine Stealer-infected communication displaying SOAP interaction and C2 server instructions (Source: Recorded Future)

RedLine Stealer C2 servers use TCP, but do not use any specific port. As mentioned in the technical analysis section above, the port can be set within the RedLine Stealer builder. RedLine Stealer C2 servers most often are observed using random, high port numbers such as 11915 or 31858. Benign SOAP traffic is often on port 80, however, RedLine Stealer C2 servers have been observed operating on port 80 as well.

Not all of these elements are specific to RedLine Stealer, and in fact those such as the use of SOAP or port 80/TCP are quite common in network traffic. But by combining some of these features, effective detections may be developed. Based on this data, Snort IDS rules were created using aspects of the preceding elements these are available on the Recorded Future Platform.

Active C2 Server Detection

Insikt Group detects active RedLine Stealer C2 servers based on configuration data extracted from RedLine Stealer samples, which are then validated by checking for the appropriate response from the server. C2 servers so identified can be found in the Recorded Future Platform.

There are also open-source resources available for organizations to keep informed of RedLine Stealer C2 servers observed in the wild, such as the ThreatFox compilation of RedLine Stealer C2 servers provided by Abuse.ch.

Outlook

RedLine Stealer has become increasingly popular since its launch in 2020 based on a general increase in reference count observed among underground sources monitored by Insikt Group. This increase has been furthered by the influx of cracked versions of RedLine Stealer distributed across English-language cybercriminal forums, such as Raid Forums, that are easily accessible even to actors with less experience with similar tooling. RedLine Stealer's role as a secondary payload that supplements threat activity tied to other popular underground tooling, such as SmokeLoader, raises the probability that this stealer will continue to be a reliable method of data harvesting for the near future. The demand for stolen login information derived from RedLine Stealer infections for sale within the criminal underground similarly ensures that shops and marketplaces will continue to rely on it as a primary source of stolen information to sell. This continues to be reflected on multiple popular infostealer shops, such as Russian Market, where RedLine Stealer infections are associated with the highest volume of infected machines when compared to other popular infostealers including Vidar and AZORult.

Several links to cracked versions of RedLine Stealer distributed within underground sources are no longer active, with REDGlade likely to have taken steps to prevent old builds of the infostealer from working with the new admin panel. However, threat actors who have already downloaded the older, cracked RedLine Stealer package, which includes a builder and control panel, can continue using and sharing the malware without any cost.

Despite the release of a cracked version of the RedLine Stealer, REDGlade has continued to develop the malware and now sells a new, updated version. It is expected that both the "legitimate" and cracked versions of the malware will remain popular due to the free or minimal cost of this effective infostealer. We expect that the criminal marketplaces currently selling data collected by RedLine Stealer will continue doing so as long as the malware remains an effective means of accomplishing this task.

Since REDGlade continues to update RedLine Stealer with new functionality and continues to add new features to the admin panel, detections will need to be verified and updated accordingly in the future.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.