AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas

FILED
November 03, 2022
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY: LRT
DEPUTY

United States of America
v.
Maxim Rudometov

Case No. **1:22-MJ-00906-ML**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of see affidavit in the county of Travis in the Western District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
18 USC 1029	Access Device Fraud
18 USC 1030(a)(4) & 371	Conspiracy to Commit Computer Intrusion and Aiding and Abetting Computer Intrusion
18 USC 1956	Money Laundering

This criminal complaint is based on these facts:

See affidavit

☑ Continued on the attached sheet.

[redacted]
Complainant's signature

Special Agent [redacted]
Printed name and title

Sworn to before me and signed in my presence.

Date: November 3, 2022

[redacted]
Judge's signature

City and state: Austin, Texas

Mark Lane, U.S. Magistrate Judge
Printed name and title

SEALED

INTRODUCTION

I, [redacted], being first duly sworn, hereby state as follows:

1. I am a Special Agent with the U.S. Naval Criminal Investigative Service (NCIS) in the Cyber Field Office, assigned to the FBI's Cyber Task Force in Austin, TX. I have been employed by NCIS since 2006 and am certified as a Department of Defense Cyber Crime Investigator. I have received specialized training in the identification and preservation of digital evidence and have conducted dozens of cybercrime investigations involving computer intrusions, malware, or other cyber-facilitated crimes. As a Federal Agent, I am authorized to investigate violations of laws of the United States.

2. I make this affidavit in support of an application for an arrest warrant for Maxim RUDOMETOV for access device fraud, in violation of 18 U.S.C. § 1029, conspiracy to commit computer intrusion and aiding and abetting computer intrusion, in violation of 18 U.S.C. § 1030(a)(4) and 371, and money laundering, in violation of 18 U.S.C. § 1956.

3. As detailed below, Maxim RUDOMETOV has conspired to distribute and operate the RedLine Infostealer (also referred to as "RedLine"), a malware used to steal information from victims around the world. The malware was specifically designed to illegally remove important personal and financial information from computers. The malware is hosted on servers controlled by RUDOMETOV where paying affiliates can select specific program options and then deploy the malware against victims they choose.

4. This Affidavit is based on my participation in the investigation, the participation of other law enforcement officers, my review of documents and digital data obtained or seized during the course of the investigation, and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrant. It does not set forth all of my knowledge about this matter. All statements are set forth in sum and substance and relevant part.

DEFINITIONS

5. "Infostealer" is a term for a type of malware, alternately known as "information stealers," which is intended to be deployed against computers for the express purpose of stealing information. RedLine, as an infostealer, was capable of stealing, compiling, and exfiltrating from a victim computer saved financial information (such as credit card numbers and credentials to access online banking accounts), cryptocurrency access tokens (which can allow users to duplicate a cryptocurrency wallet), information saved by a user within an internet browser's autofill fields, web cookies, and even specific files or folders.

6. "Commodity malware" refers to malware which is developed by an individual or group for the express purpose of selling it to another individual or group (an "affiliate," as described below) for their own use. Developers of commodity malware may utilize a subscription model wherein the malware is "licensed" to an affiliate for a period of time, such as a month, in exchange for a corresponding amount of money, usually paid in one or more cryptocurrencies such as Bitcoin.

SEALED

7. "Logs" are folders or files containing information stolen during the deployment of an infostealer. Logs may have a variety of information within them. This information may be used to commit additional crimes such as identity theft, financial theft, or fraud, or sold to other cyber criminals on online forums or chat groups. Most infostealer logs contain, at a minimum, three categories of information: (1) system information (such as a computer's IP information), operating system type and version, a list of installed software, and user account; (2) username and passwords for credentials saved in a user's browser, and (3) session cookies for saved browser or login sessions created by the user. Logs created by the RedLine Infostealer are prominently identified by a large banner displayed at the top of the text file containing information about the infected computer, an example of which is included, below.

Figure 1: Banner contained within a RedLine log from December, 2021.

8. A "configuration utility" in the context of an infostealer is an administrative panel, either delivered as a standalone software that can be installed on the affiliate's computer or as a website. The configuration utility which allowed the malware's operator to build deployable versions of the malware and access—or interact with—logs created during the malware's use. In the case of RedLine, this utility even contained advertisements for other services which may be useful to the malware operator, including services called "installs" (described further below) that could increase the number of computers infected with an affiliate's specific build. [1]

9. "Cookies" refer to unique identifier assigned by a server running a website which can uniquely identify an authenticated user session. In practical application, a website may issue a cookie to users after they successfully enter their credentials to access a bank account. A user's browser stores that value and submits it back to the website to prove the user has already been authenticated to avoid logging into the website multiple times during a single browsing session. Cookies are typically accompanied by an expiration date or time at which the cookie is no longer valid. There is, however, no set mandatory time for expiration and that is within the discretion of the website developer.

[1] In both forum posts and RedLine's official documentation, a "build" is an executable version of the RedLine Infostealer that can be deployed against victim devices and result in the theft of information and files.

SEALED

10. To avoid confusion, the term "affiliate" in this affidavit refers to a criminal actor using RedLine to commit crimes, including stealing information, identity theft, and fraud. The term "user" refers to other individuals or groups who operate computers, including those targeted by RedLine affiliates.

STATUTES VIOLATED

11. Title 18, United States Code, Section 371 provides, in relevant part that "[i]f two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be" punished.

12. Title 18, United States Code, Section 1029 provides, in relevant part that "[w]hoever knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices" shall be punished. The term "access device" means "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds . . . ." The term "unauthorized access device" means "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud[.]" Section 1029 also prohibits a "conspiracy of two or more persons" from committing a substantive offense under the statute.

13. Title 18, United States Code, Section 1030(a)(4) provides, in relevant part, that "[w]hoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period" shall be punished.

14. Title 18, United States Code, Section 1956 provides, in relevant part, that "[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity" shall be punished. It further provides that any person who conspires to commit money laundering shall be similarly punished. Violations of Sections 1029 or 1030 constitute "specified unlawful activity" for purposes of money laundering.

SUMMARY

15. Based on the facts set forth below, there is probable cause to believe that Maxim RUDOMETOV has conspired to distribute and operate the RedLine Infostealer malware throughout the world beginning in February 2020. RedLine Infostealer was a commodity malware provided through a Malware as a Service ("MaaS") model. MaaS schemes allowed affiliates to purchase the ability to use RedLine and then distribute the malware to unsuspecting victims by various means, including email phishing, fraudulent software downloads, and

malicious software sideloading. Various ruses have been used to trick victims into downloading RedLine, including COVID-19 related ruses. RedLine was advertised for sale on cybercrime forums and had Telegram channels that offered customer support and software updates.

16. Once it infected a victim's computer, RedLine harvested personal information, financial information, saved credentials, and cryptocurrency information. RedLine sent that data to a server controlled by the RedLine affiliate. RUDOMETOV received payment for RedLine via various cryptocurrency accounts opened in other's names. He transferred those funds to other accounts, thereby laundering the proceeds. The information stolen by RedLine included access devices, as defined under federal law, and those access devices were stolen with the intent to commit fraud.

17. Based on analysis of publicly available information regarding unique malware samples, information provided by private sector companies that track the proliferation of malware including RedLine, as well as the lawful seizure of repositories of data stolen by RedLine affiliates, I have concluded that RedLine has been used to infect millions of computers around the world since February 2020.

STATEMENT OF FACTS

Architecture of RedLine Infostealer

18. RedLine has been used to infect millions of computers around the world since its introduction in or around February 2020. Several hundred of the victim computers were used by members of the U.S. Department of Defense. Like other MaaS, RedLine was capable of stealing a range of sensitive information from a victim's computer, including saved financial information (such as credit card numbers and credentials to access online banking accounts), cryptocurrency authentication tokens, and web cookies which can be used to effectively bypass multi-factor authentication. Additionally, the software[2] provided to each RedLine affiliate after purchasing a license to use the malware enabled the "sideloading" of additional malicious programs and code, meaning that RedLine could effectively be packaged with a variety of malware to attack the victim.

19. As a commodity malware, RedLine was sold primarily through Russian-language so-called "hacker" forums that routinely featured sales posts for similar malicious software, advertised stolen credentials and financial information, and hosted discussions where cyber-criminals could collaborate on tools and techniques to defraud and otherwise attack unwitting victims, computers, and networks. One such example, posted on a forum which advertises itself as the "Best Hack Forum"[3] had been viewed approximately 115,000 times as of the time of this affidavit. The poster prominently advertised RedLine as a "stealer designed for convenient work with logs," and "[t]he program was written taking into account all the wishes of people

[2] Through an undercover purchase, law enforcement found that purchasers of the malware received a zip file containing a configuration utility software. Once executed, the software required the purchaser to enter credentials that were created following the successful purchase. After authentication, the purchaser gained access to a utility which allowed the purchaser to configure and "build" an executable version of RedLine, which could then be delivered to computers that the purchaser intended to compromise.

[3] The URL of the forum is known to law enforcement but has been omitted here to avoid advertising the forum.

professionally involved in the field of carding."[4] [5] Additionally, the post advertised that RedLine was capable of stealing "login and passwords," "cookies," "autofill fields," "credit cards," and had modules for stealing cryptocurrency information. The malware cost approximately $150 USD equivalent in cryptocurrency assets (like Bitcoin) for a monthly license, or $900 USD equivalent in cryptocurrency assets for a "lifetime" license to use the malware.[6]

20. Law enforcement analyzed several forum posts advertising the RedLine Infostealer and discovered an active community of individuals who posted reviews of the malware as well as regular updates from the seller advertising new features. In addition to each update advertising that the malware was "cleaned,"[7] the seller advertised new functionality which would increase its usefulness as a criminal tool. For example, in one such update, posted by the seller's account on August 26, 2021, the seller claimed RedLine was now capable of extracting data from Google Chrome extensions that managed cryptocurrency wallets and transactions, linking to the Google Chrome store URLs of supported extensions.

21. Once purchased, affiliates could deploy the malware in any number of schemes. One early example in March 2020—near the beginning of the COVID-19 pandemic—included at least one affiliate using the Folding@Home project to lure unsuspecting individuals into downloading and executing a version of the RedLine Infostealer.[8] This example was particularly notable because users who likely intended to donate computing resources to the fight against COVID-19 were instead infected with RedLine.[9]

22. The malware was often bundled with a so-called "crypter," or tool used to encrypt, obfuscate, and manipulate the malware in such a way as to make it harder to detect by antivirus or anti-malware software. In addition, numerous messages sent by the official RedLine sales account on the encrypted messaging service Telegram directly linked to "install" services, explicitly advertising their use in conjunction with the malware.[10] Comments on the "Best Hack Forum" thread included hundreds of apparently satisfied customers, many of whom commented on the post to attest to the success of RedLine. For example, on or about February 20, 2022,

---

[4] I know based on my training and experience that "carding" refers to the criminal practice of trafficking and using stolen credit cards. Carding may also describe the general exploitation of personal data for financial fraud, and money laundering techniques.

[5] The posts were written in Russian and the translated using publicly-available machine translation tools that I believe to be reliable based on my training and experience.

[6] The price of a lifetime license increased from $800 to $900 USD over the course of the investigation.

[7] In the context of malware, "cleaned" typically refers to a process of changing the code of a malicious program such that existing signatures developed by antivirus companies to detect the malware are unsuccessful in detecting the malware or associating it with a known malware variant.

[8] Based on publicly-available sources, I have learned that Folding@Home is a distributed computing project intended to help scientists and researchers develop new techniques for countering diseases by studying complex simulations of protein dynamics. The program, which was stated at Stanford University and has grown to involve numerous other colleges, universities, and multinational technology companies like Microsoft and Google, is active as of the date of this affidavit.

[9] See: https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign.

[10] In the context of malware, "install" services (commonly referred to as "installs") refer to a system of malware delivery wherein malicious scripts or software are bundled with other software – commonly, cracked legitimate software or software which mimics legitimate software in name and appearance – or delivered through an existing network of compromised devices. In this way, install services are used by cybercriminal actors to increase delivery of malware to a broader victim pool, and can often even be targeted geographically, such as for a criminal actor seeking to compromise computers in the US or EU.

SEALED

affiliate "Ch3l0v3k" posted a screenshot of a statistics page, apparently from their own RedLine configuration utility. The screenshot showed the following statistics describing files and information stolen through "Ch3l0v3k's" deployment of RedLine:[11]

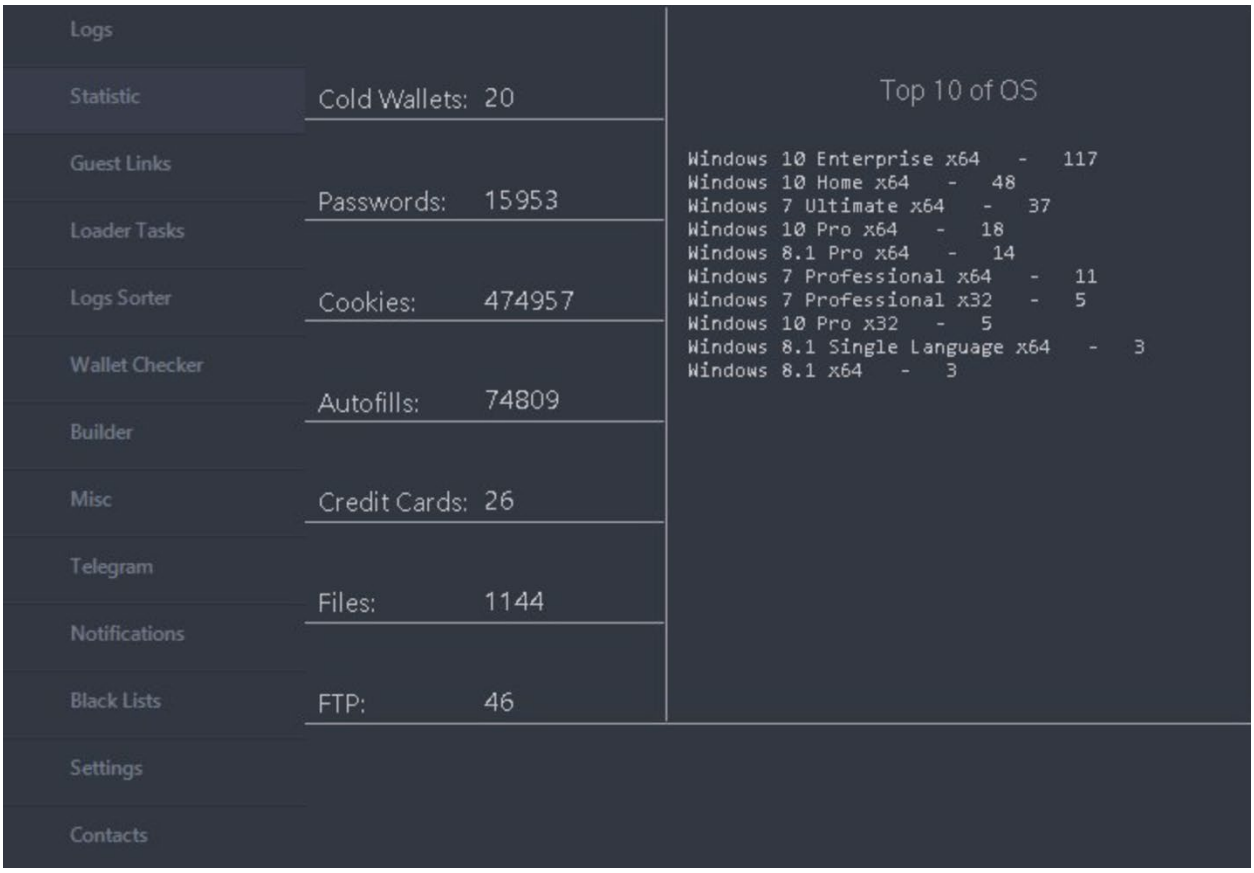


Figure 2: Screenshot posted by an alleged user of RedLine.

Based on my training and experience, I know that "cold wallets" typically refer to a method of storing cryptocurrency and "autofills" refers to information saved by a user that is automatically filled by a victim's browser onto a website. "Cookies" refer to session cookies used by many websites to uniquely identify a user or authenticated session that are targeted by criminals in order to bypass security mechanisms such as multi-factor authentication, or MFA. I believe that this screenshot thus shows that the affiliate used RedLine to successfully steal hundreds of thousands of cookies, files, login credentials, cryptocurrency information, among other data.

[11] Law enforcement's analysis of the RedLine configuration utility included the capture of screenshots of the various pages of the utility, including the statistics page displayed herein. The screenshots captured by law enforcement closely matched the format of the screenshot posted by affiliate "Ch3l0v3k." Thus, I believe that the affiliate's posting is an accurate depiction of a version of the RedLine configuration utility statistics page.

SEALED

Law Enforcement Analysis of RedLine

23. While located in Austin, Texas, investigators purchased RedLine and conducted an analysis of the malware in a controlled environment.[12] Through this analysis, investigators observed that RedLine could be configured to target specific accounts, such as those related to financial services, and could be encrypted in a manner that rendered many antivirus programs ineffective at detecting the malware. In its default configuration, RedLine was prevented from operating on computers with language settings indicative of use in the Commonwealth of Independent States ("CIS"), an area which approximately describes the territory of the former Soviet Union. This is a common feature of malware created in Russia and Russian-speaking countries and is intended to dissuade Russian law enforcement officials from interfering with cyber criminals focused on victims in non-CIS countries.

24. Investigators also learned that the configuration utility provided to the affiliate after purchase of the malware permitted full customization of RedLine for deployment against unsuspecting individuals and computer systems. The utility, which used the same format and other details as the screenshot posted by "Ch3l0v3k" above, allowed access to logs of victim data, included tools to track deployment statistics, and even processed stolen information to make it easier for affiliates to make use of the stolen data. A screenshot of the utility viewed by law enforcement is below. The utility relied on one or more external servers for the process of building the malware and performing user authentication (the "Licensing Server").[13]

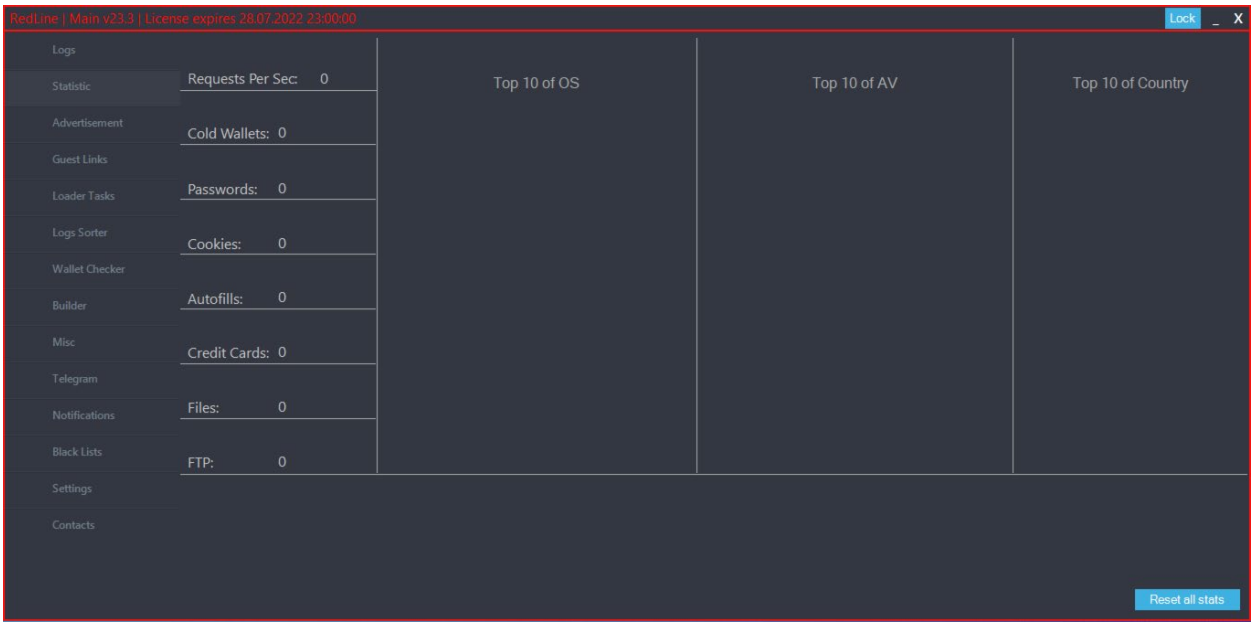


Figure 3: Screenshot of configuration utility, captured by law enforcement.

[12] Investigators accomplished the forensic analysis of RedLine with the assistance of a Computer Scientist assigned to the FBI. The Computer Scientist who conducted a hands-on analysis of the malware's source code has received extensive training through both his college education as well as additional training during his employment with the FBI and has considerable experience in analyzing malware written in the C# coding language, the same language which was used to write the RedLine Infostealer.

[13] The URL of the Licensing Server is known to law enforcement but has been omitted here.

SEALED

Identification of RUDOMETOV

25. Through open-source research, law enforcement discovered a blog post written by someone using a moniker alleging that that RedLine was created by two actors, identified by the monikers "Dendimirror" and "Alinchok," respectively. The posting moniker had been identified by a private security firm as having been used by an individual behind a different malware scheme known to U.S. law enforcement. In my training and experience, while cyber criminals can change and use multiple monikers over time, in many instances cyber criminals are incentivized to use the same moniker in order to establish their reputation within the cybercrime community. That reputation is key to their ability to monetize their cybercrime skills.

26. The blog post was archived by the Internet Archive on or about March 11, 2020. The blog post included a rough malware analysis on an apparent version of RedLine. Based on my review of the post and various Russian hacker forums, I believe that the post was shared widely. One of the alleged creators of RedLine, "Alinchok," even commented on the blog post. While the original post alone is not enough to associate RedLine with the "Dendimirror" and "Alinchok" monikers, subsequent investigation, as described below, corroborated the initial allegations made by the pseudonymous writer.

27. Investigators identified posts made in 2017 on various Russian-language hacker forums and other publicly-accessible websites which used the moniker "Dendimirror" in association with another infostealer malware, called "MysteryStealer". During the period of time when the Dendimirror moniker was in use, a U.S. private security firm discovered an email address contained within a leaked database used by an unnamed Russian-language hacker forum which was used to register an account that used the Dendimirror moniker. The email address, which is known to law enforcement, was serviced by the Russian communications firm Yandex (the "Yandex Email Address"), and later investigative steps described below linked the Yandex Email Address online accounts which used monikers connected to Dendimirror. Those include "GHackiHG" and "bloodzz.fenix" (discussed in detail below) as well as services used by RUDOMETOV in his personal capacity, such as Google and Apple.

SEALED

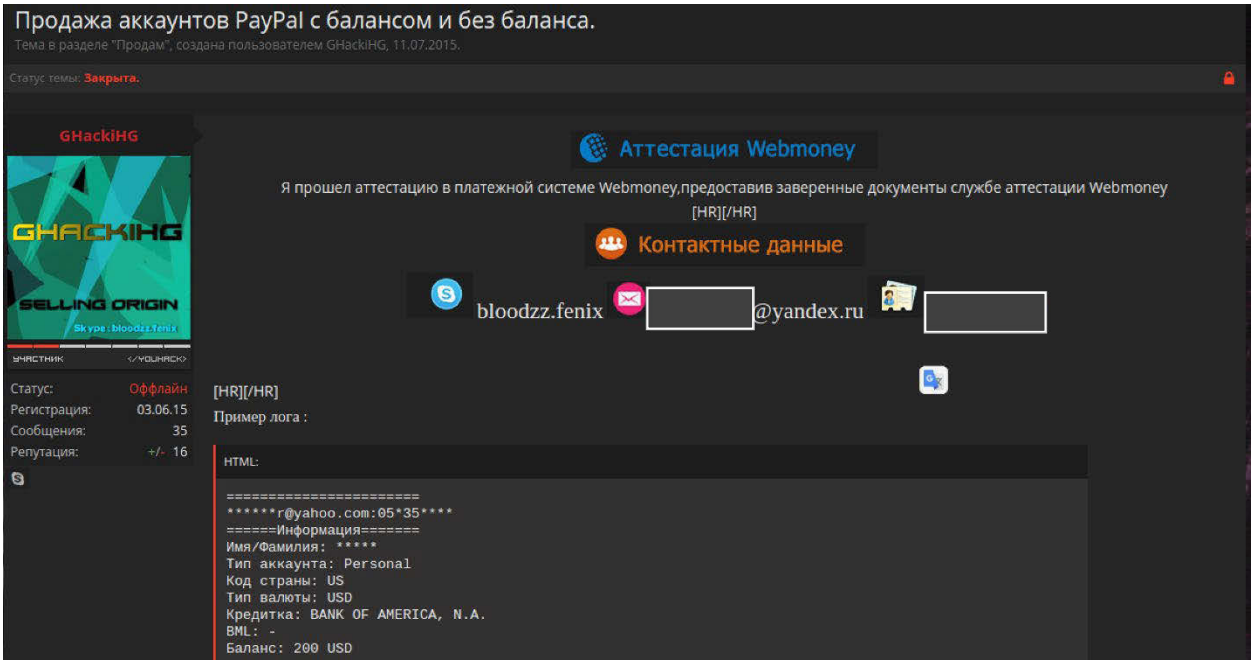


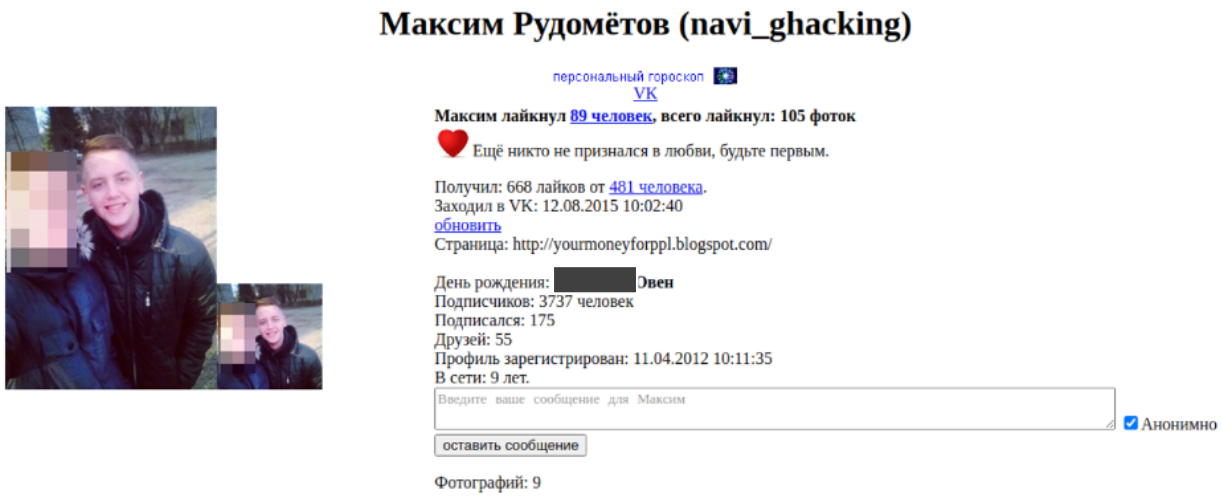
Figure 4: Forum post listing the Yandex email address as a means of contact in addition to a Skype address, which was also linked to RUDOMETOV.

28. The Yandex Email Address was found on Russian-language hacker forum "YouHack" to have been used as early as 2015 by an individual using moniker "GHackiHG" to sell "PayPal accounts with and without balance," according to an automated translation of the thread's title. The association between moniker GHackiHG and Dendimirror was further corroborated by information shared on several hacker forums by users bearing both monikers, including several which included in their contact information: a Skype username known to law enforcement, the Yandex Email Address, and a VK profile owned by an individual named "Максим Рудомётов (Maxim Rudometov)". VK is a Russian social media and social networking service. Law enforcement examined the publicly viewable VK profile and found that the individual depicted in photos posted by the account bore a close resemblance to an individual depicted in an advertisement included within the March 11, 2020, blog post. That advertisement promoted the individual's skill in coding in the C# programming language and "writing botnets and stealers."[14]

[14] The RedLine Infostealer is written using the C# programming language.

SEALED

Figure 5: Comparison photos of Maxim; from VK profile (top-left), advertisement for C# stealer training (top-center), an Apple account registered by the Yandex Email Account (top-right), and dating profile (bottom).



29. In response to legal process, investigators received data from several U.S. providers, including Apple, Google, and Microsoft for accounts related to one or more of the common identifiers for both the GHackiHG and Dendimirror monikers. The Yandex Email Address was used to register an Apple account by Maxim RUDOMETOV. A judicially-authorized search of this Apple account revealed an associated iCloud account[15] and numerous files that were identified by antivirus engines as malware, including at least one that was analyzed by the Department of Defense Cybercrime Center ("DC3") and determined to be RedLine. Notably, among the malicious files saved to RUDOMETOV's Apple iCloud Drive was

[15] Apple Inc. is a United States-based electronic communications service provider and/or remote computing service that provides its users with, among other things, the ability to create an Apple account/authentication method also known as an AppleID. The AppleID may then be used for various services including the cloud storage and service bundles iCloud or iCloud+. An iCloud account and the associated iCloud Drive often contains various forms of user data, including photographs, location data, text messages or iMessages, emails, financial information, or records of purchases. An AppleID and iCloud account may also be associated with services like iTunes or Apple Music. For convenience, I use the terms "Apple account" and "iCloud account" interchangeably to refer to accounts and services provided to users by Apple and which contain data that investigators have obtained and reviewed during this investigation.

a file entitled "MysteryPanel.rar" which correlates to the information stealing malware referenced above.[16] In addition to the registration information indicating RUDOMETOV was the owner of the Apple account, the account contained photos that included RUDOMETOV's official identification documents and apparent personal photos.

RUDOMETOV Connections to the RedLine Digital Infrastructure

30. In August 2021, law enforcement obtained a copy of a portion of the Licensing Server (one of the servers used by RedLine) from a security firm that voluntarily disclosed the information to the government. The firm collected the information independently and not at the direction of law enforcement. The firm is staffed by individuals who have training and experience in malware analysis and who have provided reliable information about malware in the past. Investigators obtained a search warrant to analyze the data in the server and found additional evidence linking RUDOMETOV to the development and deployment of RedLine, including him interacting or accessing the Licensing Server using multiple usernames. The following are a selection of examples of data found within server logs and linked to accounts or services attributed to RUDOMETOV:

a. At about 21:21 on May 16, 2021 (time zone unknown), username "Heijs" using an IP address ending in -.180 requested a build of RedLine from the Licensing Server. Approximately nine minutes later, the same IP address was logged by Apple as having been used to interact with the iCloud account attributed to RUDOMETOV that is described above. Proximate IP address use correlated between other online accounts under RUDOMETOV's control and the License Server revealed other usernames on the License Server apparently controlled by RUDOMETOV, including "Admin12" and "testpanel."[17]

b. An individual using an IP address ending in -.96 logged into the Licensing Server with computer command "sign on" 25 times on July 12, 2021, starting at 00:35:00 and ending at about 02:39. The same IP address was used approximately 701 times to access or interact with the iCloud account attributed to RUDOMETOV throughout July 2021.

c. An individual using an IP address ending in -.14 signed a malicious file using the Licensing Server on May 2, 2021.[18] Approximately one hour earlier, the same IP address was used to play a mobile game while logged into the Apple iCloud account attributed to RUDOMETOV. According to registration and location information published by the registrar of the IP address, Yug-Link Ltd., the IP address was assigned to an Internet Service Provider in the city of

[16] As discussed above, "MysteryStealer" may refer to a previous information stealer malware also alleged by the pseudonymous writer of the aforementioned blog post to have been developed by the individual using the Dendimirror and/or Alinchok monikers.

[17] Based on the time of the interactions, which preceded any customer interaction with this server (unlikely to be the first used by RUDOMETOV), law enforcement believes these accounts to be controlled by RUDOMETOV and likely used in the testing and validation of RedLine's components.

[18] Based on my training and experience, I know that "signing" software means adding a digital certificate to a file which is often used to verify the authenticity – and sometimes safety – of a file. In malware, files are signed to decrease the likelihood of detection by antivirus or antimalware software.

SEALED

Krasnodar, Russia. Several photos in RUDOMETOV's iCloud account had metadata indicating they were taken in Krasnodar, Russia, just four days after the -.14 IP address was used to interact with RUDOMETOV's iCloud account and the Licensing Server.

d. Investigators have also uncovered a Binance cryptocurrency exchange account ending in number -8286 registered using the Yandex Email Address. Common IP addresses were used to log into or access this account as well as the Licensing Server and/or RUDOMETOV's iCloud account. For example, on January 11, 2022, at 21:19:28 UTC, an IP address ending in -.246 was used to access RUDOMETOV's iCloud account. Approximately four minutes later, the same IP address was used to interact with the Binance account ending in -8286.

e. In all, 33 incidents of IP re-use, defined as the use of the same IP address to access or otherwise interact with two services within 48 hours, were observed between the Licensing Server, RUDOMETOV's iCloud account, and/or the -8286 Binance account.

31. Additionally, law enforcement has discovered numerous other links between RUDOMETOV, accounts linked to RUDOMETOV, and the malware, including:

a. The monikers GHackiHG and Dendimirror were associated with a common Skype account investigators observed to be listed publicly on various hacker forums. RUDOMETOV has interacted with his iCloud account from the same IP address used by the user of the Skype account. For example, on or about October 14, 2019, at about 12:52:56, an individual using an IP address ending -.76 accessed the Skype account and then, approximately two hours later, the same IP address accessed the Apple AppStore from an Apple iPhone 7 registered to RUDOMETOV's iCloud account.

b. The -8286 Binance account (registered to the Yandex Email Address) conducted an SMS verification at about 13:42:15 on or about May 13, 2021 using the same -.180 IP address used by username "Heijs" (described above). Approximately two minutes later, the same IP address was used to play a multiplayer game "Tennis Clash" on a device registered to RUDOMETOV's iCloud account. Notably, the Binance account ending in -8286 made use of an unknown woman's passport and photo in order to satisfy the Binance "Know Your Customer" requirements. A photo of the same passport was found saved to RUDOMETOV's iCloud Account.

c. GitHub account[19] GHackiHG was repeatedly accessed by the same IP addresses used to interact with RUDOMETOV's iCloud account often within minutes of each other. For example, on March 5, 2019, an IP address ending -.110 was used at about 21:44:25 to play a game on an Apple Watch registered to RUDOMETOV's iCloud account. Approximately four minutes later, the same IP address was used to access a GitHub repository which

[19] GitHub is an online service that provides repositories for computer code development as well as collaboration tools for software developers.

contained a common exploit used against Windows devices.[20] In another example, an address ending -.254 was used to access a repository which contained information about CVE-2019-5418[21], a critical vulnerability in a common web application framework, while logged into the GHackiHG account. Approximately 15 minutes later, the same IP was used to access Viber Messenger from an iPhone registered to RUDOMETOV's iCloud account.

d. In March 2022, investigators analyzed a newly-released configuration utility for RedLine, provided to paying users and affiliates of RedLine as an update to prior versions of the configuration utility. Through this analysis, and subsequent analysis of information obtained from GitHub in response to legal process, law enforcement found that the user that owned a GitHub repository containing an encryption key required by RedLine for routine functions was linked by device cookies to the GitHub account GHackiHG whose user, in turn, and as described above, is believed to be RUDOMETOV. Investigators believe that the encryption key was critical to the function of the malware and was used in the validation process to allow an affiliate to access and compile RedLine.

e. The -8286 Binance account described above and linked to RUDOMETOV by way of the Yandex Email Address received approximately 150 USD (+/- 5 USD) of cryptocurrency assets 54 times between April 2021 and August 2021.[22] The -8286 Binance account sent $70,226.54 USD-equivalent in cryptocurrency assets to a Binance account ending in -3821 through 39 transactions between May 2020 and August 2021. That -3821 Binance account received approximately 150 USD (+/- 5 USD) of cryptocurrency assets in 104 instances between July 2021 and October 2021 and was initially identified as one of the accounts used by the operator(s) of RedLine to receive payments for leases to use the malware.[23] IP address ending in -.157 was used to access both the -8286 Binance account and the -3821 Binance account within approximately seven hours of each interaction, both of which occurred on March 4, 2018.

32. In summary, there are numerous financial and IP connections between online accounts registered to RUDOMETOV and the server which is used by the RedLine malware to configure deployable versions of the infostealer. There are also numerous connections between registration information used in RUDOMETOV's online accounts and the -8286 Binance account used to receive payments for RedLine. RUDOMETOV's iCloud account contained RedLine malware code. And an account used by RUDOMETOV is linked by device cookies to a GitHub account that provides one or more files that are crucial to the validation and operation of

[20] An exploit is a program or code designed to make use of vulnerabilities or security flaws in software or hardware.
[21] "CVE" stands for Common Vulnerabilities and Exploits. The CVE system provides a method for publicly sharing information on cybersecurity vulnerabilities and exposures.
[22] During this period, RedLine was being leased for approximately $150 USD per month.
[23] Law enforcement gained access to an account used to sell the RedLine Infostealer on a Russian-language hacker forum. Cryptocurrency addresses found within direct messages sent by the account in response to unknown individuals seeking to purchase a license to use RedLine were traced to the -3821 Binance account.

RedLine.[24] Therefore, there is probable cause to believe that RUDOMETOV is in a conspiracy to distribute the RedLine Infostealer and to launder the payments received from users of RedLine Infostealer.

RedLine Victim Information

33. RedLine has been used to access protected computers in the Western District of Texas and elsewhere without authorization and by means of such unauthorized access, furthered fraud and obtained information of value.

34. In April 2021, law enforcement was contacted by Company A, whose headquarters are in Dayton, OH, who reported an employee's account was compromised by an unidentified information-stealer type malware that was masquerading as a messaging application. Upon forensic analysis of the malware by the Defense Cybercrime Center, law enforcement determined that RedLine had been used to attempt to steal information from Company A via the compromised employee's account. Company A is a member of the U.S. defense industrial base and a contractor for the U.S. Army and U.S. Navy. An investigation by a third-party incident response company contracted by Company A to investigate the incident could not identify any evidence of exfiltration of data.

35. In March 2022, law enforcement was contacted by Company B, whose headquarters are in the Western District of Texas, regarding an attempted intrusion into their corporate network. Company B provided email addresses which were used to attempt to gain access to their internal network via phishing attempts. Using this information, law enforcement queried databases which contained records of information stolen by RedLine which had been made available online and determined that an account owned by Company B and used in the attempted intrusion appeared in RedLine log that predated the attack on Company B by approximately three months.[25] The log also contained stolen user information for several internal services owned by Company B, including the email account which was used in the initial attack. The Company B server that was the target of the attempted breach was located in the Western District of Texas. The Company B employee whose information was used in the attempted breach resided in China at the time their computer was infected with RedLine.

36. Company C, headquartered in Redmond, WA, has disclosed publicly that a group they identified as DEV-0537 but which has been identified elsewhere as "Lapsus$," utilized the RedLine Infostealer to obtain passwords and cookies, which it then used to access an employee account. According to information published by Company C on public websites, the employee's access was used to obtain, and subsequently leak, limited source code owned by Company C.

37. Victim A, an individual with residence in Portage, Indiana, reported that they lost approximately $370,000 USD equivalent in cryptocurrency assets after their online wallet was taken over by unknown individual(s). After the theft, Victim A hired a computer forensics firm to determine the cause of the account takeover. The forensics firm identified malicious software

[24] As part of this Affidavit, I am attaching a diagram, Figure 6, which illustrates some of those connections.

[25] In my experience, credentials are commonly sold one or more times before being used in an intrusion. While some affiliates deploy RedLine with the explicit intention of gaining access to computer networks to perform their own criminal intrusions, many others sell the derivative logs – and access granted by the information contained therein – to other criminals, including ransomware operators, for use in later intrusion attempts.

which had been run on the victims' device and used to steal credentials, including Victim A's cryptocurrency exchange account. Subsequently, DC3 conducted an independent analysis of the malicious code introduced to Victim A's computer, and concluded it contained a version of RedLine.

38. A private security firm, which was conducting independent research into RedLine and has provided reliable information in the past, identified personal information stolen via RedLine and then shared or sold on online forums. On or about April 29, 2022, the firm provided investigators with the logs of stolen information, which included over 2,000 individual records containing at least one credential for an account, service, or website, owned, or administered by the Department of Defense.

39. Separately, law enforcement deployed a copy of RedLine in a controlled environment on or about August 18, 2021. The logs obtained from the controlled environment were identical in format to the logs obtained by the private security firm.

40. Law enforcement recovered a U.S. hosted server via a search warrant which acted as a command and control server for a build of RedLine deployed against victims, including victims described above as Company A and Victim A. Law enforcement identified the server based on their investigations into the use of RedLine to victimize Company A and Victim A. Found within the server were thousands of folders which matched the naming convention associated with logs created through the deployment of RedLine, and the folders contained files which listed apparent victim data, such as user names, passwords, financial data, and cookies. Notably, the files and folders were structured almost identically to other RedLine log files described herein as having been received from other sources.

41. Based on my review of the logs from the private security firm and command and control server described above, I have determined that at least 42,197 access devices (including login usernames with associated passwords) were stolen from computers located within the Western District of Texas. My conclusion rests on an analysis of the IP addresses for the victim computers at relevant times. The stolen Western District of Texas credentials include those for websites like MyPay (the Department of Defense paycheck portal), the U.S. Army's Office 365 email environment, and a website owned by the Defense Manpower Data Center, which serves as a repository for personal information including sensitive information about a service members' dependents. Law enforcement confirmed that email addresses owned by the Department of Defense were legitimate and assigned to individuals actively serving in the U.S. Military who were stationed at locations including Fort Hood, TX, which is located within the Western District of Texas, at the time the logs were created. Additionally, I spoke with Victim B who is an employee of the City of Austin, TX and whose computer was in the Western District of Texas. Victim B was identified through an examination of the command and control server containing the victim information described above. Victim B had over 600 passwords stolen from his computer including passwords to government websites, online banking, Thrift Savings Plan, online tax preparation services and insurance among others.

CONCLUSION

42. Because of his control over RedLine's digital and financial infrastructure; because RedLine enters into an agreement with each of its affiliates to receive payment to enable computer intrusion and RedLine aids and abets its affiliates each time its servers build a version of RedLine specifically to commit computer intrusion; because RUDOMETOV directly and with

SEALED

others received payment for RedLine using methods to conceal the source, nature, and ownership of the funds; and because RedLine was used to steal access devices (including financial accounts and usernames with passwords) in order to commit financial crimes, I submit that there is probable cause to believe Maxim RUDOMETOV, together with others, committed violations of federal law within the Western District of Texas and elsewhere, including access device fraud, computer intrusion, and money laundering. Accordingly, I request the issuance of a warrant for his arrest.

Electronically submitted,

[redacted]

NCIS Special Agent
FBI Cyber Task Force

Subscribed and sworn to me via telephone pursuant to Federal Rule of Criminal Procedure 4.1 on November 3, 2022.

[redacted]

HONORABLE MARK LANE
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF TEXAS

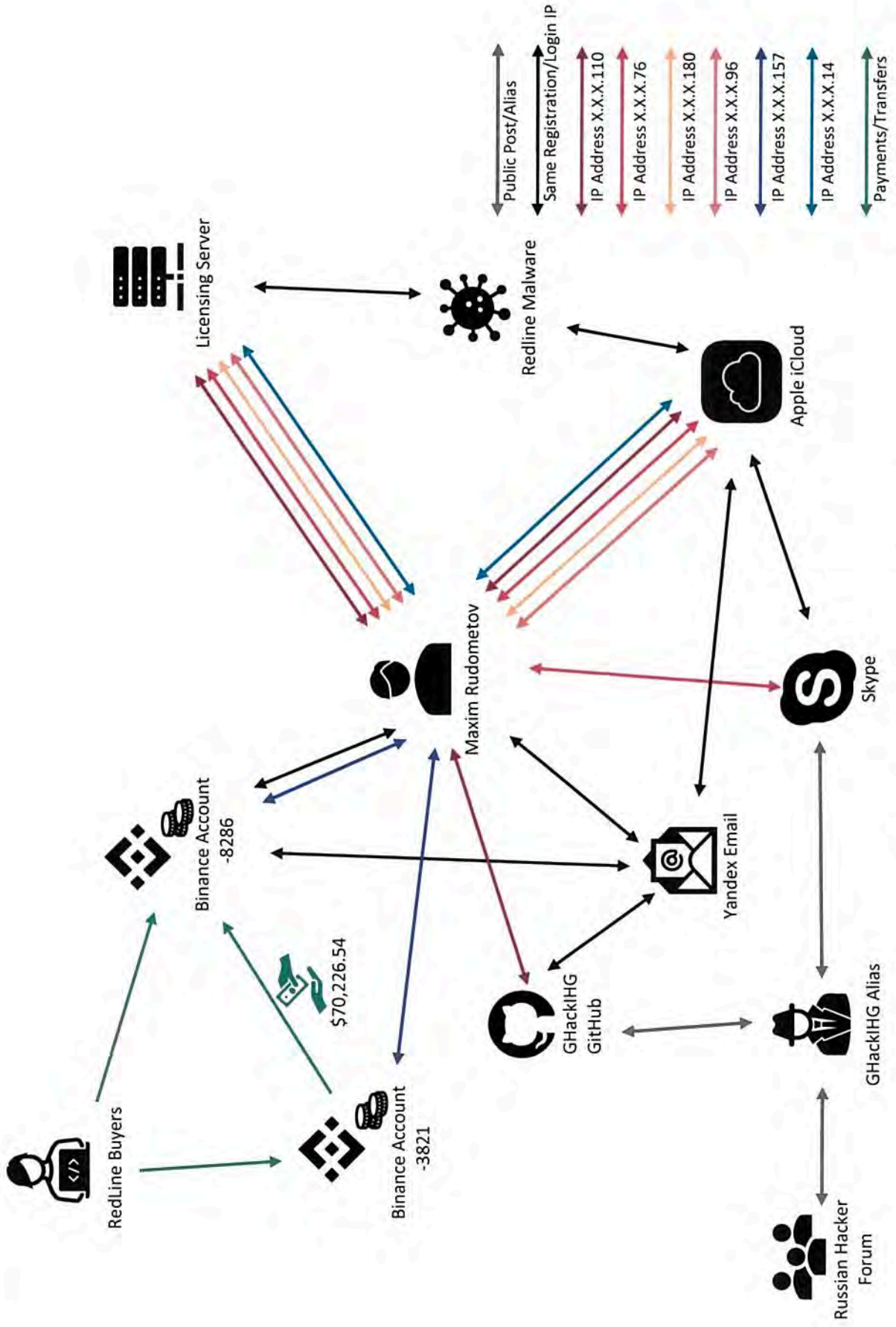


Figure 6: Relational diagram. Diagram is for illustration only and is not exhaustive.