BI.ZONE

The seven faces of darkness

How the malware-as-a-service model is being used by cybercriminals to attack Russian organizations

Contents

The report was prepared by BI.ZONE Threat Intelligence experts:

- Andrey Chizhov
- Polina Bochkareva
- Nikolay Golentsov

Introduction

There are many threads on underground forums in which developers offer malware as a service. This model allows even the least skilled adversaries to incorporate the malware into their arsenal, without the need to develop their own.

In most cases, developers offer one of the three types of malware: loaders, RATs, or stealers. In rare cases, the software includes the functionalities of all the three types at once.

With the malware-as-a-service model, the attackers are able to target even large organizations and conduct post-exploitation, often by uploading additional components, such as payloads of popular frameworks.

The attackers also often use this malware to collect authentication data for whatever purpose, one of which is to sell it. See the case with Leak Wolf,[1] which targeted authentication data with the RedLine stealer.

The underground forum community tends to prohibit the use of such malware for attacks in Russia and other CIS countries. However, buyers can modify it. As a result, attacks with the use of software purchased on underground forums are becoming commonplace. In addition, geopolitical events have an impact on underground forums: in some cases, sellers no longer impose any restrictions.

In this research, we will look at seven popular malware families that have already been weaponized against more than 100,000 companies. We will explain how these tools are sold in the dark segment of the Internet and will explore the tactics, techniques, and procedures of the adversaries.

1. "A BI.ZONE study of malware-free attacks by Leak Wolf," *BI.ZONE*.

Agent Tesla

The Agent Tesla malware appeared in 2014. Its developer marketed the tool as legitimate software for monitoring personal computers, yet this did not prevent malicious actors from employing it in both mass and targeted attacks. The malware was sold through the developer's official website `agenttesla[.]com` (fig. 1).

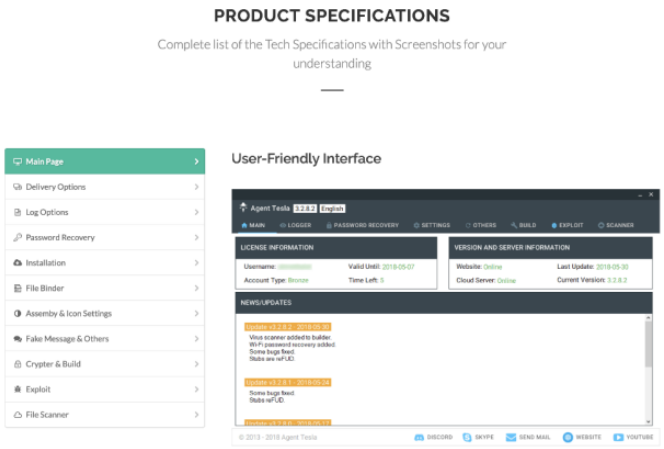


Fig. 1. The website that sold Agent Tesla

The website operated until 2018, at which time a subscription cost between $15 and $69 depending on the term. As of the report date (October 2023), the developer offers the product only to a limited number of customers. However, some offers can reach about $500 for the latest version with a full set of features, annual updates, and support (fig. 2).

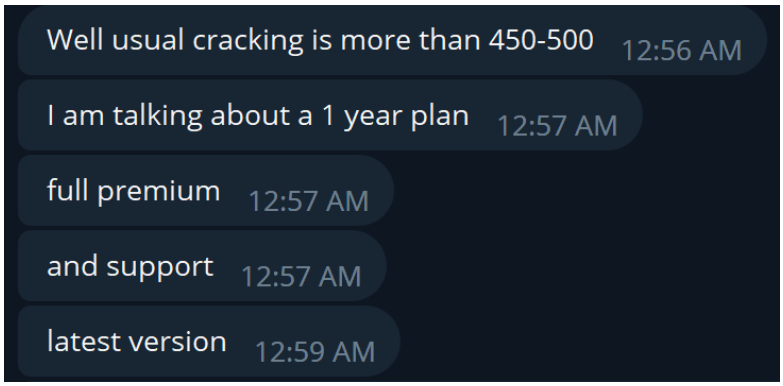


Fig. 2. Chat with the vendor of the cracked Agent Tesla versions in Telegram

A free cracked version, dated around 2020, is also circulating on underground forums (fig. 3).

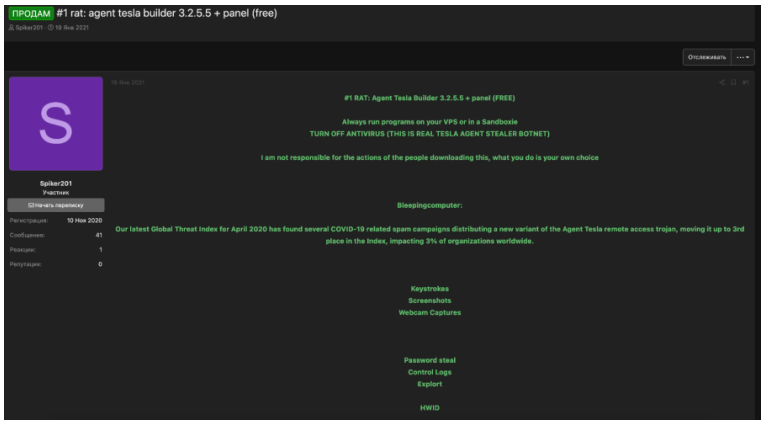


Fig. 3. Forum thread with the free version of Agent Tesla

Channels of distribution

Agent Tesla is most often distributed via phishing emails with malicious attachments disguised as agreements, invoices, scanned documents, etc. (fig. 4). For example, phishing emails in 2023 had the following subject lines:

- Business proposal request
- New purchase order
- Supplemental agreement
- Shipping information
- See invoice paid today

Because of their wide circulation, the attached files, whether archived or not, can range in formats: `.doc`, `.xls`, `.exe`, `.scr`, `.vbs`, `.js`, `.one`.

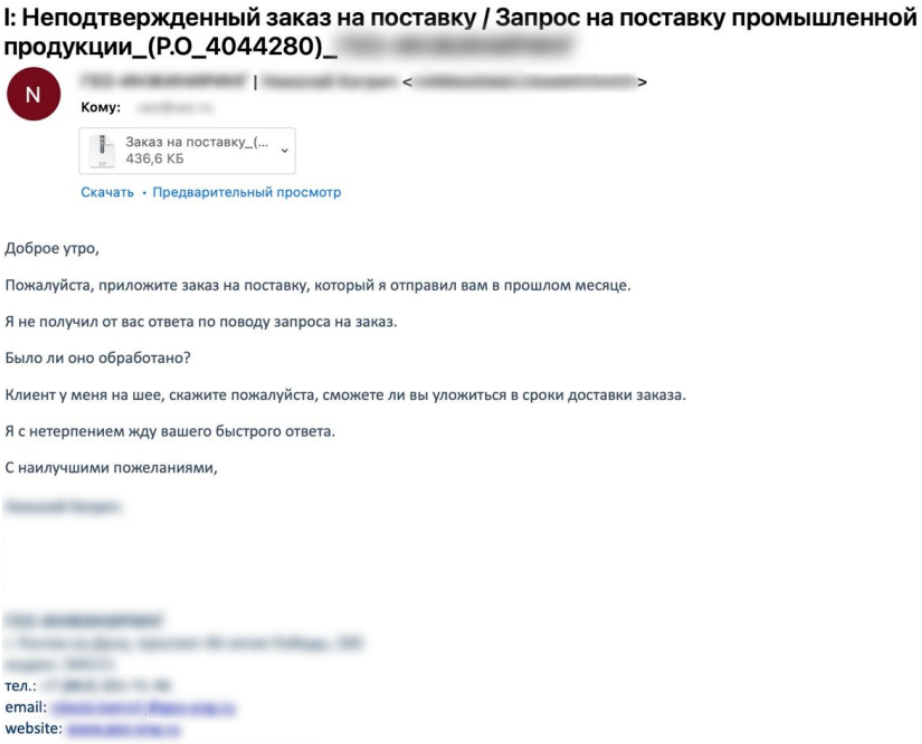


Fig. 4. Phishing email from Agent Tesla targeting Russian real estate developers

While the attackers used Microsoft Office documents and tables to deliver Agent Tesla, the malicious code was executed by exploiting the CVE-2017-11882 and CVE-2018-0802 vulnerabilities. When an attached document or table was opened and one of the vulnerabilities was successfully exploited, `EQNEDT32.EXE` executed a malicious code that downloaded and launched an instance of Agent Tesla on the compromised system.

OneNote (`.one`) notes merit special attention. They have also begun to appear in attacks, including those aimed at spreading Agent Tesla. Such files prompt the victim to click a button to view the protected content of a note. Sure enough, Agent Tesla is then downloaded using PowerShell or similar programs (fig. 5).

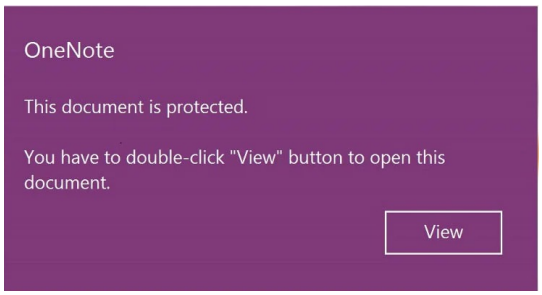


Fig. 5. OneNote with malicious content

Attackers also made ample use of SEO poisoning, redirecting victims to websites with malware disguised as legitimate software. Agent Tesla was masqueraded as Galaxy Swapper, OBS Studio, Onion Browser, Brave Wallet, LastPass, AnyDesk, and even as MSI Afterburner (fig. 6).

To convince users to download the malicious file, Agent Tesla operators disguised it as a familiar legitimate program

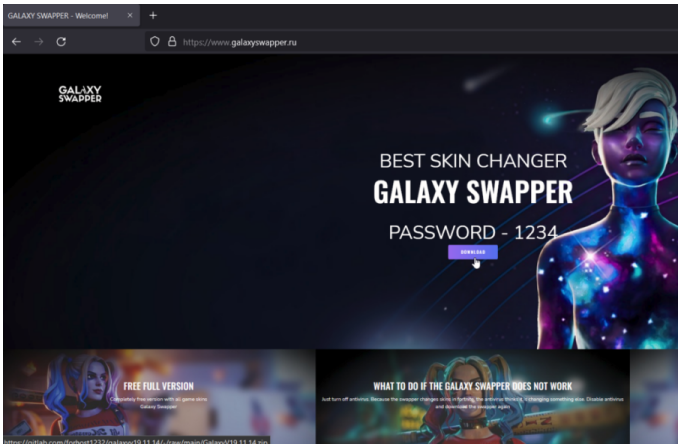


Fig. 6. The phishing website from which Agent Tesla was downloaded

Features

Agent Tesla operators make heavy use of packagers that allow the malware to be installed through multiple download stages. They also ensure that virtualization and debugging tools are not employed.

The malware is moved to a created folder inside AppData. The folder and all the files inside are assigned ReadOnly, Hidden, System, NotContextIndexed attributes. With these attributes, the folder will not be visible even if the user has *Show hidden files* enabled. Agent Tesla then changes the access permissions for the folder, allowing ReadOnly and ExecuteOnly access while preventing Windows tools from deleting, overwriting, and changing attributes and ownership.

The attackers changed the attributes so that the folder with the malware would not be visible even if *Show hidden files* was enabled

Agent Tesla relies on PowerShell to bypass defenses. For example, it is used to add the working directory of an executable to the Windows Defender exclusion:

```
powershell.exe Add-MpPreferenceExclusionPath
\[folder where the Agent Tesla executable is
located]
```

Agent Tesla can inject payloads into the memory of legitimate processes, including those using Process Hollowing techniques such as `MSBuild.exe`, `vbc.exe`, `RegSvcs.exe` or others if specified in the configuration. Deployment is done in sections rather than as a whole file so that security tools cannot detect an executable file in the memory of another process.

To ensure persistence in the compromised system, Agent Tesla creates a task in the Windows Scheduler:

```
schtasks.exe /Create /TN "Updates" /XML
"[path to the temporary XML file]"
```

The XML file contains information about the startup parameters, for example, when logging in, waking from sleep mode, terminating alongside a running process, and the maximum priority of the task.

As an additional method of gaining persistence in a compromised system, Agent Tesla modifies the following registry sections:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKCU\Software\Microsoft\Windows\CurrentVersion\
Explorer\Startup Approved\Run
```

Agent Tesla accesses the stored user authentication data from browsers similar to Chromium and Firefox: Brave, Yandex, WaterFox, and others. Furthermore, Agent Tesla can intercept keystrokes, create screenshots and send them to a C2 server at regular intervals (20 seconds by default).

The C2 servers for Agent Tesla can be FTP and HTTP servers as well as a bot in Telegram, which can be interacted with through a token.

FormBook

FormBook was first discovered in 2016. Many cybercriminals use this tool to launch attacks on various industries: finance, healthcare, manufacturing, public sector, and others.

On underground forums, FormBook was marketed as a formgrabber that could retrieve stored data from Edge, Firefox, Chrome, Internet Explorer, Outlook, Thunderbird, intercept traffic, and record keystrokes.

At the end of 2018, sales of FormBook stopped because the developer did not want the tool to be used in phishing emails. At the time of writing, only the cracked version of FormBook is freely available (fig. 7).

The developers of FormBook were against its use in phishing emails and even revoked the licenses of those who used their product this way

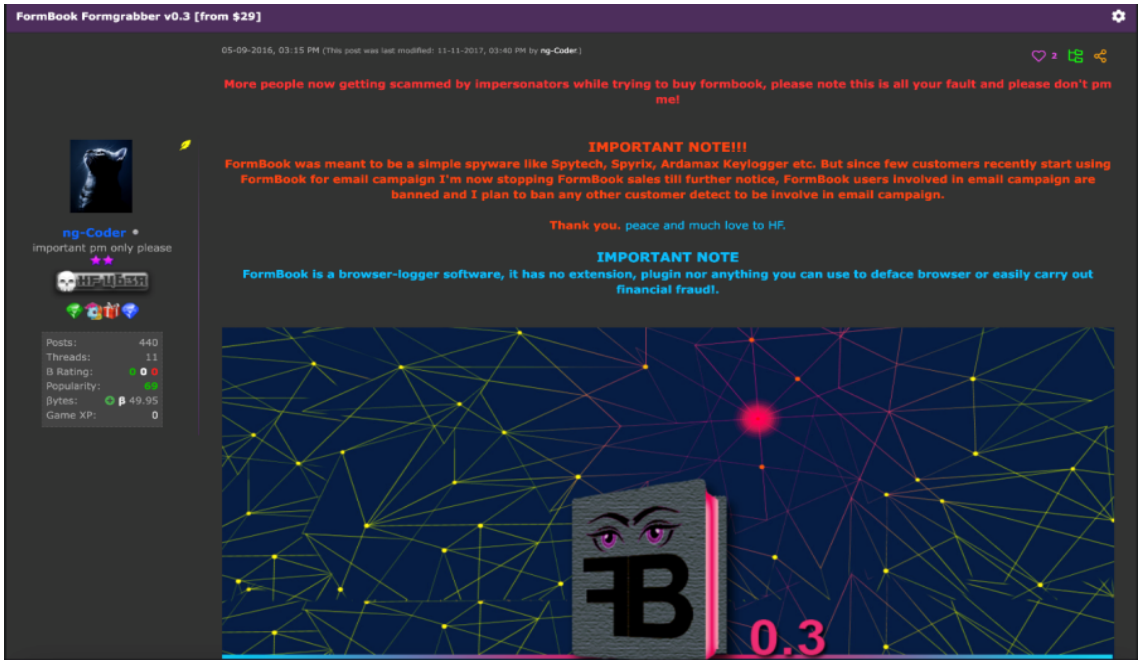


Fig. 7. Thread with FormBook for sale on an underground forum

Channels of distribution

The primary method of FormBook distribution is phishing emails. As in the case of Agent Tesla, archived executable files (including those disguised as PDFs and other documents) as well as non-archived malicious documents and tables can be used to deliver this malware (fig. 8). The CVE-2017-11882 and CVE-2018-0802 vulnerabilities are exploited to execute the malicious code on the target system.

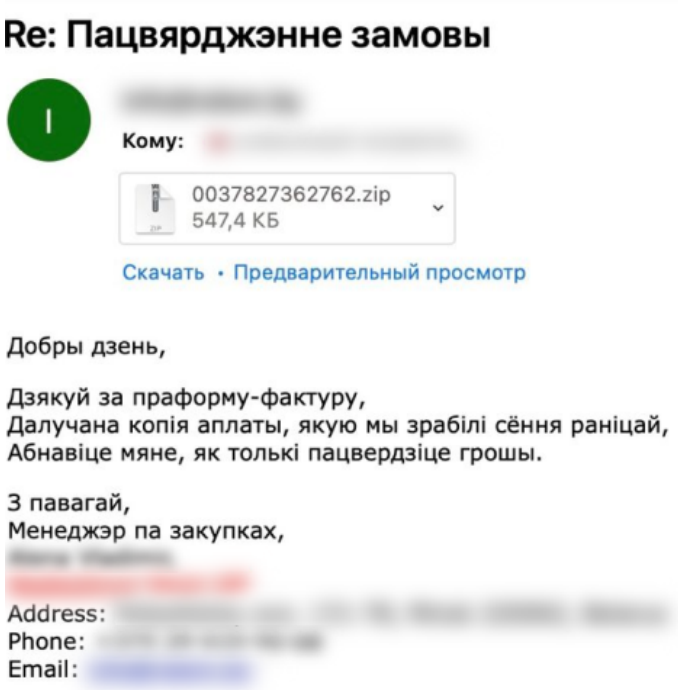


Fig. 8. Phishing email with FormBook in the attached archive

In addition to phishing emails, FormBook was also spread through SEO poisoning. For example, in one campaign, the attackers used the MalVirt loader and malicious ads disguised as websites for downloading Blender 3D (fig. 9).

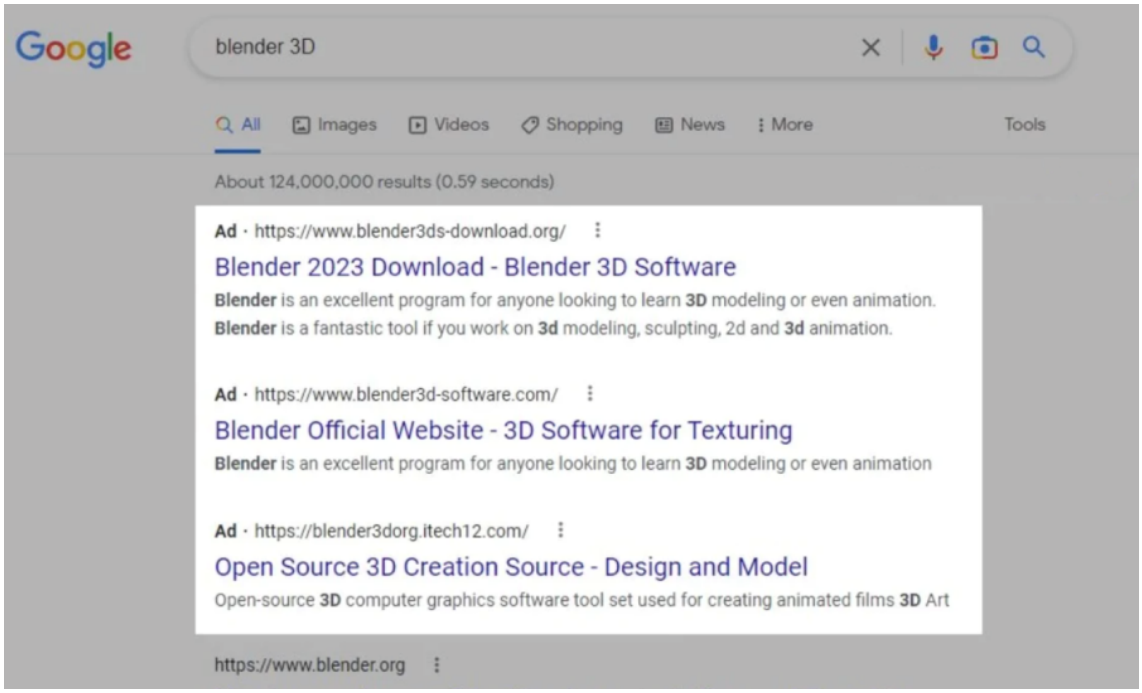


Fig. 9. Malicious sites distributing FormBook through search engine poisoning

Notably, FormBook was also leveraged by state-sponsored groups. Attackers used various types of attachments to deliver the malware: `.xlsx`, `.shtml`, `.doc`, `.xlsm`, `.jar`, `.lnk` и `.cmg`, with `.xlsm` being the most common. The group sent phishing emails on behalf of the Estonian Ministry of Foreign Affairs, the Ministry of Defense of Ukraine, and even the administrator of mil.gov.ua.

FormBook has been exploited both for financial gains and for espionage purposes

Features

To gain persistence in a compromised system, FormBook can, among other things, create tasks in the scheduler:

```
"C:\Windows\System32\schtasks.exe" /Create /TN
"Updates\lVOVDVOZXdPgss" /XML "C:\Users\admin\
 AppData\Local\Temp\tmp5D3B.tmp"
```

Persistence is ensured by modifying the following sections of the registry:

```
(HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\
Run
```

```
(HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\
Policies\Explorer\Run
```

FormBook can inject payloads into the memory of more than 20 processes, such as `svchost.exe` or `msiexec.exe`.

The malware collects the following data:

- credit card numbers
- bank account numbers
- email addresses
- screenshots (e.g., user interaction with a banking application)
- keystrokes
- clipboard activity capture

The stealer gathers this information from sources such as:

- browsers
- mail clients
- file managers
- remote desktop clients
- FTP clients

FormBook can execute the following commands from the C2 server:

- additional files download, including malicious ones
- process management
- device power management
- additional files upload from an infected host

RedLine

Having appeared on underground forums in 2020, the RedLine stealer sells for $150 per month or up to $900 for the unlimited use (fig. 10).

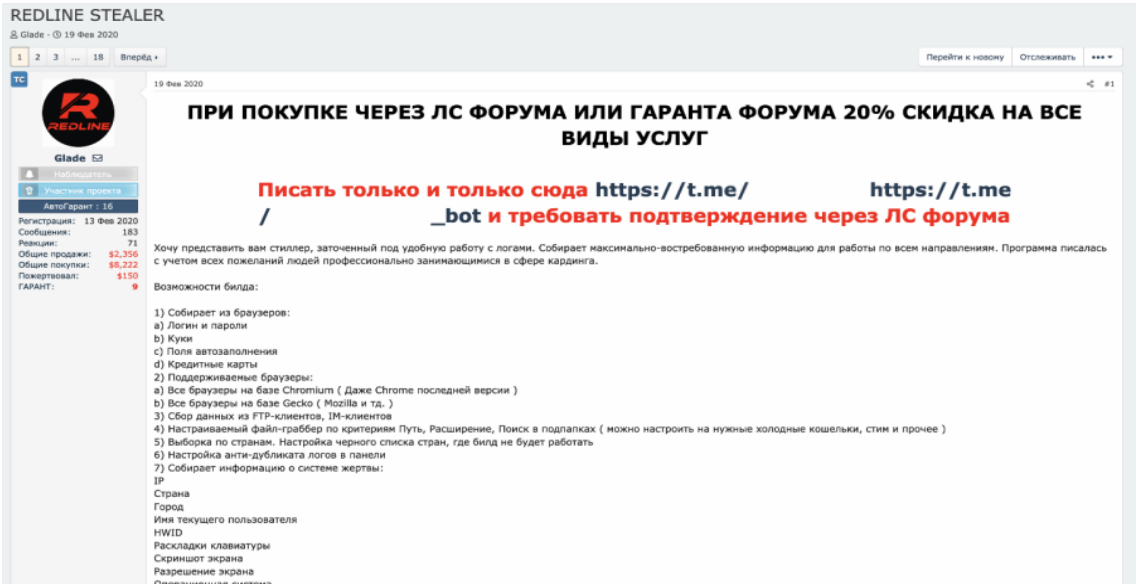


Fig. 10. Thread dedicated to RedLine on an underground forum

In addition to official offers in the dark segment, there are ads for resale of a lifetime license for $500. This is a way for criminals to obtain the malware, bypassing the official vendor (fig. 11).

Malicious actors do not buy RedLine for their own use only, they also resell it to others

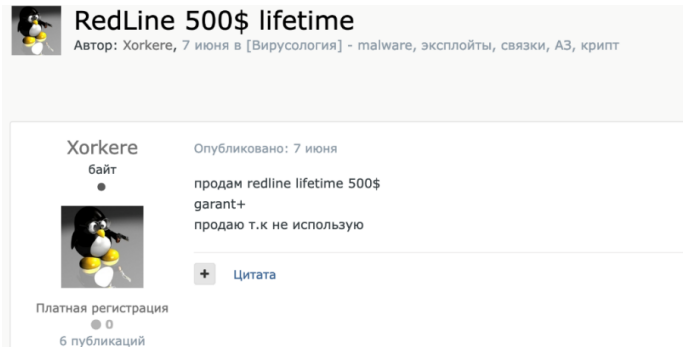


Fig. 11. RedLine lifetime license resale ad

Channels of distribution

Like previous tools, RedLine spreads through phishing emails as well as search engine poisoning.

For example, the stealer was disguised as Lightshot, a tool for taking screenshots (fig. 12).

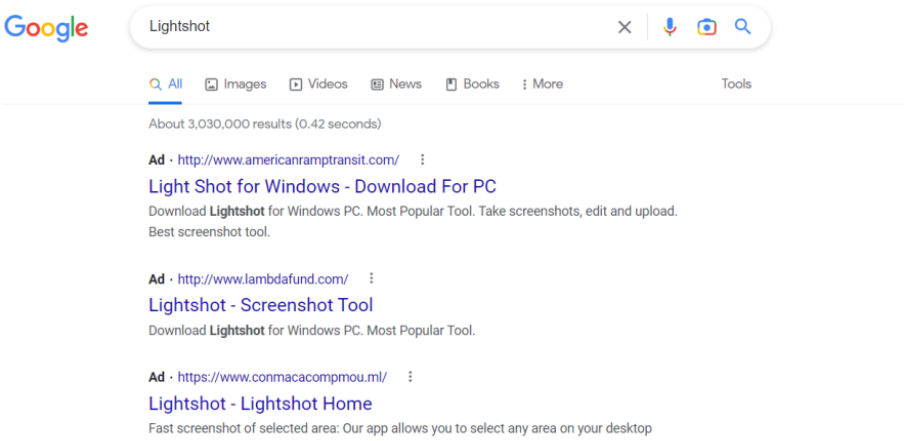


Fig. 12. RedLine distribution under the guise of Lightshot software

The RedLine payload was stored in the Bitbucket repository and was downloaded at least 2,500 times.

As the topic of artificial intelligence is becoming increasingly popular, attackers began using it as bait in Google ads. In this case, the RedLine installer masqueraded as DALL-E, MidJourney, and ChatGPT (fig. 13).

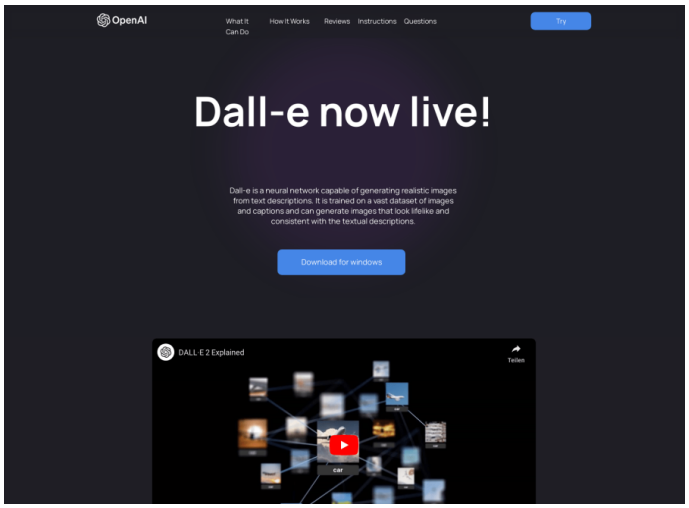


Fig. 13. Phishing website from which the malicious RedLine file is downloaded

Running the downloaded file prompts a fake installation window of the tool (for which there is no desktop version) and the execution of malicious code. Interestingly, if the website is visited from a blocked IP address (e.g., of a search bot) or by manually entering the URL, it redirects to a legitimate domain.

RedLine was also distributed under the guise of the NPM package manager. The source of the stealer download was a fraudulent channel in Telegram, which purportedly provided software to customize graphics cards for mining. This campaign targeted Russian developers.

Features

RedLine activity can be detected when processing network connections. The stealer uses C# DataFactory. This causes strings to appear in the traffic, which contain access endpoints as well as authorization and DataFactory protocol data (i.e., the string http://tempuri.org/). RedLine can also be traced by a query to https://api.ip.sb/ip, which is used to obtain information about the IP address of the compromised device.

Similar to Agent Tesla, RedLine injects the payload into the address space of another process, such as `vbc.exe`.

RedLine sends WMI queries to retrieve information about the system and its hardware, such as CPU, graphic card, and installed security tools:

```
SELECT * FROM Win32_Processor
SELECT * FROM Win32_VideoController
SELECT * FROM AntivirusProduct
```

Furthermore, the stealer collects information about installed applications and browsers to retrieve credentials, bookmarks, cookies, and search history. It can obtain data from FTP clients, such as FileZilla, and installed VPN services, like NordVPN and ProtonVPN. The stealer can also dump files from a compromised device that match the masks set by the attackers.

There are many channels available on Telegram that offer to download stealer logs. Most of these channels publish several log archives per week—these are logs of the RedLine stealer and its copies, such as Meta. These channels also offer commercial access to private logs. Prices for private access start at $40 per week and go up to $3,000 for lifetime access.

Malicious actors do not need to use the stealers by themselves: they can buy the logs collected by such malware and obtain compromised accounts

DarkCrystal

A modular trojan written in C# that has been selling on underground forums since 2019. There is a group dedicated to it on Telegram where they publish news and updates. The trojan is provided on subscription: when purchasing, the user receives a builder and a separate server to manage infected devices (fig. 14).

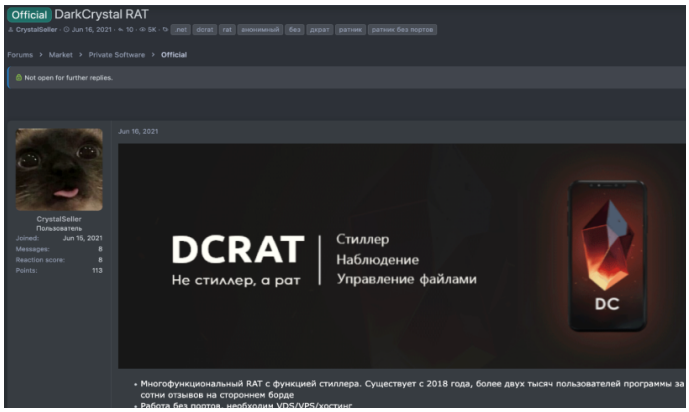


Fig. 14. Thread on one of the underground forums dedicated to DarkCrystal

There are also offers to sell the cracked version starting at ₽299 per month (fig. 15).

Threat actors can expand their arsenal with DarkCrystal for as little as ₽299

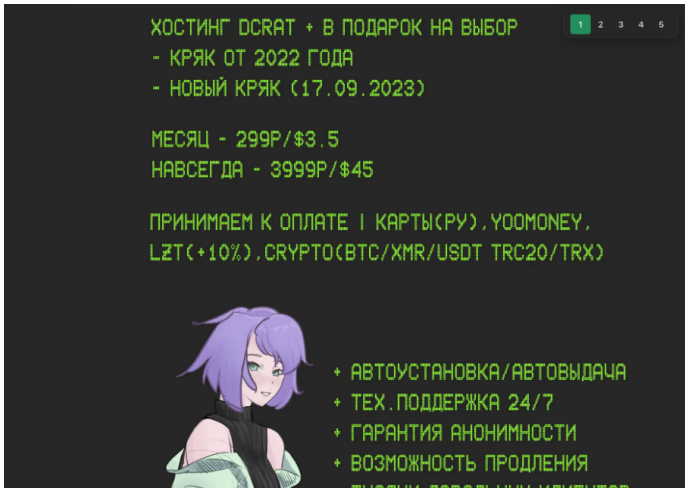


Fig. 15. Cracked version of DarkCrystal for sale ad

It is important to note that many researchers do not differentiate between DCRAT and DarkCrystal. However, this can cause confusion as there is another trojan named DcRat in open sources that has nothing to do with DarkCrystal (fig. 16). To avoid mixing the two, we will introduce the following distinction:

- DcRat, an open-source trojan available in the GitHub repository
- DarkCrystal, a trojan sold on the underground forums that we talk about here

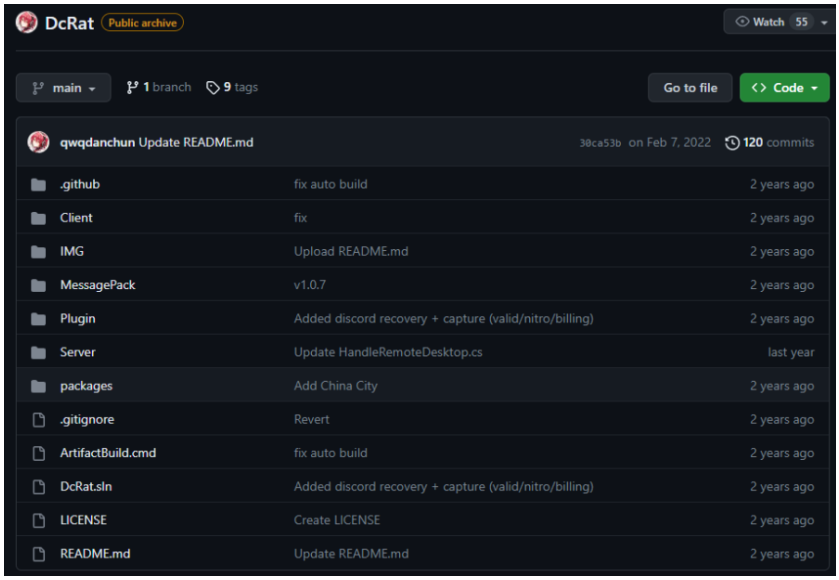


Fig. 16. DcRat trojan source code (not DarkCrystal) on GitHub

Channels of distribution

Further proliferation of DarkCrystal is achieved by phishing. For example, in June 2023, the attackers actively exploited the topic of mobilization.

However, there are also more interesting methods. For instance, the attackers were spreading the trojan masked as an archive with exclusive photos of the porn actress Mia Khalifa. Sure enough, instead of photos, the archive contained a VBScript downloaded by DarkCrystal.

Another example is a phishing webpage mimicking the Kaspersky website that offered a free download of antivirus software. Instead, the visitors downloaded the DarkCrystal malware archive (fig. 17).

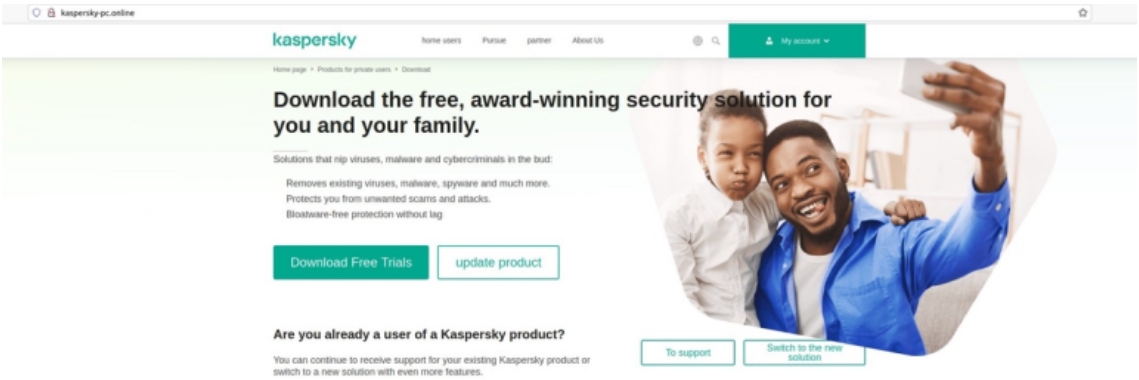


Fig. 17. Phishing page kaspersky-pc.online

The attackers also distributed DarkCrystal with the help of a modified version of the Steam Desktop Authenticator application (https://github.com/Jessecar96/SteamDesktopAuthenticator/). They applied two methods at the same time to make the application look as legitimate as possible:

- cloned the original repository, including HTML, CSS, JavaScript, PHP codes, etc.
- registered domains similar to the original one

The phishing links looked as follows:

```
https://gthub.org/Jessecar96/SteamDesktopAuthenticator/
releases/download/1.0.10/SDA-1.0.10.zip

http://glthub.org/jessecar96/steamdesktopauthenticator/
releases/download/1.0.10/sda-1.0.10.zip

https://gllthub.com/Jessecar96/
SteamDesktopAuthenticator/releases/download/1.0.10/sda-
1.0.10.zip
```

There are also known cases of DarkCrystal being spread via unlicensed versions of Microsoft Office 2019. The sample was obtained from the Torrent Toloka tracker (https://toloka.to/t661196), as a BitTorrent file named `Microsoft.Office-x64.v2019.x.iso.torrent`. As a result, it installed the software with a trojan that can mimic other applications.

Features

To keep a low profile, DarkCrystal creates a subfolder in the folder with some legitimate software installed on the compromised system

During the first startup, DarkCrystal selects a random process from those running on the system and moves its files to its own directory. For example, if the selected process is `Code.exe` located in the directory `C:\Users\[user]\AppData\Local\Programs\Microsoft VS Code`, the trojan will create a folder in that directory with a name identical to the process name (in this case, `Code`), move the executable file into it, and name it the same as the selected process (`Code.exe`). The final path to the installed file will be `C:\Users\[user]\AppData\Local\Programs\Microsoft VS Code\Code\Code.exe`.

To find out where the installation was done, you can check:

- registry hive `HKCU\Software [sha1 from the name of mutex, version, and tag]`
- file `C:\Users\[user]\AppData\Local\Temp\tmp[5 first 5 characters from sha1 from version, and tag].tmp`
- file `C:\Users\[user]\AppData\Local\Temp\[sha1 from mutex name][version][tag][sha1 from mutex name and "builds" string]`

DarkCrystal uses the following to gain persistence in a compromised system:

- Task scheduler:

```
schtasks.exe /create /tn "[executable file
name][first character of file name]" /sc
MINUTE /mo [random string from 1 to 15] /tr
"[path to executable file]" /f

schtasks.exe /create /tn "[executable file
name]" /sc ONLOGON /tr "[path to executable
file]" /rl HIGHEST /f

schtasks.exe /create /tn "[executable file
name][first character of file name]" /sc
MINUTE /mo [random string from 1 to 15] /tr
"[path to executable file]" /rl HIGHEST /f
```

- Autoload by modifying the registry:

```
HKCU\Software\Microsoft\Windows\
CurrentVersion\Run

HKLM\Software\Microsoft\Windows\
CurrentVersion\Run

HKLM\Software\Microsoft\Windows NT\
CurrentVersion\Winlogon
```

The main module can only collect basic system information such as username, location (https://ipinfo.io/json), camera and microphone availability, and basic information about Steam, Discord, and Telegram applications.

Modules selected by the attackers in the builder are downloaded from the C2 server during execution, allowing them to control the vector of interaction with the compromised device. Encrypted modules can be downloaded from the DarkCrystal distribution server specified in the Telegram group.

White Snake

We already spoke about the distribution of White Snake[2] under the pretense of a request from Roskomnadzor (Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media). After our research, the thread selling White Snake was blocked on a popular underground forum and the developer was suspended because of the attacks on Russian organizations. This was reported by the developer of White Snake in its Telegram channel (fig. 18).

The rules set by the developers are not always observed: some of the White Snake clients have attacked Russian organizations despite the prohibition

Fig. 18. Official White Snake channel post

At the time of writing the report, the thread and the developer are still blocked on the forum. The stealer is distributed via a Telegram bot. The sales start at $140 per month and can reach up to $1,950 for a lifetime license (fig. 19).

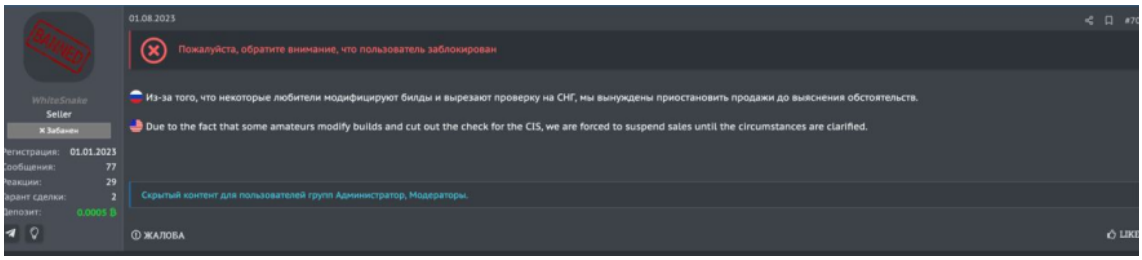


Fig. 19. White Snake developer account suspension information

2. "White Snake is weaponized against Russian companies," *BI.ZONE*.

Channels of distribution

As part of the campaign, the victim would receive a phishing email that had an archive with several files attached:

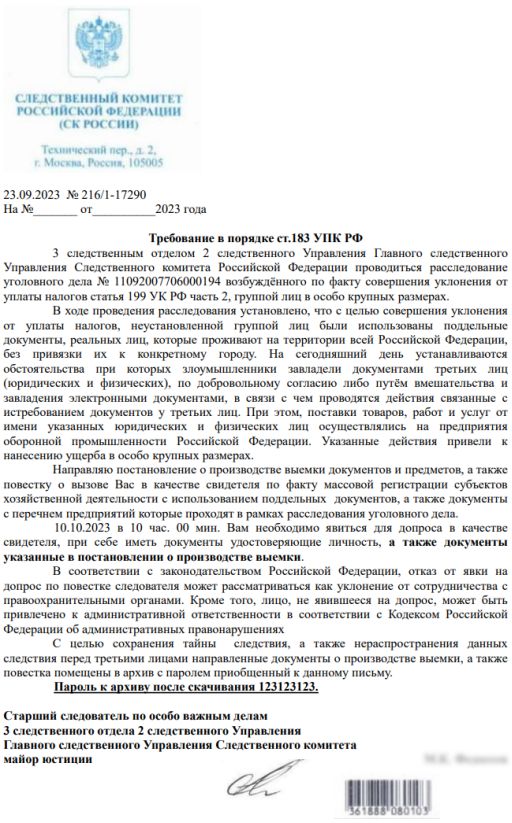
`Требование РОСКОМНАДЗОР № 02-12143.odt`
(Roskomnadzor requirement)

`Приложение к требованию РОСКОМНАДЗОРА`
(attachment to the Roskomnadzor requirement)

`РОСКОМНАДЗОР.png`

The first file is a phishing document intended to distract the victim and provide false confidence that the second file, which is a White Snake stealer, is safe.

The attackers also carried out a phishing campaign on behalf of the Investigative Committee of the Russian Federation. The file `Запрос следователя (уклонение от уплаты налогов) – копия.pdf` (a file dealing with tax evasion) designed to divert the victim's attention, stated that the recipient should appear for questioning as a witness in a case involving forged documents (fig. 20).



СЛЕДСТВЕННЫЙ КОМИТЕТ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(СК РОССИИ)

Технический пер., д. 2,
г. Москва, Россия, 105005

23.09.2023 № 216/1-17290
На №_____ от_____2023 года

Требование в порядке ст.183 УПК РФ

3 следственным отделом 2 следственного Управления Главного следственного Управления Следственного комитета Российской Федерации проводиться расследование уголовного дела № 11092007706000194 возбуждённого по факту совершения уклонения от уплаты налогов статья 199 УК РФ часть 2, группой лиц в особо крупных размерах.

В ходе проведения расследования установлено, что с целью совершения уклонения от уплаты налогов, неустановленной группой лиц были использованы поддельные документы, реальных лиц, которые проживают на территории всей Российской Федерации, без привязки их к конкретному городу. На сегодняшний день устанавливаются обстоятельства при которых злоумышленники завладели документами третьих лиц (юридических и физических), по добровольному согласию либо путём вмешательства и завладения электронными документами, в связи с чем проводятся действия связанные с истребованием документов у третьих лиц. При этом, поставки товаров, работ и услуг от имени указанных юридических и физических лиц осуществлялись на предприятия оборонной промышленности Российской Федерации. Указанные действия привели к нанесению ущерба в особо крупных размерах.

Направляю постановление о производстве выемки документов и предметов, а также повестку о вызове Вас в качестве свидетеля по факту массовой регистрации субъектов хозяйственной деятельности с использованием поддельных документов, а также документы с перечнем предприятий которые проходят в рамках расследования уголовного дела.

10.10.2023 в 10 час. 00 мин. Вам необходимо явиться для допроса в качестве свидетеля, при себе иметь документы удостоверяющие личность, **а также документы указанные в постановлении о производстве выемки**.

В соответствии с законодательством Российской Федерации, отказ от явки на допрос по повестке следователя может рассматриваться как уклонение от сотрудничества с правоохранительными органами. Кроме того, лицо, не явившееся на допрос, может быть привлечено к административной ответственности в соответствии с Кодексом Российской Федерации об административных правонарушениях

С целью сохранения тайны следствия, а также нераспространения данных следствия перед третьими лицами направленные документы о производстве выемки, а также повестка помещены в архив с паролем приобщенный к данному письму.

Пароль к архиву после скачивания 123123123.

Старший следователь по особо важным делам
3 следственного отдела 2 следственного Управления
Главного следственного Управления Следственного комитета
майор юстиции

Fig. 20. The diversion document

In addition to this file, there was an archive with the White Snake stealer `Перечень юридических лиц и предприятий, уклонение от уплаты налогов, требования и дополнительные материалы.exe`. (list of legal entities and enterprises, tax evasion, requirements, and additional materials).

The attackers also targeted developers who worked with packages from PyPI repositories. White Snake was detected in the following packages: aeodatav04, aeodata, testwhitesnake, testwhitesnake123a, testwhitesnakemodule, test24234, test23414234234, test-23234231, tiktokthon, androidspyeye, support-dev, support-hub, social-checker, scrappers, aeivasta, scrappers-dev, detection-telegram, parser-scrapper, pandirequests, panderequests, libidrequest, and pandarequest.

Features

Here are the key performance features of White Snake:

- initialization of the Tor network node to enable communication between the C2 server and the compromised device takes place
- creation of malware copies on external media and in the autoload directory of other system users
- retrieval of the country and IP address of the device through a query to http://ip-api.com/line?fields=query,country

White Snake infects not only compromised systems but also connected external drives

White Snake collects credentials from Chromium and Firefox-like browsers, files such as documents, and registry data. In addition, it can record the screen, execute commands, and download additional malware.

DarkGate

DarkGate was first used in 2018 in campaigns to compromise systems for the purpose of cryptocurrency mining and ransomware. Five years later, in June 2023, DarkGate appeared on underground forums as a tool for carrying out sophisticated cyberattacks (fig. 21).

The price for the tool set by the developer is higher than the market with strict limits on the number of available licenses. There are several subscription options, and payment can be made in cryptocurrencies. A one-day lease costs $1,000, and this option is single-use. A monthly lease is priced at $15,000.

DarkGate is designed for sophisticated attacks: the license costs $15,000 per month

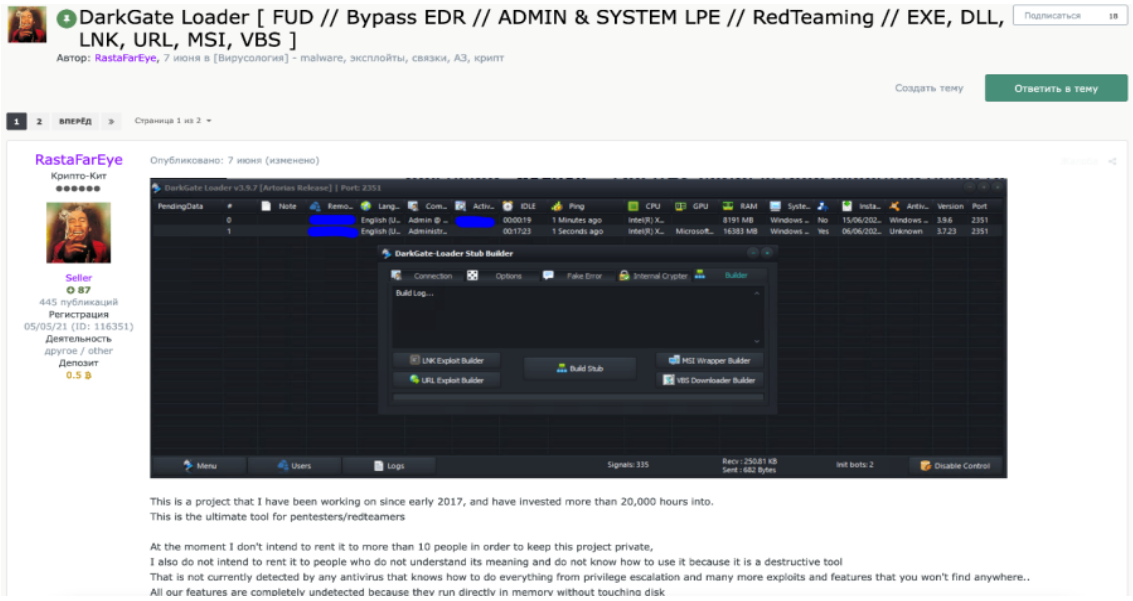


Fig. 21. DarkGate sales offer

By purchasing DarkGate, the buyer also receives a builder and a packager. The builder allows the user to create an LNK file (shortcut) with any settings, which will load the payload from the C2 server. Additionally, a VBS loader can be purchased, as well as the developer-recommended AU3+MSI compiler, which promises fast and stealthy deployment of malware on a compromised system.

Channels of distribution

The main way to distribute DarkGate is through phishing emails, both with malicious attachments and links.

It is worth noting that the attackers continue to experiment with phishing formats and look for new distribution methods. For example, they leveraged the Microsoft Teams corporate messenger to deliver malicious files.

The attack was initiated by several compromised Office365 accounts that sent out phishing emails to corporate addresses of employees at various organizations via Microsoft Teams chats. It is interesting that both accounts were compromised in advance and purchased presumably on the darknet. The sent messages had the same content: they used HR-related topics, offering recipients a link to download a ZIP file `Changes to the vacation schedule` (fig. 22).

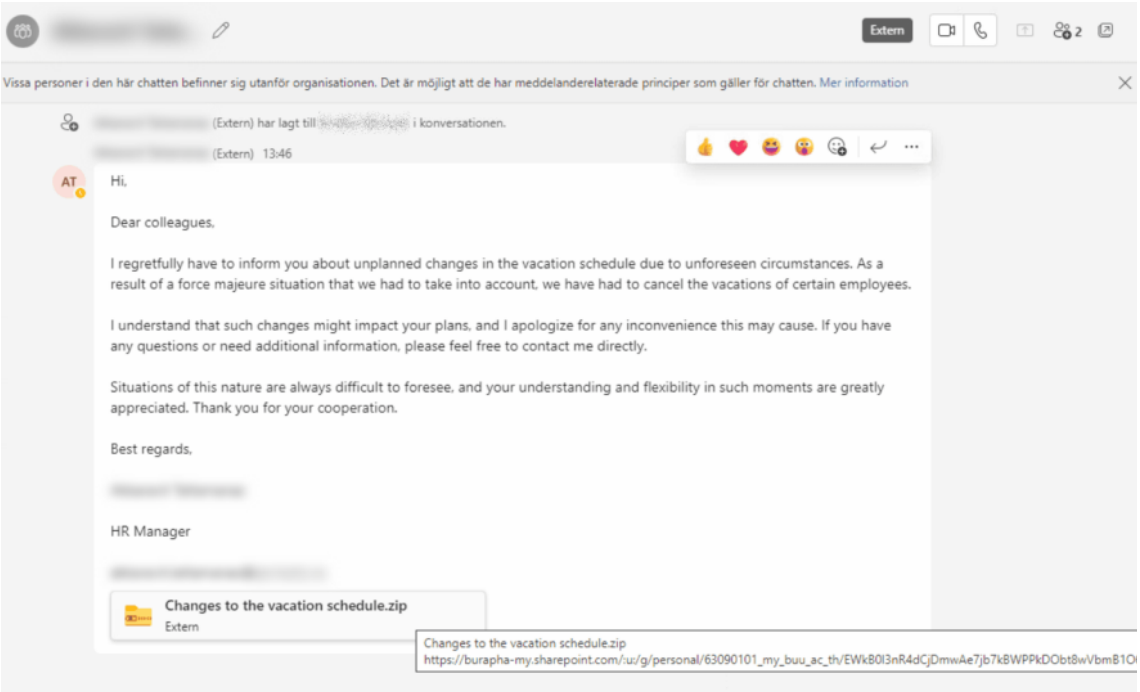


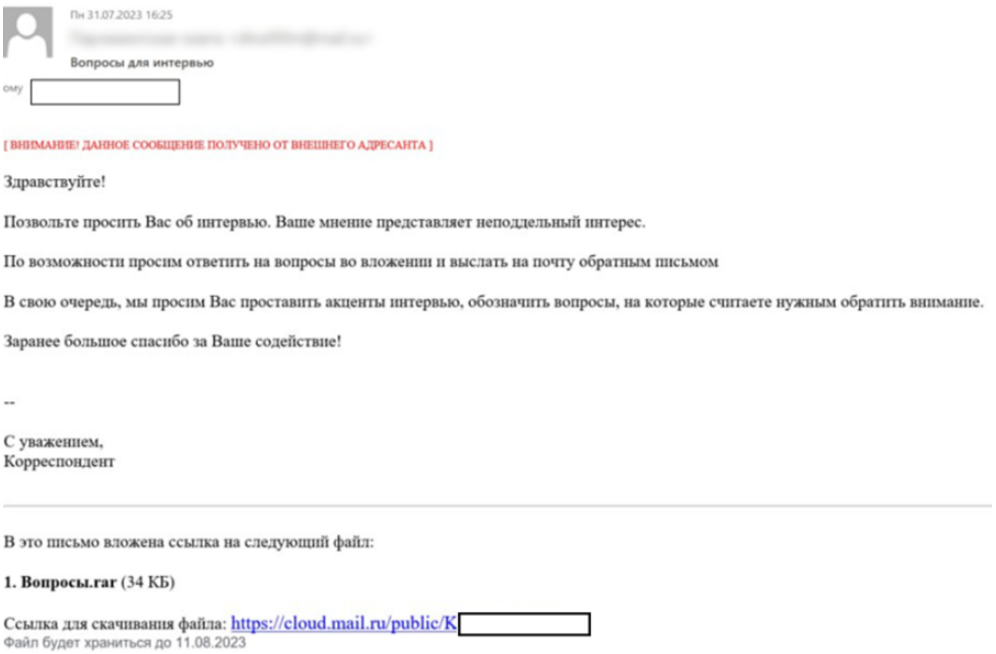
Fig. 22. DarkGate mailing using Microsoft Teams

When the victim clicked the URL, they were redirected to SharePoint that contained the above ZIP file. Inside the archive, was an LNK file masquerading as a PDF document, which, when launched, downloaded the payload from the C2 server.

The attacks on Russian organizations were mainly phishing emails. For example, adversaries tended to attach encrypted archives containing an obfuscated VBScript that launched the DarkGate installation (fig. 23).

The following email subject lines and file names were used in attacks against Russian companies:

- Subject: List of questions received from the editorial office for the preparation of the interview. File name: `Перечень вопросов, поступивших из редакции для подготовки интервью 31_07_2023.vbs`. (list of questions received from the editorial staff for the preparation of the interview)
- Subject: Request for MTPL insurance forms. File name: `osago_blanki.vbs`
- Subject: Please familiarize yourself with the latest changes
- Subject: Interview questions



Пн 31.07.2023 16:25

Вопросы для интервью

кому

[ВНИМАНИЕ! ДАННОЕ СООБЩЕНИЕ ПОЛУЧЕНО ОТ ВНЕШНЕГО АДРЕСАНТА]

Здравствуйте!

Позвольте просить Вас об интервью. Ваше мнение представляет неподдельный интерес.

По возможности просим ответить на вопросы во вложении и выслать на почту обратным письмом

В свою очередь, мы просим Вас проставить акценты интервью, обозначить вопросы, на которые считаете нужным обратить внимание.

Заранее большое спасибо за Ваше содействие!

--

С уважением,
Корреспондент

В это письмо вложена ссылка на следующий файл:

1. Вопросы.rar (34 КБ)

Ссылка для скачивания файла: https://cloud.mail.ru/public/K

Файл будет храниться до 11.08.2023

Fig. 23. Phishing email containing the link to download the DarkGate loader

Features

DarkGate creates a key in a registry hive for autoloading and then creates a flow that periodically checks active processes for monitoring tools. If such a tool is found, DarkGate removes all traces of its activity on the system until the tool monitoring process terminates.

DarkGate launches the suspended `cmd.exe` process and injects malicious shellcode into its address space. The shellcode is responsible for communicating with the C2 server and executing commands.

To download additional files sent by the attacker, DarkGate can use nodes on the Torrent network. DarkGate also has stealer functionality:

- steals user credentials from browsers, cryptocurrency wallets, Telegram, and Discord
- intercepts keystrokes
- collects system data, such as installed antivirus software versions, user and device names

In addition, DarkGate can manage device files, processes and power, install a proxy server and malicious browser extensions, utilize the Remote Desktop Protocol and install a miner on the compromised device.

Snake Keylogger

Snake Keylogger (also known as 404 Keylogger) was first spotted on a popular forum in May 2019, where it was introduced as a tool that allows adversaries to spy on users in real time. Subscription prices for Snake Keylogger range from $40 per month to $195 per six months. Payments can be made in cryptocurrency or as a PayPal transfer (fig. 24).

Not all threat actors deal solely in cryptocurrency. The Snake Keylogger developer also accepted PayPal transfers

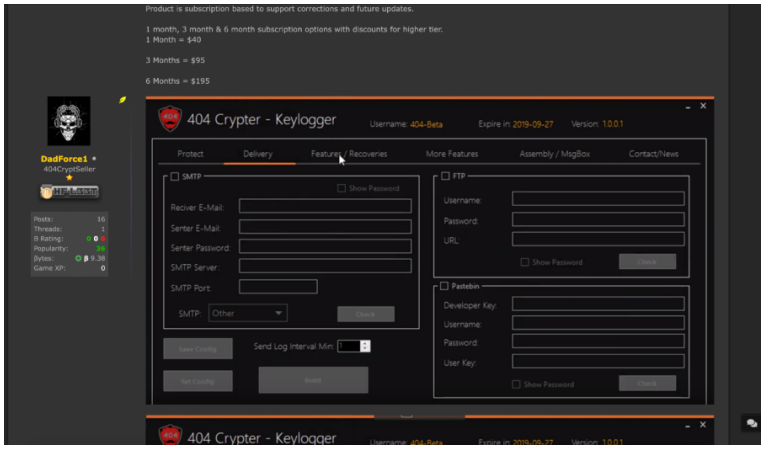


Fig. 24. Post about the sale of Snake Keylogger on one of the forums

At the time of writing, the source code and some modifictions of one of the stealer's early version are in the public domain (fig. 25).

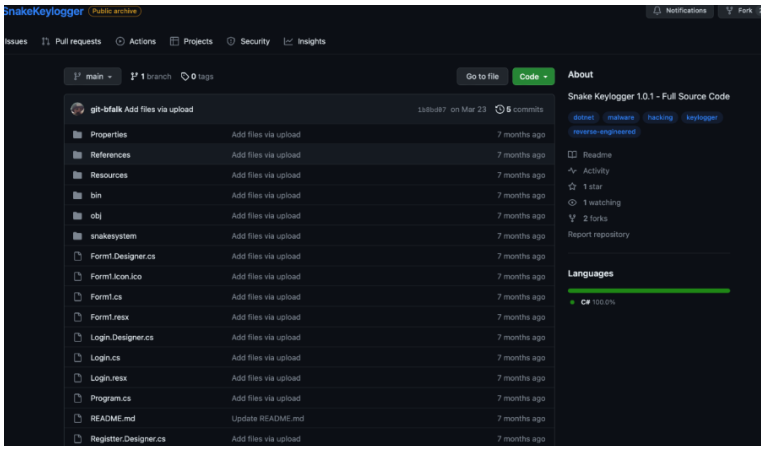


Fig. 25. Source code repository on GitHub

Channels of distribution

The primary method of Snake Keylogger distribution is phishing emails with malicious attachments, most often archives. Attacks can be aimed at both ordinary users and predetermined targets: specific individuals or organizations.

In 2023, the threat actors used predominantly English language email subject lines and file names. They typically included words such as quote, purchase order, invoice, payment, SWIFT, and shipping.

In one campaign, the attackers exploited the name of the University of Bologna by distributing a DOCX file `Elenco richieste dall'Università di Bologna (BO XXXX)`. In another instance, they tried to pass for a Bolivian brokerage and insurance organization (Customs Clearing Agency), using the BMW Group logo in the message. Another way to divert the victim's attention was to use a fake email address of a certain company, while the real sender's address was `cobranzas@***.com.ar`.

Some of the Snake Keylogger attacks on Russian companies were carried out in the name of organizations from Georgia (fig. 26).

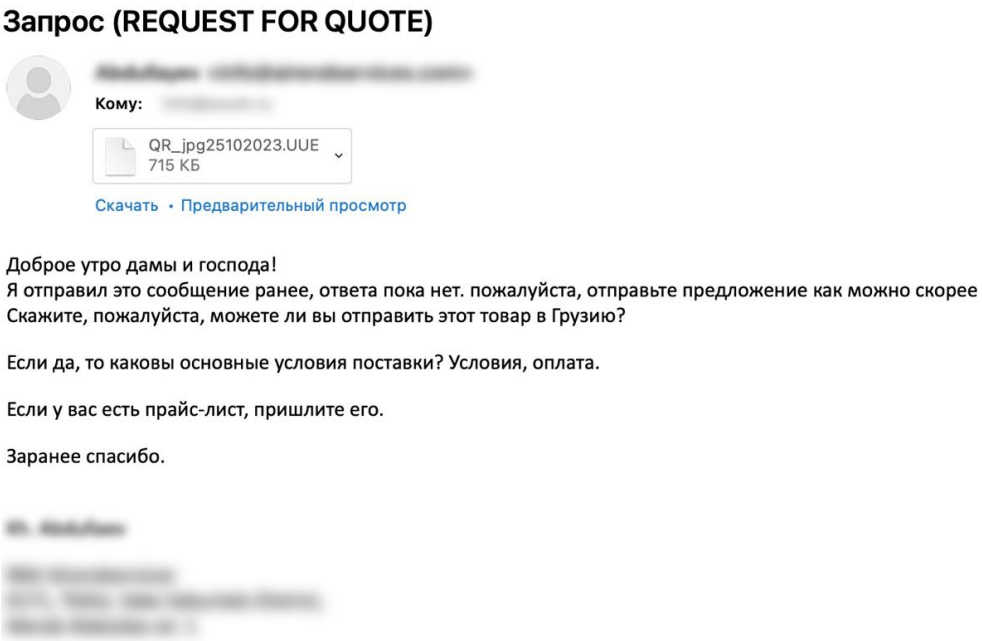


Fig. 26. Phishing email from Snake Keylogger

The archives attached to the emails mostly contained executable files, sometimes double-extended to disguise them as PDF documents. Attackers also used malicious LNK files, OneNote notes, and VBScripts to deliver Snake Keylogger.

Although Snake Keylogger is not often seen in attacks on Russian organizations, we come across logs containing user credentials of Russian companies all the time. In particular, many such logs are found in BI.ZONE Threat Intelligence.

Features

Snake Keylogger is a stealer written in C# that can retrieve credentials from over 40 browsers and applications such as Discord, Outlook, Foxmail, and FileZilla. It can also capture user keystrokes, create screenshots, and collect the following system data:

- username
- device name
- date and time
- external IP address of the device (by querying http://checkip.dyndns.org/)
- location
- device hardware and operating system version

On startup, the Snake Keylogger executable file is moved to the following location: `C:\Users\[user]\AppData\Local\Temp\tmpG[value from 0 to 999].tmp`.

A key is created in the registry hive `Software\Microsoft\Windows\Currentversion\Run` to run it during system startup.

Snake Keylogger uses the following command for the command line to remove a file from its original location:

```
/C choice /C Y /N /D Y /T 3 & Del "[location]".
```

The stealer can also terminate process threads of security tools and Chrome and Firefox browsers.

Snake Keylogger's C2 server can be an FTP server, an email address, and a chatbot in Telegram.

Conclusion

Underground forums and Telegram channels allow unimpeded access to various types of malware. This accounts for its widespread use by hacktivists, cybercriminals, and state-sponsored hackers.

Previously, the creators of such software could prevent its use for criminal purposes or at least prohibit its use in attacks against organizations in Russia and other CIS countries. In the current geopolitical context, however, many criminal groups are finding ways to circumvent such restrictions, and some vendors purposely ignore them altogether. This helps the attackers to expand their arsenal unhindered or use the services of numerous initial access brokers.

MITRE ATT&CK matrix with a heat map

This section presents the tactics and techniques that attackers used during the attack life cycle.

Tactic	Technique		
Initial Access	**T1566.001:** Phishing: Spearphishing Attachment		
Execution	**T1047:** Windows Management Instrumentation	**T1059.003:** Command and Scripting Interpreter: Windows Command Shell	**T1106:** Native API
	T1204.002: User Execution: Malicious File		
Persistence	**T1053.005:** Scheduled Task/Job: Scheduled Task	**T1547.001:** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	
Defense Evasion	**T1112:** Modify Registry	**T1497:** Virtualization/Sandbox Evasion	**T1027.002:** Obfuscated Files or Information: Software Packing
	T1070.004: Indicator Removal: File Deletion	**T1027.008:** Obfuscated Files or Information: Stripped Payloads	**T1055.012:** Process Injection: Process Hollowing

Malware families with the observed five and more techniques

five and more | four | three

Tactic	Technique		
Credential Access	**T1528:** Steal Application Access Token	**T1555.004:** Credentials from Password Stores: Windows Credential Manager	**T1552.001:** Unsecured Credentials: Credentials In Files
	T1555.003: Credentials from Password Stores: Credentials from Web Browsers		
Discovery	**T1010:** Application Window Discovery	**T1057:** Process Discovery	**T1083:** File and Directory Discovery
	T1614: System Location Discovery	**T1518:** Software Discovery	**T1087.001:** Account Discovery: Local Account
	T1124: System Time Discovery	**T1082:** System Information Discovery	
Collection	**T1005:** Data from Local System	**T1041:** Exfiltration Over C2 Channel	**T1115:** Clipboard Data
	T1125: Video Capture	**T1056.001:** Input Capture: Keylogging	**T1113:** Screen Capture
Command and Control	**T1071.001:** Application Layer Protocol: Web Protocols		

Malware families with the observed five and more techniques

five and more | four | three

About BI.ZONE

We help organizations develop their business safely in the digital age. Our innovation driven products enable clients to take the best approach to their tasks, irrespective of company size, budget, or geography.

BI.ZONE cyber threat monitoring, response, and investigation services are designed to help you quickly detect and repel complex attacks:

BI.ZONE TDR (Threat Detection and Response)

Expert managed detection, response and prediction of threats.

BI.ZONE Threat Intelligence

Threat intelligence platform, which acts as a knowledge base of the latest cyber threats.

BI.ZONE Forensics and Investigation

Quick response to threats and incident investigation.

We can help you tackle incidents of varying degrees of complexity:

- ransomware attacks
- data leaks
- financial theft

500+
protected clients

1,200+
completed projects

800+
investigated incidents

800+
cybersecurity experts

Check out the full list of solutions on our website

4 Olkhovskaya St., Bld. 2,
Moscow 105066, Russia

+44 20 3808 3511

info@bi.zone