


# Vietnamese Information Stealer Campaigns Target LinkedIn...

---

 [appgate.com/blog/vietnamese-information-stealer-campaigns-target-professionals-on-linkedin](https://www.appgate.com/blog/vietnamese-information-stealer-campaigns-target-professionals-on-linkedin)



- [Zero Trust Access](#)
- [Threat Services](#)
- [Federal](#)
- OTHER
- [Contact Us](#)

Appgate SDP

## Appgate SDP Overview

Learn how the industry's most comprehensive universal ZTNA solution strengthens security and transforms your network with the flexibility, extensibility and integration advantages of direct-routed architecture.



## How Appgate SDP Works

Find out about the inner-workings of the most flexible and adaptable Zero Trust Network Access solution available today.

## Zero Trust Platform

## Integrations and Tech Partners

## Appgate SDP for Developers

Attend a Live Demo

[Register Now >](#)

# ZTNA Free Trial

[Start Now >](#)

# Watch a Demo

[Visit Demo Hub >](#)

Risk-Based Authentication



Overview

Learn how Risk-Based Authentication provides a frictionless, intelligent and data-informed approach to user authentication.



Strong Authentication

Find out how you can provide secure, frictionless access with the right multi-factor authentication method.

Transaction Monitoring

Explore the tools you can use to intelligently identify and prevent online fraud.

Behavioral Biometrics Service

Learn how behavioral analysis and machine learning stop fraudulent online web activity in real-time.

Secure Consumer Access for:



## SECURE NETWORK ACCESS

Felipe Tarijon November 1, 2023

### **Vietnamese Information Stealer Campaigns Target Professionals on LinkedIn**

---

*Our Threat Advisory Services Malware Analysis and Research Team (MART) recently found LinkedIn posts from professionals in Brazil warning about opening files sent by unknown recruiters as part of a fictional hiring process. According to the posts, the fake malicious recruiter instructed potential victims to open a PDF file which was infected with a virus. Our team obtained these reported files from one of the victims and conducted a thorough analysis of the attack.*

The viral malware is an information stealer targeting browser data such as credentials, cookie and browsing history. It also focuses on stealing data related to Facebook accounts, including Business accounts and Ads campaigns. All the information is encrypted and exfiltrated via Telegram API to a chat controlled by the attacker.

After our investigation, we were able to link this campaign to the previously documented Duckport malware based on many TTPs (Tactics Techniques and Procedures) common in multiple campaigns involving this malware. According to The Hacker News, Duckport is operated by Vietnamese threat actors who leverage shared tooling and tactics to pull off fraudulent schemes and it is a copycat of another threat called Ducktail.

The stolen data can only be retrieved from the Telegram chat by having a private key necessary for decrypting the data. Therefore, it is possible that this malware is used by different threat actors under the malware-as-a-service model. These attacks were carried out by one of many social engineering lures used by this group to disseminate malware, so it is safe to say this is a broader campaign not only targeting victims in Brazil, but all over the world.

#### **Social Engineering and How Victims Get Infected**

These campaigns start with fake job positions offered on LinkedIn that can occur in different ways. Our MART analysts investigated two campaigns that ended up infecting machines with different versions of the same malware family.

In both campaigns, the victims received a PDF file that is not malware per se, but it entices the victim to download a Microsoft OneDrive ZIP file that contains “more details” about the hiring process. In one of the campaigns, the PDF file’s metadata had its language set to vi-VN (Vietnamese) although its content was written in English.

As shown below, the ZIP file contains some files disguised as documents that are, in fact, executable files to trigger the malicious behavior as pictured below.

Backup	29/09/2023 01:58	Pasta de arquivos	
log	29/09/2023 01:58	Pasta de arquivos	
Brand_products_10_2023	29/09/2023 01:59	Aplicativo	68.988 KB
Company_Salary_10_2023	29/09/2023 01:59	Aplicativo	68.992 KB
DetailsSalary_RevenueBonus_Excel_10_2...	29/09/2023 02:00	Aplicativo	68.992 KB
Policy_interview_recruitment_2023	29/09/2023 01:58	Arquivo MP4	9.365 KB

### What to watch for

By default, Windows machines are configured to **not** display known file extensions. Because of that, targeted victims may think the files are not executable (.exe) because they have icons related to PDF and documents like Microsoft Excel. Depending on the fake document executed, it performs a different deceptive action while it executes the malicious actions in the background. The executable file “Brand\_products\_10\_2023” disguised as a PDF, for example, downloads a legitimate PDF file from Dropbox that contains information about well-known brands with which the candidate could supposedly choose to work.

All the executable files disguised as documents end up executing an embedded malware. Also, all of them get the Dropbox URL from the online content-hosting domain “note.2fa.live.” During our analysis, we noticed that no antivirus engines flagged the files as malicious when they were first submitted to VirusTotal. Some days later, only two anti-virus engines flagged one of them as malware.

### Malware capabilities

We were able to analyze the malware source code and reproduce its data exfiltration behavior to understand how it works from the attacker’s perspective. It all starts with the main function. The malware needs to check if it is not being executed more than once. To assure that, it creates a Mutex that changes its name on every campaign (i.e., “ABANDONMT,” “ICollectVASD”).

A mutual exclusion (mutex) prevents simultaneous access to a shared resource. According to [SANS](#), malicious software often uses mutex objects for the same purpose as legitimate software.

Furthermore, **malware might use a mutex to avoid reinfecting the host.**

Additionally, the source code contains several modules executed by the main function, and every string used by the malware is encrypted with AES in the CBC mode. All encrypted strings have the following format:

"LBDVENyVhogHnCfcawHcCw==.oCaTNAg6M0BE862Y7ZQmcsXNB62uTQ/ete7ToFTzKBXLdF2/qi3RvkQJLddsYm3K";  
**Key** **Encrypted string**

The key and the string are separated by a dot used for retrieving the decrypted string.

After decrypting all the strings, we gained a better understanding of the malware's source code. We noticed that there were a lot of strings related to Meta's Facebook APIs such as:

- "business.facebook.com"
- "graph.facebook.com"
- "adsmanager-graph.facebook.com"

The malware has many different modules that are executed altogether. We summarize them below because they are comprised of many different files and sub modules.

### Persistence mechanism

First, the malware copies itself to the **%LOCALAPPDATA%** folder and renames it with the machine's generated UUID (Universal Unique Identifier). To achieve persistence and execute itself every time the machine starts, the malware adds its path to the Registry key:

"Software\Microsoft\Windows\CurrentVersion\Run".

### Caching mechanism

This module can store and retrieve information about the machine using a JSON file. The file is stored in the Windows TEMP folder with the name "ic" + a number that identifies the campaign version. Examples:

- "%TEMP%/ic303"
- "%TEMP%/ic300"

The information stored in the JSON file comprises:

- **GUID:** Globally unique identifier
- **RT:** Stands for "Ran Times," the number of times that the malware was executed
- **CLIENT\_IP:** IP address retrieved from <https://www.whatismybrowser.com/detect/what-is-my-ip-address>
- **CLIENT\_ADDRESS:** IP address location retrieved from <https://www.whatismybrowser.com/detect/ip-address-location>
- **PROFILE\_UID\_:** Used by the Facebook stealer module
- **UA\_PROCESS\_:** Used by the Facebook stealer module
- **SOCIAL\_PROFILE\_:** Used by the Facebook stealer module

Example of the JSON file before the malware stealing the social media data:

```
{"RT": "1", "GUID": "CF5D9969", "CLIENT_ADDRESS": " <REDACTED> ", "CLIENT_IP": " <REDACTED> "}
```

## Information stealing capabilities

This malware family focuses on collecting social media-related data and browser data. The social media-related data is collected by interacting with several other sub-modules that will retrieve different kinds of information from the following URLs:

- <https://www.facebook.com/adsmanager/manage/campaigns>
- <https://business.facebook.com/adsmanager/manage/accounts>
- [https://graph.facebook.com/v17.0/me/businesses?fields={0}&limit=50&access\\_token={1}](https://graph.facebook.com/v17.0/me/businesses?fields={0}&limit=50&access_token={1})

## What to watch for

It can also manipulate Ads campaigns by setting up threat actor-controlled email addresses as administrator of the campaigns. The emails are retrieved from the malware's configuration stored in its resources. It targets the following browsers to steal data:

- Microsoft Edge
- Google Chrome
- Brave
- Mozilla Firefox

It decrypts and queries the browsers' data using an SQLite library to get information like credit card data, cookies, downloads history, browsing history and saved credentials. Below are all the SQL queries that the malware performs in the browsers' databases:

- **SELECT** name\_on\_card, expiration\_month, expiration\_year, card\_number\_encrypted **FROM** **credit\_cards**
- **select** name, path, expires\_utc, is\_secure, is\_httponly, host\_key, encrypted\_value, top\_frame\_site\_key, samesite, has\_expires **from** **cookies**
- **select** name, path, expires\_utc, is\_secure, is\_httponly, host\_key, encrypted\_value, samesite, has\_expires **from** **cookies**
- **select** name, path, expiry, isSecure, isHttpOnly, host, value, sameSite **from** **moz\_cookies**
- **SELECT** current\_path, end\_time, referrer, tab\_url, tab\_referrer\_url, mime\_type **FROM** **downloads** **order by** end\_time desc
- **SELECT** url, title, last\_visit\_time **FROM** **urls** **WHERE** id =
- **SELECT** url **FROM** **visits** **order by** visit\_time desc
- **SELECT** action\_url, username\_value, password\_value **FROM** **logins** **order by** date\_password\_modified desc

## Data exfiltration

The *MainExporter* module is responsible for sending all the victim's data to the attacker via Telegram (<https://api.telegram.org/>). It encrypts and compresses all the data into ZIP archives. The malware can send the following data:

- Browser data (cookies, credit cards, credentials, downloads, and browsing history)
- Processes running on the machine
- User agent

- Log information generated during malware execution
- IP address
- Facebook accounts
- Facebook personal information like email, name, data of birth, and phone
- Other consolidated information such as: User, IP, OS Name, OS Version, Number of Monitors, CPU, GPU, RAM, Country, CC (Credit Card), City, Coordinator, Hardware ID, GUID, SDCV (malware/campaign version), and FPXUrl (unknown).

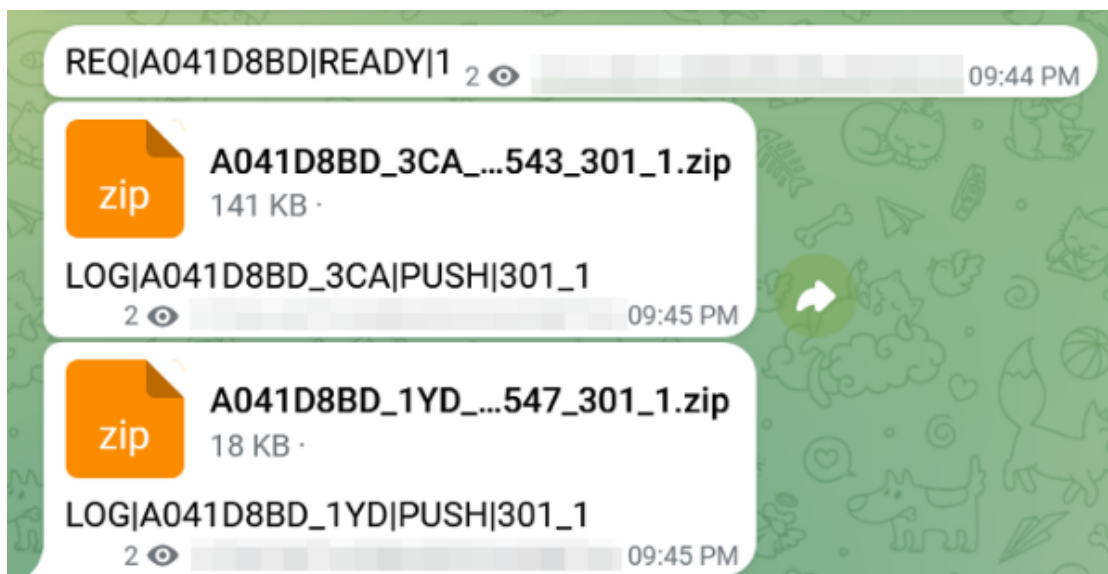
To send the exfiltrated data back to the attacker, this malware uses two different types of cryptography: symmetric (AES) and asymmetric (RSA). The symmetric one is faster and requires a key (like a password) to encrypt/decrypt the data, therefore it is used to encrypt all the stolen data by generating a random key in the victim's machine.

The asymmetric cryptography requires a public key to encrypt the data (stored in the malware) and a private key to decrypt it (not present in the malware). In this case, the encrypted data is the randomly generated AES key (password). Therefore, to obtain the stolen data, the attacker needs to decrypt the AES key first by using the corresponding private RSA key.

### What does that mean?

The malware is generated with a public key that probably only the developer has access to its corresponding private key. This is common in malware-as-a-service businesses where the malware is purchased or rented, and the developer wants to prevent people from using it without paying for it, protecting the stolen data from being easily obtained.

The encrypted AES key is stored in the text file named "{CYR}.txt" inside one of the ZIP files. The attacker then receives the following information on their Telegram chat as depicted below:



The first message is sent every time the malware is executed. It is identified by the first string "REQ," followed by the victim's GUID, "READY," and an integer number which represents the "Ran Times" calculated by the malware ... these values are separated by a pipe "|."



As soon as the malware runs its collector module, it stores all stolen data into those ZIP files, and sends them as documents to the Telegram chat along with the following message:

```
“LOG|<GUID>_<PROFILE NAME>|PUSH|<CAMPAIGN_VERSION>_<RAN TIMES>”
```

As explained earlier, to decrypt the stolen data, it is necessary to decrypt the AES key (inside the “{CYR}.txt” file) by using a private RSA key that only the attacker has. Finally, the AES key can be used to decrypt all the stolen data. Decrypting the stolen data manually can take some time, so probably the malware developer created a script that gets and decrypts the data from the Telegram chat and shows it in a web panel for example.

### **Attribution: Identifying the malware family**

Based on the IOCs (Indicators of compromise) and TTPs (Tactics, Techniques, and Procedures), we found similar campaigns ([WithSecure](#), [Cyble](#), and [Meta](#)) with the same modus operandi:

- Fake job offering approach on LinkedIn that sends a ZIP file containing the same structure analyzed in this report.
- Usage of 2fa.note.live service.
- Executable files disguised as documents with low detection rate.
- Usage of SmartAssembly and .NET Framework to build the malware samples.
- AES + RSA Cryptography.
- Meta/Facebook hijacking capabilities.
- Data exfiltration via Telegram.

Therefore, it's safe to attribute this attack to the Vietnamese Duckport malware, active since late March 2023 that performs information stealing alongside Meta Business account hijacking. Duckport is described by WithSecure's research as Ducktail's copycat. Ducktail is said to be one of the many Vietnamese threat actors leveraging shared tooling and tactics to pull off such fraudulent schemes, according to [The Hacker News](#).

The campaigns analyzed by our MART researchers have many of the TTPs found in common with the other previously documented attacks. Also, the fact that it is a Vietnamese threat is supported by the metadata found in the fake documents.

### **Conclusion**

This attack shows how creative threat actors can be to infect victims using LinkedIn fake job positions as social engineering. We spotted these campaigns because potential victims from Brazil suspected the fake recruiters' approach and complained in a post on LinkedIn. After that, more than 6,000 people liked and interacted with the post, indicating that a lot of them were also targeted.

However, these campaigns are just the tip of the iceberg. After we linked this campaign to the previously documented Duckport threat group, we learned that the attackers use many different lure themes to infect victims' devices across the world.

Given the usage of a random AES key encrypted with RSA for securing the stolen data, it's possible that this threat is distributed in the [malware-as-a-service model](#). The stolen data can only be retrieved if the attacker has the correct private key that was carefully generated along with the public key stored in the malware in an obfuscated format.

It's also important to note that information stealer threats can easily sell their established access within compromised devices and sell the data (including personal and business related) to other attackers. Other threat actors then can use this to carry out more dangerous attacks such as ransomware, data extortion, and even espionage attacks against victims' organizations.

To protect against this type of threat, we recommend not downloading software from unknown websites, including if they are advertised at the top of the results by search engines. If you receive a job offer and the recruiter sends a suspicious file to be executed, beware and don't do anything! If you are using a corporate device, always report suspicious behavior to your IT department.

Our Threat Advisory Services Malware Analysis and Research Team (MART) frequently monitors and reports on trends like this to keep you up-to-date on emerging threats. Learn more about our world-class [Threat Advisory Services offerings here](#).

## **IOCs**

### **Campaign #1**

#### **Files**

##### **Details\_Advertisement\_Campaign\_2023\_MCMA.zip**

Hash sha256: b5cd6b969e8b29d3102800ca64b575fec6f28a4f477a31177bb263559eb964c8

##### **Brand\_products\_10\_2023.exe**

Hash sha256: 61cfe06e6db1c93b8bbb63fdf3f58538edab85dafc4f8c65d9403bf89bd540dd

##### **Brand\_products\_10\_2023.pdf**

Hash sha256: 2843b74a2f6013b93e0344cdfac6fc68f321bb45ab352d28681fb16a319eb503

##### **Company\_Salary\_10\_2023.exe**

Hash sha256: 284a8c7ea86b9e8694ecbfc38d0808f2afc1fede2dd749700bee62a61091f997

##### **Company\_Salary\_10\_2023.docx**

Hash sha256: 3c03cb70625d9ccfd41c288bfd6dfc9632cfb3fc7093395146b5149bc41974c9

##### **DetailsSalary\_RevenueBonus\_Excel\_10\_2023.exe**

Hash sha256: 1d941cb5dcb8bfa06f300a50da871118d693234e005f58fdcf4b6bb69258f70c

##### **DetailsSalary\_RevenueBonus\_Excel\_10\_2023.xlsx**

Hash sha256: 2f75be8ab634b69d101d827099c486ba41d88c8477339b1fff70b16bb06f4b3b

### **Overlay (embedded malware):**

Hash sha256: 2a2e189d5d778bf443419ee1b3289e8a11404f20b5cd261ce86fecaabbe6636e

### **URLs**

- [https://note.2fa\[.\]live/note/Brand\\_products\\_10\\_2023](https://note.2fa[.]live/note/Brand_products_10_2023)
- [https://www.dropbox\[.\]com/scl/fi/coflcpbv8kjdsl7akwtj/Brand\\_products\\_2023\\_Pdf.pdf?rlkey=2d8srnf18ep9t9eli40jzsn8p&dl=1](https://www.dropbox[.]com/scl/fi/coflcpbv8kjdsl7akwtj/Brand_products_2023_Pdf.pdf?rlkey=2d8srnf18ep9t9eli40jzsn8p&dl=1)
- [https://note.2fa\[.\]live/note/Company\\_Salary\\_10\\_2023](https://note.2fa[.]live/note/Company_Salary_10_2023)
- [https://www.dropbox\[.\]com/scl/fi/dak1zudqyo7nu4uzpwrw7/Company\\_Salary\\_2023\\_Word.docx?rlkey=6wbv7uhj1z20fw21e525gnkek&dl=1](https://www.dropbox[.]com/scl/fi/dak1zudqyo7nu4uzpwrw7/Company_Salary_2023_Word.docx?rlkey=6wbv7uhj1z20fw21e525gnkek&dl=1)
- [https://note.2fa\[.\]live/note/DetailsSalary\\_RevenueBonus\\_Excel\\_10\\_2023](https://note.2fa[.]live/note/DetailsSalary_RevenueBonus_Excel_10_2023)
- [https://www.dropbox\[.\]com/scl/fi/h4ddsyhsw5gs6airlhqd/DetailsSalary\\_RevenueBonus\\_Excel.xlsx?rlkey=y9kdl3dIntva1djzly4ua8zua&dl=1](https://www.dropbox[.]com/scl/fi/h4ddsyhsw5gs6airlhqd/DetailsSalary_RevenueBonus_Excel.xlsx?rlkey=y9kdl3dIntva1djzly4ua8zua&dl=1)

### **Paths**

JSON file containing the infected machine's data:

`%temp%\ic303`

Persistence mechanism (malware is copied to the folder below and renamed with the machine's GUID) to execute malware every time machine is initialized:

`%localappdata%\<GUID>.exe`

### **Campaign #2**

#### **Files**

##### **Senior\_Manager\_EA\_Sport.zip**

Hash sha256: 054822987c6597d7a916f6ea29333f20767c1f65e6b5f8edab1f328f3c749dc

##### **Job\_Description\_of\_Senior\_Manager.exe, Salary\_and\_Comprehensive\_Benefits\_Package.exe**

Hash sha256: 3097d80d4aa3abf2599058bf58d85aa8cec6ca6894c13c6d360dce162a5dd626

##### **Job\_Description\_of\_Senior\_Manager.pdf**

Hash sha256: 14feebb67d7c46a63afe94149d4f3607ef8d0ed9ccefdcc4615a9fa8b3fe5ec0

### **Overlay (embedded malware)**

Hash sha256: ed73b42ea6d26324d3a6cd3f8217b177d68f1d44d5eefaaaef23ee4b4a5787ac

### **URLs**

- [https://onedrive.live\[.\]com/download?resid=7531E499827B967F!163&authkey=!AO41K9-bCwOPW64](https://onedrive.live[.]com/download?resid=7531E499827B967F!163&authkey=!AO41K9-bCwOPW64)
- [https://note.2fa\[.\]live/note/Job\\_Description\\_of\\_Senior\\_Manager](https://note.2fa[.]live/note/Job_Description_of_Senior_Manager)
- [https://www.dropbox\[.\]com/scl/fi/xlljfln36gg3vhl6v8mhn/Job\\_Description\\_of\\_Senior\\_Manager.pdf?rlkey=jlcq8jiu77myq1rj9rtlyjq8g&dl=1](https://www.dropbox[.]com/scl/fi/xlljfln36gg3vhl6v8mhn/Job_Description_of_Senior_Manager.pdf?rlkey=jlcq8jiu77myq1rj9rtlyjq8g&dl=1)

## **Paths**

JSON file containing the infected machine's data:

`%temp%\ic300`

Persistence mechanism:

`%localappdata%\<GUID>.ex`

## **Receive News and Updates From Appgate**

---

**Thank you for subscribing**

---