APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure

By Allison Ebel

Published: 2020-09-22 · Archived: 2026-04-05 17:00:57 UTC

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

Source: https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/