Accenture: Russian hackers using Brexit talks to disguise phishing lures

By Zaid Shoorbajee

Published: 2018-11-29 · Archived: 2026-04-06 01:16:57 UTC

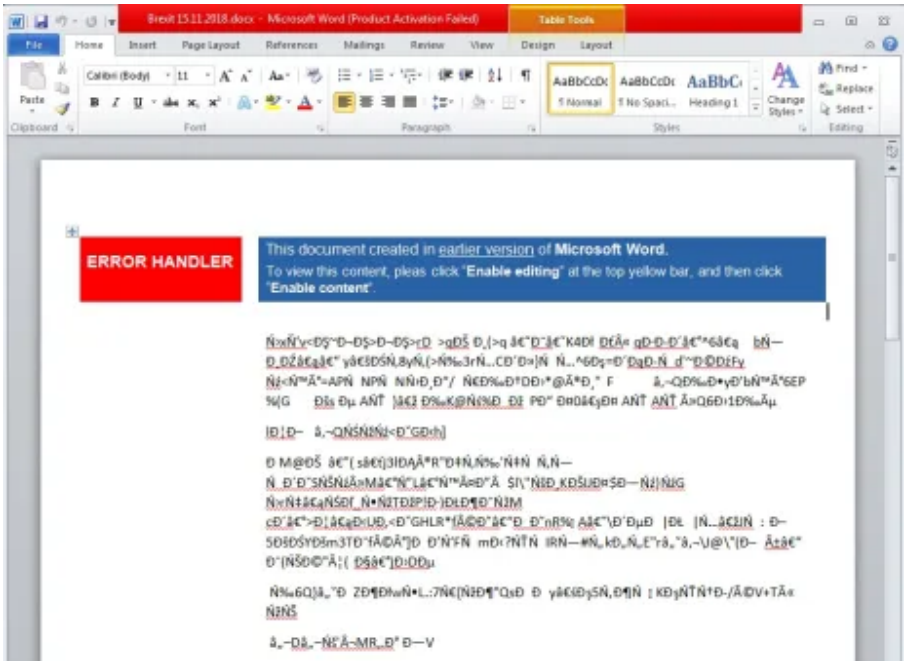
A notorious Russian hacking group tried to exploit the latest flurry of Brexit-related news to spread malware to unsuspecting victims, according to a report from Accenture released Thursday.

APT28, which Accenture refers to as SNAKEMACKEREL, used a malware-laced Microsoft Word document that appeared to be about the United Kingdom's planned separation from the European Union to try breaching a wide variety of targets' systems, researchers said.

APT28 is widely believed to be the product of Russian intelligence services. Also known as Fancy Bear, Pawn Storm and other names, its the same group researchers have blamed for the 2016 breach on the Democratic National Committee, for leaks relating to the 2018 Winter Olympics and for the targeting of various government, political, critical infrastructure and other organizations.

"Based on observed targeting by this threat group over the past few years, we assess with moderate confidence that they are likely to have targeted government, politics, think tanks and defense organizations in the US, Europe and a former eastern bloc country," Michael Yip, security principal at Accenture's iDefense team, told CyberScoop in an email.

Accenture said it observed activity relating to this malware campaign around the same time that government leaders in the U.K. announced a draft deal for Brexit earlier this month. The name of the Word document used in the campaign is "Brexit 15.11.2018.docx," suggesting that the Russian hacking group is exploiting current events to make its messages seem legitimate. The document displays garbled text in an attempt to get targets to enable macros, unleashing the "Zekapab" malware.



Researchers said this document displays garbled text in an attempt to get victims to enable macros. (Accenture Security)

Zekapab, which has previously been observed by Accenture and others, is a first-stage malware that establishes a backdoor on a victim's system and collects information about the host. The malware is also known as Zebrocy and was spotted by Palo Alto Networks researchers in another APT28-linked campaign late October and early November.

"The use of weaponized Microsoft Office documents to deliver first stage malware such as Zekapab (aka Zebrocy) and the use of news headline themes for document lures are hallmarks of SNAKEMACKEREL's modus operandi," Yip said. "The speed in which fresh news headlines are used for document lures in attacks particularly highlights the group's knowledge of foreign affairs and provides strong indications of their targeting remit."

Sean Lyngaas contributed to this story.
