

SNAKEMACKEREL delivers Zekapab malware

[accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware](https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware)



As the United Kingdom (UK) Prime Minister Theresa May announced the initial BREXIT draft agreement with the European Union (EU), iDefense analysts identified a new campaign by SNAKEMACKEREL using a BREXIT-themed lure document to deliver the Zekapab (also known as Zebrocy) first-stage malware.

What's the story?

SNAKEMACKEREL is an espionage-motivated cyber threat group, also known as Sofacy, Pawn Storm, Sednit, Fancy Bear, APT28, Group 74, Tsar Team, and Strontium.

Both the British and Dutch governments have publicly attributed SNAKEMACKEREL activities to the Russian military intelligence service (RIS)¹ and have linked specific cyberattacks to the group, including the targeting of the Organisation for the Prohibition of Chemical Weapons (OPCW)², the United Kingdom Defence and Science Technology Laboratory (DSTL) and the United Kingdom Foreign and Commonwealth Office (FCO).

In foreign countries, RIS actors conducted damaging and/or disruptive cyberattacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack."

According to the FBI, the SNAKEMACKEREL threat group "is part of an ongoing campaign of cyber-enabled operations directed at the United States government and its citizens. These cyber operations have included spear phishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, leading to the theft of information.

[Download the report \[PDF\].](#)

What does it mean?

The creation of this malicious document, coming on the day the UK government announced an initial agreed draft of the BREXIT agreement, suggests that SNAKEMACKEREL is a group that pays close attention to political affairs and is able to leverage the latest news headlines to develop lure documents to deliver first-stage malware, such as Zekapab, to its intended targets. The theme also reflects the targeting of the group which primarily focuses on NATO members, countries in Central Asia and those neighboring Russia.

Given the assumed association with the Russian military service, it is clear that the group has significant resources to target and compromise organizations. As a result, it requires extra investment in defensive measures. To protect the confidentiality, integrity and availability of business operations, Accenture Security recommends that organizations ensure their staff members receive security hygiene training and deploy intelligence-driven network and host-based defensive measures.

Why does it matter?

Despite the public reporting and government accusations, SNAKEMACKEREL remains highly active. It is behind a large number of cyberattacks targeting global aerospace and defense contractors, military units, political parties, the International Olympic Committee (IOC), anti-doping agencies, government departments and various other verticals. NATO and EU member countries, as well as the United States, are of particular interest to the group.

SNAKEMACKEREL operations continue to be some of the most far-reaching and sophisticated cyber espionage and intelligence campaigns to date.

Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us [@AccentureSecure](#) on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

Copyright © 2020 Accenture. All rights reserved. Accenture, its logo, and High Performance Delivered are trademarks