SNAKEMACKEREL delivers Zekapab malware

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.