

Russia-Linked APT 'Winter Vivern' Targeting Governments in Europe, Asia

A Russia-linked advanced persistent threat (APT) actor tracked as Winter Vivern has been observed targeting government entities in several European and Asian countries.

Initially detailed in early 2021, the group is known to support the interests of Belarus and Russia's governments, and was previously observed targeting government organizations in India, Lithuania, Slovakia, and Vatican.

Following reports published in February by Polish and Ukrainian authorities regarding new Winter Vivern activity targeting Ukraine, cybersecurity firm SentinelOne discovered additional campaigns that can be attributed to the group.

The recent Winter Vivern attacks targeted government entities in Poland, Ukraine, Italy, and India, as well as telecommunications organizations in Ukraine, SentinelOne has discovered.

As part of the observed attacks, the threat actor created individual pages on a malicious domain mimicking the pages of a Polish anti-cybercrime agency and those of Ukraine's security service and ministry of foreign affairs.

Winter Vivern uses malicious Office documents in attacks, and was seen using government email credential phishing webpages and targeting individuals associated with a Ukrainian government project guiding Russian and Belarus soldiers looking to voluntarily surrender, via malicious Excel

spreadsheets.

According to SentinelOne, the APT likely has limited resources, but makes use of shared toolkits and legitimate Windows utilities in attacks, which make it effective.

“Recent campaigns demonstrate the group’s use of lures to initiate the infection process, utilizing batch scripts disguised as virus scanners to prompt downloads of malware from attacker-controlled servers,” the cybersecurity firm notes.

Malware deployed in the recent attacks included Aperetif, a remote access trojan (RAT) written in Visual C++ that can collect system information, maintain access to the infected system, and connect to the command-and-control (C&C) server to receive instructions or download additional payloads.

Winter Vivern also exploits known vulnerabilities to compromise targets and staging servers. One of the APT’s servers was seen hosting the Acunetix web application vulnerability scanner, which is likely used to identify vulnerable networks and WordPress domains.

“The Winter Vivern cyber threat actor has been able to successfully carry out their attacks using simple yet effective attack techniques and tools. Their ability to lure targets into the attacks, and their targeting of governments and high-value private businesses demonstrate the level of sophistication and strategic intent in their operations,” SentinelOne concludes.

Related: Microsoft Pins Outlook Zero-Day Attacks on Russian Actor, Offers Detection Script

Related: Russian Cyberspies Abuse EU Information Exchange Systems in Government Attacks

Related: Police Looking for Russian Suspects Following

DoppelPaymer Ransomware Crackdown

Russia-Linked APT 'Winter Vibern' Targeting Governments in Europe, Asia