Poland warns of attacks by Russia-linked Ghostwriter hacking group

Bill Toulas ⋮⋮ 1/3/2023

The Polish government is warning of a spike in cyberattacks from Russia-linked hackers, including the state-sponsored hacking group known as GhostWriter.

In an announcement on Poland's official site, the government claims that hostile cyber-activities have intensified, targeting public domains and state organizations, strategic energy and armament providers, and other crucial entities.

The Polish believe Russian hackers target their country due to the continued support they have provided Ukraine in the ongoing military conflict with Russia.

Recent cyberattacks

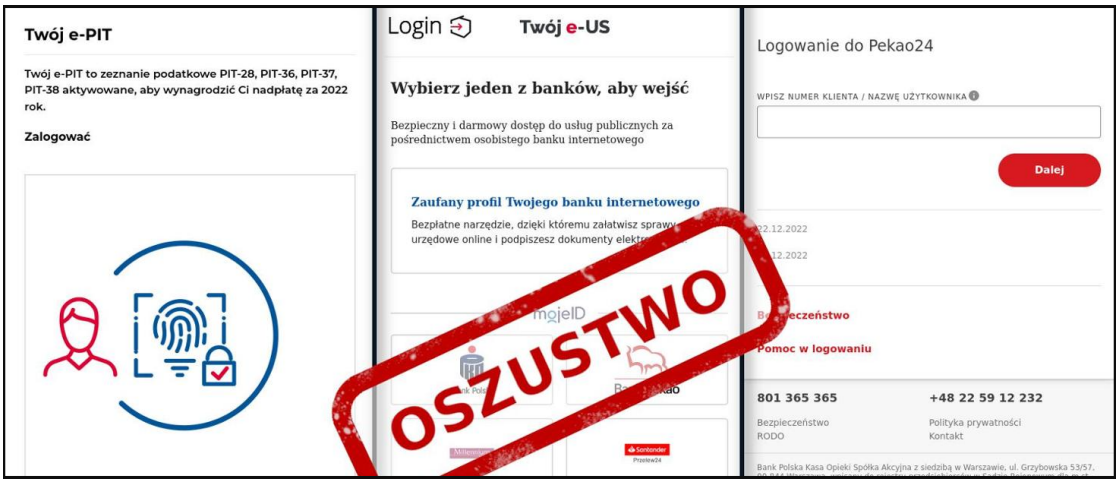
The first case highlighted by the Polish government post is a DDoS (distributed denial of service) attack against the parliament website ('sejm.gov.pl'), attributed to the pro-Russian so-called hacktivists' NoName057(16).'

The attack unfolded the day after the parliament adopted a resolution recognizing Russian as a state sponsor of terrorism, rendering the website inaccessible to the public.

Another notable incident mentioned in the announcement is a phishing attack attributed to the 'GhostWriter' group, which the European Union has associated with the GRU, Russia's military intelligence service. Cybersecurity firm Mandiant has also linked the hacking group to the Belarusian government.

According to the Polish, the Russian hackers set up websites that impersonate the gov.pl government domain, promoting fake financial compensation for Polish residents allegedly backed by European funds.

Clicking on the embedded button to learn more about the program takes victims to a phishing site where they are requested to pay a small fee for verification.



December '22 campaign impersonating the Polish tax administration *(gov.pl)*

"More and more often cyberattacks are used in order to spread Russian disinformation and serve Russian special services to gather data and vulnerable information," explained the Polish government.

"The operation that is carried out using simultaneously both of these methods is the GhostWriter campaign."

GhostWriter has been active since at least 2017, previously observed impersonating journalists from Lithuania, Latvia, and Poland, to disseminate false information and anti-NATO narratives to local audiences.

The announcement warns that GhostWriter has been focusing on Poland recently, attempting to breach email accounts to collect information, and taking control of social media accounts to spread false information.

In response to the growing cyber threats, Poland's Prime Minister has increased the cybersecurity threat level to 'CHARLIE-CRP,' introducing various measures like maintaining a 24-hour roster in designated offices and public administration organizations.