21 MAR 2019 NEWS

Russian State Hackers Phish Euro Governments Ahead of Elections

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

State-sponsored Russian hackers are targeting NATO members and European governments ahead of the upcoming European Parliament elections, according to new FireEye intelligence.

The security vendor claimed to have detected spear-phishing activity from the prolific Kremlin-linked APT28 and Sandworm Team groups.

The idea is to harvest passwords by sending the victim to a fake log-in page. To increase their chances of success, the groups are spoofing real government website portals, registering domains similar to trusted destinations and displaying the sender of these phishing emails as a trusted entity.

"The groups could be trying to gain access to the targeted networks in order to gather information that will allow Russia to make more informed political decisions, or it could be gearing up to leak data that would be damaging for a particular political party or candidate ahead of the European elections," said Benjamin Read, senior manager of cyber espionage analysis at FireEye.

"The link between this activity and the European elections is yet to be confirmed, but the multiple voting systems and political parties involved in the elections creates a broad attack surface for hackers."

Although FireEye claimed the two groups' activity appears to be coordinated, they use different tools and tactics. The Sandworm Team tends to use publicly available tools, while APT28 uses expensive customized tools, and has deployed zero-day exploits in the past, it said.

This is not the first alert to be issued about Russian hacking activity ahead of the upcoming European elections.

In February, Microsoft claimed to have spotted APT28 targeting NGOs, think tanks and other government-linked organizations. It said 104 accounts across Belgium, France, Germany, Poland, Romania and Serbia had come under attack.

The infamous APT28 group (aka Fancy Bear) has been blamed for the 2016 phishing attacks on the Democratic National Committee (DNC) which many believe helped Donald Trump to power.

Related to This Story

- Microsoft: Russians Hacking Again Ahead of Euro Elections
- Three Campaigns Targeted as Senate Pushes Security
- APT28 Back in RussianDoll Attack Using Adobe, Windows Flaws
- Microsoft Shuts Down Six APT28 Phishing Domains
- Bolton Boasts Trumps Efforts to Secure Elections

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1. 16 MAR 2020 NEWS — US Health Department Hacked Amid Coronavirus Pandemic
2. 13 MAR 2020 NEWS — Info-Stealing Coronavirus Threat Map Detected
3. 16 MAR 2020 OPINION — Working from Home Policies and the Future of Cybersecurity
4. 16 MAR 2020 NEWS — Illinois College Suffers Data Breach
5. 17 MAR 2020 NEWS — Agents Arrest 24 on $30m Money Laundering Charges
6. 17 MAR 2020 NEWS — US VPN Use Could Soar 150% as Covid-19 Spreads