

Russian cyber threat to European elections

European political institutions are shoring up their defences after predictably being targeted by Russian state-sponsored hackers ahead of elections in May to choose hundreds of new MEPs

Sep-Dec 2018: *Spear phishing* attack on 104 employee accounts at **German Council on Foreign Relations**, **The Aspen Institute in Europe** and **The German Marshall Fund**

Operations in six nations targeted

POLAND
GERMANY
BELGIUM
FRANCE
ROMANIA
SERBIA

Hacker group: *Fancy Bear* (aka **APT28**, **Pawn Storm** or **Strontium**). Described as skilled team of developers and operators collecting intelligence on defence and geopolitical issues

May 23-26, 2019: European Parliament elections. Total of **751 Members of European Parliament (MEPs)** represent more than **512m** people from 28 member states*

SPEAR PHISHING

Email sent instructing user to change web-based email password to protect them from hackers. Includes weblink (shortened to **bit.ly** link to bypass spam filters)



User follows link to **fake** **webmail** log-in page (looks identical to real one), and enters user-name and password. **Credentials stolen**

Stolen ID allows hacker to access **company systems** to gather data and install **malware** designed to spread and damage computers

EUROPEAN COUNTERMEASURES

- **Microsoft:** Expanding **AccountGuard** threat-detection system to political organisations in Europe – now totalling 14 countries
- **Google:** Extending cyber security platform **Project Shield** to European political parties – previously only offered to news and human rights groups
- **Facebook / Twitter:** Introducing safeguards to limit spread of misinformation

*At time of writing, UK due to leave EU on Mar 29, 2019. MEP count to then lower to 705 members

Sources: Financial Times, Microsoft

Picture: Gemma Brown

© GRAPHIC NEWS