The West is ill-prepared to deal with evolving cyber threats, report concludes

February 9 2023

Credit: Pixabay/CC0 Public Domain

An information and hacking campaign with links to a foreign state has potentially had a "significant cumulative impact" over many years, according to a report from Cardiff University.

The findings, from the Security, Crime and Intelligence Innovation Institute, provide the most comprehensive picture to date of the activities of the so-called Ghostwriter campaign.

Tracking its evolving activities via open-source data, the report demonstrates how it has impersonated multiple government officials, NATO representatives and journalists across Europe. According to the team's analysis, it has impacted thousands of email users, hacked dozens of social media accounts and media websites and published hundreds of false blogposts.

The integration of cyber-attacks with information manipulation has become more prominent following Russia's invasion of Ukraine. Most recently, it has been engaging in cyber-attacks against Ukrainian government websites, targeting Ukrainian military and public figures on Meta's platforms, and credential phishing on Google.

The report's analysis also covers incidents in Germany, Poland and Lithuania, which have already been publicized and linked to Ghostwriter by cyberfirm Mandiant. There is widespread consensus among Western officials that the campaign is supported by either Russia, Belarus, or both.

Lead author Anneli Ahonen said, "Ghostwriter's activities have triggered multiple yet separate responses from governments, social media platforms, media and private cyber firms. These have focused on strategic communications to counter false narratives, public but partial attribution, improvements in cyber security, and most recently the disruption of parts of Ghostwriter's activity on Facebook and Google.

"But there is no one organization with an overarching view of the scale of its activities—and so the seriousness of the threat has been poorly understood. Ghostwriter has been able to diversify its methods, targets

and the countries it is focusing upon. This has potentially had a significant cumulative impact and effect, given how its various activities have persisted over several years, across multiple social media platforms."

Ghostwriter has been active since at least 2016. Significantly, it was not really understood as a consistent campaign until 2020. Using cyber-attacks to spread false information has become integral to its tactics.

Anneli Ahonen added: "To date, much policy attention has centered on the Internet Research Agency and its interference in the U.S. election in 2016. Ghostwriter is an example of another persistent, large-scale, and well-resourced operation, but with very different tactics to the Internet Research Agency's playbook.

"Currently, cyber and influence operations are understood as separate fields, with distinct sets of expert knowledge. But the adversaries often don't make similar distinctions between the two. A more coordinated approach, which brings together both areas of research, would be a more successful way of combatting disinformation and informing the public."

Professor Martin Innes, director of the Security, Crime and Intelligence Innovation Institute, added: "Criminologists use the term 'linkage blindness' to describe the problems that arise when different police agencies are all engaged in investigating the same persistent perpetrator, and each investigator has only a partial view of how and why the harmful act is being committed.

"This concept of 'linkage blindness' describes what has happened with the response to Ghostwriter, in that different governments and organizations have been looking at different facets, but no institution is positioned to take responsibility for adopting a comprehensive approach."

This independent analysis draws together the publicly available open-source evidence of 34 incidents attributed to the Ghostwriter campaign between the summer of 2016 and the summer of 2021, as well as official government communications, media reports, fact-checks and NGOs and think tanks' analysis.

Researchers also carried out nine semi-structured, in-depth interviews with various representatives of governments, media and civil society, who have been directly involved in responding, exposing, or analyzing these incidents. Further information was also collected on how Russian language media reported them.

The report also tracks and references incidents linked to Ghostwriter after that time period—in Belarus, Germany, Lithuania, Poland, and Ukraine.

Provided by Cardiff University

Citation: The West is ill-prepared to deal with evolving cyber threats, report concludes (2023, February 9) retrieved 23 September 2023 from https://techxplore.com/news/2023-02-west-ill-prepared-evolving-cyber-threats.html