The Ghostwriter playbook

From cyber attacks to disinformation operations in Central Europe
Privet, you have just been hacked!
**FAKE NEWS ABOUT A RADIOACTIVE WASTE LEAK**

**March 17, 2021**

Hackers fabricate a report of an alleged radioactive cloud that formed in Lithuania and is moving towards Poland.

The attack originated in a hacked website of Lithuania’s nuclear regulatory agency, a breached website of Poland’s National Atomic Energy Agency and the country’s ministry of health.

In the attack, hijacked social media accounts of experts and local government officials are also used.

**How the attack unfolded**

1. **Source content** - an authentic communication from Lithuania’s State Nuclear Power Safety Inspectorate (VSI).
2. **Fabricated website** - of Lithuania’s Inspectorate with manipulated fake news about a ‘disaster’.
3. **Hacked website** - of Poland’s National Atomic Energy Agency and fake post about an increase in radiation levels.
4. **Hacked website** - of Poland’s ministry of health containing a warning about a radiological hazard.
5. **Expert’s** - hacked Twitter account lends credibility to the fake report.
6. **Hijacked accounts** - of government officials are used to spread social media.
Large scale influence operation

1. Phishing attacks
   Hacking groups target email accounts of the public figures (politicians, experts, journalists)

2. SM accounts
   Hackers gain access to SM accounts through compromised emails

3. Hacked and fabricated websites
   Attackers compromise official websites of the institutions
   Disinfo actors fabricate websites

4. SM platforms Traditional media
   Disinfo actors run manipulative campaigns across SM channels and target traditional media
In July 2020, Mandiant Threat Intelligence released a public report detailing an ongoing influence campaign we named “Ghostwriter.” Ghostwriter is a cyber-enabled influence campaign which primarily targets audiences in Lithuania, Latvia and Poland and promotes narratives critical of the North Atlantic Treaty Organization’s (NATO) presence in Eastern Europe.
Hack & leak

- Telegram channels
- Website addressed to the Polish audience
- Belarusian propaganda machine
Key findings

- similarities between **UNC1151** and the **GRU-linked groups** (Fancy Bear, Sandworm)
- data might be used in several disinfo operations by cooperating groups
- phishing attacks targeted Polish politicians, MoD infrastructure, military targets in Ukraine

Who is behind the largest cyber-espionage operation in Poland? So far, it seems as if the Belarusian regime has benefited the most from the Polish hack-and-leak scandal. But there is evidence that the leak is an offshoot of the Ghostwriter campaign, an influence operation pursuing Russian interests. Our analysis has revealed that the activities of a group that might have compromised over 700 email accounts – including Michal Dworczyk’s private email – bear striking resemblance to the attacks carried out by GRU-linked hacker groups such as Fancy Bear.

Until recently, nearly every day for two months unknown perpetrators published new documents and screenshots of emails stolen from the inbox of the chief of the Chancellery of the Prime Minister of Poland, Michal Dworczyk, on a private social media platform.
Targets

- Poland
- Lithuania
- Ukraine
- Germany
- NATO
- Belarusian opposition
> 170

likely compromised VIP email accounts in one CEE country (Poland)
Broad spectrum of goals

- destabilization
- polarization
- access to critical infrastructure
- access to critical information
- blackmail
- spy games
Attacks and markets are critical. Each is particularly dangerous in its own way. Hostile states sponsor hacking services, disinformation services, and other strategies. Hacking services provide infrastructure for campaigns, while disinformation services include content, distribution, and distribution channels. Phishing campaigns, malware, and fake news leaks are among the tools used. Troll farms and psychographic profiling are additional strategies.
Investigating large scale influence operations

- Cross-functional approach
- Infrastructure analysis
- Disinfo network analysis (distribution channels)
- SM monitoring (content and context)
- Scale, complexity, resources
- Targets, goals
- Key actors, proxies
- Impact
- Institutional response
EU condemns Russia for the Ghostwriter operation
“If we are chasing what is right now, we are late”

@agielewska
@VSquare_Project
anna.gielewska@fundacjareporterow.org

Photo credits: unsplash.com; libreshot.com