**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# UNC1151 2018 campaign: “Lithuanian minister of national defence committed sexual assault”.

## Summary

In January 2018, a Ghostwriter disinformation operation targeted the Lithuanian Defence Minister, Raimundas Karoblis. The promoted narratives were that multiple government officials and a journalist had come forward with allegations of sexual assault and claims the minister was homosexual. These narratives were promoted via targeted phishing emails and a compromised Lithuanian TV channel’s website.

## Timeline and Context

* Prior to January 18, credentials used to compromise administration accounts for a Tv3.lt website (a Lithuanian TV Channel) were harvested.
* On January 18, these credentials were used to login, perform scanning and inquiries to the Content Management System of the website.
  + Following this, permissions and system access configuration was adjusted.
  + An article was published via editing/defacing the website. Said article is indexed by GoogleBot and becomes publicly available.
  + English version of the narrative disseminated on multiple sites including Ghostwriter controlled blogs.
* An email with a malicious document attached containing defamatory information regarding the Lithuanian Defence Minister and links to said article was sent to a targeted mailing list including government ministries, politicians, embassies, and media organisations.
  + The email included contained an image, inquiries from which could be monitored by the sender. This informed them on which recipients opened the email.
  + The email included an attached document, with references to fabricated content.
    - Execution of document attempts to run malicious code that uses PowerShell commands to leverage Dynamic Data Exchange (DDE) to download a file.
  + Email delivered using SMTP2GO delivery service where senders IP can be masked.
  + The sender masqueraded as noreply@tv3.lt using [noreplay@tv3.lt](mailto:noreplay@tv3.lt)
* After successful execution of the DDE document, a string representing a secondary PowerShell command is downloaded. This runs a secondary file which sets persistence with a Run registry key - creating and running a VBS script.
  + VBS script is a basic launcher for the RADIOSTAR downloader.
    - Functionality of RADIOSTAR from here is unknown but general assumptions can be that it likely handles C&C commands to be executed on the victim’s machine.

The defamatory narrative would have aimed to decrease public opinion of the Lithuanian Defence Minister as well as encourage the emailed targets to engage with the malicious payload. Various public opinion polls have found very limited support for same-sex marriage, and opposition to same-sex marriage and homosexuality in general continues to be widespread in Lithuanian society. A GLOBSEC survey conducted in March 2023 showed that only 22% of Lithuanians supported same-sex marriage, while 60% were opposed and 18% were undecided.Only Bulgaria had lower support levels among EU countries. (Wikipedia Bulgaria, GLOBSEC, Wikipedia GLOBSEC)

## Frameworks

### ATT&CK Framework

* **TA0043: Reconnaissance**
  + **T1589.002:** Gather Victim Identity Information: Email Addresses
    - Adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.
    - *A link to the article hosted on the compromised site was also directly emailed to a targeted mailing list including government ministries and embassies.*
  + **T1591.004**: Gather Victim Org Information: Identify Roles
    - Adversaries may gather information about identities and roles within the victim organization that can be used during targeting. Information about business roles may reveal a variety of targetable details, including identifiable information for key personnel as well as what data/resources they have access to.
    - *Specific governmental entities were targeted.*
  + **T1598.001**: Phishing for Information: Spearphishing Service
    - Adversaries may send spearphishing messages via third-party services to elicit sensitive information that can be used during targeting.
    - *The email was sent using a legitimate email delivery service called SMTP2GO, which can be used to mask the sender’s real IP address. According to the report, the attacker attempted to spoof the sender to masquerade as tv3.lt but made a typo such that the sender was “*[*noreplay@tv3.lt*](mailto:noreplay@tv3.lt)*” instead of “*[*noreply@tv3.lt.*](mailto:noreply@tv3.lt.)*”*
  + **T1593.001**: Search Open Websites/Domains: Social Media
    - Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff.
    - *The lure document attached to the email purported to be a legitimate press release. It included a link to a fabricated article posted on the Tv3.lt website and an****appended legitimate copy and-pasted article on the defence minister.***
* **TA0001: Initial Access**
  + **T1078.002:** Valid Accounts: Domain Accounts
    - Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts can cover users, administrators, and services.
    - *Login details of administration accounts for Tv3.lt were harvested.*
  + **T1566.001**: Phishing: Spearphishing Attachment
    - Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing.
    - *The document was delivered via phishing email to Lithuanian media and government entities.*
  + **T1204.002**: User Execution: Malicious File
    - An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution.
  + **T1559.002**: Inter-Process Communication: Dynamic Data Exchange
    - Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands.
    - *Document contained a reference to the fabricated content, which leverages Dynamic Data Exchange (DDE) to download a file.*
  + **T1059.001**: Command and Scripting Interpreter: PowerShell
    - Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.
    - *After successful execution of the DDE document, a string representing a secondary PowerShell command is downloaded from C&C.*
  + **T1547.001**: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
    - Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.
    - *The PowerShell command downloads and runs a secondary file, h8.jse, which sets persistence with a Run registry key and created and ran splwow64.ps1.vbs.*

### DISARM Framework

* **PLAN**:
  + **TA01: Plan Strategy**
    - **T0073**: Determine Target Audiences
    - **T0074**: Determine Strategic Ends
  + **TA02: Plan Objectives**
    - **T0066**: Degrade Adversary
    - **T0079**: Divide
  + **TA13: Target Audience Analysis**
    - **T0072**: Segment Audiences
      * **T0072.002**: Demographic Segmentation
      * **T0072.004**: Psychographic Segmentation
    - **T0081**: Identify Social and Technical Vulnerabilities
      * **T0081.003**: Identify Existing Prejudices
      * **T0081.006**: Identify Wedge Issues
* **PREPARE:**
  + **TA14: Develop Narratives**
    - **T0082**: Develop New Narratives
  + **TA06: Develop Content**
    - **T0023**: Distort Facts
      * **T0023.002**: Edit Open-Source Content
    - **T0085**: Develop Text-based Content
      * **T0085.003**: Develop Inauthentic News Articles
  + **TA15: Establish Social Assets**
    - **T0013**: Create Inauthentic Websites
  + **TA16: Establish Legitimacy**
    - **T0089**: Establish Inauthentic News Sites
      * **T0098.001**: Create Inauthentic News Sites
  + **TA07: Select Channels and Affordances**
    - **T0108**: Blogging and Publishing Networks
    - **T0112**: Email
* **EXECUTE**
  + **TA09: Deliver Content**
    - **T0115**: Post Content
* **ASSESS**
  + **TA12: Assess Effectiveness**
    - **T0133**: Measure Effectiveness
      * **T0133.002**: Content
    - **T0134**: Measure Effectiveness Indicators (or KPIs)
      * **T0134.001**: Message Reach
      * **T0134.002**: Social Media Engagement

## Resources

Mandiant (2021) *GHOSTWRITER UPDATE: CYBER ESPIONAGE GROUP UNC1151 LIKELY CONDUCTS GHOSTWRITER INFLUENCE ACTIVITY*, *Ghostwriter update UNC1151*. Available at: <https://www.mandiant.com/resources/blog/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity>.

National Cyber Security Centre, Republic of Lithuania. (2018) *NATIONAL CYBER SECURITY CENTRE UNDER THE MINISTRY OF NATIONAL DEFENCE REPUBLIC OF LITHUANIA BRIEF REVIEW OF THE CYBER INCIDENT ANALYSIS No. 152827.* *National Cyber Security Centre, Republic of Lithuania*. Available at: <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion>.

Wikipedia, GLOBSEC. Available at: <https://en.wikipedia.org/wiki/GLOBSEC>

Wikipedia, Bulgaria. Available at: <https://en.wikipedia.org/wiki/Bulgaria>

*GLOBSEC Trends 2023 United We (Still) Stand* (2023) *GLOBSEC*. Available at: <https://www.globsec.org/sites/default/files/2023-05/GLOBSEC%20Trends%202023.pdf>.