**Cyber-Influence Operation Analysis:**

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

# UNC1151 2019 campaign: “Lithuanian minister of defence Raimundas Karoblis suspected of corruption”.

## Background Information

In April 2019, multiple news websites, email, and inauthentic accounts were involved in an information operation to promote a false narrative accusing the Lithuanian Minister of National Defence Raimundas Karoblis of corruption.1, 2.

Disinformation and cyber-attack vectors:1, 2.

* Direct email dissemination: email originated from an IP address identified as a dedicated actor-controlled server used by UNC1151. It was responsible for other political activism and journalism campaigns in Europe and the Middle East in January 2019.
* Spoofed emails of the Ministry of National Defence officer are distributed to representatives of state institutions of the Republic of Lithuania and other politicians.
* Compromise of multiple news sites: kaunas.kasvyksta[.]lt and baltictimes[.]com had a similar backdoor weakness, which led to both being compromised. Defamatory news articles posted on both.
* Inauthentic accounts: Multiple accounts pose as the editor of a Lithuanian media outlet to spread disinformation.
* 17-09-2018: Backdoor left in the news portal kaunas.kasvyksta[.]lt for future actions
  + File upload - lack of event logs mean we cannot determine how the file was uploaded to the system.
* 10-04-2019: Spoofed emails of the Ministry of National Defence officer are distributed including slanderous content on the Minister of National Defence.
  + IP is spoofed to avoid identification/mail server protection.
  + Content of email contained a 1x1 pixel invisible image that tells the sender who viewed the message and how many times they read the message.
* 11-09-2019: Backdoor in the news portal is used and the content of an article is replaced with defamatory information of the Minister of National Defence. Fake SIS website is hosted.
  + Using TOR network services, the adversary was able to conceal their location and usage of the network. The IP addresses of the nodes that were captured and used during the hack are associated with UNC1151.
  + The fake article had a hyperlink "notify SIS", which redirects to the same kaunas.kasvyksta[.]lt web portal. Here, there is a falsified version of the Special Investigation Service of the Republic of Lithuania website - where the defamatory content is repeated.
* 11-04-2019: An article slandering the Minister of National Defence is posted on baltictimes[.]com.
  + Similar backdoor to the kaunas.kasvyksta[.]lt portal.
  + Same defamatory information is posted here as well.

## 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.
    - *Emails were distributed to politicians and other representatives of state institutions for the Republic of Lithuania.*
  + **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.*
  + **T1598.003**: Phishing for Information: Spearphishing Link
    - Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information.
    - *A link, in the form of a 1x1 pixel invisible image, was inserted into the email. The purpose of the image is to inform the sender who has read the message and how many times they read it.*
* **TA0042: Resource Development**
  + **T1587.001:** Develop Capabilities: Malware
    - Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media.
    - *Publicly available software code was modified to create a backdoor for the operation.*
  + **T1588.001**: Obtain Capabilities: Malware
    - Adversaries may buy, steal, or download malware that can be used during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, packers, and C2 protocols.
    - *Publicly available software code was used to create a backdoor for the operation.*
  + **T1608.001**: Stage Capabilities: Upload Malware
    - Adversaries may upload malware to third-party or adversary-controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content.
    - *Publicly available software code was modified and placed in the news portal kaunas.kasvyksta[.]lt as a backdoor for the operation. Software code of a similar fashion is used to hack the news portal baltictimes[.]com*
* **TA0001: Initial Access**
  + **T1190:** Exploit Public-Facing Application
    - Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network.
    - *A backdoor was placed in the web portals kaunas.kasvyksta[.]lt and baltictimes[.]com*
  + **T1566.002**: Phishing: Spearphishing Link
    - Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing.
    - *An email sent to various Lithuanian governmental entities contained a link inserted in the message content.*
* **TA0040: Impact**
  + **T1491.002:** Defacement: External Defacement
    - An adversary may deface systems external to an organization in an attempt to deliver messaging, intimidate, or otherwise mislead an organization or users.
    - *The backdoor on the news portal kaunas.kasvyksta[.]lt was used to deface the website by publishing a fake news article on the Lithuanian Minister of National Defence. A hyperlink 'notify SIS' is placed in the fake article - redirecting to the same site and displays a fake Lithuanian Special Investigation Service website with corroborating slanderous information. Later, a backdoor is exploited on the baltictimes[.]com news portal where the website is hacked and defaced to display another slanderous article. This one references the kaunas.kasvyksta[.]lt article as the source of information.*

### DISARM Framework

* **PLAN**:
  + **TA01: Plan Strategy**
    - **T0073**: Determine Target Audiences
    - **T0074**: Determine Strategic Ends
  + **TA02: Plan Objectives**
    - **T0066**: Degrade Adversary
  + **TA13: Target Audience Analysis**
    - **T0072**: Segment Audiences
      * **T0072.005**: Political Segmentation
    - **T0081**: Identify Social and Technical Vulnerabilities
      * **T0081.003**: Identify Existing Prejudices
      * **T0081.003**: Identify Existing Conspiracy Narratives/Suspicions
      * **T0081.006**: Identify Wedge Issues
      * **T0081.007:** Identify Target Audience Adversaries
* **PREPARE:**
  + **TA14: Develop Narratives**
    - **T0022**: Leverage Conspiracy Theory Narratives
  + **TA06: Develop Content**
    - **T0085**: Develop Text-based Content
      * **T0085.003**: Develop Inauthentic News Articles
  + **TA15: Establish Social Assets**
    - **T0013**: Create Inauthentic Websites
  + **TA16: Establish Legitimacy**
    - **T0100**: Co-opt Trusted Sources
  + **TA07: Select Channels and Affordances**
    - **T0108**: Blogging and Publishing Networks
    - **T0112**: Email
* **EXECUTE**
  + **TA09: Deliver Content**
    - **T0115**: Post Content
* **ASSESS**
  + **TA12: Assess Effectiveness**
    - **T0132:** Measure Performance
      * **T0132.002**: Content Focused
    - **T0133**: Measure Effectiveness
      * **T0133.002**: Content
    - **T0134**: Measure Effectiveness Indicators (or KPIs)
      * **T0134.001**: Message Reach
      * **T0134.002**: Social Media Engagement

## Resources

[1] <https://www.mandiant.com/resources/blog/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity>

[2] <https://www.nksc.lt/doc/en/analysis/2019_04_30_Brief_targeted_attack_analysis.pdf>