**Cyber-Influence Operation Analysis:**

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

# Title of cyber-influence operation

## Summary

Provide a summary of the operation and its components.

## Timeline and Context

## ## Background Information

## Spearphishing component:

## - In response to sanctions against Russian athletes due to doping, GRU launged a multi-faceted campaign to disrupt the 2018 Winter Olympic Games.

## - Targeting Olympic partners and athletes, the IOC, South Korean government agencies, the International Olympic Committee, international and domestic visitors to South Korea, and Olympic Games IT providers.

## - From November 2017, reconnaissance, spearphishing email testing was conducted.

## - T1598.002: Phishing for Information: Spearphishing Attachment

## - From November 2017, spearphising emails were sent to the IOC, the Olympics, and Olympic partners.

## - Malicious email attachments were developed and attached to emails sent to official timekeeping partners and their subsidiaries.

## - Using the IOC's domain pyeongchang2018.com

## - Imitating the IOC Commission Chairman, Vice-President

## - olympicgameinfo@gmail[.]com used to send malware-laced Microsoft Word file.

## - Email was deleted immediately after

## - alert.safekorea@gmail[.]com used for malware-laced Microsoft Word files to download additional content from a GRU controlled domain templates-library[.]ml.

## - Malicious email links were embedded in images to redirect to GRU controlled websites that mimicked legitimate websites.

## - Spoofed email addresses were used to imitate the official domain of South Korea's National Counterterrorism Center.

## - Emails here included malware-laced documents that downloaded an image file. The file used an open-source steganography tool to establish an encrypted channel from the recipient's computer to the adversaries command-and-control server.

## - Open-source tool is Invoke-PSImage and had only been publicly available 8 days prior to use in these emails.

## - GRU registered domain names and created URLs for their malicious activities.

## - msrole[.]com/office\_conf (mimicking a Microsoft website)

## - jeojang[.]ga and a created subdomain mafra[.]go[.]kr[.]jeojang[.]ga, which mimicked a website belonging to the Korean Ministry of Agriculture, Food, and Rural Affairs.

## - olympicgameinfo@gmail[.]com used in spearphishing emails.

## - alert.safekorea@gmail[.]com used for malware-laced Microsoft Word files to download additional content from a GRU controlled domain templates-library[.]ml.

## - info@nctc[.]go.kr, the official domain of South Korea's National Counterterrorism Center, was spoofed using an email service. This was used to send malware-laced documents that downloaded an image file

## - Image file used open-source steganography tool to establish an encrypted channel from the recipient's computer to the adversaries command-and-control server. (Invoke-PSImage).

## - planning.department@pyeongchang2018[.]com, planning.department@olympic[.]org used to send malware-laced files.

## - service.department@olympic[.]org used to send emails to athletes

## - nctc.go@gmail[.]com used to send a spearphishing email, spoofed to appear to be from a South Korean telecommunications company listed as an Olympic partner at pyeongchan2018[.]com/en/partners - info.kr@nctc[.]go.kr

## - Malicious user executed powershell script sent via attachment

## - Fake resume attachment that when opened displayed a blurred version of the resume and a pop-up about needing to enable certain features to view the document. Once the option to enable the features is clicked, the blurred image is removed and a malicious PowerShell script would run and call the maliciou website msrole[.]com/office\_conf, from which the next stage of malware is downloaded.

## - GRU scanned Korean-based network infrastructure for vulnerabilities.

## - Further technical research was conducted on websites used by the Korean Sport and Olympic Committee, a Korean power company, and a Korean airport.

## - Around December 2017 to January 2018, South Korean nationals and international visitors to South Korea were targeted with malicious mobile applications.

## \* Adversaries used an email service that allowed for mass simultaneous emailing.

## \* This service enabled adversaries to send emails that appeared to come from legitimate organisations' domains i.e. IOC.

## \* Cyberattack prevented spectators from printing out reservations and attending the ceremony - resulting in an unusually high number of empty seats.

## \* Spread fear surrounding the safety of other Olympic events and the cost of sanctioning Russian athletes.

## \* The aim may have been to embarrass the International Olympic Committee and South Korean government by disrupting such a highly-viewed event.

## Malicious mobile application component:

## \* The Seoul Bus Tracker application became available to the public on December 18, 2017

## \* created and registered to a mobile application store on December 11, 2017.

## \* Application store identified and suspended the application before any downloads occurred.

## \* The HanMail application was created on December 25, 2017, and made available to the public the next day. Mimmicked the name of a legitimate Korean email service.

## \* Was promptly identified and suspended before any downloads occurred.

## \* The Hmail-App Naver Mail, Hanmail, Daum application mimicked the name of a legitimate Korean email service. It was created around December 28, 2017, and became available to the public on January 6, 2018.

## \* The application was installed on 47 accounts before the application store suspended the application.

## Olympic Destroyer malware component:

## - Around February 2018, Malware dubbed 'Olympic Destroyer' was deployed against computer systems used by the Olympic Games' information technology vendor and the PyeongChang Organizing Committee for the 2018 Olympic & Paralympic Winter Games.

## - Around February 9, 2018, employees of a company that provided IT support to the Olympic Games reported laptops unexpectedly rebooting with messages from BitLocker, a full-volume encryption feature, asking for a recovery key.

## - Multiple servers of the same IT company experienced the same behaviour.

## - This resulted in thousands of compromised devices used by the IT company and PyeongChang Organising Committee.

## - To compromise the IT company, adversaries:

## - First compromised the companies computer network, traversing the network to seek user credentials and information related to the IT services being provided to the 2018 Winter Olympics.

## - Upon compromising the workstation of a network architect employed by the IT company, the adversaries used this employee's credentials to obtain access to the IT companies network of computers supporting the 2018 Winter Olympics.

## - After successfully compromising a domain administration account, the adversaries obtained the access needed to deploy and execute the Olympic Destroyer malware.

## - The Olympic Destroyer malware was used to:

## - Steal valid user credentials from victim computers

## - Spread and replicate itself across a victim's computer network - using said credentials.

## - As the malware spread, it would overwrite itself to incorporate any additional usernames and passwords it had obtained previously.

## - This improved the success rate of spreading.

## - The malware would delete files from hard drives, force shutdowns, and impede rebooting and recovery by misconfiguring BitLocker.

## - Overall, make infected computer systems inoperable.

## - The adversaries obtained credentials, escalated privileges, and moved laterally throughout the IT company's network by:

## - Reconnaissance and lateral movement by using the initial compromised computer.

## - Stole credentials using an open-source, credential harvesting tool.

## - Sent a file to the compromised computer containing four sets of credentials, including plaintext passwords.

## - This assisted in privilege escalation, used to move laterally across the IT companies network.

## - Malicious PowerShell script containing versions of a credential harvesting tool used to gather user, IP address, and server data.

## - Script operates only in memory and is not easily detectable by antivirus software.

## - Several systems were accessed using compromised accounts. This was used to access a domain administration account. Thus, they were able to fully compromise that specific domain.

## - PowerShell scripts were used to dump credentials for more than 16,000 servers and computers of the IT company. This included approximately 400 unique account credentials associated with the compromised domain.

## - The initial compromised computer was used with the Domain Administration account and other domain computers to obtain and view Olympics-related files and to access Olympics-related websites.

## - On or about January 24, 2018, the conspirators moved stolen credentials and other files from the IT company's system to the Domain Administration Account's computer storage.

## - Accessed confidential files

## - On or about January 24, 26, 29, and 30, 2018, the conspirators used the Domain Administration Account to browse local and shared IT Company 1 network locations relating to the 2018 Winter Olympics.

## - On or about January 31, February 2, and February 7, 2018, Conspirators used Computer 1 to visit websites related to the Olympics - including pyeongchang2018.com... the other entity with computers affected by the Olympic Destroyer malware.

## - dms.pyeongchang2018.com - self-service password reset webpage

## - extranet,pyeongchang2018.com - password change, login, security check webpages

## - pwd.pyeongchang2018.com - password management webpages

## - From on or about January 24, 2018, to February 9, 2018, the conspirators repeatedly accessed and browsed files on a computer within Domain 1 that was used by a network architect for IT Company 1's Major Events team.

## - Ran malicious scripts, explored the computer for credentials and credential files relating to the PyeongChang Olympics, and pivoted to other computers.

## - Also accessed files that would be useful for understanding how IT Company 1's computer network was configured and for moving laterally across the computer network.

## - The conspirators used an IT Company 1 account to deploy the component of the Olympic Destroyer malware that wiped victim computers and servers and rendered them inoperable. The malware was also deployed to the PyeongChang Organising Committee's computer network.

## - The Olympic Destroyer (OD) malware was uploaded to IT Company 1's computer netowrk

## - the Conspirators used the IT Company 1 account to deploy and execute the wiper component of the OD malware.

## - Used a technique that permits the deployment of software to multiple computers in the same network at the same time.

## - The conspirators used a connection between IT Company 2's computer network and the PyeongChang Organising Committee's computer network to compromise computers within PyeongChang's network. The Conspirators then deployed the malware to 20 computers used by PyeongChang.

## - As before, the malware rebooted and wiped the computers.

## - Shortly after the deployment of the OD malware, the Conspirators logged into a Moscow-based server to locate news about the attacks and track the attacks' impacts.

## - The Conspirators attempted to hide their activities and avoid being identified as the perpetrators of the Olympic Destroyer attack

## - To obfuscate the true sorce of the malware, the code was created to emulated malware used by the Lazarus Group in North Korea. The Conspirators took months prior to analyse the Lazarus Group malware samples, system tools, and wipes.

## - An algorithm was used to obscure certain features of the OD malware, in order to hinder any post-attack investigation and avoid antivirus software.

## - A command-and-control implant was established on Computer 1 to create a single point of access between IT Company 1's internal network and a server hosted in France that the Conspirators controlled. This single tunnel allowed the Conspirators to better hide their activity on IT Company 1's network and to issue commands, install additional tools, and transfer data with respect to IT Company 1's computer system.Frameworks

### ATT&CK Framework

* **Tactic:** name
  + **Technique:** name
    - Description of technique.
    - *Justification of chosen technique*

### DISARM Framework

* **PHASE**:
  + **Tactic:** name
    - **Technique:** name

## Resources

## [Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment]( 2020\_10\_19\_unsealed\_indictment\_0.pdf)

## [NY Times](https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html#:~:text=The%20cyberattack%20took%20out%20internet,high%20number%20of%20empty%20seats)]

## [RAND](https://www.rand.org/pubs/commentary/2018/02/why-the-2018-winter-olympics-are-the-perfect-storm.html)

## [WIRED](https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/)

## [IT News](https://www.itnews.com.au/news/winter-olympics-suffers-cyber-attack-484949)

## [Cyberlaw](https://cyberlaw.ccdcoe.org/wiki/Olympic\_Destroyer\_(2018))