**Cyber-Influence Operation Analysis:**

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

# GRU 2018 Winter Olympics Malware and Spearphishing Campaign

## Summary

Likely in response to sanctions against Russian athletes due to doping, GRU launched a multi-faceted campaign to disrupt the 2018 Winter Olympic Games. The operation targeted 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. The threat actors used Olympic Destroyer malware in an offensive cyberattack to disrupt and disable computers and networks used in Winter Olympic operations. The malware disrupted internal servers, crashed the Olympic website, public Wi-Fi, ticketing services, and aspects of the opening ceremony. The motivation is likely political, aiming to embarrass the South Korean government and International Olympic Committee (IOC), and create diplomatic tensions and fears.

## Timeline and Context

Spearphishing component of the campaign:

* From November 2017 onwards, reconnaissance and spearphishing was conducted. Emails were sent to the IOC, the Olympics, and Olympic partners. Recipients included official timekeeping partners and their subsidiaries.
  + GRU scanned Korean-based network infrastructure for vulnerabilities.
  + Malicious email attachments were developed and attached to emails using the IOC’s domain ‘pyeongchang2018.com’ and imitating the IOC Commission Chairman and Vice-President.
  + Malware-laced Microsoft word files were sent using phishing emails ‘olympicgameinfo@gmail.com’ and ‘alert.safekorea@gmail.com’.
    - Files from the latter were used to download additional content from a GRU controlled domain, ‘templates-library.ml’.
  + Malicious email links were embedded in images to redirect users to GRU controlled websites that mimicked legitimate websites.
  + Spoofed email addresses were used to imitate the official domain of South Korea’s National Counterterrorism Centre.
    - Malware-laced documents included in these emails. Document downloads an image file that uses Invoke-PSImage, an open-source steganography tool, to establish an encrypted channel to the threat actor’s command-and-control server.
      * Invoke-PSImage became publicly available 8 days prior to emails.
  + Malicious emails contained fake resume attachment that contained a user executed PowerShell script.
    - Blurred version of resume displayed, and the user is prompted to enable certain features to view the document. Once the user enables the features, the blurred image is removed, and a malicious PowerShell script runs and attempts to download the next stage of malware.
* GRU registered domain/subdomain names and created URLs for their malicious activities.
  + Many instances, mimicking services such as a Microsoft website, the Korean Ministry of Agriculture, Food, and Rural Affairs, the Olympics, South Korea’s National Counterterrorism Center, various Olympic planning and service entities and partners, and South Korean telecommunications services.
* The threat actors used an email service that allowed for mass simultaneous emailing. This allowed emails to appear to come from legitimate organisations’ domains i.e. IOC.

Olympic Destroyer malware component of the campaign:

* Malware was deployed around February 2018 against computer systems used by the Olympic Games' information technology vendor and the PyeongChang Organizing Committee for the 2018 Olympic & Paralympic Winter Games.
  + Initially, employees of a company (company 1) 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.
  + Widespread deployment of the malware across multiple companies led to the compromise of thousands of devices used by the IT company and PyeongChang Organising Committee.
* The malware was designed to knock computers offline by deleting critical system files, which would render the machines useless. The result saw internal servers including the Olympic website, display monitors and public Wi-Fi to crash. This denied the ability to view the events schedule, print tickets for some attendees, and meant some drones intended to be used in the opening ceremony failed to deploy.
* In December 2017, the adversaries had begun compromising the computer network of the IT company that provided services to the PyeongChang Organizing Committee (company 2). Later in the month, the adversaries begun compromising another company that provided IT support to the Olympic Games (company 1).
* After compromising company 1’s computer network, the adversaries engaged in a variety of illicit activities to perform reconnaissance, obtain credentials, escalate privileges, and move laterally throughout the network.
  + Credentials were stolen using an open-source credential harvesting tool.
  + A file containing credentials and plaintext passwords was sent to a compromised computer to assist in lateral movement via privilege escalation.
  + A malicious PowerShell script was executed containing versions of a credential harvesting tool designed to gather user, IP address, and server data.
  + Stolen credentials were used to access a domain administration account.
  + PowerShell scripts were used to dump credentials from more than 16,000 computers and servers belonging to company 1.
  + Unauthorised file access was likely used to help understand the companies computer network architecture and configuration, and move laterally across the computer network.
* The adversaries used a compromised account to deploy the Olympic Destroyer malware on the computer network of company 1.
  + The account was also used to deploy and execute the wiper component of the Olympic Destroyer malware within the compromised domain of the company. This was achieved with a technique the permits the deployment of software to multiple computers in the same network at the same time. This deployment was facilitated by GRU developed malware.
* A connection between company 2’s computer network and the PyeongChang Organising Committee’s computer network was used to compromise key computers within the Committee’s network and deploy the malware on those computers.
* The adversaries attempted to hide their activities and avoid being identified by:
  + Obfuscating the true source of the malware – emulating malware used by the Lazarus Group in North Korea.
  + Obscuring certain features of the malware – hindering any post-attack investigation and avoiding antivirus software.
  + Established command-and-control implant on only one computer to create a single point of access between company 1 and the GRU controlled server. This reduced the chances of detection, while still allowing the adversaries to issue commands, install additional tools, and transfer data.
* After the attacks, the adversaries logged into a Moscow-based server to locate news about the attacks and track the attacks' impacts.

## Frameworks

### ATT&CK Framework

* TA0043: Reconnaissance
  + T1595 Active Scanning
    - T1595.002 Vulnerability Scanning
  + T1589 Gather Victim Identity Information
    - T1589.002 Email Addresses
    - T1589.003 Employee Names
  + T1590 Gather Victim Network Information
    - T1590.001 Domain Properties
  + T1591 Gather Victim Org Information
    - T1591.002 Business Relationships
      * Spoofed emails and domains mimicking several entities involved in planning and safety of the Olympic games were used in phishing campaign.
  + T1598 Phishing for Information
    - T1598.002 Spearphishing Attachment
* TA0042 Resource Development
  + T1583 Acquire Infrastructure
    - T1583.001 Domains
  + T1587 Develop Capabilities
    - T1587.001 Develop Capabilities: Malware
  + T1585 Establish Accounts
    - T1585.001 Email Accounts
  + T1588 Obtain Capabilities
    - T1588.002 Tool
      * Stenography tool
      * Mass emailing service
  + T1608 Stage Capabilities
    - T1608.001 Upload Malware
      * alert.safekorea@gmail[.]com used for malware-laced Microsoft Word files to download additional content from a GRU controlled domain templates-library[.]ml.
      * malware-laced documents that downloaded an image file, which used open-source steganography tool to establish an encrypted channel from the recipient's computer to the adversaries command-and-control server.
      * Malicious mobile applications uploaded to application store.
* TA0001 Initial Access
  + T1566 Phishing
    - T1566.001 Spearphishing Attachment
  + T1078 Valid Accounts
    - T1078.002 Domain Accounts
* TA0002 Execution
  + T1059 Command and Scripting Interpreter
    - T1059.001 PowerShell
  + T1569 System Services
    - T1569.002 Service Execution
      * Olympic Destroyer uses PsExec to help propagate itself across a network.
  + T1204 User Execution
    - T1204.002 Malicious File
  + T1047 Windows Management Instrumentation
    - Olympic Destroyer uses WMI to help propagate itself across a network
* TA0003 Persistence
  + T1078 Valid Accounts
    - T1078.002 Domain Accounts
* TA0005 Defense Evasion
  + T1070 Indicator Removal
    - T1070.001 Clear Windows Event Logs
* TA0006 Credential Access
  + T1555 Credentials from Password Stores
    - T1555.003 Credentials from Web Browsers
  + T1003 OS Credential Dumping
    - T1003.001 LSASS Memory
* TA0007 Discovery
  + T1135 Network Share Discovery
    - Olympic Destroyer will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares.
  + T1018 Remote System Discovery
    - Olympic Destroyer uses WMI to enumerate all systems in the network.
  + T1016 System Network Configuration Discovery
    - Olympic Destroyer uses API calls to enumerate the infected system's ARP table.
* TA008 Lateral Movement
  + T1570 Lateral Tool Transfer
    - Olympic Destroyer attempts to copy itself to remote machines on the network.
  + T1021 Remote Services
    - T1021.002 SMB/Windows Admin Shares
      * Olympic Destroyer uses PSExec to interact with the hidden, full control administrator account ADMIN$ network share to execute commands on remote systems.
* TA0009 Collection
  + T1119 Automated Collection
    - PowerShell script credential harvesting tool used.
  + T1074 Data Staged
    - T1074.001 Local Data Staging
      * Stolen credentials and other files were moved to the Domain Administration Account's computer storage prior to exfiltration.
* TA0011 Command and Control
  + T1001 Data Obfuscation
    - T1001.002 Steganography
  + T1105 Ingress Tool Transfer
* TA0040 Impact
  + T1485 Data Destruction
    - Olympic destroyer overwrites files locally and on remote shares.
  + T1490 Inhibit System Recovery
    - Olympic Destroyer uses the native windows utilities vssadmin, wbadnim, and bcdedit to delete and disable operating system recovery features such as the Windows backup catalog and Windows Automatic Repair. It forced shutdowns, and impeded rebooting and recovery by misconfiguring BitLocker.

### DISARM Framework

**PLAN**

* TA01 Plan Strategy
  + T0073 Determine Target Audiences
  + T0074 Determine Strategic Ends
* TA02 Plan Objectives
  + T0066 Degrade Adversary
* TA13 Target Audience Analysis
  + T0080 Map Target Audience Information Environment
    - T0080.005 Assess Degree/Type of Media Access
  + T0081 Identify Social and Technical Vulnerabilities

**EXECUTE**

* TA11 Persist in the Information Environment
  + T0129 Conceal Operational Activity
    - T0129.003 Break Association with Content
    - T0129.10 Misattribute Activity
  + T0130 Conceal Infrastructure

**ASSESS**

* TA12 Assess Effectiveness
  + T0132 Measure Performance
    - T0132.003 View Focused
  + T0133 Measure Effectiveness
    - T0133.001 Behaviour Changes
    - T0133.003 Awareness
    - T0133.004 Knowledge
    - T0133.005 Action/attitude
  + T0134 Measure Effectiveness Indicators (or KPIs)
    - T0134.002 Social Media Engagement

## Resources

## Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment (2020) Unsealed Indictment. Available at: <https://autonome-antifa.org/IMG/pdf/2020_10_19_unsealed_indictment_0.pdf>.

## Perlroth, N. (2018) Cyberattack caused olympic opening ceremony disruption, The New York Times. Available at: <https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html#:~:text=The%20cyberattack%20took%20out%20internet,high%20number%20of%20empty%20seats>.

## Silfversten, E. (2018) *Why the 2018 Winter Olympics are the perfect storm for cyberattacks | Rand*, *Why the 2018 Winter Olympics Are the Perfect Storm for Cyberattacks*. Available at: <https://www.rand.org/pubs/commentary/2018/02/why-the-2018-winter-olympics-are-the-perfect-storm.html>.

## Greenberg, A. (2019) *Inside olympic destroyer, the most deceptive hack in history*, *Wired*. Available at: <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>.

## Grohmann, K. (2018) *Winter Olympics suffers cyber attack*, *iTnews*. Available at: <https://www.itnews.com.au/news/winter-olympics-suffers-cyber-attack-484949>.

## International cyber law: interactive toolkit (2021) *Olympic destroyer (2018)*, Available at: <https://cyberlaw.ccdcoe.org/wiki/Olympic_Destroyer_(2018)>.

*Olympic Destroyer, Software S0365 | MITRE ATT&CK®*. Available at: <https://attack.mitre.org/software/S0365/>.