**Cyber-Influence Operation Analysis:**

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

# 2016 Attack on Ukraine Treasury and Financial services

## Summary

Ukraine is subject to many cyberattacks and disinformation campaigns as part of the ongoing Russo-Ukrainian war. In December 2016, Ukraine was subject to attacks on its finance and defence ministries and the State Treasury that allocates cash to government institutions. The attack halted the State Treasury systems for several days, meaning state workers and pensioners had been unable to receive their salaries or payments on time. Destructive malware was used in conjunction with KillDisk to destroy data and block access to networks. The State Treasury Service’s regional subdivisions were disconnected from the State Treasury Service's automated payment system. This prevented the execution of approximately 150,000 electronic transactions and temporarily disabled the Ministry of Finance's information and telecommunication infrastructure.

This attack supports the ongoing Russian fear-based narratives directed towards Ukraine. These narratives rely on degrading trust in Ukrainian services, segmenting populations, and fostering concern and distress through offensive cyberspace operations.

## Timeline and Context

October 2016

* Spearphishing campaign using malicious malware-laced attachments targeted State Treasury Service’s system administrators.
  + Malicious Microsoft Excel file developed that required user to enable macros. Allowing macros to run resulted in the execution of the malware-laced file ‘explorer.exe’.
* A system administrator for the State Treasury Service opens the Excel file and enables macros. This establishes an unauthorized, cover encrypted communication between the computer and a third-party service used by the adversaries.
* A dedicated network connection between the State Treasury Service and Ukraine’s Ministry of Finance is exploited to obtain unauthorised access to the Ministry of Finance’s computer network.

December 2016

* As Ukraine prepared for end-of-year pension payments as well as the following year’s budget, destructive malware was deployed against the Ministry of Finance and State Treasury Service.
* On or about December 6, the adversaries deployed an updated version of the KillDisk malware-which was very similar to the version of the KillDisk malware the Conspirators used in the December 2015 cyber-attacks against Ukraine's electric power grid.
* KillDisk used three different options to invoke different behaviours:

1. delete the infected computers' Windows event logs.
2. Delete all the files that matched a list of file extensions hardcoded into the malware.
3. Overwrite portions of the infected computers' hard drives, thus rendering the computers inoperable.

## Frameworks

### ATT&CK Framework

* **TA0043: Reconnaissance**
  + T1589 Gather Victim Identity Information
    - T1589.002 Email Addresses
    - T1589.003 Employee Names
  + T1593 Search Open Websites/Domains
* **TA0042 Resource Development**
  + T1585 Establish Accounts
    - T1585.002 Email Accounts
  + T1588 Obtain Capabilities
    - T1588.001 Malware
      * KillDisk
  + T1608 Stage Capabilities
    - T1608.001 Upload Malware
* **TA0001 Initial Access**
  + T1566 Phishing
    - T1566.001 Spearphishing Attachment
* **TA0002 Execution**
  + T1106 Native API
    - KillDisk has called the Windows API to retrieve the hard disk handle and shut down the machines.
* **TA0005 Defense Evasion**
  + T1070 Indicator Removal
    - T1070.001 Clear Windows Event Logs
      * KillDisk deletes application, security, setup, and system windows event logs.
    - T1070.004 File Deletion
      * KillDisk can quit and delete itself.
* **TA0007 Discovery**
  + T1124 System Time Discovery
    - KillDisk option to set a specific date and time to execute the malware's destructive mode.
* **TA0011 Command and Control**
  + T1573 Encrypted Channel
    - Execution of Excel file macros established encrypted communications between the computer and a third-party service used by the adversaries.
* **TA0040 Impact**
  + T1485 Data Destruction
    - KillDisk deletes key system files to make the OS unbootable.
    - KillDisk option enabled to destroy all files on the infected computer that ended with one of more than 100 different file extensions.
  + T1565 Data Manipulation
    - T1565.001 Stored Data Manipulation
      * KillDisk malware overwrites files in a set area of the computer's memory.
  + T1491 Defacement
    - T1491.001 Internal Defacement
      * KillDisk malware draws "fsociety" mask image in memory and displays the image on the victim's computer screen on top of all other graphical windows.
  + T1529 System Shutdown/Reboot
    - KillDisk rebooted the compromised computer systems.

### DISARM Framework

**PLAN**

* TA01 Plan Strategy
  + T0073 Determine Target Audiences
  + T0074 Determine Strategic Ends
* TA02 Plan Objectives
  + T0066 Degrade Adversary
  + T0078 Dismay
  + T0079 Divide
* TA13 Target Audience Analysis
  + T0081 Identify Social and Technical Vulnerabilities

**PREPARE**

* TA14 Develop Narratives
  + T0068 Respond to Breaking News Event or Active Crisis

**EXECUTE**

* TA18 Drive Online Harms
  + T0123 Control Information Environment through Offensive Cyberspace Operations
* TA11 Persist in the Information Environment
  + T0129 Conceal Operational Activity
    - T0129.003 Break Association with Content
    - T0129.006 Deny Involvement
  + T0130 Conceal Infrastructure
    - T0130.004 Use Cryptocurrency
    - T0130.005 Obfuscate Payment

**ASSESS**

* TA12 Assess Effectiveness
  + T0132 Measure Performance
    - T0132.003 View Focused
  + T0133 Measure Effectiveness
    - 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\_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))