**Cyber-Influence Operation Analysis:**

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

# GRU 2017 NotPetya malware deployment on Ukrainian entities

## Summary

The NotPetya malware-based attack that occurred starting June 27, 2017 was part of the Kremlin's ongoing effort to destabilize Ukraine, particularly by disrupting Ukraine's financial systems. Ultimately, it affected systems globally, including those in Russia, the UK, the US, and Australia. NotPetya successfully infected thousands of computers used in financial, energy and government institutions throughout Ukraine - demanding a ransom payment and self-propagating itself within a network. The attack was executed on the eve of Ukraine's Constitution Day, commemorating the country's departure from the Soviet Union. It rendered inoperable the computer systems used by Ukrainian organisations such as banks, newspapers, transportation, and electricity companies.

While NotPetya appears as a form of ransomware, its main purpose was to destroy data and disk structures on compromised systems; the attackers never intended to make the encrypted data recoverable. Referencing the $300 ransomware demand, Ukraine's state security service said "the virus is cover for a large-scale attack on Ukraine. This is evidenced by a lack of a real mechanism for taking possession of the funds ... enrichment was not the aim of the attack. The main purpose of the virus was the destruction of important data, disrupting the work of public and private institutions in Ukraine and spreading panic among the people.".

This style of highly visible cyberattack on Ukrainian services is part of the Kremlin's hybrid warfare approach to the ongoing Russo-Ukrainian conflict. This approach aims to foster fear-based narratives within Ukraine and display strength and aggression. It can also attract media to disseminate narrative and/or draw attention away from other actions.

## Timeline and Context

See resources - in particular, the indictment "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment" - for a detailed technical analysis of the cyberattack.

* The GRU disseminated the NotPetya malware using a popular Ukrainian accounting software called M.E.Doc that was used to facilitate the communication of tax information to the Ukrainian government.
* The software was periodically updated through an update server.
  + Attacks were facilitated by rerouting internet traffic from (1) computers attempting to update the M.E.Doc software via the Update Server to (2) a France-based server controlled by the GRU. This France-based server delivered the malware to the victim computers that connected to it.

April 2017

* GRU hackers familiarise themselves with M.E.Doc software and the Ukrainian EDRPOU number (equivalent of a tax file number in the US). This includes querying the EDRPOU website and computer language sets specific to the Ukrainian alphabet.
* GRU gains access to the software code for the M.E.Doc software prior to the NotPetya attacks. Allowing the hackers to test malicious functionality.
* The GRU publishes the first malicious update file to the update server.

June 2017

* On or about June 27, the NotPetya malware was delivered to computers that attempted to receive a malicious software update from the Update Server.
  + Once a victims computer downloaded the malicious update file and the GRU rerouted the network traffic, victim computers could remotely receive and execute GRU commands.
* The malware propagated itself and wiped data from victim computers.
* The malware appeared to be ransomware. Perhaps in an attempt to appear as if some other group other than a nation state were the culprits of the attack.

## Frameworks

### ATT&CK Framework

* TA0043 Reconnaissance
  + T1593 Search Open Websites/Domains
    - Querying the EDRPOU website and computer language sets specific to the Ukrainian alphabet.
* TA0042 Resource Development
  + T1587 Develop Capabilities
    - T1587.001 Malware
  + T1588 Obtain Capabilities
    - T1588.006 Vulnerabilities
      * GRU gains access to the software code for the M.E.Doc software prior to the NotPetya attacks.
* TA0001 Initial Access
  + T1078 Valid Accounts
    - T1078.003 Local Accounts
      * NotPetya can use valid credentials to spread itself to remote systems.
* TA0002 Execution
  + T1053 Scheduled Task/Job
    - T1053.005 Scheduled Task
      * NotPetya creates a task to reboot the system one hour after infection.
  + T1569 System Services
    - T1569.002 Service Execution
      * NotPetya can use PsExec to help propagate itself across a network.
  + T1047 Windows Management Instrumentation
    - NotPetya can use wmic to help propagate itslef across a network.
* TA0003 Persistence
  + T1053 Scheduled Task/Job
    - T1053.005 Scheduled Task
  + T1078 Valid Accounts
    - T1078.003 Local Accounts
* TA0005 Defense Evasion
  + T1070 Indicator Removal
    - T1070.001 NotPetya uses wevtutil to clear the Windows event logs.
  + T1036 Masquerading
  + T1218 System Binary Proxy Execution
    - T1218.011 NotPetya installs itself on remote systems.
  + T1078 Valid Accounts
    - T1078.003 Local Accounts
* TA0006 Credential Access
  + T1003 OS Credential Dumping
    - T1003.001 LSASS Memory
      * NotPetya contains a modified version of Mimikatz to help gather credentials that are later used for lateral movement.
* TA0007 Discovery
  + T1083 File and Directory Discovery
    - NotPetya searches for files ending with dozens of different file extensions prior to encryption.
  + T1518 Software Discovery
    - T1518.001 Security Software Discovery
      * NotPetya determines if specific antivirus programs are running on an infected host machine.
* TA0008 Lateral Movement
  + T1210 Exploitation of Remote Services
    - NotPetya can use two exploits in SMBv1 to spread itself to other remote systems on the network.
  + T1021 Remote Services
    - T1021.002 SMB/Windows Admin Shares
      * NotPetya can use PsExec which interacts with administrator network (ADMIN$) share to execute commands on remote systems.
* TA0040 Impact
  + T1486 Data Encrypted for Impact
    - NotPetya encrypts user files and disk structures with 2048-bit RSA.
  + T1529 System Shutdown/Reboot
    - NotPetya will reboot the system one hour after infection.

### 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
      * T0072.001 Geographic Segmentation
      * T0072.003 Economic Segmentation
      * T0072.005 Political Segmentation
* **PREPARE**
  + TA14 Develop Narratives
    - T0003 Leverage Existing Narratives
    - T0068 Respond to Breaking News Event or Active Crisis
    - T0083 Integrate Target Audience Vulnerabilities into Narrative
  + TA16 Establish Legitimacy
    - T0097 Create personas
* **EXECUTE**
  + TA08 Conduct Pump Priming
    - T0042 Seed Kernel of truth
  + TA11 Persist in the Information Environment
    - T0129 Conceal Operational Activity
      * T0129.006 Deny involvement
      * T0129.010 Misattribute Activity
  + TA12 Assess Effectiveness
    - T0132 Measure Performance
      * T0132.002 Content Focused
      * T123.003 View Focused
    - T0133 Measure Effectiveness
      * T0133.001 Behaviour Changes
      * T0133.002 Content
      * T0133.003 Awareness
      * T0133.005 Action/Attitude
    - T0134 Measure Effectiveness Indicators (or KPIs)
      * T0134.001 Message Reach
      * T0134.002 Social Media Engagement

## Resources

<https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-russian-cyber-unit-that-hacks-targets-on-site/>

<https://cyberscoop.com/uk-government-blames-russian-military-infamous-notpetya-cyberattacks/>

<https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P/>

<https://arstechnica.com/information-technology/2017/06/notpetya-developers-obtained-nsa-exploits-weeks-before-their-public-leak/>

<https://attack.mitre.org/software/S0368/>

<https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

<https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html>

<https://www.washingtonpost.com/world/national-security/this-weeks-global-ransomware-attack-was-a-ruse-to-deflect-attention-from-the-true-culprit-researchers-say/2017/06/29/da455a0e-5cf0-11e7-9b7d-14576dc0f39d_story.html>