**Cyber-Influence Operation Analysis:**

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

# GRU & IRA 2016 hacking and leaking of Clinton presidential campaign emails

## Summary

During the 2016 United States elections, Russian interference through the GRU and IRA aimed to sabotage the presidential campaign of Hillary Clinton and increase support for Donald Trump's presidential campaign while amplifying social and political discord in the U.S. The adversaries used a variety of means to hack Clinton campaign officials, the Democratic Congressional Campaign Committee (DCCC), and the Democratic National Committee (DNC). The adversaries stole hundreds of thousands of documents from the compromised email accounts and networks. This data was publicly released through the fictitious online personas “DCLeaks” and “Guccifer 2.0.”, later releasing additional materials through the organization WikiLeaks.

The IRA supported the data leak with troll farms and thousands of social media accounts purported to be Americans supporting radical political groups. These accounts encouraged attendance and/or created events in support of the Trump campaign. The social media campaign and the GRU hacking operations coincided with a series of contacts between Trump Campaign officials and individuals with ties to the Russian government. One such method was using click-fraud malware to enhance the visibility of troll farm content created by the IRA. This malware was dubbed ’FaceMusic’. FaceMusic was a click-fraud malware developed by the IRA in 2016 that aimed to enhance the visibility of troll farm content used by the IRA to disseminate Russian narratives. This is represented at a high-level in the model, and a complete version can be found in the ceios database.

## Timeline and Context

September – November 2015

* The FBI contacts the DNC to caution the IT department of a compromised computer by Russian hackers. DNC management states IT technicians failed to respond appropriately to the breach.

March onwards 2016

* Starting in at least March 2016, the adversaries used a variety of means to hack the email accounts of volunteers and employees of the Clinton campaign. This included the campaign’s chairman, John Podesta.
  + Beginning by at least March 2016, the adversaries targeted over 300 individuals affiliated with the Clinton campaign, DCCC, and DNC.
    - Used URL-shortening services in conjunction with leased VPN.
    - Spearphishing campaigns conducted with an email account created in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton campaign.
      * Spoofing email address
    - Emails looked like security notification from Google, stating that another user had tried to access the account and instructing users to change their password by clicking an embedded link.
    - Used embedded links purporting to direct the recipient to a document titled "hillary-clinton-favorable-rating.xlsx" - in fact this redirected to a GRU-created website.
  + Research into the names of victims and their association with the Clinton campaign on various social media sites led to targeted spearphishing operations.
* John Podesta receives the phishing email masked as an alert from Google. The form in the embedded link is filled and the hackers are allowed access to his email.
* Credentials of a DCCC employee stolen through phishing email.
* In addition to spearphishing efforts, research conducted into the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.
  + Ran technical query for the DNC's internet protocol configurations to identify connected devices.
  + Searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.
  + Ran technical query for the DCCC's internet protocol configurations to identify connected devices.

April onwards 2016

* On or about April 12, 2016, stolen credentials of a DCCC employee used to access the DCCC network.
  + Installed and managed different types of malware to explore the DCCC network and steal data.
  + Installed multiple version of the X-Agent malware on at least ten DCCC computers, which allowed them to monitor individual employees' computer activity (e.g., keylogging), steal passwords, and maintain access to the DCCC network, transmit information between victim devices and a GRU-leased server located in Arizona. Overseas computer configured to relay communications between X-Agent malware and Arizona server.
* On or about April 18, 2016, the adversaries hacked into the DNC’s computers through their access to the DCCC network. The adversaries then installed and managed different types of malware (as with the DCCC network) to explore the DNC network and steal documents.
  + By in or around June 2016, access gained to approximately thirty-three DNC computers.
  + The Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees.
* To steal the large volume of documents at once without detection, the adversaries used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. GRU malware, known as “X-Tunnel,” was used to exfiltrate the stolen documents through encrypted channels.
  + Operational evidence obfuscated by intentionally deleting logs and computer files.
* FaceMusic was promoted through Facebook ads on or about May 2016. Promotions ran through one of the IRA’s fraudulent profiles “Stop All Invaders”.
  + More than 13,000 machines were likely infected by the malware.
  + The malware was used to enhance the visibility of troll farm content used by IRA accounts. Thus, expanding the reach of the content.
* Domain dcleaks.com registered through a service that anonymized the registrant. Website was hosted through a leased server in Malaysia.
  + On or about June 8, 2016, approximately the same time that the dcleaks.com website was launched, a DCLeaks Facebook page is created using a pre-existing fictitious social media account.
  + Twitter account @dcleaks\_ was also created and operated from Russian military computer infrastructure.
* On or about June 14, 2016, the adversaries created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.
  + Published post on a blog site created through WordPress titled "DNC's servers hacked by a lone hacker".
* Guccifer 2.0 used to release and share stolen documents - some to candidates for the U.S. Congress/media/news/reporters.
  + GRU purchased VPN used to log into Guccifer profiles including @Guccifer\_2 Twitter account. VPN account opened from the same server used to register malicious domains for the hacking of the DCCC and DNC networks.

July onwards, 2016

WikiLeaks publishes emails and documents hacked from the DNC server.

## Frameworks

### ATT&CK Framework

* **TA0043: Reconnaissance**
  + T1592 Gather Victim Host Information
    - Research conducted into the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.
    - Ran technical query for the DNC's and DCCC's internet protocol configurations to identify connected devices.
    - Ensuring malware and other applications worked on DCCC and DNC networks.
  + T1589 Gather Victim Identity Information
    - T1589.001 Gather Victim Identity Information: Credentials
      * Gathering login credentials for DNC and DCCC accounts.
    - T1589.002 Gather Victim Identity Information: Email Addresses
      * Used for spearphishing campaign.
    - T1589.003 Gather Victim Identity Information: Employee Names
      * Used for spearphishing campaign.
  + T1590 Gather Victim Network Information
    - T1590.004 Gather Victim Network Information: Network Topology
      * Used to find/gather information, create backdoors, install malware appropriately.
  + T1598 Phishing for Information
    - T1598.003 Phishing for Information: Spearphishing Link
      * Spearphishing emails containing malicious links sent to over 300 individuals affiliated with the Clinton Campaign, DCCC, and DNC.
  + T1593 Search Open Websites/Domains
    - T1593.001 Search Open Websites/Domains: Social Media
      * Research into the names of victims and their association with the Clinton Campaign.
    - T1593.002 Search Open Websites/Domains: Search Engines
      * Research into the names of victims and their association with the Clinton Campaign.
  + T1594 Search Victim-Owned Websites
    - The conspirators targeted state and county offices responsible for administering the 2016 U.S. elections. visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.
* **TA0042: Resource Development**
  + T1583 Acquire Infrastructure
    - T1583.001 Acquire Infrastructure: Domains
      * Notable domain registered was dcleaks.com.
    - T1583.003 Acquire Infrastructure: Virtual Private Server
      * The Conspirators purchased a virtual private network (“VPN”) account and to leased a server in Malaysia.
    - T1583.004 Acquire Infrastructure: Server
      * The Conspirators purchased a virtual private network (“VPN”) account and to leased a server in Malaysia.
    - T1583.005 Acquire Infrastructure: Botnet
      * IRA extensively used botnets to distribute to proliferate designated messaging.
  + T1586 Compromise Accounts
    - T1586.002 Compromise Accounts: Email Accounts
      * Outcome of spearphishing campaign.
  + T1587 Develop Capabilities
    - T1587.001 Develop Capabilities: Malware
      * GRU developed X-Agent malware, which was implanted on computers during the hacking of the DCCC and DNC networks.
      * FaceMusic developed by IRA.
  + T1585 Establish Accounts
    - T1585.001 Establish Accounts: Social Media Accounts
      * Social media accounts such as DCLeaks on Facebook and @dcleaks\_ on twitter were used to support operations.
      * IRA-operated social media account “Stop All Invaders” account used to promote FaceMusic malware.
    - T1585.002 Establish Accounts: Email Accounts
      * Email accounts used to acquire infrastructure and perform the spearphishing campaign.
  + T1588 Obtain Capabilities
    - T1588.002 Tool
  + T1608 Stage Capabilities
    - 1608.001 Stage Capabilities: Upload Malware
      * Malware implemented into DCCC and DNC infrastructure.
    - 1608.002 Stage Capabilities: Upload Tool
* **TA0001 Initial Access**
  + T1189 Drive-by Compromise
    - FaceMusic was advertised as an embedded music player for Chrome. User visits the chrome plug-in website for FaceMusic and installs the malware.
  + T1566 Phishing
    - T1566.002 Spearphishing Link
      * Spearphishing links used in contexts such as mock google forms and supposed document links.
  + T1078 Valid Accounts
    - Credentials were harvested via spearphishing campaigns. These accounts facilitated initial access to DCCC and DNC infrastructure.
* **TA0005 Defense Evasion**
  + T1070 Indicator Removal
    - T1070.001 Indicator Removal: Clear Windows Event Logs
      * Logs and computer files were intentionally deleted to cover tracks.
    - T1070.002 Indicator Removal: Clear Linux or Mac System Logs
      * Linux-based version of X-Agent was used.
    - T1070.004 Indicator Removal: File Deletion
      * Computer files were intentionally deleted to cover tracks. CCleaner was used on the DCCC network in an attempt to delete traces.
  + T1027 Obfuscated Files or Information
    - T1027.001 Obfuscated Files or Information: Binary Padding
      * X-Tunnel inserts junk code into the binary in a likely attempt to obfuscate it and bypass security products.
* **TA0006 Credential Access**
  + T1056 Input Capture
    - T1056.001 Input Capture: Keylogging
      * Keylog function of X-Agent malware used to capture user keystrokes.
  + T1552 Unsecured Credentials
    - T1552.001 Unsecured Credentials: Credentials In Files
      * X-Tunnel is capable of accessing locally stored passwords.
* **TA0007 Discovery**
  + T1083 File and Directory Discovery
    - The Conspirators searched for and identified computers within the DCCC and DNC networks that stored information related to the 2016 U.S. presidential election.
* **TA0009 Collection**
  + T1560 Archive Collected Data
    - The conspirators used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.
  + T1056 Input Capture
    - T1056.001 Input Capture: Keylogging
      * X-Agent malware has keylog functionality.
  + T1113 Screen Capture
    - X-Agent malware has screen capture functionality.
* **TA0011 Command and Control**
  + T1001 Data Obfuscation
    - A remotely configured computer relayed communications between X-Agent malware and a GRU-leased server in Arizona. This computer acted as a proxy to obscure the connection between the malware at the DCCC and Arizona server.
    - T1001.001 Data Obfuscation: Junk Data
      * X-Tunnel inserts junk code into the binary in a likely attempt to obfuscate it and bypass security products.
  + T1090 Proxy
    - T1090.002 Proxy: External Proxy
      * A remotely configured computer relayed communications between X-Agent and X-Tunnel malware and a GRU-leased server in Arizona. This computer acted as a proxy to obscure the connection between the malware at the DCCC and Arizona server.
* **TA0010 Exfiltration**
  + T1041 Exfiltration Over C2 Channel
    - X-Tunnel relays traffic between a C2 server and a victim. The remote server was the GRU-leased Arizona server.

### DISARM Framework

* **Plan**
  + TA01 Plan Strategy
    - T0073 Determine Target Audiences
    - T0074 Determine Strategic Ends
  + TA02 Plan Objectives
    - T0002 Facilitate State Propaganda
    - T0066 Degrade Adversary
    - T0079 Divide
  + TA13 Target Audience Analysis
    - T0072 Segment Audiences
      * T0072.005 Political Segmentation
    - T0080 Map Target Audience Information Environment
      * T0080.005 Assess Degree/Type of Media Access
    - T0081 Identify Social and Technical Vulnerabilities
      * T0081.004 Identify Existing Fissures
      * T0081.005 Identify Existing Conspiracy Narratives/Suspicions
      * T0084.006 Identify Wedge Issues
      * T0081.008 Identify Media System Vulnerabilities
* **Prepare**
  + TA14 Develop Narratives
    - T0068 Respond to Breaking News Event or Active Crisis
    - T0082 Develop New Narratives
    - T0083 Integrate Target Audience Vulnerabilities into Narrative
  + TA06 Develop Content
    - T0019 Generate Information Pollution
    - T0089 Obtain Private Documents
      * T0089.001 Obtain Authentic Documents
  + TA15 Establish Social Assets
    - T0007 Create Inauthentic Social Media Pages and Groups
    - T0010 Cultivate Ignorant Agents
    - T0090 Create Inauthentic Accounts
      * T0090.001 Create Anonymous Accounts
      * T0090.004 Create Sockpuppet Accounts
    - T0091 Recruit Malign Actors
      * T0091.002 Recruit Partisans
    - T0094 Infiltrate Existing Networks
      * T0094.001 Identify Susceptible Targets in Networks
    - T0095 Develop Owned Media Assets
    - T0096 Leverage Content Farms
      * T0096.001 Create Content Farms
        + Amplifying content through troll farms, including those supported through FaceMusic.
  + TA16 Establish Legitimacy
    - T0011 Compromise Legitimate Accounts
    - T0100 Co-opt Trusted Sources
      * T0100.002 Co-Opt Grassroots Groups
  + TA05 Microtarget
    - T0101 Create Localized Content
    - T0102.001 Use Existing Echo Chambers/Filter Bubbles
  + TA07 Select Channels and Affordances
    - T0108 Blogging and Publishing Networks
    - T0111 Traditional Media
* **Execute**
  + TA09 Deliver Content
    - T0115 Post Content
    - T0117 Attract Traditional Media
  + TA17 Maximize Exposure
    - T0049 Flooding the Information Space
      * T0049.001 Trolls amplify and manipulate
      * T0049.003 Bots Amplify via Automated Forwarding and Reposting
      * T0049.004 Utilize Spamoflauge
  + TA18 Drive Online Harms
    - T0048 Harass
      * T0048.004 Dox
  + TA10 Drive Offline Activity
    - T0057 Organize Events
    - T0126 Encourage Attendance at Events
  + TA11 Persist in the Information Environment
    - T0060 Continue to Amplify
    - T0128 Conceal People
      * T0128.001 Use Pseudonyms
    - T0129 Conceal Operational Activity
      * T0129.006 Deny Involvement
    - T0130 Conceal Infrastructure
      * T0130.004 Use Cryptocurrency
      * T0130.005 Obfuscate Payment
  + TA12 Assess Effectiveness
    - T0132 Measure Performance
      * T0132.001 People Focused
    - T0133 Measure Effectiveness
      * T0133.001 Behaviour Changes
      * T0133.002 Content
      * T0133.003 Awareness
      * T0133.004 Knowledge
      * T0133.005 Action/Attitude
    - T0134 Measure Effectiveness Indicators (or KPIs)
      * T0134.001 Message Reach
      * T0134.002 Social Media Engagement

## Resources

U.S. Department of Justice (2018) United States of America v. Viktor Borisovich Netyksho [and 11 Others], Defendants: Case 1:18-Cr-00215-Abj. Available at: <https://www.justice.gov/archives/sco/file/1080281/dl>.

Ugochukwu Etudo, Christopher Whyte, Victoria Yoon, Niam Yaraghi, From Russia with fear: fear appeals and the patterns of cyber-enabled influence operations, *Journal of Cybersecurity*, Volume 9, Issue 1, 2023, tyad016, <https://doi.org/10.1093/cybsec/tyad016>.

Ebbott, E, *et al.* 2021, Understanding Mass Influence: Three case studies of contemporary mass influence activities. University of New South Wales, New South Wales, [JIA Mass INFLUENCE CASE STUDY (unsw.edu.au)](https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/canberra/research/defence-research-institute/2023-02-Understanding-Mass-Influence---A-case-study-of-Facebook.pdf).

Report On The Investigation Into Russian Interference In The 2016 Presidential Election (2019) Special Counsel Robert S. Mueller. Available at: <https://www.justice.gov/archives/sco/file/1373816/dl>.

U.S. District Court for the District of Columbia (2018) United States of America v. IRA Case 1:18-cr-00032-DLF. Available at: <https://www.justice.gov/d9/fieldable-panel-panes/basic-panes/attachments/2018/02/16/internet_research_agency_indictment.pdf>

Nimmo, B. and Hutchins, E. (2023) *Phase-based tactical analysis of online operations*, *Carnegie Endowment*. Available at: <https://carnegieendowment.org/2023/03/16/phase-based-tactical-analysis-of-online-operations-pub-89275>.

XTunnel (2024) XTunnel, Software S0117 | MITRE ATT&CK®. Available at: <https://attack.mitre.org/software/S0117/>

Report On The Investigation Into Russian Interference In The 2016 Presidential Election (2019a) Report On The Investigation Into Russian Interference In The 2016 Presidential Election Special Counsel Robert S. Mueller, III . Available at: <https://www.commoncause.org/wp-content/uploads/2019/06/Mueller-Report-Executive-Summaries.pdf>.

2016 Presidential Campaign Hacking Fast Facts (2023) CNN. Cable News Network. Available at: <https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>