**Cyber-Influence Operation Analysis:**

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

# IRA 2016 Campaign: “FaceMusic”.

## Summary

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 particular narratives. In April of 2016, the FaceMusic website, fbmusic.com, was registered. In May, the IRA purchased Facebook ads promoting the app through one of its fraudulent profiles, "Stop All Invaders". This profile was typically used to push xenophobic anti-immigration memes in support of the Donald Trump campaign.

The malware was advertised as an embedded music player allowing users to listen to free music while browsing Facebook. Users installed the malware as a Chrome plug-in. It would request permission to change all your data on the websites you visit, display notifications, and modify data you copy and paste. Hidden functionality pulled browsers into a botnet and was active even when victims were not using Facebook. The malware would contact a control server, which would iterate through a provided list of web addresses, connecting to each one from the victim's machine. There would be no outward evidence of this occurring to the victim.

The Facebook ads successfully targeted U.S. teenage female users between 14 and 17 years old. Less successful avenues were interest categories such as Shazam, Spotify, Apple Music, or Soundcloud. A post to Reddit advertising FaceMusic was also created. More than 13,000 machines were likely infected by the malware, mainly in Ukraine and the U.S.

## Timeline and Context

* FaceMusic website registered in April 2016. Registered to a Russian man who claims his identity was stolen to register the website – denies any connection to the IRA.
* FaceMusic was promoted through Facebook ads on or about May 2016. Promotions ran through one of the IRA’s fraudulent profiles “Stop All Invaders”
  + These ads garnered approximately 25,000 impressions from 107 ads. However, this only produced 85 clicks.
  + The most successful ad, with 28 clicks, utilised the targeted ad system within Facebook to promote to U.S. teenage female users between the ages of 14 and 17.
  + FaceMusic was also advertised through Reddit on the subreddit r/UsefulWebsites.
* 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.
  + On or about June 2016, one FaceMusic user posted to Imgur claiming that FaceMusic had spammed their friends with a message that contained a direct download link.
* Google removed the app from the Chrome Store and the FaceMusic website is no longer available.

The IRA is well understood to employ a variety of key tactics, systems, and technology to assist its campaign and maintain astute awareness and sensemaking. These translate to tactics and techniques from the DISARM framework. We can apply many of these tactics and techniques to the FaceMusic malware as it was one of many operations apart of a larger campaign to disrupt the 2016 U.S. presidential election.

Some key tactics:

* Microtargeting. The IRA harvests large amounts of user data from various social media platforms. This is analysed and provides the IRA with clear segmented populations and microtargeted audiences to target with tailored messaging.
* Sock Puppet accounts. The IRA frequently uses sock puppet and other false/counterfeit sites to grow and target large audiences. These create or infiltrate existing social media groups, actively engaging and targeting members the IRA wishes to cultivate as assets. These assets sometimes go on to post and organise rallies and demonstrations.

Some systems and technology:

* Virtual Private Networks are often used to hide identity and location
* Cryptocurrency allows the IRA to establish and operate location relevant email accounts, PayPal accounts, purpose political advertising, and operate false social media accounts for long periods without detection.

## Frameworks

### ATT&CK Framework

* TA0043: Reconnaissance
  + T1593 Search Open Websites/Domains
    - T1593.001 Search Open Websites/Domains: Social Media
      * To target specific audiences with Facebook advertisements, information about individual’s location, age, and sex would be searched for on social media.
* TA0042: Resource Development
  + T1583 Acquire Infrastructure
    - T1583.001 Acquire Infrastructure: Domains
      * Registers domain fbmusic.com.
    - T1583.003 Acquire Infrastructure: Virtual Private Server
      * IRAs use of VPN’s to hide identity and location is well known.
    - T1583.004 Acquire Infrastructure: Server
      * Control server used to provide web addresses to the malware.
  + T1586 Compromise Accounts
    - T1586.001 Compromise Accounts: Social Media Accounts
      * Compromised social media accounts were claimed to have been used to spam direct download links to friends of the accounts in an attempt to spread FaceMusic to other machines.
  + T1584 Compromise Infrastructure
    - T1584.005 Compromise Infrastructure: Botnet
      * Victim’s machines are pulled into botnet as a consequence of the malware.
  + T1587 Develop Capabilities
    - T1587.001 Develop Capabilities: Malware
  + T1585 Establish Accounts
    - T1585.001 Establish Accounts: Social Media Accounts
      * “Stop All Invaders” account was used to promote the malware.
  + T1608 Stage Capabilities
    - T1608.001 Stage Capabilities: Upload Malware
* TA0001 Initial Access
  + T1189 Drive-by Compromise
    - User visits the chrome plug-in website for FaceMusic and installs the malware.
* TA0002 Execution
  + T1053 Scheduled Task/Job
    - FaceMusic is programmed to communicate with a control server every minute as long as the victim’s browser is open. The server tells the app to connect to a web address from the victim’s machine.
* TA0003 Persistence
  + T1176 Browser Extensions
  + T1053 Scheduled Task/Job

### DISARM Framework

* **PLAN**
  + TA01 Plan Strategy
    - T0073 Determine Target Audiences
    - T0074 Determine Strategic Ends
  + TA02 Plan Objectives
    - T0075 Dismiss
      * T0075.001 Discredit Credible Sources
    - T0077 Distract
    - T0079 Divide
  + TA13 Target Audience Analysis
    - T0072 Segment Audiences
      * T0072.001 Geographic Segmentation
      * T0072.002 Demographic Segmentation
      * T0072.003 Economic Segmentation
      * T0072.004 Psychographic Segmentation
      * T0072.005 Political Segmentation
    - T0080 Map Target Audience Information Environment
      * T0080.001 Monitor Social Media Analytics
      * T0080.003 Identify Trending Topics/Hashtags
      * T0080.004 Conduct Web Traffic Analysis
    - T0081 Identify Social and Technical Vulnerabilities
      * T0081.001 Find Echo Chambers
      * T0081.003 Identify Existing Prejudices
      * T0081.004 Identify Existing Fissures
      * T0081.005 Identify Existing Conspiracy Narratives/Suspicions
      * T0081.006 Identify Wedge Issues
      * T0081.007 Identify Target Audience Adversaries
      * T0081.008 Identify Media System Vulnerabilities
* **PREPARE**
  + TA14 Develop Narratives
    - T0003 Leverage Existing Narratives
    - T0068 Respond to Breaking News Event or Active Crisis
    - T0083 Integrate Target Audience Vulnerabilities into Narrative
  + TA06 Develop Content
    - T0019 Generate Information Pollution
    - T0023 Distort facts
      * T0023.001 Reframe Context
    - T0084 Reuse Existing Content
      * T0084.001 Use Copypasta
      * T0084.002 Plagiarize Content
    - T0085 Develop Text-based Content
      * T0085.002 Develop False or Altered Documents
      * T0085.003 Develop Inauthentic News Articles
    - T0086 Develop Image-based Content
      * T0086.001 Develop Memes
    - T0087 Develop Video-based Content
    - 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
    - T0013 Create Inauthentic Websites
    - T0090 Create Inauthentic Accounts
      * T0090.003 Create Bot Accounts
      * T0090.004 Create Sockpuppet Accounts
    - T0091 Recruit Malign Actors
      * T0091.003 Enlist Troll Accounts
    - T0092 Build Network
      * T0092.003 Create Community of Sub-group
    - T0093. Acquire/Recruit Network
      * T0093.001 Fund Proxies
      * T0093.002 Acquire Botnets
    - T0094 Infiltrate Existing Networks
      * T0094.001 Identify Susceptible Targets in Networks
    - T0096 Leverage Content Farms
      * T0096.001 Create Content Farms
  + TA16 Establish Legitimacy
    - T0097 Create Personas
    - T0098 Establish Inauthentic News Sites
      * T0098.001 Create Inauthentic News Sites
      * T0098.002 Leverage Existing Inauthentic News Sites
    - T0099 Prepare Assets Impersonating Legitimate Entities
      * T0099.001 Astroturfing
      * T0099.002 Spoof/parody account/site
  + TA05 Microtarget
    - T0016 Create Clickbait
    - T0018 Purchase Targeted Advertisements
    - T0101 Create Localized Content
  + TA07 Select Channels and Affordances
    - T0104 Social Networks
      * T0104.001 Mainstream Social Networks
* **EXECUTE**
  + TA08 Conduct Pump Priming
    - T0046 Use Search Engine Optimization
  + TA09 Deliver Content
    - T0114 Deliver Ads
      * T0114.001 Social Media
    - 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
    - T0121 Manipulate Platform Algorithm
  + 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
      * T0128.002 Conceal Network Identity
    - T0129 Conceal Operational Activity
    - T0130 Conceal Infrastructure
      * T0130.004 Use Cryptocurrency
* **ASSESS**
  + TA12 Assess Effectiveness
    - T0132 Measure Performance
      * T0132.001 People Focused
      * T0132.002 Content Focused
      * 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)
      * T0134.001 Message Reach
      * T0134.002 Social Media Engagement

## Resources

Imgur post claiming FaceMusic messenger spam: <https://imgur.com/gallery/psa-facemusic-released-spam-bot-OahBl>

Poulsen, K. (2018) *Russian troll farm hijacked American teen girls’ computers for likes*, *The Daily Beast*. Available at: <https://www.thedailybeast.com/russia-troll-farm-hijacked-american-teen-girls-computers-for-likes>.

Whyte, C. (2024) *Russia’s use of malware to enhance election influence operations sign of things to come*, *CSO Online*. Available at: <https://www.csoonline.com/article/1310222/russias-use-of-malware-to-enhance-influence-operations-sign-of-things-to-come.html>.

Castillo, M. (2018) *Facebook was manipulated by Russians, who used the same targeting tools that advertisers love*, *CNBC*. Available at: <https://www.cnbc.com/2018/12/17/facebook-ad-platform-made-it-easy-for-russians-to-manipulate-users.html>.

Lapowsky, I. (2018) *Russia-linked facebook ads targeted a sketchy chrome extension at teen girls*, *Wired*. Available at: <https://www.wired.com/story/russia-facebook-ads-sketchy-chrome-extension/>.

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, Saletta, M, Stearne, R, Stjellja, M, Dowse, A, Wilk, V, Legrand, T, de Zwart, M, Stephens, D, Ashenden, D, Webb, M, Leckie, C, Ahmad, A, Perfors, A, de Rozario, R, van Gelder, T, Sciacca, L, Kashima, Y, Ruppanner, L, Karunasekera, S, Whitty, M, Dowling, M-E, Farina, M, Meek, S, Jacques, C, Matthews, D, Semmler, C, Legrand, T, Mitchell, L, White, M, Young, G, Job, P, Carter, L, McLaughlin, C, Schreer, B, Ballsun-Stanton, B, Droogan, J, Waldek, L, Hutchinson, J, Lau, JH, Doherty, S, Guilfoyle, D, Keller, J, Nicholls, R, Ozdemir, S & Wong, R 2021, *Understanding Mass Influence: Three case studies of contemporary mass influence activities*. University of New South Wales, New South Wales.