**Cyber-Influence Operation Analysis:**

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

# APT 2017 Campaign: “French election spearphishing and malware campaign”.

## Summary

From April to May 2017, leading to the French presidential election on May 7, a string of interferences in the French elections targeted now-President Macron's "La Republique En Marche!" political party, other French politicians and high-profile individuals, and several email addresses associated with local French governments. These interferences were enacted through spearphishing campaigns with the intention of disrupting the public opinion and harm the reputation of the En Marche! Campaign. More than 100 individuals who were members of Emmanuel Macron's political party were targeted as well as several email addresses associated with local French governments. Data stolen from En Marche! party members was leaked online along with falsified data to drive harmful narratives towards the party.

## Timeline and Context

* A month prior to phishing campaign - APT 28 registers decoy internet addresses to mimic the name of Macron's movement, En Marche!
  + Domains include onedrive-en-marche.fr (mimicking an official Microsoft address) and mail-en-marche.fr (mimicking a webmail site).
* APT registers web addresses which could plausibly fool a target into thinking they were logging into a legitimate website.
  + One such is "myaccount.google.com-changepasswordmyaccount-idx8jxcn3ufdmncudd.gq". Designed to look like an official Google page.
  + Fake login pages scrape confidential information from users.
* From approximately April 12 to April 26, 2017, a GRU-controlled social media account communicated with various French individuals offering to provide them with internal documents from En Marche! that the user(s) of the account claimed to possess.
  + These spearphishing emails are used to scrape confidential information from users. This utilises the web addresses registered by APT.
* From approximately May 3 and May 5, 2017, unidentified individuals began to leak documents purporting to be from the En Marche! campaign's email accounts.
  + Around 9GB of data consisting of emails, accounting documents and contracts were then leaked onto social media. From hacked accounts (professional and personal) of the En Marche! political party staff members.
    - #MacronLeaks used
    - Posted on the document-sharing site Pastebin.
    - False documents were added to genuine stolen documents and leaked. An attempt at influencing the outcome of the French presidential election by influencing public opinion and harm the reputation of E. Macrons Political party.
  + Narratives included public security announcements regarding terrorist attacks, email account lockouts. software updates for voting machines, journalist scoops on political scandals, En Marche! press relationships, and En Marche! internal cybersecurity recommendations.

## Frameworks

### ATT&CK Framework

* TA0043: Reconnaissance
  + T1589: Gather Victim Identity
    - T1589.002: Email Addresses
      * Adversaries may gather email addresses that can be used during targeting.
    - T1589.003: Employee Names
  + T1590: Gather Victim Network Information
    - T1590.001: Domain Properties
      * APT 28 uses this information to establish operational services (domains) to carry out their phishing campaign.
  + T1591: Gather Victim Org Information
    - T1591.004: Identify Roles
  + T1598: Phishing for Information
    - T1598.003: Spearphishing Link
* TA0042: Resource Development
  + T1583: Acquire Infrastructure
    - T1583.001: Domains
  + T1586: Compromise Accounts
    - T1586.002: Email Accounts
  + T1585: Establish Accounts
    - T1585.002: Email Accounts
* TA0001: Initial Access
  + T1078: Valid Accounts
    - T1078.002: Domain Accounts
  + T1566: Phishing
    - T1566.001: Spearphishing Attachment
* TA0003: Persistence
  + T1078: Valid Accounts
    - T1078.002: Domain Accounts
* TA0005: Defence Evasion
  + T1078: Valid Accounts
    - T1078.002: Domain Accounts
* TA0009: Collection
  + T1114: Email Collection
    - T1114.002: Remote Email Collection

### DISARM Framework

**PLAN**

* TA01 Plan Strategy
  + T0073 Determine Target Audiences
  + T0074 Determine Strategic Ends
* TA02 Plan Objectives
  + T0066 Degrade Adversary
  + T0075 Dismiss
    - T0075.001 Discredit Credible Sources
  + T0076 Distort
  + T0079 Divide
* TA13 Target Audience Analysis
  + T0072 Segment Audiences
    - T0072.005 Political Segmentation
  + T0081 Identify Social and Technical Vulnerabilities
    - T0081.008 Identify Media System Vulnerabilities
* **PREPARE**
* TA14 Develop Narratives
  + T0072 Leverage Existing Narratives
  + T0083 Integrate Target Audience Vulnerabilities into Narrative
* TA06 Develop Content
  + T0015 Create Hashtags and Search Artifacts
  + T0019 Generate Information Pollution
  + T0023 Distort Facts
  + T0085 Develop Text-based Content
    - T0085.002 Develop False or Altered Documents
  + T0089 Obtain Private Documents
    - T0089.001 Obtain Authentic Documents
    - T0089.003 Alter Authentic Documents
* TA15 Establish Social Assets
  + T0007 Create Inauthentic Social Media Pages and Groups
  + T0013 Create Inauthentic Websites
  + T0090 Create Inauthentic Accounts
    - T0090.001 Create Anonymous Accounts
    - T0090.004 Create Sockpuppet Accounts
  + T0094 Infiltrate Existing Networks
    - T0094.001 Identify Susceptible Targets in Networks
* TA16 Establish Legitimacy\
  + T0099 Prepare Assets Impersonating Legitimate Entities
    - T0099.002 Spoof/parody account/site
* TA05 Microtarget
  + T0102 Leverage Echo Chambers/Filter Bubbles
    - T0102.002 Create Echo Chambers/Filter Bubbles
    - T0102.003 Exploit Data Voids
* TA07 Select Channels and Affordances
  + T0104 Social Networks
    - T0104.001 Mainstream Social Networks
    - T0104.005 Use Hashtags
    - T0104.006 Create Dedicated Hashtag
  + T0105 Media Sharing Networks
  + T0108 Blogging and Publishing Networks

**EXECUTE**

* TA09 Deliver Content
  + T0115 Post Content
* TA17 Maximise Exposure
  + T0049 Flooding the Information Space
  + T0119 Cross-Posting
    - T0119.002 Post Across Platform
  + T0121 Manipulate Platform Algorithm
* TA11 Persist in the Information Environment
  + T0059 Play the Long Game

**ASSESS**

* TA12 Assess Effectiveness
  + T0132 Measure Performance
    - T0132.002 Content 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

Office of Public Affairs (2020) *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in Cyberspace*, *Office of Public Affairs*. Available at: <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.

International cyber law: interactive toolkit (2021) *French presidential election leak (2017)*, *The Cyber Law Toolkit* Available at: <https://cyberlaw.ccdcoe.org/wiki/French_presidential_election_leak_(2017)>.

Condliffe, J. (2017) *Election hacks are beginning to look like the new normal*, *MIT Technology Review*. Available at: <https://www.technologyreview.com/2017/05/08/151839/election-hacks-are-beginning-to-look-like-the-new-normal/>.

Hosenball, M. (2017) *U.S. increasingly convinced that Russia hacked French election: Sources | Reuters*, *Reuters*. Available at: <https://www.reuters.com/article/us-france-election-russia/u-s-increasingly-convinced-that-russia-hacked-french-election-sources-idUSKBN1852KO/>.

O’Neill, P.H. (2017) *Researchers link macron hack to apt28 with ‘moderate confidence’*, *CyberScoop*. Available at: <https://cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/>.

Hern, A. (2017) *Macron hackers linked to Russian-affiliated group behind US attack*, *The Guardian*. Available at: <https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack>.

Auchard, E. (2017) *Macron campaign was target of cyber attacks by spy-linked group | reuters*, *Reuters*. Available at: <https://www.reuters.com/article/idUSKBN17Q200/>.

Ferrara, E. (2017) *DISINFORMATION AND SOCIAL BOT OPERATIONS IN THE RUN UP TO THE 2017 FRENCH PRESIDENTIAL ELECTION*, *University of Southern California, Information Sciences Institute*. Available at: <https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf>.