**Cyber-Influence Operation Analysis:**

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

# Iranian involvement in 2024 US Election

## Summary

In June 2024, an email containing a spear phishing link was sent from the compromised account of a former senior advisor for Donald Trump, Roger Stone. The email was sent to a high-ranking official in the Trump campaign. The email contained a link that would direct traffic through a domain controlled by the group that orchestrated this attack. It was confirmed by the FBI that the hack of the Trump campaign was conducted by an Iranian hacker group. The specific compromise of Stone’s email account was linked to APT 42 (aka Mint Sandstorm).

Additionally, Politico, a media company, received emails from an anonymous account in August, around the time at which the Trump campaign had revealed that it was hacked. The emails contained private documents from the Trump campaign. These documents included research on JD Vance (Trump’s running mate) and Marco Rubio (Finalist for VP nomination). The sender identified themselves as ‘Robert’ and used an AOL email account. The documents were verified as real documents from within the Trump campaign, evidencing that a successful hack of the campaign had occurred.

## Timeline and Context

June 2024

* Spear phishing email sent to official in the Trump campaign from the compromised account of a former senior advisor

August 2024

* Politico receives emails from anonymous AOL account containing authentic documents from within the Trump campaign
* Trump campaign reveals it has been hacked

Context:

A potential motivation for the attacks on the Trump campaign has been identified. In 2020, Trump ordered the assassination of Qassem Soleimani, an Iranian military officer. There is intel of evidence to suggest that Iran was plotting to retaliate against (and potentially kill) Trump. However, this cannot be confirmed. Their involvement could also be attributed to wanting to influence the election, gain information, or causing general disarray.

## Frameworks

### ATT&CK Framework

* **TA0043: Reconnaissance**
  + T1591.002: Gather Victim Org Information: Business Relationships
    - Identify public figures and officials related to the Trump campaign for targeting
* **TA0042: Resource Development**
  + T1586.002: Compromise Accounts: Email Accounts
  + T1583.001: Acquire Infrastructure: Domains
  + T1585.001: Establish Accounts: Social Media Accounts
    - Whatsapp accounts created posing as support agents for tech companies
  + T1650: Acquire Access
* **TA0001: Initial Access**
  + T1566: Phishing: Spearphishing
    - Specific details regarding access of Roger Stone's account unknown, probable that access was achieved using a form of spearphishing
  + T1078: Valid Accounts
  + T1199: Trusted Relationship
  + T1566.002: Phishing: Spearphishing Link
    - Link attached to email from Roger Stone account sent to Trump officials
    - Microsoft reports Mint Sandstorm used a compromised account of a former senior advisor to send a spearphishing email to a high-ranking official in the Trump campaign
  + T1566.003: Phishing: Spearphishing via Service
    - Meta reports APT 42 using services such as WhatsApp to contact US officials and public figures associated with Trump and Biden
    - No evidence of successful spearphishing, unlikely how Roger Stone account was compromsed
* **TA0011: Command and Control**
  + T1090.004: Proxy: Domain Fronting
    - Spearphishing link would direct traffic through domain controlled by adversary before routing to website of the link
    - No evidence that the spearphishing attempts through the Stone account were successful

### DISARM Framework

* **PLAN**:
  + TA01: Plan Strategy
    - T0073: Determine Target Audiences
  + TA13: Target Audience Analysis
    - T0081: Identify Social and Technical Vulnerabilities
* **PREPARE**:
  + TA15: Establish Social Assets
    - T0090.001: Create Anonymous Accounts
  + TA06: Develop content
    - T0089.001: Obtain Authentic Documents
  + TA16: Establish Legitimacy
    - T0011: Compromise legitimate accounts
    - T0100.001: Co-Opt Trusted Individuals
  + TA07: Select Channels and Affordances
    - T0112: Email
* **EXECUTE**:
  + TA09: Deliver Content
    - T0114.002: Traditional Media
  + TA11: Persist in the Information Environment
    - T0129.006: Deny Involvement
    - T0128.001: Use Pseudonyms

## Resources

This includes resources used to produce a timeline, technical information, tactics, techniques, and procedures used in the operation. It can also include any relevant resources that support modelling decisions such as technical methods for cyber components or societal/psychological context for influence components.

Politico: We received internal Trump documents from ‘Robert.’ Then the campaign confirmed it was hacked.

<https://www.politico.com/news/2024/08/10/trump-campaign-hack-00173503>

Politico: US officials have gathered increasing amount of intel about Iran plotting to assassinate Trump

<https://www.politico.com/news/2024/07/16/iran-plot-assassinate-trump-00168830>

The Guardian: Roger Stone’s email account breached by alleged Iranian hackers

<https://www.theguardian.com/us-news/article/2024/aug/13/roger-stone-email-hack-iran-trump>

CNN: Suspected Iranian hackers breached Roger Stone’s personal email as part of effort to target Trump campaign, sources say

<https://edition.cnn.com/2024/08/12/politics/trump-campaign-hack-personal-email-account-fbi/index.html>

Google: Uncharmed: Untangling Iran's APT42 Operations

<https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations?e=48754805>

Google: Iranian backed group steps up phishing campaigns against Israel, U.S.

<https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/>

Foreign Policy: Why Everyone’s Suddenly Talking About Iranian Election Hacking

<https://foreignpolicy.com/2024/08/21/iran-hack-trump-harris-campaign-election-2024/>

The George Washington University: Media Tip Sheet: Trump Campaign Alleges Foreign Hack Amid Release of VP Vetting Document

<https://mediarelations.gwu.edu/media-tip-sheet-trump-campaign-alleges-foreign-hack-amid-release-vp-vetting-document>

FBI: Joint ODNI, FBI, and CISA Statement on Iranian Election Influence Efforts

<https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts>

Microsoft: Iran steps into US election 2024 with cyber-enabled influence operations

<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf>

Microsoft: Iran Targeting 2024 US Election

<https://blogs.microsoft.com/on-the-issues/2024/08/08/iran-targeting-2024-us-election/>

Intelligencer: What We Know About the Trump-Campaign Hack

<https://nymag.com/intelligencer/article/what-we-know-about-the-trump-campaign-hack.html>

Taking Action Against Malicious Accounts in Iran

<https://about.fb.com/news/2024/08/taking-action-against-malicious-accounts-in-iran/>

Donald Trump’s campaign says its emails were hacked

<https://apnews.com/article/donald-trump-campaign-hacked-036ffd3ed07cf3fe9fb74d4958808b65>

The Iranians who hacked Trump's campaign have deep expertise

<https://www.reuters.com/world/trump-campaigns-iranian-hackers-have-dangerous-history-deep-expertise-2024-08-23/>