Q1 2024 Briefing

U.S. Election Assistance Commission (EAC)

Google Cloud
Security

TLP: GREEN

AGENDA

- □ Introduction
- □ Intelligence Methodology
- □ The Threat Landscape
- □ Observed Activity
- □ Strategic Outlook
- □ Discussion

MANDIANT
NOW PART OF Google Cloud

Introduction

Executive Summary

Cyber-enabled threat actors across a wide spectrum of intrinsic motivations and geographical origin continue to target U.S. elections infrastructure with malicious operations designed to influence, manipulate, monitor, or disrupt elections, or enable intelligence collection efforts.

MANDIANT®

NOW PART OF Google Cloud

Intelligence Methodology

Information Sourcing & Fidelity

Information Sources:

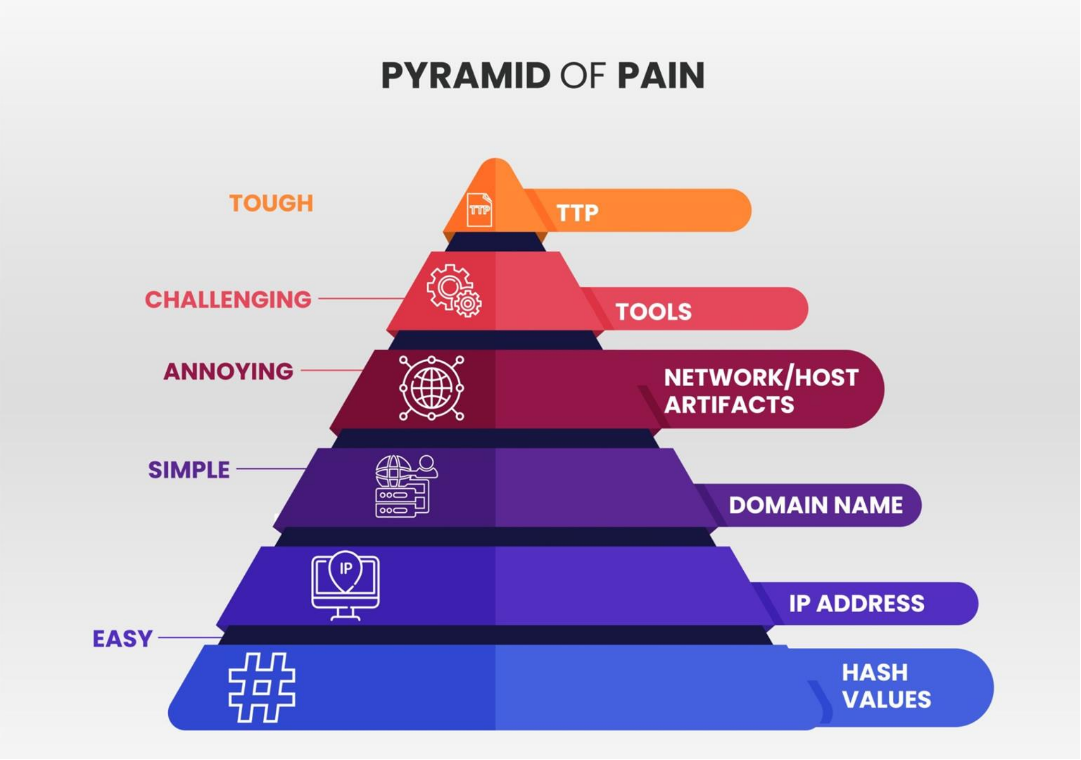
- Mandiant Engagements
- Information Sharing Partnerships
- Open-Source Reporting
- Advanced Research Methods

Indicators of Compromise (IoCs):

- Static observables, e.g. files, network artifacts, and command strings
- Inverse relationship between ease of acquisition and ongoing usefulness

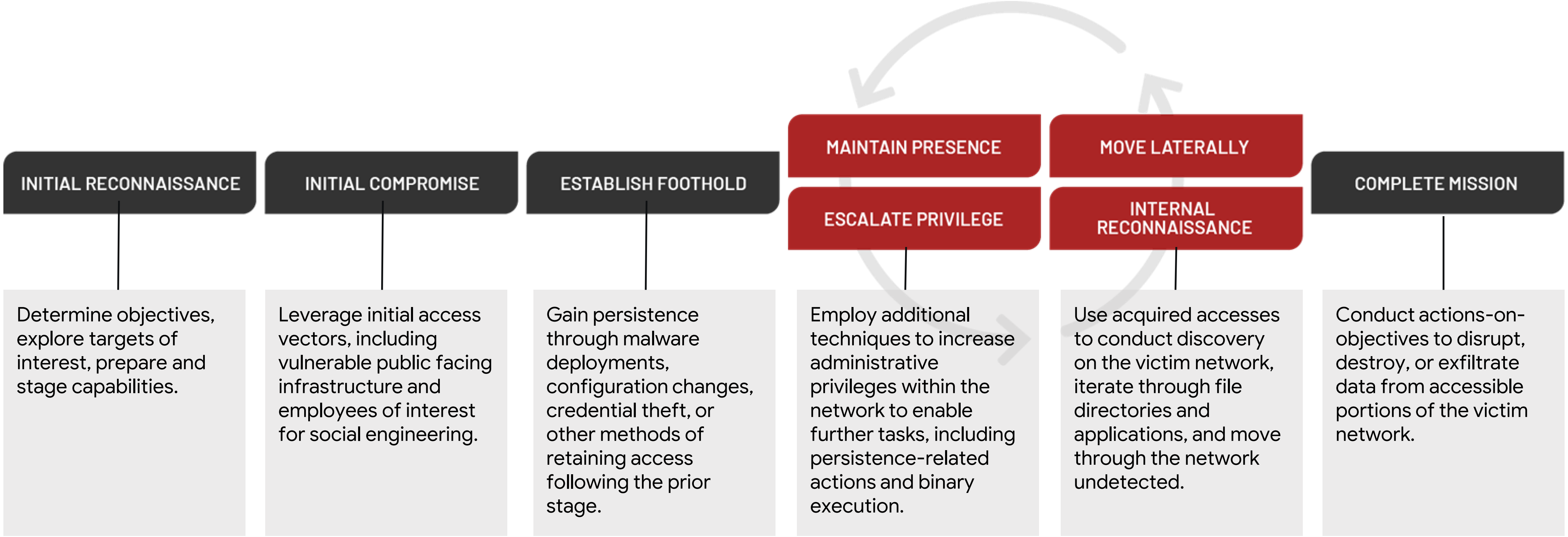
Behavioral Indicators:

- Attack patterns providing buckets to standardize the way we communicate adversarial actions
- Alone provide limited information, but in combination can give critical context
- Much more difficult to identify, analyse, and act on in comparison to static indicators



Source: https://www.linkedin.com/pulse/pyramid-pain-how-make-attackers-life-harder-murray-pearce/

Attack Lifecycle



INITIAL RECONNAISSANCE

Determine objectives, explore targets of interest, prepare and stage capabilities.

INITIAL COMPROMISE

Leverage initial access vectors, including vulnerable public facing infrastructure and employees of interest for social engineering.

ESTABLISH FOOTHOLD

Gain persistence through malware deployments, configuration changes, credential theft, or other methods of retaining access following the prior stage.

MAINTAIN PRESENCE

ESCALATE PRIVILEGE

Employ additional techniques to increase administrative privileges within the network to enable further tasks, including persistence-related actions and binary execution.

MOVE LATERALLY

INTERNAL RECONNAISSANCE

Use acquired accesses to conduct discovery on the victim network, iterate through file directories and applications, and move through the network undetected.

COMPLETE MISSION

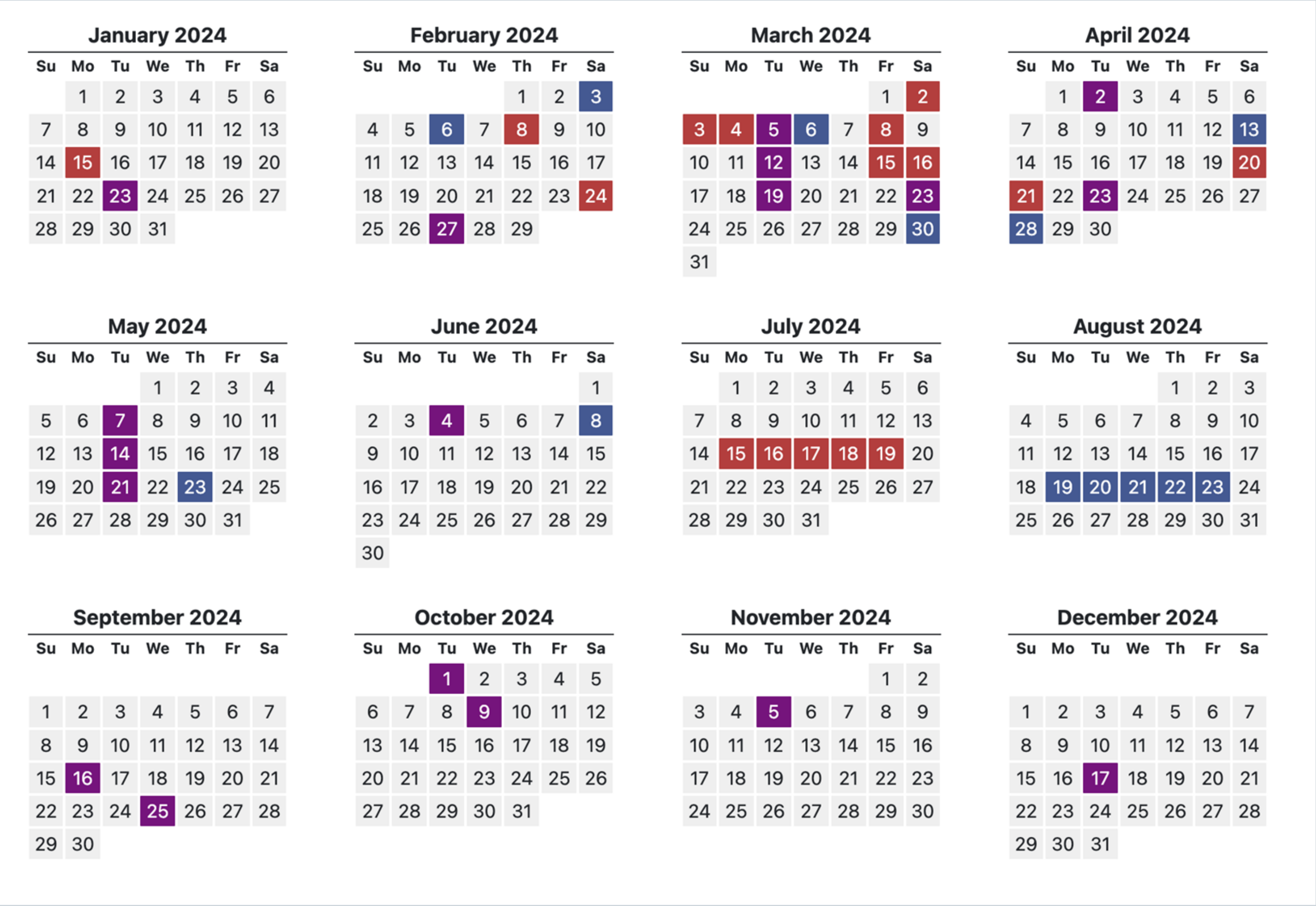
Conduct actions-on-objectives to disrupt, destroy, or exfiltrate data from accessible portions of the victim network.

MITRE ATT&CK: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

MANDIANT®
NOW PART OF Google Cloud

The Threat Landscape

2024 U.S. Presidential Elections Calendar



January 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February 2024

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

March 2024

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

April 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

May 2024

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

June 2024

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

July 2024

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

August 2024

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

September 2024

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

October 2024

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

November 2024

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

December 2024

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

This election calendar includes dates for presidential primary and caucus events, party conventions and presidential debates. Purple indicates both parties are holding an event on that date.
Source: 270towin

March 05: Super Tuesday

June 04: Final Primaries Held

July 15 - 18: Republican National Convention

August 19 - 22: Democratic National Convention

September 16: First Presidential Debate

September 25: Vice Presidential Debate

October 1: Second Presidential Debate

October 09: Final Presidential Debate

November 05: General Election Day

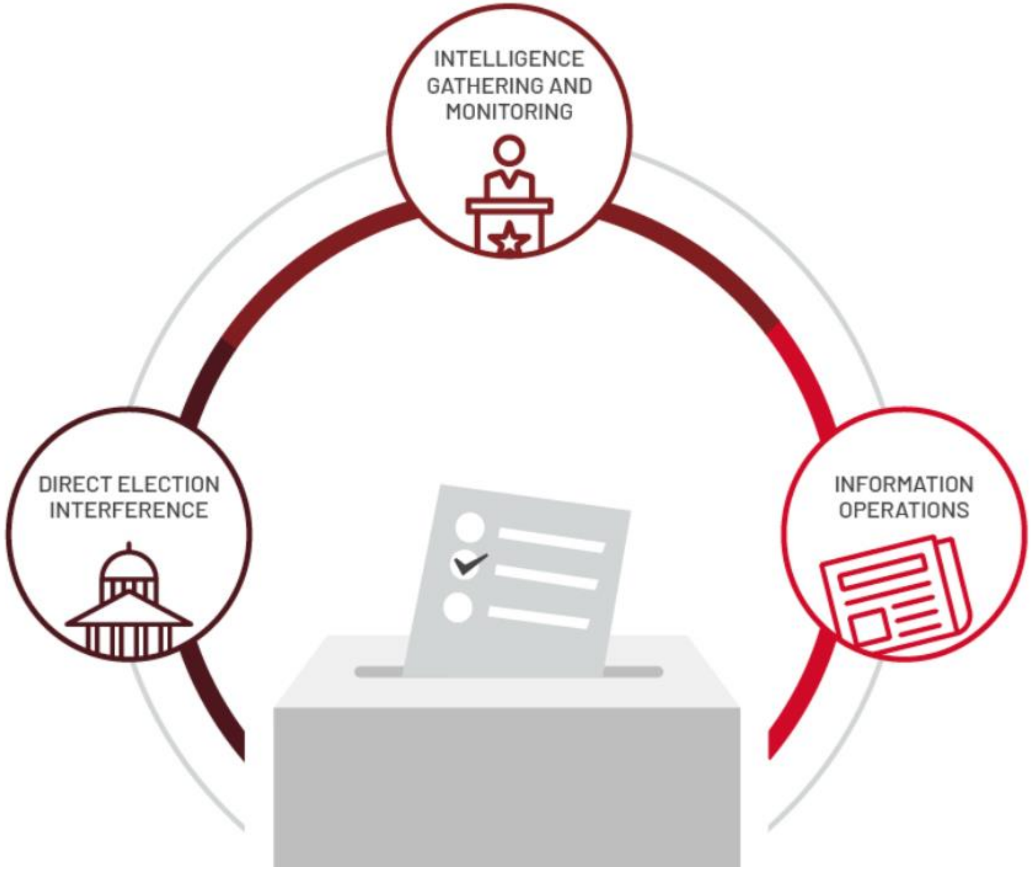
December 17: Electors Cast Votes

Identifying Adversary Objectives

- An adversary's primary underlying motivations inform targeting as well as the manner and speed they conduct operations

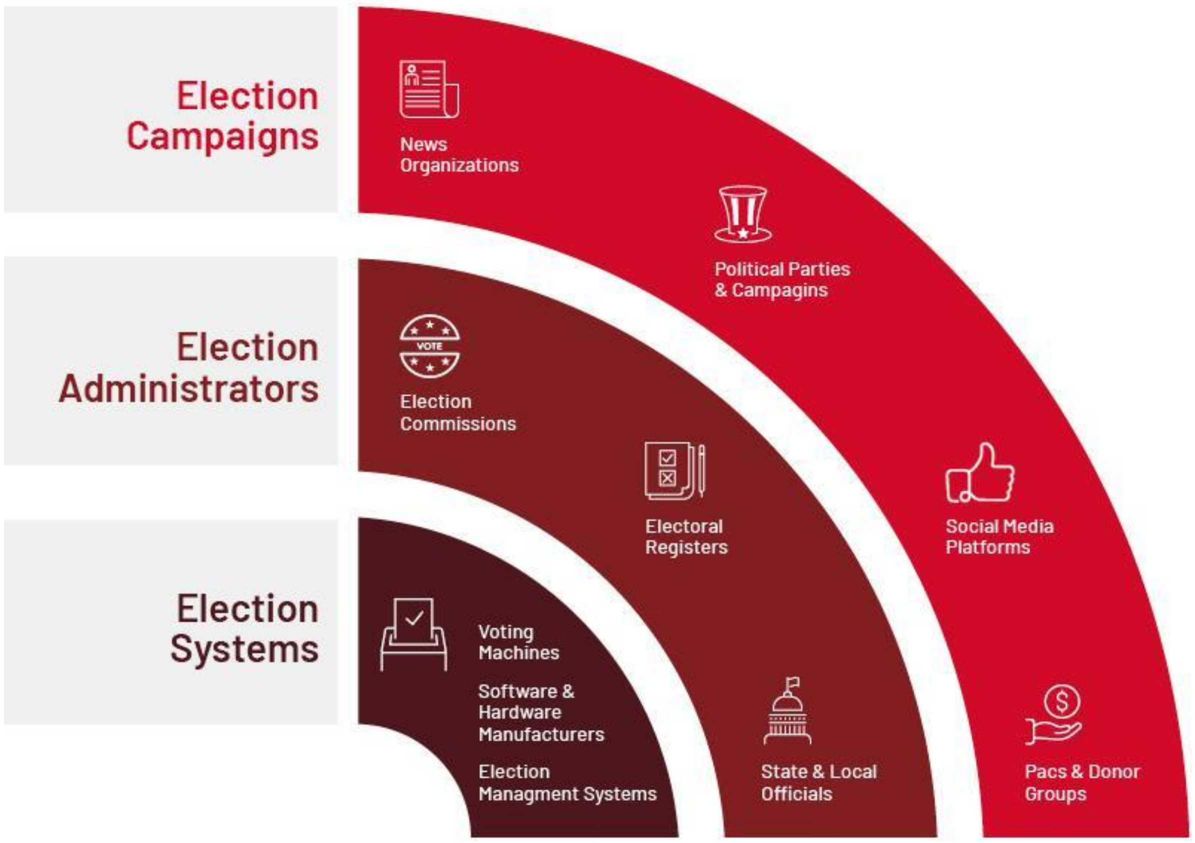
- Three primary motivations:
  - Direct Election Interference
  - Intelligence Gathering / Monitoring
  - Information Operations (IO)

- Individual objectives are often multi-dimensional and can reflect amorphous, evolving, and/or overlapping adversary motivations


INTELLIGENCE GATHERING AND MONITORING
DIRECT ELECTION INTERFERENCE
INFORMATION OPERATIONS

Distinguishing Targets within the Elections Ecosystem

- Campaigns
  - News Organizations
  - Political Parties & Campaigns
  - Social Media Platforms
  - PACs & Donor Groups
- Administration
  - Election Commissions
  - Electoral Registres
  - State & Local Officials
- Systems
  - Voting Machines
  - Software & Hardware Manufacturers
  - Election Management Systems



Election Campaigns

News Organizations

Political Parties & Campagins

Social Media Platforms

Pacs & Donor Groups

Election Administrators

Election Commissions

Electoral Registers

State & Local Officials

Election Systems

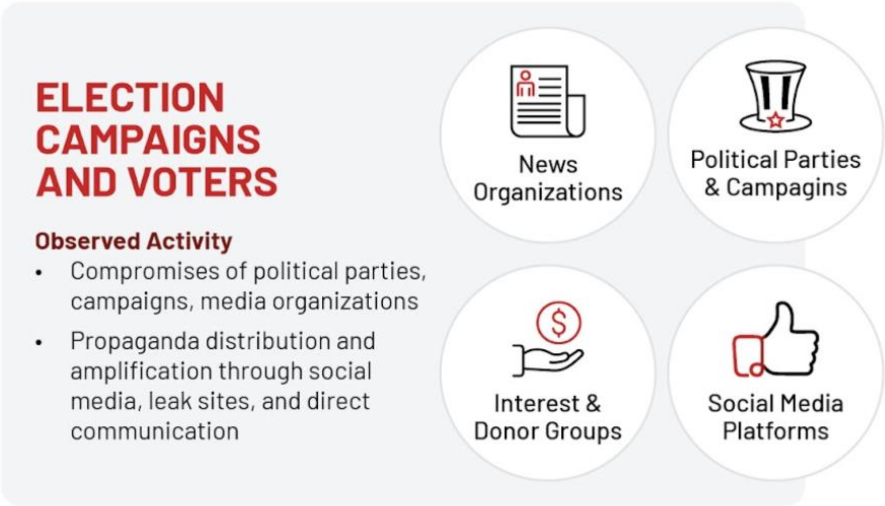
Voting Machines

Software & Hardware Manufacturers

Election Managment Systems

MANDIANT

Distinguishing Targets within the Elections Ecosystem (cont.)



ELECTION CAMPAIGNS AND VOTERS

Observed Activity

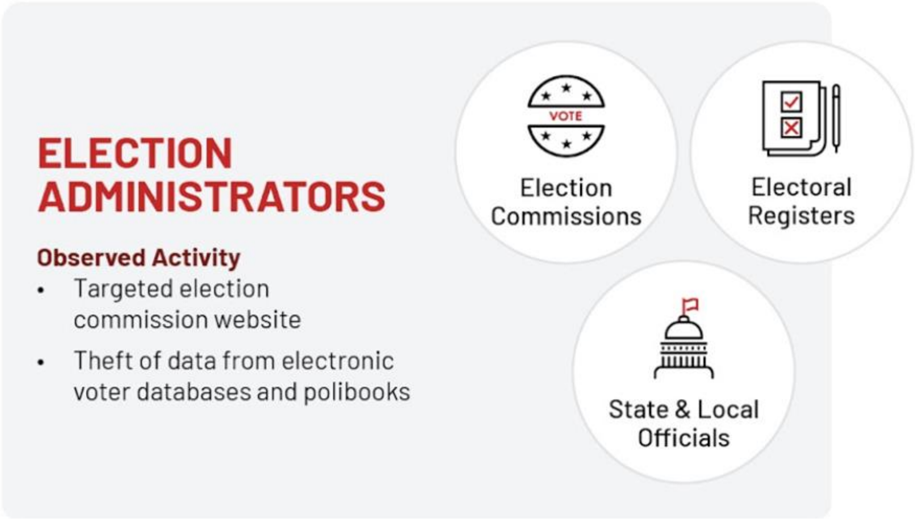
- Compromises of political parties, campaigns, media organizations
- Propaganda distribution and amplification through social media, leak sites, and direct communication

News Organizations

Political Parties & Campagins

Interest & Donor Groups

Social Media Platforms



ELECTION ADMINISTRATORS

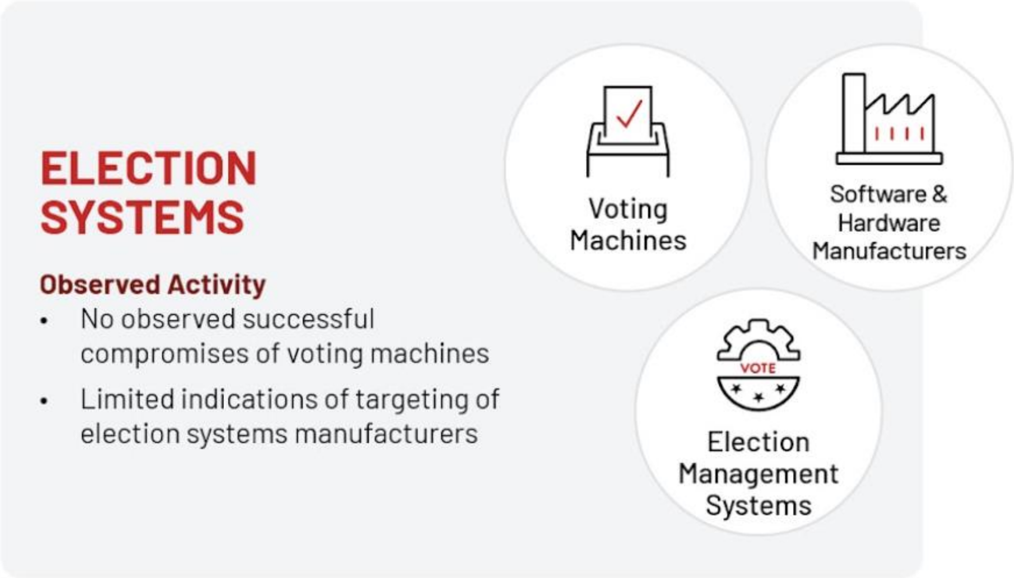
Observed Activity

- Targeted election commission website
- Theft of data from electronic voter databases and polibooks

Election Commissions

Electoral Registers

State & Local Officials



ELECTION SYSTEMS

Observed Activity

- No observed successful compromises of voting machines
- Limited indications of targeting of election systems manufacturers

Voting Machines

Software & Hardware Manufacturers

Election Management Systems

A Dynamic Threat Landscape

Underlying Motivations Drive Decision Making

- Malicious activity represents humans at a keyboard
- Activity may be highly tailored toward particular sectors or individual organizations
- Underlying motivations range from destruction and disruption to information theft, among others

Professionalism, Structure, and Resourcing

- Attackers may flexibly calibrate their capabilities depending on the target
- Threats may linger carefully for months or even years within a network
- Attackers may pivot their tactics based on findings from within a victim network

Persistence in Pursuit of Set Objectives

- Resolute objectives motivate threats to continuously pursue targets over the long term
- Greater familiarity with a given network means a threat is more likely to identify and leverage additional access vectors
- Persistence mechanisms mean partial eviction may not result in complete remediation

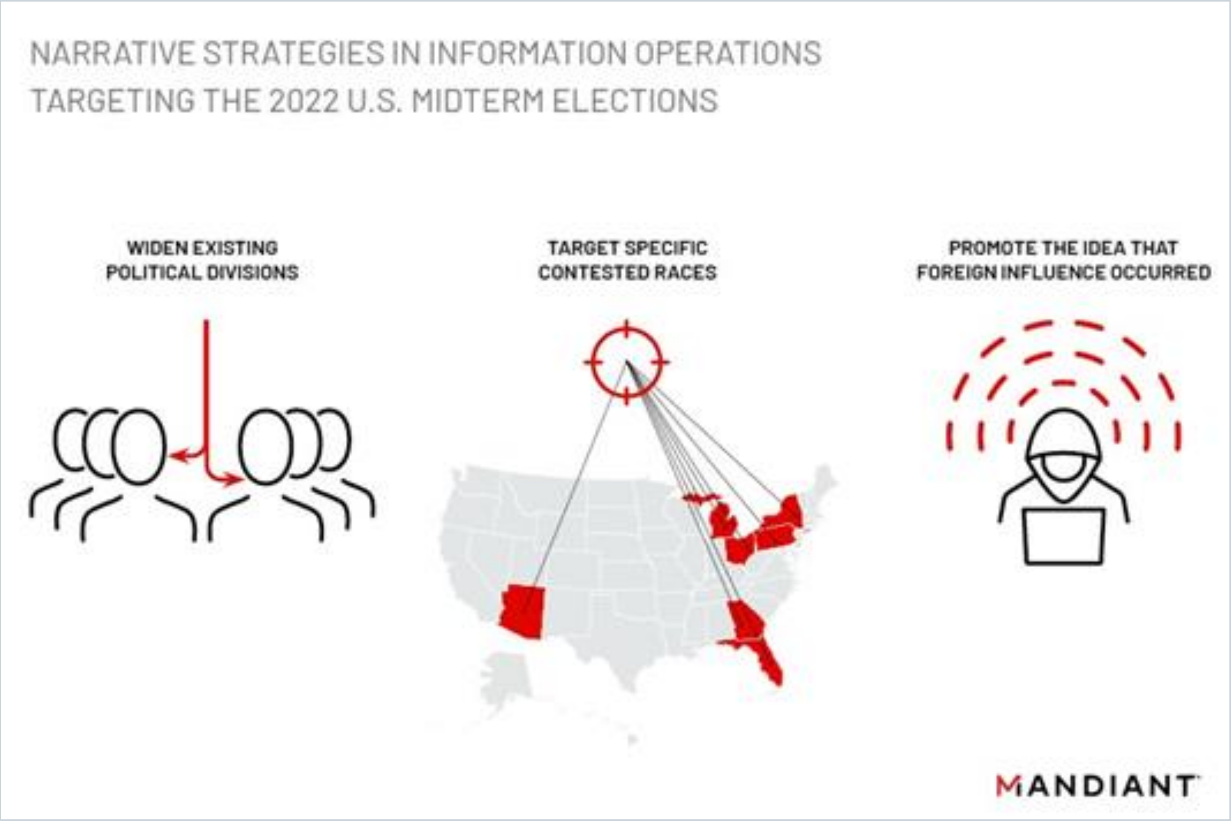
The Spectrum of Contemporary IO Activity

Primary IO Objectives Observed During 2022 Midterm Elections:

- Widen existing political divisions
- Target specific contested races
- Promote speculation of foreign interference

IO Strategies:

- Coordinated inauthentic activity
- Hack-and-leak operations
- Production and publication of disinformation
- Claims of disruptive activity targeting election infrastructure
- Claims of activity targeting the confidentiality of election data



NARRATIVE STRATEGIES IN INFORMATION OPERATIONS
TARGETING THE 2022 U.S. MIDTERM ELECTIONS

WIDEN EXISTING POLITICAL DIVISIONS
TARGET SPECIFIC CONTESTED RACES
PROMOTE THE IDEA THAT FOREIGN INFLUENCE OCCURRED
MANDIANT

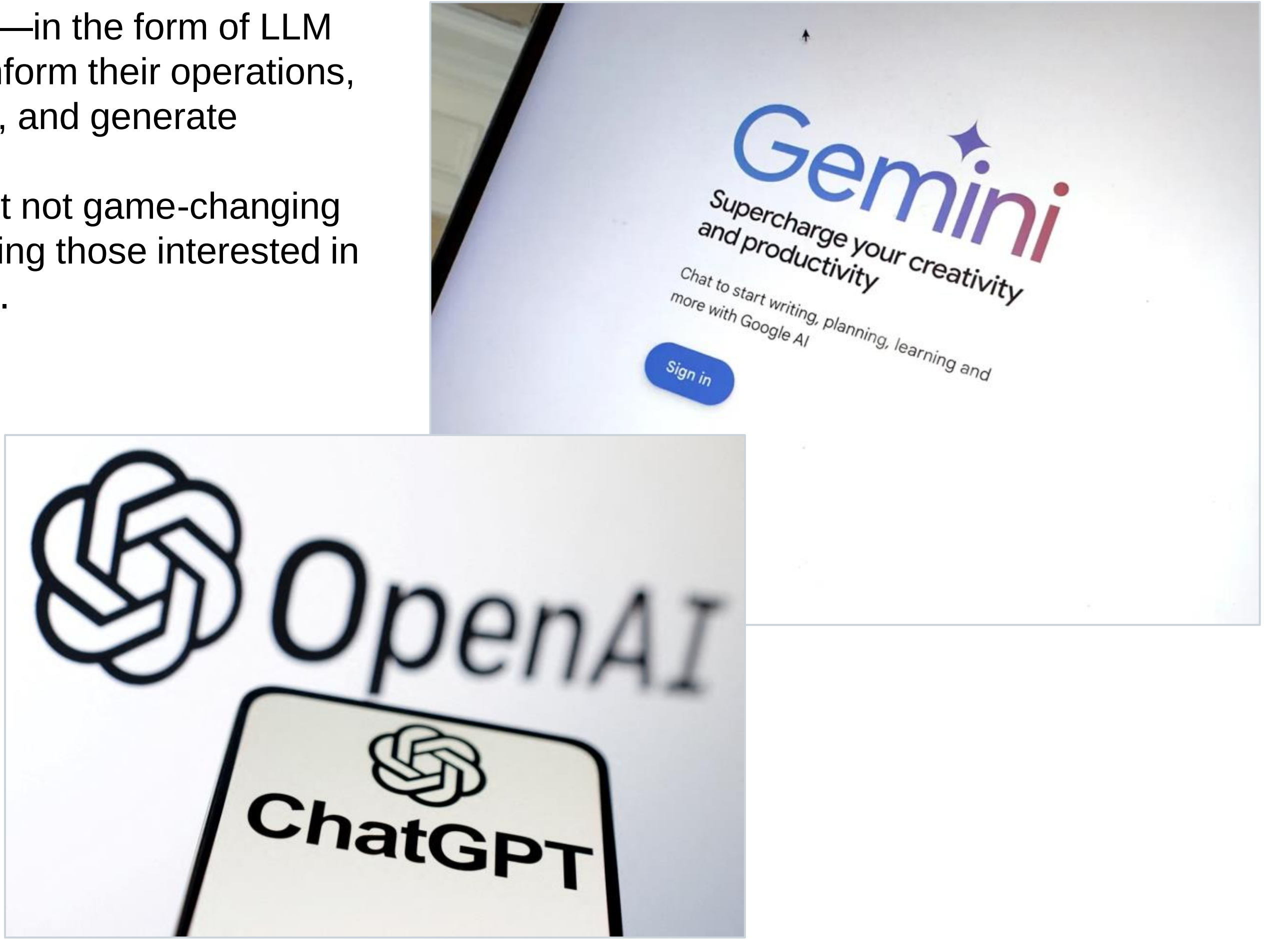
Defining the Current State of AI-Enabled TTPs

Background:

- Current research and open-source reporting indicates that AI—in the form of LLM platforms—has assisted a number of threat actors to better inform their operations, craft lure content and malware payloads, interact with victims, and generate misleading photo and video content to mislead audiences.
    - TL;DR: AI has become a substantial force multiplier, but not game-changing capability, for contemporary cyber threat groups, including those interested in gathering intelligence from or influencing U.S. elections.

Example Definitions of Initially Observed Tactics:

- LLM-informed reconnaissance
- LLM-enhanced scripting techniques
- LLM-aided development
- LLM-supported social engineering
- LLM-assisted vulnerability research
- LLM-optimized payload crafting
- LLM-enhanced anomaly detection evasion
- LLM-directed security feature bypass
- LLM-advised resource development


Gemini
Supercharge your creativity and productivity
Chat to start writing, planning, learning and more with Google AI
Sign in
OpenAI
ChatGPT

MANDIANT
NOW PART OF Google Cloud

Observed Activity

Key Takeaways:

- Mandiant continues to anticipate espionage-based intelligence collection and enablement efforts targeting election-related entities in 2024:
  - The time-sensitive nature of any such operation, the fleeting intelligence value of most collected information, and difficulties taking action on most such information may hold many threat actors from conducting election-specific operations; however:
    - Presidential campaigns, auxiliary party members and leadership, and other election-related entities pose highly valuable targets for intelligence collection activities looking to glean information on future U.S. policy, foreign and domestic.
    - Controversies surrounding current presidential candidates—including health, personal and professional relationships, and business dealings—highlight the amplified risks of personal data leaks and the incentives threat actors have to pursue them.

- Threat actors from around the world continue to conduct Information Operations (IO) to foment discontent, mislead Western audiences, and otherwise share and amplify information in ways meant to influence and degrade the conduct and outcomes of U.S. and foreign elections.
  - Russia, Iran, and PRC-aligned IO campaigns continue to constitute the greatest volume of such activity, leveraging social media networks, hacktivist fronts, and other means to share and amplify information to Western audiences.

- Hacktivist fronts and ransomware threat actors continue to pose a serious disruptive threat to elections, whether explicitly designed to or not.
  - Hacktivist fronts carry out frequent denial-of-service attacks alongside nationalistic, anti-West rhetoric, and have demonstrated prior activity parallel to elections.
  - Ransomware attacks against government infrastructure timed (whether purposefully or not) to coincide with elections may paralyze their conduct and force substantial delays.

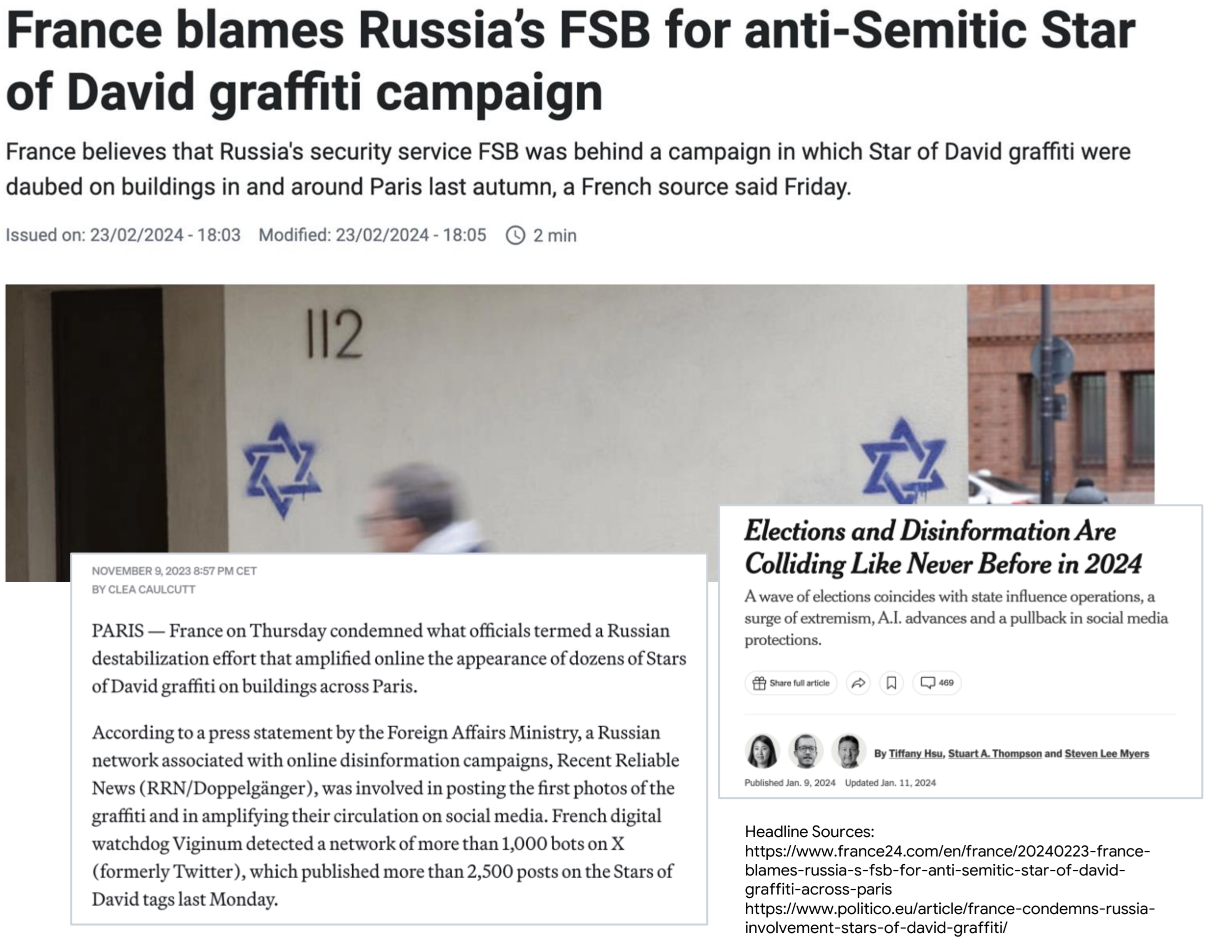
IO Campaigns, Impacts, and FUD

Background:

- Foreign states continue to deploy information operations (IO) to attempt to influence the conduct and outcome of elections globally.

Observations:

- Not all IO campaigns are created equally, and most fall short
  - Obvious script-following/bot use, poor language skills, lack of cultural awareness
- Successful campaigns often leverage current events by calling into question official narratives or providing alternative facts that are not easily verifiable or that provide an easy, malicious explanation for an otherwise nuanced, sensitive topic.
  - Campaigns may make varied and creative use of various vehicles for information transfer, including potential physical operations (See Figures).
  - Audiences presented with multiple narratives may become fatigued by choice and trust none, gravitate toward those most sensational, or trust the first source they encounter rather than the most reputable.



France blames Russia's FSB for anti-Semitic Star of David graffiti campaign

France believes that Russia's security service FSB was behind a campaign in which Star of David graffiti were daubed on buildings in and around Paris last autumn, a French source said Friday.

Issued on: 23/02/2024 - 18:03 Modified: 23/02/2024 - 18:05 2 min

NOVEMBER 9, 2023 8:57 PM CET
BY CLEA CAULCUTT

PARIS — France on Thursday condemned what officials termed a Russian destabilization effort that amplified online the appearance of dozens of Stars of David graffiti on buildings across Paris.

According to a press statement by the Foreign Affairs Ministry, a Russian network associated with online disinformation campaigns, Recent Reliable News (RRN/Doppelgänger), was involved in posting the first photos of the graffiti and in amplifying their circulation on social media. French digital watchdog Viginum detected a network of more than 1,000 bots on X (formerly Twitter), which published more than 2,500 posts on the Stars of David tags last Monday.

Elections and Disinformation Are Colliding Like Never Before in 2024

A wave of elections coincides with state influence operations, a surge of extremism, A.I. advances and a pullback in social media protections.

By Tiffany Hsu, Stuart A. Thompson and Steven Lee Myers

Published Jan. 9, 2024 Updated Jan. 11, 2024

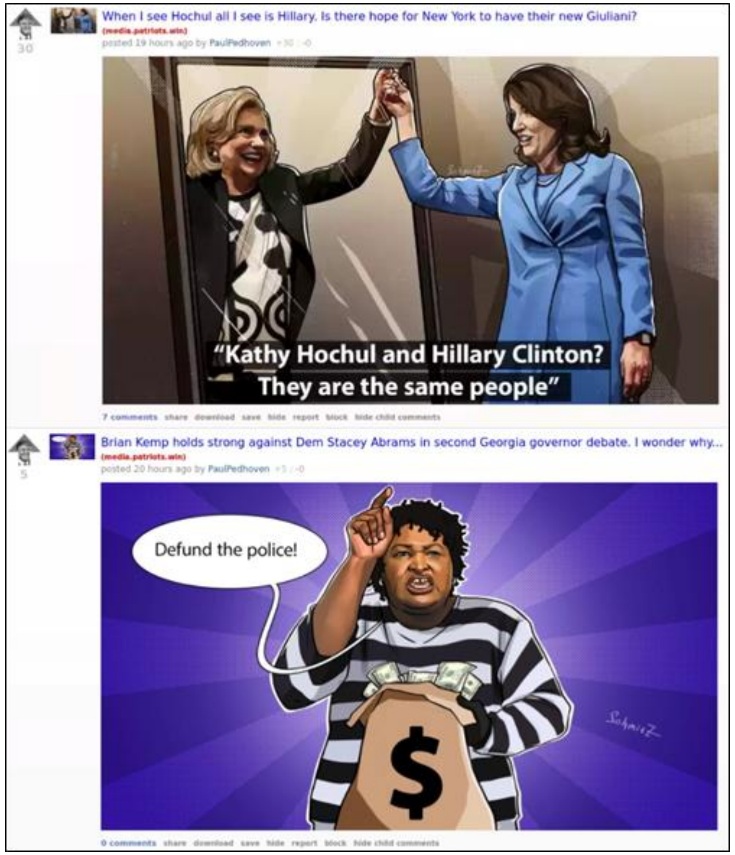
Headline Sources:
https://www.france24.com/en/france/20240223-france-blames-russia-s-fsb-for-anti-semitic-star-of-david-graffiti-across-paris
https://www.politico.eu/article/france-condemns-russia-involvement-stars-of-david-graffiti/
https://www.nytimes.com/2024/01/09/business/media/election-disinformation-2024.html

Russia-Aligned Campaigns

Mandiant has recently highlighted continued observations surrounding threat activity we attribute to "Newsroom for American and European Based Citizens" (NAEBC), a pro-Russia influence campaign allegedly run by individuals associated with Russia's Internet Research Agency (IRA). Activity attributed to NAEBC, which has periodically fluctuated between key events such as U.S. elections, has markedly persisted despite repeated public exposure and has continued to target specifically right-leaning U.S. audiences on a range of issues.

Additionally, we note that covert assets within the pro-Russia propaganda and disinformation ecosystem, including those that have been attributed to Russian intelligence services, continue to amplify pro-Russia messaging targeting U.S. audiences in the run-up to the 2024 U.S. presidential election. For example, we continue to observe well-known disinformation sites such as "NewsFront" and "Southfront" increasingly incorporate specific messaging surrounding these upcoming elections; content published to these sites is often further amplified by both inauthentic and genuine sources, the latter of which increases the ability of these campaigns to breakout and reach larger audiences.

Similar to observed threat activity targeting the U.S. 2022 midterm elections, we expect both pre-existing and possibly newly emerged hacktivist personas to engage in potentially wide-ranging threat activity targeting the U.S. 2024 elections, including both disruptive and conventional information operations.



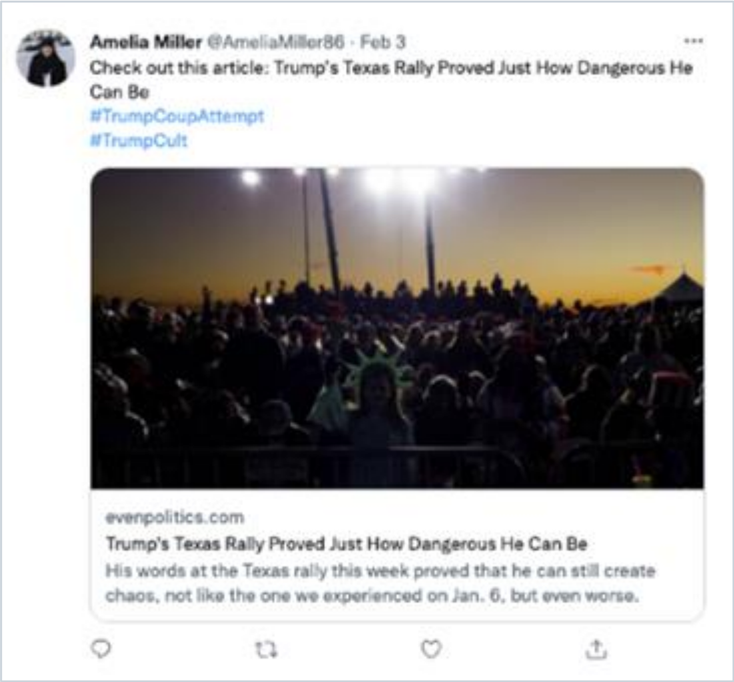
30 When I see Hochul all I see is Hillary. Is there hope for New York to have their new Giuliani?
(media.patriots.win)
posted 19 hours ago by PaulPedhoven +30 / -0

7 comments share download save hide report block hide child comments

5 Brian Kemp holds strong against Dem Stacey Abrams in second Georgia governor debate. I wonder why...
(media.patriots.win)
posted 20 hours ago by PaulPedhoven +5 / -0

0 comments share download save hide report block hide child comments

Iran-Aligned Campaigns



Amelia Miller @AmeliaMiller86 · Feb 3

Check out this article: Trump's Texas Rally Proved Just How Dangerous He Can Be

#TrumpCoupAttempt
#TrumpCult

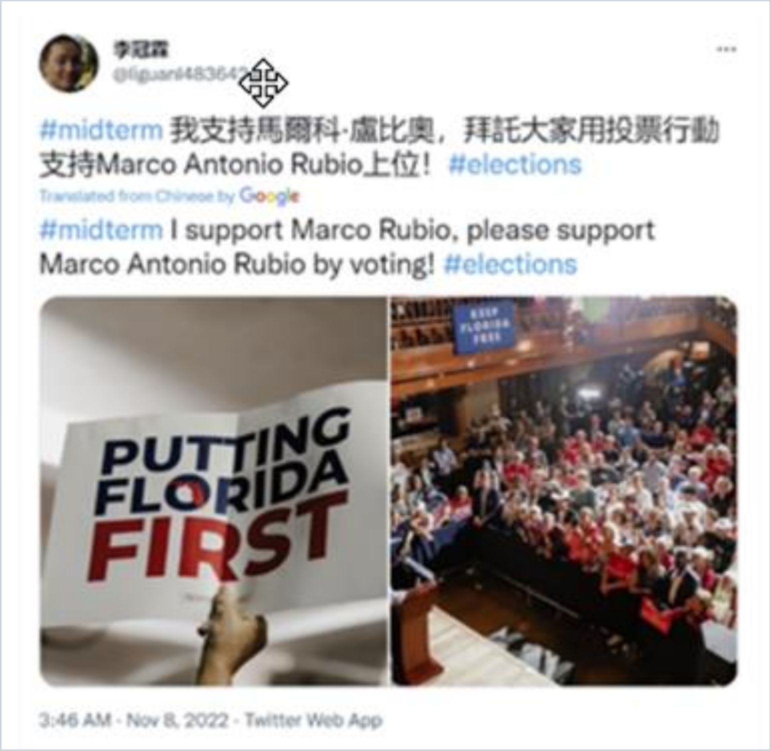
evenpolitics.com

Trump's Texas Rally Proved Just How Dangerous He Can Be

His words at the Texas rally this week proved that he can still create chaos, not like the one we experienced on Jan. 6, but even worse.

We note an established precedent for Iran-aligned information operations activity targeting U.S. audiences; notable campaigns have leveraged suspected inauthentic news sites, impersonated U.S.-based individuals, and in some cases, U.S. political candidates.

PRC-Aligned Campaigns



李冠霖
@liguanl48364

#midterm 我支持馬爾科·盧比奧，拜託大家用投票行動支持Marco Antonio Rubio上位！ #elections

Translated from Chinese by Google

#midterm I support Marco Rubio, please support Marco Antonio Rubio by voting! #elections

3:46 AM · Nov 8, 2022 · Twitter Web App

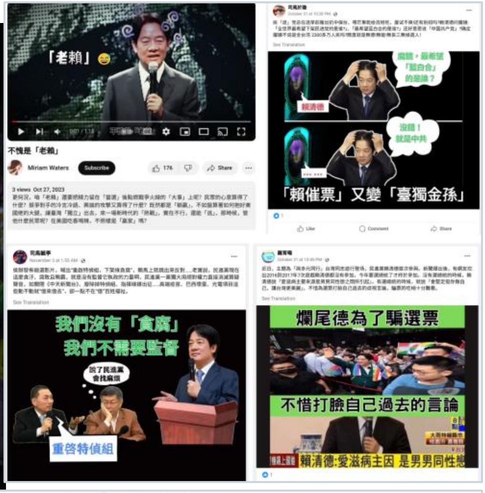
Throughout 2023, pro-PRC IO activity exhibited a pattern of aggressiveness manifested primarily in attempts to target elections in the U.S., as well as elections in Taiwan, and Hong Kong, including with activity flagrantly attempting to engage with voters and influence their electoral choices.

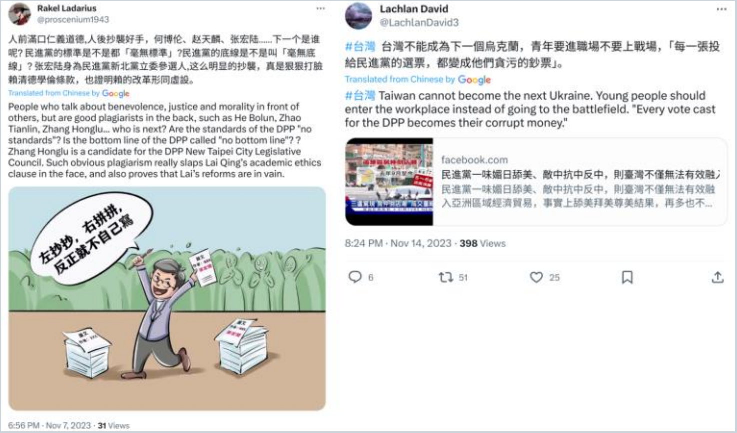
We continue to observe concerted, and in some cases ongoing, efforts attributed to the pro-PRC campaigns "DRAGONBRIDGE" and "HaiEnergy" to target U.S. domestic political discourse. Observations surrounding threat activity attributed to these groups include past concerted efforts targeting the U.S. 2022 midterm elections as well as recent activity focused on the U.S. 2024 election cycle.

IO Surrounding Taiwan’s Presidential Elections

Mandiant assesses with high confidence that social media accounts we judge to comprise part of the pro-People's Republic of China (PRC) DRAGONBRIDGE information operations campaign promoted content pertaining to the 2024 Taiwan presidential election on multiple platforms, including content attempting to discourage Taiwanese from voting for the ruling Democratic Progressive Party (DPP).

- ○ Narratives promoted by this activity set negatively portrayed the DPP and its presidential candidate Lai Ching-te, describing the DPP and its members as vote-seeking, ineffective, corrupt, and unfit for leadership.
- ○ The promoted narratives also aimed to portray Taiwan and its people as experiencing economic woes under DPP's leadership. These narratives suggested that if Lai and the DPP were to be elected, the situation would worsen for Taiwan and its citizens.





Rakel Ladarius
@proscenium1943

人前滿口仁義道德,人後抄襲好手，何博伦、赵天麟、张宏陆......下一个是谁呢? 民進黨的標準是不是都「毫無標準」?民進黨的底線是不是叫「毫無底線」? 张宏陆身為民進黨新北黨立委参選人,这么明显的抄襲，真是狠狠打臉賴清德學倫條款，也證明賴的改革形同虛設。

Translated from Chinese by Google

People who talk about benevolence, justice and morality in front of others, but are good plagiarists in the back, such as He Bolun, Zhao Tianlin, Zhang Honglu... who is next? Are the standards of the DPP "no standards"? Is the bottom line of the DPP called "no bottom line"? ? Zhang Honglu is a candidate for the DPP New Taipei City Legislative Council. Such obvious plagiarism really slaps Lai Qing's academic ethics clause in the face, and also proves that Lai's reforms are in vain.

6:56 PM · Nov 7, 2023 · 31 Views

Lachlan David
@LachlanDavid3

#台灣 台灣不能成為下一個烏克蘭，青年要進職場不要上戰場，「每一張投給民進黨的選票，都變成他們貪污的鈔票」。

Translated from Chinese by Google

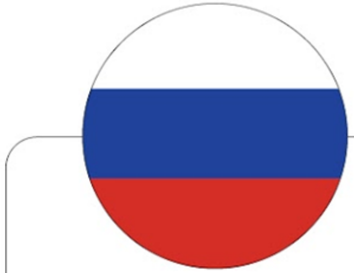
#台灣 Taiwan cannot become the next Ukraine. Young people should enter the workplace instead of going to the battlefield. "Every vote cast for the DPP becomes their corrupt money."

facebook.com
民進黨一味媚日舔美、敵中抗中反中，則臺灣不僅無法有效融入
民進黨一味媚日舔美、敵中抗中反中，則臺灣不僅無法有效融入亞洲區域經濟貿易，事實上舔美拜美尊美結果，再多也不...

8:24 PM · Nov 14, 2023 · 398 Views

6 51 25

Notable Russia-, Iran-, and PRC-Aligned Campaigns Targeting U.S. Audiences

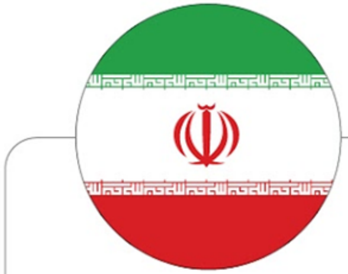


Internet Research Agency (IRA)

- Peace Data
- NAEBC

Doppelganger

Hacktivist Personas



Liberty Front Press

Endless Mayfly

Roaming Mayfly

EvenPolitics

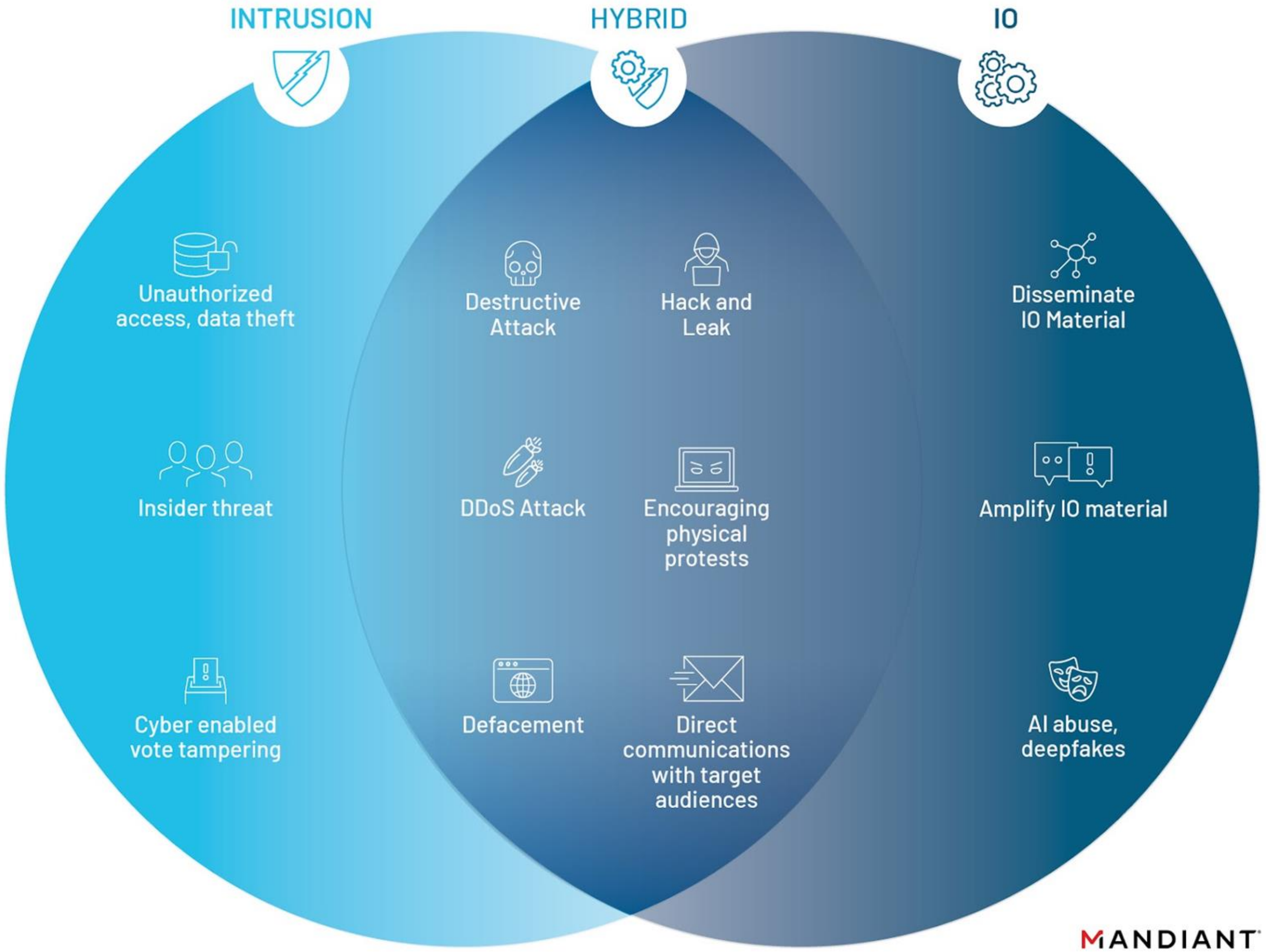
Enemies of the People

Proud Boys

DRAGONBRIDGE

HaiEnergy

Understanding Hybrid Operations



INTRUSION

Unauthorized access, data theft

Insider threat

Cyber enabled vote tampering

HYBRID

Destructive Attack

Hack and Leak

DDoS Attack

Encouraging physical protests

Defacement

Direct communications with target audiences

IO

Disseminate IO Material

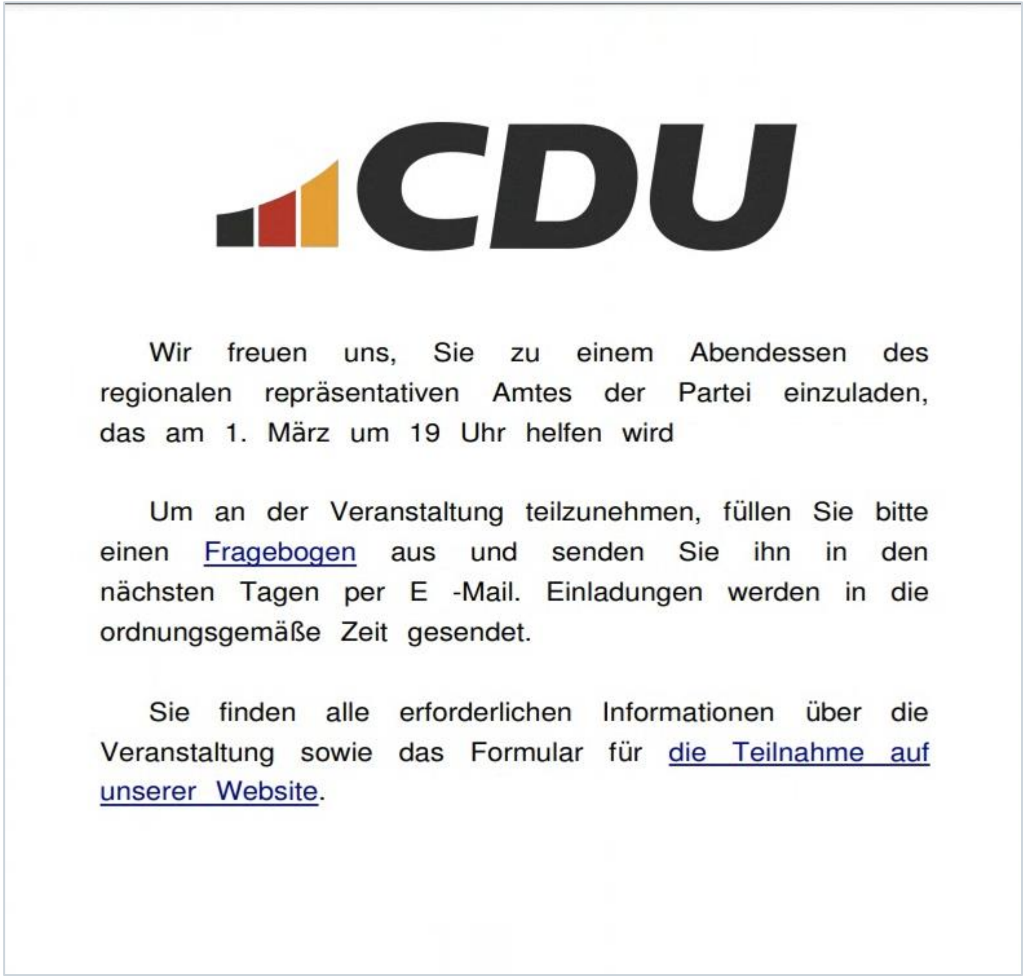
Amplify IO material

AI abuse, deepfakes

Espionage Targeting European Political Groups in Q1

In late February 2024, a Russia-nexus cluster of activity that has previously targeted diplomacy-related entities conducted a phishing campaign likely centered around German political parties and their affiliates:

- Phishing emails were sent to victims using an invite to a dinner reception bearing a logo from the Christian Democratic Union (CDU), a political party in Germany.
- The campaign represented a departure from the group's typical remit of targeting foreign embassies around the world, demonstrating the evolving nature of geopolitically motivated intelligence collection requirements.
- The German-language lure document contains a link directing the victims to a ZIP file containing a custom dropper hosted on an actor-controlled compromised website.
- The dropper delivered a second-stage CDU-themed lure document and a custom next-stage payload retrieved from the same compromised domain.



CDU

Wir freuen uns, Sie zu einem Abendessen des regionalen repräsentativen Amtes der Partei einzuladen, das am 1. März um 19 Uhr helfen wird

Um an der Veranstaltung teilzunehmen, füllen Sie bitte einen Fragebogen aus und senden Sie ihn in den nächsten Tagen per E -Mail. Einladungen werden in die ordnungsgemäße Zeit gesendet.

Sie finden alle erforderlichen Informationen über die Veranstaltung sowie das Formular für die Teilnahme auf unserer Website.

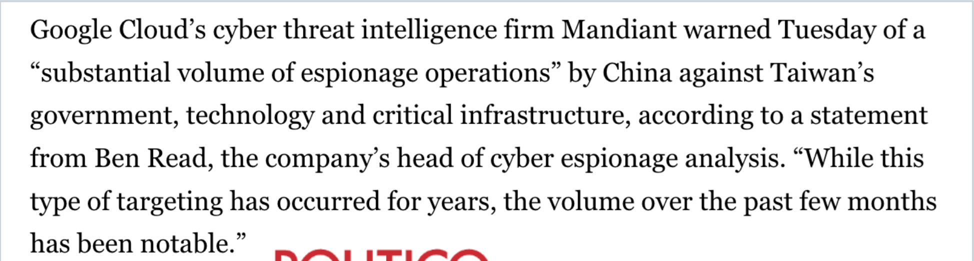
Interrelations between Chinese Capabilities, Posturing, and Election-Specific Targeting

Observed Activity:

- Phishing campaigns leveraging Taiwanese presidential election-themed lures to deliver malware.
- Targeting of the energy, telecommunications, and government sectors with tools that are shared to a limited degree among China-linked threat actors to include POISONPLUG and SOGU malware.
- Commercially available tools including Cobalt Strike BEACON have been used to target Taiwanese entities in phishing campaigns.
- Tangential impact has also been observed in 2023 and into 2024 as threat actors leverage zero days that targeted edge devices and security appliances.

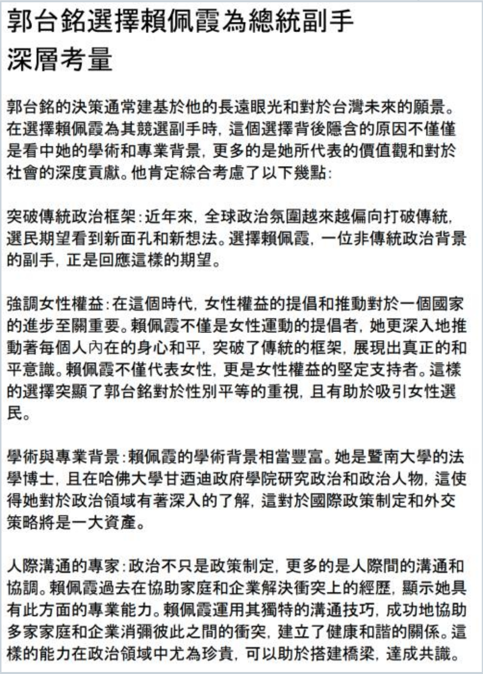
Analysis:

- Ongoing intelligence interest in the candidates, support organizations, and other interested parties surrounding elections in areas of interest
  - Especially amplified by the perceived closeness of an election as contentious as that of January 13
- Various capabilities—including initial access techniques, enablement preparations, tooling, and obfuscation efforts—are interoperable and fungible across a range of core state-nexus objectives.



Google Cloud's cyber threat intelligence firm Mandiant warned Tuesday of a "substantial volume of espionage operations" by China against Taiwan's government, technology and critical infrastructure, according to a statement from Ben Read, the company's head of cyber espionage analysis. "While this type of targeting has occurred for years, the volume over the past few months has been notable."

POLITICO



郭台銘選擇賴佩霞為總統副手深層考量

郭台銘的決策通常建基於他的長遠眼光和對於台灣未來的願景。在選擇賴佩霞為其競選副手時，這個選擇背後隱含的原因不僅僅是看中她的學術和專業背景，更多的是她所代表的價值觀和對於社會的深度貢獻。他肯定綜合考慮了以下幾點：

突破傳統政治框架：近年來，全球政治氛圍越來越偏向打破傳統，選民期望看到新面孔和新想法。選擇賴佩霞，一位非傳統政治背景的副手，正是回應這樣的期望。

強調女性權益：在這個時代，女性權益的提倡和推動對於一個國家的進步至關重要。賴佩霞不僅是女性運動的提倡者，她更深入地推動著每個人內在的身心和平，突破了傳統的框架，展現出真正的和平意識。賴佩霞不僅代表女性，更是女性權益的堅定支持者。這樣的選擇突顯了郭台銘對於性別平等的重視，且有助於吸引女性選民。

學術與專業背景：賴佩霞的學術背景相當豐富。她是暨南大學的法學博士，且在哈佛大學甘迺迪政府學院研究政治和政治人物，這使得她對於政治領域有著深入的了解，這對於國際政策制定和外交策略將是一大資產。

人際溝通的專家：政治不只是政策制定，更多的是人際間的溝通和協調。賴佩霞過去在協助家庭和企業解決衝突上的經歷，顯示她具有此方面的專業能力。賴佩霞運用其獨特的溝通技巧，成功地協助多家家庭和企業消弭彼此之間的衝突，建立了健康和諧的關係。這樣的能力在政治領域中尤為珍貴，可以助於搭建橋梁，達成共識。

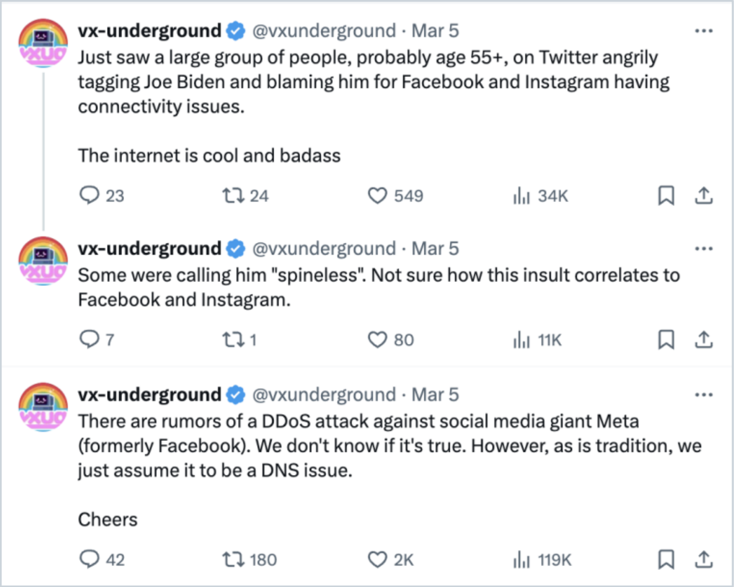
Super Tuesday

Background:

- On 05 March, over a dozen states held primaries or caucuses to choose their respective party candidates.
- Mandiant observed at least one event parallel to, but not necessarily related to, the day of elections:
  - Throughout the day, a technical issue at Meta led to a social media outage preventing users from accessing their Facebook and Instagram accounts.
  - The hacktivist front *Anonymous Sudan*—which supports pro-Russia narratives, amplifies storylines opposing the West in general, and often claims DDoS attacks against Western entities—quickly claimed responsibility alongside affiliated threat actors *Skynet* and *Godzilla*.

Takeaways:

- Even disruptive events with no substantive relation to (or that are demonstrably unrelated to) the conduct of an election can have the narrative hijacked by opportunistic threat actors.
  - Threat actors seeking to disrupt real-world events do not always need to even deploy capabilities to do so.
  - Hacktivist fronts (as well as extortionary cybercriminals) continue to benefit the most from the rapid publicity malicious claims often receive.



vx-underground @vxunderground · Mar 5

Just saw a large group of people, probably age 55+, on Twitter angrily tagging Joe Biden and blaming him for Facebook and Instagram having connectivity issues.

The internet is cool and badass

vx-underground @vxunderground · Mar 5

Some were calling him "spineless". Not sure how this insult correlates to Facebook and Instagram.

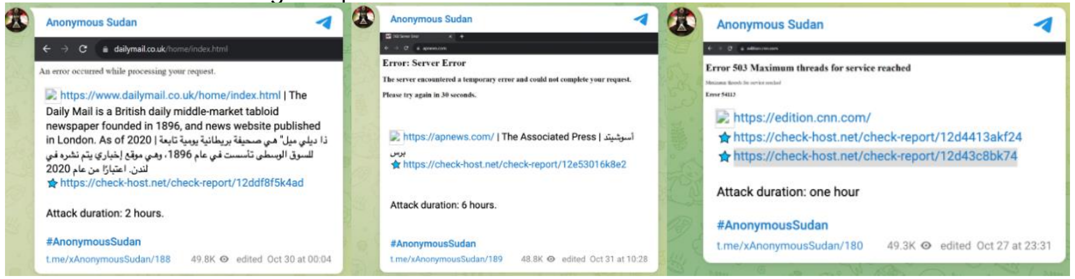
vx-underground @vxunderground · Mar 5

There are rumors of a DDoS attack against social media giant Meta (formerly Facebook). We don't know if it's true. However, as is tradition, we just assume it to be a DNS issue.

Cheers

Above: Speculation regarding the source of Super Tuesday's social media outage, as well as commentary on public reactions.

Below: Prior claims by Anonymous Sudan targeting Western media outlets in stated support for Gaza, reflecting their ongoing conduct of activity directly parallel to U.S. domestic as well as global political issues.



Anonymous Sudan

An error occurred while processing your request.

https://www.dailymail.co.uk/home/index.html | The Daily Mail is a British daily middle-market tabloid newspaper founded in 1896, and news website published in London. As of 2020 | ذا ديلي ميل" هي صحيفة بريطانية يومية تابعة
للسوق الوسطى تأسست في عام 1896، وهي موقع إخباري يتم نشره في
لندن. اعتبارًا من عام 2020
https://check-host.net/check-report/12ddf8f5k4ad

Attack duration: 2 hours.

#AnonymousSudan
t.me/xAnonymousSudan/188 49.8K edited Oct 30 at 00:04

Anonymous Sudan

Error: Server Error

The server encountered a temporary error and could not complete your request.

Please try again in 30 seconds.

https://apnews.com/ | The Associated Press | أسوشيتد
برس
https://check-host.net/check-report/12e53016k8e2

Attack duration: 6 hours.

#AnonymousSudan
t.me/xAnonymousSudan/189 48.8K edited Oct 31 at 10:28

Anonymous Sudan

Error 503 Maximum threads for service reached

https://edition.cnn.com/
https://check-host.net/check-report/12d4413akf24
https://check-host.net/check-report/12d43c8bk74

Attack duration: one hour

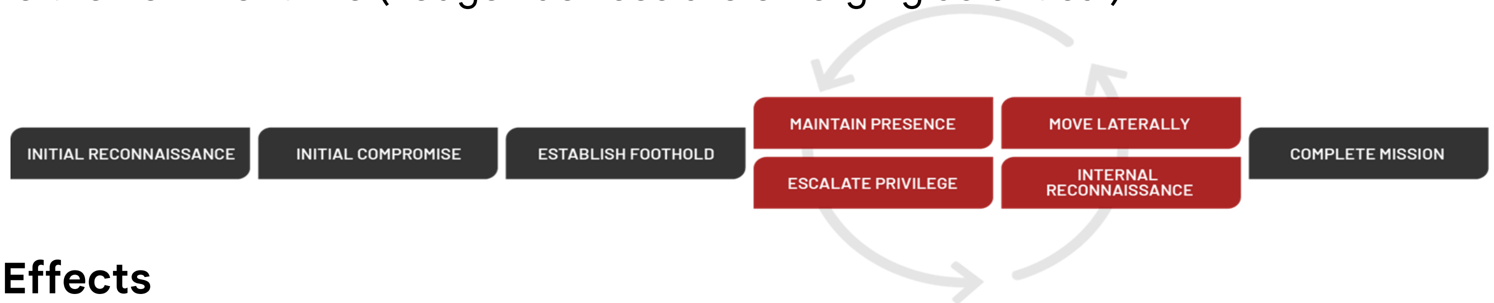
#AnonymousSudan
t.me/xAnonymousSudan/180 49.3K edited Oct 27 at 23:31

Strategic Outlook

Threat Commonalities

“Traditional” Cyber Threats

- Generic phishing and spear-phishing continue to provide indispensable initial access vectors for threat actors
- A “campaign” still requires a mix of skills and capabilities
- Non-election specific issues such as ransomware can quickly play a role in public confidence, integrity, and availability
    - Activity doesn’t have to directly target elections to impact them, either immediately or down the line
- Supply chains are the new front line (“edge” devices are emerging as critical)



Cognitive Domain Effects

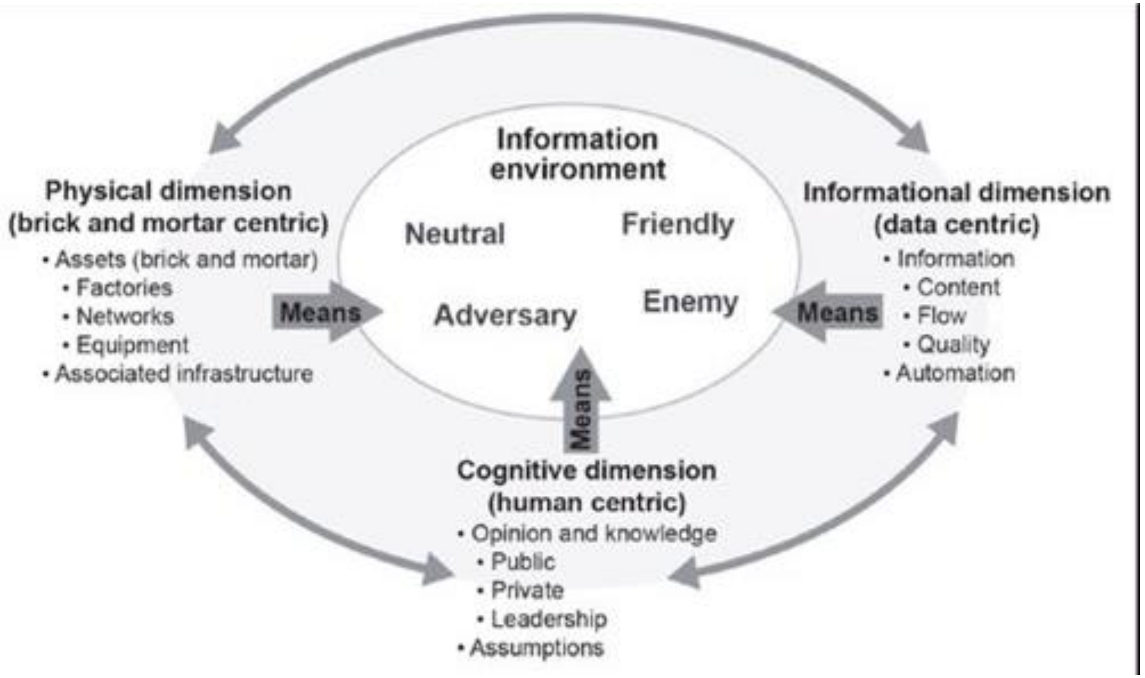
- Perception of the attack and its consequences
- There is no nuance in the media
- The future isn’t now, but some may think it is (AI, deepfakes, etc.)

Identification of Key Terrain

Placing Resources Where They Do the Most Good

Domains to Address:

- Traditional Network Defenses
- Leadership Education
- Private Sector Partnerships
- Data Resilience and Redundancy
  - COOP Planning
- Adversarial Intelligence
  - Prioritized requirements



Hardening and Resilience Considerations

Cyber:

- ➔ Hunting
- ➔ Exercises
- ➔ Threat intel for the masses

Cyber-Cognitive:

- ➔ “Two-person” integrity
- ➔ Wargaming decisions

Cyber-Physical:

- ➔ Where does the IT work happen?

Discussion & Questions

EAC Contact Form:
https://www.eac.gov/contactuseac

EAC Contact Email:
clearinghouse@eac.gov

MANDIANT®
NOW PART OF Google Cloud

Thank you