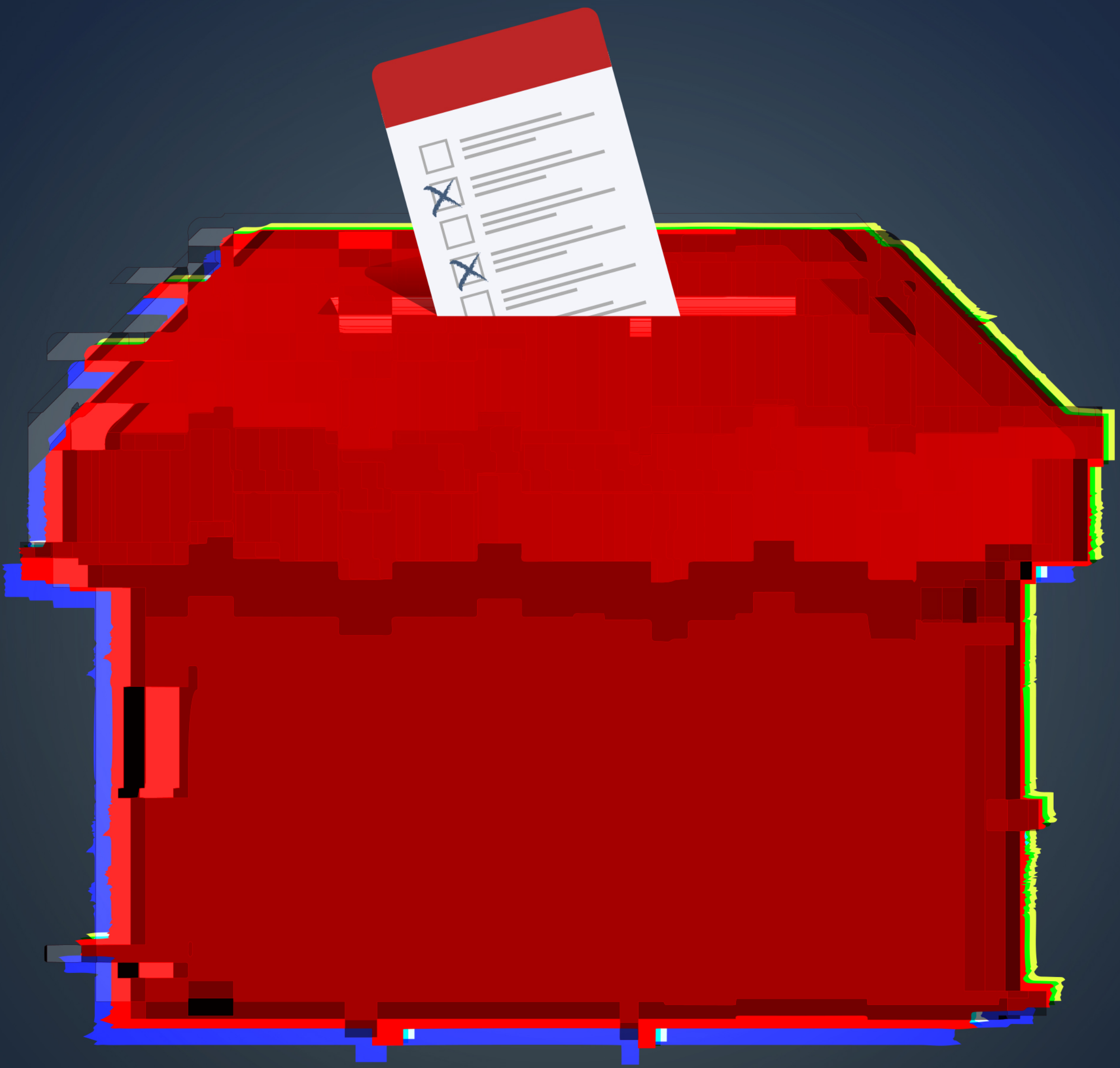
ELECTION CYBER INTERFERENCE THREATS & DEFENSES:

A DATA-DRIVEN STUDY



TIDAL CYBER

THREAT-INFORMED DEFENSE

tidalcyber.com

EXECUTIVE SUMMARY

This report provides a comprehensive look at cyber threats to global elections in 2024 and insights on how to prioritize defenses against top adversaries & election interference tactics, techniques, and behaviors ("TTPs").

TIDAL CYBER ASSESSES THAT THERE IS A CONSIDERABLE THREAT OF CYBER TECHNICAL INTERFERENCE FACING GLOBAL ELECTIONS THIS YEAR. Considering that 2024 is a historic year for elections – with an estimated half of the world's population taking part in democratic votes – this high threat of cyber interference has significant implications for global free society, threatening to undermine confidence in voting processes or – at worst – even alter electoral outcomes. We assess that cyber actors aligned with multiple adversarial nations are continuing to evolve their TTPs in an effort to successfully attack both historical & new targets for election-related interference.

Our study leans on actual data & evidence to pinpoint the most notable potential hotspots for interference, spotlight known & emerging interference TTPs, and use those insights to provide a *prioritized* list of *relevant* guidance that can be used by defenders protecting organizations & personnel involved in election administration, political & campaign staff, the media, and many other entities supporting (or even exposed to) elections and election-related content.

HOW THE REPORT IS STRUCTURED

- *Measuring Election Cyber Interference Threats* introduces our data-driven analysis and rankings around the relative level of cyber interference facing dozens of countries holding major elections this year. The full list of rankings and supporting cyber adversary data is available in *Appendix I*.
- *Key Cyber Interference Attack Methods* dives into eight sets of known & emerging interference TTPs, identifying the techniques most likely to be observed this year based on review of dozens of historical interference cases since 2008 and our analysis of trends in the broader cyber threat landscape. This list of cases, clustered by adversarial group & country, is provided again in *Appendix II*.
- We provide numerous links to cyber adversary threat profiles, victimology data, historical & recent TTPs, and defenses resources from Tidal's freely available *Community Edition* throughout this report, and a complete list of links, grouped by topic, is provided again in *Appendix IV*. We also used Tidal's *Enterprise Edition* to generate a prioritized list of defensive recommendations, which are summarized in *Section 3* and shared in full in *Appendix III*.

MEASURING ELECTION CYBER INTERFERENCE THREATS

For this study, we developed a data-driven methodology to measure the relative threat of election cyber interference facing countries that are holding major, nationwide elections in 2024. This section provides a summary of the methodology and analysis of top results, which are also visualized in Figure 2. More details and a full list of rankings & supporting data are provided in *Appendix I*.

Leaning on the definitions provided in the 2021 U.S. Intelligence Community Assessment ("ICA"), *Foreign Threats to the U.S. 2020 Federal Election*, we define "election cyber interference threat" as the potential for cyber adversary-driven malicious activity targeting the technical aspects of democratic election processes. Our study focuses on these technical aspects rather than the broader threat of "election influence operations", which includes dis- & misinformation efforts. The study mainly focuses on foreign sources of cyber election interference (emanating from outside the target country) – specifically those associated with the four clear top perpetrator countries (Russia, China, Iran, and North Korea), as cited by both *U.S. officials* and *major security vendors*.

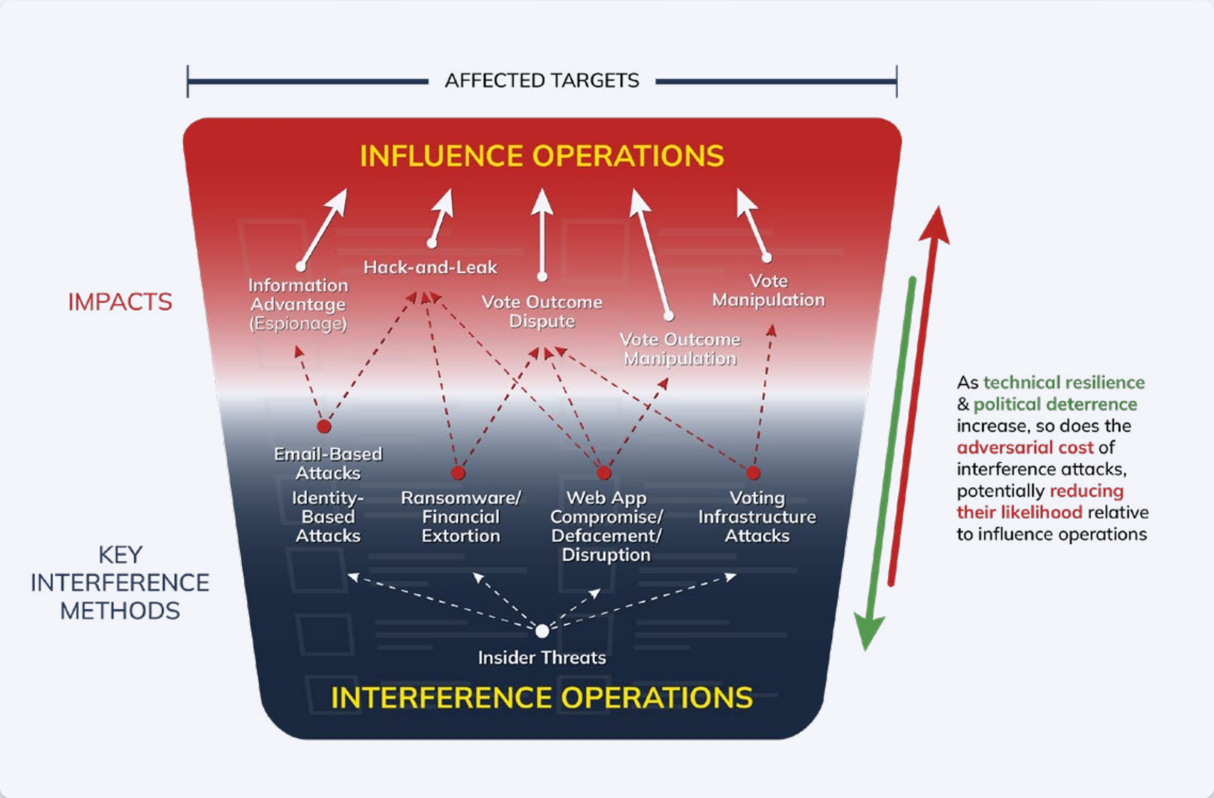
As the ICA notes, interference is a subset of wider influence operations, and the results of interference-focused attacks (see many examples in later sections) are indeed often used to support disinformation, misinformation, and other influence campaigns. They can also yield access to sensitive information useful for espionage purposes, and in the most concerning scenario, potentially even alter real (or perceived) election outcomes.

CYBER INTERFERENCE: THREATS VS. RISKS

Our study, including our ranking methodology, focuses on interference *threats* – the potential for interference activity to occur, based on actors' *motivation* and *ability* to carry out such attacks. Other critical factors can influence the level of interference *risk* that a country/election might face, including technical defenses & resilience measures against these threats (which provide actual protection, as well as deterrence value), plus adversaries' perceived impact of interference attacks versus other influence operations.

For example, a *2022 ICA*, released in December 2023, noted how such factors might have contributed to the decline in persistent interference efforts in U.S. elections since 2016. A *vendor assessment* similarly noted the lack of "impactful" cyber operations around the 2022 U.S.

midterm elections but also highlighted how midterm elections offer “limited gains” for adversarial governments, while spotlighting how “Election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome”. Convergence of potential adversarial interest in a given country is a significant factor in our interference threat rankings.



As technical resilience & political deterrence increase, so does the adversarial cost of interference attacks, potentially reducing their likelihood relative to influence operations

Figure 1: The interplay of factors that might drive or deter adversaries from pursuing election interference and/ or influence operations, and the key methods & impacts of interference attacks.

Clearly, many factors (often opposing forces) must be considered if attempting to estimate cyber interference risk levels (*Figure 1* models the interplay of some of these factors), and factors like deterrence & resilience ability are difficult to widely quantify, at least using public sources. But the *considerable presence of underlying election-related vulnerabilities*, often in countries less geopolitically prominent than ones like the United States or United Kingdom (where the deterrence effect of an exposed interference attempt might be lower), underscores our assessment that many voting countries are likely facing a significant and real potential for cyber-enabled election interference this year. Meanwhile, the continued evolution of interference TTPs (outlined in later sections) highlights the need for ongoing vigilance against interference actors, even in countries that might possess greater resilience or deterrence potential.

ANALYSIS

Metrics derived from our relative rankings of 64 countries holding major nationwide elections in 2024 (full list in *Appendix I*) underscore the scale & scope of cyber interference threats globally this year:

- Per our methodology, the **10 COUNTRIES FACING THE HIGHEST LEVELS OF ELECTION CYBER INTERFERENCE THREATS** are: the United States, United Kingdom, South Korea, India, Belgium, Pakistan, Belarus, Mexico, Georgia, Indonesia. These represent top potential hotspots for cyber defenders supporting organizations involved in or related to elections in these areas.

- 31% of countries (20 of 64) face the *highest threat levels*, defined as facing state-backed groups associated with multiple priority adversary nations (top known cyber interference offenders), including multiple specific priority adversary groups. These countries also typically face many state-backed groups associated with the priority adversary countries generally.[1]

  - The United States, United Kingdom, and South Korea face adversaries from all four "priority" adversary countries, including multiple priority threat actor groups each.

- Most voting countries this year most face at least some interference threat.

  - Nearly two thirds (41, or 64%) face at least one state-backed cyber threat actor attributed to Russia, China, or Iran (and most of these face multiple such actors).

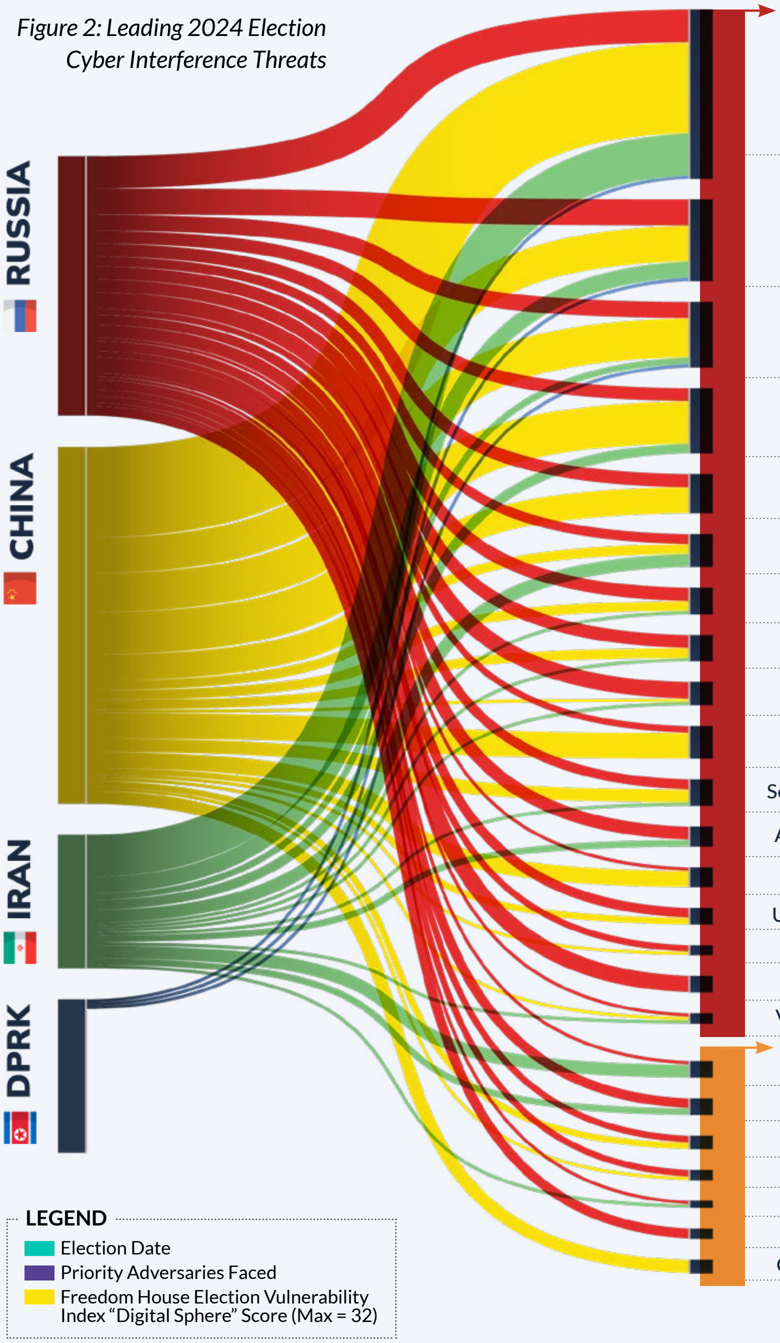
  - 27 countries (42%) face state-backed actors associated with multiple priority adversary countries. 11 face actors from the three top offenders (Russia, China, & Iran).

- Pakistan, Indonesia, Venezuela, Uzbekistan, India, Belarus, and Ethiopia face considerable interference threats and face the strongest *underlying concerns* with digital infrastructure as it relates to electoral processes. These represent top locations where successful cyber interference could occur, leading to data access/exfiltration, amplification of influence operations, or potential electoral disruption or manipulation.

LEADING 2024 ELECTION CYBER INTERFERENCE THREATS

Flow size reflects tally of state-backed cyber actors observed per victim country

Figure 2: Leading 2024 Election Cyber Interference Threats



LEGEND

- 🟩 Election Date
- 🟪 Priority Adversaries Faced
- 🟨 Freedom House Election Vulnerability Index "Digital Sphere" Score (Max = 32)

United States	November 5	8	21
United Kingdom	TBA	7	--
South Korea	April 10	4	19
India	TBA	3	14
Belgium	June 9	4	--
Pakistan	February 8	3	8
Belarus	February 25	3	14
Mexico	June 2	3	17
Georgia	TBA	3	26
Indonesia	February 14	1	13
South Africa	May 1	2	26
Azerbaijan	February 7	2	--
Mongolia	June 28	2	--
Uzbekistan	TBA	2	12
Slovakia	March 23	2	--
Romania	TBA	2	--
Venezuela	TBA	1	7
Lebanon	TBA	1	19
Austria	TBA	1	--
Portugal	May 10	1	--
Croatia	TBA	1	--
Ireland	March 8	1	--
Lithuania	May 12	1	--
Cambodia	February 25	1	--

Real evidence (unfortunately) already provides some early support behind our assessment and ranking methodology. Reports indicate Taiwan (which faces 17 adversaries associated with China) was *"bombarded"* with cyberattacks, many attributed to China, ahead of its January 13 national elections. Several Finnish government websites (Finland faces multiple actors linked to Russia and other priority countries) allegedly suffered *denial-of-service attacks* from the Russia-aligned NoName group during its presidential election month, while also facing a *spree* of ransomware attacks. Russia itself, which holds presidential elections in March, appears relatively high in our rankings, facing its own adversaries (while also suffering from a very poor Election Vulnerability Index). In this case, APT28 was recently linked to *spearphising attacks targeting Russian dissidents*, including within its borders.

ADVERSARIES

Below is a summary of the key, named cyber adversary groups known to carry out and support election cyber interference activity. Links are provided to adversary profiles, victimology data, and TTPs in Tidal's freely available *Community Edition*. A searchable list of these (and many more) adversaries is also available in the platform *here*.

The data summarized here informed the full list of interference threat rankings in *Appendix I*, and more detailed lists of observed activities per group can be found in *Appendix II*.

ADVERSARY-CENTRIC THREAT PROFILING

The metadata we used to build our cyber interference rankings, including observed victim locations and adversary attribution & motivation, represent prime data points for populating threat profiles – collections of relevant threats to your organization. Explore our free 60-page ebook, *The Ultimate Guide to Cyber Threat Profiling*, to learn more about exactly how to build & maintain (and take action) on an adversary-centric threat profile.

Group	Suspected Attribution	Observed Election Cyber Interference Activity	Observed Victim Countries	MITRE ATT&CK® Techniques
APT28	🇷🇺	A prolific perpetrator of election-related interference attacks in multiple regions, especially *email phishing-based attacks* and more recently, *credential exploit attacks*. Multiple *denial-of-service attacks* timed around elections have also been linked to APT28 or groups backed by it.	17	*104*
APT29	🇷🇺	Attributed to the *2015-16 compromise* of the network of the U.S. Democratic National Committee ahead of 2016 national elections and more recent election-related mass phishing attacks.	18	*135*
Magic Hound (aka Phosphorous, APT35, et al)	🇮🇷	Targets individuals associated with U.S. presidential campaigns by *abusing password reset & account recovery features* and *sending phishing emails to staffers' personal accounts*.	5	*78*
ZIRCONIUM (aka APT31)	🇨🇳	Also targeted personal email accounts of U.S. presidential campaign staffers with *credential harvesting- and information gathering-focused phishing emails.*	5	*26*
APT41	🇨🇳	Attributed to a *spearphishing campaign* targeting media reps ahead of legislative elections in Hong Kong. APT41 has also carried out *multiple wide-reaching campaigns* targeting U.S. state government entities.	11	*76*
Leviathan (aka TEMP.Periscope)	🇨🇳	Perpetrated a *broad series of malware-based compromises* of election-related entities in Cambodia ahead of general elections.	4	*44*
APT3	🇨🇳	Carried out *spearphishing attacks targeting government agencies* ahead of Hong Kong's legislative elections.	3	*43*
Kimsuky	🇰🇵	Linked to *multiple attacks* that leveraged phishing lures themed around regional as well as international elections.	4	*89*

KEY CYBER INTERFERENCE ATTACK METHODS

Tidal Cyber conducted an extensive review of publicly reported election-related cyber interference cases, in order to identify common and emerging tactics, techniques, and procedures associated with these types of attacks. This section details those TTPs and trends, organized under eight higher-level "attack methods".

To aid defenders, we've provided links throughout this section to collections of those TTPs – helpfully mapped to the MITRE ATT&CK® knowledge base – hosted in Tidal's freely available *Community Edition*. ATT&CK alignment enables quick, direct pivoting from intelligence on attacker techniques to myriad defensive resources across the spectrum of capability types (e.g., mitigations, protections, detections, responses, logging, and tests). A set of prioritized guidance – based on our analysis of common defensive measures relative to interference TTPs – is provided in the next section.

SOCIAL ENGINEERING & IDENTITY-BASED THREATS

Primary Targets: Election-related personnel & organizations, including politicians & political staff, campaign teams, election administrators & workers (including volunteers), and media representatives

EMAIL-BASED ATTACKS

Notable Examples:

- **2008:** U.S. presidential campaign staff targeted with *malicious spearphishing email attachments* attributed to **unspecified Chinese espionage actors**.
- **2015-2016:** Actors, attributed to **APT28 & APT29 (Russia)**, compromised the network of the U.S. Democratic National Committee ahead of national elections. Responders *suspect initial access was gained via spearphishing emails*.
- **March 2016:** U.S. presidential campaign chair's *personal email compromised via a credential harvesting-focused spearphishing attack* attributed to **APT28.**
- **July & August 2016:** Ahead of legislative elections, media representatives in Hong Kong received *spearphishing emails intended to deliver malware*, in a campaign attributed to **APT41 (China).**

- **August 2016:** Actors attributed to **APT3 (China)** carried out at least *three spearphishing attacks targeting two government agencies* in Hong Kong in the month ahead of legislative elections.

- **November 2016: Russian military intelligence actors** sent spearphishing emails with malicious attachments to Florida election administrators, "*[gaining] access* to the network of at least one Florida county government".

- **2017: APT28** compromised the professional & personal accounts of French presidential campaign staff via *credential harvesting-focused spearphishing attacks*. 9GB worth of data was leaked.

- **May 2017:** Malta's government IT systems allegedly experienced a *40% increase in phishing, DDoS and malware-based attacks*, attributed to **APT28**, in the month before the country's general election.

- **August 2017:** Staffers supporting a U.S. Senator running for re-election in 2018 midterms received *credential harvesting-focused spearphishing emails* attributed to APT28.

- **2018: TEMP.Periscope actors (China)** perpetrated a *broad series of malware-based compromises* of election-related entities & individuals in Cambodia ahead of the country's July 2018 elections, including the National Election Commission, a politician, human rights groups, and media entities. In at least one case, initial access was achieved via a phishing email containing a link to download malware.

- **2020: Magic Hound (Iran)** and **ZIRCONIUM (China)** targeted the personal and *work email accounts* of U.S. presidential campaign staffers with *credential harvesting- and information gathering-focused phishing emails*.

- **2020:** *Reports indicated* that unspecified North Korea-aligned actors carried out phishing attacks targeting organizations supporting U.S. presidential candidates.

- **April 2020:** Suspected **Kimsuky (North Korea)** actors attempted to *deliver malware to select targets using phishing lures* designed as identifying North Korean citizens running in South Korea's legislative elections that month.

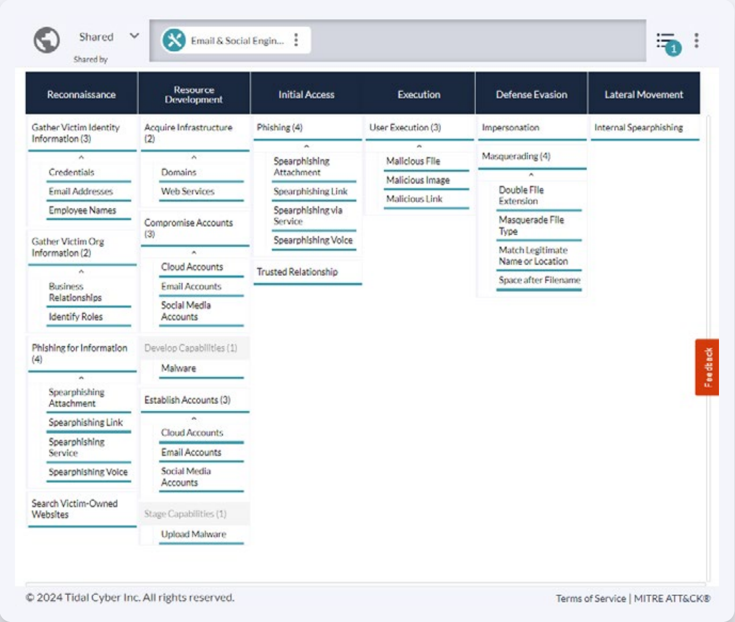
- **May 2021:** Suspected **APT29** actors used a *legitimate mass-emailing service to conduct a wide-ranging phishing campaign* that used election-fraud-related lures.

- **May-August 2022:** Researchers observed a *dramatic increase in email-based attacks* targeting election workers in "battleground" U.S. states ahead of national midterm elections. Unattributed attackers sent credential harvesting-focused phishing emails and "hijacked" existing email threads related to absentee voting processes, in an attempt to further lower targets' guards.

As these findings show, email-based attacks, especially *spearphishing*, are a leading attack method for gaining initial access into election-related networks. *Phishing attachments* are used to deliver malware for longer-term data collection and/or persistence, while *malicious links* are used to harvest credentials for access and also to initiate malware downloads.

While phishing in general has remained a consistent threat around elections worldwide for many years, the mechanics of these attacks have evolved as adversaries adapt to multiple external factors. First, adversaries have adopted new ways to evade reinforced defenses and awareness of social engineering schemes. Attacks like those in 2016 & 2020 in the United States and 2017 in France underscore the threat of phishing targeting election personnel's personal email accounts, where organization-wide protections might not be present.[2] Magic Hound, the Iran-backed group responsible for targeting presidential campaign staff in 2020, is also *known* to send phishing links over *social media platforms*. Reports from 2022 highlighted more recent credential phishing targeting election workers via email "thread hijacking", an improved impersonation technique designed to lower a target's guard for engaging with malicious content (this technique requires existing access to a victim account, but this can then be leveraged for greater impact).

Adversaries are also adapting to global events in constant effort to make their social engineering lures as convincing as possible. The evidence above highlights multiple instances where adversaries crafted phishing lures around current election cycles, including 2022 cases whereresearchers observed new lures themed around absentee voting, which *remained popular* even after the height of the COVID-19 pandemic. (*Prominent cybercriminals* that threaten a wide range of organization types, including enterprises, also use *timely election-related lures*.) In line with *trusted assessments*, we also expect to see cyber adversaries adopting generative AI technology to make election-related phishing & social engineering attacks more convincing during upcoming election cycles.



Reconnaissance	Resource Development	Initial Access	Execution	Defense Evasion	Lateral Movement
Gather Victim Identity Information (3)	Acquire Infrastructure (2)	Phishing (4)	User Execution (3)	Impersonation	Internal Spearphishing
Credentials	Domains	Spearphishing Attachment	Malicious File	Masquerading (4)	
Email Addresses	Web Services	Spearphishing Link	Malicious Image	Double File Extension	
Employee Names	Compromise Accounts (3)	Spearphishing via Service	Malicious Link	Masquerade File Type	
Gather Victim Org Information (2)	Cloud Accounts	Spearphishing Voice		Match Legitimate Name or Location	
Business Relationships	Email Accounts	Trusted Relationship		Space after Filename	
Identify Roles	Social Media Accounts				
Phishing for Information (4)	Develop Capabilities (1)				
Spearphishing Attachment	Malware				
Spearphishing Link	Establish Accounts (3)				
Spearphishing Service	Cloud Accounts				
Spearphishing Voice	Email Accounts				
Search Victim-Owned Websites	Social Media Accounts				
	Stage Capabilities (1)				
	Upload Malware				

© 2024 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®

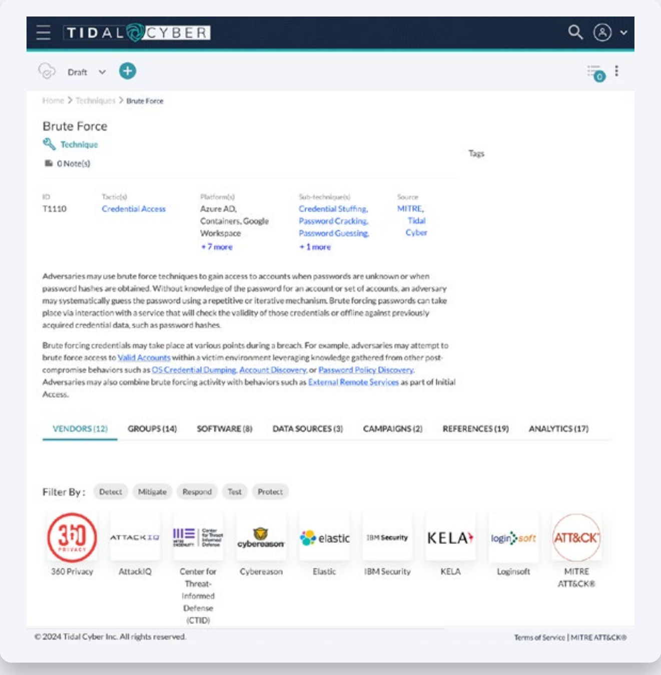
Figure 3: A collection of ATT&CK Techniques relevant to the interference attack method discusses in this section, available in Tidal's free Community Edition here.

Defenders should remember that a whole TTP ecosystem exists around phishing and other social engineering attacks – the mechanics of these campaigns aren't entirely encapsulated in just the *single Phishing technique* defined in ATT&CK, for example. Important surrounding behaviors often involve *standing up infrastructure* (such as *domains* or using *third-party email delivery services*) and the ways users engage with malicious content (e.g., clicking a link, downloading an attachment, and maybe executing it).[3] When viewed through the lens of *threat-informed defense*, these all present additional opportunities to defend against adversaries' email- & social engineering-based election interference methods. We've provided a helpful collection of common TTPs used for these attacks in Tidal's free Community Edition *here*, where users can easily pivot from the techniques into resources around related adversaries and/or relevant defenses.

IDENTITY-BASED ATTACKS

Notable Examples:

- **August-September 2019:** Researchers observed **Magic Hound (Iran)** actors attempting to *abuse password reset and account recovery features* to access email accounts associated with a U.S. presidential campaign and other political and media targets, often using extensive amounts of previously collected personal information and or previously compromised secondary email accounts to support these attacks.
- **September 2019-September 2020: APT28 (Russia)** appeared to *"evolve" its approach to targeting election-related personnel*, carrying out a massive brute force and password spray campaign directed at targets including unspecified U.S. and UK organizations "directly involved in political elections" and NGOs working on issues like *election integrity*. Attacks featured *special IP address anonymization tooling* to persistently evade detection.



Brute Force

Technique

0 Note(s)

Tags

ID	Tactic(s)	Platform(s)	Sub-technique(s)	Source
T1110	Credential Access	Azure AD, Containers, Google Workspace + 7 more	Credential Stuffing, Password Cracking, Password Guessing, + 1 more	MITRE, Tidal Cyber

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to Valid Accounts within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as OS Credential Dumping, Account Discovery, or Password Policy Discovery. Adversaries may also combine brute forcing activity with behaviors such as External Remote Services as part of Initial Access.

Figure 4: Numerous defensive resources & capabilities, including mitigations, detections, logging sources, analytics, & simulation tests, exist around Brute Forcing, a technique used by Russia's APT28 to target election-related personnel.

While the technical targets (email/user accounts) and goals (initial access for information access) for these attacks are the same as for social engineering schemes like phishing, this category differs in that it does not require direct engagement with or interaction from a target user, such as clicking a malicious link or downloading/opening a malicious attachment.

Prominent public examples of these identity-based attacks for election-related targeting mainly exist since 2019, making this a relatively newer attack method. The first cases, associated with Magic Hound, involved "gaming" password reset processes. While actors had existing access to secondary email accounts in some cases, the key differentiator is that they appeared to gain access to the target account *without user interaction*, making them potentially harder to detect.

The more recent case, involving APT28, required no user interaction or pre-existing secondary access at all. While brute forcing and password spraying are hardly sophisticated techniques, they can clearly be used to capitalize on vulnerabilities like weak password policies and represent a viable initial access method for "persistent" actors with the will & patience to wait for successful compromises. The fact that APT29, another known election interference actor, has also been *recently observed using similar techniques to compromise prominent organizations*, this appears to represent a noteworthy new technique set worth tracking ahead of so many votes this year.

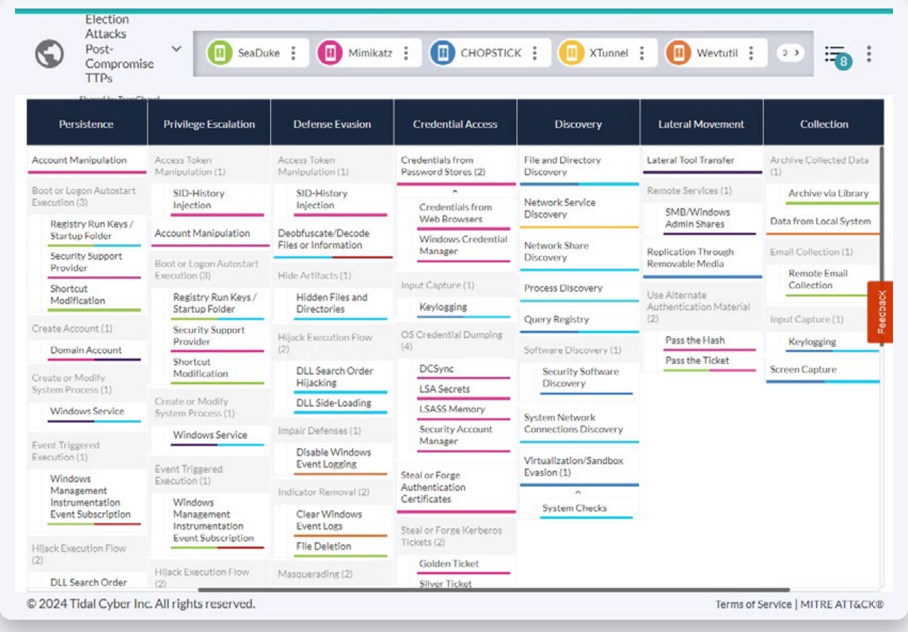
COMMON POST-COMPROMISE TTPS

With all the nuance and evolution around election-related social engineering & identity-based techniques, it can be easy to forget that these represent just the initial means of adversary network access. Actors can then use a huge range of potential post-compromise TTPs to achieve various goals, including data collection, exfiltration, tampering, network disruption, and more. (In ATT&CK terms, there are still 11 (of 14) Tactics and more than 500 (of 625) Techniques & Sub-Techniques after the Initial Access phase!)

In order to grant some focus, we've provided a roundup of known TTPs associated with two prominent election-related social engineering attacks (and the tools & malware used during them) – the 2015-16 DNC attacks and 2016 attacks on media in Hong Kong – in *this collection*.

ELECTION-RELATED WEB APPLICATIONS

Primary Targets: Election-related websites (voter/voting information and poll/turnout results), campaign websites, voting infrastructure (rare)



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Account Manipulation	Access Token Manipulation (1)	Access Token Manipulation (1)	Credentials from Password Stores (2)	File and Directory Discovery	Lateral Tool Transfer	Archive Collected Data (1)
Boot or Logon Autostart Execution (3)	SID-History Injection	SID-History Injection	^	Network Service Discovery	Remote Services (1)	Archive via Library
Registry Run Keys / Startup Folder	Account Manipulation	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	Network Share Discovery	SMB/Windows Admin Shares	Data from Local System
Security Support Provider	Boot or Logon Autostart Execution (3)	Hide Artifacts (1)	Windows Credential Manager	Process Discovery	Replication Through Removable Media	Email Collection (1)
Shortcut Modification	Registry Run Keys / Startup Folder	Hidden Files and Directories	Input Capture (1)	Query Registry	Use Alternate Authentication Material (2)	Remote Email Collection
Create Account (1)	Security Support Provider	Hijack Execution Flow (2)	Keylogging	Software Discovery (1)	Pass the Hash	Input Capture (1)
Domain Account	Shortcut Modification	DLL Search Order Hijacking	OS Credential Dumping (4)	Security Software Discovery	Pass the Ticket	Keylogging
Create or Modify System Process (1)	Create or Modify System Process (1)	DLL Side-Loading	DCSync	System Network Connections Discovery		Screen Capture
Windows Service	Windows Service	Impair Defenses (1)	LSA Secrets	Virtualization/Sandbox Evasion (1)		
Event Triggered Execution (1)	Event Triggered Execution (1)	Disable Windows Event Logging	LSASS Memory	^		
Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription	Indicator Removal (2)	Security Account Manager	System Checks		
Hijack Execution Flow (2)	Hijack Execution Flow (2)	Clear Windows Event Logs	Steal or Forge Authentication Certificates			
DLL Search Order		File Deletion	Steal or Forge Kerberos Tickets (2)			
		Masquerading (2)	Golden Ticket			
			Silver Ticket			

© 2024 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®

Figure 5: A collection of TTPs from two prominent election-related social engineering attacks – the 2015-16 DNC attacks and 2016 attacks on media in Hong Kong.

DATA ACCESS / EXFILTRATION / TAMPERING ATTACKS

Notable Examples:

- **October 2014:** Four days before national elections, hacktivists with suspected ties to **APT28 (Russia)** *compromised Ukraine's central election system*, deleting critical files that temporarily rendered vote-counting features inoperable and installing malware apparently designed to change vote tallies. Exfiltrated data was also released online.

- **2016:** Leading up to national elections, **Russian military intelligence actors** *repeatedly performed vulnerability scans* on the websites & voter registration systems associated with dozens of U.S. states and various municipalities. In some instances, actors *exploited identified Structured Query Language injection (SQLi) vulnerabilities* to access and exfiltrate thousands of voter registration records. Investigators *determined* that actors "were in a position to delete or change voter data", although no evidence indicated that they did.

- **2020:** Unspecified **"Iranian hackers"** *compromised a system* used by a U.S. municipal government to publish election results.

- **September 2020: Unspecified Iranian advanced persistent threat actors** scanned election-related U.S. state websites for vulnerabilities and used directory traversal and SQL injection exploits and web shells to *collect and exfiltrate voter data*, using the stolen information to widely disseminate intimidating and misleading emails to U.S. citizens.

- **2022:** The *joint report* on foreign interference related to 2022 U.S. federal elections indicated unspecified **Russian, Iranian,** and **Chinese government-affiliated actors** "connected to campaign infrastructure" around the federal elections, in some cases carrying out "[broad] scanning" ahead of the attacks and resulting in access to "some components" of that infrastructure.

The prominence of social engineering & identity attacks can make it easy to forget that technical-based compromise of election infrastructure can and does continue to occur, including recently. Many web application access cases appear to be relatively opportunistic in nature, but the *continued presence of vulnerabilities* & misconfigurations in these applications give interference adversaries ample opportunity to compromise intended targets. *Recent CISA advisories* highlight potential post-compromise TTPs for data access. When visibility into application logs isn't strong, the fact that these attacks also do not require user interaction can allow them to fly largely under defenders' radars, and they therefore represent a continually appealing attack vector for data access or potentially even manipulation purposes.

DEFACEMENT ATTACKS

Notable Examples:

- **October 1999:** The website of a U.S. presidential campaign was *compromised and defaced*.
- **October 2020:** Attackers *compromised the campaign website* of a U.S. presidential candidate, defacing pages to promote an apparent cryptocurrency scam.
  - A *2021 ICA* highlights an attack of this type around this time, noting the actors probably achieved website access using administrative credentials.
- **November 2020:** Actors promoting Turkish nationalist themes *compromised and defaced* a website linked to a U.S. presidential candidate.
- **November 2022:** Bahrain's government *blamed* Iran for *apparent DoS and defacement attacks* against government websites during parliamentary and local elections

Initial access TTPs for defacement attacks can be similar to the previous attack method, but since they are carried out for different goals, *post-compromise TTPs* for these attacks will typically differ considerably. The *resurgence* of *politically motivated defacement* & disruption attacks in *recent months* is cause for concern that these actors may turn their attention towards elections in attempts to impact parties they oppose. This trend will be covered more in the next section.

DENIAL OF SERVICE

Notable Examples:

- **May 2014:** *Denial of service ("DoS") attacks on a management software web platform* used by political campaigns rendered multiple U.S. primary candidates' websites inaccessible shortly before voting took place.
- **October 2014:** After the conclusion of voting in national elections, a *distributed denial of service ("DDoS") attack on Ukraine's Central Election Commission website* rendered the site inaccessible.
- **October 2015:** A *DoS attack targeted the websites of Bulgaria's electoral commission*, presidency, and other institutions on the day of national referendum and local elections. The president *suggested* that **APT28 (Russia)** was behind the attack.

- **October 2016:** A *DDoS attack, linked by a security analyst to APT28, took Montenegro's national government web portal and other websites offline* on national election day.
- **May 2017:** Malta's government IT systems allegedly experienced a *40% increase in phishing, DDoS and malware-based attacks*, attributed to **APT28**, in the month before the country's general election.
- **April 2019:** A web service used to publish voting results in Finland suffered a DoS attack days before national elections.
- **January 2021:** An online voting event to elect the leadership of Germany's leading political party was *targeted by a DDoS attack*. The attack caused a live stream of the event to be taken down but did not disrupt the voting process, which relied on a distinct computer server.
- **2022:** According to the *joint report* on foreign interference related to 2022 U.S. federal elections, "**Pro-Russian hacktivists** claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website".
- **November 2022:** Bahrain's government *blamed* **Iran** for *apparent DoS and defacement attacks* against government websites during parliamentary and local elections.

Like phishing attacks, the evidence shows that *DoS/DDoS* have been a mainstay election interference threat for many years. By their nature, these attacks require no pre-existing target compromise or interaction from their intended victims, making them a readily available attack method for interference actors.

The 2021 case in Germany highlights the most concerning potential impact of an election-timed DoS attack, where actual voting would be disrupted (in this case, the voting system was hosted on a separate server, and online voting in high-level elections is rare). But DoS attacks can have considerable secondary impacts, being used as fuel for influence operations. Actual or even perceived/alleged disruption to voting processes, including availability of voting information or the posting of election results, enable influence actors to question the integrity of elections and their outcomes.

The extensive history of election-related DoS attacks means *considerable focus* is placed on defending against them. But, like with defacement attacks, *considerable numbers* of recent cases of *politically motivated DoS attacks* have been observed. Some examples are perpetrated by *groups aligned with* or possibly even supported by known election interference adversary countries, while *others* have affected countries that previously saw election-timed DoS activity. These methods are clearly a ready tool in actors' arsenals for attacking targets that don't align with their ideologies and therefore represent a threat to watch throughout this year's election cycles.

VOTING INFRASTRUCTURE & INSIDER THREATS

Primary Targets: Voting machines or online voting platforms/services. Most other targets referenced in other sections could also represent targets for insiders, but additional concern is placed on election administration teams (workers and/or volunteers) and voting infrastructure since an insider here would ostensibly have the greatest opportunity to directly interfere with voting outcomes

Notable Examples:

- **2016: Russian military intelligence actors** targeted employees of a U.S. manufacturer of voting technology used by numerous U.S. counties, *compromising the company's network* and installing malware in an apparent attempt to collect sensitive information. The actors are believed to have used data harvested in the operation to support a subsequent *voter registration-themed spearphishing campaign targeting local government entities*.
- **2020:** Officials, including a political candidate, allegedly *convinced local clerks to provide unauthorized access to voting tally machines* in an attempt to dispute the 2020 presidential election result.
- **January 2021:** A group allegedly attempted to *gain unauthorized access to voting machines* in a Georgia municipality in an effort to copy machine software and data in opposition to the 2020 presidential election result.
- **January 2021:** An online voting event to elect the leadership of Germany's leading political party was *targeted by a DDoS attack*. The attack caused a live stream of the event to be taken down but did not disrupt the voting process, which relied on a distinct computer server.
- **May 2021:** A Coloroda county clerk two others employed by the official's office allegedly *facilitated unauthorized access to voting machines in an effort to copy the devices' hard drives* and dispute the 2020 presidential election result.

Attacks involving voting infrastructure represent high-profile concerns because of the serious impact they could have: direct manipulation or disruption of voting and/or vote results. Fortunately, there aren't many public examples of these attacks, although the series of cases stemming from 2020 U.S. presidential elections are certainly worrisome and demonstrate that *insider threats* are more than hypothetical hazards. The first instance above is also notable as an example of a *supply chain attack*, underscoring the importance of not only first-party protection for organizations responsible for voting infrastructure, but also visibility into and due diligence around external parties as well.

RANSOMWARE

Primary Targets: Computer networks supporting most of the other targets referenced in other sections, such as voting administration offices, political staff and campaign teams, and infrastructure and hardware/software suppliers

Notable Examples:

- **October 2020:** A *ransomware attack* temporarily rendered election-related "infrastructure" in a Georgia (U.S.) county inaccessible.
- **October 2020:** Actors *encrypted* 300 computers and 22 servers on the network of a New York county with **"Ragnarok" ransomware**, preventing the county from connecting to a state voter registration system.
- **September 2023:** A ransomware attack *interrupted the poll worker training process* ahead of state general elections in Mississippi.
- **October 2023:** The District of Columbia Board of Elections suffered an apparent ransomware attack. The **RansomedVC** *group claimed responsibility for the attack* and offered data (voter registration records) allegedly exfiltrated during the attack for sale via its dark web data leak site. Authorities temporarily took down the contents of the organization's website while responding to the incident.

We assess that ransomware and extortion operations represent a serious threat to organizations in most sectors globally, with few exceptions. The cases above show that election administration and other election-related entities are not immune to these *near-indiscriminate* threats, where access to systems seized during a ransomware attack has delayed and disrupted election activities. While global ransomware victim counts have *ebbed and flowed* in recent years, the incredibly high overall level and wide targeting of ransomware activity makes this threat a noteworthy security concern for most organizations, including election-related entities.

Some of the reports above note that election organizations might not have been intentionally targeted by ransomware operators. But for defenders seeking to prioritize among the myriad TTPs used by the many ransom & extortion actors active today (Tidal tracks around 100 from the previous two years, but many more certainly exist), some additional, data-driven focus can be helpful. *Figure 6* highlights 14 operations that appear to pose a disproportionate threat to state, local, and federal government entities, and links are provided to TTP collections for each group. Readers are also encouraged to consult Tidal's popular *Ransomware & Data Extortion Landscape TTP matrix*, which provides a large number of ATT&CK-mapped TTPs associated with 40+ of the most prominent groups from recent years, most of which are not yet tracked in the formal ATT&CK knowledge base.

Ransomware/ Extortion Operation	Victims in "Government Administration", 2021-24	Total Claimed Victims, 2021-24	Associated ATT&CK Techniques
BlackSuit	5	24%	*7*
Pysa	23	7%	*16*
Rhysida	6	7%	*24*
Everest	10	7%	*14*
Cuba	7	7%	*23*
Vice Society	11	6%	*14*
NoEscape	6	5%	*21*
Medusa	7	4%	*8*
LockBit	85	3%	*33*
Royal	6	3%	*13*
ALPHV/BlackCat	15	2%	*17*
Play	6	2%	*15*
BianLian	6	2%	*39*
Cl0p	9	1%	*17*

Figure 6: Select ransomware & extortion operations that claimed especially high numbers of victims in the "government administration" sector in absolute terms, and relative to their total (alleged) victim tally over the past 3+ years. Victim claims sourced from the ransomwatch project, with automatic sector enrichment performed by Tidal Cyber.

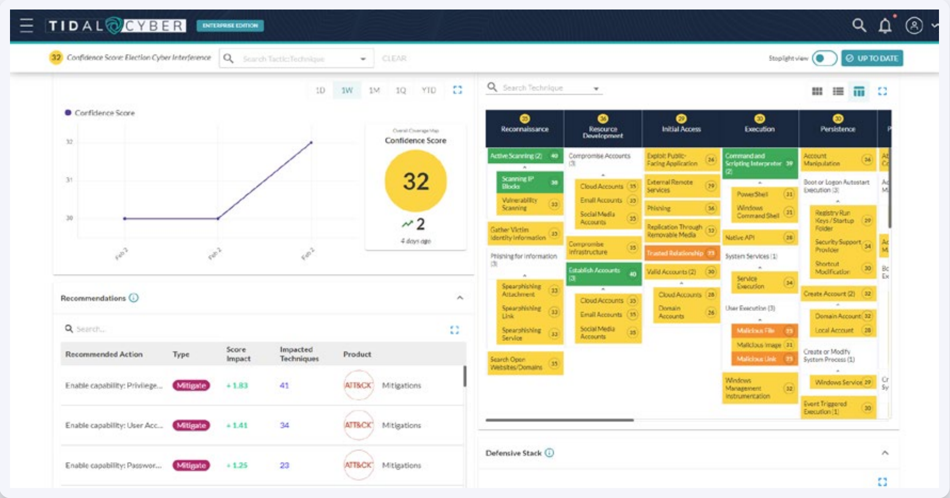
The recent D.C. Board of Elections case demonstrates that ransomware impacts to election organizations extend beyond just encryption of files & systems. Many of today's leading extortion groups use a mix of encryption-focused attacks and data exfiltration TTPs, with some groups now *shifting entirely* to the latter. As *Figure 1* highlighted, leaked data serves as important fuel for influence actors, even those that might not be involved in underlying interference operations.

PRIORITIZED GUIDANCE FOR DEFENDERS

As proponents of *threat-informed defense*, after we identified top-priority adversaries and collected the attack methods & specific TTPs they are most likely to use for election interference, we naturally sought to use this intelligence to drive optimized defensive outcomes. The MITRE ATT&CK® knowledge base unlocks *alignment opportunities* between discrete adversary behaviors and the range of defensive capabilities within an organization's defensive stack. The collection of threats & TTPs discussed earlier in the report can then be used to prioritize which of those behaviors – and therefore which relevant defensive resources – defenders at election-related organizations should consider first, to most effectively combat the interference threats they are facing.

Appendix III provides the full set of prioritized defensive recommendations we surfaced, and highlights are provided just below. We built a "Threat Profile" consisting of ATT&CK-aligned TTPs across the eight interference attack methods described above (versions of those collections in our free Community tool are provided *here*). We then aligned these threats & their TTPs with three popular security control-related resources & frameworks – the *MITRE ATT&CK Mitigations*, *NIST 800-53 Revision 5*, and the *Center for Internet Security ("CIS") Controls version 8.0* – using Tidal's *Enterprise Edition* to streamline surfacing which controls applied to the most common and most important techniques from the Election Cyber Interference Profile.

In total, the Profile comprised 182 ATT&CK Techniques & Sub-Techniques used across the eight interference attack methods – *nearly 30% of the entire ATT&CK knowledge base*. Clearly, that represents many attacker behaviors for defenders to consider all at once, underscoring the need for prioritization. Defenders will ideally consider the unique modeling of their own defensive stack's capabilities as it aligns with relevant adversary behaviors to give the most accurate picture of defensive coverage and potential gaps to close.



Recommended Action	Type	Score Impact	Impacted Techniques	Product
Enable capability: Privilege...	Mitigate	+ 1.83	41	ATT&CK Mitigations
Enable capability: User Acc...	Mitigate	+ 1.41	34	ATT&CK Mitigations
Enable capability: Passwor...	Mitigate	+ 1.25	23	ATT&CK Mitigations

Figure 7: A summary of the alignment of the Election Cyber Interference Threat Profile with popular security control frameworks in Tidal's Enterprise Edition. Full results are provided in Appendix III and a summary of those results is shared in this section.

DEFENSIVE GUIDANCE HIGHLIGHTS

Seasoned security professionals will recognize that many of the recommendations below are not novel (consult resources like CISA's *advisory feed* for many past examples). And indeed, steps such as ensuring access controls, inventorying and patching assets, and backing up sensitive data remain essential measures that the large majority of organizations should seek to implement.

But as adversaries *continue to evolve* and do so with *increasing regularity*, continual *reassessment and review* of even "baseline" controls becomes a necessity to account for assets, systems, or users where visibility or control might have drifted as a matter of regular business, technological, or security control change. Our methodology emphasizes which areas should be prioritized for those regular reassessments and reviews, in terms of which reinforcements can have the greatest (positive) defensive effects. Tying defensive reinforcements to specific priority threats or TTPs can also help nudge forward improvements among many other potential competing business & security priorities.

The top election cyber interference defensive guidance fell into a few key thematic areas:

- **User-focused security controls** (multi-factor authentication, account & privilege management, strong password policies, and user training) are overwhelmingly top recommendations, addressing the key initial access vectors for many of the attack methods. **Defenders should prioritize regular review & reinforcement of these controls**, especially as relevant adversaries continue to evolve their TTPs to evade the latest defenses.

- **Software & application secure configuration policies** help address disruptive techniques used for denial of service, defacement, and data tampering. **Software updates** – and especially **timely inventories** of software products & other assets – are critical for ensuring configurations and updates are applied widely as intended.

- **Endpoint & network threat prevention technology** can help address a wide range of observed post-compromise techniques used for privilege escalation, lateral movement, and sensitive data collection.

- **Data backup** and other controls for especially **sensitive & critical information** are other important controls, although these controls map to a relatively smaller number of techniques, including ones less commonly observed in *targeted* election cyber interference attacks.

APPENDIX I:

MEASURING ELECTION CYBER INTERFERENCE THREATS: METHODOLOGY & COMPLETE RANKINGS

The list of countries we consulted for this study was sourced from *here*. Only countries with at least one relevant data point (e.g. at least one adversary aligned with one of the priority adversary countries) appear in our results table below.

Tidal enriched the list with the following key metadata points sourced from our free *Community Edition* knowledge base. If you are a defender or researcher who could benefit from API access to this data, please *let us know*.

- **Relevant Adversaries Observed:** A tally of the adversary groups observed carrying out cyber activity against victims in the specified country. The data here only focuses on **nation-state-backed adversary groups**, specifically ones attributed to the following countries. This tally is used as proxy measures for the overall level of potential of foreign cyber interference a country might be facing.
- **Adversary Attribution Countries:** Cyber adversaries with observed activity that high-confidence public reporting attributes to a particular nation-state. We focused on the three greatest offenders of election cyber interference attacks – Russia, China, and Iran. We also included North Korea only when a victim country faced *Kimsuky*, another group known to carry out election-related interference attacks (other North Korea-backed actors have carried out high levels of non-election-related activity in many countries globally, which clouded the results).
- **Priority Threats:** In an effort to place added emphasis on countries where known election cyber interference actors had been observed, we took an additional specific tally of observed activity from groups in *this Tidal-curated list*, referenced throughout this report.

After the adversary group, priority adversary, and adversarial country data was compiled, we sorted the list high-to-low in the following sequence: Relevant Adversaries Observed, Adversary Attribution Countries, Priority Threats. We banded this ranked list into three tiers, according to the following criteria:

- **Highest:** Countries facing state-backed groups associated with multiple priority adversary nations, including multiple priority groups specifically. These countries also typically face many state-backed groups associated with the priority adversary countries generally.*
- **Significant:** Countries facing at least one priority adversary group and/or state-backed actors associated with multiple priority adversary nations.
- **Elevated:** Countries facing at least one state-backed actor associated with one priority adversary nation. We used this metric as a general approximation of potential foreign cyber interference for the country's 2024 election and consider this as a "watch list" of additional countries worth keeping a closer eye on this year.

*Four countries – Indonesia, Taiwan, Romania, and Venezuela – received manual bumps into higher tiers since they all faced relatively high levels of priority adversaries, threats from multiple adversarial nations and/or high levels of state-backed adversary activity generally, even though other factor(s) fell short of the higher threshold.

The Freedom House *Election Vulnerability Index* "Digital Sphere" metric is provided for an additional (and very helpful) point of additional context, but these metrics were not structurally incorporated into our threat-focused rankings.

Country	Election Date	Relevant Adversaries Observed	Adversary Attribution Countries	Count of Adversarial Countries	Priority Threats	Priority Threat Tally	Freedom House Election Vulnerability Index "Digital Sphere" Score (Max = 32)	Relative Threat Level
United States	November 5	51	China, Iran, Russia, North Korea	4	APT28, APT29, APT3, APT41, Kimsuky, Leviathan, Magic Hound, ZIRCONIUM	8	21	Highest
United Kingdom	TBD	24	China, Iran, Russia, North Korea	4	APT28, APT29, APT3, APT41, Kimsuky, Leviathan, Magic Hound	7		Highest
South Korea	April 10	20	China, Iran, Russia, North Korea	4	APT28, APT29, APT41, Kimsuky	4	19	Highest
India	TBD	20	China, Iran, Russia	3	APT28, APT29, APT41	3	14	Highest
Belgium	June 9	11	China, Russia	2	APT28, APT29, APT3, Leviathan	4		Highest
Pakistan	February 8	10	China, Iran, Russia	3	APT28, APT41, Magic Hound	3	8	Highest
Belarus	February 25	8	China, Iran, Russia	3	APT28, APT29, ZIRCONIUM	3	14	Highest

Country	Election Date	Relevant Adversaries Observed	Adversary Attribution Countries	Count of Adversarial Countries	Priority Threats	Priority Threat Tally	Freedom House Election Vulnerability Index “Digital Sphere” Score (Max = 32)	Relative Threat Level
Mexico	June 2	7	China, Iran, Russia	3	APT28, APT29, APT41	3	17	Highest
Georgia	TBD	7	China, Iran, Russia	3	APT28, APT29, APT41	3	26	Highest
Indonesia	February 14	10	China, Russia	2	APT41	1	13	Highest
Russia	March 15	17	China, Iran, North Korea	3	Kimsuky, ZIRCONIUM	2	4	Highest
Taiwan	January 13	17	China	1	APT41	1	21	Highest
South Africa	May 1	8	China, Iran, Russia	3	APT28, APT41	2	26	Highest
Finland	January 28	5	China, Iran, Russia	3	APT41, ZIRCONIUM	2		Highest
Azerbaijan	February 7	6	Iran, Russia	2	APT28, APT29	2		Highest
Mongolia	June 28	6	China, Russia	2	APT28, ZIRCONIUM	2		Highest
Uzbekistan	TBD	5	China, Russia	2	APT28, APT29	2	12	Highest
Slovakia	March 23	3	China, Russia	2	APT28, APT29	2		Highest
Romania	TBD	5	Russia	1	APT28, APT29	2		Highest
Venezuela	TBD	3	China, Iran, Russia	3	Magic Hound	1	7	Highest
Iran	March 1	9	China, Russia	2	APT28	1	0	Significant
Lebanon	TBD	5	Iran, Russia	2	APT29	1	19	Significant
Austria	TBD	5	Iran, Russia	2	APT29	1		Significant
Portugal	March 10	4	China, Russia	2	APT29	1		Significant
Croatia	TBD	3	China, Russia	2	APT28	1		Significant
Ireland	March 8	2	Iran, Russia	2	APT29	1		Significant
Cambodia	February 25	4	China	1	LEVIATHAN	1		Significant
Lithuania	May 12	3	Russia	1	APT29	1		Significant
Bangladesh	January 7	2	China, Russia	2		0	11	Significant
Nepal	January 25	3	China	1		0		Elevated
Bhutan	January 9	1	China	1		0		Elevated
El Salvador	February 4	1	China	1		0	24	Elevated
Panama	May 5	1	China	1		0		Elevated
Dominican Republic	May 19	1	China	1		0		Elevated
Ethiopia	October 1	1	China	1		0	11	Elevated
Uruguay	October 27	1	Russia	1		0		Elevated
Mauritius	November 1	1	Iran	1		0		Elevated
Moldova	TBD	1	Russia	1		0	22	Elevated
Algeria	TBD	1	Russia	1		0		Elevated
Botswana	TBD	1	Russia	1		0		Elevated
South Sudan	TBD	1	China	1		0		Elevated

APPENDIX II:
ELECTION INTERFERENCE ATTACKS BY ADVERSARY

We compiled this extensive (but certainly not exhaustive) list through research across a wide range of public sources. This *2020 Australian Strategic Policy Institute study & interactive resource* provides a phenomenal collection of interference (as well as influence) operations up until that time.

RUSSIA

UNSPECIFIED

- **2016:** Leading up to national elections, **Russian military intelligence actors** *repeatedly performed vulnerability scans* on the websites & voter registration systems associated with dozens of U.S. states and various municipalities. In some instances, actors *exploited identified Structured Query Language injection (SQLi) vulnerabilities* to access and exfiltrate thousands of voter registration records. Investigators *determined* that actors "were in a position to delete or change voter data", although no evidence indicated that they did.

- **2016: Russian military intelligence actors** targeted employees of a U.S. manufacturer of voting technology used by numerous U.S. counties, *compromising the company's network* and installing malware in an apparent attempt to collect sensitive information. The actors are believed to have used data harvested in the operation to support a subsequent *voter registration-themed spearphishing campaign targeting local government entities*.

- **November 2016: Russian military intelligence actors** sent spearphishing emails with malicious attachments to Florida election administrators, "*[gaining] access* to the network of at least one Florida county government".

- **2022:** According to the *joint report* on foreign interference related to 2022 U.S. federal elections, "Pro-Russian hacktivists claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website".

- **2022:** The *joint report* on foreign interference related to 2022 U.S. federal elections indicated unspecified **Russian, Iranian,** and **Chinese government-affiliated actors** "connected to campaign infrastructure" around the federal elections, in some cases carrying out "[broad] scanning" ahead of the attacks and resulting in access to "some components" of that infrastructure.

APT28

- **October 2014:** Four days before national elections, hacktivist attackers with suspected ties to **APT28** *compromised Ukraine's central election system*, deleting critical files that temporarily rendered vote-counting features inoperable and installing malware apparently designed to change vote tallies. Exfiltrated data was also released online. A DDoS attack on the Central Election Commission website after the conclusion of voting also rendered the site inaccessible.
- **October 2015:** A *denial of service ("DoS") attack targeted the websites of Bulgaria's electoral commission*, presidency, and other institutions on the day of national referendum and local elections. The president *suggested* that **APT28** was behind the attack.
- 2015-2016: Actors, attributed to **APT28 & APT29,** compromised the network of the U.S. Democratic National Committee ("DNC") ahead of national elections. Responders *suspect initial access was gained via spearphishing emails*.
- **March 2016:** U.S. presidential campaign chair's *personal email compromised via a credential harvesting-focused spearphishing attack* attributed to **APT28.**
- October 2016: A *distributed denial of service attack ("DDoS") attack, linked by a security analyst to APT28, took Montenegro's national government web portal and other websites offline* on national election day.
- **2017: APT28** compromised the professional & personal accounts of French presidential campaign staff via *credential harvesting-focused spearphishing attacks*. 9GB worth of data was leaked.
- **May 2017:** Malta's government IT systems allegedly experienced a *40% increase in phishing, DDoS and malware-based attacks*, attributed to **APT28,** in the month before the country's general election
- **August 2017:** Staffers supporting a U.S. Senator running for re-election in 2018 midterms received *credential harvesting-focused spearphishing emails* attributed to **APT28.**

- **September 2019-September 2020: APT28 (Russia)** appeared to *"evolve" its approach to targeting election-related personnel*, carrying out a massive brute force and password spray campaign directed at targets including unspecified U.S. and UK organizations "directly involved in political elections" and NGOs working on issues like *election integrity*. Attacks featured *special IP address anonymization tooling* to persistently evade detection.

APT29

- **2015-2016:** Actors, attributed to **APT28 & APT29,** compromised the network of the U.S. Democratic National Committee ahead of national elections. Responders *suspect initial access was gained via spearphishing emails*.
- **May 2021:** Suspected **APT29 (Russia)** actors used a *legitimate mass-emailing service to conduct a wide-ranging phishing campaign* that used election-fraud-related lures.

IRAN

UNSPECIFIED

- **2020:** Unspecified **"Iranian hackers"** *compromised a system* used by a U.S. municipal government to publish election results
- **September 2020: Unspecified Iranian advanced persistent threat actors** scanned election-related U.S. state websites for vulnerabilities and used directory traversal and SQL injection exploits and web shells to *collect and exfiltrate voter data*, using the stolen information to widely dissemination intimidating and misleading emails to U.S. citizens.
- **November 2022:** Bahrain's government *blamed* **Iran** for *apparent DoS and defacement attacks* against government websites during parliamentary and local elections.
- **2022:** The *joint report* on foreign interference related to 2022 U.S. federal elections indicated unspecified **Russian, Iranian,** and **Chinese government-affiliated actors** "connected to campaign infrastructure" around the federal elections, in some cases carrying out "[broad] scanning" ahead of the attacks and resulting in access to "some components" of that infrastructure.

MAGIC HOUND

- **August-September 2019:** Researchers observed **Magic Hound** actors attempting to *abuse password reset and account recovery features* to access email accounts associated with a U.S. presidential campaign and other political and media targets, often using extensive amounts of previously collected personal information and or previously compromised secondary email accounts to support these attacks.

- **2020: Magic Hound** and **ZIRCONIUM (China)** targeted the personal and *work email accounts* of U.S. presidential campaign staffers with *credential harvesting- and information gathering-focused phishing emails*.

CHINA

UNSPECIFIED

- **2008:** U.S. presidential campaign staff targeted with *malicious spearphishing email attachments* attributed to **unspecified Chinese espionage actors.**

- **2022:** The *joint report* on foreign interference related to 2022 U.S. federal elections indicated unspecified **Russian, Iranian,** and **Chinese government-affiliated actors** "connected to campaign infrastructure" around the federal elections, in some cases carrying out "[broad] scanning" ahead of the attacks and resulting in access to "some components" of that infrastructure.

ZIRCONIUM (AKA APT31)

- **2020: Magic Hound** and **ZIRCONIUM (China)** targeted the personal and *work email accounts* of U.S. presidential campaign staffers with *credential harvesting- and information gathering-focused phishing emails*.

APT41

- **July & August 2016:** Ahead of legislative elections, media representatives in Hong Kong received *spearphishing emails intended to deliver malware*, in a campaign attributed to **APT41.**

- This group has also been observed carrying out *multiple campaigns targeting U.S. state governments* in 2021, including attacks that involved exploits of vulnerabilities in web-facing applications and *others* targeting U.S. Covid relief benefits.

LEVIATHAN (AKA TEMP.PERISCOPE)

- **2018: TEMP.Periscope actors** perpetrated a *broad series of malware-based compromises* of election-related entities & individuals in Cambodia ahead of the country's July 2018 elections, including the National Election Commission, a politician, human rights groups, and media entities. In at least one case, initial access was achieved via a phishing email containing a link to download malware.

APT3

- **August 2016:** Actors attributed to **APT3** carried out at least *three spearphishing attacks targeting two government agencies* in Hong Kong in the month ahead of legislative elections.

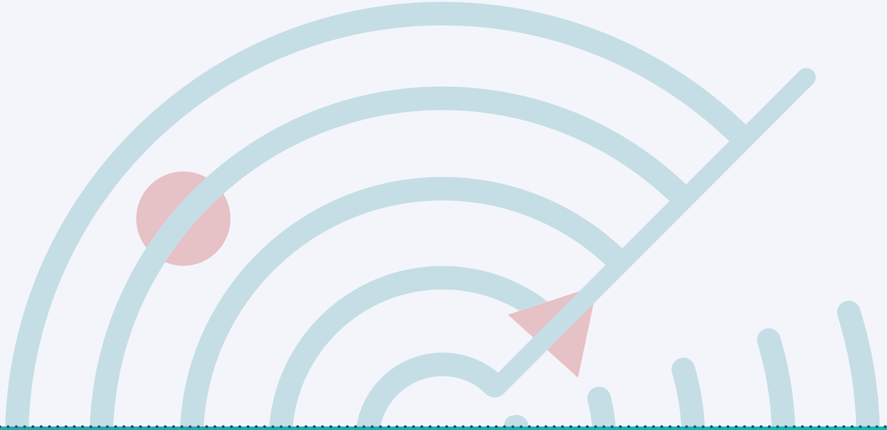
NORTH KOREA

UNSPECIFIED

- **2020:** *Reports indicated* that **unspecified North Korea-aligned actors** carried out phishing attacks targeting organizations supporting U.S. presidential candidates.

KIMSUKY

- **April 2020:** Suspected **Kimsuky actors** attempted to *deliver malware to select targets using phishing lures* designed as identifying North Korean citizens running in South Korea's legislative elections that month.
- **November 2020: Kimsuky actors** sent *phishing lures* likely targeting users in South Korea that claimed to predict the outcome of the U.S. national election.



Category	Mitigation (ATT&CK Name & ID)	Related Election Interference Techniques	Related Interference Methods (of 8)	*D3FEND* Countermeasures	Top-Mapped NIST 800-53 Controls	Top-Mapped CIS Control Safeguards
User-Focused Controls	Multi-factor Authentication (M1032)	24	6	163	AC-3, SI-4, CM-6, AC-6, AC-2, IA-2, AC-5, CM-2, CM-5, CA-7	6.1, 6.2, 6.8, 4.1, 4.7, 5.4, 5.3, 18.3, 18.5, 3.3
	User Account Management (M1018)	35	5	244		
	User Training (M1017)	32	5	191		
	Password Policies (M1027)	23	5	202		
	Account Use Policies (M1036)	10	5	39		
	Privileged Account Management (M1026)	41	4	373		
	Active Directory Configuration (M1015)	15	4	47		
	Restrict File and Directory Permissions (M1022)	14	4	128		
	Restrict Web-Based Content (M1021)	11	4	143		
Endpoint- & Network-Focused Controls	Network Intrusion Prevention (M1031)	24	5	294	SI-4, CM-6, CM-7, CM-2, SI-3, AC-3, SC-7, CA-7, AC-6, AC-4	4.1, 18.3, 18.5, 2.5, 6.2, 6.1, 6.8, 4.8, 13.8, 13.3
	Network Segmentation (M1030)	15	5	146		
	Behavior Prevention on Endpoint (M1040)	19	4	99		
	Execution Prevention (M1038)	19	4	219		
	Operating System Configuration (M1028)	17	4	132		
	Disable or Remove Feature or Program (M1042)	17	4	201		
	Filter Network Traffic (M1037)	17	4	120		
Inventory & Secure Software	Audit (M1047)	24	5	175	CM-6, SI-4, AC-6, CM-2, AC-3, AC-2, IA-2, RA-5, AC-5, SI-7	18.3, 18.5, 4.1, 6.1, 6.2, 6.8, 4.7, 5.3, 5.4, 7.2
	Update Software (M1051)	9	5	114		
	Application Developer Guidance (M1013)	8	4	3		
	Software Configuration (M1054)	7	3	96		
	Vulnerability Scanning (M1016)	2	3	29		
Secure Sensitive & Critical Information	Encrypt Sensitive Information (M1041)	9	3	60	SI-4, CM-2, AC-3, AC-16, SI-7, SI-3, CM-6, SI-12, AC-6, AC-17	3.10, 4.1, 11.3, 18.3, 18.5, 3.12, 12.8, 6.8, 3.11, 4.2
	Data Backup (M1053)	6	3	2		
	Data Loss Prevention (M1057)	5	2	1		

APPENDIX III:

ELECTION CYBER INTERFERENCE THREAT PROFILE & DEFENSIVE GUIDANCE RESULTS

Using Tidal's *Enterprise Edition*, we built a Threat Profile consisting of the ATT&CK techniques associated with each of the interference attack methods discussed above (versions of these collections can be found in Tidal's free *Community Edition* at the links provided *here*) and aligned it with popular security control-related resources and frameworks. The results are summarized *above* and provided in greater detail here.

The top results (*ATT&CK Mitigations*) – organized into higher-level Categories and aligned with relevant controls from *NIST 800-53 Revision 5* and *CIS Controls version 8* – are provided in this table. A list of remaining Mitigations and tallies of relevant aligned Techniques are provided in a final bulleted list farther down.

Additional results:

- **Pre-compromise (M1056):** 25 Techniques
- **Antivirus/Antimalware (M1049):** 9 Techniques
- **Code Signing (M1045):** 7 Techniques
- **Restrict Registry Permissions (M1024):** 5 Techniques
- **User Account Control (M1052):** 4 Techniques
- **Limit Access to Resource Over Network (M1035):** 4 Techniques
- **Limit Hardware Installation (M1034):** 4 Techniques
- **Privileged Process Integrity (M1025):** 3 Techniques
- **Restrict Library Loading (M1044):** 3 Techniques
- **Remote Data Storage (M1029):** 3 Techniques
- **SSL/TLS Inspection (M1020):** 3 Techniques
- **Exploit Protection (M1050):** 2 Techniques
- **Application Isolation and Sandboxing (M1048):** 2 Techniques
- **Credential Access Protection (M1043):** 1 Techniques
- **Threat Intelligence Program (M1019):** 1 Techniques

APPENDIX IV:

ADVERSARY & TTP RESOURCE ROUNDUP

Below is a central collection of the key resources from Tidal's free *Community Edition* that were referenced throughout this report. While there is a lot to digest, the central *threat-informed defense workflow* is similar for each of these threats. Pivot from threat intelligence into associated techniques and onward into relevant defensive resources, or overlay entire sets of capabilities from your own defensive stack to identify threat overlaps & potential gaps.

ELECTION INTERFERENCE ATTACK METHODS: TECHNIQUE COLLECTIONS

Collections of ATT&CK Techniques discussed in the *Key Cyber Interference Attack Methods* section, hosted in Tidal's free *Community Edition*. These sets of Techniques drove the prioritized guidance provided in the report via analysis performed in Tidal's *Enterprise Edition*.

1. *Email & Social Engineering TTPs*
2. *Identity-Based Attacks*
3. *Social Engineering & Identity Attack Post-Compromise TTPs*
4. *Election Interference Web App Attacks*
5. *Defacement Attack Techniques*
6. *Denial-of-Service Techniques*
7. *Insider Threat Knowledge Base - Heatmap*
8. Common Ransomware Techniques: *Ransomware & Data Extortion Landscape*

GROUPS

Searchable list of all groups in Tidal's knowledge base: *https://app.tidalcyber.com/groups*

ANONYMOUS SUDAN

https://app.tidalcyber.com/groups/132feaeb-a9a1-4ecc-b7e9-86c008c15218

APT28

https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5

APT29

https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447

APT3

https://app.tidalcyber.com/groups/9da726e6-af02-49b8-8ebe-7ea4235513c9

APT41

https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9

CYBERAV3NGERS

https://app.tidalcyber.com/groups/44a9c8ac-c287-45d2-9ebc-2c8a7d0a1f57

KILLNET

https://app.tidalcyber.com/groups/35fb7663-5c5d-43fe-a507-49612aa7960e

KIMSUKY

https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1

LEVIATHAN (AKA TEMP.PERISCOPE)

https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871

MAGIC HOUND (AKA PHOSPHOROUS, APT35, ET AL)

https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4

ZIRCONIUM (AKA APT31)

https://app.tidalcyber.com/groups/5e34409e-2f55-4384-b519-80747d02394c

SOFTWARE

Searchable list of all software in Tidal's knowledge base: *https://app.tidalcyber.com/software*

APT29 DNC POWERSHELL BACKDOOR

https://app.tidalcyber.com/share/7a119bd1-988d-4fcb-a43b-9effb3112b7f

CHOPSTICK

https://app.tidalcyber.com/software/01c6c49a-f7c8-44cd-a377-4dfd358ffeba

MIMIKATZ

https://app.tidalcyber.com/software/b8e7c0b4-49e4-4e8d-9467-b17f305ddf16

PLUGX

https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10

PSEXEC

https://app.tidalcyber.com/software/73eb32af-4bd3-4e21-8048-355edc55a9c6

SEADUKE

https://app.tidalcyber.com/software/ae30d58e-21c5-41a4-9ebb-081dc1f26863

WEVTUTIL

https://app.tidalcyber.com/software/2bcbcea6-192a-4501-aab1-1edde53875fa

XTUNNEL

https://app.tidalcyber.com/software/133136f0-7254-4cec-8710-0ab99d5da4e5

CAMPAIGNS

Searchable list of all campaigns in Tidal's knowledge base: *https://app.tidalcyber.com/campaigns*

IRANIAN APT TARGETING U.S. VOTER DATA

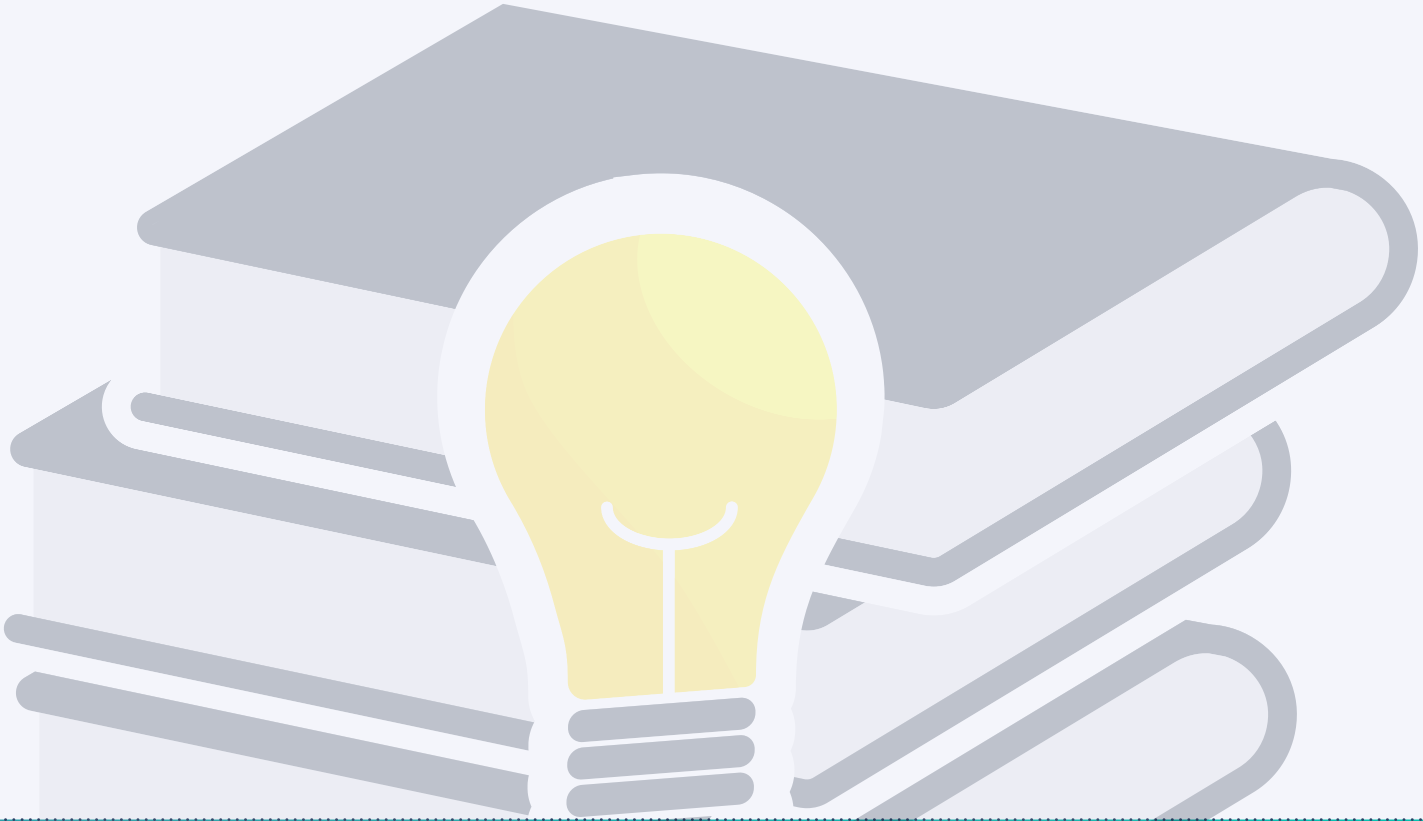
https://app.tidalcyber.com/campaigns/18cf25b5-ed3a-40f6-bf0a-a3938a4f8da2

U.S. GOVERNMENT APT EXPLOIT CHAINING ATTACKS

https://app.tidalcyber.com/share/techniqueset/a531ff61-3472-4d8e-8285-ed162b2d4c35

EXPLORE OUR RAPIDLY EXPANDING LIBRARY OF THREAT-INFORMED DEFENSE COMMUNITY RESOURCES

- *Tidal Cyber Community Edition*
- *The Ultimate Guide to Cyber Threat Profiling*
- *Tidal Cyber Blog*
- *BrightTalk Webcast Channel*



ENDNOTES

[1] Four countries – Indonesia, Taiwan, Romania, and Venezuela – received manual bumps into this highest tier since they all faced relatively high levels of priority adversaries, threats from multiple adversarial nations and/or high levels of state-backed adversary activity generally, even though other factor(s) fell short of the top threshold.

[2] Information- & credential-stealing malware ("infostealers") represent another major & growing threat to personnel. Credentials stolen from personal devices (or corporate devices used for personal purposes) infected by infostealers are *known to* lead to organizational compromise. Learn all about rising infostealer risks and defenses against them in our *two-part blog series* from last year.

[3] An October 2020 U.S. federal *announcement* highlights the added threat of "domain spoofing" related to election cycles.

ABOUT TIDAL CYBER

Tidal Cyber makes threat-informed defense achievable for organizations of all sizes. The Tidal Platform helps our customers map the security capabilities of their unique environment against the industry's most complete knowledgebase of adversary tactics and techniques including the MITRE ATT&CK® knowledge base, additional open-source threat intelligence sources, and a Tidal-curated registry of security product capabilities mapped to specific adversary techniques. The result is actionable insight to track and improve their defensive coverage, gaps, and overlaps.

COMMUNITY EDITION

Tidal's Community Edition is the freely-available threat-informed defense platform for researching threat actors, building technique sets, and so much more. Community Edition Users are able to share their work and participate in the larger Tidal Cyber community of defenders.

ENTERPRISE EDITION

Tidal Enterprise Edition brings a full-featured threat-informed defense experience to large enterprises and security teams. By pairing the threats most relevant to the organization with the tools in an organization's defensive stack, Tidal Enterprise Edition gives a complete picture of an enterprise's cyber posture, and quantifies how confident the organization can be in the Tidal Confidence Score™.

ABOUT THE AUTHOR

Scott Small is Director of Cyber Threat Intelligence at Tidal Cyber. Scott is a career intelligence researcher & analyst and an expert in cyber threat intelligence & threat profiling, open source research & investigations, and data analysis & automation. He has advised enterprise and public sector security teams across maturity levels on technical and strategic applications of intelligence and on using technology to help identify and mitigate organizational risk.

Throughout his career, Scott has briefed and trained large and small audiences and has presented original content at major security conferences and industry events. He is also an active member of the professional security & intelligence communities, contributes to community projects, and has published several independent projects, tools, & resources.

TIDAL CYBER
THREAT-INFORMED DEFENSE

info@tidalcyber.com   @tidalcyber   company/tidalcyber/   tidalcyber.com