



| Brief |

Cyber Threats to the U.S. Elections

B-2024-10-03b

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Election Threats, Information Campaigns,
Synthetic Media, Espionage, Deep and Dark Web

October 3, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on October 3, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Cyber Threats to the U.S. Elections

Executive Summary

The cyber threats posing risks to the U.S. presidential election to be held on November 5, 2024, illustrate the increasing interconnectivity of the cyber and geopolitical domains. There is substantial variance in the types of threat actors that demonstrate a level of perceived investment in the future U.S. leader, American political stability, or Western nations' ability to maintain their democratic processes.

These threat actors are harnessing a more diverse arsenal than ever before—placing increasing strain on security teams to ensure the election remains transparent and trustworthy. Threat actors are using malicious tools to cause disruption or breach networks and steal data, either as a part of an espionage campaign or in pursuit of financially or ideologically motivated objectives. Legitimate tools are also being leveraged, with threat actors using social media platforms and online forums as vehicles to deliver payloads of mis-, dis-, and malinformation (MDM).

In the coming weeks, it is very likely that the tempo and potency of cyber activity that actively targets or otherwise exploits the election will increase. While this will likely culminate on November 5, malicious cyber activity will very likely continue for as long as associated elements remain sufficiently topical for use in malicious activities.

This report should be read in conjunction with ZeroFox's Intelligence brief **Physical Threats to the U.S. Election (B-2024-10-03c)**.

| Threat Actors Targeting the U.S. Election

The run-up to the 2024 U.S. presidential election has drawn active engagement from the full suite of cyber threat actors, and this trend is expected to continue up to and beyond voting day. Broadly, these threat actors include:

➤ Adversarial Nation-states	Nation-state apparatus engaged in widespread campaigns to impact the election outcome, undermine democratic processes and institutions, or pursue state agendas
➤ Cybercriminals	Collectives that seek to leak sensitive information or engage in mass-influence campaigns, either for personal gain or working in conjunction with adversarial entities such as nation-states
➤ The Willing Influencer	Members of the public that actively seek to stoke divisions, sow discord, influence en-masse, and knowingly spread falsehoods
➤ The Accidental Influencer	Members of the public who may have no intent to spread falsehoods but want to voice truly-held beliefs, engage in debate, or unwittingly engage with actors that have more nefarious intentions

Threat actor activity aimed at targeting or leveraging the U.S. election varies substantially depending on the actor's motive, capability, and intent. The election process, outcome, or associated elements may be the primary targets of activity but can also be a vehicle or means to achieve predefined—and either adjacent or unrelated—ends. Threat actor motivations can broadly be categorized into three buckets; these categories are not mutually exclusive, and threat actors may sit within more than one of them.

- **Election Interference** - Seeking to directly induce a specific change, such as determining the winner of the election; obstructing or sabotaging electoral processes to delay, damage, or otherwise impede their proficiency and output.
- **Election Influence** - Seeking to undermine or subvert electoral institutions and organizations; affecting, influencing, or shaping the electorate in order to change their perception of political candidates or an ongoing foreign affair.
- **Election Opportunism** - Seeking to capitalize on or leverage the election to achieve certain political or financial strategic objectives, albeit often with indifference to the election itself or its outcome.

The majority of election threats very likely fall within the election influence category and involve the malicious or inaccurate use of information. The weaponization of information poses a greater and more nuanced threat today than ever before. Social media platforms, online forums, alternative media platforms, synthetic media, and a growing skepticism toward traditional media outlets have created a fertile ground in which actors can exaggerate, misconstrue, or synthesize a deliberate narrative that can assist them in achieving a given end-state. Such activity falls into one of three categories, which—while closely related and often overlap—carry distinct meaning and threats.

	Definition	Is the information true or based on truth?	Is it spread with intent to cause harm?
Misinformation	Content that is false, misleading, or taken out of context but is shared without the intent to deceive or cause harm	✗	✗
Disinformation	Deliberately false, misleading, manipulated, or biased content spread with the intent to deceive or cause harm	✗	✓
Malinformation	Genuine information, or information based on reality, spread with the intent to cause harm	✓	✓

Definitions of MDM*Source: ZeroFox Intelligence***| Pre-Election**

The vast majority of cyber activity targeting or leveraging the 2024 U.S. election will almost certainly take place before November 5 due to the substantial length of time in which threat actors can conduct planning and reconnaissance, direct various types of cyberattacks, adjust techniques, and repeat. Attack techniques utilized during this time period are very likely to carry a low risk for the threat actor, with the potential for a low to moderate impact on the election.

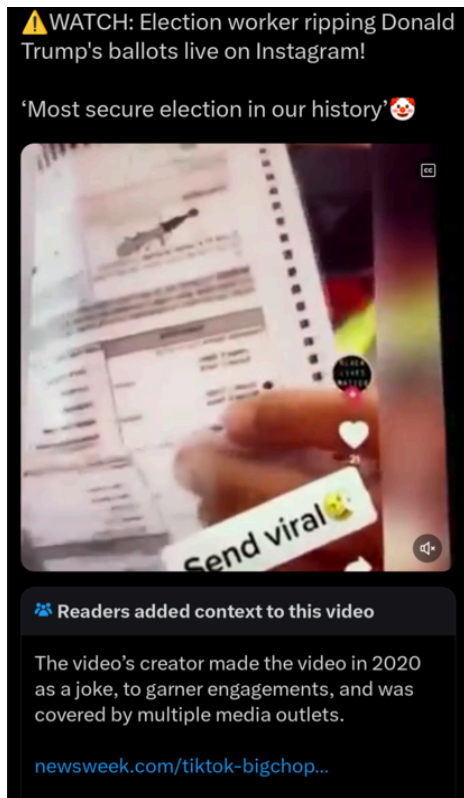
Domestic Activity

Widespread activity very likely consistent with attempts to influence the election outcome has been identified online and on social media platforms, including X (formerly Twitter), Facebook, Instagram, and TikTok. ZeroFox has observed various domestic actors spreading MDM, as well as information that could not have been verified before it was posted. These are most likely being published by willing interferers—and promoted by accidental interferers—although it is likely more organized criminal and nation-state

actors are behind some of the posts. The influence campaigns are varied in nature, although prominent themes include:

- Claims that the opposing side is seeking to undermine democratic processes
- Stoking discord on socially divisive topics, including immigration, abortion, gun rights, and foreign affairs
- False or exaggerated claims of celebrity endorsements for candidates

Disinformation on social media platforms by the respective voterbases is widespread and most often intended to accuse political rivals (such as parties, individuals, and opposing voter bases) of inappropriate behavior in a bid to shore support for their affiliated party. This threat is increased when such information is intentionally shared by those with large followings, such as celebrities and influential figures, as well as by those whose position or stature lends credibility to the information.



Posts alleging anti-Republican and anti-Democratic behavior and inciting action

Source: X (formerly Twitter)

In isolation, this type of content poses very little threat to the election, with the majority of individual posts on social media platform X, for example, typically garnering relatively small engagement. However, their sheer quantity can lead to the creation of narratives which, in some cases, become broadly agreed upon by a large number of people. Additionally, metadata-type tools such as hashtags (as well as clickbait-type titles, mentions, and tags) can be used to increase the likelihood of a single post becoming widely seen, as well as enable the author to reach a specific demographic.

Mis- and disinformation surrounding both presidential candidates is widespread and is typically focused on garnering domestic support, disparaging political opponents, or furthering a narrative. Fabricated media poses a significant risk to the way that voter bases view, share, and use media to formulate their opinions and inform their voting behavior.¹²³

- While synthetic media does not necessarily equate to false or malicious information, it is often offered as low-effort evidence for a claim (which may be true or false).
- This can lead to recipients believing the claim due to apparent visual evidence or resonating more with the claim because of visually appealing synthetic media, which also increases the likelihood of it being shared.
- AI-generated media almost certainly poses a larger threat to the upcoming election than any previous one.

Multiple instances of such posts surrounding former U.S. President and current Republican nominee Donald Trump have been identified during the campaigning period. During the presidential debate hosted by ABC News in Philadelphia, Pennsylvania, on September 10, Donald Trump claimed that household pets have been eaten in Springfield, Ohio, by “the people that came in”—likely referring to illegal migrants.⁴ His claims were shared by James David (JD) Vance, the Republican Party’s Vice President nominee.

¹ [hXXps://x.com/elonmusk/status/1816974609637417112](https://x.com/elonmusk/status/1816974609637417112)

² [hXXps://truthsocial.com/@realDonaldTrump/posts/112981017774094658](https://truthsocial.com/@realDonaldTrump/posts/112981017774094658)

³ [hXXps://twitter.com/muratokcu32/status/1830676349981217161](https://twitter.com/muratokcu32/status/1830676349981217161)

⁴ [hXXps://www.bbc.co.uk/news/articles/c77128myezko](https://www.bbc.co.uk/news/articles/c77128myezko)

- The claims sparked an online discussion surrounding their authenticity, characterized by a flurry of AI-generated “memes” depicting Donald Trump protecting various animals.
- While initially shared by likely Republican-leaning voters in a manner that supported Donald Trump, they later became synonymous with political disinformation and shared by those supportive of the Democratic Party.
- The ongoing trend demonstrates how the use of synthetic media alongside a statement can be used to evoke emotion to both garner support for and ridicule a political candidate.



AI-generated images depicting Donald Trump as a guardian of a cat and a duck

Source:

[hXXps://www.dailymail\[.\]co\[.\]uk/news/article-13837875/Pets-Trump-AI-memes-explode-social-media.html](https://www.dailymail.co.uk/news/article-13837875/Pets-Trump-AI-memes-explode-social-media.html)

The use of synthetic media and disinformation has also been leveraged to promote likely fake celebrity endorsements for candidates. While unlikely to directly impact the election outcome, these examples highlight the ways in which false information regarding prominent figures or events can be used, intentionally or otherwise, to influence large numbers of people.⁵ AI-generated content related to both legitimate and fabricated endorsements have been observed throughout 2024.⁶

⁵ [hXXps://www.theguardian\[.\]com/us-news/article/2024/aug/19/trump-ai-swift-harris-musk-deepfake-images](https://www.theguardian.com/us-news/article/2024/aug/19/trump-ai-swift-harris-musk-deepfake-images)

⁶ [hXXps://www.marca\[.\]com/en/lifestyle/celebrities/2024/08/20/66c3dea146163f46068b459d.html](https://www.marca.com/en/lifestyle/celebrities/2024/08/20/66c3dea146163f46068b459d.html)

Instances of seemingly-innocuous information that have been widely shared or misconstrued—regardless of original intent—have also been observed. During the August 2024 Democratic National Convention, rumors circulated online that singer Beyoncé was due to make a surprise appearance during an acceptance speech by Vice President and presidential nominee Kamala Harris. Representatives of Beyoncé later confirmed that the singer “was never scheduled to be there.”⁷ It is not clear how the rumors began, but both figures associated with the Democratic party and media outlets are alleged to have circulated this information.

- Fox News speculated that the Democratic Party and the DNC may have deliberately espoused false information in a bid to inflate DNC attendance and associate the party with one of the most popular singers of all time.
- Some X users suggested that the “no-show” is indicative of Beyoncé’s support for Donald Trump.

Reporting from the prior 2020 U.S. election period suggests that a majority of Americans think that false news had a major impact on the outcome of the election. An even higher number claimed that they had come across election news that they deemed outright false, almost certainly leading to increased skepticism when ingesting information.⁸ However, MDM will almost certainly contribute to the electorate’s voting patterns—despite growing awareness about it—due to its widespread reach and increasing difficulty in distinguishing it from objective truth.

- False information that continues to circulate poses a significant threat to the truth. According to the “validity effect”, people’s familiarity with information often overrides their rationality.
- Information which is adverse to widely-believed ideas or flagged by online moderation tools very likely carries its own appeal to people untrusting of “mainstream” media outlets.⁹

⁷ [hXXps://www.hollywoodreporter\[.\]com/news/politics-news/beyonce-not-attending-2024-dnc-1235982694/](https://www.hollywoodreporter.com/news/politics-news/beyonce-not-attending-2024-dnc-1235982694/)

⁸ [hXXps://www.pewresearch\[.\]org/journalism/2021/02/22/misinformation-and-competing-views-of-reality-abounded-throughout-2020/](https://www.pewresearch.org/journalism/2021/02/22/misinformation-and-competing-views-of-reality-abounded-throughout-2020/)

⁹ [hXXps://www.theguardian\[.\]com/technology/2024/sep/20/trump-tweets-false-label-credibility-supporters](https://www.theguardian.com/technology/2024/sep/20/trump-tweets-false-label-credibility-supporters)

Overseas Activity

International actors have also been observed leveraging false information regarding the election. The United States' geopolitical stature and international presence ensures that both friendly and opposing states have a continued interest in the country's leader, foreign affairs, and domestic policies. Foreign states view the shaping of U.S. elections as a means by which to ensure their own security, achieve strategic objectives, and pursue preferred outcomes to ongoing geopolitical events.



On August 16, 2024, AI research organization OpenAI announced that it had banned a number of ChatGPT accounts that had been observed using the tool to create both long-form blog posts and short-form social media comments related to the elections. The activity is linked to "Storm-2035", an ongoing Iranian influence campaign that very likely seeks to sway the opinions of American voters. According to OpenAI, it enacted similar bans against the collective "Crimson Sandstorm" earlier this year as well, and none of this content achieved significant readership before its removal.

Iranian cyber activity targeting this year's election has very likely been higher-effort than that observed in previous years, with a likely chance that such activity is intended to influence American voters in favor of Kamala Harris. The Donald Trump campaign has attempted to use Iran's supposed favor of the Democratic Party to garner support by claiming that "Iran loves the weakness of Kamala Harris."¹⁰ While unlikely to be a primary objective, Tehran likely views such rhetoric as positive and undermining to American political stability.

¹⁰

[hXXps://www.huffingtonpost\[.\]co\[.\]uk/entry/donald-trump-iran-assassination-threats_n_66f5264fe4b08b9c8c8c3eb0](https://www.huffingtonpost[.]co[.]uk/entry/donald-trump-iran-assassination-threats_n_66f5264fe4b08b9c8c8c3eb0)



For 248 years, Americans have been warned about someone like Donald Trump trying to crown himself King. I'm ready to fight like hell to protect our democracy. [#DumpTrump](#)

8:27 AM · Aug 12, 2024 · 8 Views

Storm-2035 social media post and article headline

Source: [hXXps://openai\[.\]com/index/disrupting-a-covert-iranian-influence-operation/](https://openai[.]com/index/disrupting-a-covert-iranian-influence-operation/)



ZeroFox has also identified malicious cyber activity emanating from China that is targeting and leveraging the election to pursue strategic state objectives.

Much of this activity is considered a part of “Spamouflage”, an ongoing disinformation campaign that is almost certainly at the behest of the Chinese government. Active since as early as 2017, Spamouflage seeks to promote pro-Chinese Communist Party propaganda, target political dissidents, and influence public opinion surrounding geopolitical topics important to Beijing.



Anti-NATO/America Spamoflage posts

Source: [hXXps://openai\[.\]com/index/disrupting-a-covert-iranian-influence-operation/](https://openai[.]com/index/disrupting-a-covert-iranian-influence-operation/)

Many recently-observed Spamoflage operations have taken place on social media platforms such as X and Meta, where large numbers of fake accounts appear to impersonate American voters. The accounts do not appear to overtly support either presidential candidate but, rather, seek to sow division via sharing of divisive content about immigration, veterans' welfare, and female reproductive rights.¹¹

While there is a roughly even chance that such material may dissuade some American citizens from voting, these cyber activities are unlikely to directly affect the outcome of the election. Instead, they are very likely in line with Chinese state ambitions to undermine Western democratic processes and institutions, as well as long-term shaping activity intended to weaken international opposition surrounding contentions in Taiwan and the South China Sea. The Spamoflage campaign is very likely to continue past the upcoming election, increasingly leveraging synthetic media and a growing number of social media platforms.

¹¹ [hXXps://public-assets.graphika\[.\]com/reports/graphika-report-the-americans.pdf](https://public-assets.graphika[.]com/reports/graphika-report-the-americans.pdf)



Of the foreign states, Russian cyber activity likely poses the greatest threat to the outcome of the upcoming election. Multi-pronged Kremlin MDM efforts reflect the prioritization of a relatively short-term objective: the successful election of Donald Trump in November 2024. As such, information campaigns seeking to denigrate and undermine both Kamala Harris and the Democratic Party are almost certain to continue in the coming weeks, with voters in swing states such as Arizona, Georgia, North Carolina, and Nevada likely to be targeted specifically.

- The Russian government almost certainly favored Donald Trump in the 2016 and 2020 U.S. presidential elections. His foreign policy preferences and approach to international relations are very likely a key contributor to this. As well as having isolationist ambitions, Trump has been overtly skeptical of the U.S. and NATO approach to the ongoing Russia-Ukraine conflict, as well as NATO in general. On July 4, 2024, Russian President Vladimir Putin outlined these topics in relation to pre-conditions to ceasing aggression in Ukraine.¹²

In September 2024, a video went viral on social media platforms that depicted a woman claiming to have been paralyzed following a 2011 car accident in San Francisco that involved Kamala Harris. The video had initially been published by an alleged San Francisco media outlet named “KSBF-TV”, and it was later shared by a self-professed broadcaster for Russian state media agency Sputnik-Aussie Cossack.¹³ Subsequent research by Microsoft suggested that KSBF-TV and the incident are entirely fabricated, and the woman featured in the video is a paid actor. The threat group purportedly responsible is “Storm-1516”, an alleged Kremlin-aligned troll farm that has also been observed distributing fabricated media surrounding an alleged attack by Kamala Harris supporters at a Donald Trump rally.¹⁴

¹²[hXXps://www.reuters.com/world/putin-says-preference-biden-remains-unchanged-despite-debate-2024-07-04](https://www.reuters.com/world/putin-says-preference-biden-remains-unchanged-despite-debate-2024-07-04)¹³[hXXps://www.reuters.com/world/us/fake-kamala-hit-and-run-story-is-work-russian-propaganda-group-microsoft-says-2024-09-17/](https://www.reuters.com/world/us/fake-kamala-hit-and-run-story-is-work-russian-propaganda-group-microsoft-says-2024-09-17/)¹⁴[hXXps://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/](https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/)

**KBSF-TV video depicting alleged victim**

Source: [hXXps://twitter\[.\]com/krassenstein/status/1831065332410446093](https://twitter.com/krassenstein/status/1831065332410446093)

Other activity has stemmed from Russian state media outlets such as Russia Today (RT) and Tass, as well as fabricated news sites that attempt to spoof the domains of legitimate U.S. media outlets in order to lure unsuspected visitors before presenting them with disinformation. One such website published an audio file titled “Top Democrats Are Behind the Assassination Attempt on Trump; Obama Knows About the Details”, as well as an article claiming that a Ukrainian troll farm seeks to disrupt the U.S. elections.¹⁵

- Many of these domains were allegedly seized following a press release by the U.S. Department of State outlining RT’s “global covert activities”, accusing the platform of being involved in information operations, covert influence, and military procurement targeting countries around the world.¹⁶
- Earlier in September 2024, the U.S. Justice, State, and Treasury Departments announced sanctions targeting Russian state media executives amid accusations of election interference.¹⁷

¹⁵

[hXXps://www.france24\[.\]com/en/live-news/20240819-pro-russia-news-sites-spew-incendiary-us-election-falsehoods](https://www.france24.com/en/live-news/20240819-pro-russia-news-sites-spew-incendiary-us-election-falsehoods)

¹⁶ [hXXps://www.state\[.\]gov/alerting-the-world-to-rts-global-covert-activities/](https://www.state.gov/alerting-the-world-to-rts-global-covert-activities/)

¹⁷ [hXXps://www.bbc\[.\]co\[.\]uk/news/articles/c8rx28v1vpro](https://www.bbc.com/uk/news/articles/c8rx28v1vpro)

Espionage-focused operations are very likely heightened in the pre-election period, as opposing states seek to understand the implications of potential outcomes, gain insight into future policy, and understand how it impacts their strategic objectives, geopolitical interests, and domestic security. Additionally, the expanded communications, election infrastructure, and databases lead to a growth in attack surface, which is more likely to consist of short-term, hastily assembled security protocols. While instances of intelligence-gathering activity have been observed, there is a likely chance that additional operations are ongoing and remain covert.

Throughout 2024, likely Iranian state-affiliated cyber threat actors have been observed leveraging spear phishing, account takeover, and password spraying in attacks against Donald Trump's election campaign.¹⁸ Alleged network breaches resulted in the theft of internal communications, which in the following weeks were reportedly sent to senior figures within the then-Joe Biden election campaign, as well as select media outlets.¹⁹ While the primary intent of this campaign was likely election interference, the allegedly successful leveraging of social engineering to breach victim networks demonstrates a notable risk to potentially sensitive information.

- As of the writing of this report, three Iranian nationals have allegedly been indicted in relation to this activity.²⁰

Deep and Dark Web Actors

ZeroFox has observed numerous incidents of deep and dark web (DDW) actors monetizing the election by selling malicious services designed to target the voter base, as well as illicitly obtained personally identifiable information (PII) and personal financial information (PFI).

On September 10, 2024, an untested Russian-speaking threat actor named "Robi Good" posed in the DDW forum xss advertising a turnkey (ready to use) phishing service which targets both Donald Trump and Kamala Harris supporters. The tool allegedly enables buyers to deploy malicious domains that mimic official donation websites. Users seeking

¹⁸ [hXXps://blogs\[.\]microsoft\[.\]com/on-the-issues/2024/08/08/iran-targeting-2024-us-election/](https://blogs.microsoft.com/on-the-issues/2024/08/08/iran-targeting-2024-us-election/)

¹⁹ [hXXps://www.odni\[.\]gov/index.php/newsroom/press-releases/press-releases-2024/3994-odni-pr-22](https://www.odni.gov/index.php/newsroom/press-releases/press-releases-2024/3994-odni-pr-22)

²⁰ [hXXps://www.bbc\[.\]co\[.\]uk/news/articles/czxdw5l5vxgo](https://www.bbc.co.uk/news/articles/czxdw5l5vxgo)

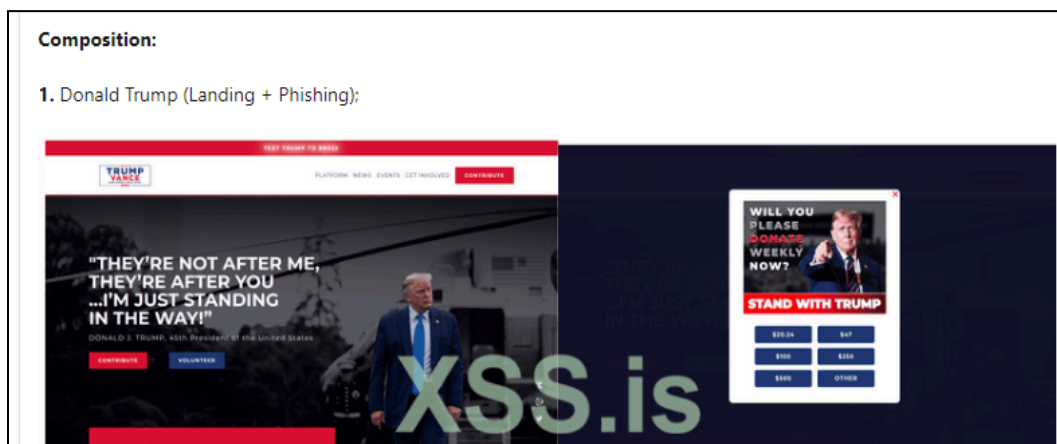
to donate to a preferred campaign are then tricked into providing PII, PFI, and one-time passwords (OTPs).



Robi Good's xss advertisement

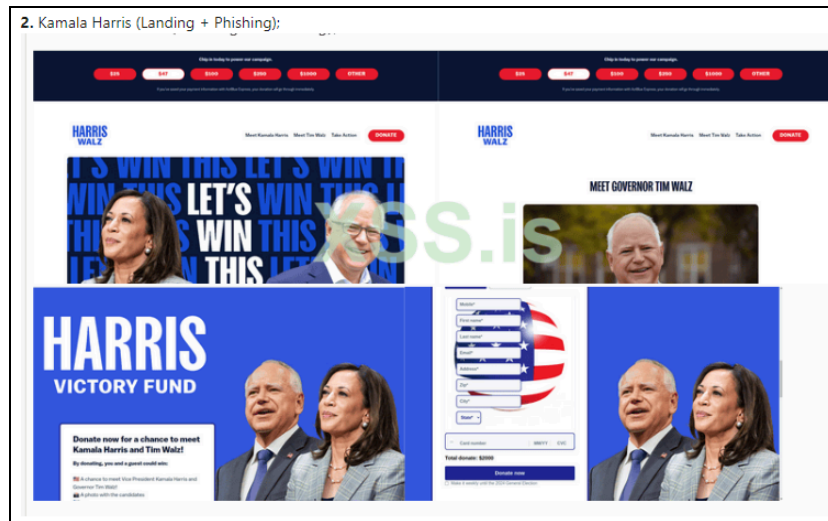
Source: ZeroFox Intelligence

The service is priced at USD 1,260 and reportedly comes with numerous customization options. Robi Good specified that escrow services are available, increasing the credibility of the actor and the service. Sales and further enquiries are to be made via an advertised Telegram channel, where buyers also receive a demonstration.



Phishing page targeting Donald Trump supporters

Source: ZeroFox Intelligence



Phishing page targeting Kamala Harris supporters

Source: ZeroFox Intelligence

The finding accentuates both the propensity for financially motivated DDW actors to opportunistically leverage high-profile events for personal gain and the bipartisan stance taken by threat actors that are likely to be based in or associated with Russia. Services such as these are very likely to be popular among DDW forum users and will likely pose a threat to American voters. If phishing scams such as these are widely successful, there is also a roughly even chance that imitated official entities will suffer from both reputational damage and less overall financial donations.

On August 19, 2024, the likely Morocco-based hacktivist group “Mr Hamza” made an announcement in its Telegram channel claiming responsibility for an alleged network breach that targeted the official government website of the state of New Jersey, nj[.]gov. Mr Hamza, known for targeting U.S. government entities, claimed that “all data” from the website “has been removed” and “pulled.” A ZIP file was attached, named nj[.]gov[.]zip, comprising five CSV files that allegedly contain PII pertaining to New Jersey mayors—including names, term dates, municipal codes, address, and contact details from between 2016 and 2020.

- The announcement appeared to be presented as a part of a larger campaign targeting U.S.-based victims, using the hashtag #Ops_USA.

- It is unclear when the alleged breach took place or whether data pertaining to website visitors is also compromised.
- If Mr Hamza's claims are legitimate, there is a very likely chance that implicated New Jersey officials face a significantly higher risk from social engineering activity, even if parts of the information are up to eight years old. The activity poses a low overall threat to the upcoming election, however.

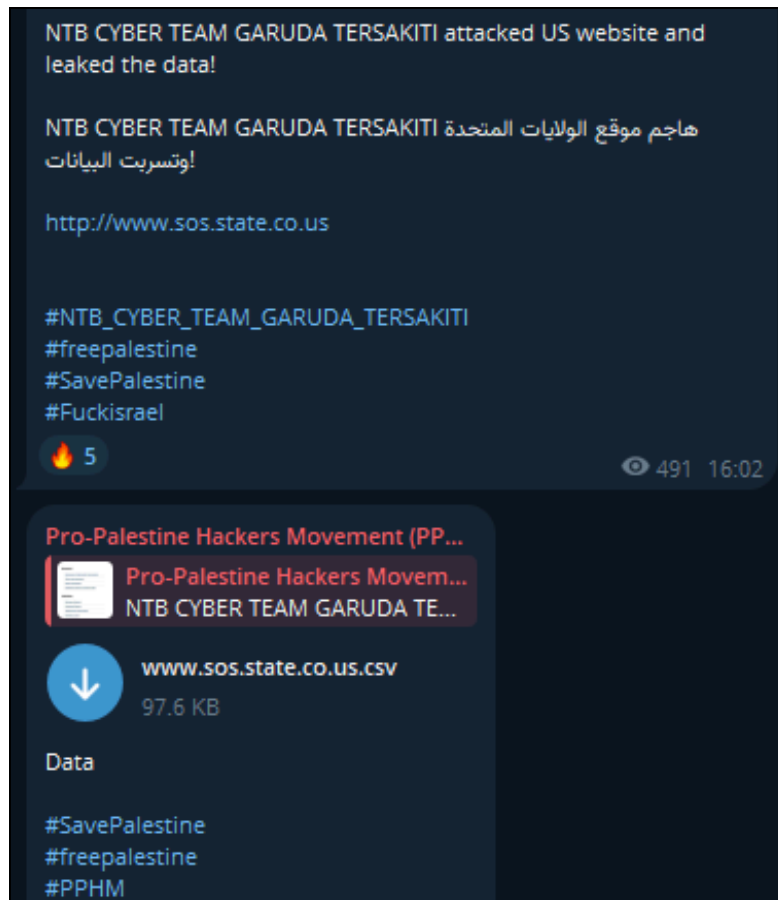


Telegram advertisement by Mr Hamza

Source: ZeroFox Intelligence

On April 14, 2024, an announcement was made on the Telegram channel Pro-Palestine Hackers Movement claiming that the “NTB CYBER TEAM”, also known as “TERSAKITI”, had hacked the Colorado Secretary of State’s official website, sos.state[.]co[.]us. The channel posted a CSV file allegedly containing 637 records pertaining to business listings and registered entities within the region.

- TERSAKITI is a politically motivated hacktivist collective very likely linked to Indonesia. Its activity is usually aligned to pro-Palestinian causes, targeting perceived opponents of Palestine or Islam.



Telegram advertisement by TERSAKITI

Source: ZeroFox Intelligence

This data, if legitimate, is very unlikely to pose a threat to the upcoming election but could be leveraged to conduct social engineering campaigns, target specific businesses, and undermine Colorado government institutions. This activity highlights the threat posed from ideologically motivated hacktivist groups that have no stake in the outcome of the election but likely view the election period as a lucrative time to conduct malicious activity.

| Voting Period

Due to a shortened time frame demanding more direct and decisive action from malicious actors that seek to have an effect, cyber threats during the voting period of the election are more likely intended to directly impact the outcome or obstruct and delay electoral processes. The voting period and the pre-election period overlap to some extent, as early in-person voting and mail-in voting began in some states in early September 2024.

At this stage, there is a high threat from attacks seeking to prevent votes from being effectively cast. To achieve this, both domestic and international threat actors will likely leverage MDM to sow confusion regarding election protocols.

- In January 2024, some members of the public located in New Hampshire received a phone call alleging to be from Joe Biden stating, “your vote makes a difference in November, not this Tuesday” (January 23). While the audio mimicked Joe Biden, the phone call was fabricated and likely leveraged synthetic media in an effort to discourage residents from voting in the New Hampshire presidential primary election.²¹ Similar incidents were identified prior to the 2020 U.S. election.²²

On or close to November 5, ZeroFox anticipates a heightened threat from overt and aggressive last-minute smear campaigns, most likely targeting prominent politicians within a political party or associated influential individuals, such as political family members, donors, or endorsers. This does not necessarily need to be MDM to have an effect, as even objective or proven information surrounding a negative incident that is reinvigorated at a critical point in the election process can cause significant reputational damage.

- In the days prior to the November 3, 2020, U.S. presidential election, a series of articles were published regarding allegations made against Hunter Biden.²³ Many attributed this to an attempt to sway voters away from his father, Democratic candidate Joe Biden.

²¹ [hXXps://www.doj.gov/news-and-media/voter-suppression-robocall-complaint-election-law-unit](https://www.doj.gov/news-and-media/voter-suppression-robocall-complaint-election-law-unit)

²² [hXXps://www.nature.com/articles/d41586-024-01696-z](https://www.nature.com/articles/d41586-024-01696-z)

²³ [hXXps://www.nytimes.com/2020/10/22/us/politics/hunter-biden-laptop.html](https://www.nytimes.com/2020/10/22/us/politics/hunter-biden-laptop.html)

There is also a low-risk but potentially very high-impact threat posed to voting machinery and digital infrastructure used by balloting authorities to scan, store, tally, and tabulate votes. A range of cyber threat actors (from ideologically-motivated hacktivist collectives to foreign state intelligence services) almost certainly deem direct interference with this digital infrastructure as a high pay-off means of either altering election results or delaying the outcome by causing disruption.

- In 2018, the U.S. Department of Justice charged 12 Russian intelligence officers with a range of offenses linked to attempted election disruption. Among the accusations was that the actors had obtained illicit access to electronic voting equipment to gain information surrounding software and hardware solutions.²⁴

The security of digital voting infrastructure almost certainly increases each election cycle in response to the increasingly complex cyber threat landscape and growing number of threat actors that perceive a benefit from targeting U.S. elections. Guidance for digital security is issued by both the Cybersecurity & Infrastructure Security Agency (CISA) and the U.S. Election Assistance Commission, and resources are provided surrounding registered manufacturers and test laboratories.^{25,26,27,28}

As security protocol is deliberated at the state level, this guidance is voluntary. However, a successful network breach is very unlikely to occur if:

- Networks remain air-gapped, segmented, and disconnected from any external networks such as the internet.
- Hardware and software is sourced from recommended suppliers.
- Login credentials are kept secure.
- Security patches are kept up to date.
- Appropriate user guidance is readily available, and incident response plans are in place and rehearsed.

²⁴ [hXXps://apnews\[.\]com/article/13b494bab84d45e0bf82145573e2cac3](https://apnews.com/article/13b494bab84d45e0bf82145573e2cac3)

²⁵

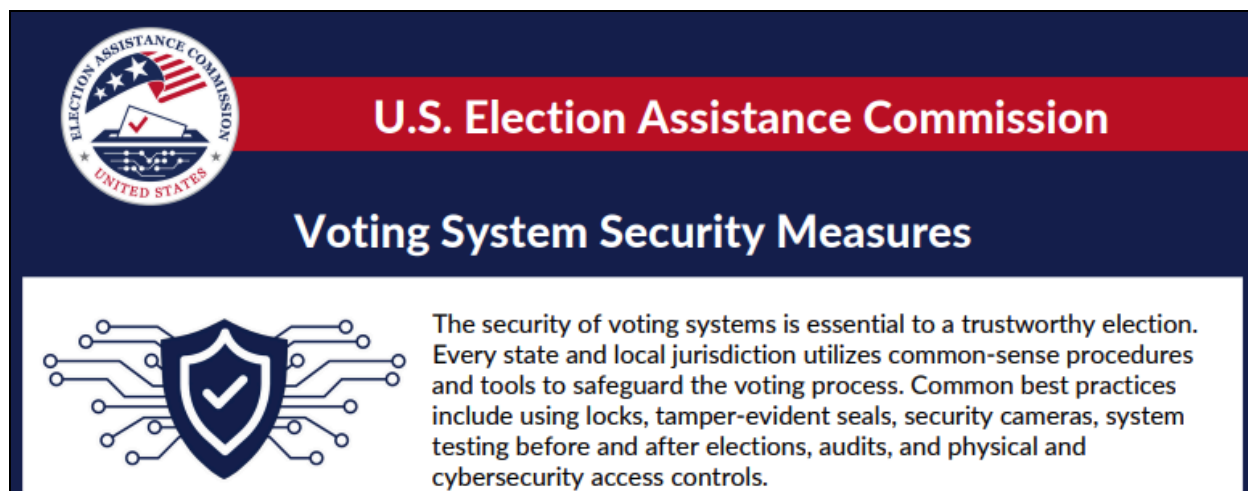
[hXXps://www.eac\[.\]gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.p](https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.p)

²⁶ [hXXps://www.eac\[.\]gov/voting-equipment/registered-manufacturers](https://www.eac.gov/voting-equipment/registered-manufacturers)

²⁷ [hXXps://www.eac\[.\]gov/voting-equipment/voting-system-test-laboratories-vstl](https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl)

²⁸

[hXXps://www.cisa\[.\]gov/sites/default/files/2024-09/Readiness-and-Resilience-Checklist-for-Election-Offices-508.p
df](https://www.cisa.gov/sites/default/files/2024-09/Readiness-and-Resilience-Checklist-for-Election-Offices-508.pdf)

**Excerpt from U.S. Election Assistance Commission security pamphlet**

Source: ZeroFox Intelligence

Failure to enact proper security protocols in election equipment and associated networks will significantly raise the threat of illicit network access by malicious cyber actors, potentially resulting in distributed-denial-of-service (DDoS) attacks, inaccurate counts, or delayed results. Any successful compromise—even if overstated or exaggerated—also significantly increases the risk of claims from the voter base, political parties, or prominent individuals that proper procedures were not followed and results may not be accurate. Narratives such as these can then be leveraged as justification for undermining electoral institutions or the new government administration.

| Post-Election

Post-election cyber threats will almost certainly revolve mostly around the continued use of information campaigns to drive narratives aimed at undermining democratic procedures, questioning the authenticity of the electoral processes and results, and maintaining political relevance by denigrating opposition parties. In 2024, there is almost no chance that this would result in a direct threat to the election outcome, but it would very likely lead to instability that can be capitalized upon by those willing to perpetuate the threat.

With the closure of polling offices across the United States between approximately 7:00 PM and 9:00 PM (local times) on November 5, 2024, the greatest threat will likely be from prominent figures seeking to establish an early narrative that can later be used to garner support and incite unrest or discontent should final voting counts lead to outcomes considered unfavorable. Some likely claims include:

- Votes were not properly counted, and a recount should take place. This is most likely to occur in swing states that will have a disproportionate impact on the outcome of the election.
- Votes in certain states have been “rigged” or otherwise tampered with. This is most likely to occur in states within which pre-election polls had indicated alternative results.
- Voters have been misled or confused by changes made to voting methods, rules, times and dates, or legislation.
- Significant domestic or international events, such as natural disasters or epidemics, have led to mass confusion and disarray.
- Earlier examples of interference, disruption, or malpractice associated with election procedures are reinvigorated and used to explain unexpected outcomes, even if such activity has already been accounted for or rectified.

Comments from prominent politicians have already indicated in 2024 that the outcome of the upcoming election would only be accepted if “everything is honest.”²⁹ The danger posed by comments such as these is two-fold:

- It espouses and normalizes a sentiment that an element of uncertainty exists and that election outcomes may not be as they seem. This could be construed as justification for recourse action by a large number of voters, which is innately undermining of Western democratic procedures.
- It raises questions surrounding the lack of any arbiter of election integrity, as well as a lack of protocol should an adverse situation arise.

²⁹

[hXXps://www.jsonline\[.\]com/story/news/politics/elections/2024/05/01/economy-and-immigration-takeaways-from-donald-trumps-wisconsin-rally/73501778007/](https://www.jsonline.com/story/news/politics/elections/2024/05/01/economy-and-immigration-takeaways-from-donald-trumps-wisconsin-rally/73501778007/)

Prolonged information campaigns that question election integrity are almost certainly perceived as undermining democracy and strategically beneficial to opposing states such as Russia, China, and Iran. Such action could be used as justification for promoting alternative governing styles and as leverage in diplomatic affairs. Furthermore, it offers a more volatile, partisan, and divided U.S. social and political landscape for influence campaigns targeting upcoming events, such as future elections or international affairs. Opposing nation-states will very likely continue to evolve novel methods of creating, perpetuating, and exacerbating these situations.

Unbound by the electoral timeline, DDW actors will continue to pose a significant threat following the election. The spike in activity observed by DDW actors leveraging the election to target voters, associated personnel, and digital infrastructure will very likely result in an increase of exploitation in the coming months that will mostly impact those implicated in cyberattacks resulting in the theft of personal information.

PII leaked in data breaches will continue to be sold and procured in DDW forums and marketplaces, often staying in circulation for long periods of time and bought repeatedly. This significantly increases the threat from activity such as social engineering, malware, and digital extortion.

| Outlook

Safeguarding the 2024 U.S. election requires an understanding of the threat posed by a cyber threat election landscape that is likely more diverse and complex than ever before. Within this landscape, actors with a full spectrum of intents, motives, and capabilities perceive a vested interest in the outcome of the election and its associated future policy, the efficacy of its underpinned procedures and institutions, or the successful showcasing of democratic procedure on a global stage.

MDM poses a greater threat than ever before thanks to an ever-growing array of platforms granting it viewership and circulation, a populace increasingly distrustful of mainstream media outlets, and prominent figures espousing often-uninformed views while creating permissible digital norms. This is further exacerbated by the rise in synthetic media and the proliferation of tools that enable its creation, which is often

unimpeded in its use due to its relative novelty and a subsequent lack of vigilance among users of social media platforms and alternative media outlets. This information is almost certainly already swaying voter opinions and will very likely have an effect on the election result, the extent of which cannot be easily quantified.

Activity emanating from state-associated actors—such as the spurring of misinformation campaigns, espionage, or “hack and leak” discrediting attacks—will likely continue over the coming weeks and reduce in tempo following November 5, 2024. This activity is unlikely to directly affect the outcome of the election but will likely be considered a success in terms of contribution to strategic objectives. Following the election, these actors will almost certainly continue to pursue the same objectives, leveraging alternative vectors.

Individuals and organizations must proactively adopt responsible security practices, including verifying information consumed and monitoring for sensitive data disclosures online. Tools and resources are available that can assist in verifying the legitimacy of online content, and digital risk protection services can assist in identifying and mitigating the spread of sensitive information should such disclosures occur.

| Recommendations

Countering mis-, dis-, and malinformation

- Question the credibility of information sources, such as the date the content was published, and identify any potential source biases. Consider content in its entirety, not just the headline.
- Use fact-checking websites like FactCheck[.]org, the News Literacy Project, and NewsGuard.
- Conduct training on how MDM works to boost defenses to, and recognition of, false claims.
- For organizations that find themselves a victim of MDM, have a crisis response plan in place to evaluate the content and formulate an approach to neutralize and contain the malicious information.
- Ensure a thorough understanding of the exposure of key individuals and organizations in open and closed sources.

Protecting networks

- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.

Voting security

- Proactively seek and identify disinformation spreading on social media platforms regarding voting dates, times, locations, and protocols. Official information is published by the U.S. Election Assistance Commission.
 - [hXXps://www.eac\[.\]gov/voters/register-and-vote-in-your-state?field_state_target_id=18406](https://www.eac.gov/voters/register-and-vote-in-your-state?field_state_target_id=18406)
- Minimize the chance of human error (very likely the greatest threat to voting systems) by ensuring staff receive cyber hygiene training, appropriate user guidance is readily available, and incident response plans are in place and rehearsed.
- Enact prudent physical security measures, scrutinizing access to individuals, unfamiliar IT equipment, and portable storage devices.
- Ensure that digital voting equipment and associated networks are secure and certified. Guidance is issued by the U.S. Election Assistance Commission.
 - <https://www.eac.gov/election-technology>
- Utilize recommendations and training resources offered by CISA designed to reduce the threat from phishing, ransomware, and DDoS activity.
 - [hXXps://www.cisa\[.\]gov/cybersecurity-toolkit-and-resources-protect-elections](https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%