CHECK POINT

EXPOSURE MANAGEMENT

2026 U.S. Midterm Election Threat Outlook

By Danielle Hess

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The 2026 U.S. midterm election cycle is expected to drive elevated cyber threat activity across the broader election ecosystem, including political organizations, fundraising and media platforms, government services, campaign personnel, and the providers that support them.

Current intelligence and reporting indicate that the most likely 2026 election-related threats involve phishing, impersonation, influence activity, AI-enabled content abuse, and opportunistic disruption. In practice, the most immediate operational risks are concentrated in the accounts, platforms, and services that campaigns and election-adjacent organizations rely on to communicate, raise funds, publish information, and maintain public trust.

The current threat environment favors operations that are inexpensive, scalable, and capable of producing outsized political or psychological impact. The most consequential risks center on identity, access, trust, and narrative control. Phishing, brand impersonation, manipulated media, coordinated misinformation, and abuse of third parties can all create confusion, reputational harm, and operational disruption without requiring direct compromise of core election infrastructure.

Check Point Exposure Management identified sustained election-related infrastructure creation throughout early 2026. Continued registration of election-themed domains expanded the available infrastructure that may later support phishing, impersonation, fraudulent donation activity, misinformation, or abuse of election-related brands and services.

Credential exposure remained elevated across major political fundraising platforms and government-related assets, while election-related data and claims of voter-data exposure appeared on criminal forums, reinforcing continued interest in trusted platforms, public-sector data, and election-related information.

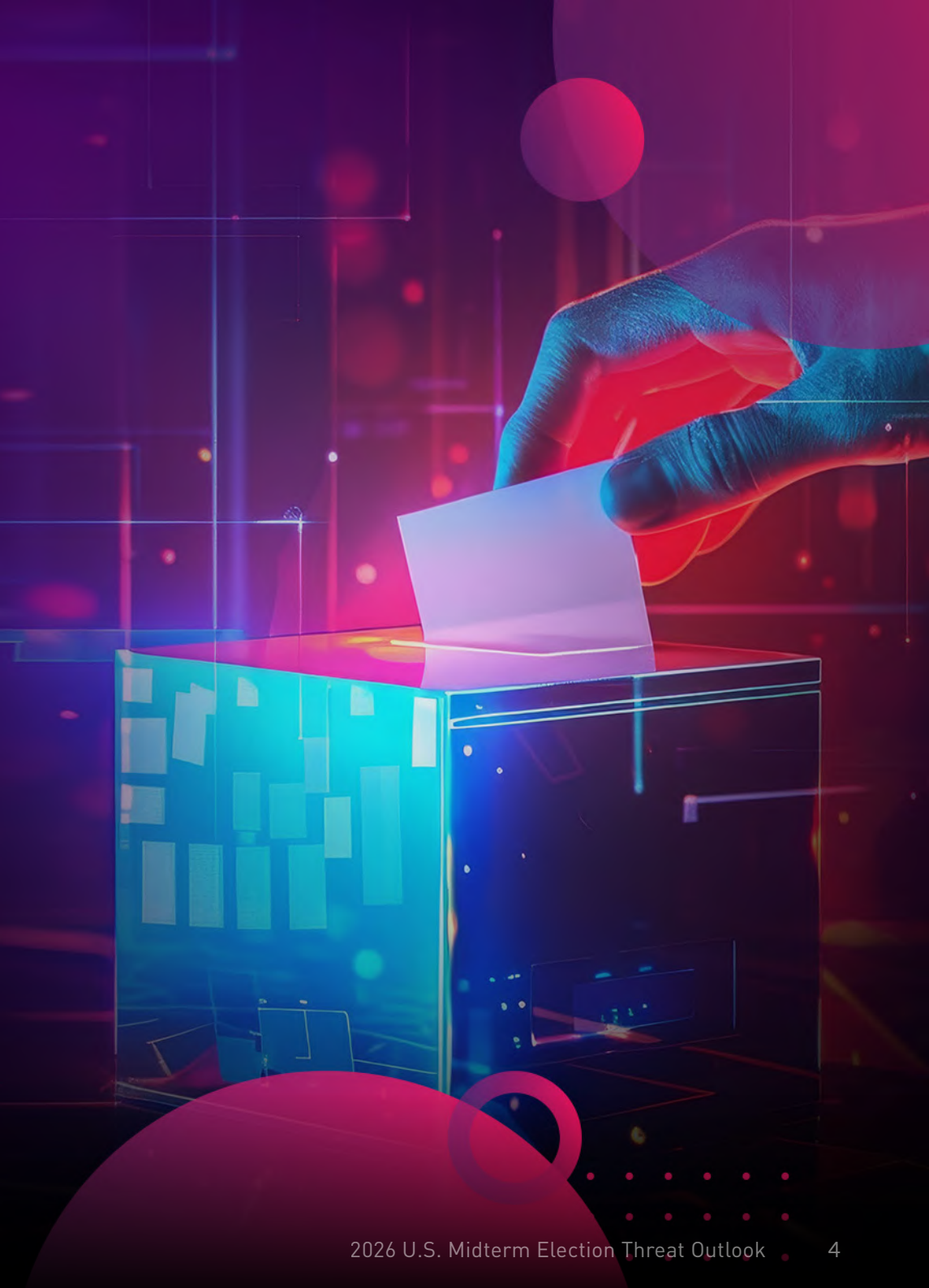
Check Point ERM identified sustained election-related infrastructure creation throughout early 2026. Continued registration of election-themed domains expanded the available infrastructure that may later support phishing, impersonation, fraudulent donation activity, misinformation, or abuse of election-related brands and services.

Credential exposure remained elevated across major political fundraising platforms and government-related assets, while election-related data and claims of voter-data exposure appeared on criminal forums, reinforcing continued interest in trusted platforms, public-sector data, and election-related information.
That same environment also favors AI-assisted phishing, deepfake video, cloned audio, manipulated imagery, and scalable impersonation content, all of which can accelerate election-related influence activity by lowering production costs and increasing the speed and scale of distribution.

DDoS and website defacement should also be treated as recurring but usually indirect election risks. They are unlikely to prevent voting or alter ballots, but they can interrupt access to information, damage trust, and amplify narratives about election insecurity.

Foreign interference remains part of the 2026 threat picture, with Russia, Iran, and China continuing to stand out as the principal state-linked actors in recent election cycles.

Overall, the most significant 2026 risks center on the trusted accounts, platforms, services, and information channels that election-related organizations rely on to operate and maintain public trust, with election-adjacent systems presenting the more immediate source of operational exposure.




Cloned Audio
DDOS
Media Manipulation
PHISHING
Coordinated misinformation
WEBSITE DEFACEMENT
DEEP FAKE
Impersonation
Abuse of Third Parties
Foreign Interference
CREDENTIAL EXPOSURE

2026 U.S. MIDTERM ELECTION THREAT OUTLOOK

The 2026 U.S. midterm elections are expected to expand the cyber threat environment across the systems, services, and organizations that support election-related activity, including campaigns, party committees, fundraising platforms, media organizations, government services, and the vendors and platforms that support them.

As political activity intensifies, the main operational risks tend to affect the systems used for fundraising, communications, public information, and other election-related services. In practice, attacks often target those supporting systems because they are easier to reach and can still create disruption, confusion, or reputational damage.

Organizations may be affected directly, through third-party providers, or through the systems they use to communicate with the public and handle politically relevant information. In practice, that often includes phishing lures and impersonation of trusted services that can mislead users, enable access, or damage credibility.

AI-assisted content and phishing increase this risk by making deception faster, cheaper, and easier to scale. Manipulated video, cloned audio, deceptive imagery, and more convincing phishing lures can make false content harder to verify and help misleading material spread more quickly across election-related organizations.

Check Point's 2026 Cyber Security Report found that 82 percent of malicious file attacks were delivered by email, reinforcing that email remains a major delivery channel for phishing and other malicious lures across election-related organizations[3].

PAST ELECTION THREATS

Recent U.S. election cycles show that the same broad threat categories continue to recur, even as tactics continue to evolve. For a 2026 midterm assessment, the 2022 midterms provide the closest historical comparison by election type, while the 2024 presidential election shows how those same risks scaled during a larger national cycle.

2022 Midterm Elections

The 2022 midterm elections showed that election-related cyber activity could affect the broader election environment without directly disrupting voting or vote counting.

Google Project Shield reported a fourfold increase in weekly DDoS attacks during the second half of 2022, with especially sharp targeting of sites that identified themselves as providing election monitoring and public information [19].

Google also reported that attacks on election-information sites rose sharply beginning in August 2022 and continued through mid-December, while candidate websites saw a similar increase before dropping quickly after Election Day [19].

Phishing was also a practical threat during the 2022 cycle. In the three months leading up to the midterms, Cloudflare processed more than 20 million emails for campaigns, election officials, and supporting public organizations, and blocked around 150,000 phishing attempts before they reached campaign inboxes [2].

Influence activity was also visible during the 2022 midterms. Mandiant reported that the PRC-linked DRAGONBRIDGE campaign aggressively targeted U.S. interests during the period, including efforts to discourage Americans from voting while using personas that posed as members of the target audience to push politically themed content [21].

The 2022 midterms showed how risk played out through disruption of public information, phishing activity, and influence operations across the broader election environment.

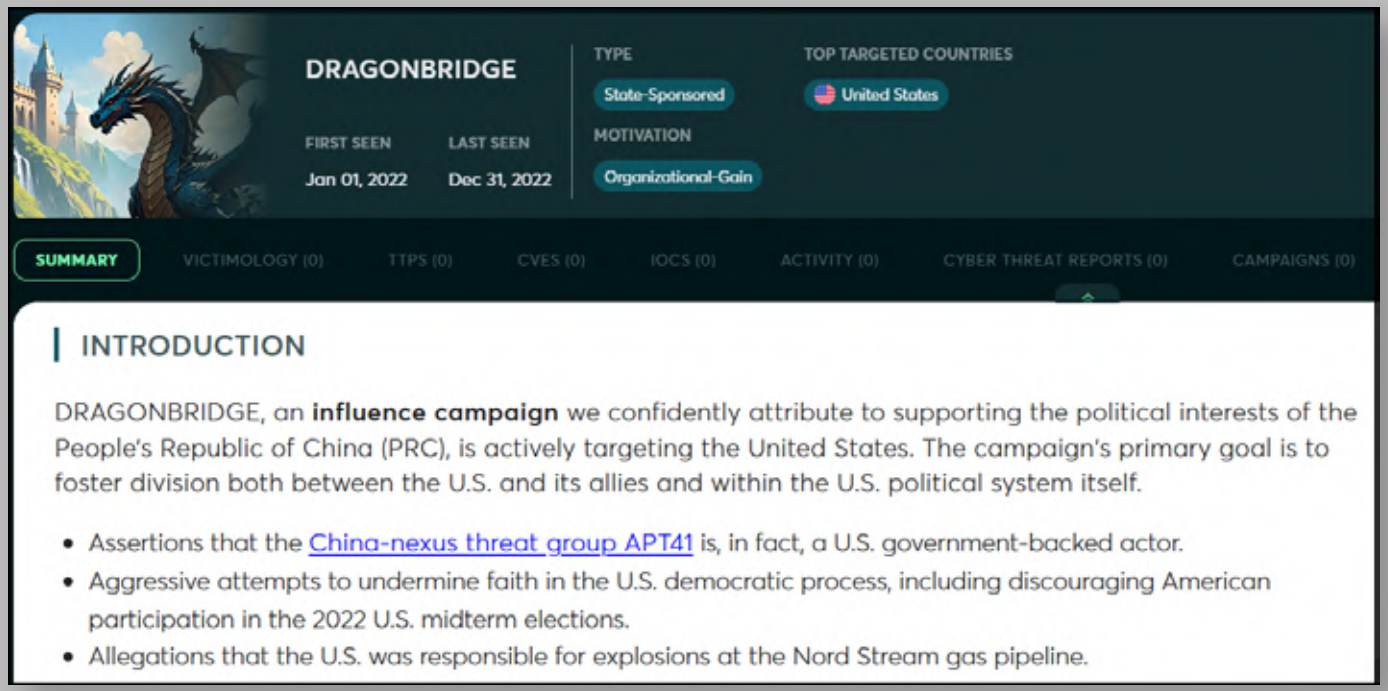


Figure 1: Check Point Exposure Management's DRAGONBRIDGE campaign page.

2024 Presidential Elections

The 2024 presidential election showed how election-related cyber risk scaled during a larger national cycle, especially through influence operations, impersonation infrastructure, and disruption of public-facing systems.

Justice Department materials described a coordinated influence effort that used written narratives, memes, and edited video content to respond quickly to political developments.[13]

Russian-linked influence operations during the 2024 cycle also relied on cloned media infrastructure and lookalike domains designed to imitate major outlets, extending the reach and credibility of false or manipulated political content. [11,12]

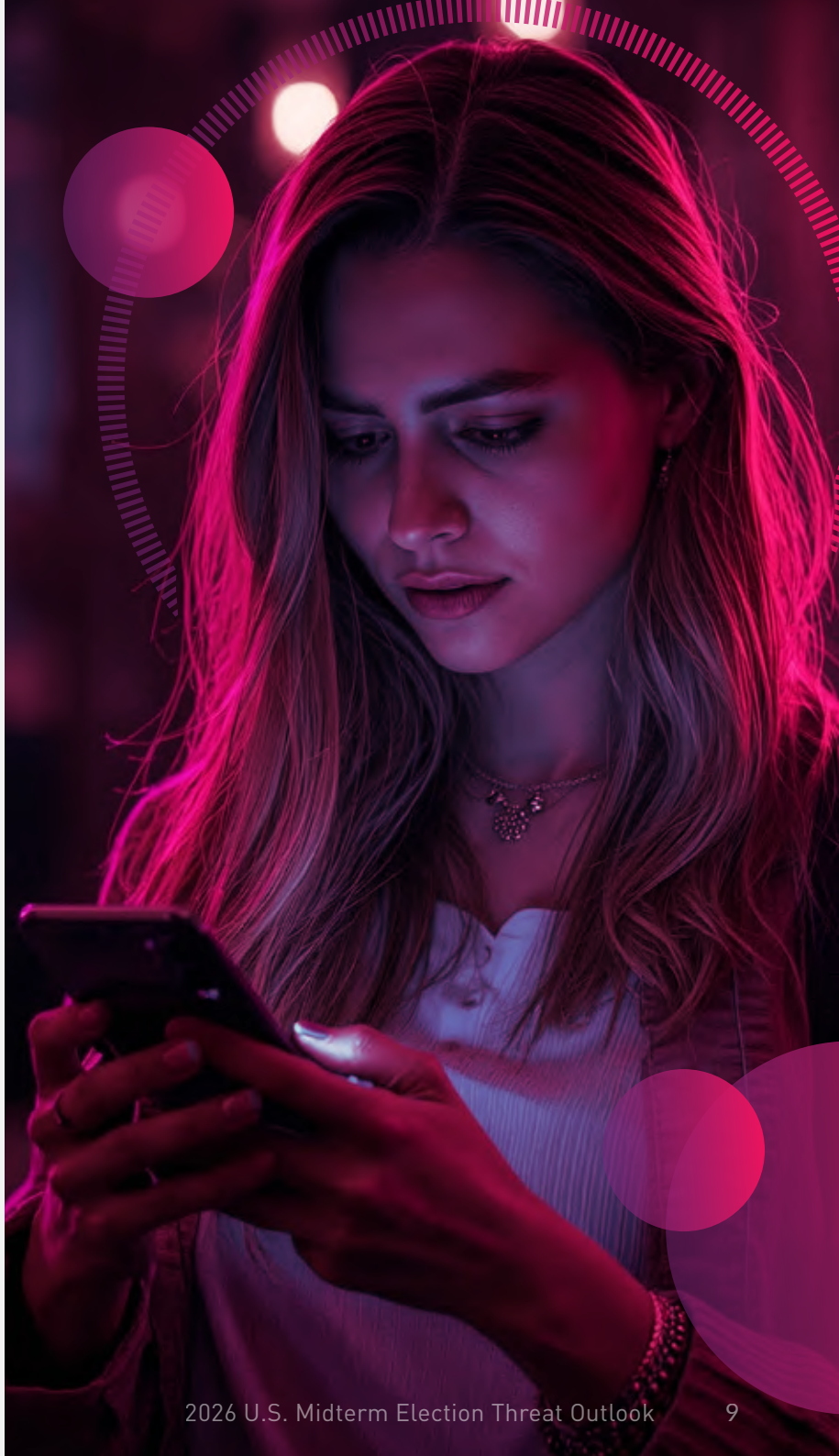
Iranian-linked activity was also visible during the 2024 cycle. Microsoft reported that Mint Sandstorm compromised a U.S. political operative's personal account and used that access for spear phishing against campaign personnel. Microsoft also reported that Cotton Sandstorm sent threatening emails while impersonating the Proud Boys, and that Peach Sandstorm accessed county government accounts in swing states.[14]

Chinese activity remained focused largely on covert influence and reconnaissance. Microsoft described large networks of fake social media accounts posing as U.S. voters while amplifying divisive political narratives and testing audience response to election-related themes.[17]

Public-facing disruption also intensified during the 2024 election cycle. Cloudflare reported blocking more than six billion malicious HTTP requests targeting election-related infrastructure during a six-day period around the election. Peak attacks reached approximately 700,000 requests per second, and systems protected under the Athenian Project saw approximately 290 million malicious requests beginning September 1, 2024 [1].

Cloudflare and the FBI indicated that this activity did not prevent voting, alter ballots, or interfere with vote counting[1,16]. It mainly disrupted access to public information and fueled claims about election insecurity.

The 2024 cycle showed how influence activity, impersonation infrastructure, and public-facing disruption could operate at the same time and at a greater scale than in earlier election periods.



CURRENT ELECTION THREATS

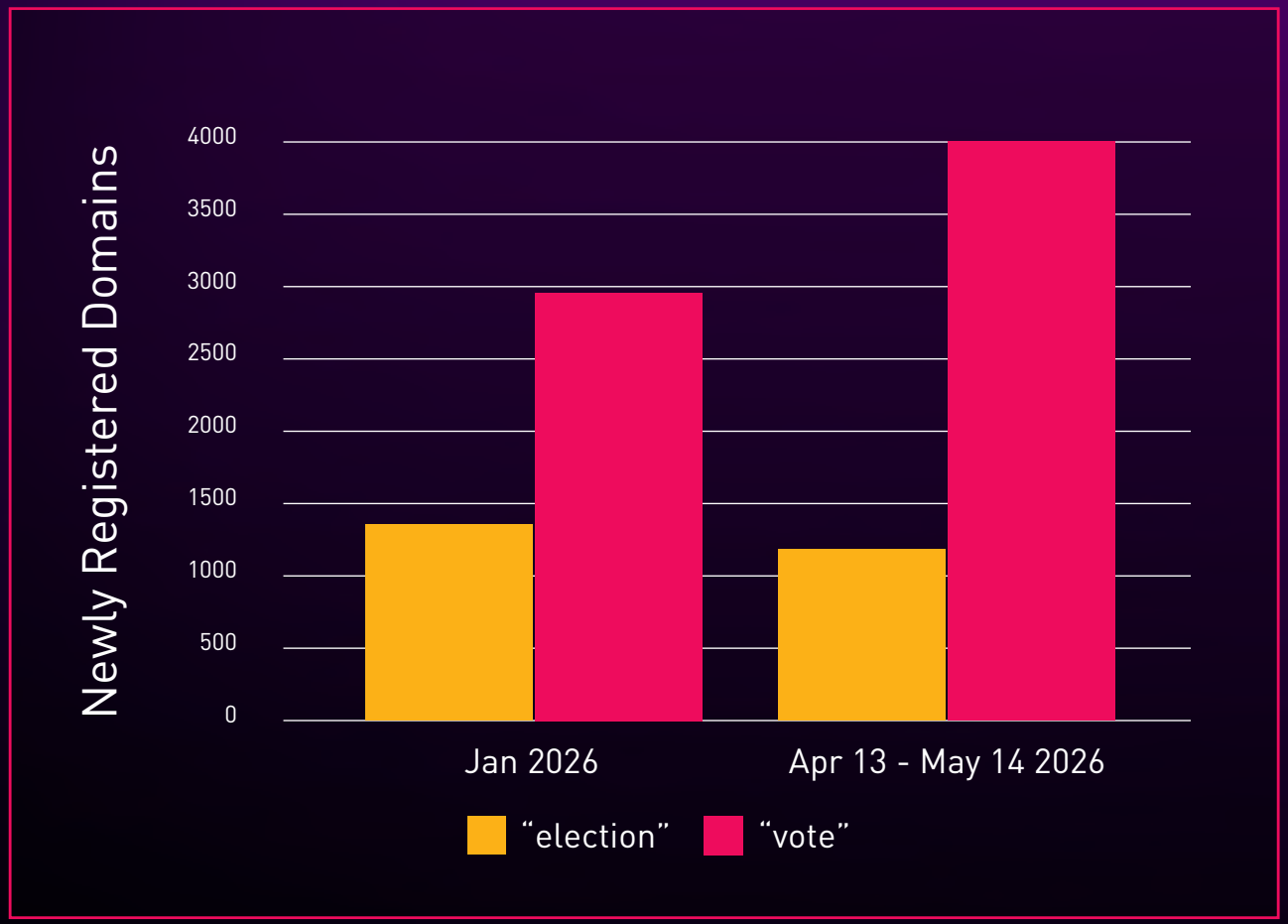
Current reporting indicates that several threats relevant to the 2026 election cycle are already being seen. Infrastructure monitoring, credential exposure, darkweb activity, and reporting on recent election activity help show where risk is increasing and how it may be used in the 2026 midterm elections.

The primary categories at this stage include election-themed infrastructure development, credential exposure, phishing, influence operations, manipulated media, and disruption of public-facing systems.

Election-related Domain Activity

Domain registrations tied to election-related terms remain relevant because they can point to infrastructure that may later be used for phishing, impersonation, fraud, misinformation, or influence activity.

The increase in "vote"-related registrations indicates continued growth in election-related domain activity as the midterm cycle approaches. The registrations do not, by themselves, establish malicious intent, but they increase the pool of domains that may later be used for phishing, impersonation, fraudulent donation activity, or the distribution of misinformation.



Check Point Exposure Management identified continued registrations of domains containing election-related terms throughout early 2026.

In January 2026, approximately 1,300 newly registered domains contained the keyword "election," and approximately 2,957 contained "vote." Between April 13 and May 14, 2026, approximately 1,140 newly registered domains contained "election," and approximately 4,010 contained "vote."

Figure 2: Election-Related Domain Registrations in 2026.

Credential Exposure

Citizens' credential exposure remains relevant because compromised accounts can support social engineering, phishing, account takeover, donor fraud, and unauthorized access across election-related organizations.

The clearest concentrations of leaked credentials currently involve shared fundraising platforms, party assets, and government-related services. Check Point Exposure Management observed exposure status in May 2026, including:

- ActBlue.com (Democrats Fundraise): approximately 9,500 leaked credentials
- WinRed.com (Republicans Fundraise): approximately 6,500 leaked credentials
- gop.com (Republicans' Official): approximately 600 leaked credentials
- democrats.org (Democrats' Official): approximately 130 leaked credentials
- usa.gov (Citizens' Services): approximately 150 leaked credentials

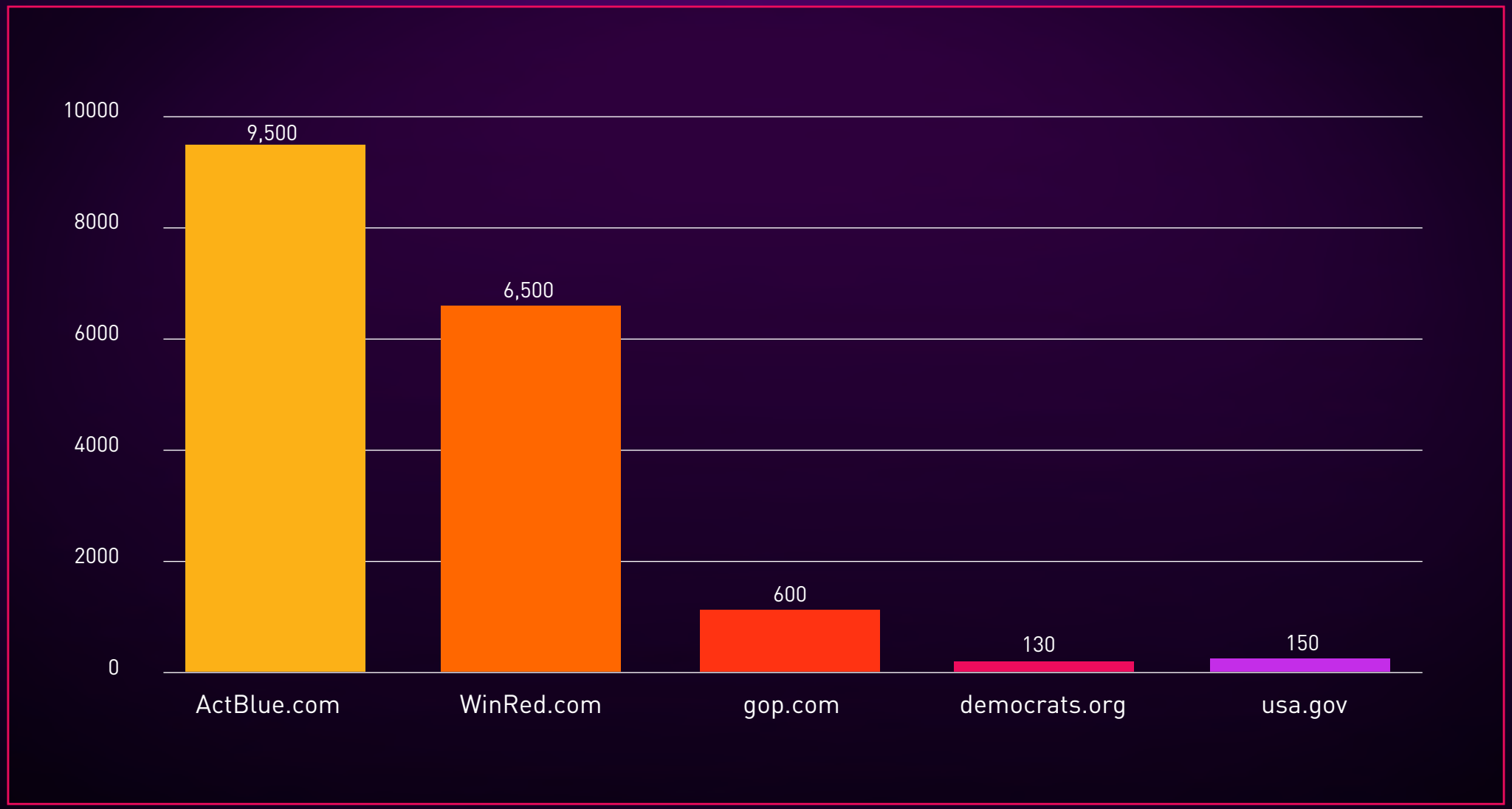


Figure 3: Election-Related Leaked Credentials Exposure for May 2026.

Individual political campaign domains showed little to no observed credential exposure across a sample of swing-state candidates from both major political parties, reinforcing that current exposure is concentrated in centralized platforms rather than campaign-specific infrastructure. A single campaign domain stood out as an exception, with around 90 leaked credentials identified.

Darkweb and Forum Activity

Election-related data exposure is already appearing across criminal forums and underground communities in 2026. Check Point Exposure Management identified a January 30, 2026, BreachForums post advertising data tied to fremontcountyelectionsco.gov, including names, email addresses, IP address data, and election-related portal submission information.

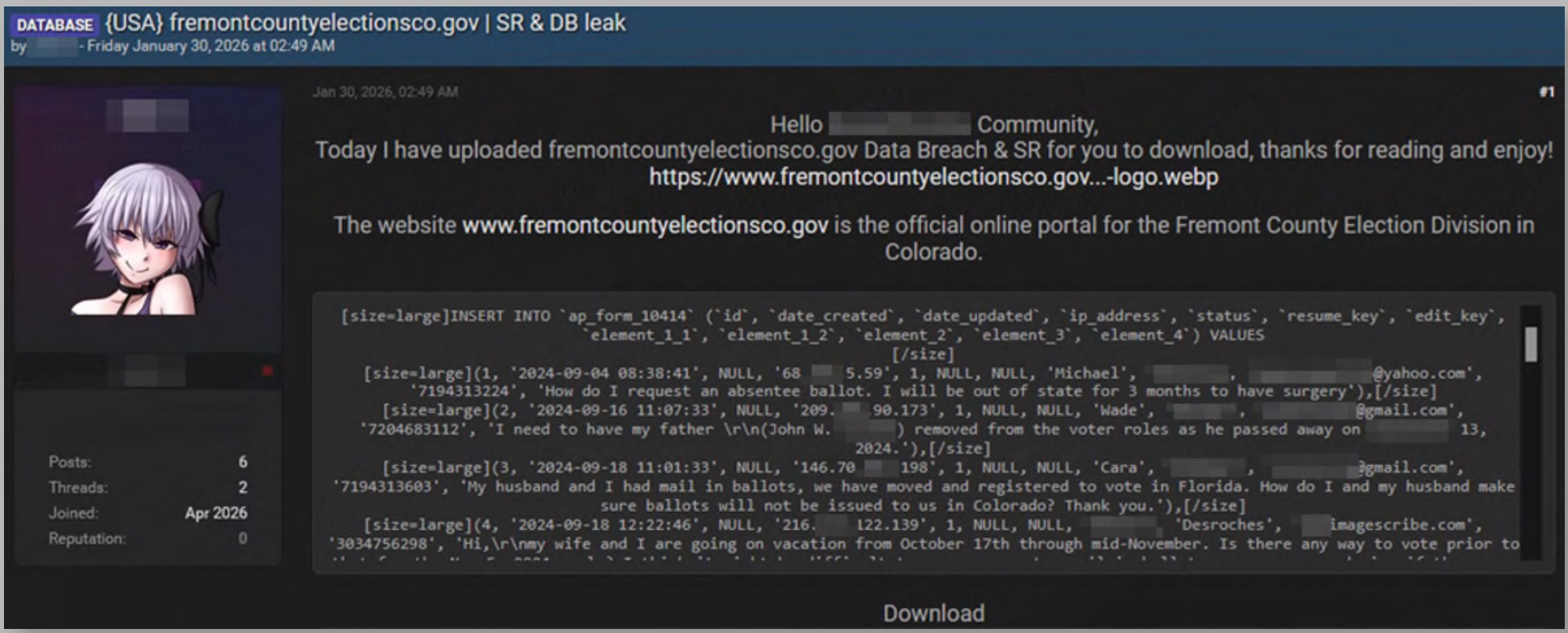


Figure 4: Breached Fremont County elections data published for free.

Check Point Exposure Management also identified an April 26, 2026, post on Spear[.]cx, a criminal forum, claiming to offer a multi-state U.S. voter database covering more than two dozen states and Washington, D.C. The claim reinforces continued criminal interest in election-related data and voter information.

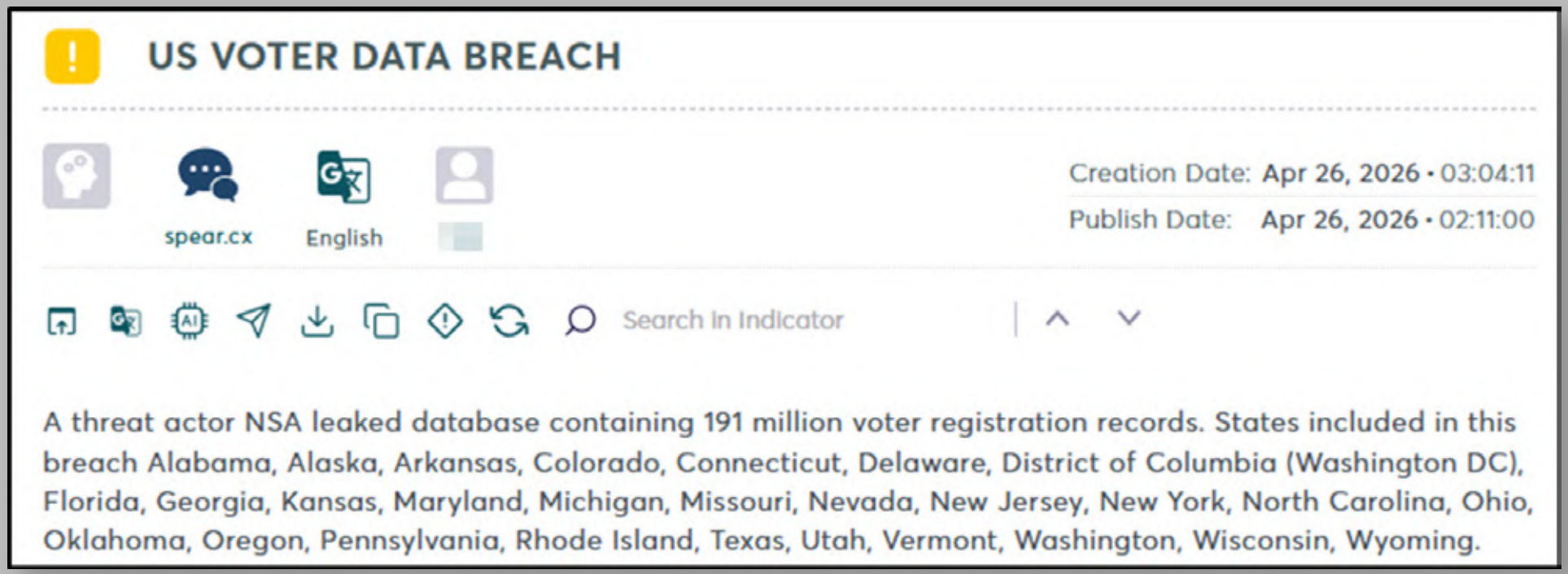


Figure 5: US-Voters' data breach post as detected by Check Point's Exposure Management.

Even where breach claims cannot be independently confirmed, datasets circulating on criminal forums and darkweb marketplaces may still support phishing, impersonation, fraud, harassment, or misinformation, particularly when timed around politically sensitive events.

These incidents reinforce a recurring risk throughout election cycles: localized breaches or exposure affecting election-related systems can generate disproportionate reputational and political impact even where operational consequences remain limited.

Phishing

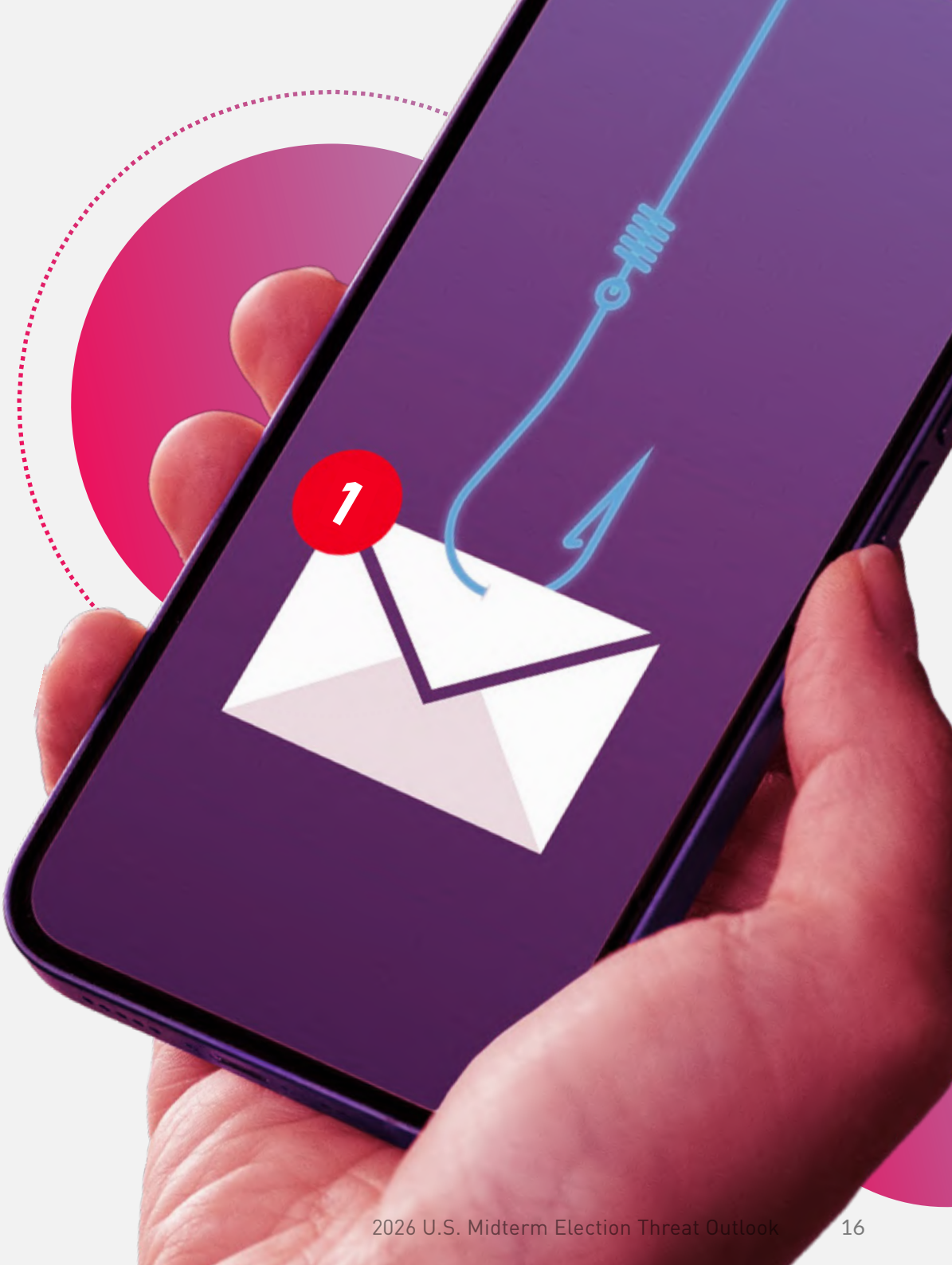
Phishing remains one of the most likely operational threats surrounding the 2026 election cycle due to its scalability, low cost, and consistent effectiveness against politically exposed organizations.

Campaign staff, consultants, journalists, donors, vendors, election officials, and politically affiliated organizations all remain viable targets for credential theft, donor fraud, account takeover, and intelligence collection.

Check Point Research reported that one in every 10 newly registered tax-related domains in March 2026 was flagged as malicious or suspicious, highlighting how quickly time-sensitive public themes and government impersonation can be converted into credential-harvesting infrastructure.[4]

In April 2026, the Federal Voting Assistance Program (FVAP) warned of a phishing campaign impersonating FVAP.gov through fraudulent newsletter emails and malicious links.[5]

This demonstrates how trusted government election services may be directly leveraged as phishing lures during politically sensitive periods.



AI-Generated Content

AI-generated content is already shaping the 2026 election threat landscape. Its operational value is clear: it lowers production costs, accelerates content creation, improves impersonation quality, and enables influence activity to scale more rapidly than in previous election cycles.

Earlier reporting tied Russian influence actor Storm-1516 to staged or AI-generated political content that achieved significant engagement after spreading through mainstream platforms, with several videos generating millions of views.[15]

This pattern is continuing into 2026. Reuters reported in March 2026 that AI-generated campaign content had become increasingly visible, including an NRSC advertisement featuring Texas State Representative James Talarico and a separate deepfake campaign targeting Senator Jon Ossoff.[6]

Reuters also noted that disclosure requirements and enforcement standards remain inconsistent, increasing the likelihood that manipulated political content will continue to circulate widely even where technical labeling requirements exist.[6]

The impact of AI-generated content extends beyond campaign content. The same capabilities can support phishing lures, impersonation attempts, multilingual propaganda, and large-scale misinformation campaigns, increasing both the speed and scale of election-related influence activity.

ELECTION INTERFERENCE ACTIVITY

Election interference activity surrounding recent U.S. election cycles has remained concentrated among a small group of state-linked foreign actors, most notably Russia, Iran, and China. Across multiple election periods, these actors have relied on a relatively consistent mix of phishing, influence operations, impersonation infrastructure, reconnaissance, hack-and-leak activity, and public-facing disruption to shape narratives, collect intelligence, and undermine trust in election-related systems.

Current U.S. government reporting continues to support the expectation of foreign election interference in 2026. In April 2026 testimony before the Senate Armed Services Committee, Army General Joshua Rudd stated that foreign interference should be expected based on patterns observed during previous election cycles[22], reinforcing the likelihood that state-linked activity from Russia, Iran, and China will remain operationally relevant throughout the current cycle.

Russia

Russian-linked election activity continues to combine cyber intrusion, influence operations, impersonation infrastructure, and coordinated propaganda distribution.

By 2024, Russian activity shifted more heavily toward scalable influence operations designed to shape narratives, amplify division, and undermine trust in political institutions and election processes.

The Good Old USA campaign relied on coordinated advertising, influencer engagement, edited video content, and large-scale social media amplification across Facebook, Instagram, YouTube, X, and Reddit. Justice Department materials described a coordinated influence effort that used written narratives, memes, and edited video content to react quickly to political developments [13].

Russian-linked Doppelganger operations further expanded the use of cloned media infrastructure and cybersquatted domains designed to imitate major organizations, including Reuters, The Washington Post, and Fox News. The operation relied on fake personas, AI-assisted content, paid amplification, and article-specific links intended to appear legitimate while avoiding routine detection [11,12].

Microsoft additionally identified Russian influence actors, including Storm-1516, Volga Flood, and Storm-1679, distributing staged or deceptively edited political content designed to amplify distrust, deepen polarization, and increase narrative confusion during politically sensitive periods.[15]

Based on prior trends, Russian-linked election activity entering 2026 is likely to continue focusing on influence operations, impersonation, public-facing disruption, and narrative amplification.[13,15]

China

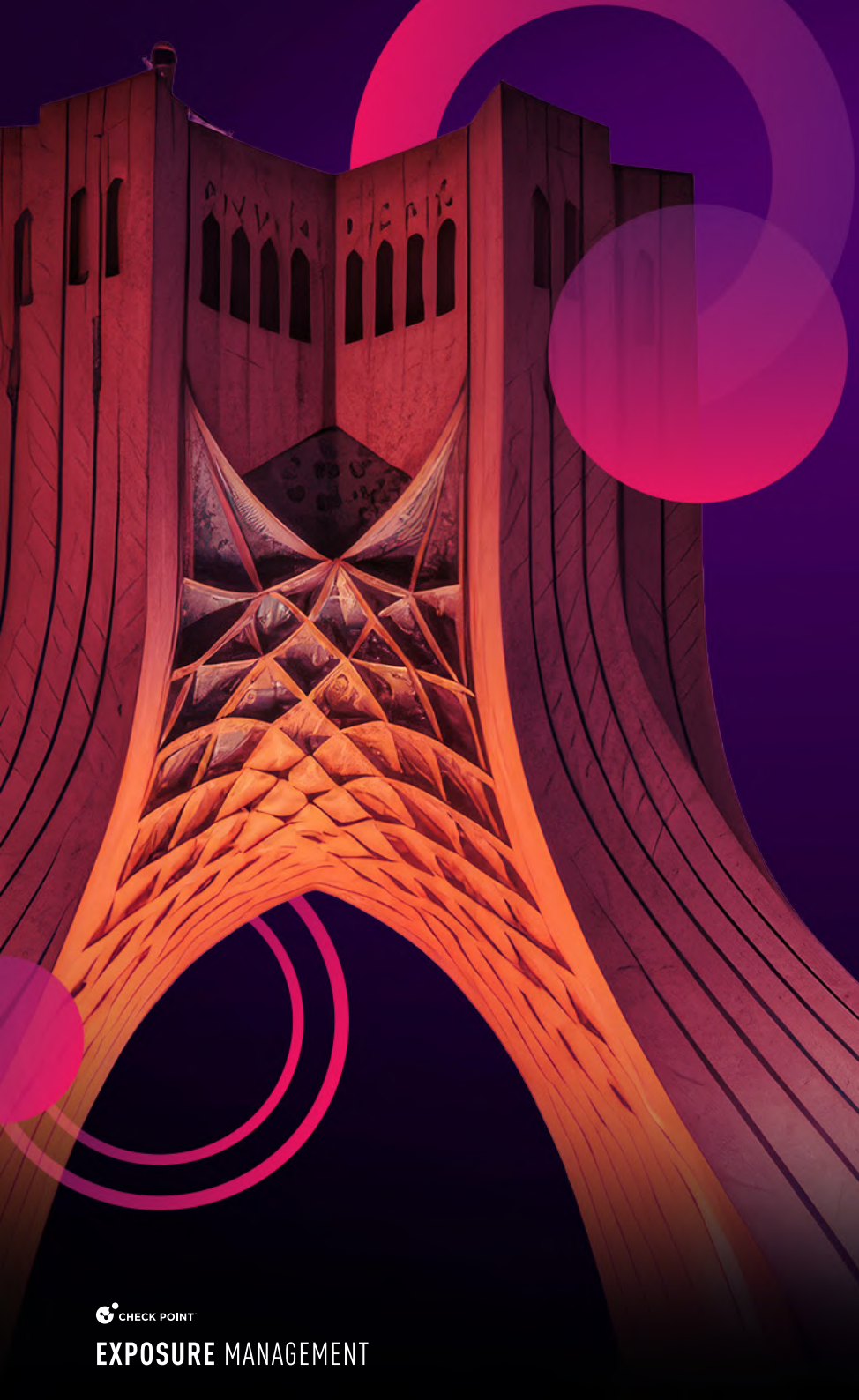
Chinese-linked election activity has historically centered on reconnaissance, covert influence, and access to politically relevant networks rather than overt disruption.

Previous reporting linked Chinese intrusion activity to targeting of political organizations, foreign-policy entities, and U.S. state government networks through exploitation of internet-facing systems and known vulnerabilities.

Chinese-linked influence activity also remained visible throughout the 2022 and 2024 election cycles. DRAGONBRIDGE operations used inauthentic personas posing as U.S. voters while amplifying divisive narratives tied to inflation, labor unrest, abortion rights, and political polarization [17].

Microsoft also reported that covert Chinese account networks posed as U.S. voters, tested politically divisive narratives, and monitored audience response to election-related themes across social platforms [17].

Chinese-linked election activity appears more focused on reconnaissance, influence testing, and narrative analysis than on direct election disruption. The broader pattern is less about immediate voter persuasion and more about understanding, amplifying, and exploiting existing social and political divisions.



Iran

Iranian-linked election activity has historically combined intrusion activity, intimidation campaigns, reconnaissance, and influence operations.

Iranian activity remained operationally relevant during the 2024 presidential election. Microsoft reported that Mint Sandstorm compromised a U.S. political operative's personal account and used that access for spear phishing targeting campaign personnel.[14]

Cotton Sandstorm conducted reconnaissance and limited probing of election-related infrastructure in battleground states, while Peach Sandstorm reportedly accessed county government accounts associated with swing-state infrastructure.[14]

In September 2024, the Justice Department announced charges against three IRGC-linked cyber actors tied to a hack-and-leak operation targeting the Trump campaign.[12]

Based on patterns observed during prior election cycles, Iranian-linked actors have combined reconnaissance, voter-data targeting, and spoofed intimidation campaigns designed to create confusion and amplify distrust surrounding election activity.

The ongoing Israel-Iran conflict also remains relevant to the 2026 threat environment, as periods of regional tension can increase the likelihood of Iranian-linked cyber activity affecting U.S. political or public-sector organizations.

MUNICIPAL ELECTIONS

Municipal and local election environments remain relevant to the broader election threat landscape because they often operate with fewer resources, smaller security teams, older technology, and lower visibility than state or federal systems.

These environments are more exposed to opportunistic intrusion, ransomware, credential compromise, and third-party risk, particularly where public-facing systems or election-adjacent services are involved. Even when election operations are not directly affected, disruption at the local government level can still create confusion, delay public communications, and undermine confidence during politically sensitive periods.

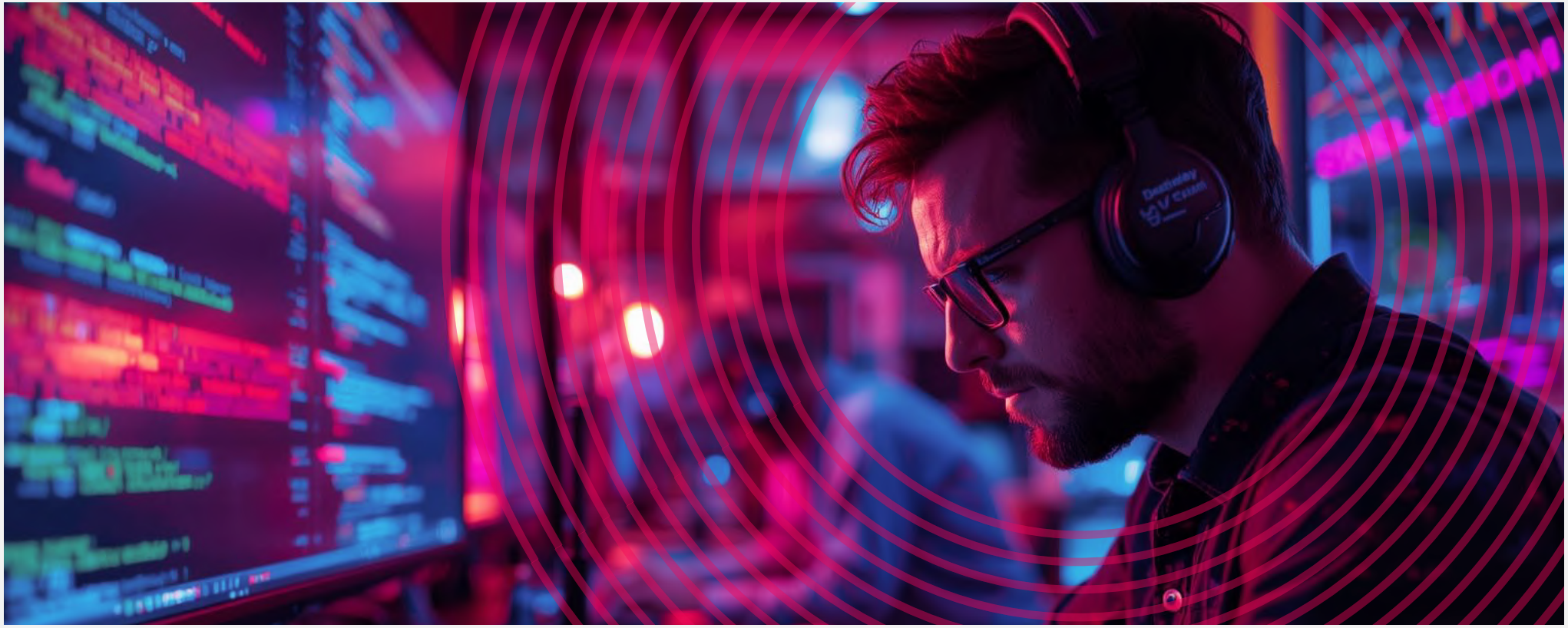
Municipal Ransomware Activity

Recent ransomware incidents involving U.S. municipalities continue to demonstrate how quickly local government operations can experience disruption following compromise.

In January 2026, Winona County, Minnesota, declared a local emergency following a ransomware incident affecting county systems, phone lines, and records-related functions. Emergency services reportedly remained operational while outside forensics and law enforcement supported containment and recovery efforts.[23]

In March 2026, Foster City, California, similarly declared a local emergency after a ransomware attack forced portions of municipal infrastructure offline and disrupted non-emergency city services.[24]

Neither incident appeared directly tied to election operations. However, both illustrate how ransomware affecting local governments can still create operational disruption in the broader election environment, especially where public communications, records systems, or election-related services are involved.



GENERAL LOOK AHEAD

Looking ahead to 2026, the most likely risks are those that have remained consistent across recent election cycles and continue to scale effectively against election-adjacent organizations. The primary concerns are phishing, credential theft, impersonation, third-party exposure, public-facing disruption, misinformation, AI-assisted abuse, and ransomware affecting local or adjacent infrastructure.

Phishing and Credential Theft

Phishing is likely to remain the most persistent election-related threat in 2026 because it is inexpensive, adaptable to political events, and consistently effective against campaign staff, consultants, donors, vendors, journalists, election officials, and public-sector personnel.

Check Point's 2026 Cyber Security Report found that 82 percent of malicious file attacks were delivered by email. The same research also found that Microsoft accounted for 22 percent of observed brand impersonation attempts in Q1 2026, reinforcing the continued use of trusted brands and fake login pages to support credential theft.[3]

Cisco Talos reported that phishing re-emerged as the top initial access vector in Q1 2026, accounting for more than one-third of engagements where initial access could be determined[9]. For election-related organizations, this reinforces the likelihood that email-based intrusion, fake login portals, SMS lures, malvertising, and deceptive web infrastructure will remain primary access paths.

Infostealer activity adds to this risk by increasing the volume of exposed credentials available for reuse, resale, or social engineering. Mandiant reported that stolen credentials from infostealer operations accounted for 16 percent of investigations, making them the second-highest initial infection vector in the reviewed dataset.[10]

That exposure can then directly support unauthorized access or enable phishing and other social engineering activities.
Third-party exposure remains a significant risk because election-related organizations depend on shared vendors, SaaS platforms, consultants, cloud services, payment processors, and communications providers to operate at scale.

Black Kite's 2026 Third-Party Breach Report found that each vendor breach in 2025 led to an average of 5.28 downstream publicly compromised organizations, illustrating how a single trusted provider can create cascading exposure across multiple customers[8].

Trusted vendors and shared platforms can create indirect access to political organizations, public-sector entities, fundraising infrastructure, and other election-related services.

DDoS and Public-facing Disruption

Public-facing disruption remains a recurring election-period risk. DDoS activity is unlikely to prevent voting or alter ballots, but it can still interrupt access to election information, create confusion, and amplify narratives about election insecurity.

Cloudflare's 2026 Threat Report noted that the company blocks more than 230 billion threats per day across its network, underscoring the broader attack environment in which election-related organizations operate.[18]

Website defacement is less common than denial-of-service activity but can still generate reputational damage and public concern. In June 2025, Arizona's statewide online candidate portal was defaced and candidate photographs were replaced with images of Ayatollah Ruhollah Khomeini, the former supreme leader of Iran. State officials said voter registration and segmented election systems were not affected, but the incident showed how visible compromise of an election-facing public system can draw outsized attention and fuel confusion during a politically sensitive period.[19]

Misinformation and Impersonation

Misinformation and impersonation are likely to remain central to the threat environment in the 2026 election. False narratives are more persuasive when they are delivered through cloned brands, fake personas, deceptive domains, and coordinated amplification that make misleading content appear legitimate during fast-moving political events.

Check Point Research reported that Microsoft accounted for 22 percent of all brand impersonation attempts in Q1 2026, while the top four impersonated brands together represented nearly half of the observed phishing activity[3]. The same approach can be adapted to election-related login portals, donation requests, public notices, media-branded content, and voter information pages.

Prior influence operations also showed persistent interest in swing states and closely contested jurisdictions, where limited narrative reach or localized confusion can still have outsized political and media impact. In 2026, this makes competitive races, high-profile candidates, election-related organizations, and local media ecosystems especially relevant targets for misinformation and impersonation activity.

AI-assisted Threats

AI-assisted threats are likely to expand further in 2026 because they make election-related deception faster, cheaper, and easier to scale. The same tools can support manipulated political content, impersonation, phishing lures, and other influence activity across the broader election environment.

Check Point's 2026 Cyber Security Report found that AI is increasingly embedded across the attack lifecycle, including reconnaissance, social engineering, and operational decision-making.[3]

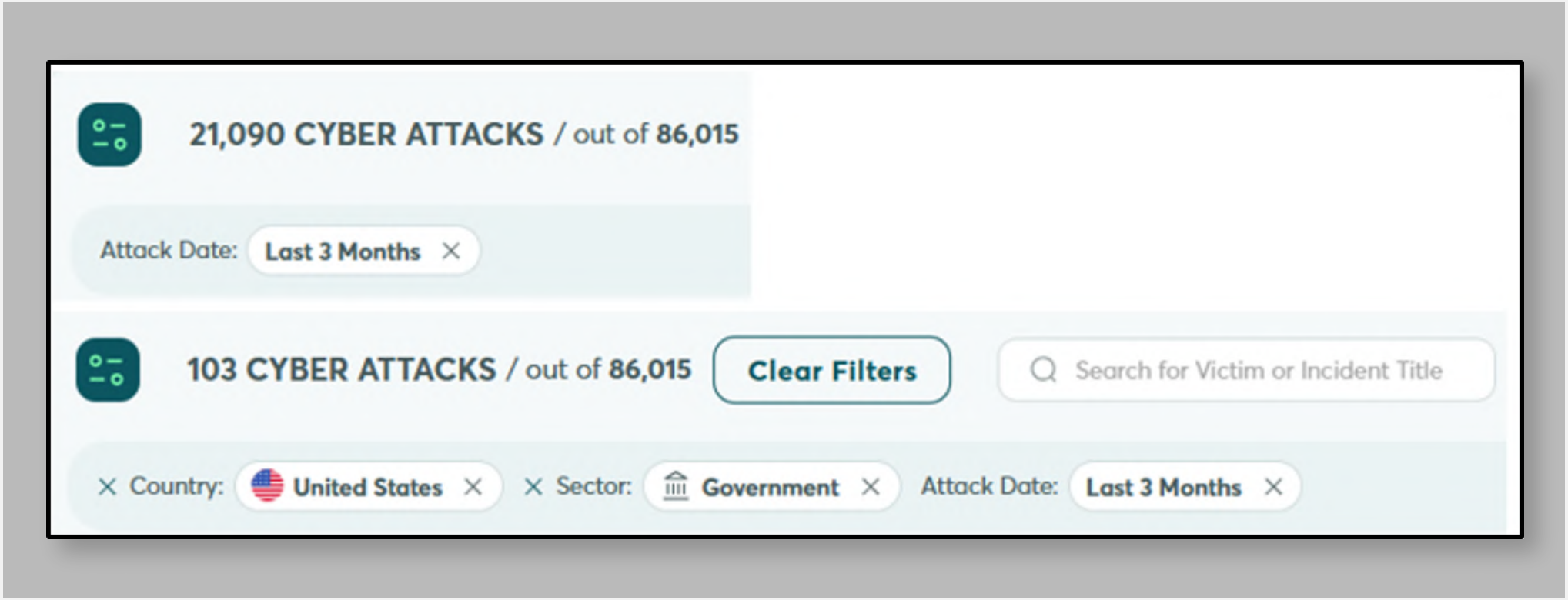
In election-related activity, these capabilities make phishing, impersonation, and influence content faster to produce, easier to tailor, and harder to dismiss. As these tools become easier to use, deceptive content can also be adapted more quickly across multiple channels.

Ransomware and Extortion

Ransomware and extortion are still relevant to the broader election environment, particularly for local governments, public-facing services, vendors, and other politically adjacent organizations.

Ransomware activity stayed elevated in Q1 2026, with 2,122 victims posted on ransomware data leak sites, making it the second-highest first quarter on record. The ecosystem also became more concentrated: the top 10 groups accounted for 71 percent of victims, Qilin was the most active operation with 338 victims, and LockBit re-entered the top tier with 163 victims.[25]

Check Point Research tracked more than 70 active ransomware leak sites during the quarter, with an average of roughly 700 victims posted per month.26 Over the 3-month period from March through May 2026, Check Point ERM tracked 21,090 cyberattacks globally, including 103 in the U.S. government sector.



These figures do not indicate that election systems are a primary ransomware target. Instead, they reinforce the risk that disruption affecting local governments, public services, vendors, or other election-related organizations could still create confusion, leverage, or reputational harm during the election cycle.

CONCLUSIONS

The 2026 U.S. midterm election threat environment centers on the systems and services that surround the election process, especially the accounts, platforms, services, and information channels that campaigns, donors, voters, media, and public institutions rely on to communicate, operate, and maintain trust. Direct attacks on voting technology remain a concern, but the more immediate pressure is on the systems around it.

Phishing and credential theft, impersonation, influence activity, AI-generated deception, public-facing disruption, third-party exposure, and ransomware affecting local or adjacent infrastructure are the most persistent themes entering 2026. New domain registrations tied to election-related terms, continued credential exposure across trusted platforms, activity on darkweb and criminal forums involving election-related data, and foreign interference tied primarily to Russia, Iran, and China point in the same direction.

Compromise of election-related infrastructure is likely to be more significant than direct attacks on voting systems themselves. Current reporting does not point to widespread destructive activity against vote counting or election result processing, but it does show persistent pressure on fundraising platforms, public websites, donor and campaign accounts, government services, media channels, vendors, and local government systems that can be used to create confusion, reputational harm, or political leverage.

The clearest concern entering 2026 is not a single technical failure but the cumulative effect of compromise, impersonation, disruption, and manipulation across the systems people rely on for election information and public trust.

RECOMMENDATIONS

The following recommendations address the forms of compromise, disruption, impersonation, and confusion most likely to affect election-related systems, services, and communications in 2026.

Protect trusted accounts and core services.

- Treat email, public websites, donation systems, administrative portals, and other highly trusted services as priority assets, and review who can access or change them.
- Require phishing-resistant MFA for high-trust accounts and separate privileged access from routine use wherever possible.
- Tighten email security controls so phishing and impersonation are harder to deliver, including stronger attachment and link protections, domain authentication, and review of suspicious forwarding or mailbox-rule changes.
- Review where reused passwords, exposed credentials, unmanaged devices, or infostealer activity could create follow-on access to email, cloud services, or other sensitive systems.

Protect public information and communication channels.

- Keep official communications consistent and easy to recognize, and decide in advance how urgent updates, public notices, and operational changes will be announced.
- Plan for disruption in public-facing systems by preparing alternate communication methods and verified fallback channels before they are needed.
- Monitor for suspicious domain registrations, impersonation activity, and exposed credentials early, especially when they involve trusted brands, public information channels, or election-related services.
- Be prepared to correct impersonated messages, deceptive pages, manipulated content, or misleading public information quickly once it begins to circulate.

Reduce shared exposure and improve early response.

- Review dependence on vendors and shared platforms, especially where a single provider supports communications, fundraising, administration, or public operations.
- Decide in advance who verifies unusual information, who communicates publicly, and how suspicious activity is escalated so technical disruption and trust-related incidents can be addressed quickly.

REFERENCES

[1] Cloudflare Blog. "Exploring Internet traffic shifts and cyber attacks during the 2024 US election." https://www.blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/

[2] Cloudflare Blog. "How Cloudflare helps secure the inboxes of democracy." https://blog.cloudflare.com/securing-the-inboxes-of-democracy/

[3] Check Point Research. "Cyber Security Report 2026." https://research.checkpoint.com/2026/cyber-security-report-2026/

[4] Check Point Research. "Tax Season 2026: How Cyber Criminals Are Preparing Their Attacks Months in Advance." https://blog.checkpoint.com/research/tax-season-2026-how-cyber-criminals-are-preparing-their-attacks-months-in-advance/

[5] Federal Voting Assistance Program. "Phishing Campaign Impersonating FVAP.gov." https://www.fvap.gov/info/news/2026/4/29/phishing-campaign-impersonating-fvapgov

[6] Reuters. "AI deepfakes blur reality in 2026 U.S. midterm campaigns." https://www.aol.com/articles/ai-deepfakes-blur-reality-2026-100554748.html

[7] CISA. "CISA Releases Security Advisory on Dominion Voting Systems Democracy Suite ImageCast X." https://www.cisa.gov/news-events/alerts/2022/06/03/cisa-releases-security-advisory-dominion-voting-systems-democracy-suite-imagecast-x

[8] Black Kite. "2026 Third-Party Breach Report." https://blackkite.com/reports/third-party-breach-report-2026

[9] Cisco Talos. "IR Trends Q1 2026: Phishing reemerges as top initial access vector, as attacks targeting public administration persist." https://blog.talosintelligence.com/ir-trends-q1-2026/

[10] Mandiant. "M-Trends 2025: Data, Insights, and Recommendations From the Frontlines." https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/

[11] Qurium. "Exposing the Evil Empire of Doppelganger Disinformation." https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/

[12] U.S. Department of Justice. "United States v. Certain Domains." https://www.justice.gov/archives/opa/media/1366261/dl

[13] U.S. Department of Justice. "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Campaign." https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; https://www.justice.gov/archives/opa/media/1366201/dl

[14] Microsoft Threat Intelligence. "Iran steps into US election 2024 with cyber-enabled influence operations." https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

[15] Microsoft Threat Intelligence. "Microsoft Elections Report 4 on Russian Influence." https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf

[16] FBI / IC3. "DDoS Attacks: Could Hinder Access to Election Information, Would Not Prevent Voting." https://www.ic3.gov/PSA/2024/PSA240731

[17] Microsoft Threat Intelligence. "China tests US voter fault lines and ramps AI content to boost its geopolitical interests." https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

[18] Cloudflare. "Cloudflare 2026 Threat Intelligence Report: Nation-State Actors and Cybercriminals Shift from 'Breaking In' to 'Logging In'." https://www.cloudflare.com/press/press-releases/2026/cloudflare-2026-threat-intelligence-report-nation-state-actors-and/

[19] CyberScoop. "After website hack, Arizona election officials unload on Trump's CISA." https://cyberscoop.com/arizona-secretary-of-state-website-hack-candidate-portal-criticizes-cisa/

[20] Google Cloud. "DDoS attack trends during U.S midterm elections." https://cloud.google.com/blog/products/identity-security/ddos-attack-trends-during-us-midterm-elections

[21] Mandiant. "Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections." https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections/

[22] U.S. Senate Armed Services Committee. "Hearing to Receive Testimony on United States Cyber Command and United States Space Command in Review of the Defense Authorization Request for Fiscal Year 2027 and the Future Years Defense Program." Full transcript, April 28, 2026. https://www.armed-services.senate.gov/imo/media/doc/full_transcript-04-28-2026.pdf

[23] Winona County, Minnesota. "Press Release: 1/23/26 - Winona County Responds to Ransomware Incident." January 26, 2026. https://www.winonacounty.gov/CivicAlerts.aspx?AID=350

[24] City of Foster City. "Foster City Services Impacted by Cyber Security Breach." March 19, 2026. https://www.fostercity.org/community/page/foster-city-services-impacted-cyber-security-breach

[25] Check Point Research. "The State of Ransomware - Q1 2026." May 11, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

CONTACT US

ISRAEL
Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA
Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE
Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES
Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND
Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN
Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management