



Threat Intelligence Report





A Deep Dive into Cyber Threats surrounding U.S. Election 2024

Oct 08, 2024 | Medium

TLP ●●●

Executive Summary:

The United States election process is a fundamental pillar of its democracy, involving a vast network of federal and state agencies, political parties, candidates, and, most importantly, the voting public. As elections approach, it's imperative to recognize and understand the array of cyber threats that could impact the integrity and trustworthiness of this critical process.

Cyber adversaries, including state-sponsored actors and hacktivist groups, are increasingly active in the lead-up to elections. For US-specific threats, the dark web has become a hub for malicious actors to trade sensitive information and develop strategies to exploit vulnerabilities. Hacktivist groups are also mobilizing, aiming to disrupt proceedings or sway public opinion through coordinated cyber campaigns.

However, one of the biggest threats is state-sponsored entities that employ sophisticated tactics to infiltrate systems, steal data, and disseminate misinformation. Their activities can undermine confidence in the electoral process and potentially alter outcomes. Malicious actors are also utilizing artificial intelligence to create and automate the spread of disinformation and misinformation, thereby shaping public opinion in unintended ways. Commonly exploited vulnerabilities, such as outdated software and inadequate security protocols, make systems more susceptible to attacks.

Election infrastructure, government agencies engaged in electoral processes, political campaigns, media organizations, and technology providers could all be at risk during this time. These and similar entities must prioritize cybersecurity measures to protect against potential breaches and ensure the integrity of the electoral process. This report provides a comprehensive overview of the potential cyber threat landscape and critical vulnerabilities that could impact the election process. This analysis is crucial for preparing and safeguarding against cyberattacks that could disrupt or influence election outcomes.

In this report, FortiGuard Labs Threat Research provides an in-depth analysis of threats gathered from January 2024 to August 2024 that may affect US-based entities and the electoral process. It also examines the diverse array of challenges posed by cyber threats, assesses their impact on the present US elections, and provides guidance on how to protect critical environments and systems.

Content:

- Scam targeting US Elections
- Darknet Landscape
- Espionage Landscape
- Hacktivist Landscape
- Ransomware Landscape
- Vulnerability Landscape
- Conclusion
- Recommendations

Key Observations

It is important to note that while not all these data points may seem directly connected to the US election, they indicate a spike in threat activity that coincides with that event. In addition, they all include either access to the private data of US citizens, which could be used for voter fraud or the distribution of misinformation, access to compromised government and business entities that could be targeted for things like fraud or the disruption of critical infrastructures, or a rise in malicious activities which could be used to exploit users, such as those interested in the election, or to disrupt information systems or critical infrastructure.

Scams Targeting US Elections:

- Since January 2024, we have identified the registration of over 1,000 new domain names. These domains follow particular patterns, frequently incorporating election-related terms and references to prominent political figures.
- The majority of these domains are registered in the United States (636 domains), followed by Canada (72 domains) and Germany (22 domains).
- The most used hosting providers for these election-themed websites are AMAZON-02, which currently hosts 458 domains, CLOUDFLARENET, with 71 domains, and NAMECHEAP-NET, which hosts 70 domains.
- One threat actor (TA) sells two distinct phishing kits, priced at \$1,260 each, designed to impersonate political leaders Donald Trump and Kamala Harris.

Darknet Landscape:

- Over 1.3 billion rows of combo lists, which include usernames, email addresses, and passwords, signify a considerable risk for credential-stuffing attacks. In such attacks, cybercriminals use these stolen credentials to gain unauthorized access to accounts, making it a valid and substantial security concern.
- The discovery of 300,000 rows of credit card data, which include CVV, name, card number, expiry date, and date of birth, highlights potential financial fraud risks targeting voters and election officials.
- Over 2 billion rows of user databases on the Darknet indicate a heightened exposure to identity theft and targeted phishing attacks.
- 10% of the posts on Darknet forums are associated with Social Security Number (SSN) databases, which poses a significant threat by increasing the risk of personal data breaches.
- Around 3% of the posts on Darknet forums involve databases related to business and government entities. These databases hold critical organizational data that is vulnerable to cyber exploits.
- The majority of network access advertisements on the Darknet focus on corporate VPNs (35%), followed closely by Remote Desktop Protocol (RDP) access (32%) and Remote Desktop Web (RDWeb) access (25%).

Espionage Landscape:

- A total of 23 state-sponsored adversaries have been documented targeting the US, with actors from China leading in activity, followed by Russia and Iran.
- We anticipate increased cyber espionage activities from China, Russia, Iran, and North Korean threat actors aimed at disrupting or manipulating the US electoral process and political landscape.
- AI-enhanced and AI-generated audio content are becoming increasingly potent tools in disinformation campaigns. Our research has revealed that threat actors on the Darknet are advertising deepfake services starting at just USD 15, making this technology highly accessible for malicious purposes. A recent instance demonstrated the danger of this technology when a deepfake of [President Joe Biden's voice was used in a robocall during the New Hampshire primary](#), highlighting how easily such technology can be weaponized.

Hacktivist Landscape:

- NoName057(16), CyberArmyofRussia_Reborn, and Killnet are pro-Russian hacktivist groups with recently increased activity that could play a significant role in disrupting elections. Their capabilities and historical activities suggest they have the means to impact processes if they choose to engage in such actions.
- GARNESIA_TEAM, FromLammerToMastah, and Z-BL4CX-H4T are two prominent groups that have conducted the most operations since January 2024.

Ransomware Landscape:

- Over 1000 ransomware victims have been reported from January 2024 to the time of publication of this report.
- 'Lockbit3', 'Play', and 'RansomHub' are the top three ransomware groups focused on targeting the US. Their primary target is the Manufacturing sector, followed by the Business Services and Construction industries.
- We have observed a notable spike in ransomware attacks against the US Government (+28%), Hospitality (+18%), Real Estate (+5%), and Transportation (+5%) compared to 2023.

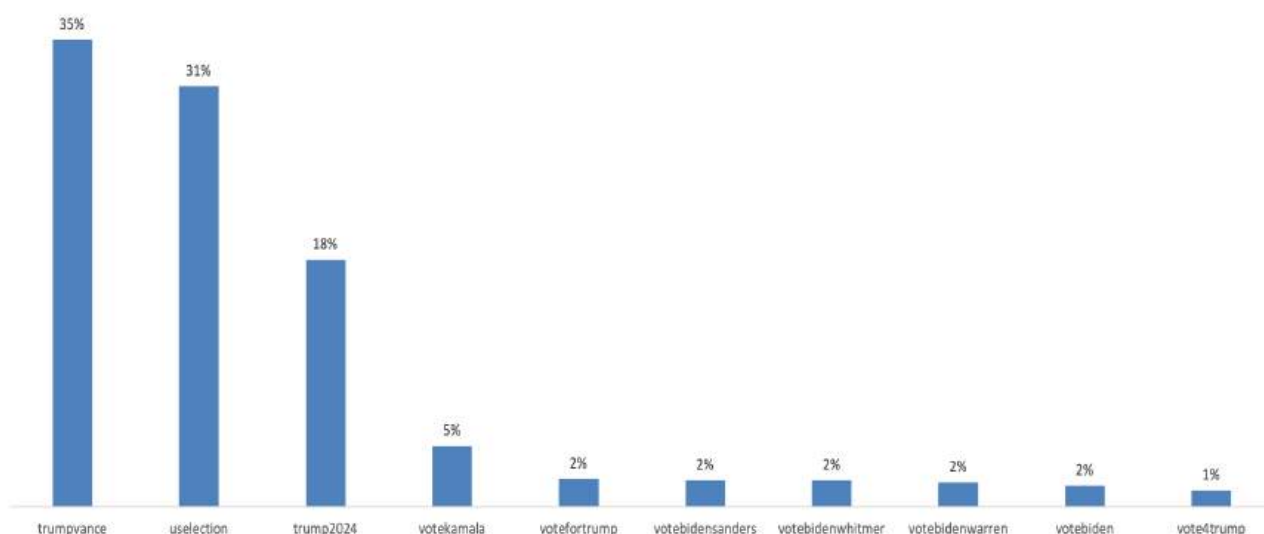
Vulnerability Landscape:

- In 2024, there were 291 known exploited CVEs, with 128 added to CISA's KEV and 55 specifically used in targeted threat campaigns against US infrastructure.
- Of the vulnerabilities that have been exploited, espionage actors have exploited 46%, cybercrime actors are responsible for exploiting 39%, and ransomware groups account for 15%.

Scams Targeting US Elections

Since January 2024, FortiGuard Labs Threat Research has identified the registration of over **1000+ new domain names**. These domains follow particular patterns, frequently incorporating election-related terms and references to prominent political figures. Examples of these patterns include "**vote4for**," "**vote4**," "**trump2024**," "**voteharris**," "**2024harris-kelly**," "**trumpvancetransition**," "**uselection**," etc.

The prevalence of these terms suggests that threat actors are interested in leveraging the heightened interest surrounding the 2024 US elections to potentially conduct malicious activities such as phishing campaigns, disinformation, or launching cyberattacks to influence voter behavior and undermine electoral integrity.



(Newly registered domain names incorporating election-related terms)

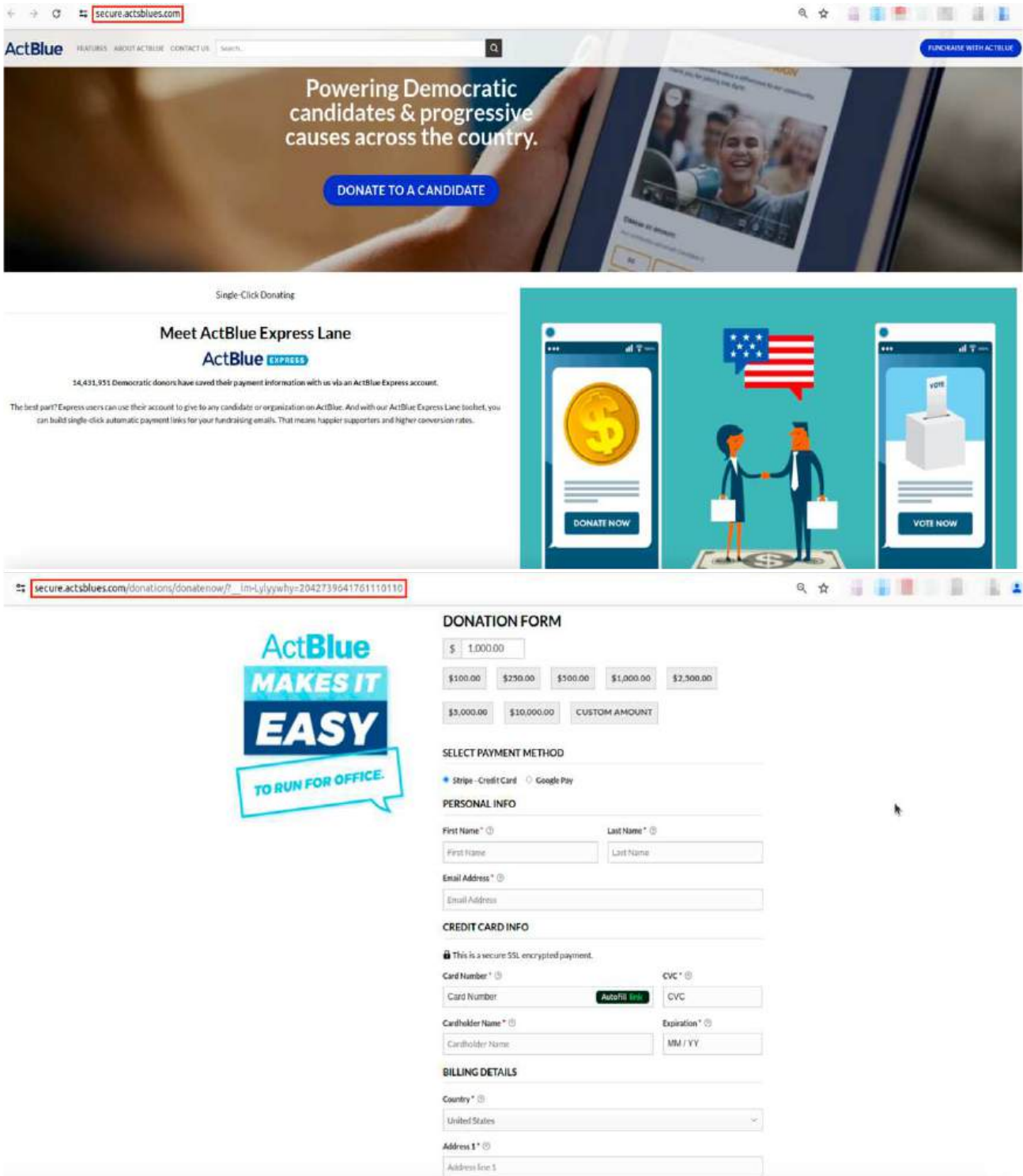
Analysis of Potentially Malicious Domain Registrations

- **Domains by IP Address:** A notable concentration of domains is associated with a limited number of IP addresses. Specifically, the IP addresses 15.197.148.33 and 3.33.130.190 each host 126 domains, making them the most active in our dataset. These domains hosted on the IPs indicate a centralized approach by threat actors to efficiently manage multiple malicious domains to execute large-scale cyber campaigns.
- **Dominance of Registrant Countries:** The majority of these domains are registered in the United States (636 domains), followed by Canada (72 domains) and Germany (22 domains). The high number of US-based registrations indicates either the presence of domestic threat actors or the utilization of US hosting services to hide the origin of malicious activities.
- **Preferred Hosting Providers:** Analysis of hosting providers reveals a strong preference for well-known and widely used services. AMAZON-02 leads with 458 domains, followed by CLOUDFLARENET (71 domains) and NAMECHEAP-NET (70 domains). The reliance on major hosting platforms such as Amazon Web Services (AWS) and Cloudflare suggests that threat actors are leveraging these reputable services to enhance the legitimacy and resilience of their malicious domains.

Donation Scam

With the US election approaching, the surge in political engagement and donations provides a fertile ground for cybercriminals. As seen in past elections, particularly the 2020 race, where contributions reached unprecedented levels, the influx of funds makes campaigns attractive targets for malicious actors. The increase in financial activity around elections creates numerous opportunities for exploitation, especially by those seeking to take advantage of heightened public interest and large-scale political donations.

FortiGuard Labs Threat Research has identified a number of fraudulent fundraising websites, including [secure\[.\]actsblues\[.\]com](https://secure.actsblues.com), which is designed to imitate the legitimate ActBlue site ([secure\[.\]actsblue\[.\]com](https://secure.actsblue.com)). ActBlue is a nonprofit American fundraising platform and political action committee founded in 2004. This deceptive website is set up to collect donations and personal details such as credit card information, names, emails, and full residential addresses.

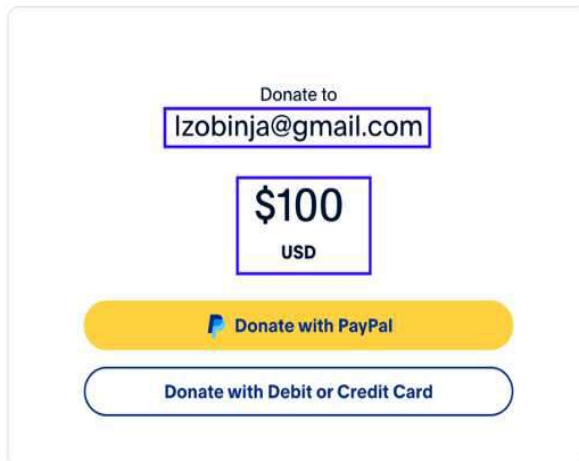
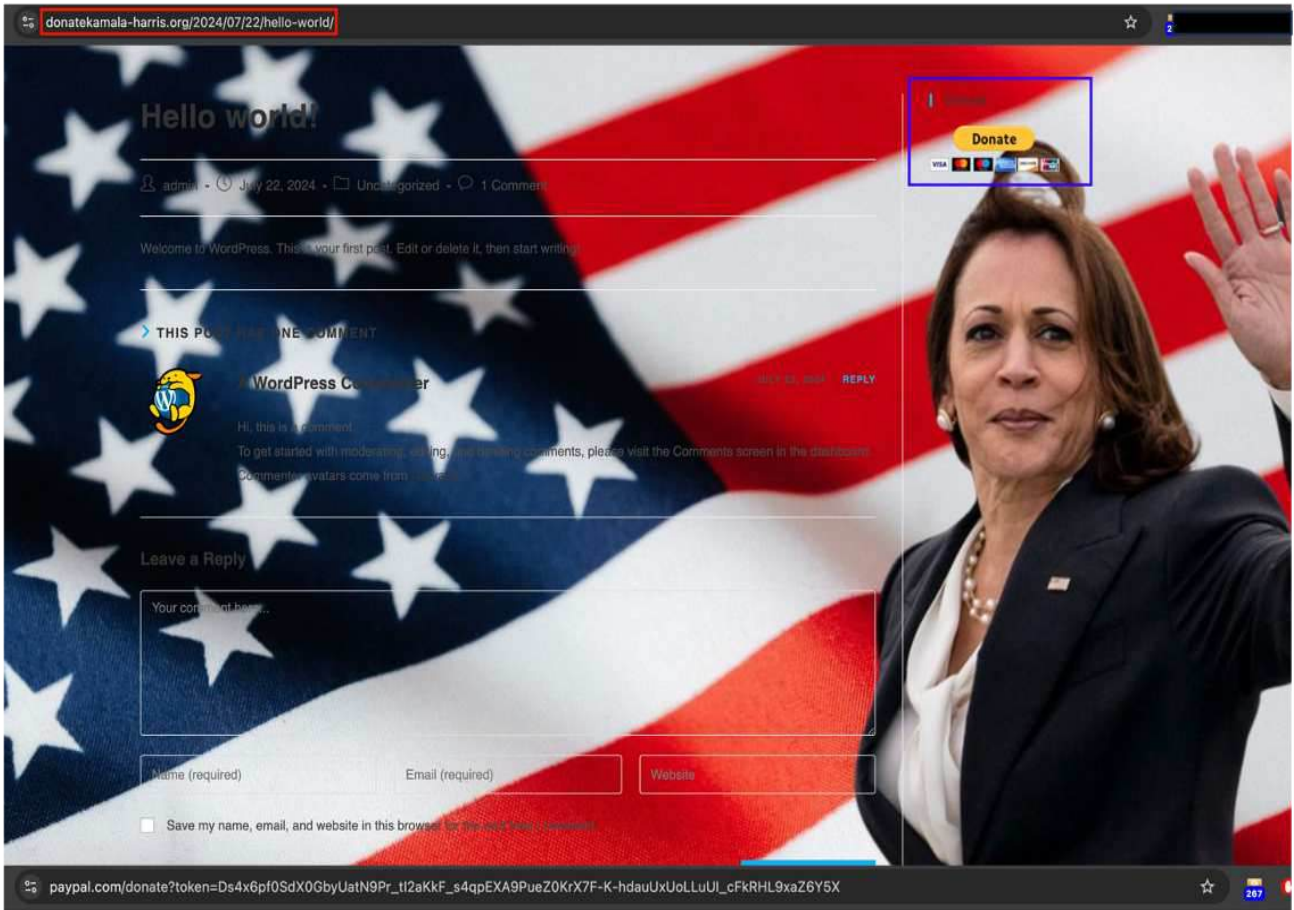


(Newly registered website impersonating ActBlue)

| | |
|---------------|---------------------|
| Domain Name | ACTSBLUES.COM |
| Registered On | 12th September 2024 |

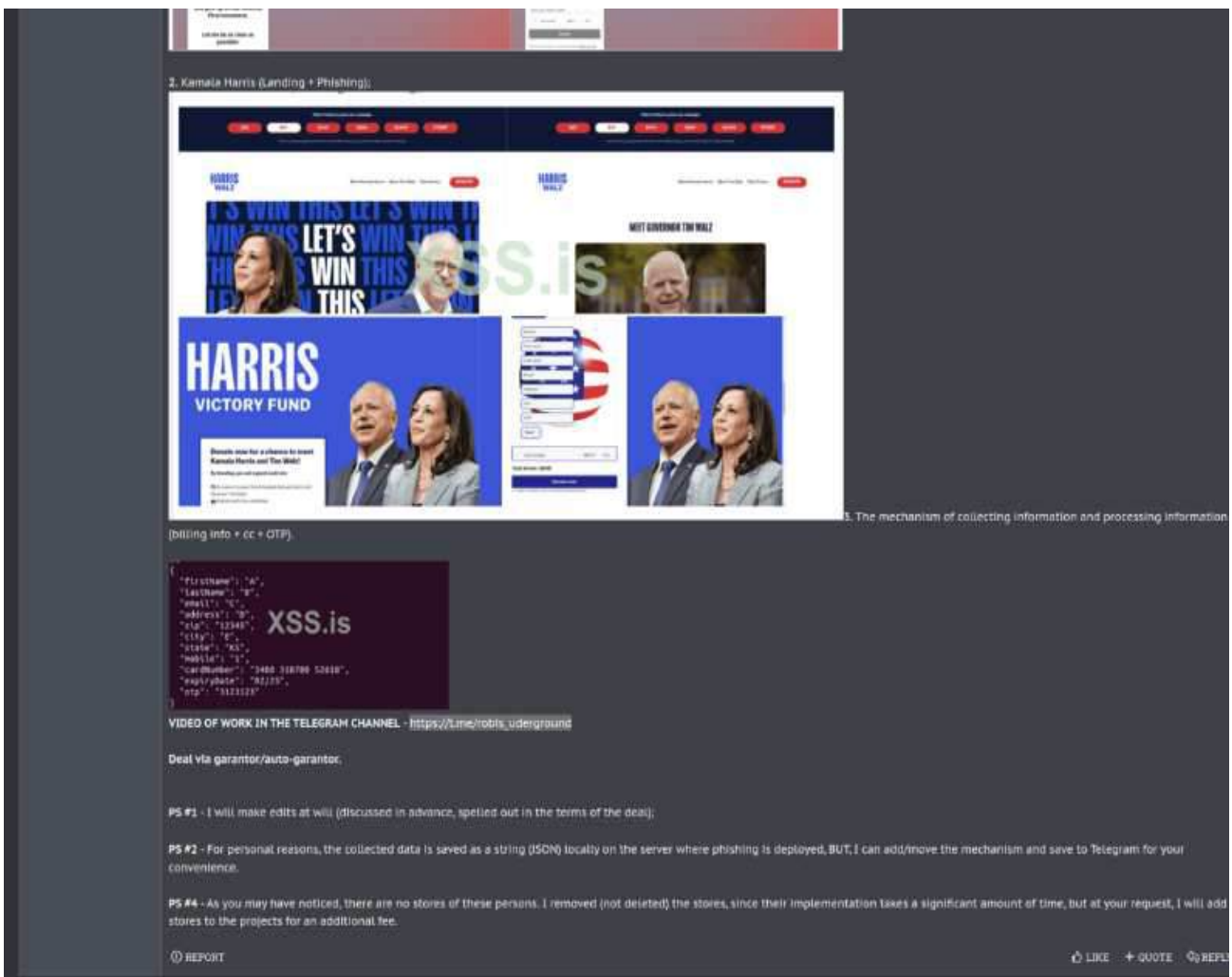
| | |
|-------------------------|---|
| Registrar | Hosting Concepts B.V. d/b/a Registrar.eu |
| Name Servers | jaime.ns.cloudflare.com treasure.ns.cloudflare.com |
| IP Address | 104.21.1.2310 (Cloudflare) 172.67.152.143 (Cloudflare) |
| Hosting Provider | Cloudflare, Inc. |

Another fraudulent website registered in July 2024 designed to collect donations is [donatekamala-harris\[.\]org](https://donatekamala-harris[.]org).



(A new website featuring Kamala Harris to solicit donations)

| | |
|--------------|----------------------------------|
| Domain Name | DONATEKAMALA-HARRIS.ORG |
| Registered | 22nd July 2024 |
| Registrar | Namesilo, LLC |
| Name Servers | rs92.rcnoc.com rs91.rcnoc.com |



(Darknet forum post advertisement of phishing project)

Darknet Landscape

The Darknet serves as a central platform for many of the cyber threats that pose significant risks to the integrity of the US elections. Malicious actors use this platform to exchange sophisticated tools, exploit methods, and unauthorized network access credentials that could result in political influence and disruption. Dark web forums can also facilitate the sale of sensitive electoral information, discussions on vulnerabilities within election systems, and the coordination of cyberattacks to undermine the electoral process.

Threats to US elections from these Darknet activities include data breaches of voter databases, theft of intellectual property related to election technology, and the sale of insider information that could be used to manipulate election outcomes. Such activities can lead to operational disruptions and erosion of public trust, along with significant financial repercussions.

The following section will delve deeper into the security landscape surrounding election databases and the types of access being advertised and shared by threat actors, highlighting the substantial risks these activities pose to the US electoral system.

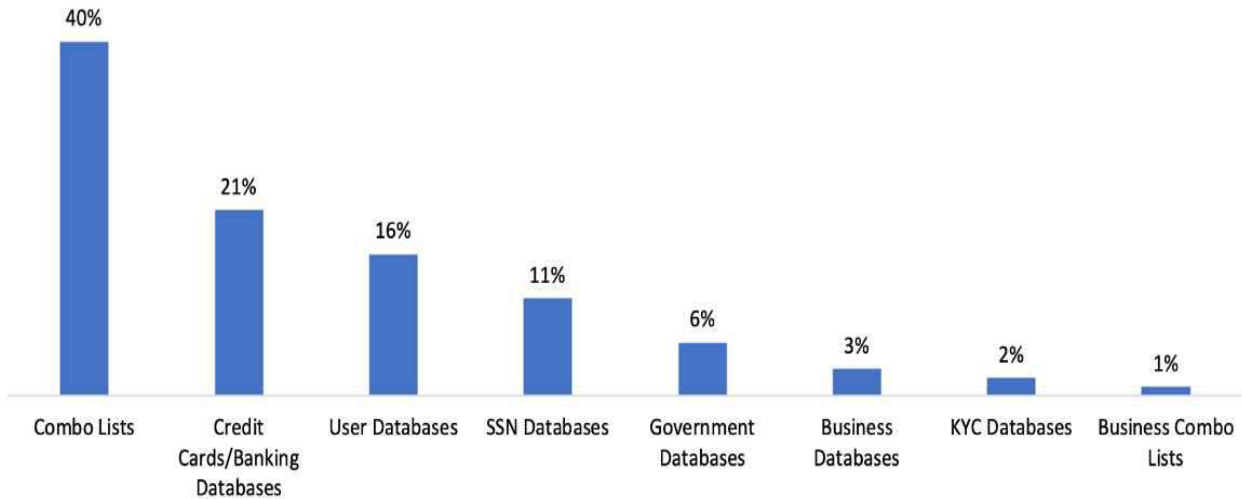
Database Advertisements

Our analysis reveals a significant number of diverse databases available on Darknet forums targeting the United States, posing serious threats to the integrity of US elections.

- Approximately 40% of the posts on Darknet involve combo lists (usernames/email addresses and passwords). These combo lists can be used for large-scale credential stuffing and unauthorized access, potentially compromising voter data, election systems, and sensitive information. More than 1.3 billion rows of combo lists are currently being advertised across different Darknet forums.
- Credit card and banking data, constituting about 21% of the posts with 300k rows, pose significant risks of financial fraud and phishing, targeting users in the US. These actions could lead to campaign disruptions, undermining voter outreach, destabilizing financial support

for candidates, or enabling fraudulent campaign funding.

- User databases, such as those for doctors, musicians, and investors, make up roughly 19% of the posts, with over 2 billion rows. These databases can facilitate identity theft and targeted phishing, risking the security of those involved in elections and eroding public trust.
- Social Security Number (SSN) databases, about 10% of the posts, increase the risk of data breaches and cyberattacks, with one instance advertising an SSN database with over 19 gigabytes (about 80 million rows) of data.
- Business and government databases each account for about 3% of posts, holding records on user information and government details. Notably, a threat actor from the group CyberNiggers claimed a breach of the US Department of Transportation's database, leaking over 5.8 million entries.
- Lastly, although less common at 2% and 1%, KYC databases and business combo lists still pose substantial risks for sophisticated cyberattacks. One reported case involved a KYC database containing over ten terabytes of data.

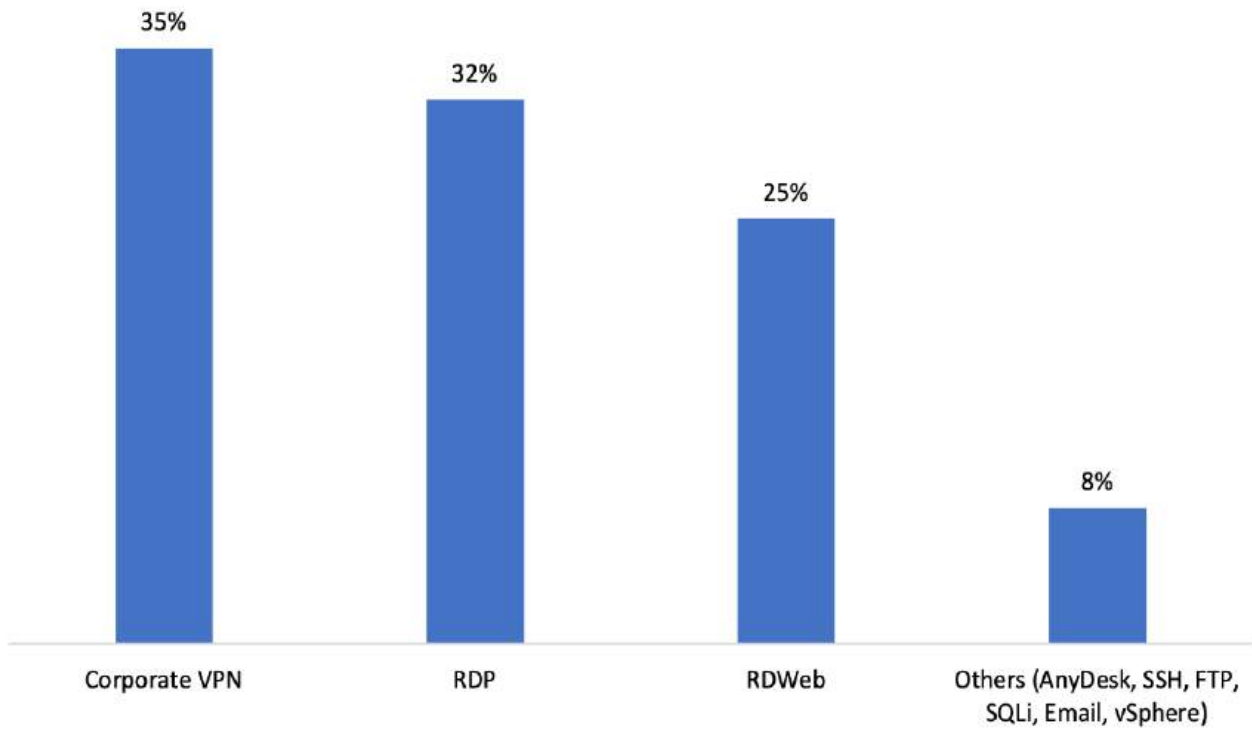


(Darknet database proliferation posing challenges to US electoral security and citizens)

Network Access Advertisements

Network access refers to the various levels or methods of unauthorized access to digital assets and systems advertised or offered for sale on Darknet forums. These include access credentials, remote access tools, exploits, backdoors, or compromised accounts, among others. These advertisements typically target TAs seeking unauthorized access to systems or data for malicious purposes. The pricing of access advertised on the Darknet forums can fluctuate significantly, depending on the type of organization and the country. Based on our observation, these types of accesses are often obtained through private stealer logs.

The table below presents the most commonly advertised network access types on Darknet forums targeting the United States.



(Network access advertisement types)

Below are the various types of network access predominantly shared and advertised by the following threat actors (TAs).

- **Corporate VPNs:**
 - [Yesdaddy](#): 104 VPN posts (primarily targeting the USA)
- **Remote Desktop Protocol (RDP):**
 - [k005](#): 65 RDP posts targeting the USA
 - [myKarma](#): 30 RDP posts targeting the USA
- **RDWeb Access:**
 - [sandocan](#): Over 90 RDWeb targeting the USA
 - [ProfessorKliq](#): More than 30 RDWeb targeting the USA

Espionage Landscape

Nation-state actors or APT groups have the resources to engage in cyber espionage, such as gathering intelligence on the US electoral process, political landscape, and strategic interests. Espionage can involve reconnaissance, phishing, and malware attacks targeting government agencies, political organizations, and critical infrastructure or the distribution of disinformation.

This section examines the data we have compiled on espionage activities targeting the US by foreign adversaries this past year and highlights those APT groups that have targeted the US in previous campaigns.



(China)

| APT Group | Source |
|-----------|--------|
|-----------|--------|

| | |
|--------------------|--|
| UNK_SweetSpecter | Artificial Sweetener: SugarGh0st RAT Used to Target American Artificial Intelligence Experts |
| Earth Krahang | Earth Krahang APT campaign targets several government entities worldwide, including U.S |
| UNC5174 | Chinese group UNC5174 exploiting ScreenConnect, F5 bugs to attack U.S defense |
| Volt Typhoon | VOLTZITE Espionage Operations Targeting US Critical Systems |
| Volt Typhoon | PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure |
| UNC5325 UNC3886 | Chinese APT groups exploiting Ivanti vulnerabilities to attack US defense industrial base sector |



(Iran)

| APT Group | Source |
|----------------|---|
| Fox Kitten | Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations |
| APT33 | APT33 deploys new custom Tickler malware to target federal and state government sectors in the United States and UAE |
| Storm-2035 | Disrupting a covert Iranian influence operation that uses ChatGPT to generate content focused on multiple topics, including the US presidential campaign |
| APT42 | Iranian backed group steps up phishing campaigns against Israel, US |
| TA453 | TA453 utilized BlackSmith Malware targeting a series of diplomatic and political entities, ranging from embassies in Tehran to US political campaigns. |
| Mint Sandstorm | Sandstorm (PHOSPHORUS) targeting high-profile individuals working on Middle Eastern affairs at universities and research organizations in Belgium, France, Gaza, Israel, the United Kingdom, and the United States. |



(Russia)

| APT Group | Source |
|-----------|--------|
| | |

Unit 29155 [Russian Military Cyber Actors Target US and Global Critical Infrastructure](#)

COLDRIVER [A Russian state-sponsored spear phishing campaign has been found to be targeting Western and Russian civil society targets, including nongovernmental organizations, independent media and former US ambassador](#)

[APT28 using GooseEgg as part of post-compromise activities against targets including Ukrainian, Western European, and North American government, non-governmental, education, and transportation sector organizations](#)

APT28 [Russian hackers hijack Ubiquiti routers to launch stealthy attacks targeting militaries, governments, and other organizations worldwide](#)

[Pawn Storm Uses Brute Force and Stealth Against High-Value Targets](#)

APT29 [American multinational technology company Microsoft's actions following attack by nation state actor 'APT29'](#)

[Tech Giant HP Enterprise Hacked by Russian Hackers Linked to DNC Breach](#)



(North Korea)

| APT Group | Source |
|-----------------|---|
| Silent Chollima | North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting US Hospitals and Health Care Providers |
| APT45 | North Korean Hackers Target USA Critical Infrastructure and Military Bases |
| TA427 | TA427 Targeting Experts for Insight into US and the Republic of Korea (ROK or South Korea) Foreign Policy |

(Unknown)

| State-Sponsored Country | APT Group | Source |
|-------------------------|------------|--|
| Unknown | TA866 | TA866 Returns with a Large Email Campaign Targeting North America |
| | LilacSquid | Lilacsquid Targets Information Technology Organizations Building Software for the Research & Industrial Sectors in the United States |

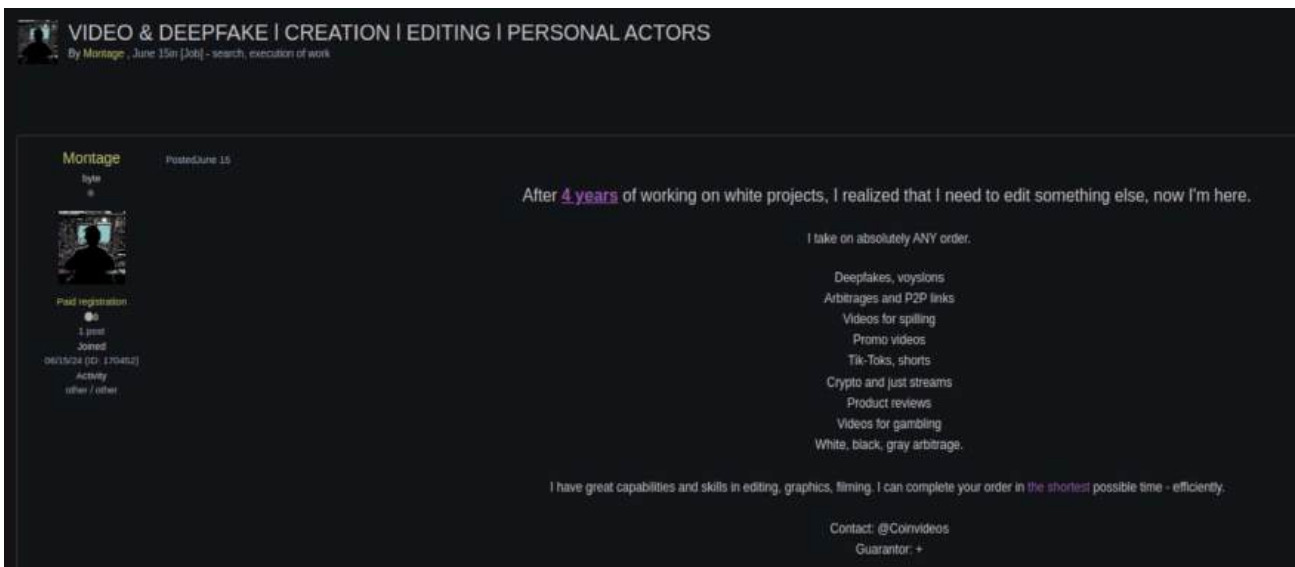
Void Banshee [Void Banshee Campaign Targets Highly Skilled North American Professionals and Students Who Often Use Reference Materials](#)

TAG-100 [TAG-100 Targeted Various Internet-Facing Products in North America](#)

Exploring AI and Disinformation Campaigns in Shaping Public Opinion

Threat actors often launch coordinated disinformation campaigns to spread false narratives, propaganda, and misleading information to manipulate public opinion and influence voter behavior. These campaigns can target social media platforms, messaging apps, and online forums to spread false information and propaganda.

AI-enhanced and AI-generated audio content are becoming powerful tools in disinformation campaigns, potentially significantly impacting US elections. Deepfake technology, which can create convincing audio and video imitations, allows threat actors to fabricate statements, speeches, or interviews of political candidates, spreading false information that can manipulate public opinion. Our research has revealed advertisements on Darknet platforms offering Deepfake services starting at just USD 15. These AI-generated disinformation and fake audio clips designed to mimic the voices of political figures could be circulated widely on social media, generating controversy or altering voter behavior.



(Deepfake services advertised on darknet)

AI technology has demonstrated its potential to influence public opinion and manipulate voter behavior in elections. Instances such as the mimicking of President Joe Biden's voice in a robocall during the New Hampshire primary, the circulation of an AI-generated voice discussing false plans by a candidate in Slovakia, the manipulation of audio clips to falsely implicate candidates in Nigeria, and the spread of deepfake videos in Bangladesh all highlight the impact of AI in shaping electoral outcomes.

To emphasize this point, [the US Office of the Director of National Intelligence \(ODNI\) released a document](#) indicating that Russia, China and Iran are increasing their election influence operations using generative AI tools to speed development and reach.

Below are some recent disinformation campaigns by various threat actors that have targeted the US.

| State-Sponsored Group's Origin | Description | Source |
|--------------------------------|-------------|--------|
|--------------------------------|-------------|--------|

| | | |
|------------------------|---|--|
| Iran | OpenAI banned accounts linked to an Iranian influence operation using ChatGPT to generate content focused on multiple topics, including the US presidential campaign. | Disrupting a covert Iranian influence operation |
| Multiple Threat Groups | Russia is deeply invested in undermining US support for Ukraine | Russian US election interference targets support for Ukraine after slow start |
| Russia | The US DOJ seized 32 internet domains used in the "Doppelganger," campaign to influence US-based persons. | Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere |
| Russia | Russian Disinformation Videos Smear Biden Ahead of US Election | Russian Disinformation Videos Smear Biden Ahead of US Election |
| China | China is using fake social media accounts to poll voters on what divides them most to sow division and possibly influence the outcome of the US presidential election in its favor. | China tests US voter fault lines and ramps AI content to boost its geopolitical interests |
| China | Campaign to impersonate American voters to spread divisive narratives ahead of the election. | The #Americans - Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election |

This year, on Taiwan's election day, a sophisticated threat group 'Storm-1376' posted suspected AI-generated audio clips of Foxconn owner Terry Gou, an Independent Party candidate in Taiwan's presidential race, who bowed out of the contest in November 2023. The audio recordings portrayed Gou's voice endorsing another candidate in the presidential race. Gou's voice in the recordings is likely AI-generated, as Gou made no such statement.

It's important to highlight that Storm-1376 has a track record of conducting disinformation campaigns across different regions and events. According to [Microsoft](#), in August 2023, as wildfires raged on the northwest coast of Maui, Hawaii, Storm-1376 seized the chance to spread conspiratorial narratives on multiple social media platforms. These posts alleged the US government had deliberately set the fires to test a military-grade weather weapon. In addition to posting the text in at least 31 languages across dozens of websites and platforms, Storm-1376 used AI-generated images of burning coastal roads and residences to make the content more eye-catching.

Based on observed behavior, it's highly likely that state-sponsored threat actors from China, Russia, and Iran could use similar tactics to target the US government and critical infrastructure and cause disruption during the election process. This poses a serious threat to election security and public trust.

Hacktivist Landscape

There has been a notable increase in cyber hacktivism activities this past year, particularly by pro-Russian groups aimed at disrupting high-profile events, such as US elections. These groups have demonstrated significant capabilities in deploying distributed denial-of-service (DDoS) attacks against critical infrastructure. In May 2024, the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with Canadian and U.K. cybersecurity bodies, issued a [joint alert](#) about a surge in pro-Russian hacktivist activities. These groups targeted small-scale OT systems in critical sectors such as water, energy, and agriculture.

[CyberArmyofRussia_Reborn \(CARR\)](#), a pro-Russian hacktivist group linked to state actors, has been particularly active in targeting US and European infrastructure. In January 2024, CARR claimed responsibility for manipulating water tanks in Texas, showcasing the group's ability to exploit known vulnerabilities in industrial control systems (ICS). CARR's activities extend to low-impact but persistent DDoS attacks and ICS manipulations across various sectors.

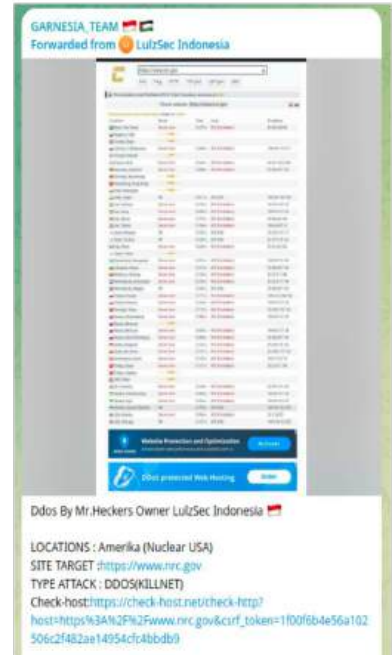
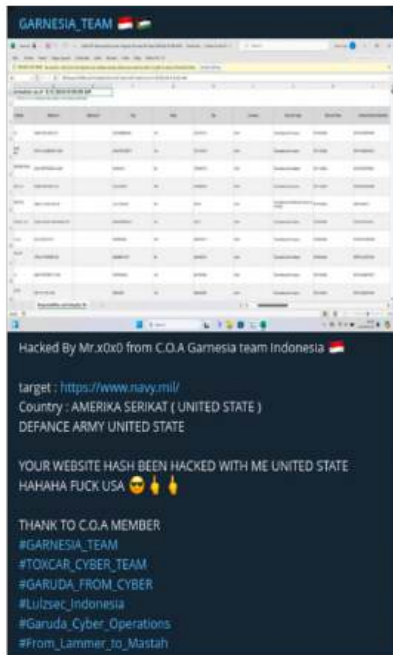
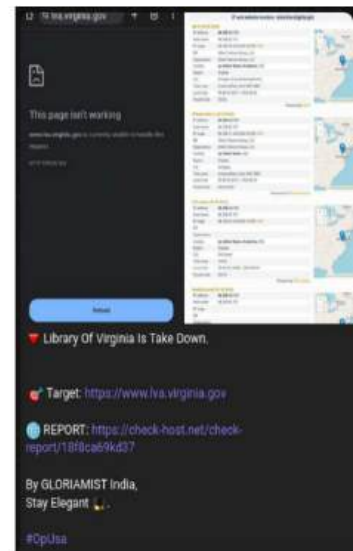
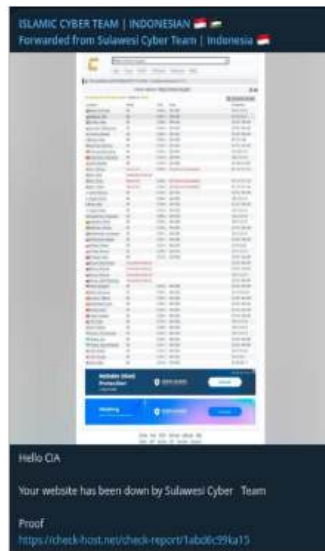
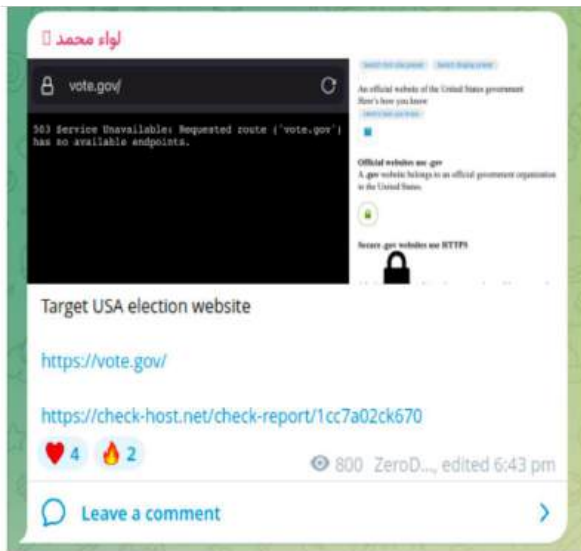
Based on our observations and their group's previous campaigns, we have compiled a list of hacktivist groups based on their activities that could likely play a pivotal role in disrupting the US elections. The chart represents the most active groups and their activities.

| Channels | DDoS | Defacement | Database | Destructive Attacks |
|--|--------|------------|----------|---------------------|
| NoName057(16) | High | Low | Medium | High |
| Народная CyberАрмия (CyberArmyofRussia_Reborn) | High | Low | Medium | High |
| WE ARE KILLNET | High | Medium | Low | High |
| Dark Strom Team | High | Low | Medium | - |
| RipperSec (ريفرسيك) | High | Medium | Low | - |
| ISLAMIC CYBER TEAM INDONESIA | Medium | High | Low | - |
| GANOSEC TEAM | High | Medium | Low | - |
| StarsX Team (PUB) | High | Medium | Low | - |
| GANOSEC TEAM PALESTINA | High | Medium | Low | - |
| Pro-Palestine Hackers Movement (PPHM) | Medium | High | Low | High |
| INFINITE INSIGHT.ID | High | Medium | Low | - |
| Moroccan Black Cyber Army | Medium | High | Low | - |
| GARNESIA_TEAM | High | Medium | Low | - |
| From Lammer To Mastah | High | Medium | Low | - |
| Z-BL4CX-H4T | Medium | High | Low | - |



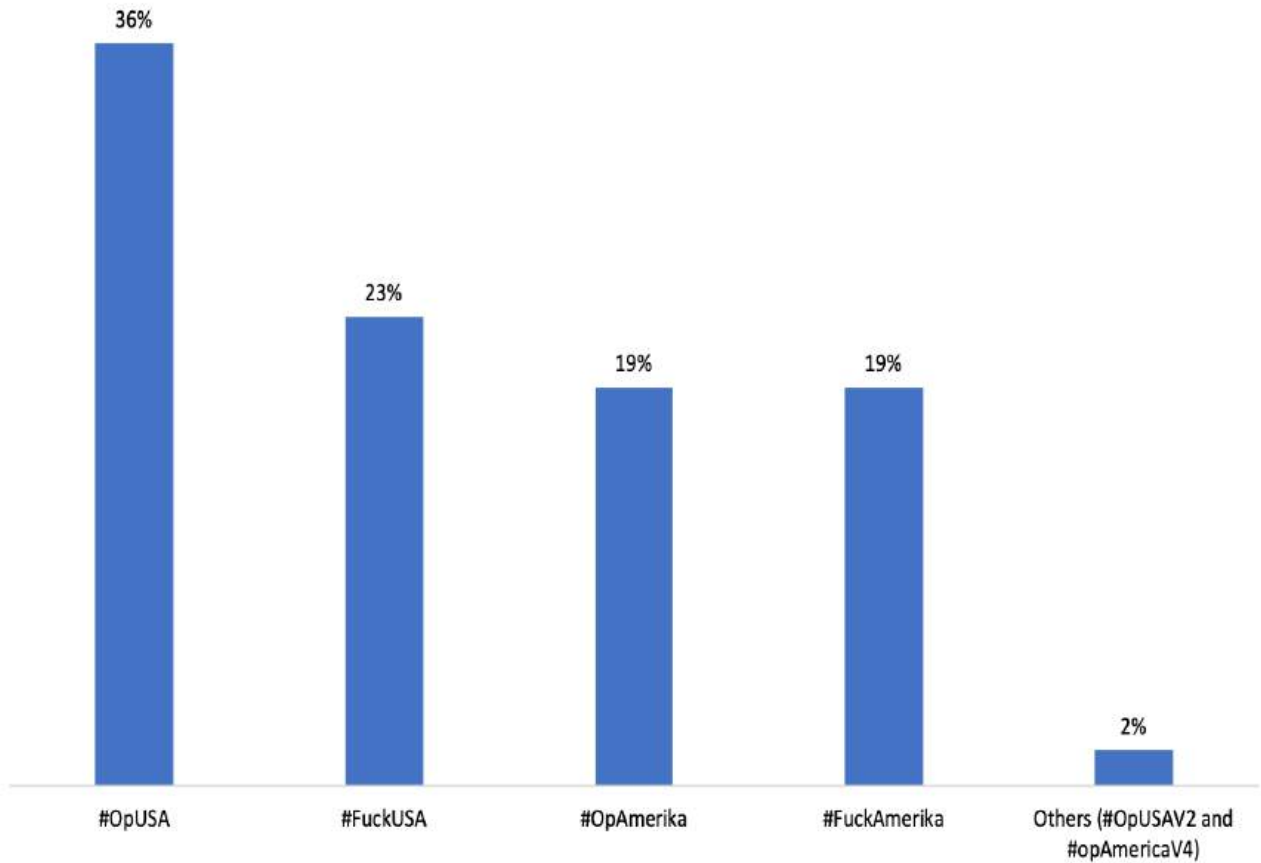
(Active hacker groups along with their overall activities)

The following are the screenshots of cyberattacks on US-based entities carried out by various hacker groups.



(Cyber attacks by hacktivist groups)

The chart below represents the campaigns launched by hacktivist groups primarily targeting US infrastructure. **GARNESIA_TEAM**, **FromLammerToMastah**, and **Z-BL4CX-H4T** are the groups that have performed the most operations since January 2024.

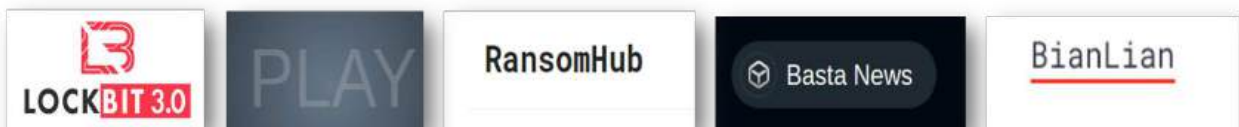


(Campaigns launched by hacktivist groups targeting the US)

Ransomware Landscape

Ransomware attacks raise concerns about the integrity and security of sensitive data, including voter information and election results. There's also the risk of political manipulation if attackers choose to selectively target certain government entities or election-related systems.

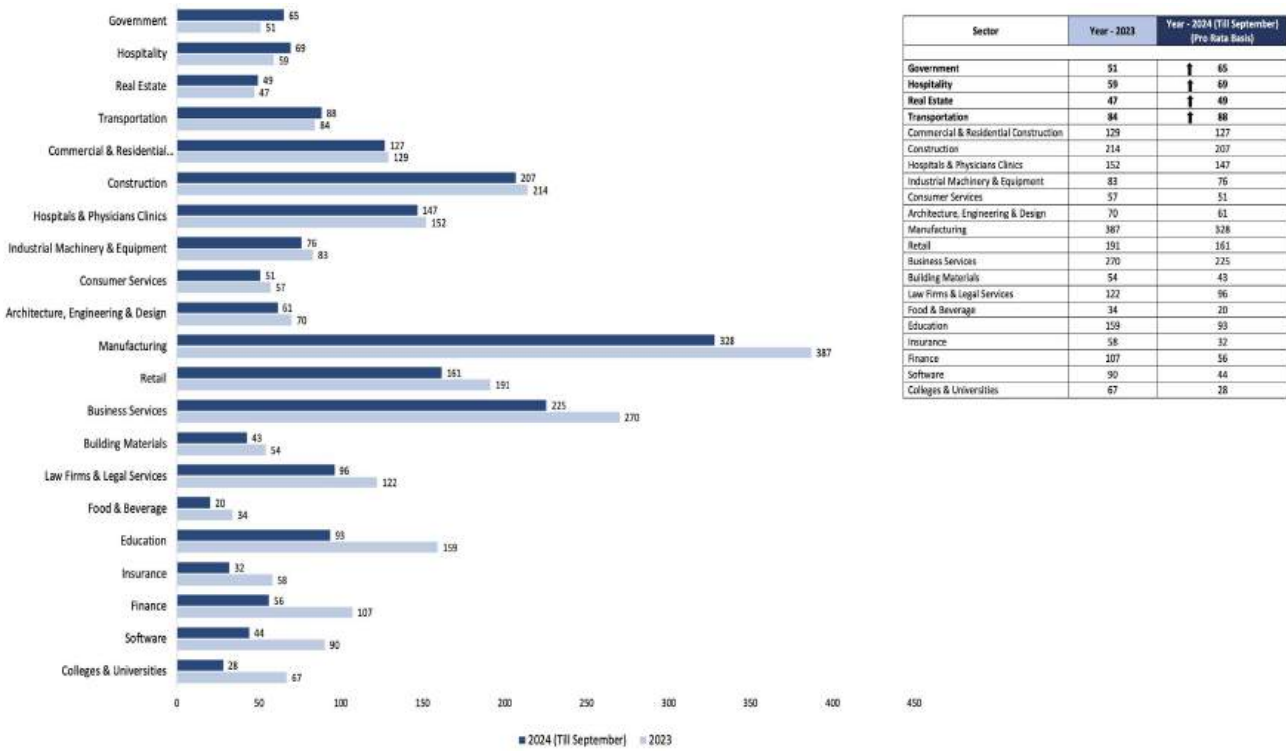
Ransomware attacks targeting government agencies before an election can seriously affect the electoral process and public trust in government institutions. Before an election, such attacks could disrupt critical government functions related to the electoral process, such as voter registration databases, election management systems, or communication channels used by election officials. This could lead to delays in voter registration, voting process disruptions, and results.



(Top 5 ransomware groups targeting the US in 2024)

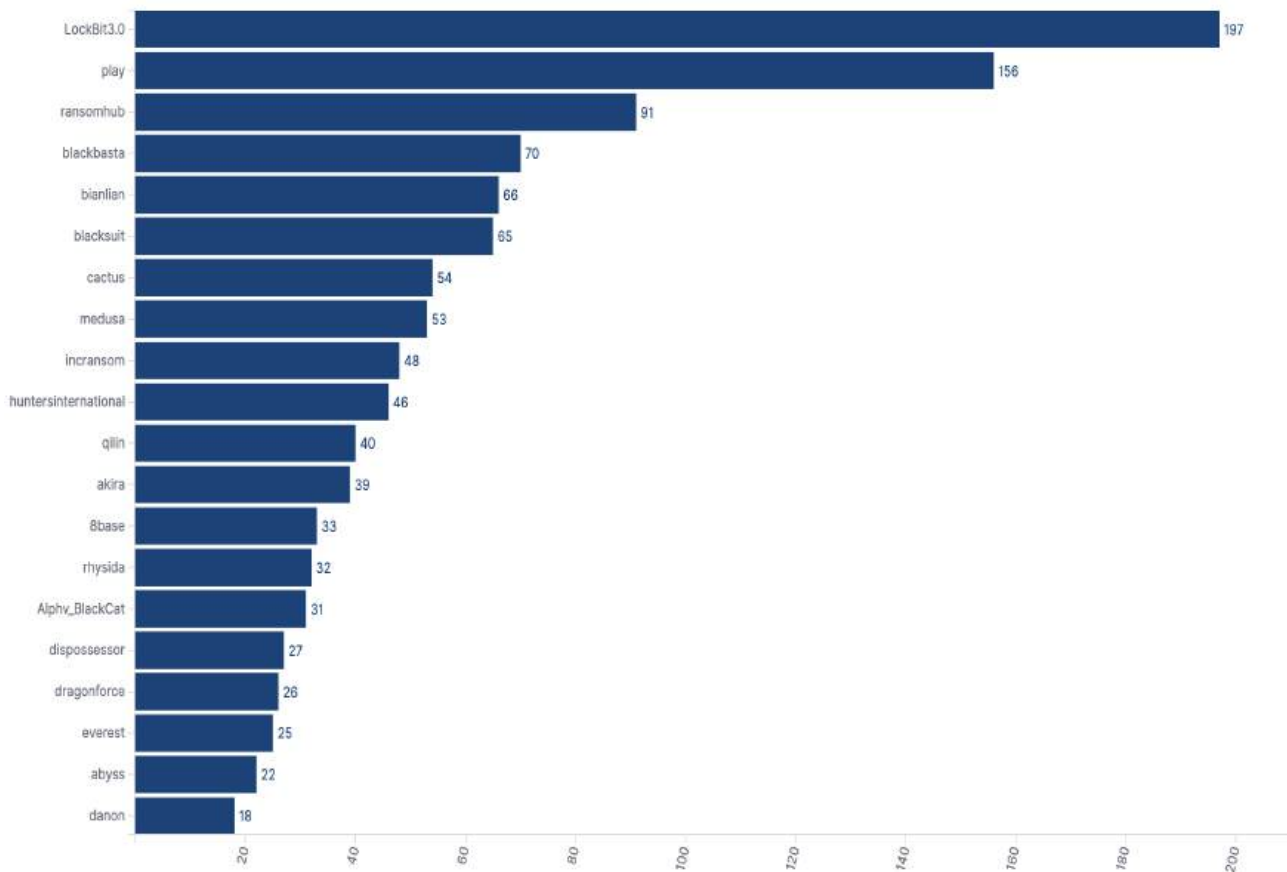
Over the past eight months, our data indicates that the US manufacturing sector has been the primary target of cyberattacks, followed closely by business services and construction. Ransomware groups frequently target multiple sectors to cause widespread disruption and chaos.

While examining the shifts in sectoral activity between 2023 and 2024, it's essential to point out that we've adjusted the 2023 figures to cover just the first eight months. This adjustment ensures we're comparing the same timeframe—the first eight months of each year—making our year-over-year analysis as precise as possible.



(Year-over-year comparison of ransomware victims targeting US-based entities)

The graph below provides detailed insights, including victim counts, showing how many victims each ransomware group has targeted in the US.

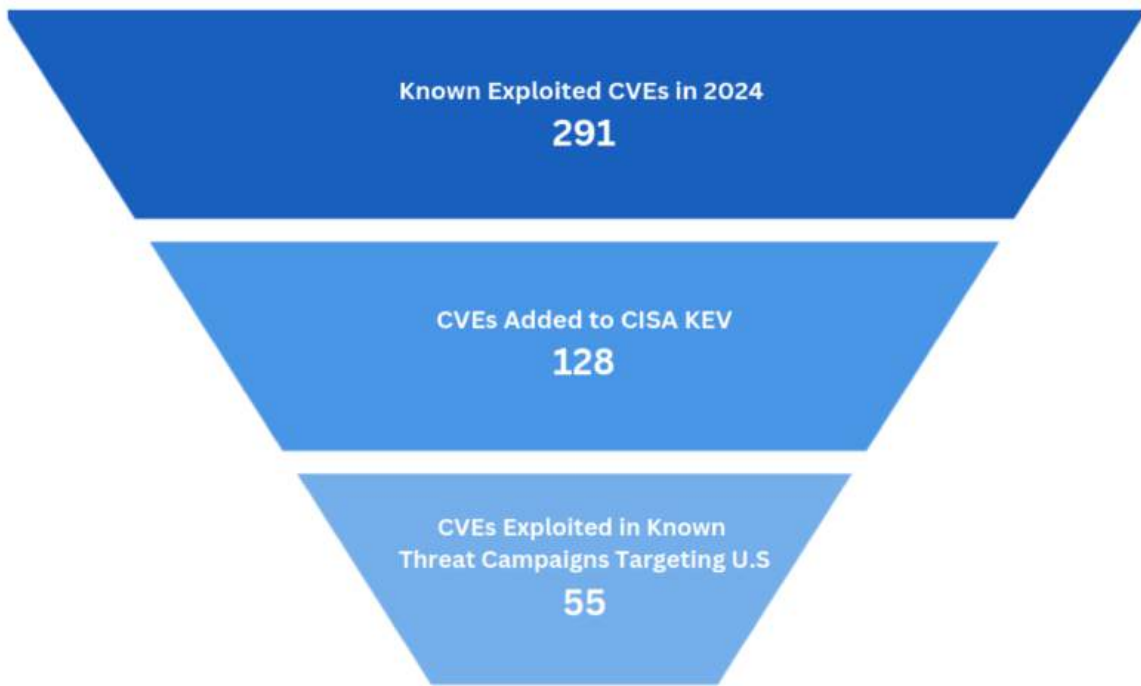


(2024 - Victims by top ransomware groups targeting US-based entities)

Vulnerability Landscape

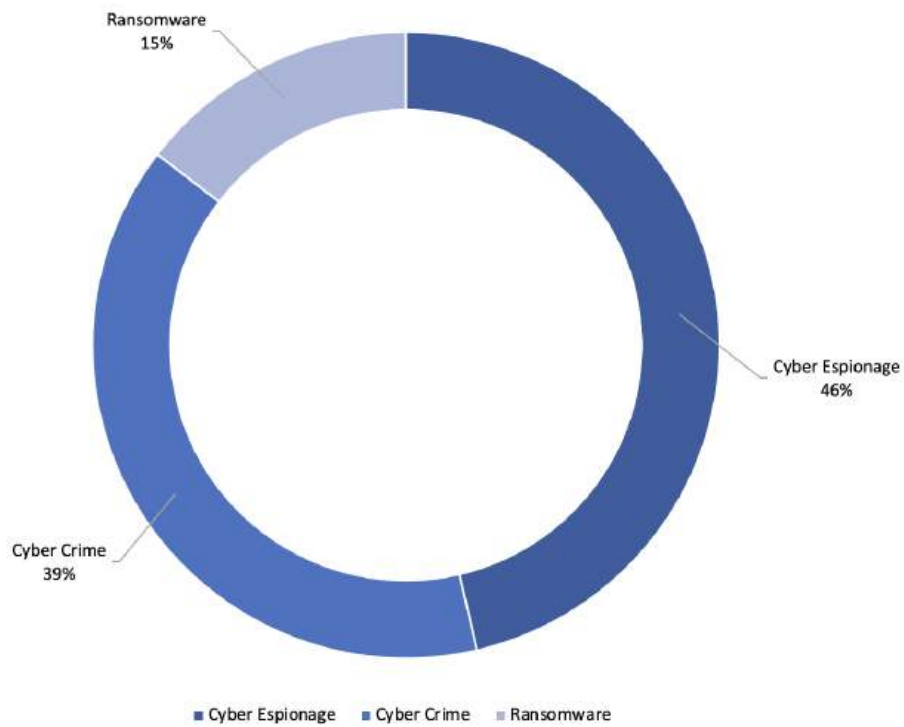
While not all of these vulnerabilities are being used against voters or to target the election, this section does highlight the extensive range of exploitable vulnerabilities available to those wishing to do so. Commonly exploited vulnerabilities represent a crucial aspect of the cybersecurity landscape. These vulnerabilities, often stemming from weaknesses in software, networks, or systems, serve as prime targets for threat actors seeking to exploit them for malicious purposes. Threat actors leverage a variety of techniques to exploit these vulnerabilities, ranging from known exploits to newly developed ones, to breach systems and gain unauthorized access.

TAs also continuously monitor security advisories and patches released by software vendors to identify vulnerabilities that users may have not yet patched. Once identified, they quickly capitalize on these vulnerabilities before patches are widely implemented, maximizing their window of opportunity to launch attacks. However, it's also common for threat actors to exploit old vulnerabilities using tried and tested methods. In 2024, [291 unique known vulnerabilities](#) are reported to be being actively exploited.



(Exploitation of CVEs)

Using data on vulnerability exploitation from the past eight months, we developed a comparison chart that highlights which categories of threat actors are actively exploiting different vulnerabilities.



(CVE exploitation by threat actor motivation)

Conclusion

The upcoming 2024 US elections face a range of cyber threats, many of which could have serious implications for electoral integrity. Based on the current landscape and the recent growth of related dark web activity, state-sponsored actors, hacktivist groups, and cybercriminals may likely target election infrastructure and associated systems. The rise of dark web activities, including the sale of sensitive electoral data, combo lists, and network access credentials, suggests that malicious actors can leverage these resources to disrupt election processes. Threats may manifest in various forms, such as credential-stuffing attacks, ransomware, or disinformation campaigns powered by deepfake

and AI-generated content to sway public opinion and undermine voter confidence. With state-sponsored actors from China, Russia, and Iran likely to play a significant role in these efforts, it is essential to anticipate and mitigate these risks through proactive cybersecurity strategies. Without adequate defense measures in place, the election process could be vulnerable to manipulation, misinformation, and operational disruptions, potentially altering the electoral outcome and shaking the public's trust in democratic institutions.

FortiGuard Labs Threat Research anticipates the following sectors are at higher risk and prone to cyberattacks during the US election:

- **Political Parties and Candidates:** Adversaries may target political parties and candidates with cyberattacks aimed at stealing sensitive information, disrupting campaign activities, or spreading disinformation to undermine their credibility.
- **Media Outlets:** Adversaries could target media outlets to manipulate public opinion by spreading false narratives, fabricating endorsements, or disseminating misleading information to sway voter perceptions.
- **Government Institutions:** Adversaries may target government institutions involved in organizing and overseeing elections, such as election commissions and administrative bodies, to disrupt electoral processes, compromise voter registration data, or manipulate election results.
- **Critical Infrastructure:** Adversaries could target critical infrastructure sectors, such as power grids, transportation networks, or telecommunications systems, to create chaos and disrupt the electoral process, potentially leading to voter disenfranchisement or logistical challenges.
- **Telecommunications Sector:** Adversaries may target telecommunications companies to disrupt communication networks, intercept sensitive communications, or launch cyberattacks to disrupt voter outreach efforts or manipulate public discourse.
- **Technology Organizations:** Adversaries may target technology organizations, including software companies, IT service providers, and cloud service providers, to steal intellectual property, exploit vulnerabilities, or compromise digital infrastructure to steal data or show their technological prowess.
- **Civil Society:** Adversaries may target individuals, such as voters, campaign volunteers, or influential public figures, through phishing attacks, social engineering tactics, or surveillance activities to gather intelligence, manipulate opinions, or compromise their personal information.

The potential cyberattacks on these various sectors highlight the multifaceted nature of election security challenges and underscore the need for comprehensive cybersecurity measures to safeguard the integrity of the US election.

Recommendations

FortiGuard Labs Threat Research recommends the following best security practices to safeguard against cyber-attacks:

- **Employee Training and Awareness:** Conduct regular training sessions for election officials, political campaign staff, and volunteers to educate them about the risks of phishing attacks. Raise awareness about common phishing tactics, such as deceptive emails and fake websites, and teach employees how to identify and report suspicious emails.
- **Public Awareness Campaigns:** Launch public awareness campaigns to educate voters about the risks of phishing attacks and how to protect themselves from online threats. Provide guidance on recognizing phishing emails, avoiding suspicious links and attachments, and reporting potential phishing attempts to election authorities.
- **Protect Your Sensitive Data:** Organizations should make use of SOAR (Security Orchestration, Automation, and Response), which can detect unusual activities by privileged users and, if needed, block such activities. With the advent of ransomware, having complete and current backups of all your data can be a lifesaver. Backing up data is one of information security's best practices that has been gaining increased relevance in recent years. A strong backup strategy also means you are resilient to accidents. NOTE: Don't rely solely on online backups, and don't use the same passwords for your production environment and backups. It is always safe to have a backup of your cloud backup in another offsite backup location. All these backups should also be encrypted and should have access control set.
- **Monitor External Attack Surface:** It is vital to discover IT infrastructures your organization is exposed to, and that may be vulnerable to attack. We have commonly seen attackers selling RDP access and databases by abusing misconfigurations on web servers. Monitoring external attack surfaces allows security teams to protect their organizations from vulnerabilities and discover unknown assets and commonly abused services.
- **Enforce Multi-Factor Authentication and a Strong Password Policy:** We continuously monitor the Darknet for leaked credentials of organizational portals used by employees and regularly find them compromised and sold on the Darknet. Organizations can reduce the risk of such exposure by enforcing Multi-Factor Authentication and a strong password policy.
- **Endpoint Protection:** Even the best-trained staff occasionally makes mistakes. Antivirus and antimalware software installed on computers adds an extra layer of protection, especially against phishing attacks and credential stealers. The best antivirus and antimalware programs are only as good as their latest patches. Regularly installing patches will prevent hackers from exploiting the system's weaknesses.

- **Patch Operating Systems and Software Regularly**: Update software promptly as updates become available. Prioritize patching known exploited vulnerabilities, especially those CVEs that are reported as critical and high and that allow for remote code execution or denial-of-service on internet-facing equipment. Implement vendor-approved workarounds if a patch for a known exploited or critical vulnerability cannot be quickly applied.
 - **DDoS Protection**: Secure your infrastructure with DDoS attack prevention solutions. Equip your network, applications, and infrastructure with multi-level protection strategies. This may include prevention management systems that combine firewalls, VPNs, anti-spam, content filtering, and other security layers to monitor activities and identify traffic inconsistencies that may be symptoms of DDoS attacks.
 - **Preventing ransomware attacks**: Organizations must implement proactive measures, including regularly updating software and operating systems to patch known vulnerabilities. Additionally, organizations should regularly back up critical data and ensure that backups are stored securely offline to prevent them from being encrypted by ransomware. User education and awareness training are also essential to help employees recognize and avoid ransomware threats. By taking a multi-layered approach to ransomware prevention, organizations can significantly reduce their susceptibility to damaging attacks.
 - **Website Defacement**: Organizations should ensure the implementation of Web Application Firewalls (WAFs) that can provide an additional layer of defense by filtering and blocking malicious traffic before it reaches the website.
 - **Stealer Infection**: Carry out robust threat hunting based on the compromised account. Check AV/EDR and SIEM logs to identify any malicious activities. Once an infected system is identified, isolate it and perform reimaging.
 - **Threat Intelligence**: Cyber Threat Intelligence (CTI) helps enterprises collect data about current and potential cyber risks and determine those cyberattacks that can threaten their security. Darknet Threat Intelligence can also help organizations monitor any Darknet chatter related to the organization or any data leaks that can result in financial losses to the organizations before they are even out in the public. Such crucial and time-sensitive data can help organizations handle incidents appropriately and take the necessary legal steps.
-

Appendix A : Reliability Rating Criterion

FortiGuard Threat Research's Reliability rating is based upon the Admiralty System which is internationally accepted method for evaluating collected items of intelligence. The system comprises a two-character notation assessing the reliability of the source and the assessed level of confidence on the information.

Reliability of Source

A source is assessed for reliability based on a technical assessment of its capability, or in the case of Human Intelligence sources their history. Notation uses Alpha coding, A-F:

| | | |
|---|----------------------|--|
| A | Reliable | No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability. |
| B | Usually reliable | Minor doubts. History of mostly valid information. |
| C | Fairly reliable | Doubts. Provided valid information in the past. |
| D | Not usually reliable | Significant doubts. Provided valid information in the past. |
| E | Unreliable | Lacks authenticity, trustworthiness, and competency. History of invalid information. |
| F | Cannot be judged | Insufficient information to evaluate reliability. May or may not be reliable. |

Reliability of Information

An item is assessed for credibility based on likelihood and levels of corroboration by other sources. Notation uses a numeric code, 1-6.

| | | |
|---|----------------------|--|
| 1 | Reliable | Logical, consistent with other relevant information, confirmed by independent sources. |
| 2 | Usually reliable | Logical, consistent with other relevant information, not confirmed. |
| 3 | Fairly reliable | Reasonably logical, agrees with some relevant information, not confirmed. |
| 4 | Not usually reliable | Not logical but possible, no other information on the subject, not confirmed. |
| 5 | Unreliable | Not logical, contradicted by other relevant information. |
| 6 | Cannot be judged | The validity of the information cannot be determined. |

Appendix B : Relevance Rating Criterion

High

The Intelligence Report could be flagged with "High" Relevance under below criteria,

- > Threat Actor leaked or selling data pertaining to the customer organization in Public/Private Forum.
- > Threat Actor mentioned about customer organization in a Public/Private Forum
- > Public reporting on Organization was targeted.
- > Customer technology/product involved in an attack or being targeted.
- > Potential reputation harm to customer brand.
- > Customer related domains Typo-squat Fraudulent domains registered.
- > Proprietary customer related data found on internet. (Ex: GitHub containing source code)
- > Customer related domain email addresses found to be part of a data breach.
- > Customer specific keywords match identified across FortiGuard Threat Research's produced Intelligence.

Medium

The Intelligence Report could be flagged with "Medium" Relevance under below criteria,

- > Identification of Threat Actor targeting related Industry.
- > Vulnerability disclosed Potentially impacting Organization.
- > Public/Private breaches or incidents relating the organization's sector.
- > Public/Private Incident identified is Unique and Provides insights into new TTPs.





Low

The Intelligence Report could be flagged with "Low" Relevance under below criteria,

- > Public/Private Incident identified targeting non Customer specific industry.
- > Public/Private Incident identified outside of Customer geography vertical.
- > Public/Private Incident gaining significant Media Attention.
- > Data breaches or exposed data potentially impacting customer organization.

Appendix C : TLP Criterion

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared.

| TLP Level | How may it be shared ? |
|--|---|
|  <p>TLP : Red Not for disclosure, restricted to FortiGuard Threat Research and its customers who need to know the information.</p> | <p>Recipients may not share TLP:RED information with any parties outside of the organization. The information could only be shared within the organization and should be restricted to the ones who needs to know the information.</p> |
|  <p>TLP : Amber Limited disclosure, restricted to FortiGuard Threat Research's customer organization</p> | <p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.</p> |
|  <p>TLP : Green Limited disclosure, restricted to the community.</p> | <p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community.</p> |
|  <p>TLP : White Disclosure is not limited.</p> | <p>TLP:WHITE information may be distributed without restriction</p> |