Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems | CISA

Published: 2020-10-22 · Archived: 2026-04-05 19:14:25 UTC

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are warning that Iranian advanced persistent threat (APT) actors are likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process.

The APT actors are creating fictitious media sites and spoofing legitimate media sites to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud.

The APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, structured query language (SQL) injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns.

Click here for a PDF version of this report.

Technical Details

These actors have conducted a significant number of intrusions against U.S.-based networks since August 2019. The actors leveraged several Common Vulnerabilities and Exposures (CVEs)—notably CVE-2020-5902 and CVE-2017-9248—pertaining to virtual private networks (VPNs) and content management systems (CMSs).

- CVE-2020-5902 affects F5 VPNs. Remote attackers could exploit this vulnerability to execute arbitrary code. [1].
- CVE-2017-9248 affects Telerik UI. Attackers could exploit this vulnerability in web applications using Telerik UI for ASP.NET AJAX to conduct cross-site scripting (XSS) attacks.[2]

Historically, these actors have conducted DDoS attacks, SQL injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns. These activities could render these systems temporarily inaccessible to the public or election officials, which could slow, but would not prevent, voting or the reporting of results.

- **A DDoS attack** could slow or render election-related public-facing websites inaccessible by flooding the internet-accessible server with requests; this would prevent users from accessing online resources, such as voting information or non-official voting results. In the past, cyber actors have falsely claimed DDoS attacks have compromised the integrity of voting systems in an effort to mislead the public that their attack would prevent a voter from casting a ballot or change votes already cast.

- **A SQL injection** involves a threat actor inserting malicious code into the entry field of an application, causing that code to execute if entries have not been sanitized. SQL injections are among the most dangerous and common exploits affecting websites. A SQL injection into a media company's CMS could enable a cyber actor access to network systems to manipulate content or falsify news reports prior to publication.
- **Spear-phishing messages** may not be easily detectible. These emails often ask victims to fill out forms or verify information through links embedded in the email. APT actors use spear phishing to gain access to information—often credentials, such as passwords—and to identify follow-on victims. A malicious cyber actor could use compromised email access to spread disinformation to the victims' contacts or collect information sent to or from the compromised account.
- **Public-facing website defacements** typically involve a cyber threat actor compromising the website or its associated CMS, allowing the actor to upload images to the site's landing page. In situations where such public-facing websites relate to elections (e.g., the website of a county board of elections), defacements could cast doubt on the security and legitimacy of the websites' information. If cyber actors were able to successfully change an election-related website, the underlying data and internal systems would remain uncompromised..
- **Disinformation campaigns** involve malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, or discredit the electoral system. Malicious actors often use social media as well as fictitious and spoofed media sites for these campaigns. Based on their corporate policies, social media companies have worked to counter these actors' use of their platforms to promote fictitious news stories by removing the news stories, and in many instances, closing the accounts related to the malicious activity. However, these adversaries will continue their attempts to create fictitious accounts that promote divisive storylines to sow discord, even after the election.

Mitigations

The following recommended mitigations list includes self-protection strategies against the cyber techniques used by the APT actors:

- Validate input—input validation is a method of sanitizing untrusted input provided by web application users. Implementing input validation can protect against security flaws of web applications by significantly reducing the probability of successful exploitation. Types of attacks possibly prevented include SQL injection, XSS, and command injection.
- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP; do not have open RDP ports, unless there is a valid business reason to do so. Place any system with an open RDP port behind a firewall, and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- Apply multi-factor authentication, when possible.
- Apply system and software updates regularly, particularly if you are deploying products affected by CVE-2020-5902 and CVE-2017-9248.

    - For patch information on CVE-2020-5902, refer to F5 Security Advisory K52145254 .
    - For patch information on CVE-2017-9248, refer to Progress Telerik details for CVE-2017-9248 .
- Maintain a good information back-up strategy that involves routinely backing up all critical data and system configuration information on a separate device. Store the backups offline; verify their integrity and restoration process.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days, and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access are required to follow internal policies on remote access.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as VPNs, recognizing VPNs are only as secure as the connected devices.
- Be aware of unsolicited contact on social media from any individual you do not know.
- Be aware of attempts to pass links or files via social media from anyone you do not know.
- Be aware of unsolicited requests to share a file via online services.
- Be aware of email messages conveying suspicious alerts or other online accounts, including login notifications from foreign countries or other alerts indicating attempted unauthorized access to your accounts.
- Be suspicious of emails purporting to be from legitimate online services (e.g., the images in the email appear to be slightly pixelated and/or grainy, language in the email seems off, the email originates from an IP address not attributable to the provider/company).
- Be suspicious of unsolicited email messages that contain shortened links (e.g., via `tinyurl` , `bit.ly`).
- Use security features provided by social media platforms, use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches; automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed at which threat actors create exploits after a patch is released. These "N-day" exploits can be as damaging as a zero-day exploits. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to ensure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.[3] In addition to updating the application, use tools (e.g., the OWASP Dependency-Check Project tool[4]) to identify publicly known vulnerabilities in third-party libraries that the application depends on.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (SQL injection, cross-site scripting, etc.); use a commercial web application vulnerability scanner in combination with a source code scanner.[5] As vulnerabilities are found, they should be fixed or patched. This is especially crucial for networks that host older web applications; as sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

Deploy a web application firewall (WAF) to help prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware.[6] Malicious cyber actors often deploy web shells—software that can enable remote administration—on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands, which are commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, with remote access, and/or used on high value assets.[7] Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs).[8] Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remedite critical web application security risks first; then, move on to other less critical vulnerabilities. Follow available guidance on securing web applications.[9],[10],[11]

How do I respond to unauthorized access to election-related systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.dhs.gov or 888-282-0870) or the Federal Bureau of Investigation (FBI) through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

Resources

- CISA Tip: Best Practices for Securing Election Systems
- CISA Tip: Securing Voter Registration Data
- CISA Tip: Website Security
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Securing Network Infrastructure Devices
- CISA Activity Alert: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Insights: Actions to Counter Email-Based Attacks On Election-related Entities
- FBI and CISA Public Service Announcement (PSA): Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- FBI and CISA PSA: Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- FBI and CISA PSA: Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- FBI and CISA PSA: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- FBI and CISA PSA: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

References

[1] F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902

[2] Progress Telerik details for CVE-2017-9248

[4] OWASP Dependency-Check

[10] OWASP Top Ten

[11] 2020 CWE Top 25 Most Dangerous Software Weaknesses

Revisions

October 22, 2020: Initial Version
