



## Iran Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Iranian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes [a complete list of related CISA publications](#), many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Iranian government actors). Additionally, this page provides instructions on how to [report related threat activity](#).



Iranian cyber threat actors have been continuously improving their offensive cyber capabilities. Iran has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries. They continue to engage in conventional offensive cyber activities ranging from website defacement, spearphishing, distributed denial-of-service attacks, and theft of personally identifiable information, to more advanced activities—including destructive malware, social media-driven influence operations, and, potentially, cyberattacks intended to cause physical consequences.

The U.S. intelligence community and various private sector threat intelligence organizations have identified Iran's Islamic Revolutionary Guard Corps (IRGC) as a driving force behind Iranian state-sponsored cyberattacks, either through IRGC contractors in the Iranian private sector or by the IRGC itself. According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US and allied networks and data." The Assessment states that "Iran has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities."<sup>[1]</sup>

### Latest U.S. Government Report on Iranian Malicious Cyber Activity

On November 17, 2021, CISA, the Federal Bureau of Investigation (FBI), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) released a joint Cybersecurity Advisory highlighting ongoing malicious cyber activity by an advanced persistent threat (APT) group that CISA, FBI, ACSC, and NCSC assess is associated with the government of Iran. FBI and CISA have observed this Iranian government-sponsored APT group exploit Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware this APT group has used the same Microsoft Exchange vulnerability in Australia. See [AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities](#).

The [Iranian Malicious Cyber Activity](#) section below lists all CISA Advisories, Alerts, and Malware Analysis Reports (MARs) on Iranian malicious cyber activities.

[Expand All Sections](#)

#### Iranian Malicious Cyber Activity

Much of the information contained in the Advisories, Alerts, and MARs listed below is the result of analytic efforts between CISA, the U.S. Department of Defense, and FBI to provide technical details on the tools and infrastructure used by Iranian state-sponsored cyber actors. The publications below include descriptions of Iranian malicious cyber activity, technical details, and recommended mitigations. Users and administrators should flag activity associated with the information in the products listed in table 1 below, report the activity to [CISA](#) or [FBI Cyber Watch \(CyWatch\)](#)<sup>☞</sup>, and give the activity the highest priority for enhanced mitigation.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
November 17, 2021	<ul style="list-style-type: none"><li><a href="#">CISA-FBI-ACSC-NCSC Joint Cybersecurity Advisory: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities</a></li></ul>	<ul style="list-style-type: none"><li>CISA, FBI, ACSC, and NCSC have released a joint CSA on Iranian government-sponsored APT actors exploiting Microsoft Exchange and Fortinet vulnerabilities to gain initial access in advance of follow-on operations. The Iranian government-sponsored APT actors are actively targeting a broad range of multiple U.S. critical infrastructure sectors as well as Australian organizations.</li></ul>
July 20, 2021	<ul style="list-style-type: none"><li><a href="#">JSAR-12-241-01B: Shamoon/DistTrack Malware (Update B)</a></li></ul>	<ul style="list-style-type: none"><li>U.S. Government attributed previously published activity targeting industrial control systems to Iranian nation-state cyber actors.</li></ul>
October 30, 2020	<ul style="list-style-type: none"><li><a href="#">CISA and FBI Joint Cybersecurity Advisory: Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data</a></li></ul>	<ul style="list-style-type: none"><li>CISA and FBI released a Joint CSA on an Iranian APT actor targeting U.S. state websites, including elections websites, to obtain voter registration data. The Advisory provides indicators of compromise (IOCs) and recommended mitigations for affected entities.</li></ul>
October 22, 2020	<ul style="list-style-type: none"><li><a href="#">CISA-FBI Joint Cybersecurity Advisory: Iranian Advanced Persistent Threat Actors Threaten Election-Related System</a></li></ul>	<ul style="list-style-type: none"><li>CISA and FBI released an Advisory warning about Iranian APT actors likely intent on influencing and interfering with the 2020 U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process.</li></ul>
September 15, 2020	<ul style="list-style-type: none"><li><a href="#">CISA-FBI Joint Cybersecurity Advisory: Iran-Based Threat Actor Exploits VPN Vulnerabilities</a></li><li><a href="#">MAR-10297887-1.v2 – Iranian Web Shells</a></li></ul>	<ul style="list-style-type: none"><li>CISA and FBI released a Joint CSA on an Iran-based malicious cyber actor targeting several U.S. federal agencies and other U.S.-based networks. The Advisory analyzes the threat actor's tactics, techniques, and procedures (TTPs); IOCs; and exploited Common Vulnerabilities and Exposures.</li><li>The MAR details the functionality of malicious files—including multiple components of the China Chopper Web Shell—used by Iranian-based malicious cyber actors.</li></ul>
January 06, 2020	<ul style="list-style-type: none"><li><a href="#">CISA Alert: Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad</a></li><li><a href="#">CISA Insights: Increased Geopolitical Tensions and Threats</a></li></ul>	<ul style="list-style-type: none"><li>In light of heightened tensions between the United States and Iran, CISA released an Alert and an “Insights” analysis providing Iranian government and affiliated cyber threat actor TTPs and an overview of Iran’s cyber threat profile, respectively.</li></ul>

#### Report Activity Related to This Threat

CISA encourages all organizations to urgently report any additional information related to this threat. Users and administrators should flag associated activity, report the activity to CISA (see below) or [FBI Cyber Watch \(CyWatch\)](#)<sup>☞</sup>, and give the activity the highest priority for enhanced mitigation.

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- [Central@cisa.gov](mailto:Central@cisa.gov)<sup>☞</sup> (UNCLASS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA homepage at <https://www.us-cert.cisa.gov/>.


#### Mitigate and Detect This Threat

#### Respond to an Incident

#### References

### Contact Us

 (888)282-0870

 [Send us email](mailto:Send us email)<sup>☞</sup>

 Download PGP/GPG keys

 Submit website feedback

### Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

Report

HSIN

