

Learn more about [LSEG](#)



My News

Cybersecurity

The Iranians who hacked Trump's campaign have deep expertise

By Christopher Bing and Gram Slattery

August 23, 2024 8:01 PM GMT+9:30 · Updated 9 days ago



Figurines with computers are seen in front of USA and Iran flags in this illustration taken, September 10, 2022. REUTERS/Dado Ruvic/Illustration/File Photo [Purchase Licensing Rights](#)

Summary Companies

Hacker group APT42 may be linked to Iranian military intelligence division known for invasive espionage
Experts highlight APT42's use of mobile malware for surveillance
APT42 targets anti-Iran activists, journalists and U.S. officials

Aug 23 (Reuters) - The Iranian [hacking team that compromised the campaign](#) of Republican presidential candidate [Donald Trump](#) is known for placing surveillance software on the mobile phones of its victims, enabling them to record calls, steal texts and silently turn on cameras and microphones, according to researchers and experts who follow the group.

Known as APT42 or CharmingKitten by the cybersecurity research community, the accused Iranian hackers are widely believed to be associated with an intelligence division inside Iran's military, known as the Intelligence Organization of the Islamic Revolutionary Guard Corps or IRGC-IO. Their appearance in the U.S. election is noteworthy, sources told Reuters, because of their invasive espionage approach against high-value targets in Washington and Israel.

"What makes (APT42) incredibly dangerous is this idea that they are an organization that has a history of physically targeting people of interest," said John Hultquist, chief analyst with U.S. cybersecurity firm Mandiant, who referenced [past research](#) that found the group

Feedback

surveilling the cell phones of Iranian activists and protesters. Some of them were imprisoned or physically threatened in the country shortly after being hacked.

Advertisement · Scroll to continue

A spokesperson for Iran's permanent mission to the United Nations in New York said in an email that "the Iranian government neither possesses nor harbors any intent or motive to interfere in the United States presidential election."



Spokespeople for Trump have said that Iran is targeting the former president and current Republican candidate because they disfavor his policies toward Tehran.

HIGHLY TARGETED

The APT42 crew that targeted Trump has never been formally named in U.S. law enforcement indictments or criminal charges, leaving questions about their structure and identity. But experts believe they represent a significant threat.

Advertisement · Scroll to continue

"The IRGC-IO is entrusted with collecting intelligence to defend and advance the interests of the Islamic Republic," said Levi Gundert, chief security officer for U.S. cyber intelligence firm Recorded Future and a former Secret Service special agent. "Along with the Quds Force, they are the most powerful security and intelligence entities inside Iran."

In March, Recorded Future analysts discovered hacking attempts by APT42 against a U.S.-based media group named Iran International, which British authorities [previously said](#)  were the target of [physical violence](#)  and terror threats by Iranian-linked agents.

Advertisement · Scroll to continue

Feedback

Hultquist said the hackers commonly use mobile malware that allows them to "record phone calls, room audio recordings, pilfer SMS (text) inboxes, take images off of a machine," and gather geolocation data.

In recent months, Trump campaign officials sent a message to employees warning them to be diligent about information security, according to one person familiar with the message. The message warned that cell phones were no more secure than other devices and represented an important point of vulnerability, said the person, who requested anonymity as he was not permitted to speak to the media.

The Trump campaign did not respond to a request for comment. The FBI and the Office of the Director of National intelligence both declined to comment.

The Secret Service did not answer questions about whether the Iranian hacking activity could be intended to support physical attacks planned for the future. In a statement sent to Reuters, a Secret Service spokesperson said they work closely with intelligence community partners to ensure the "highest level of safety and security" but could not discuss matters "related to protective intelligence."

APT42 also commonly impersonates journalists and Washington think tanks in complex, email-based social engineering operations that aim to lure their targeting into opening booby-trapped messages, which let them takeover systems.

The group's "credential phishing campaigns are highly targeted and well-researched; the group typically targets a small number of individuals," said Josh Miller, a threat analyst with email security company Proofpoint. They often target anti-Iran activists, reporters with access to sources inside Iran, Middle Eastern academics and foreign-policy advisers. This has included the hacking of western government officials and American defense contractors.

For example, in 2018, the hackers targeted nuclear workers and U.S. Treasury department officials around the time the United States formally withdrew from the Joint Comprehensive Plan of Action (JCPOA), said Allison Wikoff, a senior cyber intelligence analyst with professional services company PricewaterhouseCoopers.

The public emergence of APT42 in the [ongoing presidential race](#) began earlier this month following a [report](#) [↗] by Microsoft ([MSFT.Q](#)) [↗] on Aug. 9, which said the group was attempting to hack staffers on an unnamed presidential campaign.


APT42 is still actively targeting campaign officials and former Trump administration figures critical of Iran, according to [a blog post](#) [↗] by Google's cybersecurity research team.

| The Reuters Daily Briefing newsletter provides all the news you need to start your day. Sign up [here](#).

Reporting by Christopher Bing and Gram Slattery in Washington; Editing by Chris Sanders and Matthew Lewis

Our Standards: [The Thomson Reuters Trust Principles](#). [↗]


Purchase Licensing Rights





Christopher Bing


Thomson Reuters

Award-winning reporter covering the intersection between technology and national security with a focus on how the evolving cybersecurity landscape affects government and business.












Gram Slattery


Thomson Reuters

Washington-based correspondent covering campaigns and Congress. Previously posted in Rio de Janeiro, Sao Paulo and Santiago, Chile, and has reported extensively throughout Latin America. Co-winner of the 2021 Reuters Journalist of the Year Award in the business coverage category for a series on corruption and fraud in the oil industry. He was born in Massachusetts and graduated from Harvard College.









Feedback

Read Next

World
South Korea police launch probe into Telegram over online sex crimes, Yonhap reports
ago

World
Behind the arrest of Telegram boss, a small Paris cybercrime unit with big ambitions
August 30, 2024

Cybersecurity
CrowdStrike exec to testify before Congress on IT outage
August 30, 2024

World
Russia uses Telegram boss Pavel Durov's case to rally doubters against West
August 30, 2024

World >

Feedback

Malaysia, New Zealand PMs call for immediate ceasefire in Gaza

Asia Pacific · September 2, 2024 · 1:31 PM GMT+9:30 · 10 min ago

Malaysia Prime Minister Anwar Ibrahim and his New Zealand counterpart Chris Luxon on Monday said they were united in calling for an immediate ceasefire in the conflict in Gaza and

Cybersecurity

South Korea police launch probe into Telegram over online sex crimes, Yonhap reports

16 min ago

Europe

Russian 'spy whale' Hvaldimir found dead near Norway

38 min ago

Europe

Russia pounds Kyiv with missiles, Ukraine's military says

42 min ago

Woman dead, 120,000 without power as damaging storms hit Australia

an hour ago

Latest

Home

Authors

Topic sitemap

Archive

Sitemap

Media

 Videos

 Pictures

 Graphics

Browse

World

Business

Markets

Sustainability

Legal

Breakingviews

Technology

Investigations

Sports

Science

Lifestyle

About Reuters

About Reuters 

Careers 

Reuters News Agency 

Brand Attribution Guidelines 

Reuters Leadership 

Reuters Fact Check

Reuters Diversity Report 

Stay Informed

Download the App (iOS) 

Download the App (Android) 

Feedback

Newsletters

Information you can trust

Reuters, the news and media division of Thomson Reuters, is the world’s largest multimedia news provider, reaching billions of people worldwide every day. Reuters provides business, financial, national and international news to professionals via desktop terminals, the world's media organizations, industry events and directly to consumers.

Follow Us



Thomson Reuters Products

Westlaw [↗](#)

Build the strongest argument relying on authoritative content, attorney-editor expertise, and industry defining technology.

Onesource [↗](#)

The most comprehensive solution to manage all your complex and ever-expanding tax and compliance needs.

Checkpoint [↗](#)

The industry leader for online information for tax, accounting and finance professionals.

LSEG Products

Workspace [↗](#)

Access unmatched financial data, news and content in a highly-customised workflow experience on desktop, web and mobile.

DataCatalogue [↗](#)

Browse an unrivalled portfolio of real-time and historical market data and insights from worldwide sources and experts.

World-Check [↗](#)

Screen for heightened risk individual and entities globally to help uncover hidden risks in business relationships and human networks.

[Advertise With Us \[↗\]\(#\)](#) [Advertising Guidelines](#) [Purchase Licensing Rights \[↗\]\(#\)](#)

All quotes delayed a minimum of 15 minutes. See [here](#) for a complete list of exchanges and delays.

[Cookies \[↗\]\(#\)](#) [Terms of Use](#) [Privacy \[↗\]\(#\)](#) [Digital Accessibility \[↗\]\(#\)](#) [Corrections](#) [Site Feedback \[↗\]\(#\)](#)

© 2024 Reuters. All rights reserved

Feedback

