Iranian ODMAI Server NRZ

Overview

A threat actor with ties to Iran has had their entire working infrastructure exposed after carelessly leaving an open directory on their own staging server, handing researchers a rare look into a live botnet operation. A significant operational security failure by Iranian-nexus threat actors has exposed an active cyberespionage campaign against the Omani government. An exposed staging server hosted on a United Arab Emirates virtual private network exposed the attackers' entire playbook in plain sight, including. An open directory on 172. The leak revealed a 15-node relay network, a mass SSH deployment framework, DDoS. The Justice Department announced the seizure of four domains as part of an ongoing effort to disrupt hacking and transnational repression schemes conducted by the Islamic Republic of Iran's Ministry of Intelligence and Security (MOIS). The affidavit supporting the seizure warrant can be found here. The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center (DC3) are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders that, as of August 2024, a group of Iran-based cyber actors. APT35: APT35 (Charming Kitten) is an Iranian state-

linked hacking group known for cyber-espionage, targeting global organizations with phishing and malware.

Iranian ODMAI Server NRZ

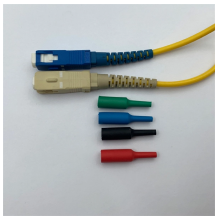
A significant operational security failure by Iranian-nexus threat actors has exposed an active cyberespionage campaign against the Omani government. An exposed staging server hosted ...

Live cyber conflict dashboard tracking Iran–Israel cyber activity: attacks, hacktivist claims, threat actors, and key events — curated for journalists and cybersecurity professionals.

Iran-linked hacker exposed after open server leak reveals botnet tools, SSH scripts, DDoS binaries, and active C2 development infrastructure.

This repository is a compiled list of public information about websites hosted in Iran. It is intended for informational purposes only and is not intended to provide guidance on how to connect to or create ...

The Bureaucracy of Espionage Dubbed “Episode 4,” the data leak offers a rare, unvarnished look into the machinery behind Iran''s state-sponsored cyberattacks. The files—three CSV ...



"Iran Hosted Domains" is a comprehensive list of Iranian domains and services that are hosted within the country. - Releases · bootmortis/iran-hosted-domains.

The FBI further assesses these Iran-based cyber actors are associated with the Government of Iran (GOI) and—separate from the ransomware activity—conduct computer network ...

"Iran Hosted Domains" is a comprehensive list of Iranian domains and services that are hosted within the country. - Ghasem22/iran-shiravsni

An exposed UAE-hosted VPS revealed an Iranian-nexus operation against Oman''s government, with 26,000 citizen records pulled from the Justice Ministry.

The Justice Department announced the seizure of four domains as part of an ongoing effort to disrupt hacking and transnational repression schemes conducted by the Islamic Republic of ...

Contact Us

For more information, pricing, or custom data center solutions, please contact us:

Website: https://yoahorroenergia.es
Email: hello@yoahorroenergia.es
Phone: +233 54 318 7269
Address: Plot 28, Spintex Road, Accra, Greater Accra, Ghana

This document is for informational purposes only. Specifications subject to change without notice.