CyberAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- The Evolution Of Cybersecurity Companies In Virginia: From Startups To Industry Leaders (VA)
- GuidePoint Security Champions Cybersecurity Awareness Month With New Educational Resources, Events (VA)
- Budget Restrictions, Staff Issues And AI Are Threats To States' Cybersecurity (VA)
- Time To Act: CISA & FBI Call For Vigilance Against Iranian Cyberattacks
- American Water Hit By Cyber-Attack, Billing Systems Disrupted
- Large Scale Google Ads Campaign Targets Utility Software
- Man Pleads Guilty To Stealing $37 Million In Crypto From 571 Victims
- Elaborate Deepfake Operations Takes A Meeting With US Senator
- MoneyGram Confirms Customer Data Breach
- Chinese Hackers Reportedly Breached ISPs Including AT&T, Verizon
- Company Behind Major Social Security Number Leak Files For Bankruptcy
- UN: Telegram Harbors Underground Network For Deepfake Software Sales?
- The Three "T's" Of Device Lifecycle Management

Training Opportunities:

Must be a US Criminal Justice Practitioner for the below courses

- NW3C - Lunch And Learn With Binance, Roblox, And Kodex - Virtual - 10/22/2024
- NW3C - ICAC - Navigating Risks On Social Media: A Guide To Online Monitoring And Collection - Virtual - 10/29/2024
- NW3C - Crime Risks Enabled By Generative AI - Virtual - 10/31/2024

    - NW3C - Telegram Investigations - Virtual - 11/14/2024
- **Webinars**
    - Social Engineering: New Tricks, New Threats, New Defenses - Virtual - 10/22/2024
    - 10 Emerging Vulnerabilities Every Enterprise Should Know - Virtual - 10/29/2024
    - Data-Driven Security: Turning Incidents Into Strategic Assets - Virtual - 10/29/2024
    - Don't Get Hacked Twice: The Critical Role Of Clean Backups In Cyber Resilience - Virtual - On Demand?
    - How To Assess And Hone Your Security Program - Virtual - 10/17/2024
    - 10 Emerging Vulnerabilities Every Enterprise Should Know - Virtual - 10/29/2024

- Tools and Resources -

Resource | Joint Cybersecurity Advisory

Iranian Cyber Actors' Brute Force And Credential Access Activity Compromises CI Organizations

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Communications Security Establishment Canada (CSE), Australian Federal Police (AFP), and Australian Signals Directorate?s Australian Cyber Security Centre (ASD?s ACSC) are releasing this joint Cybersecurity Advisory to warn network defenders of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The actors likely aim to obtain credentials and information describing the victim?s network that can then be sold to

enable access to cybercriminals.

Since October 2023, Iranian actors have used brute force, such as password spraying, and multifactor authentication (MFA) ?push bombing? to compromise user accounts and obtain access to organizations. The actors frequently modified MFA registrations, enabling persistent access. The actors performed discovery on the compromised networks to obtain additional credentials and identify other information that could be used to gain additional points of access. The authoring agencies assess the Iranian actors sell this information on cybercriminal forums to actors who may use the information to conduct additional malicious activity.

View Advisory

Resource | PWC

Technology Risk: So Pervasive, It's Hard To See

Some risks are so all-encompassing they go unnoticed. Hiding in plain sight, their sheer scale, paradoxically, can obscure their sheer scale. Instead, we get glimpses here and there but rarely connect the dots across the enterprise.

This is a central problem of technology risk, a term describing the many vulnerabilities associated with an organization's information technology (IT), operational technology (OT) and communications technology (CT). Because technology touches everything a company does, all its assets (physical, digital, intellectual), its people, processes and systems, its vendors and suppliers, its reputation - even its very existence - the scope and layers of risk associated with technology's use can be difficult to comprehend, much less mitigate.

View Resource

Resource | Joint Advisory

Update On SVR Cyber Operations And Vulnerability Exploitation

The National Security Agency joins the Federal Bureau of Investigation, the United States Cyber Command's Cyber National Mission Force, and the United Kingdom National Cyber Security Centre to warn network defenders about ongoing Russian Federation Foreign Intelligence Service (SVR) cyber threats and to recommend rapid countermeasures for security patching and mitigating systems.

The attached joint Cybersecurity Advisory highlights how Russian SVR cyber actors are currently exploiting a set of software vulnerabilities and have intentions to exploit additional vulnerabilities. It provides a detailed list of publicly disclosed common vulnerabilities and exposures and a list of mitigations to improve cybersecurity posture based on the SVR cyber actors operations.

View Advisory

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online

Not a VFC Shield Member?

Join Today

Useful Links

webversion

VFC Fusion Site

VFC Shield

Report SAR

Shield Homepage

Virginia Fusion Center
7700 Midlothian Turnpike
N. Chesterfield, VA 23235

Email Coordinator

All Products

— — —