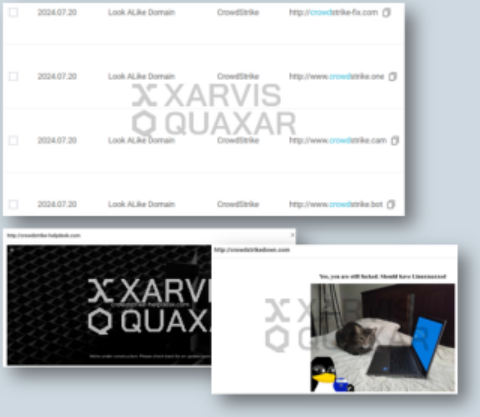
Dark web & Telegram
Weekly Highlights

August Week 1

Numerous Phishing Sites Detected Following CrowdStrike IT Crisis

- On July 19, following a global IT crisis triggered by CrowdStrike, numerous websites impersonating CrowdStrike or falsely offering remediation services were detected by S2W.
- S2W's analysis identified around 150 websites using terms like 'CrowdStrike,' 'Fix,' or 'Repair,' or substituting '.com' with other suffixes since the incident. Many were likely established to capitalize on the event, with some posing security risks.
- Given these developments, such incidents often lead to malicious activities targeting businesses and consumers. It is crucial to seek professional advice immediately in these situations.



Venezuelan Military Data Leak in Response to Dictator's Reelection and Alleged Corruption

- On July 31st, BreachForums published a post revealing leaked Venezuelan military data.
- A Threat actor named 'Valerie' leaked Venezuelan military data, which includes personal information of military personnel and various internal documents.
- Valerie attributed the leak to the Venezuelan presidential election on July 28th, where dictator Nicolas Maduro secured reelection amid allegations of electoral fraud, sparking both domestic protests and extensive online condemnation.

Islamic Hacktivist Group 'LulzSec Muslim' Leaks Thousands of Personal Details from Paris Olympics Website

- Amid the 2024 Paris Olympics, LulzSec Muslims, an active hacktivist group on Telegram, claimed to have breached the Olympics website and leaked data.
- On July 31st , the group announced a successful attack on the Paris Olympics website via their Telegram channel, which resulted in the leak of personal information for approximately 3,000 rows.
- The group cited religious motivations for their attack, aligning with their support for Palestine in the Israel-Palestine conflict and targeting France due to its backing of Israel.

COPYRIGHT © 2024 S2W Inc. All rights reserved