LevelBlue - Open Threat Exchange

By Q.Vashti

Archived: 2026-04-29 08:01:22 UTC

- 138 Subscribers

- 267 Subscribers

Breaking Down the Role of Cyber Operations Taken in the Iran Crisis

CVE: 1 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 1 | **Domain:** 1

The report analyzes the cyber aspects of the ongoing conflict between Iran, the US, and Israel. It details a massive cyberattack launched by the US and Israel against Iran, causing widespread internet disruptions and infrastructure failures. The report also covers the activation and retooling of Iranian APT groups for retaliatory operations, targeting critical infrastructure in the US, Israel, and allied countries. Key actors include MuddyWater, Charming Kitten, OilRig, and Elfin. The analysis covers tactics, techniques, and procedures used by these groups, as well as their strategic objectives. The report also discusses the involvement of hacktivist proxies and the victimology of the attacks, affecting multiple countries and industries.

- 379,496 Subscribers

- 267 Subscribers

- 183 Subscribers

- 183 Subscribers

- 848 Subscribers

remcos rat

CVE: 1 | **FileHash-MD5:** 34 | **FileHash-SHA1:** 14 | **FileHash-SHA256:** 9 | **URL:** 10 | **Domain:** 1 | **Email:** 1 | **Hostname:** 2

- 128 Subscribers

- 164 Subscribers

- 61 Subscribers

Microsoft investigates Iranian attacks against the Albanian government - Microsoft Security Blog

CVE: 2 | **FileHash-MD5:** 7 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 20

Shortly after the destructive cyberattacks against the Albanian government in mid-July, the Microsoft Detection and Response Team (DART) was engaged by the Albanian government to lead an investigation into the attacks. At the time of the attacks and our engagement by the Albanian government, Microsoft publicly stated that “Microsoft is committed to helping our customers be secure while achieving more. During this event, we quickly mobilized our Detection and Response Team (DART) to help the Albanian government rapidly recover from this cyber-attack. Microsoft will continue to partner with Albania to manage cybersecurity risks while continuing to enhance protections from malicious attackers.” This blog showcases the investigation, Microsoft’s process in attributing the related actors and the observed tactics and techniques observed by DART and the Microsoft Threat Intelligence Center (MSTIC) to help customers and the security ecosystem defend from similar attacks in the future.

- 267 Subscribers

Author Url

Microsoft investigates Iranian attacks against the Albanian government - Microsoft Security Blog

CVE: 2 | **FileHash-MD5:** 7 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 19 | **Domain:** 1

Microsoft assessed with high confidence that on July 15, 2022, actors sponsored by the Iranian government conducted a destructive cyberattack against the Albanian government, disrupting government websites and public services. At the same time, and in addition to the destructive cyberattack, MSTIC assesses that a separate Iranian state-sponsored actor leaked sensitive information that had been exfiltrated months earlier. Various websites and social media outlets were used to leak this information.

- 128 Subscribers

- 164 Subscribers

- 267 Subscribers

- 354 Subscribers

Iran attack on Albania IOCs

CVE: 1 | **FileHash-MD5:** 18 | **FileHash-SHA1:** 14 | **FileHash-SHA256:** 9

The FBI and CISA have released a report on recent cyber attacks against the Government of Albania, which was targeted by Iranian state cyber actors in July and September 2022, as well as a series of similar attacks in September.

- 128 Subscribers

- 848 Subscribers

- 354 Subscribers

- 848 Subscribers

- 848 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:ZeroCleare