uMercs Threat Intel

April 2026 | Offensive Security Intelligence

Iran Goes Dark. The Threat Doesn't.

April 2026 -- Geopolitical Escalation, Ransomware Evolution, and the Cisco Zero-Day You May Have Missed

FEATURE

Operation Epic Fury and the New Cyber Threat Landscape

uMercs Research Team | April 2026

On February 28, 2026, the United States and Israel launched coordinated strikes -- Operation Epic Fury and Operation Roaring Lion -- triggering an immediate multi-vector Iranian cyber retaliation campaign. Within hours, Iran's internet connectivity collapsed to between 1% and 4% of normal capacity, where it has remained for over 27 days.

The good news: Iran's primary nation-state cyber units are operating in near-total isolation. Command and control infrastructure is degraded. Coordinated, high-sophistication attacks from within Iran are unlikely in the short term.

The bad news: proxy groups and Iran-aligned threat actors operating outside Iran are active, unsupervised, and increasingly autonomous. Unit 42 has identified a surge in conflict-themed phishing campaigns spanning 7,381 URLs across 1,881 hostnames -- targeting telecoms, airlines, law enforcement, and energy corporations.

For organizations with exposure to Middle Eastern supply chains, government contractors, or critical infrastructure: this is a live threat environment. The sophistication bar is temporarily lower, but volume and opportunism have increased significantly.

Operationally, this is the security equivalent of a distributed cell going rogue -- unpredictable, lower-coordination, but capable of real damage. Monitor for impersonation lures exploiting geopolitical themes or regional brand trust.

This Month's Threats

- Iranian APT activity surging via proxy groups
- Uragan ransomware: double-extortion strain
- Cisco FMC zero-day exploited by Interlock
- Conflict-themed phishing: 7,381+ URLs
- Seedworm targets U.S. banks and airports

Threat Actor Spotlight

Seedworm (Iranian APT): Active on U.S. bank, airport, and software company networks since Feb 2026. TTPs: spear-phishing, known CVE exploitation, covert C2 infrastructure.

Tarnished Scorpius: Iran-aligned, opportunistic targeting of perceived adversaries. Low-medium sophistication, high volume.

CVE WATCH

CVE-2026-20131

Cisco FMC Zero-Day -- RCE

Actively exploited by Interlock ransomware since January 2026. Grants root access on Cisco Firepower Management Center. Patch immediately.

CVE-2026-21262

SQL Server -- Elevation of Privilege

Publicly disclosed before patch. Escalates to SQLAdmin via improper access control. High-value in post-compromise lateral movement. Affects SQL Server 2016+.

CVE-2026-26144

Excel / Copilot -- Data Exfiltration

Zero-click information disclosure via Microsoft Copilot Agent mode. Exfiltrates data through unintended network egress. DLP tools are blind to this vector. Audit Copilot deployments.

RANSOMWARE WATCH

Uragan Ransomware: Double Extortion, No Decryptor

CYFIRMA's threat intelligence team identified a new ransomware strain -- Uragan -- circulating on underground forums this month. The malware encrypts files, appends a .uragan extension, and drops a README.txt ransom note. Standard double extortion: pay or your data leaks.

What makes Uragan worth flagging is its operational profile: no sector-specific targeting, indicating broad opportunistic campaigns across enterprise endpoints. TTPs map cleanly to MITRE: T1059 (scripting), T1055 (process injection), T1486 (data encryption), T1003 (credential dumping).

Key defensive implication: Uragan specifically warns victims against third-party recovery tools -- the operators are actively trying to block IR playbooks. Backup integrity and offline recovery are your primary mitigations. No public decryptor exists.

Uragan TTPs (MITRE)

- T1059 -- Command and Scripting Interpreter
- T1055 -- Process Injection
- T1486 -- Data Encrypted for Impact
- T1003 -- OS Credential Dumping
- T1562.001 -- Disable Security Tools
- T1112 -- Modify Registry
- T1489 -- Service Stop

GEOPOLITICAL INTELLIGENCE

Conflict-Themed Phishing: Scale and Sophistication

Unit 42's tracking since February 28 reveals the full operational playbook: parallel campaigns across financial fraud, credential harvesting, and wiper staging -- using domain rotation, subdomain chaining, and purpose-built infrastructure to evade blocklists.

Specific targets include UAE-focused Emirates brand impersonation, Saudi Arabia ERP credential phishing, Iranian bank masquerading, and Dubai government authority impersonation for credit card theft. Technical fingerprints: newly registered domains, cdn-cgi/phish-bypass paths, Outlook subdomain chaining.

For security teams: threat intel feeds may lag on this volume. Proactive domain monitoring for conflict-keyword registrations and brand impersonation patterns will catch campaigns before they reach inboxes.

Additional CVEs

CVE-2026-26127 -- .NET DoS

Out-of-bounds read, unauthenticated network attacker. Low-effort disruption of .NET services.

CVE-2026-26110/26113 -- Office RCE

Preview Pane exploitable. No file open required. Prioritize Outlook patching.

Android / Qualcomm Zero-Day

Actively exploited display component flaw. Fixed in March Android security bulletin.

DEFENDER CHECKLIST -- APRIL 2026

- [ ] Patch Cisco FMC immediately -- CVE-2026-20131 is actively exploited by Interlock ransomware for root access
- [ ] Patch SQL Server 2016+ -- CVE-2026-21262 is publicly disclosed; treat as known exploit risk
- [ ] Audit Microsoft Copilot deployments -- CVE-2026-26144 enables zero-click data exfil invisible to DLP
- [ ] Patch Outlook and disable Preview Pane -- Office RCE pair CVE-2026-26110/26113 exploits preview rendering
- [ ] Push Android security updates -- Qualcomm display zero-day actively exploited in the wild
- [ ] Verify offline backup integrity -- Uragan ransomware specifically targets and disrupts recovery tooling
- [ ] Enable conflict-themed domain monitoring -- 7,381 phishing URLs active targeting enterprise sectors

Threat Context

The March-April threat landscape is defined by two converging trends: geopolitical conflict driving proxy-group cyber operations, and continued AI-assisted malware industrialization lowering the barrier for sophisticated attacks. The common thread is speed -- attackers operate at a tempo that outpaces traditional detection and patching cycles. Organizations that treat security as a periodic exercise rather than a continuous program are the most exposed.

Cyber Tip of the Month

Assume your AI assistant has read everything. Microsoft Copilot operates with the full permissions of the user who activated it -- emails, documents, SharePoint, Teams messages. CVE-2026-26144 demonstrates that a vulnerability in that assistant can exfiltrate that data silently. Before deploying AI productivity tools broadly, map what data they can access and apply least-privilege principles. If your Copilot can read HR files, legal documents, and executive communications -- so can the bug that hits it next month.

Sources and Intelligence Feeds

- Unit 42 -- Threat Brief: Iran Escalation (March 26, 2026)
- CYFIRMA -- Weekly Intelligence Report (March 27, 2026)
- BleepingComputer -- March 2026 Patch Tuesday
- Tenable -- Microsoft Patch Tuesday Analysis
- The Hacker News -- Weekly Recap March 2026
- Security.com -- Seedworm APT Report
- SANS ISC Diary Archive -- March 2026

The Security Desk

[Monday morning. Ops center. CVE dashboard glowing.]

Junior Analyst:

"Good news -- Iran's internet is down to 1%. Nation-state threat is basically neutralized, right?"

[Senior analyst does not look up from screen]

Senior Analyst:

"Their operators outside the country just became unsupervised. So no."

[Junior analyst stares at 7,381 phishing URLs on screen]

Junior Analyst:

"...so it's actually worse."

Senior Analyst:

"Welcome to geopolitical threat intelligence. Coffee's in the back."