THE FORENSICS WAY

⚡ SPECIAL EDITION | CYBER WAR REPORT | U.S.–ISRAEL–IRAN CONFLICT

ISSUE 06 | FORENSICS AWARENESS THIS WEEK | TUESDAY, MARCH 10, 2026

FRONT PAGE

STATE-SPONSORED INTRUSION

Seedworm Strikes the Homeland: Iranian APT Infiltrates US Bank, Airport, and Defense Supply Chain

Symantec's threat intelligence team confirmed this week that **Seedworm** — an Iranian state-sponsored APT also tracked as MuddyWater — has successfully infiltrated networks belonging to a US financial institution, a major airport operator, and multiple defense supply chain firms. The campaign leverages spearphishing and living-off-the-land techniques to avoid detection, making behavioral forensics the only reliable detection path.

For forensic examiners, Seedworm intrusions present a compounded challenge: the group deliberately times operations to overlap with hacktivist noise campaigns, using the influx of false-positive alerts to mask lateral movement. Investigators responding to Seedworm incidents must segregate threat streams carefully — hacktivist DDoS activity hitting the same target is frequently a deliberate smoke screen.

ESPIONAGE UNDER COVER

WezRat Resurges: APT42 Harvests Credentials While the World Watches the Hacktivists

While 60+ hacktivist groups dominate headlines with defacement campaigns and DDoS attacks, **APT42** — Iran's elite intelligence cyber unit — has quietly resumed **WezRat** infostealer operations targeting media organizations, academic institutions, and defense contractors. WezRat establishes persistence through legitimate cloud services, harvesting credentials and session tokens with minimal system footprint.

The pattern is deliberate: APT42 uses the operational cover of loud hacktivist activity to conduct methodical, long-term espionage. Examiners should treat any concurrent hacktivist activity on a target network as a potential distraction operation

Threat Bulletin

CRITICAL

CVE-2026-0145

Palo Alto PAN-OS GlobalProtect Authentication Bypass. Allows unauthenticated remote access to VPN infrastructure — a preferred initial-access vector for Iranian APT groups including Seedworm and APT42. Emergency patching ordered across federal agencies. *Forensic Note:* Audit GlobalProtect session logs for anomalous authentication patterns predating the alert.

ACTIVE EXPLOIT

CVE-2026-1834

Fortinet FortiGate SSL-VPN Remote Code Execution. Actively weaponized by Iran-aligned actors as a secondary access mechanism when PAN-OS targets are patched. *Forensic Note:* Look for unauthorized SSL-VPN session initiations and anomalous HTTPD child processes in FortiGate logs.

MALWARE SPOTLIGHT

BaqiyatLock Wiper

Iran-aligned destructive malware deployed simultaneously as a ransomware facade and true wiper — no decryption key is ever issued. Forensic recovery is largely impossible post-execution. Targets the Master Boot Record and overwrites file headers. *Forensic Note:* Prioritize volatile memory and network flow capture the moment BaqiyatLock is

and prioritize hunting for subtle persistence mechanisms in cloud-connected environments alongside the more obvious indicators.

suspected — disk artifacts will not survive.

⚡ SPECIAL EDITION — CONFLICT ZONE REPORT — MARCH 10, 2026

Cyber War: The Digital Front in the U.S.–Israel–Iran Conflict

On February 28, 2026, the United States and Israel launched Operations Epic Fury and Roaring Lion against Iranian military infrastructure. Within hours, the conflict expanded into full-spectrum hybrid warfare. The following four briefings examine the cyber and digital forensics dimensions of an ongoing and rapidly evolving conflict — and what they mean for defenders right now.

BREAKING

OPERATION EPIC FURY AND THE 4-HOUR DIGITAL BLACKOUT

Within hours of the February 28 strikes, Iran's available internet connectivity collapsed to between **1–4% of normal capacity** — a near-total blackout assessed to be the result of both physical infrastructure damage and deliberate offensive cyber operations targeting routing infrastructure. The connectivity loss created a double-edged forensic consequence: while it initially degraded Iran's ability to coordinate sophisticated retaliatory attacks, it also severed real-time logging and telemetry from networks inside the country, creating significant gaps in the evidentiary record. Investigators working attribution cases tied to this period must account for the blackout window when reconstructing attacker timelines — network artifacts that would normally provide corroborating evidence may simply not exist for the February 28 – March 2 window.

INTELLIGENCE

60 GROUPS, ONE ROOM: INSIDE IRAN'S ELECTRONIC OPERATIONS ROOM

On February 28, Iran's Ministry of Intelligence and Security (MOIS) formally activated what threat analysts are calling the "**Electronic Operations Room**" — a coordinated command structure bringing together 60+ state-aligned and hacktivist groups under unified operational direction. Key actors include Handala Hack (MOIS-linked), Cyber Islamic Resistance, Dark Storm Team, Sicarii ransomware operators, and pro-Russian hacktivist collectives. The formation of this room represents a significant evolution in Iranian cyber doctrine: for the first time, the MOIS is openly coordinating criminal, hacktivist, and state APT assets under a single operational umbrella. For forensic investigators, this creates a deliberate attribution maze — attacks may appear to originate from independent hacktivist groups while actually executing state intelligence directives, with persona fragmentation designed specifically to frustrate forensic attribution.

ANALYSIS

WIPERS ON THE FRONTLINE: WHEN "RANSOMWARE" BECOMES PERMANENT ERASURE

BaqiyatLock and **Sicarii** — the primary destructive tools deployed by Iran-aligned actors in this conflict — present a forensic crisis unlike standard ransomware: *no decryption is ever possible*. Both tools present as ransomware to confuse the initial triage, displaying ransom notes and wallet addresses, but their actual function is immediate, irreversible data destruction

ADVISORY

CISA AT 38%: AMERICA'S CYBER SHIELD IS CRITICALLY UNDERSTAFFED

As Iran-aligned actors execute their most coordinated cyber campaign since 2021, CISA — the United States' primary civilian cyber defense agency — is operating at just **38% staffing capacity** due to a federal funding lapse. The agency's public-facing threat advisories have not been actively updated since February 17, 2026. CISA's website itself carries a notice acknowledging the lapse. The consequences for private-sector organizations are

targeting Master Boot Records, partition tables, and file system headers. By the time an organization recognizes the ransom demand as a facade, the evidence is already gone. Forensic examiners responding to suspected wiper incidents must immediately pivot to volatile evidence — RAM dumps, network flow captures, and out-of-band logging — before touching the disk. Post-execution disk forensics on BaqiyatLock targets typically yield little beyond confirming the method of destruction. The only viable forensic record lives in what was preserved before detonation.

significant: the agency's usual role of rapid threat indicator sharing, joint advisories, and emergency coordination is severely degraded precisely when it is needed most. Forensic teams and security operations centers should not assume federal support will arrive in the standard timeframe. Organizations must increase their reliance on private threat intelligence feeds, sector-specific ISACs, and peer information sharing immediately. The gap in federal coordination is itself a vulnerability that Iran-aligned threat actors are likely aware of and actively exploiting.

— SPECIAL EDITION INSERT —

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, MARCH 10, 2026

CASE STUDIES: HISTORICAL GRID

STUXNET / OPERATION OLYMPIC GAMES (2010)

The First Cyberweapon Deployed Against Iran

Jointly developed by the NSA and Israel's Unit 8200, Stuxnet was the world's first known cyberweapon — a precision instrument designed to destroy Iranian centrifuges at the Natanz nuclear facility while reporting normal status to operators. Its forensic discovery by Kaspersky and Symantec researchers established the foundational methodology for ICS/SCADA malware analysis that defenders apply to Iranian wiper incidents today.

NOTPETYA WIPER ATTACK (2017)

The $10 Billion Lesson in Destructive Malware

Disguised as ransomware, Russia's NotPetya was a pure wiper that caused an estimated $10 billion in global damages — the most destructive cyberattack in history. Forensic analysts at ESET and Kaspersky determined that the ransom facade was deliberate misdirection, a lesson that directly informs how investigators must approach today's BaqiyatLock and Sicarii deployments in the Iran conflict.

THE KEVIN MITNICK MANHUNT (1995)

A Digital Trail Through Stolen Networks

The world's most wanted hacker was caught when security expert Tsutomu Shimomura traced Mitnick's intrusions through cellular

SONY PICTURES HACK (2014)

When Attribution Became a Geopolitical Act

The FBI attributed the catastrophic Sony Pictures breach to North Korea's Lazarus Group through malware code analysis, linguistic pattern

network logs and TCP/IP sequence number fingerprinting. Shimomura rebuilt the attack timeline in real time, pioneering techniques in network forensics and live digital pursuit foundational to modern incident response.

matching, and infrastructure correlation. It was the first time a nation-state cyberattack produced official government sanctions — establishing digital attribution as an instrument of foreign policy.

TOOLS OF THE TRADE

OPEN SOURCE

MISP

MALWARE INFO SHARING PLATFORM

The industry standard for structured threat intelligence sharing. During active conflicts, MISP instances allow DFIR teams to rapidly share and consume Iran-conflict IoCs — IP ranges, file hashes, C2 infrastructure — across organizations and ISACs in real time.

OPEN SOURCE

Arkime

FULL-PACKET CAPTURE & ANALYSIS

Full-packet capture and indexed search at scale. Essential for hunting APT lateral movement that leaves no host-based artifacts. Arkime's session reconstruction capability is particularly valuable for tracing WezRat's cloud-channel exfiltration paths through legitimate service traffic.

OPEN SOURCE

Volatility 3

MEMORY FORENSICS FRAMEWORK

The premier open-source memory forensics framework. Against wiper malware like BaqiyatLock — which destroys disk evidence on execution — RAM acquisition and Volatility 3 analysis may be the only path to reconstructing attacker actions, process trees, and injected payloads.

COMMERCIAL

Recorded Future

THREAT INTELLIGENCE PLATFORM

Provides real-time, AI-aggregated threat intelligence with specific coverage of Iranian APT groups, hacktivist personas, and conflict-driven infrastructure. During the current escalation, Recorded Future's Iran-focused intel modules are providing the fastest updated IoC feeds available to enterprise defenders.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-20127 (CISCO)

Cisco Catalyst SD-WAN remote root exploitation. NSA joint alert confirms active use. *Forensic Note:* Diff running configs against known-good baselines and audit control-plane logs for unauthorized changes.

ARCHIVE ALERT

CVE-2026-25108 (FILEZEN)

FileZen command injection under active exploit, CISA emergency mitigations ordered. *Forensic Note:* FileZen's file-monitoring logs may be the primary evidence source for scoping exfiltration timelines.

RECENT MALWARE WATCH

ARCHIVE: MAR 3, 2026

"SANDWORM_MODE" NPM

Typosquatted NPM supply-chain packages harvesting CI/CD secrets and poisoning AI coding assistants via rogue MCP servers. Targets developer environments directly.

ARCHIVE: MAR 3, 2026

RESURGE (IVANTI)

Persistent malware on Ivanti Connect Secure appliances operating beyond EDR coverage. CISA issued fresh IoCs. Requires appliance-specific acquisition and network-side flow analysis.