RiskIQ Illuminate® Internet Intelligence Platform Cyber Threat Intelligence

Adaptive, continuous intelligence—from a single threat to thousands

Unmask and Defeat Adversaries

Ever-increasing cyber threats are boosted by easy access to malicious systems, kits, and tooling capable of effective cyberattacks. Even the best security professionals can miss today's global-scale threat campaigns with thousands to identify, track, and update.

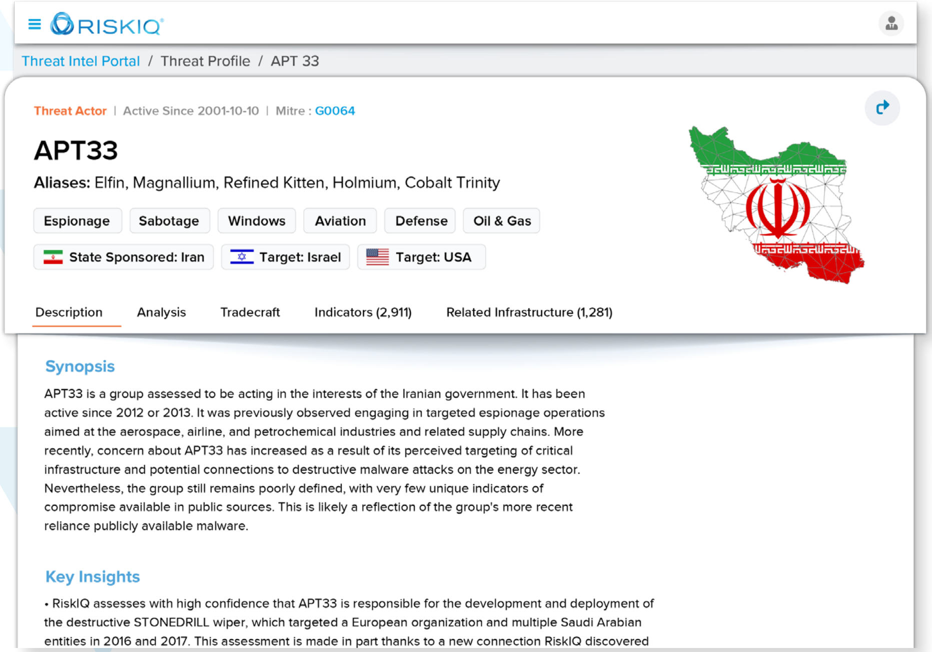
Cybercriminals, hacktivists, and nation-state threats all evolve tactics, techniques, and procedures (TTPs) to improve their malicious capabilities. But sustainable, scalable threat indicators come from observing threat infrastructure and behavior—active and historic. Whether tagged to a single threat actor or an entire threat system of thousands, adaptive intelligence is the new standard.

Key Capabilities

- Continuous Adversary-Threat Tracking
- Identify Attack Systems and Infrastructure
- Sustainable Threat Indicators and TTPs
- Connect and Map Related Infrastructure

Key Benefits

- Global defense for threats today and tomorrow
- Increase security and resilience against external threats
- Reduce risks inherent to digital change and expansion


≡ RISKIQ
Threat Intel Portal / Threat Profile / APT 33
Threat Actor | Active Since 2001-10-10 | Mitre : G0064

APT33

Aliases: Elfin, Magnallium, Refined Kitten, Holmium, Cobalt Trinity

Synopsis

APT33 is a group assessed to be acting in the interests of the Iranian government. It has been active since 2012 or 2013. It was previously observed engaging in targeted espionage operations aimed at the aerospace, airline, and petrochemical industries and related supply chains. More recently, concern about APT33 has increased as a result of its perceived targeting of critical infrastructure and potential connections to destructive malware attacks on the energy sector. Nevertheless, the group still remains poorly defined, with very few unique indicators of compromise available in public sources. This is likely a reflection of the group's more recent reliance publicly available malware.

Key Insights

- RiskIQ assesses with high confidence that APT33 is responsible for the development and deployment of the destructive STONEDRILL wiper, which targeted a European organization and multiple Saudi Arabian entities in 2016 and 2017. This assessment is made in part thanks to a new connection RiskIQ discovered

ADVERSARY-THREAT INFRASTRUCTURE

RiskIQ Illuminate Cyber Threat Intelligence uses automated discovery and continuous scanning across worldwide infrastructure to map and monitor threats and threat actors. By rapidly identifying adversary-threat infrastructure to transform observations into actionable indicators and TTPs drawn directly from threat infrastructure, including history, distribution, trends, and guided insights from RiskIQ Labs.

ADAPTIVE DEFENSE AT GLOBAL-SCALE

Fingerprint adversary infrastructure to scale defense, even when infrastructure is reused or repurposed by many threat actors. Leverage cyber threat intelligence to assign an identity to threat infrastructure, security teams can future-proof global defenses against threats today and those yet to be deployed.

AUTOMATED THREAT DETECTION

RiskIQ Illuminate Cyber Threat Intelligence continuously updates adversary-threat insights as well as related infrastructure for faster, smarter threat defenses for the elastic global attack surface. Map the composition of threat infrastructure to identify malicious activity, embedded capabilities, and shareable attack tools (e.g., kits, C2 components).

Dynamic threat indicators prepare your protections for external threats—the inherent risk of a digital, interconnected world.

TTPs, ANALYSIS, and INDICATORS

Take advantage of automated analysis packed with high-fidelity indicators of compromise (IOCs), open-source intelligence (OSINT), direct infrastructure crawling and tracking, and machine learning based on trillions of real-world observations. Use one-click pivots to find related infrastructure, including certificates, hashes, malware, NetFlow, and deep/dark web reconnaissance to get ahead of threats that matter—from a single threat actor to thousands with access and opportunity to leverage attacker systems.

Security expertise from RiskIQ Labs and proprietary methods are fused with deep machine learning for rapid context, guidance, and action — backed by factful, real-world observations.

DURABLE THREAT INTELLIGENCE

Security teams rely on RiskIQ for cyber threat intelligence that adapts to change. Pinpoint adversary-threat infrastructure—active and historic—identifying activity and behavior, TTPs, and related infrastructure to adversaries that matter to you.

Safeguard the digital enterprise from rapidly evolving threats with automation and deep machine learning. Increase resilience and predetermine defense with up-to-the-moment threat indicators and insight into malicious activity targeting you, your industry, peers, third parties, and everything else on the internet.

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com