DARKTRACE

Defending against nation-state attacks with Darktrace

The boundary between nation-state, state-affiliated, and criminal cyber activity is often blurred.

Generally, nation-state-linked cyber operations tend to be better resourced, longer-term, and strategically motivated, and are more likely than purely criminal actors to target government and critical infrastructure, though they also heavily pursue espionage and intellectual property theft across private sectors.

Latest trends in nation state attacks

The accelerating convergence of geopolitical tensions and the digital transformation of critical infrastructure has elevated cyber operations as a primary instrument of state power and strategic signalling. Darktrace observed three recurring trends in analysis behind these state-linked attacks:

01 Attacks on critical national infrastructure to disrupt national services, threatening national security and public stability.

E.g. the Russian-Ukraine conflict has led to an increase in cyber-physical attacks on Ukrainian and Western energy infrastructure from state-sponsored and criminal hacktivists.

02 Changing use of cyber capabilities from passive outcomes like espionage to active disruption.

E.g. Chinese APT Salt Typhoon's infiltration of US telecommunications infrastructure enabled intelligence gathering, but implants deployed in several US CNI organizations, including Energy, created the potential for disruptive OT attacks.

03 Usage of proxy agents to further geopolitical interests.

E.g. In 2025, Darktrace observed DPRK affiliated threat actors employing multiple intrusion methods to mine crypto currency. These activities included the deployment of trojanized malware within a UK financial services organization and the exploitation of the React2Shell zeroday vulnerability in a Singaporebased financial services organization.

Common nation state **attack techniques**

Nation-state actors use sophisticated techniques to avoid detection.

Valid credentials and legitimate tools

- **Abusing** remote administration tools
- **Conducting** low-and-slow lateral movement
- **Masquerading** as normal IT operations

Darktrace detects when legitimate tools are used in abnormal ways, surfacing suspicious behavior that traditional methods overlook.

Cross-domain operations

- **Starting** in email or edge infrastructure
- **Pivoting** into cloud and identity systems
- **Blending** into normal software development workflows

Darktrace correlates anomalies across all environments to reconstruct and reveal multi-stage intrusion paths.

Covert command-and-control

- **Encrypted** outbound channels
- **Beaconing** hidden in legitimate traffic

Darktrace identifies these anomalies by detecting unusual outbound connectivity and encrypted communication patterns

■ Darktrace nation-state threat finds

CAMPAIGN	INITIAL ACCESS / TECHNIQUE	WHY IT WAS HARD TO DETECT	WHAT DARKTRACE DETECTED
Campaign targeting South Korean end users Read the full blog	Abuse of Visual Studio Code development tooling for remote access	Activity appeared as legitimate developer behavior rather than malware	Behavioral deviations in remote access patterns and anomalous connectivity
ShadowPad malware Read the full blog	Deployment of modular backdoor associated with state-linked campaigns	Stealthy command-and-control and persistence designed to evade signature detection	Unusual outbound communications and persistence behavior
Salt Typhoon intrusion Read the full blog	Long-term persistence and lateral movement across environments	Low-and-slow activity blended with normal operations	Behavioral anomalies revealing coordinated lateral movement
Medusa ransomware Read the full blog	Abuse of Remote Monitoring and Management (RMM) tools	Activity resembled legitimate IT administration	Correlated behavioral anomalies revealing ransomware preparation

How Darktrace **stops** nation state threats

The Darktrace ActiveAI Security Platform delivers the capabilities required to detect, investigate, and respond to sophisticated nation-state threats across the enterprise.

Built on Self-Learning AI that continuously learns from your organization's evolving data across network, cloud, email, identity, endpoint, and operational environments, the platform identifies deviations from normal activity rather than relying on known attack signatures. Cyber AI Analyst automatically investigates alerts across domains, while Autonomous Response can contain threats in real time—enabling security teams to shift from reactive alert triage to proactive defense.

AI built for novel threats

Darktrace's Self-Learning AI learns the normal behavior of users, devices, and services across the enterprise to detect subtle deviations that signal malicious activity. This allows Darktrace to identify nation-state actors who gain legitimate access to systems and operate using trusted tools. Suspicious behaviors detected by darktrace include: unusual device communications, unexpected administrative activity, or systems interacting with previously unseen external infrastructure.

Real-time detection

Darktrace detects threats without relying on malware signatures, external threat intelligence, or historical attack data. By understanding normal activity across the enterprise, it identifies anomalous behavior associated with the early stages of sophisticated attacks, including unusual authentication patterns, unexpected data transfers, and lateral movement following the exploitation of internet-facing infrastructure.

Cross-domain investigation

Nation-state intrusion campaigns rarely remain confined to a single system. Cyber AI Analyst automatically investigates and correlates anomalous activity across network, cloud, email, identity, and endpoint environments to determine whether isolated events form part of a coordinated attack. The system reconstructs attack timelines and produces structured incident narratives to help security teams understand attacker behavior and respond faster.

Autonomous threat containment

When malicious activity is confirmed, Darktrace's Autonomous Response can take targeted action to contain threats while minimizing operational disruption. This includes restricting suspicious connections, limiting compromised device activity, and interrupting unusual administrative sessions. These actions help disrupt command-and-control communications, prevent lateral movement, and stop persistence techniques associated with advanced nation-state attacks.

DARKTRACE 2026 THREAT REPORT ↗