paloalto NETWORKS | UNIT 42

Cyber Threats to Milan-Cortina 2026

Executive Summary

Defending the 2026 Milan-Cortina Winter Games

During the Olympics, cyber threat actors are going for gold, too.

They disrupted WiFi and other digital infrastructure during PyeongChang 2018. In Tokyo 2024, Russian threat actors attempted to sabotage pre-Games activities. In Paris 2024, we observed a spike in DDoS attempts, Olympics-themed phishing attempts and scam traffic. No doubt about it — infrastructure, venues and local suppliers contributing to the games also become part of the wider Olympic attack surface. With over 3 billion people around the world expected to watch the games, there is a lot at stake.

For athletes and defenders alike, winners will be determined by preparation and strategy.

Why Attackers Love Global Events

A target-rich environment

The sheer volume of people, systems, money, and data surrounding the Milano-Cortina 2026 Winter Games create a target-rich environment for attackers. Cyber criminals may cast a wide net with their scams and phishing campaigns. Like a futbol striker, making one out of a thousand attempts can make the difference.

High-value marks

Celebrities, politicians, and business leaders will likely be in attendance. Well-resourced nation-state actors may take advantage of this rare opportunity for close access and mount sophisticated attacks to compromise and surveil these VIPs and/or their staff. The stakes are high, in terms of strategic intelligence and impact.

Critical infrastructure

Attackers will attempt to disrupt critical infrastructure to apply pressure and extort a ransom. This infrastructure may be a utility like power or water services, transit systems like buses, trains, and light rail, or they may be event-based like ticketing systems and POS terminals. The integration of so many systems often creates complexity and security gaps that attackers can exploit.

Geopolitical tensions

Global events attract politically motivated groups to make their statements on an occasion that underlines their cause. Given the divisive geopolitical climate, any number of groups and even individual actors may attempt to hijack, disrupt, or deface digital infrastructure to amplify their stance.

Attackers, Motives, & Tactics

The Milano-Cortina 2026 Winter Games will draw attackers of all types, from nation-state actors down to petty scammers. Though some of their tactics may overlap, their motives and degree of sophistication will vary widely. Understanding what they're after and how they'll go about it will go a long way in informing your defenses.

Ransomware gangs | Financially motivated crime

Ransomware gangs extort money from victims by encrypting and stealing data, or otherwise disrupting critical systems to create a chokepoint, then demanding payment for restoration and to prevent the public release of stolen information.

They'll follow the same opportunistic pattern for the Milano-Cortina 2026 Winter Games, disrupting ticketing systems, event websites, or other critical infrastructure to frustrate fans and using the threat of stolen data to increase pressure on the victim organization. While data theft and encryption may not directly affect the attendee experience, they can undermine confidence in the event and damage victims' reputations. Not only does the Milano-Cortina 2026 Winter Games present a huge financial opportunity, but the complexity of the tournament's immense organizational ecosystem gives attackers camouflage to gain access, move laterally, and create excruciating leverage.

Example: Dark Scorpius

Dark Scorpius, which has attacked over 500 victims since first appearing in 2022, uses email bombing and social engineering to trick victims into granting them initial access. From there, they pose as IT staff to trick legitimate users into granting remote control through a tool like Windows Quick Assist. At this point, they're off to the races. They can disable security tools, deploy back doors, and escalate their own privileges for lateral movement.

Once they find extortion-worthy data, they encrypt and exfiltrate that data for maximum leverage. Dark Scorpius and the like move fast. We've observed them obtain initial access and exfiltrate data within a span of just 14 hours.

Ransomware is just one type of financial crime that will likely be conducted during the Milano-Cortina 2026 Winter Games. Scams and phishing campaigns against attendees will be common, using fake websites, bogus QR codes, fraudulent apps, and other tools to scam victims out of their cash.

Nation-state actors | Espionage

Not all attackers are after money. Nation-state groups target diplomats, NGOs, think tanks, and others to collect strategic intelligence that would be helpful to their parent government's goals. These groups often operate with the flexibility of cybercriminals while also enjoying the resources that come with government sponsorship. They have background intelligence on targets, custom capabilities, and dedicated patience that many cybercriminals simply do not.

Time is perhaps their greatest luxury. These attackers infiltrate targets and deepen their position over months or years, using stealthy, sophisticated, and persistent methods to do so. Sometimes their campaigns compromise entire ecosystems of people, systems, and third-party software. All the while, they steal data quietly and incrementally to maintain their stealth.

The Milano-Cortina 2026 Winter Games will bring together important figures from many nations, who will be utilizing event infrastructure.

Example: Fighting Ursa aka APT28

Believed to be a Russia-backed espionage group, **Fighting Ursa** has some big headlines to its name, from attacking German and Norwegian parliaments to the 2024 Paris Olympics. This group also favors phishing, especially through spoofed websites and spear phishing emails with weaponized documents and links. They excel at creating realistic-looking fraudulent assets that trick victims into handing over their credentials.

Once inside, they use proprietary software for tunneling, reconnaissance, and command-and-control – all serving to maintain persistence and avoid detection.

China's Stately Taurus/Mustang Panda and North Korea's Kimusky serve as additional examples, having carried out attacks against government entities representing the U.S., Europe, South Korea, Vietnam, and others.

Hacktivist groups | Disruption

Hacktivist groups want to draw attention to themselves and their cause. They undermine their targets – ostensibly perpetrators of corporate crime, human rights abuses, environmental destruction, etc. — by creating instability through disruption.

Attacks are often two-pronged. First, they obtain confidential or scandalous documents, data, communications, or personal information. Then, they broadcast their findings to the world. They may conduct distributed denial of service (DDoS) attacks that knock services offline; hijack websites, streams, and social media handles to amplify their message; and doxx key figures to incite harassment against them.

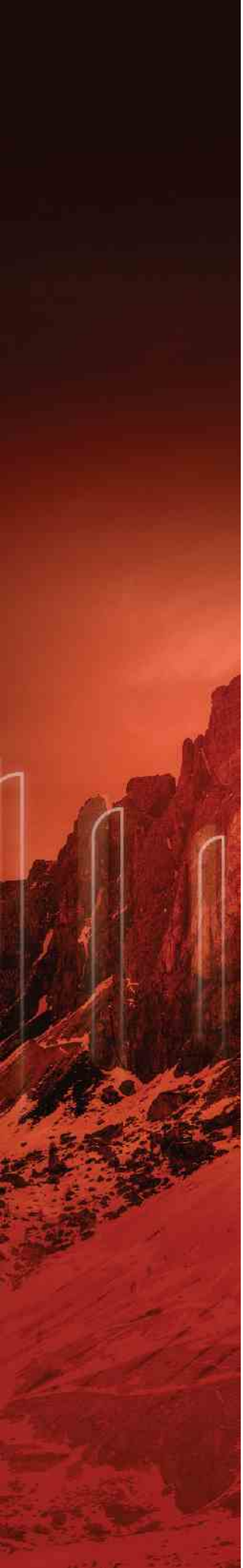
Example: Anonymous

Anonymous's attacks on a wide range of targets from the CIA to the Church of Scientology have earned a space in the mainstream public consciousness, along with their signature Guy Fawkes masks. The distributed group of actors supports broadly ideological causes like anti-censorship and anti-corruption.

In a typical attack chain, Anonymous gains access by scanning public systems for open ports, unsecured servers, leaked credentials, and misconfigured services. Once inside, they deface websites and social media accounts to shame their targets.

Other types of cybercriminals may prefer to lay low and attack easy targets, but for Anonymous and other hacktivist groups, bigger targets mean more influence and heighten their reputation.

The global geopolitical scene is rife with conflict. The Milano-Cortina 2026 Winter Games draws billions of eyes. For hacktivist groups, perhaps no occasion offers as much exposure and publicity for their ideology.



Tactics to Guard Against

These attackers and tactics share plenty of overlap. For example, both hacktivist and nation-state groups may use their position to spread misinformation. Both ransomware groups and hacktivist groups employ the tactics of disruption. Both nation-state actors and ransomware groups need stealth and persistence to reach their ideal attack positions. Some nation-state actors, like North Korea, are financially motivated — their plunder works to fuel government military initiatives.

Here are a few common tactics we've observed threat actors deploy in Olympic Games scenarios.

Phishing

According to our Unit 42 2025 Incident Response Report, phishing stands as attackers' favorite initial access vector, especially leading towards financial theft via business email compromise (BEC). Powered by advancing AI capabilities, attackers can create more convincing phishing assets quickly and at scale. The vast array of organizations and contractors involved in the Milano-Cortina 2026 Winter Games will offer even more phishing opportunities for bad actors. They may pose as partner organizations, regulatory agencies, or other entities.

Software and API vulnerabilities

Just think of the cumulative attack surface of the Milano-Cortina 2026 Winter Games's digital infrastructure, many systems of which will be spun up quickly. This complex ecosystem will be replete with vulnerabilities both old and new, along with misconfigurations from unpatched versions of frameworks to dangling DNS records to overlooked access controls. AI helps attackers scan for these weak points quickly and identify the easiest path to access.

Previously compromised credentials

As common as phishing may be, it's not always necessary. Threat actors frequently buy previously compromised or leaked credentials on the Dark Web, saving them the trouble of phishing. If staff, vendors, or contractors reuse passwords across multiple accounts, a single set of credentials may lend broad access to cloud, CMS, logistics systems and more — especially if MFA isn't enforced.

DDoS attacks

A popular disruption tactic, DDoS attacks flood the target service, API, or site/system with traffic, often with botnets, in order to knock that target offline. Sometimes, DDoS attacks are also used as a distraction from data exfiltration, ransomware deployment, or efforts to establish persistent access. In the Milano-Cortina 2026 Winter Games context, DDoS attacks can disable stadium functions like turnstiles and ticketing platforms, take down event websites, and generally cause frustration for fans and reputational damage for host organizations.

Spotlight On Social Engineering

With social engineering attacks, malicious actors exploit the trust organizations must place in each other. Global events provide ample social engineering opportunities because many organizations must interact with each other in new ways that create gaps and complexity.

Business email compromise

In 76% of phishing cases, attackers gained access through business email compromise (BEC). BEC relies on carefully crafted socially engineered messages that appear to come from trusted sources like leadership, vendors or partners. Attackers impersonating these figures can pressure victims into approving fraudulent invoices, committing fake vendor changes, circumventing multifactor authentication (MFA) and other controls and more.

AI attacks and deepfakes

We've seen attackers create highly convincing deepfakes and emails with minimal technical effort or expense. With just a few samples of, say, a CEO's emails and speaking engagements, attackers can train malicious AI to impersonate anyone. Under this disguise, the typical signs of a scam, like urgency and commands to shortcut approved policies, are more likely to go unnoticed.

High touch impersonation

IT staff hold the keys to the digital kingdom, and attackers target them to gain access. They research a target's service desk processes, staff, and systems, so they can impersonate a legitimate user convincingly request password resets or bypass MFA. When successful, the attacker logs into the target's account, where they can escalate their own privilege, set up forwarding rules, register new MFA devices and create backdoor accounts.

ClickFix campaigns

ClickFix attacks trick users into self-remediating a supposed problem by clicking a malicious link or accidentally executing malicious code. An attacker may send a phishing email that looks like an automated alert or system notification, prompting the victim to "Click here to reset an expired password" or engage with a fraudulent CAPTCHA test. When they click, the victim may download malware or be redirected to a fake login page where their credentials are harvested.

SEO poisoning

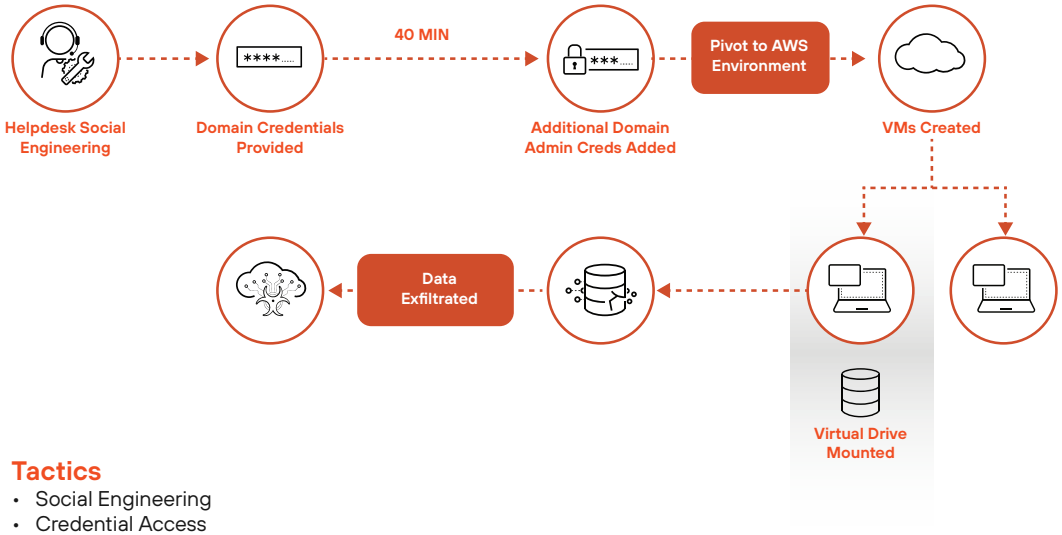
For this tactic, attackers deploy malicious websites, then manipulate search engine optimization (SEO) techniques to make that site or page rank high on search results. These pages often look like legitimate sites or imitate login portals that users access through search engines. Engaging with the fraudulent site can trigger malware downloads, steal credentials or perpetuate fake software updates and tech support manipulation.

Threat Profile: Muddled Libra

In 2025 alone, we've observed Muddled Libra (aka Scattered Spider, UNC3944) activity in the government, retail, insurance and aviation sectors. They extract large ransoms, in the tens of millions, often in cryptocurrency. It is undetermined whether this group is state-sponsored, but they operate with a high degree of sophistication and are fluent in English. Unlike other cyber actors, Muddled Libra performs extensive reconnaissance, accessing the target's own technical documentation and incident response processes to understand where to place implants and how defenders are likely to respond.

They research employees, too, so when they call the help desk — a shift from text-based phishing to voice-based phishing — impersonating executives or remote workers, they sound that much more convincing. By using details gathered from data breaches, previous compromises, and even social media accounts, they can answer identity verification questions and pressure help desk staff to reset passwords or enroll new MFA devices. This direct exploitation of human trust and standard IT workflows allows Muddled Libra to bypass several layers of defense and gain deep access to corporate environments.

Here's how the group could hypothetically pivot from initially access via social engineering a help desk employee, to escalating privileges, to domain admin rights in about 40 minutes.



Tactics

- Social Engineering
- Credential Access
- Lateral Movement
- Privilege Escalation
- Persistence Mechanisms
- Credential Reuse
- Obfuscation and Evasion
- Data Staging for Exfil

Threat Profile: Insidious Taurus and Salt Typhoon

Insidious Taurus and Salt Typhoon are Chinese state-sponsored groups carrying out campaigns against the U.S. Though they are often grouped and talked about interchangeably, their operations are drastically different.

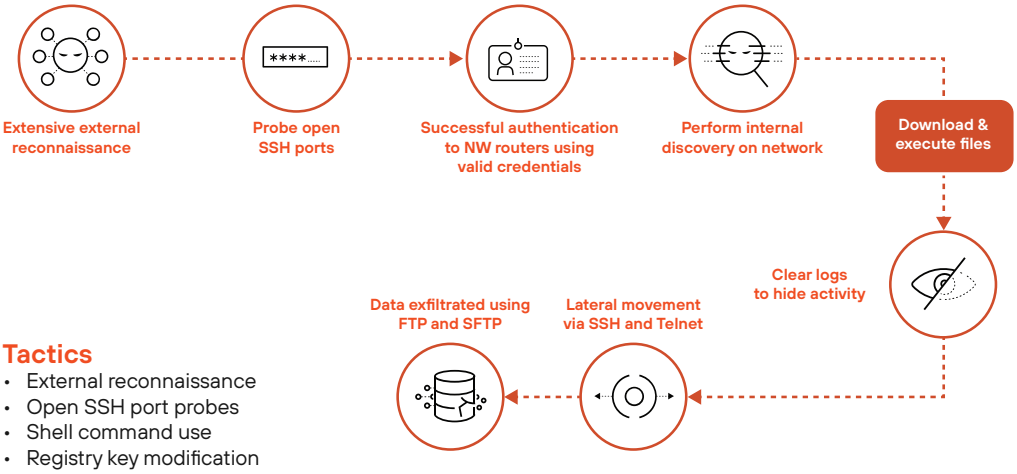
Insidious Taurus: Operational positioning

Insidious Taurus works to compromise and maintain persistent access to America's critical infrastructure. By pre-positioning themselves on IT networks, they are prepared to move laterally, perhaps into OT environments to cause mass disruption in energy, transportation, water and other essential services. These actors are playing the long game, using living-off-the-land techniques to evade detection and maintain footholds for years.

Salt Typhoon: Intelligence-gathering espionage

Salt Typhoon (tracked by Unit 42 as CL-STA-0967) compromises telecommunications companies across the world to conduct surveillance and espionage. They steal customer call records data, copy certain information subject to U.S. law enforcement requests pursuant to court orders and compromise the private communications of select individuals involved in government.

Below is an example of how Salt Typhoon could execute a prolonged series of network intrusions, beginning with extensive reconnaissance.



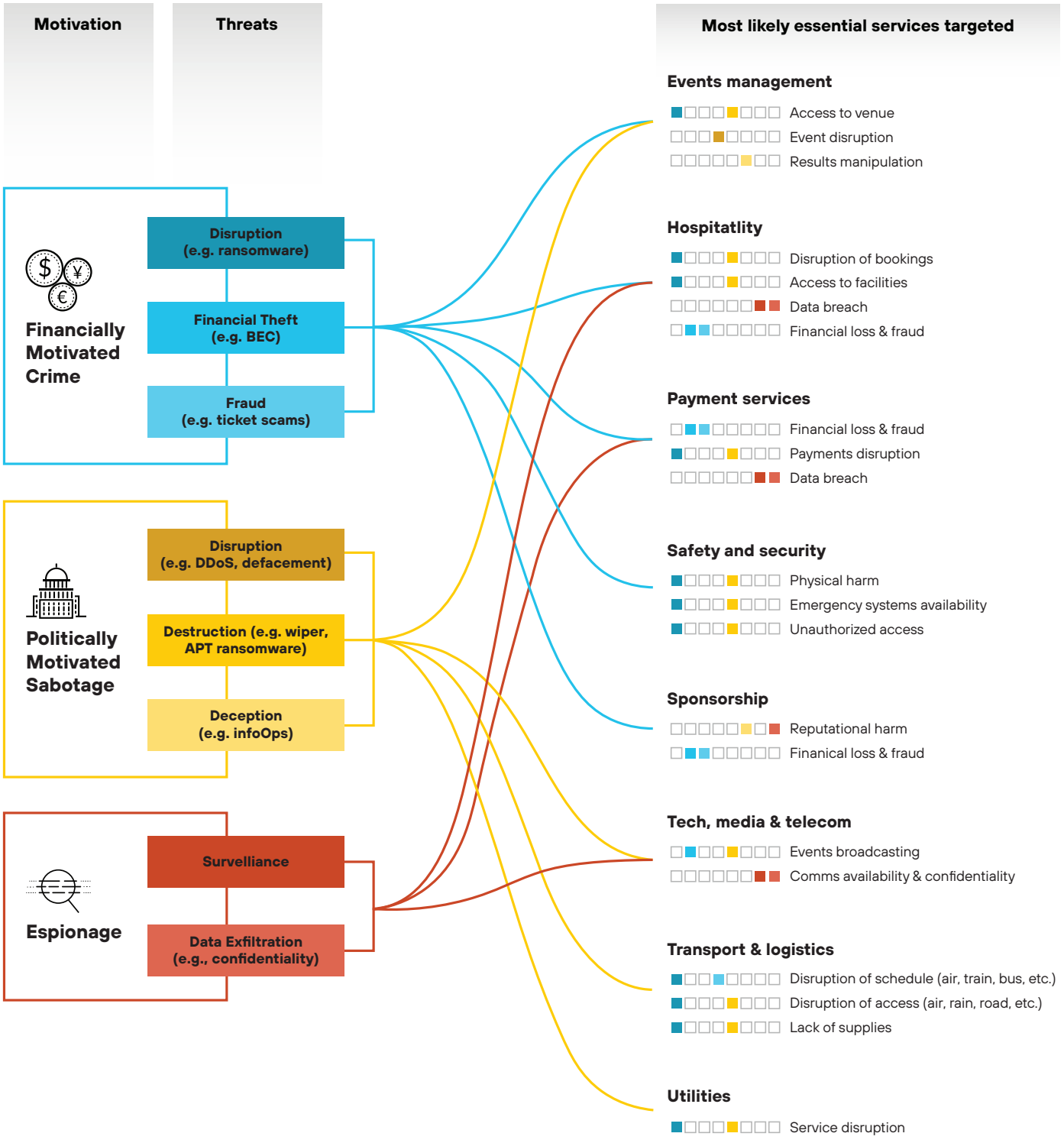
Tactics

- External reconnaissance
- Open SSH port probes
- Shell command use
- Registry key modification
- Lateral movement
- Data exfiltration

Either or both of these groups may target the Milan-Cortina 2026 Winter Games. They may target vendors, service providers or event equipment that connect routers or network appliances, giving them the ability to pivot into more critical systems. Living-off-the-land tools such as PowerShell or Windows Management Instrumentation are common to these typhoons' playbooks and can help them fly under the radar.

Safeguarding Essential Services

Organizations participating in the Milano-Cortina 2026 Winter Games must understand where they fit in the event's ecosystem and coordinate defenses together. Outlined below are the most critical services necessary for the successful execution, along with the perceived motives driving threat actors to potentially target them.



Shoring up your defenses

Just as venue preparations begin well in advance, cybersecurity preparations should also start early. This gives you time to build on and sharpen your existing practices well before the big event. As an athlete would put it, **staying ready is better than getting ready.**

See more, respond faster

Empower your SOC with comprehensive visibility across the enterprise, and the technology to identify the signal in the noise. Visibility gaps give attackers more cover. Gain full visibility from network to endpoint to cloud, and map internal and external attack surfaces to inventory all assets and connections. To reduce complexity, consolidate telemetry into a universal hub, then apply AI and machine learning to filter out the noise, gain a full picture of each threat, and respond with precision.

Accelerate zero trust adoption

Eliminate implicit trust, enforce least privilege access, and continuously verify users and devices. In the case of an intrusion, zero-trust controls drastically mitigate the impact. Work to tailor controls to support least privilege principles. Monitor users to establish behavioral baselines, so you can recognize aberrant activity. Finally, identify and verify users, devices, and apps on a continuous basis.

Secure apps and the cloud from dev to runtime

Implement MFA, just-in-time access, and continuous monitoring to reduce attack surfaces. The cloud can no longer be a blindspot. Prioritize misconfigurations, vulnerabilities, and excessive permissions by risk, so teams can achieve the most coverage for their effort. During the CI/ACD process, run continuous scans that detect issues before they reach production. Apply real-time threat detection and proactive controls to protect apps, APIs, and workloads.

Strengthen detection and automated response

Use AI-driven automation to cut response times from hours to minutes. Automate analysis of security logs to surface high-priority threats faster. Use artificial intelligence and machine learning to sift through vast datasets, identifying hidden threats and anomalous behaviors. AI-assisted behavioral analytics help predict attacks before they fully materialize. The SOC should measure MTTD to gauge improvements. Regular threat hunting and correlation of signals from multiple sources tackle the "needle in a haystack" problem.

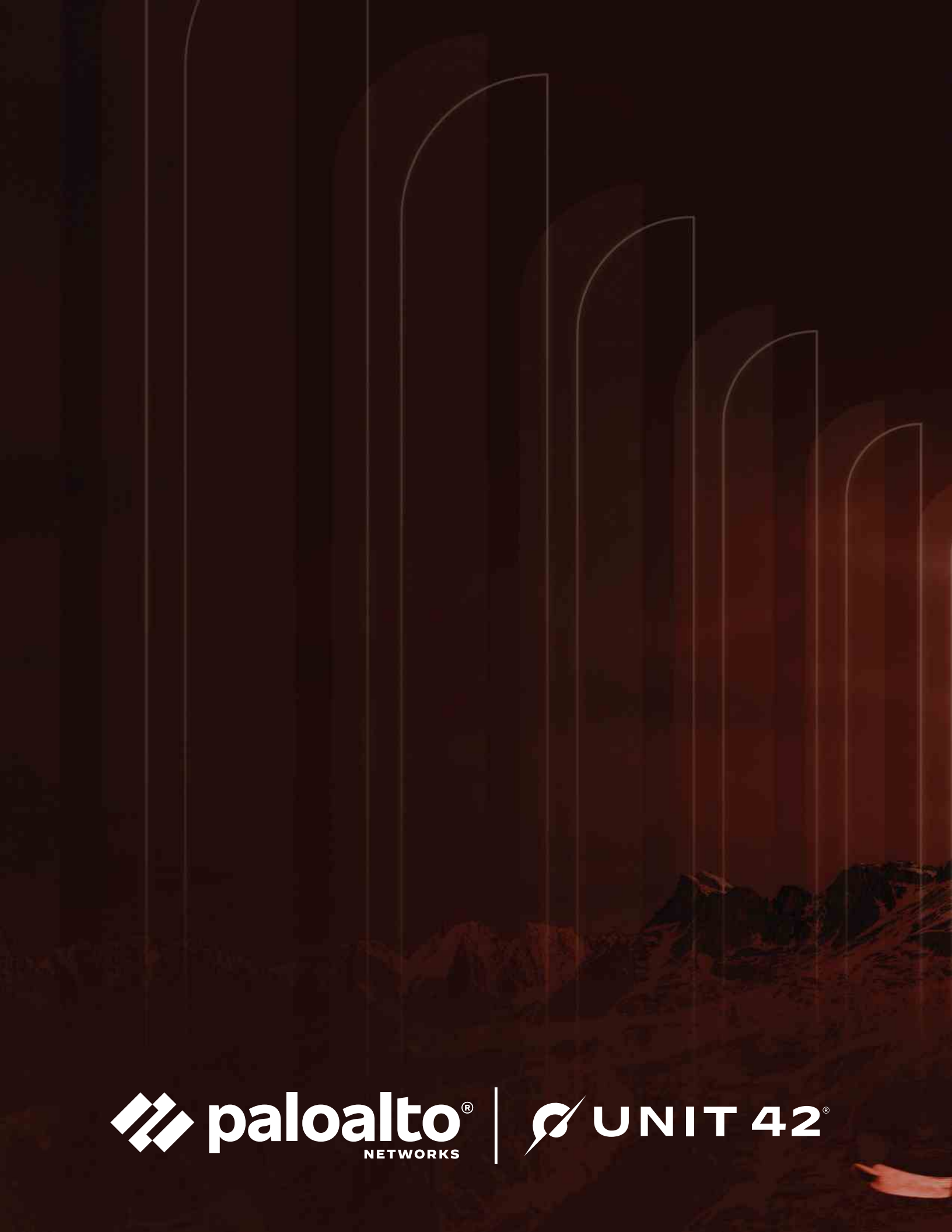
Unit 42 Threat Research Center

For more details about the threat landscape, visit Unit42.com

3000 Tannery Way
Santa Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com


paloalto®
NETWORKS
UNIT 42®