Introducing the 2026 Cloudflare Threat Report

By Cloudforce One

Published: 2026-03-03 · Archived: 2026-04-29 02:09:18 UTC

Introducing the 2026 Cloudflare Threat Report

2026-03-03

5 min read

Today’s threat landscape is more varied and chilling than ever: Sophisticated nation-state actors. Hyper-volumetric DDoS attacks. Deepfakes and fraudsters interviewing at your company. Even stealth attacks via trusted internal tools like Google Calendar, Dropbox, and GitHub.

After spending the last year translating trillions of network signals into actionable intelligence, Cloudforce One has identified a fundamental evolution in the threat landscape: the era of brute force entry is fading. In its place is a model of high-trust exploitation that prioritizes results at all costs. In order to equip defenders with a strategic roadmap for this new era, today we are releasing the inaugural **2026 Cloudflare Threat Report**. This report provides the intelligence organizations need to navigate the rise of industrialized cyber threats.

The new barometer for risk: Measure of Effectiveness (MOE)

Cloudforce One has observed a broader shift in attacker psychology. To understand how these methods win, we have to look at the why behind them: the **Measure of Effectiveness**, or MOE.

In 2026, the modern adversary is trading the pursuit of "sophistication" (complex, expensive, one-off hacks) in favor of throughput. MOE is the metric attackers use to decide what to exploit next. It is a cold calculation of the **ratio of effort to operational outcome.**

- Why use an expensive zero-day exploit when a stolen session token (Identity) has a higher MOE?
- Why build a custom server when a reputation shield (LotX) provides free, nearly untraceable infrastructure with a high delivery rate?
- Why write code manually when AI can automate the discovery of the connective tissue that links your most sensitive data?

In 2026, the most dangerous threat actors aren't the ones with the most advanced code; it's the ones who can integrate intelligence and technology into a single, continuous system that achieves their mission in the shortest time possible.

Key findings from the 2026 Cloudflare Threat Report

Eight key trends — all driven by their MOE — will define the threat landscape in 2026:

1. **AI is automating high-velocity attacker operations.** Threat actors use generative AI for real-time network mapping, exploit development, and the creation of deepfakes, enabling low-skill actors to conduct high-impact operations.
2. **State-sponsored pre-positioning is compromising critical infrastructure resilience.** Chinese threat actors, including Salt Typhoon and Linen Typhoon, are prioritizing North American telecommunications, commercial, government, and IT services, anchoring their presence now for long-term geopolitical leverage.
3. **Over-privileged SaaS integrations are expanding the blast radius of attacks.** As demonstrated by the GRUB1 breach of Salesloft, the connective tissue of third-party API integrations allows a single compromised API to cascade into a breach affecting hundreds of distinct corporate environments.
4. **Adversaries are weaponizing trusted cloud tooling to mask attacks.** Threat actors actively target legitimate SaaS, IaaS, and PaaS tools such as Google Calendar, Dropbox, and GitHub to camouflage malicious actions within benign enterprise activity.
5. **Deepfake personas are embedding adversarial operatives within Western payrolls.** North Korea has operationalized the remote IT worker scheme, using deepfakes and fraudulent identities to embed state-sponsored operatives directly into Western payrolls for espionage and illicit revenue.
6. **Token theft is neutralizing multi-factor authentication.** By weaponizing infostealers like LummaC2 to harvest active session tokens, attackers bypass traditional multi-factor authentication and move straight to post-authentication actions.
7. **Relay blind spots are enabling internal brand spoofing.** Phishing-as-a-service bots are exploiting a blind spot where mail servers fail to re-verify a sender's identity, allowing high-trust brand impersonations

delivered directly to user inboxes.

8. **Hyper-volumetric strikes are exhausting infrastructure capacity.** Hyper-volumetric distributed denial-of-service (DDoS) attacks, fueled by massive botnets like Aisuru, are breaking records on a regular basis, closing the window for human response.

Deep dive: How attackers are weaponizing cloud tooling

Now let's take a deeper look at one high-MOE tactic we identified: weaponized cloud tooling. Instead of using known malicious servers, attackers are utilizing legitimate cloud ecosystems like Google Drive, Microsoft Teams, and Amazon S3 to mask their command-and-control (C2) traffic. This is known as "living off the land" (or off of anything-as-a-service): wearing the uniform of trusted providers, attackers make their activity nearly indistinguishable from benign corporate traffic.

SaaS platforms are also being used by threat actors to host, launch, redirect, or scale attacks. For instance, services like Amazon SES and SendGrid, designed for legitimate bulk email delivery, are frequently exploited to launch sophisticated phishing and malware distribution campaigns.

How some groups are applying these tactics

While the exploitation of cloud resources is an established tradecraft, 2025 investigations highlighted an accelerated maturation in nation-state strategy: actors are continuing to shift from mere infrastructure abuse toward pervasive living-off-the-land. We predict that for 2026, threat actors will attempt to standardize these techniques as a strategic aim for their operational playbooks.

Here are some of those threat actor groups, where they are based, and examples of their approaches.

Threat Actor	Country	Technique	Details	Example
FrumpyToad	China	Logic-based C2	Moving "inside the box" of reputable SaaS logic to evade detection.	Weaponizes Google Calendar for cloud-to-cloud C2 loop, reading and writing encrypted commands directly into event descriptions.
PunyToad	China	Encrypted tunneling	Utilizing legitimate developer tools to bypass egress filtering.	Uses tunneling capabilities and cloud computing to create resilient, living-off-the-cloud architectures, masking backend origin IPs and prioritizing long-term persistence.
NastyShrew	Russia	Paste site dead drop resolvers	Using public "paste" sites to coordinate shifting infrastructure.	Uses services like Teletype.in and Rentry.co as dead drop resolvers (DDR); infected hosts poll these sites to retrieve rotating C2 addresses.

Threat Actor	Country	Technique	Details	Example
PatheticSlug	North Korea	PaaS-ing the perimeter	Exploiting the "reputation shield" of cloud ecosystems to mask malicious delivery.	Used Google Drive and Dropbox to host XenoRAT payloads, leveraging GitHub for covert C2, successfully blending into legitimate enterprise traffic.
CrustyKrill	Iran	SaaS-hosted phishing	Blending credential harvesting into common cloud hosting.	Hosts C2 pages on Azure Web Apps (.azurewebsites.net) and uses ONLYOFFICE to host payloads, giving their operations a veneer of legitimacy.

How Cloudforce One unmasked the 2026 landscape

Establishing MOE requires more than just high-level observation. To truly unmask the 2026 landscape, this report details how Cloudforce One leverages a unique blend of internal expertise and global telemetry to uncover insights that traditional security models miss.

Our methodology is varied. For example:

- As part of our AI-driven defense research, we tasked an AI coding agent with a self-vulnerability analysis, using the agent to uncover its own security gaps. This "dogfooding" uncovered **CVE-2026-22813 (9.4 CVSS)**, a critical flaw in markdown rendering pipelines allowing for unauthenticated Remote Code Execution.
- Our deep dives into **Phishing-as-a-Service** (PhaaS) reveal that the barrier to entry has a vanished barrier to entry. Analysts observed attackers leveraging high-reputation domains (Google Drive, Azure, etc.) to bypass filters. Email telemetry found an identity gap, where **nearly 46% of analyzed emails failed DMARC** (an email authentication protocol), revealing a large surface area that PhaaS bots are rapidly exploiting.
- We tracked the transition from stealthy exploitation to attempted blackout, uncovering a **31.4 Tbps baseline** for DDoS. Our telemetry also showed that, in the past 3 months, 63% of all logins involve credentials already compromised elsewhere and that 94% of all login attempts now originate from bots.

Through every stage of this research, Cloudforce One has leveraged our massive global telemetry and frontline threat intelligence to connect the dots across seemingly isolated incidents. Whether we are dogfooding our own AI agents to preempt zero-day exploits or tracking attacks launched by millions of bot-infected hosts tunneling through residential proxies, this unified visibility allows us to see the throughline between a single phished credential and a multi-terabit blackout.

The path forward: Drive MOE to zero with autonomous defense

Identifying these throughlines is only the first step. When threats move at machine speed, human-centric defense is no longer a viable shield. To counter "offense by the system," defenders across the industry must pivot to a model of **autonomous defense** in order to drive the adversary's MOE to zero**.**

This shift toward autonomous defense requires moving beyond manual checklists and fragmented alerts. Organizations must harden the connective tissue of their networks, using real-time visibility and automated response capabilities. In this new era, the goal isn't just to build a better wall — it's to ensure your system can act faster than the attacker, even when no one is watching.

To support this shift, today we are debuting a major upgrade to our threat events platform: evolving from simple data access to a fully automated, visual command center for your security operations center.

Get the 2026 Cloudflare Threat Report

Through our unmatched threat visibility and the expertise of our Cloudforce One researchers, we provide the intelligence you need to outpace industrialized cyber threats. **To explore the full data set, deep-dive case studies, and tactical recommendations, read the complete 2026 Cloudflare Threat Report**.

And if you're interested in learning more about our threat intelligence, managed defense, or incident response offerings, **contact Cloudforce One experts.**

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Threat IntelligenceCloudforce OneThreats
