



1H 2026 THREAT INTELLIGENCE REPORT

Cybercriminals Are Scaling Faster Than Defenders as the Cost of Attack Continues to Fall

Executive Summary

The first half of 2026 reinforced a significant shift in the threat landscape: the most effective attacks increasingly do not look like attacks at all. They look like a Microsoft Teams message from someone claiming to be in IT, a login prompt from a trusted brand, a software package from a familiar repository, or a routine request that appears legitimate on the surface.

As organizations invest in stronger security controls, attackers are adapting by targeting the trust relationships that businesses rely on every day. Rather than deploying sophisticated malware or exploiting technical vulnerabilities, many threat actors are achieving greater scale by abusing legitimate identities, trusted platforms, business workflows, and increasingly automated criminal ecosystems.

This report examines the most significant threat activity, emerging techniques, and operational trends observed during the first half of 2026, drawing on observations from customer environments, incident investigations, threat intelligence research, and data from Ontinue's Advanced Threat Operations team.

Three developments stand out for CIOs, CISOs, and other business leaders.

The Three Most Important Developments in 1H 2026

Identity remains the most reliable path to compromise

Device code phishing, token theft, credential harvesting, and session hijacking continued to provide efficient access to enterprise environments without requiring endpoint exploitation. Ontinue identified an uptick of device-code phishing compromises in a two-month period. The continued adoption of passkeys reflects growing recognition that password-centric authentication models remain vulnerable to modern attack techniques.

Trusted platforms are increasingly being used as attack infrastructure

Microsoft Teams, SaaS integrations, package repositories, cloud services, and blockchain networks all appeared in campaigns observed during the reporting period. Nearly one in three monitored organisations experienced at least one Microsoft Teams IT-support impersonation attempt, and approximately one in every 990 external Teams contacts showed signs of impersonation activity. More than one in four confirmed ClickFix findings used blockchain-based command-and-control infrastructure. By operating through services users and security tools already trust, adversaries can blend into routine business activity and complicate detection.

Automation and criminal ecosystems are lowering the cost of attack

Researchers observed 6,188 delivery domains tied to just 158 payload hosts, illustrating the increasing industrialisation of attacker infrastructure. Mature criminal ecosystems now provide access, malware, phishing infrastructure, tooling, and operational support as services. This specialisation lowers barriers to entry, enables campaigns to scale quickly, and increases the speed at which attackers can move from initial access to operational impact.

Key Findings from the Report

- Approximately **1 in 3 monitored organizations** experienced at least one Microsoft Teams IT-support impersonation attempt.
- Approximately **1 in every 990 external Teams contacts** showed signs of impersonation activity.
- **Ontinue identified 10 confirmed** device-code phishing compromises in a two-month period.
- **More than 25% of confirmed** ClickFix findings leveraged blockchain-based command-and-control infrastructure.
- **Researchers observed 6,188 delivery domains** tied to just 158 payload hosts, highlighting the increasing industrialization of attacker infrastructure.
- Attackers are **increasingly achieving scale through trusted identities**, legitimate platforms, automation, and mature criminal ecosystems

Supporting Trends

- **Software supply-chain risk is extending beyond traditional vulnerabilities.** Stolen credentials can be used to compromise trusted development ecosystems at scale, while emerging AI agent research points to growing potential for automation in software manipulation and dependency abuse.
- **Social engineering is becoming more effective because it mirrors normal work.** Teams-based attacks, fake support interactions, ClickFix campaigns, and device code phishing exploit the workflows employees encounter every day.

- Traditional **malware-focused detection is less sufficient when attackers rely on legitimate identities**, platforms, and processes. Visibility across identity, collaboration, SaaS, and cloud activity is therefore increasingly important.

Recommended Priorities for Security Leaders

- **Make identity a primary security control.** Reduce reliance on password-based authentication, harden authentication workflows, and improve the ability to detect **token theft, device-code phishing, session hijacking**, and anomalous identity activity.
- **Extend visibility across collaboration and trusted business platforms.** Treat **Microsoft Teams, SaaS applications, cloud services**, and other everyday communication channels as part of the attack surface. Prioritise visibility into external contacts, impersonation attempts, unusual access, and misuse of trusted workflows.
- **Detect malicious behaviour, not just malicious software.** Expand detection beyond malware and known indicators to identify **suspicious use of legitimate identities, tools, platforms, and business processes**.
- **Strengthen governance of SaaS, third-party, and software supply-chain exposure.** Improve oversight of integrations, package repositories, dependencies, service accounts, cloud applications, and the access granted to external providers.
- **Accelerate investigation, decision-making, and containment.** Reduce the time between detection and action by giving security teams the context, authority, and response capabilities needed to **contain threats before they create wider operational impact**.

Management Takeaway

The central lesson from 1H 2026 is that attackers are achieving greater scale by abusing existing trust relationships. Identity systems, collaboration platforms, SaaS integrations, software supply chains, and routine business processes all featured prominently in observed campaigns. For executives, the priority is not simply to add more controls, but to focus investment on the areas where trusted activity can be manipulated: identity, platform visibility, behavioural detection, third-party exposure, and response speed.



© 2026 Ontinue. All Rights Reserved. Approved for public use

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.

[LEARN MORE](#)