



1H 2026 THREAT INTELLIGENCE REPORT

Geringe Angriffskosten lassen Cyberkriminelle im ersten Halbjahr schneller skalieren als Verteidiger

Das Advanced-Threat-Operations-Team von Ontinue hat die aktuelle Bedrohungslandschaft intensiv untersucht. Im ersten Halbjahr 2026 stellte es einen deutlichen Wandel fest, sodass die wirkungsvollsten Hackerattacken immer seltener wie Angriffe aussehen. Stattdessen erscheinen sie oft wie eine reguläre Microsoft-Teams-Nachricht mit einer gewöhnlichen Anfrage von jemandem aus der IT-Abteilung. Häufig sehen sie für User auch wie eine Anmeldeaufforderung einer vertrauenswürdigen Plattform oder für Entwickler wie ein Softwarepaket aus einem bekannten Repository aus. In allen Fällen ist die erste Stufe moderner Cyberangriffe zunächst einmal eines: unauffällig.

Während Unternehmen in stärkere Sicherheitskontrollen und den Perimeterschutz investieren, passen sich Angreifer an. Hacker nehmen heute gezielt die Vertrauensbeziehungen ins Visier, auf die sich Unternehmen täglich verlassen. Statt also ausgefeilte Schadsoftware einzusetzen oder technische Schwachstellen auszunutzen, verlassen sich Cyberkriminelle heute mehr auf Social Engineering, um legitime Identitäten, vertrauenswürdige Plattformen oder Business-Prozesse zu missbrauchen. Dabei gehen sie über kriminelle Ökosysteme heute zunehmend automatisiert vor.

Der aktuelle Threat Intelligence Report von Ontinue untersucht die bedeutendsten Bedrohungsaktivitäten, neuen Techniken und operativen Trends des ersten Halbjahrs 2026. Er stützt sich auf Beobachtungen aus Kundenumgebungen, Untersuchungen von Sicherheitsvorfällen, Recherchen zur Bedrohungslage sowie auf Daten des Advanced-Threat-Operations-Teams von Ontinue.

Die drei wichtigsten Entwicklungen im ersten Halbjahr 2026

Identitäten bleiben der zuverlässigste Weg, um sich Zugang zu verschaffen

Phishing über Gerätecode, Token-Diebstahl, das Sammeln von Anmeldedaten und Session-Hijacking ermöglichten weiterhin einen effektiven Zugriff auf, ohne dass Angreifer dafür Sicherheitslücken auf Endgeräten ausnutzen mussten. Ontinue stellte innerhalb eines Zeitraums von zwei Monaten einen Anstieg von Angriffen fest, bei denen Phishing über Gerätecodes zum Erfolg führte. Die anhaltende Einführung von Passkeys spiegelt wider, dass passwortbasierte Authentifizierungsmodelle gegenüber modernen Angriffstechniken weiterhin anfällig sind.

Vertrauenswürdige Plattformen werden zunehmend für Angriffe genutzt

Microsoft Teams, SaaS-Integrationen, Paket-Repositories, Cloud-Dienste und Blockchain-Netzwerke kamen in verschiedenen Angriffskampagnen vor, die im Berichtszeitraum beobachtet wurden. Fast jedes dritte überwachte Unternehmen war mindestens einem Versuch ausgesetzt, bei dem sich Angreifer in Microsoft Teams als IT-Support ausgaben. Bei etwa jedem 990. externen Teams-Kontakt gab es Anzeichen für einen solchen Identitätsmissbrauch.

Bei mehr als einem Viertel der bestätigten ClickFix-Fälle kam eine Blockchain-basierte Command-and-Control-Infrastruktur zum Einsatz. Indem Angreifer Dienste nutzen, denen Anwender und Sicherheitssysteme bereits vertrauen, können sie ihre Aktivitäten in den normalen Geschäftsalltag einbetten. Das macht es schwieriger, die Angriffe zu erkennen.

Automatisierung und kriminelle Netzwerke senken die Kosten für Angriffe

Forscher beobachteten 6.188 Domains, über die Schadsoftware verbreitet wurde und die mit nur 158 Hosts für Schadsoftware-Payloads verknüpft waren. Das zeigt, wie stark die Infrastruktur von Angreifern zunehmend industrialisiert wird. Etablierte kriminelle Netzwerke bieten inzwischen Zugangsmöglichkeiten, Schadsoftware, Phishing-Infrastruktur, Tools und operative Unterstützung als Dienste an.

Durch diese Spezialisierung sinkt die Einstiegshürde für Angreifer. Sie können ihre Kampagnen schnell ausweiten und schneller vom ersten Zugriff bis zu konkreten Auswirkungen auf den Betrieb gelangen.

Weitere Trends

- Risiken in der Software-Lieferkette gehen inzwischen über klassische Sicherheitslücken hinaus. Gestohlene Zugangsdaten können genutzt werden, um vertrauenswürdige Entwicklungsumgebungen in großem Umfang zu kompromittieren. Neue Forschung zu KI-Agenten zeigt zudem, dass Automatisierung bei der Manipulation von Software und dem Missbrauch von Abhängigkeiten zunehmend eine Rolle spielen könnte.
- Social Engineering wird immer effektiver, weil sich die Angriffe am normalen Arbeitsalltag orientieren. Angriffe über Microsoft Teams, gefälschte Support-Anfragen, ClickFix-Kampagnen und Phishing über Gerätecodes nutzen Arbeitsabläufe aus, mit denen Mitarbeitende täglich zu tun haben.
- Die klassische Erkennung von Schadsoftware reicht immer seltener aus, wenn Angreifer legitime Identitäten, Plattformen und Prozesse nutzen. Deshalb wird es immer wichtiger, Aktivitäten rund um Identitäten, Kollaboration, SaaS und Cloud-Dienste übergreifend im Blick zu behalten.

Empfohlene Maßnahmen für Sicherheitsverantwortliche:

- Identitäten als zentrale Sicherheitsmaßnahme etablieren. Die Abhängigkeit von passwortbasierter Authentifizierung reduzieren, Authentifizierungsprozesse besser absichern und die Erkennung von Token-Diebstahl, Phishing über Gerätecodes, Sitzungsübernahmen und auffälligen Aktivitäten rund um Identitäten verbessern.
- Den Überblick über Kollaborations- und vertrauenswürdige Geschäftsplattformen erweitern. Microsoft Teams, SaaS-Anwendungen, Cloud-Dienste und andere alltägliche Kommunikationskanäle als Teil der Angriffsfläche betrachten. Dabei sollte die Sichtbarkeit externer Kontakte, von Identitätsmissbrauch, ungewöhnlichen Zugriffen und dem Missbrauch vertrauter Arbeitsabläufe besonders im Fokus stehen.
- Schädliches Verhalten erkennen, nicht nur Schadsoftware. Die Erkennung über Schadsoftware und bekannte Angriffsmuster hinaus erweitern, um auch die verdächtige Nutzung legitimer Identitäten, Tools, Plattformen und Geschäftsprozesse zu erkennen.
- Die Kontrolle über SaaS, Drittanbieter und die Software-Lieferkette stärken. Die Überwachung von Integrationen, Paket-Repositories, Software-Abhängigkeiten, Dienstkonten, Cloud-Anwendungen und den Zugriffsrechten externer Dienstleister verbessern.
- Untersuchungen, Entscheidungen und die Eindämmung von Angriffen beschleunigen. Die Zeit zwischen Erkennung und Reaktion verkürzen. Dafür brauchen Sicherheitsteams den nötigen Überblick, klare Entscheidungsbefugnisse und die passenden Möglichkeiten, um Bedrohungen einzudämmen, bevor sie größere Auswirkungen auf den Betrieb haben.

Key-Takeaway für das Management:

Die zentrale Erkenntnis aus dem ersten Halbjahr 2026 ist, dass Angreifer durch den Missbrauch bestehender Vertrauensbeziehungen eine größere Reichweite erzielen. Identitätssysteme, Kollaborationsplattformen, SaaS-Integrationen, Software-Lieferketten und alltägliche Geschäftsprozesse spielten bei den beobachteten Angriffskampagnen eine wichtige Rolle. Für Führungskräfte geht es deshalb nicht einfach darum, weitere Sicherheitsmaßnahmen einzuführen. Vielmehr sollten Investitionen gezielt dort ansetzen, wo vertrauenswürdige Aktivitäten manipuliert werden können: bei Identitäten, der Sichtbarkeit von Plattformaktivitäten, der verhaltensbasierten Erkennung, den Risiken durch Drittanbieter und der Geschwindigkeit der Reaktion.

Ontinue

© 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