MONTHLY THREAT BRIEF

May 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in May 2026

At a Glance

Identity & Access Abuse

Software Supply Chain Risk

AI-Accelerated Threat Activity

Authentication Attacks Are Moving Beyond Passwords

The FBI warned organizations about Kali365, a phishing-as-a-service platform specifically designed to steal Microsoft 365 access tokens and bypass MFA protections through device-code authentication workflows. Rather than stealing passwords, attackers are increasingly targeting authenticated sessions and trusted access mechanisms.

What To Do

- Review device-code authentication usage
- Monitor OAuth and token activity
- Validate token revocation procedures

Supply Chain Attacks Continue to Expand

Microsoft identified malicious typosquatted npm packages designed to steal cloud credentials, CI/CD secrets, and software publishing tokens. These campaigns demonstrate how attackers increasingly target developer environments and software supply chains to gain downstream access into organizations.

What To Do

- Audit software dependencies
- Review CI/CD credential exposure
- Monitor package repositories
- Rotate exposed developer secrets

Brief

Kali365 MFA Bypass Campaign

FBI warns attackers are increasingly stealing authentication tokens instead of credentials to gain access to Microsoft 365 environments. These techniques allow attackers to bypass traditional MFA protections by abusing legitimate authentication workflows.

Malicious npm Packages

Microsoft uncovered active supply chain attacks involving typosquatted npm packages designed to steal cloud credentials, CI/CD secrets, and developer tokens. The campaign highlights the growing risk posed by trusted software repositories.

AI-Assisted Exploitation Activity

Google observed threat actors leveraging AI to support vulnerability research, exploitation development, and attack planning activities. As AI accelerates these processes, organizations may have less time to identify and respond to emerging threats.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and Business Risk

Identity Is Becoming The Primary Attack Surface

Organizations continue seeing attackers target identities, tokens, delegated permissions, and trusted authentication workflows rather than relying solely on credential theft. As cloud adoption increases, successful identity compromise can provide broad access across business systems.

What To Do

- Strengthen identity monitoring
- Enforce least privilege
- Review privileged accounts
- Monitor abnormal session behavior

Software Supply Chains Remain Attractive Targets

Recent npm campaigns highlight how a single compromised package can expose cloud credentials, deployment pipelines, and downstream environments. Software supply chain attacks continue providing attackers with scalable access opportunities.

What To Do

- Review dependency management practices
- Validate software sources
- Monitor package integrity
- Protect developer credentials

Trusted Platforms Continue Being Abused

Researchers identified malware campaigns leveraging Steam Community profiles as command-and-control infrastructure, highlighting how threat actors continue abusing trusted platforms to conceal malicious activity.

What To Do

- Monitor unusual outbound connections
- Review web application integrity
- Inspect third-party integrations
- Validate website file changes

Data Access Over Disruption

Many modern attacks prioritize gaining access to credentials, systems, and sensitive information, allowing threat actors to maintain long-term opportunities for exploitation rather than causing immediate disruption.

What To Do

- Monitor sensitive data repositories
- Review access controls
- Validate logging coverage
- Test incident response procedures

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Infrastructure, Vulnerabilities, and Operational Risk

AI Is Compressing Exploitation Timelines

Google Threat Intelligence reporting indicates attackers are increasingly leveraging AI to support vulnerability discovery, exploitation development, and operational decision-making. The result is a continued reduction in the time available for organizations to respond.

What To Do

- Reduce vulnerability remediation timelines
- Prioritize internet-facing systems
- Strengthen continuous monitoring
- Validate detection capabilities

Infrastructure Management Systems Remain High-Value Targets

The disclosure of significant vulnerabilities affecting enterprise infrastructure technologies reinforces the importance of securing management planes, administrative services, and externally accessible operational systems.

What To Do

- Inventory exposed infrastructure
- Secure management interfaces
- Review administrative access
- Monitor critical systems continuously

Vulnerability Prioritization Is Becoming Essential

Organizations continue facing increasing volumes of disclosed vulnerabilities. Effective risk reduction now depends on prioritizing exposure rather than attempting to address every vulnerability equally.

What To Do

- Prioritize based on exposure
- Track known exploited vulnerabilities
- Focus on critical assets first
- Measure remediation effectiveness

Operational Resilience Continues To Mature

Security programs are increasingly focusing on maintaining operations during adverse conditions rather than relying exclusively on prevention. Recovery capability, visibility, and response coordination are becoming key measures of cyber maturity.

What To Do

- Test recovery procedures
- Identify critical business functions
- Validate continuity plans
- Coordinate technical and operational teams

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

May 2026

Across this month's developments, several consistent themes are emerging for security and operational teams.

Identity Is The New Perimeter

Attackers increasingly target authentication workflows, access tokens, and trusted identities rather than passwords alone. As organizations continue moving critical systems and business processes to the cloud, identity has become one of the most important control points for both defenders and attackers.

Supply Chain Risk Extends Beyond Vendors

Developer environments, package repositories, CI/CD pipelines, and cloud credentials are becoming attractive targets for attackers seeking scalable access. Organizations must evaluate not only their own security controls, but also the integrity of the tools and dependencies that support daily operations.

AI Is Increasing Operational Speed

The gap between vulnerability discovery and exploitation continues shrinking as AI becomes more integrated into both defensive and offensive cyber operations. Faster attack cycles leave organizations with less time to assess risk, prioritize remediation, and respond effectively.

Exposure Reduction Matters More Than Vulnerability Volume

Organizations cannot patch everything, especially as vulnerability disclosures continue to increase. Success increasingly depends on understanding which exposures create meaningful operational risk and prioritizing remediation efforts accordingly.

Resilience Is Becoming A Business Requirement

Cybersecurity programs are increasingly measured by their ability to maintain and recover operations during disruptive events, not simply prevent incidents. Organizations that can quickly detect, respond, and continue operating are often better positioned to reduce long-term business impact.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

Critical Path Security Advisory:
The Future of OT Security Isn't Louder Scanning.
It's Smarter Modeling.

Traditional approaches often focus on increasing visibility through more scanning and more data collection. As operational environments become more complex, organizations need stronger modeling and a clearer understanding of how systems interact.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- Malware Uses Steam Profiles as Command-and-Control Infrastructure
- FBI Warning on Kali365 Microsoft 365 Attacks
- End-to-End Encrypted RCS Comes to Apple and Android

Threat Intelligence & Activity

- Microsoft: Typosquatted npm Packages Used to Steal Cloud and CI/CD Secrets
- Microsoft Defender Zero-Day Vulnerability Discovered
- Cisco SD-WAN Authentication Bypass Vulnerability

Stay Connected

Follow us on social media for the latest updates: