MONTHLY THREAT BRIEF

June 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in June 2026

At a Glance

Edge & Credential Abuse

Trusted-Platform Social Engineering

Critical Infrastructure Targeting

FortiBleed Turns Firewalls Into a Credential Factory

Researchers detailed FortiBleed, a global campaign that harvested tens of thousands of credentials from internet-facing FortiGate firewalls and VPNs across 194 countries. Notably, no zero-day was required. Attackers exploited weak credentials, exposed configurations, and reused sessions rather than a Fortinet software flaw.

What To Do

- Rotate all VPN and admin credentials
- Enforce phishing-resistant MFA (FIDO2)
- Revoke active sessions and API tokens

Nation-State Actors Hit U.S. Water Infrastructure

Sage Water Resources disclosed that a nation-state actor manipulated the control logic on a Utah salt-water disposal facility's PLC in March, part of a broader campaign against U.S. energy and water systems. An alert field operator caught the change before any physical or environmental damage occurred.

What To Do

- Baseline known-good PLC control logic
- Segment OT from IT behind a DMZ
- Broker remote access via a jump host
- Validate manual-failover and recovery runbooks

Brief

Decade-Long Breach of an Isolated Network

China-linked Velvet Ant hid in a critical-infrastructure network for roughly ten years by backdooring Linux PAM and OpenSSH modules. Embedding in the authentication layer let them survive password resets and observe all activity.

Cisco Unified CM Exploited

Cisco confirmed attackers are exploiting CVE-2026-20230, an unauthenticated SSRF flaw in Unified Communications Manager, weeks after patching. Over 200 instances remain exposed online. Apply the fix or disable the WebDialer service.

24 Billion Stolen Records

A massive 8.3 TB dump aggregating 24 billion records (largely infostealer logs) surfaced online. Beyond passwords, it includes session cookies and MFA tokens, letting attackers bypass logins entirely. Rotate credentials and invalidate active sessions.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and Business Risk

Attackers Are Living in the Auth Layer

Velvet Ant's decade-long intrusion shows a shift toward compromising authentication itself. By trojanizing PAM and OpenSSH, attackers captured every credential and survived resets. Identity infrastructure (not just user accounts) is now a primary persistence target.

What To Do

- Monitor integrity of PAM and sshd
- Alert on unexpected system-binary changes
- Harden and isolate identity/directory services
- Deploy file-integrity monitoring on key hosts

Credential Theft Is Outpacing Exploits

This month's largest campaigns relied on stolen or weak credentials rather than software exploits. FortiBleed and a 24-billion-record dump show that valid logins, tokens, and sessions now give attackers reliable, low-noise access into enterprise and edge environments.

What To Do

- Enforce phishing-resistant MFA (FIDO2/passkeys)
- Shorten session and token lifetimes
- Alert on impossible-travel and anomalous logins
- Vault and rotate privileged credentials

Help Desks Are Being Weaponized

Silent Ransom impersonated IT support through phone calls to push remote-access tools onto law-firm systems, moving from contact to data theft in under an hour. Any employee can be the entry point.

What To Do

- Restrict and monitor RMM tools
- Alert on unsanctioned remote-access installs
- Train staff on vishing and callback lures

Trusted Platforms Hide Malicious Traffic

DragonForce routed command-and-control through Microsoft Teams' own relay infrastructure. Blending into sanctioned collaboration and cloud services helps attackers evade network controls and defeat simple domain-based blocking.

What To Do

- Baseline normal SaaS and collaboration traffic
- Alert on outbound beaconing patterns

CONTINUED ON NEXT PAGE »

OPERATIONAL EXPOSURE

Infrastructure, Vulnerabilities, and Operational Risk

Edge Devices Remain the Front Line

Firewalls, VPNs, and gateways drove June's biggest incidents. FortiGate credential harvesting, an actively exploited Cisco Unified CM flaw, and fresh Citrix NetScaler bugs show that internet-facing appliances are still where attackers concentrate their effort.

What To Do

- Inventory all internet-facing appliances
- Prioritize patching for edge and VPN devices
- Restrict management planes to jump hosts
- Centralize and monitor appliance logs

OT Is Under Geopolitical Pressure

The Sage Water intrusion and ongoing nation-state targeting of energy and water systems show OT is now a strategic battlefield. Legacy configs, thin visibility, and internet-exposed PLCs make these environments attractive, high-impact targets.

What To Do

- Inventory and continuously monitor OT assets
- Remove PLCs and HMIs from internet exposure
- Baseline control logic; flag unauthorized changes
- Tie response to safety and process impact

Known-Exploited Flaws Demand Priority

Cisco confirmed CVE-2026-20230 under active attack weeks after patching, and Citrix fixed a CitrixBleed-style flaw. Attackers weaponize disclosures fast, so remediation should track real-world exploitation.

What To Do

- Track the CISA KEV catalog
- Prioritize actively exploited CVEs first
- Set aggressive SLAs for edge patching

Resilience Is Becoming a Mandate

CISA's CI Fortify push urges critical-infrastructure operators to master isolation and recovery, disconnecting from outside networks while keeping essential services running. Prevention alone no longer meets the bar.

What To Do

- Test network isolation and manual operation
- Maintain immutable, air-gapped backups
- Run tabletop exercises

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

June 2026

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

Identity Is the Real Perimeter

June's biggest campaigns succeeded through stolen credentials, hijacked sessions, and compromised authentication rather than novel exploits. As organizations move deeper into cloud and remote access, the identity layer (accounts, tokens, and the systems that verify them) has become the control point both sides fight over.

The Edge Is the Battleground

Firewalls, VPNs, gateways, and routers were at the center of nearly every major event this month. These devices sit exposed to the internet, hold privileged access, and are often under-monitored, making disciplined patching, credential hygiene, and log visibility on the edge non-negotiable.

Nation-State Risk Is Now Operational

Attacks on water and energy systems, decade-long infrastructure intrusions, and evolving Russian and Chinese tradecraft show geopolitical conflict is reaching operational technology. Critical-infrastructure operators should assume they are targets and plan for disruption, not just data theft.

Trust Is Being Turned Against You

Help-desk impersonation, on-site operatives, and command-and-control tunneled through Microsoft Teams show attackers increasingly abuse the tools and people employees already trust. Effective defense now depends on verifying requests, constraining remote-access software, and watching how sanctioned platforms are used.

Resilience Now Means Operating While Compromised

CISA's guidance this month makes resilience an operational requirement: critical-infrastructure operators must be able to isolate from outside networks, run essential functions manually, and recover quickly. Organizations that can absorb an intrusion and keep operating will limit both business and public impact.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

FortiBleed Turned 80,000 Firewalls Into a Global Credential Factory

One campaign defined June: attackers quietly harvested tens of thousands of FortiGate credentials worldwide using weak passwords and exposed configs — no zero-day needed. It's a clear reminder that credential hygiene and edge monitoring, not just patching, decide whether your perimeter holds.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- CISA CI Fortify: Critical Infrastructure Must Master Isolation & Recovery
- Nation-State Attack on Utah Water Infrastructure Contained
- Inside the FBI's New Kinetic Cyber Range

Threat Intelligence & Activity

- Citrix Patches NetScaler CitrixBleed-Style Flaw & HTTP/2 Bomb
- Velvet Ant Hid in an Air-Gapped Network for a Decade
- Cisco Confirms Active Exploitation of Unified CM Flaw (CVE-2026-20230)

Stay Connected

Follow us on social media for the latest updates: