THE ADVERSARY THAT WAITED 393 DAYS

THREAT BRIEFING / BRICKSTORM / AUGUST 2026

Partners should have one name on their radar this quarter: BRICKSTORM. Google Threat Intelligence and Mandiant tie it to UNC5221, a China-nexus espionage cluster, and CISA, NSA, and Canada's Cyber Centre have now published indicators for it. It is a Golang backdoor that lives on the equipment most teams cannot run an endpoint agent on - VMware vCenter, ESXi hosts, and network appliances at the edge.

The number that matters is the dwell time. Median time on target before detection was 393 days. More than a year of quiet access. The operators were not smashing through the front door - they sat on unmonitored appliances, then pivoted into identity infrastructure, cloned credentials, and read email. This is patient, strategic espionage aimed at exactly the blind spot most monitoring programs leave open.

WHY THE EDGE IS THE TARGET

vCenter, ESXi, and edge appliances rarely run an EDR agent. That is the point. BRICKSTORM chose the one layer most programs cannot see into, then used it as a launch pad into identity systems. No agent, no telemetry, no alarm.

WHAT PARTNERS SHOULD DO

Inventory every internet-facing and virtualization appliance. Assume the ones you cannot monitor are already in scope for an adversary. Validate the path from that appliance to your identity plane before someone else validation of the systems that face the internet. Prove the path from exposure to impact before someone else does.

BRICKSTORM BY THE NUMBERS

393	UNC5221	0	3 gov
median days of undetected access	China-nexus espionage cluster	EDR agents on a typical ESXi host	agencies issued BRICKSTORM IOCs

Bottom line: an adversary willing to wait 393 days will not be caught by a once-a-year look.

LIMITED-TIME PARTNER OFFER

CHRISTMAS IN JULY - 10% OFF ANNUAL PEN TESTING

Book any penetration test in Q3 2026 and take 10% off. Full details on page 3.

WHAT MOVED THIS MONTH

Three that matter, the actors behind the noise, and the operational signal underneath.

CVE-2026-50522 / MICROSOFT SHAREPOINT

Active exploitation of on-premises SharePoint has centered on stealing machine keys to keep access after the patch lands. Patching closes the door but does not evict anyone already inside. Rotate exposed secrets and hunt for persistence before you call it resolved.

CVE-2026-3055 / CITRIX NETSCALER

A memory-overread flaw in NetScaler configured as a SAML identity provider, added to CISA KEV after confirmed exploitation. Edge identity devices sit at the trust boundary. One overread there can unravel authentication for everything behind it.

CVE-2026-50751 / CHECK POINT VPN

A critical authentication bypass in deprecated IKEv1 certificate validation. If IKEv1 is not required, disable it. Legacy protocols left on for compatibility are a recurring theme - convenience today, incident tomorrow.

THE OPERATIONAL SIGNAL

Three different products, one pattern: internet-facing control planes are where reach lives. Attackers are not inventing exotic malware. They are borrowing access that already exists at the edge and moving before the maintenance window opens.

THREAT ACTOR WATCH

Storm-2603 continues to lead SharePoint key-theft activity, pairing web shells with rapid credential rotation to survive remediation. Separately, reporting points to coordinated probing of U.S. water and wastewater operators - low sophistication, high reach, aimed at exposed management interfaces.

EXPOSURE SNAPSHOT

SURFACE	SEEN	PRIORITY
Edge VPN / gateway	Rising	Critical
Identity providers	Rising	Critical
On-prem collaboration	Active	High
Legacy protocols	Steady	High
OT / utility access	Emerging	Watch

FEATURED STORY

THE EDGE IS THE NEW PERIMETER - AND IT IS UNDEFENDED

Look at this month's confirmed exploitation and one theme repeats: the initial foothold was an internet-facing appliance, not a phishing email. VPN gateways, SAML identity providers, and collaboration servers now carry the same risk a domain controller did a decade ago. They authenticate, they broker trust, and they sit exposed.

The uncomfortable part is timing. Three of this month's KEV additions were exploited before most teams finished their change-approval process. The attacker does not wait for your maintenance window. Treat every edge device as a live attack surface, inventory what actually faces the internet, and validate those paths on a schedule that matches the threat - not the fiscal calendar.

Field takeaway: if it answers on port 443 from the open internet, it belongs in scope for testing.

FROM THE TRENCHES

ONE FORGOTTEN VPN, FULL DOMAIN IN A WEEKEND

On a recent internal engagement the client swore the perimeter was clean. It mostly was. The exception was a decommissioned VPN concentrator that never got unplugged - still reachable, still running a firmware version two years past end of support. It took our operator under an hour to authenticate through it.

From there it was quiet living-off-the-land: harvested cached credentials, pivoted to a flat management VLAN, and reached domain admin before Monday. No exploit kit, no malware. Just one asset nobody owned and a network that trusted anything already inside it. The report had a single root cause - an inventory gap, not a zero-day.

FIELD TIP: HUNT THE SECOND MOVE

AFTER A CRITICAL EDGE FLAW IS PATCHED

Assume the attacker had time to authenticate, enumerate, or establish persistence before the update landed. Pull identity, VPN, web, and endpoint telemetry into one timeline. Look for impossible travel, new service principals, access from unusual networks, and authentication that continues after credentials were rotated. The patch closes a door. It does not tell you who already walked through it.

THREE QUESTIONS FOR THE NEXT SHIFT

+ Which internet-facing systems can still authenticate with legacy protocols?
+ Which privileged credentials were active on affected appliances before patching?
+ What evidence would prove the attacker did not move laterally?

THIS MONTH IN THE FIELD

> CISA KEV additions
SharePoint, NetScaler, and Check Point entries with confirmed exploitation.

> Edge-device targeting
Why VPN and identity appliances remain the shortest path to impact.

> Water-sector probing
Coordinated targeting of exposed OT management interfaces.

> Persistence after patch
Machine-key theft and the limits of remediation-as-closure.

LIMITED-TIME PARTNER OFFER / BOOK IN Q3 2026

CHRISTMAS IN JULY: 10% OFF ANY PENETRATION TEST

Compliance renewals do not wait for a convenient quarter. Neither do attackers. uMercs is running a Christmas in July offer for partners and their clients: book any penetration test in Q3 2026 and take 10% off. Network, web app, mobile, cloud, AI - if we test it, the discount applies.

This is built for teams facing SOC 2, PCI DSS, HIPAA, or ISO 27001 due diligence in the coming year. Lock the engagement in Q3, schedule the work when it fits your calendar, and satisfy the assessment requirement without the year-end scramble. One booking, the full testing catalog, a firm rate.

Partners: forward this to your clients. Clients: contact your uMercs account manager to reserve the rate before Sept 30.

SOURCES

Google Threat Intelligence Group / Mandiant, BRICKSTORM espionage campaign (UNC5221)
CISA / NSA / Canadian Cyber Centre, BRICKSTORM Malware Analysis Report AR25-338A
CISA KEV Catalog, July 2026 | Citrix CVE-2026-3055 | Check Point CVE-2026-50751
NVD entries for CVE-2026-3055, CVE-2026-50522, CVE-2026-50751