FortiBleed: The Anatomy of a Global Firewall Crisis

A CybrHawk Threat Intelligence Advisory on a global perimeter compromise affecting 73,932 FortiGate devices across 194 countries.

CYBRHAWK THREAT INTELLIGENCE ADVISORY

POWERED BY CYBRHAWK

The Incident: 75,000+ Compromised Gateways

Scale

73,932 unique FortiGate URLs were confirmed compromised. That is roughly **50%** of internet-facing FortiGate devices across **194 countries** and **21,632 domains**.

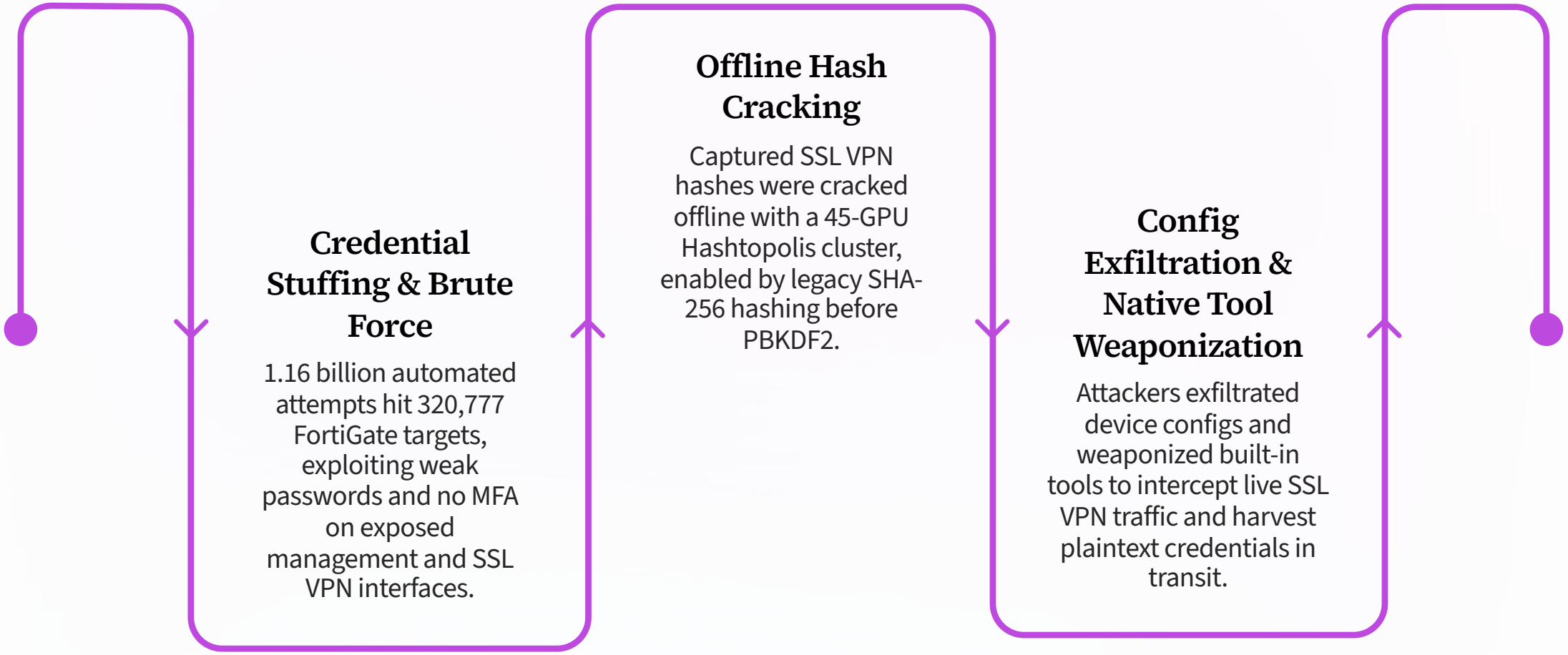
Method

A multi-vector IAB campaign used credential stuffing, brute-force attacks, dictionary attacks, and offline SHA-256 hash cracking. The effort included **1.16B+** attempts and a **45-GPU** Hashtopolis cluster.

Targets

Victims included **Chevron**, **AT&T**, **Samsung**, and **Toyota**. Critical infrastructure, government, and defense organizations were also hit.

How It Happened: The Mechanics of the Breach



FortiBleed was an industrialized credential campaign against exposed, MFA-free perimeter devices, not a zero-day.

The Aftermath: From Firewall to Internal Pivot

Initial Breach

Stolen credentials were used to gain unauthorized access to SSL VPN portals and management interfaces. In most cases, the FortiGate Management Interface was exposed directly to the internet.

Lateral Movement

Attackers pivoted into **Active Directory** and **LDAP** infrastructure. Their server contained AD credential-dumping tooling, including **Hashtopolis** for cracking AD hashes; they also targeted **Synology NAS** devices, **Sophos** firewalls, and **MSSQL** servers.

Persistence Established

Rogue administrator accounts were created as persistent backdoors, surviving firmware upgrades, reboots, and perimeter changes. Those credentials can remain valid long after the underlying device is patched.

Silent Dwell Time

Scheduled jobs, automation scripts, and operator command histories indicate long-term, organized access brokering operations. Select organizations were taken deeper into the network without triggering immediate alarms.

The Impact: A Global Enterprise Exposure

73,932

Unique Firewall URLs Compromised

21,632 domains across 194 countries, or about half of all internet-facing FortiGate devices.

1.16B+

Credential Attempts Executed

Automated brute-force and stuffing attacks hit 320,777 FortiGate targets.

319

Attacker Infrastructure Files Exposed

Scanners, automation scripts, Hashtopolis configs, credential catalogs, and operator command histories.

45 GPUs

GPU Cracking Cluster

A Hashtopolis-managed cluster cracked intercepted SSL VPN authentication hashes at industrial scale.

⊗ Chevron, AT&T, Samsung, Foxconn, Comcast, Mercedes-Benz, Toyota, and Fortinet show that no organization is immune based on brand or size.

CYBRHAWK RESPONSE

CybrHawk: Rapid Assessment & Containment

Discover

Identify all internet-facing FortiGate management interfaces and SSL VPN portals, then cross-reference against the verified 73,932-URL FortiBleed dataset via HudsonRock's checker (hudsonrock.com/fortinet).

Validate

Terminate all active admin and VPN sessions, audit for rogue administrator backdoor accounts, and review AD, LDAP, Synology NAS, Sophos, and MSSQL environments for lateral movement.

Remediate

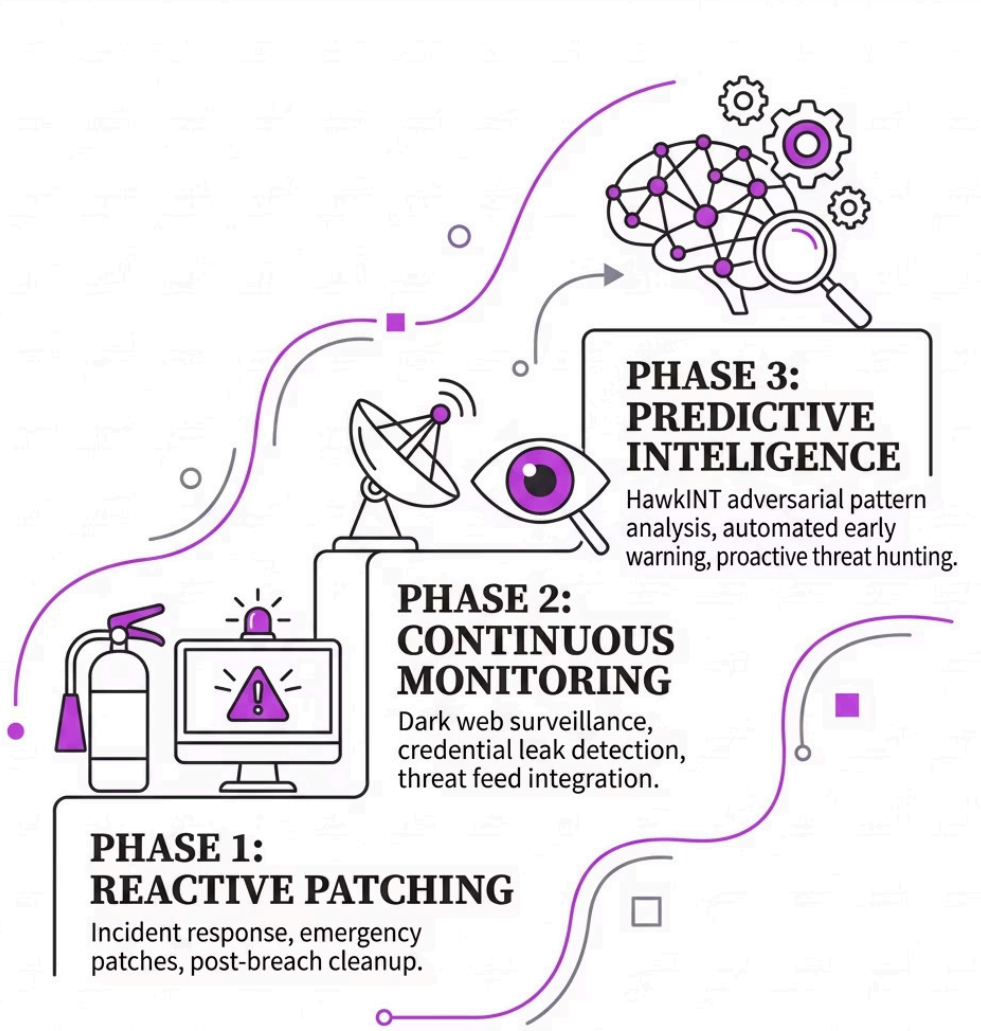
Reset all FortiGate credentials, enforce MFA on all admin and VPN accounts, upgrade firmware to FortiOS 7.4, 7.6, or 8.0 for PBKDF2 hashing, and segment management interfaces from internet exposure immediately.

STRATEGIC POSTURE

Moving Forward: Path to Cyber Threat Intelligence

FortiBleed confirms that perimeter patching alone cannot stop industrialized, automated adversaries running GPU-powered cracking and multi-operator coordination 24/7. **HawkINT** shifts your posture from reactive to predictive — detecting credential exposure and attacker recon before they reach your perimeter.

- Dark web and IAB marketplace monitoring for leaked credentials
- Real-time recon detection across your IP ranges and domains
- Early warning when threat actors target your industry stack



CYBRHAWK PLATFORM

Unified Cyber Defense Solutions

SIEM Integration

Centralizes log correlation and real-time alerts across your environment.

Cloud Detection

Detects threats across hybrid and multi-cloud environments automatically.

AI-Fortified Defense

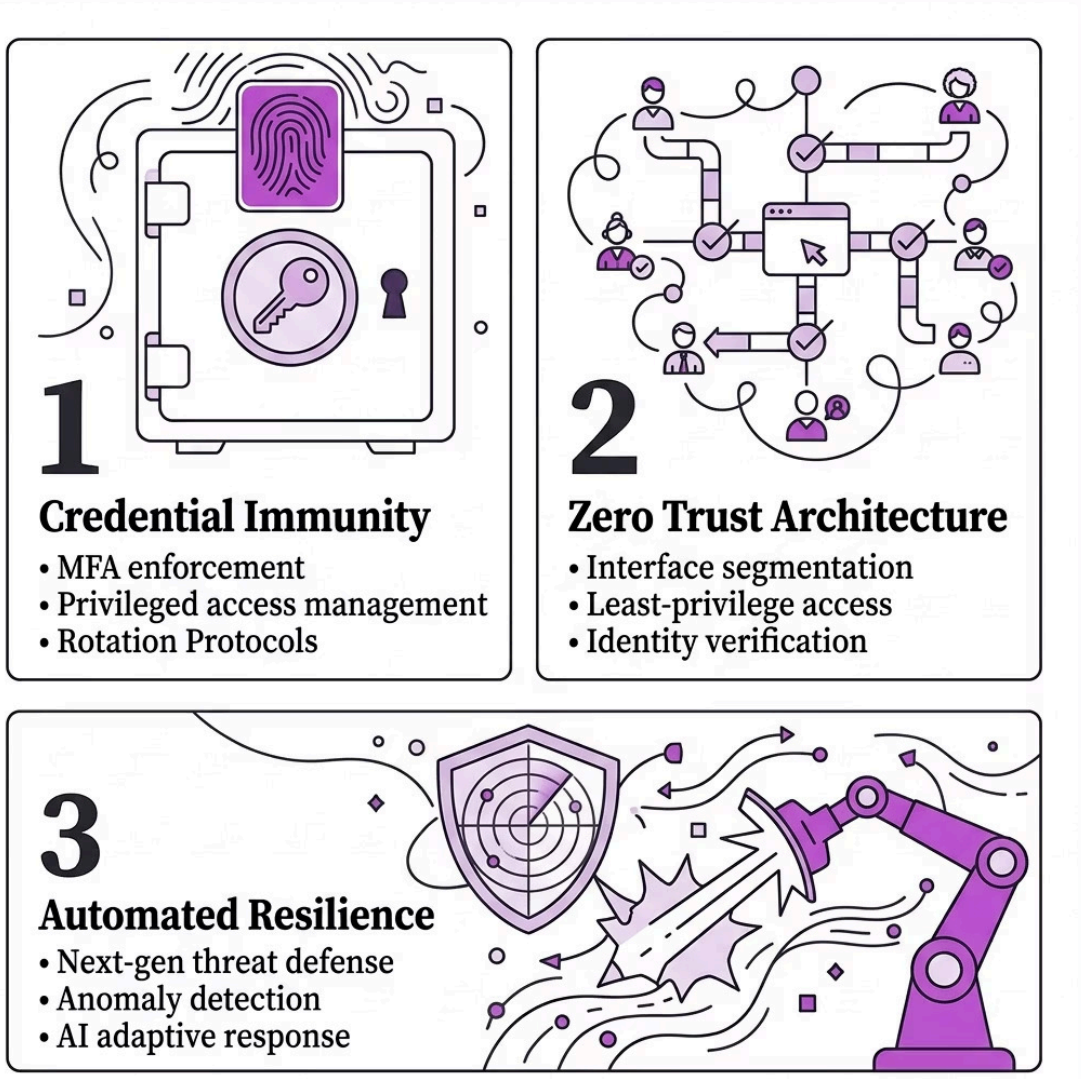
Uses machine learning to spot anomalies before they become breaches.

One Command Layer

Replaces siloed tools with a single, unified defense posture.

ENTERPRISE HARDENING

Strengthening the Enterprise



Building Immunity

Credential-harvesting campaigns like FortiBleed target weak identity hygiene. CybrHawk enforces **enterprise-grade MFA** and **privileged access controls** across every management interface.

Zero Trust Principles

Every administrative session is verified, and every interface is segmented. **No implicit trust** is granted to any user, device, or connection.

Automated Resilience

CybrHawk's AI-driven platform adapts to **next-generation automated threats**, reducing mean time to detect and respond from days to minutes.

Conclusion: Secure Your Perimeter, Own Your Future

FortiBleed is an active access-brokering operation with confirmed credentials for 73,932 organizations — **unified visibility, intelligence-led defense, and immediate credential hygiene** are the only effective responses.

1

Act Now

Cross-reference your FortiGate assets against the breach dataset, terminate sessions, reset credentials, and enforce MFA — today.

2

Assess Today

Engage CybrHawk for a Rapid Assessment covering exposure validation, rogue account audit, AD/LDAP lateral movement review, and a firmware remediation roadmap.

3

Defend Tomorrow

Transition to HawkINT for continuous, intelligence-led defense monitoring adversarial infrastructure, IAB activity, and credential exposure in real time.

CybrHawk Rapid Assessment is available immediately. Contact your CybrHawk representative or reach us at [contact info] to schedule your organization's FortiBleed exposure review.