INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 17:21 UTC

CyberStrikeAI, AI-Native Platform Compromises 600+ FortiGate Devices [SCC-2026-0004]

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0001
Type	Threat Campaign
Severity	CRITICAL
Published	20260304

Executive Summary

An AI-powered attack platform compromised 600+ firewall devices across 55 countries by targeting weak passwords, no software vulnerability needed. The same tools are available to other threat actors.

Technical Analysis

CyberStrikeAI is a Go-based AI-native offensive platform with 100+ tools and GenAI orchestration (Anthropic Claude + DeepSeek integration). Developer: Ed1s0nZ (assessed CNNVD/MSS-affiliated, medium confidence). Operator: Russian-speaking, financially motivated (medium confidence). Attack chain: credential-based, no CVE exploited. 600+ devices compromised Jan 11u2013Feb 18, 2026 across 55 countries. IOC: 212.11.64[.]250 (Switzerland, SWISSNETWORK02 AS, confirmed Team Cymru). Primary fix: configuration change, restrict management interface access, enable MFA.

Action Checklist

1. Audit FortiGate management interface exposure (remove https/ssh from WAN allowaccess)
2. Enable MFA on all FortiGate admin accounts
3. Rotate all FortiGate admin credentials
4. Block IOC 212.11.64[.]250 at perimeter
5. Review admin account list for unauthorized accounts created Jan 11u2013Feb 18
6. Run external scan to confirm management interface not internet-reachable

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO/executive team if any unauthorized admin accounts are confirmed or if external scans detect management interface still internet-reachable after remediation; engage external IR firm if device forensics indicates multi-month persistent access or secondary implants detected.
Recovery Notes	Post-containment: implement network segmentation to restrict management traffic to bastion hosts only (NIST CA-9). Deploy FortiGate logs to SIEM with 90-day retention minimum for forensic analysis. Conduct full access review across all 600+ affected devices to identify which were actively exploited vs. compromised credentials only. Establish quarterly credential audit process and monthly MFA effectiveness reviews.
Forensic Artifacts	FortiGate system logs (syslog, /var/log/messages) - admin login attempts, account creation events, CLI command history (diagnose test authd list) | FortiGate admin user database config snapshot (get system admin output) - creation timestamps, last login, privilege levels | Network packet capture on management interface (tcpdump/Wireshark) - source IPs, login protocols, payload analysis | Firewall allow/deny rules export (show firewall policy all) - document baseline access controls before/after remediation | External vulnerability scan results (Shodan, Censys, nmap) - timestamp before and after WAN interface hardening

Per-Action IR Details

Audit FortiGate management interface exposure (remove https/ssh from WAN allowaccess)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment Strategy)

Controls: NIST AC-3 (Access Enforcement), CIS 6.2 (Network Access Control)

Compensating: SSH to each FortiGate via console or bastion host. Run `config system interface` → `edit ` → list current allowaccess settings. Document baseline, then remove 'https' and 'ssh' from allowaccess string. Save config via `end`. If no bastion: use out-of-band serial console access or factory reset if device is confirmed compromised and unrecoverable.

Evidence: Capture FortiGate system logs (`diagnose debug flow trace start`) 24 hours before and after audit to document all management interface connection attempts. Export current admin user list via `get system admin` and timestamp. Preserve full config backup via `execute backup full-system ` before any changes.

Enable MFA on all FortiGate admin accounts

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 (Eradication)

Controls: NIST IA-2 (Authentication), CIS 6.3.1 (Multi-Factor Authentication)

Compensating: FortiGate supports RADIUS/LDAP-based MFA natively. If no external auth available: enable FortiToken (free, local OTP-based MFA). Configure via `config system admin` → enable `two-factor` and assign FortiToken serial. For air-gapped environments: document 2FA enablement in change log and require dual-admin approval for all future account modifications (manual compensating control per NIST AC-2).

Evidence: Export admin authentication settings before MFA enablement: `get system admin` and `get system local-user`. Capture MFA enrollment logs and backup of FortiToken activation records. Document which accounts have 2FA vs. single-factor (this data is critical for post-incident forensics to identify which accounts remained at risk during the campaign window).

Rotate all FortiGate admin credentials

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 (Eradication)

Controls: NIST IA-4 (Identifier Management), CIS 6.2.1 (Credential Reset)

Compensating: Generate 24+ character random passwords (use `openssl rand -base64 32`). Store new credentials in offline password manager (KeePass, not cloud-based). Rotate via serial console if network access is suspected compromised. After rotation, log in with new credentials and verify no additional admin accounts exist via `get system admin` (attackers often create backdoor accounts). Document old vs. new password hash timestamps from FortiGate logs.

Evidence: Capture FortiGate authentication logs before rotation: `diagnose test authd list` to show all current admin authentication attempts in last 30 days. Export admin user configuration snapshot. After rotation, capture login success/failure logs for 48 hours to detect attackers attempting old credentials (indicates active compromise).

Block IOC 212.11.64[.]250 at perimeter

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment Strategy)

Controls: NIST SC-7 (Boundary Protection), CIS 9.1 (Network Segmentation)

Compensating: If no centralized firewall: block at host-level using `iptables` (Linux) or Windows Defender Firewall (Windows). Linux: `iptables -I INPUT -s 212.11.64.250 -j DROP` and persist via iptables-save. Windows: `netsh advfirewall firewall add rule name='Block-CyberStrikeAI-IOC' dir=in action=block remoteip=212.11.64.250`. Monitor for outbound connection attempts to this IP via `netstat -anob` (Windows) or `ss -tulnap` (Linux). Escalate if C2 traffic is detected after blocking (indicates secondary implant).

Evidence: Capture network traffic 24 hours before blocking: use `tcpdump -i any host 212.11.64.250 -w ioc_traffic.pcap` (or Wireshark). Review firewall logs for any connections to this IP (connection timestamp, source port, destination port, payload size). Check proxy/web logs if applicable. Document baseline connection patterns to confirm this is actual malicious traffic vs. false positive.

Review admin account list for unauthorized accounts created Jan 11–Feb 18

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis)

Controls: NIST AC-2 (Account Management), CIS 6.1.1 (Inventory and Control of Enterprise Software)

Compensating: Export full admin user list: `get system admin` on each device. Cross-reference against change management records and documented authorized accounts. For accounts with no documented approval: check creation timestamp via `diagnose test authd list` or FortiGate syslog. Correlate creation date to network logs during Jan 11–Feb 18 window to identify source IP of account creation. Use `diagnose system logd reset stats` to clear stats, then enable syslog forwarding to external server to preserve future account changes.

Evidence: Capture admin account creation logs from FortiGate system logs (look for 'User' login events and 'admin' privilege grants). Export current admin list with timestamps. Preserve FortiGate CLI history (`show history`). Check authentication attempt logs for accounts created during campaign window to see if attacker tested new accounts immediately after creation. If FortiGate syslog is not enabled, manually review the admin account database backup captured in step 1.

Run external scan to confirm management interface not internet-reachable

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 (Post-Incident Activities, validation phase)

Controls: NIST CA-8 (Security Assessment and Authorization), CIS 11.2.4 (Network Segmentation Testing)

Compensating: Use free external scan tools: Shodan query for FortiGate HTTPS banner on your public IP range (shodan.io), or nmap from external VPS: `nmap -p 443,22 --script ssl-cert `. If results show FortiGate listening on WAN: immediate escalation. Document scan baseline before and after remediation. For air-gapped validation: use internal subnet scanner (nmap) from trusted workstation to confirm management ports NOT responding from WAN-facing interfaces.

Evidence: Capture baseline external scan results (Shodan, Censys, or nmap scan) BEFORE removing management interface from WAN. Re-run identical scan after remediation and document before/after comparison. Preserve scan reports with timestamps. Check firewall rule export to confirm deny rules were added (not just interface configs changed—rules are the enforcement layer per NIST SC-7).

Detection Guidance

Monitor FortiGate devices for anomalous management plane activity including unexpected configuration changes, new admin account creation, or modified firewall policies without corresponding change tickets. SIEM Rules: (1) Alert on multiple failed authentication attempts followed by successful login from previously unseen source IPs targeting FortiGate management interfaces on TCP/443 or TCP/8443. (2) Detect outbound connections from FortiGate management IPs to non-baseline external destinations, particularly long-duration low-bandwidth beaconing patterns with jitter intervals between 30-300 seconds. (3) Alert on CLI commands executed via SSH or web UI that include 'execute factoryreset', 'config system admin', 'set password', 'diag debug', or bulk policy deletions outside maintenance windows. (4) Correlate FortiGate syslog events for privilege escalation indicators: admin role changes, new super_admin accounts, or SSH key additions not initiated through approved IAM workflows. (5) Detect lateral movement from compromised FortiGate devices by monitoring for ARP scanning, ICMP sweeps, or TCP SYN floods originating from firewall internal interfaces toward internal subnets. (6) Flag anomalous VPN tunnel establishments: new peer IPs, unusual geographic locations, or tunnels created without corresponding user authentication events in identity provider logs. (7) Monitor for fileless persistence indicators: unexpected processes spawned from FortiGate httpsd or sshd daemons, or anomalous memory allocation in management daemon processes. (8) Baseline and alert on deviations in FortiGate SNMP trap frequency, syslog volume drops that may indicate log suppression, or NTP synchronization failures that could indicate tampering. (9) Correlate threat intelligence feeds against source IPs connecting to FortiGate management interfaces; alert on matches to known CyberStrikeAI campaign infrastructure. (10) Implement watchlist for CVE-agnostic zero-day exploitation patterns including malformed HTTP headers to management GUI, oversized POST bodies to /api/v2/ endpoints, and unexpected 500-series responses indicating server-side errors under adversary manipulation.

Indicators of Compromise

Type	Value	Context	Confidence
IPV4	`212.11.64.250`	CyberStrikeAI C2/service banner	HIGH

Framework Mappings

MITRE-ATTACK

- **T1595.001** — Scanning IP Blocks
- **T1078** — Valid Accounts
- **T1219** — Remote Access Tools

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1595.001	Scanning IP Blocks	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Amazon Security Disclosure (2026-02-21)	https://aws.amazon.com/security	T3
BleepingComputer	https://www.bleepingcomputer.com	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 17:21 UTC by TJS Security Command Center