Castellum labs

FORTIBLEED

Credential Harvesting Campaign

THREAT ADVISORY REPORT

+91 7842046995 www.castellumlabs.com reach@castellumlabs.com

Castellum labs

EXECUTIVE SUMMARY

Between June 13–17, 2026, researchers confirmed a large-scale credential-harvesting campaign FortiBleed affecting ~75,000 internet-facing FortiGate firewalls and SSL VPN gateways across **21,600+ domains in 194 countries**. Over **30,700 credentials** have been independently verified as working.

FortiBleed is not a new zero-day. It is the consolidation of years of accumulated Fortinet credential leaks, infostealer malware, and offline cracking, now packaged for resale to criminal buyers. Several actively exploited CVEs are being used in parallel to gain and maintain access.

This advisory is rated Critical due to the scale and confirmed authenticity of exposure, active exploitation of related CVEs, and confirmed cases of compromised firewalls being repurposed to harvest internal network credentials. Immediate action is required, regardless of confirmed dataset inclusion.

Metrics

Metric	Value
FortiGate Targets Scanned	320,777
FortiGate Login Attempts	1.16 Billion
Exposed Firewalls Identified.	73,932
MSSQL Servers Hit	163,650
MSSQL Brute-Force Attempts	2.1 Billion
Infected Hosts (Hostopolis)	45
Organizations Fully Compromised	4
Countries Affected	194

Castellum labs

What is FortiBleed

FortiBleed is the name of a credential-harvesting operation and dataset discovered in June 2026 not a Fortinet product or single vulnerability. Researcher **Volodymyr Diachenko** discovered it after the threat actor left their operational server publicly exposed, revealing scanning tools and a structured victim database.

Kevin Beaumont independently confirmed credential authenticity and assessed the data was sourced from exported FortiGate configuration files. Each record is enriched with industry, revenue, and headcount data – consistent with initial access broker (IAB) tooling built for resale rather than a raw dump.

Key Details

- Researchers attribute this to a **Russian-speaking** multi-operator group conducting large-scale credential harvesting against Fortinet FortiGate SSL VPN appliances worldwide.
- They intercept SSL VPN authentication, crack hashes on a 45-GPU cluster managed via Hashtopolis, and pivot into internal Active Directory environments.
- At least four organizations across **Japan, Taiwan/Vietnam, Iraq, and Turkey** were fully compromised including a **Turkish NATO defense contractor** whose classified defense documents were exfiltrated.
- The operation processed 1.16 billion credential attempts against 320,777 FortiGate targets and 2.1 billion attempts against 163,650 MSSQL servers
- Named organizations include FedEx, Samsung, Oracle, AT&T, Toyota, Siemens, PwC, Accenture, plus government and critical infrastructure entities were also affected.

FORTIBLEED Timeline

Phase 1

Threat actors accumulated credentials from previous Fortinet-related leaks, infostealer infections, and exposed credential datasets.

- Collection of leaked Fortinet credentials
- Acquisition of infostealer-harvested usernames and passwords
- Preparation of large credential databases for automated attacks

Phase 2

Attackers launched automated authentication attempts against FortiGate VPN and firewall devices worldwide.

- ~1.16 billion login attempts
- 320,777 FortiGate targets scanned
- 73,932 exposed Fortinet devices identified
- Activity observed across 194–207 countries

Phase 3

In parallel with FortiGate attacks, the threat actors targeted Microsoft SQL Server infrastructure.

- ~2.1 billion credential attempts
- 163,650 MSSQL servers targeted
- Large-scale automated brute-force activity

Phase 4

Where password reuse failed, attackers intercepted SSL VPN authentication hashes from targeted environments.

- Capture of VPN authentication hashes
- Collection of credential material from compromised devices
- Preparation for offline cracking

Phase 5

Attackers used a dedicated GPU cracking infrastructure to recover plaintext passwords.

- 45-GPU cracking cluster
- Hashtopolis management platform
- Offline cracking of captured VPN hashes

Phase 6

Recovered credentials were used to access internal corporate environments.

- Active Directory authentication
- Lateral movement
- Access to internal resources
- Establishment of persistence

Phase 7

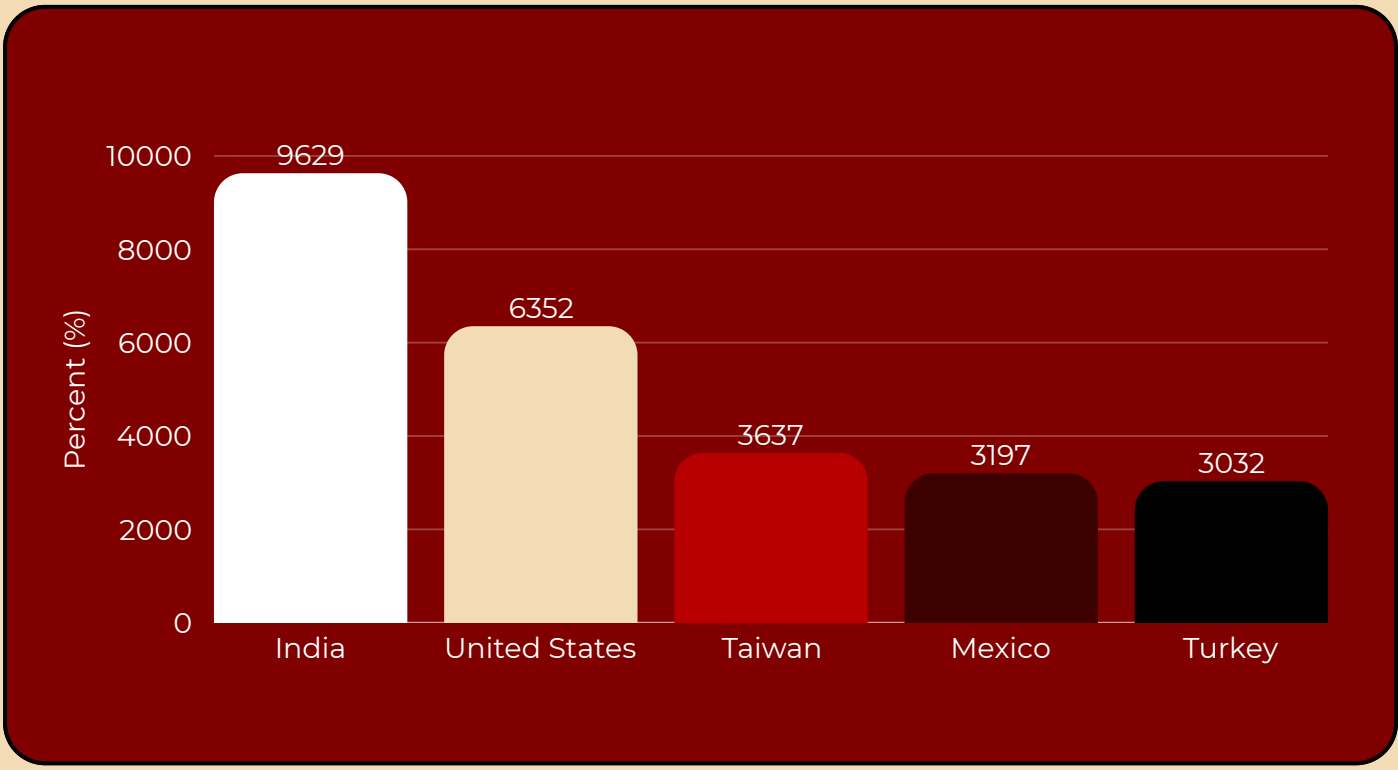
Attackers used a dedicated GPU cracking infrastructure to recover plaintext passwords.

- VPN authentication traffic
- LDAP authentication traffic
- RADIUS authentication traffic
- Active Directory authentication traffic

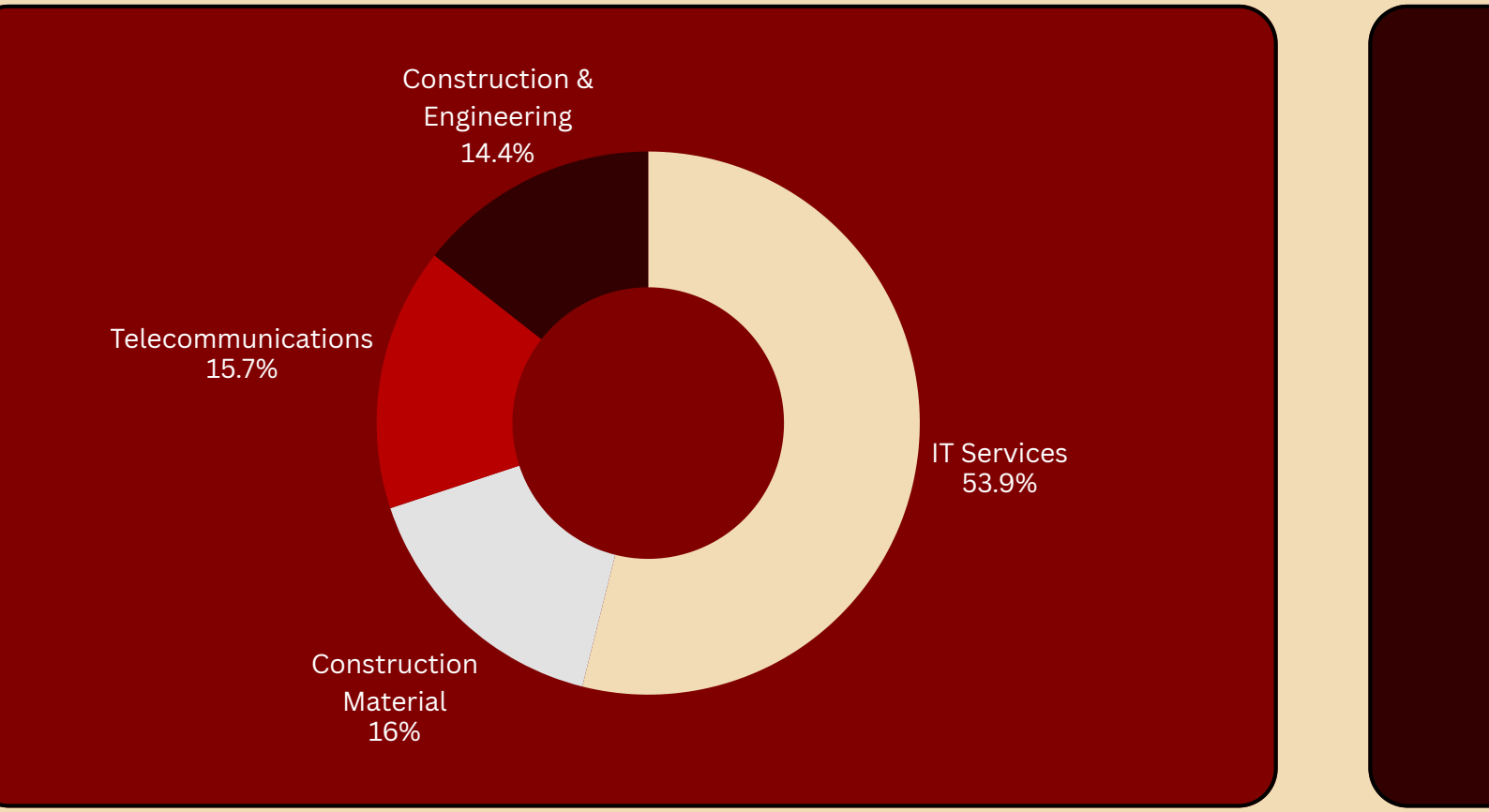
Phase 8

Security researchers publicly identified the campaign and associated it with the name "FORTIBLEED."

Top Impacted Countries



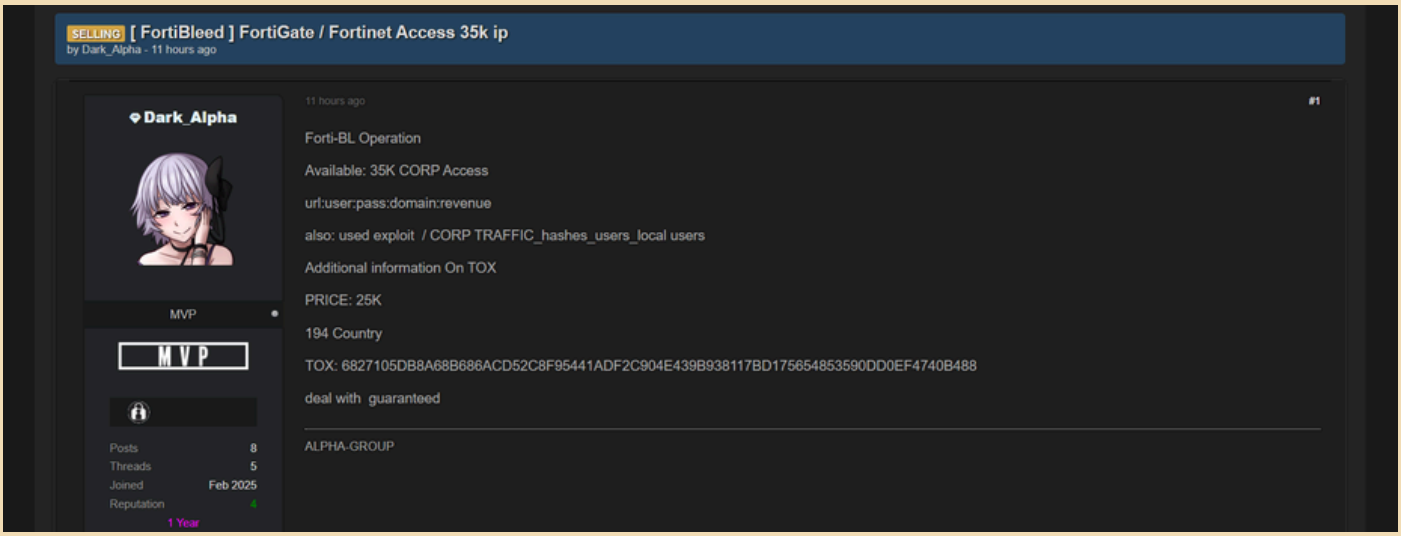
Top Impacted Industries



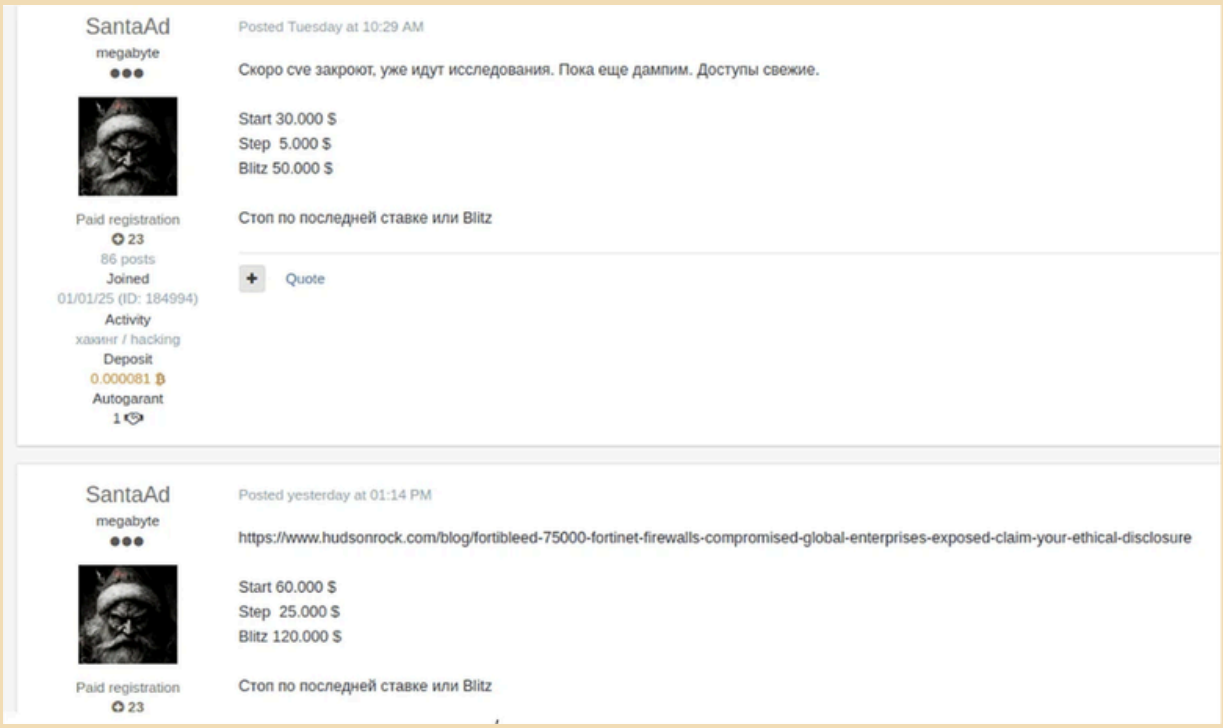
Castellum labs

Dark Web Activity related to FORTIBLEED

Actor: Dark_Alpha
Date Observed: 20th June 2026
Platform: Underground Forum
Contact Method:
TOX - 6827105DB8A68B686ACD52C8F95441ADF2C904E439B938117BD175654853590DD0EF4740B488



Actor: SantaAd
Date Observed: 16th June 2026
Platform: Underground Forum



Castellum labs

Mitigations

Organizations utilizing Fortinet FortiGate devices should assume potential credential exposure and take immediate steps to reduce the risk of unauthorized access, credential abuse, and post-compromise activity associated with the FORTIBLEED campaign.

1. **Reset and Rotate All Credentials**

Immediately rotate all credentials associated with FortiGate infrastructure, including:

- Administrative accounts
- Local user accounts
- SSL VPN accounts
- Service accounts
- Shared privileged credentials

Organizations should treat any potentially exposed credentials as compromised, regardless of whether unauthorized access has been confirmed.

2. **Upgrade to a Secure FortiOS Version**

Upgrade all affected devices to a supported FortiOS release that contains the latest security fixes:

- FortiOS 7.2.11 or later
- FortiOS 7.4.8 or later
- FortiOS 7.6.1 or later

Following the upgrade, administrators should authenticate to the device to ensure legacy password hashes are migrated to stronger password-hashing mechanisms where applicable.

3. **Strengthen Password Hashing Controls**

Enable the appropriate FortiOS settings to eliminate weaker password-hashing compatibility and enforce stronger credential protection.

Recommended settings include:

- FortiOS 7.6.x: login-lockout-upon-weaker-encryption
- FortiOS 7.2.x / 7.4.x: login-lockout-upon-downgrade

This helps prevent continued reliance on legacy password-hashing methods.

4. **Remove Public Exposure of Management Interfaces**

Restrict access to FortiGate management interfaces and administrative services.

Recommended actions:

- Remove management interfaces from direct Internet exposure
- Limit administrative access to trusted IP ranges
- Utilize VPN-based administration where possible
- Implement dedicated management networks or out-of-band administration paths
- Review firewall rules permitting management access from external networks

Management interfaces should never be publicly accessible unless there is a documented business requirement and compensating security controls are in place.

5. **Enforce Multi-Factor Authentication (MFA)**

Enable MFA for all privileged and remote-access accounts, including:

- Administrative users
- SSL VPN users
- Third-party support accounts
- Privileged service accounts where supported

MFA significantly reduces the effectiveness of credential-stuffing, password-spraying, and stolen credential attacks.

6. **Conduct a Compromise Assessment**

Perform a detailed review of security logs and authentication records to identify signs of unauthorized access.

- Unexpected administrator logins
- Newly created user or administrator accounts
- Unauthorized configuration changes

- Modified firewall policies
- Disabled logging or monitoring controls
- SSL VPN access outside normal operating hours
- Logins from unfamiliar IP addresses or geographic locations
- Suspicious authentication failures followed by successful logins

Organizations should retain and review historical logs covering at least the previous 90 days where possible.

7. **Review Active Directory and Identity Infrastructure**

Because valid credentials may have been used to access internal environments, organizations should review:

- Active Directory administrative accounts
- Domain administrator activity
- LDAP authentication logs
- RADIUS authentication logs
- Privileged group membership changes
- Service account activity

Special attention should be given to evidence of lateral movement, privilege escalation, and unauthorized account creation.

8. **Search for Persistence Mechanisms**

Conduct a comprehensive review of affected systems to identify potential persistence established by threat actors.

Review for:

- Unauthorized local accounts
- Scheduled tasks
- Startup scripts
- Administrative backdoors
- Unapproved VPN accounts
- Rogue firewall policies
- Suspicious tunnels or proxy services

Particular attention should be paid to indicators associated with tunneling and remote access tools that may facilitate covert communication.

9. **Validate Exposure Through Credential Monitoring**

Organizations should determine whether corporate credentials have been exposed through:

- Credential leaks
- Infostealer infections
- Dark web marketplaces
- Underground forums

Any identified exposed credentials should be immediately reset and investigated for evidence of unauthorized use.

10. **Apply Security Updates Across the Environment**

In addition to FortiGate remediation efforts, organizations should ensure all Internet-facing systems are fully patched and updated.

Priority should be given to:

- Remote access infrastructure
- VPN appliances
- Identity and authentication systems
- Public-facing applications
- Critical servers and management platforms

All known vulnerabilities identified during the investigation should be remediated without delay.

11. **Enhance Monitoring and Detection**

Increase monitoring of authentication and network activity for indications of continued exploitation.

Recommended controls include:

- Real-time authentication alerting
- Detection of credential-stuffing activity
- Monitoring for excessive login failures
- Geographic anomaly detection

- Privileged account monitoring
- VPN access monitoring
- Security event correlation across firewall and identity systems

Continuous monitoring should remain in place until organizations have high confidence that no unauthorized access persists.

12. **Review Incident Response Readiness**

Organizations should validate their ability to respond to follow-on attacks that may result from credential exposure.

This includes:

- Updating incident response procedures
- Verifying backup integrity
- Testing recovery processes
- Confirming security logging coverage
- Reviewing privileged access management controls
- Preparing containment procedures for ransomware or data theft scenarios

Given the observed monetization of Fortinet-related credentials on underground forums, organizations should anticipate potential secondary attacks by unrelated threat actors who acquire compromised credentials from criminal marketplaces.

Castellum labs

Top CVE’s Associated with Fortinet

CVE ID	Affected Product	CVSS	Severity
CVE-2026-24858	FortiOS / FortiGate	9.8	Critical
CVE-2025-59718	FortiOS / FortiGate	9.8	Critical
CVE-2026-35616	FortiClient EMS	9.8	Critical
CVE-2026-21643	FortiClient EMS	9.8	Critical
CVE-2026-25089	FortiSandbox	9.1	Critical
CVE-2026-39808	FortiSandbox	9.1	Critical
CVE-2026-39813	FortiSandbox	9.1	Critical

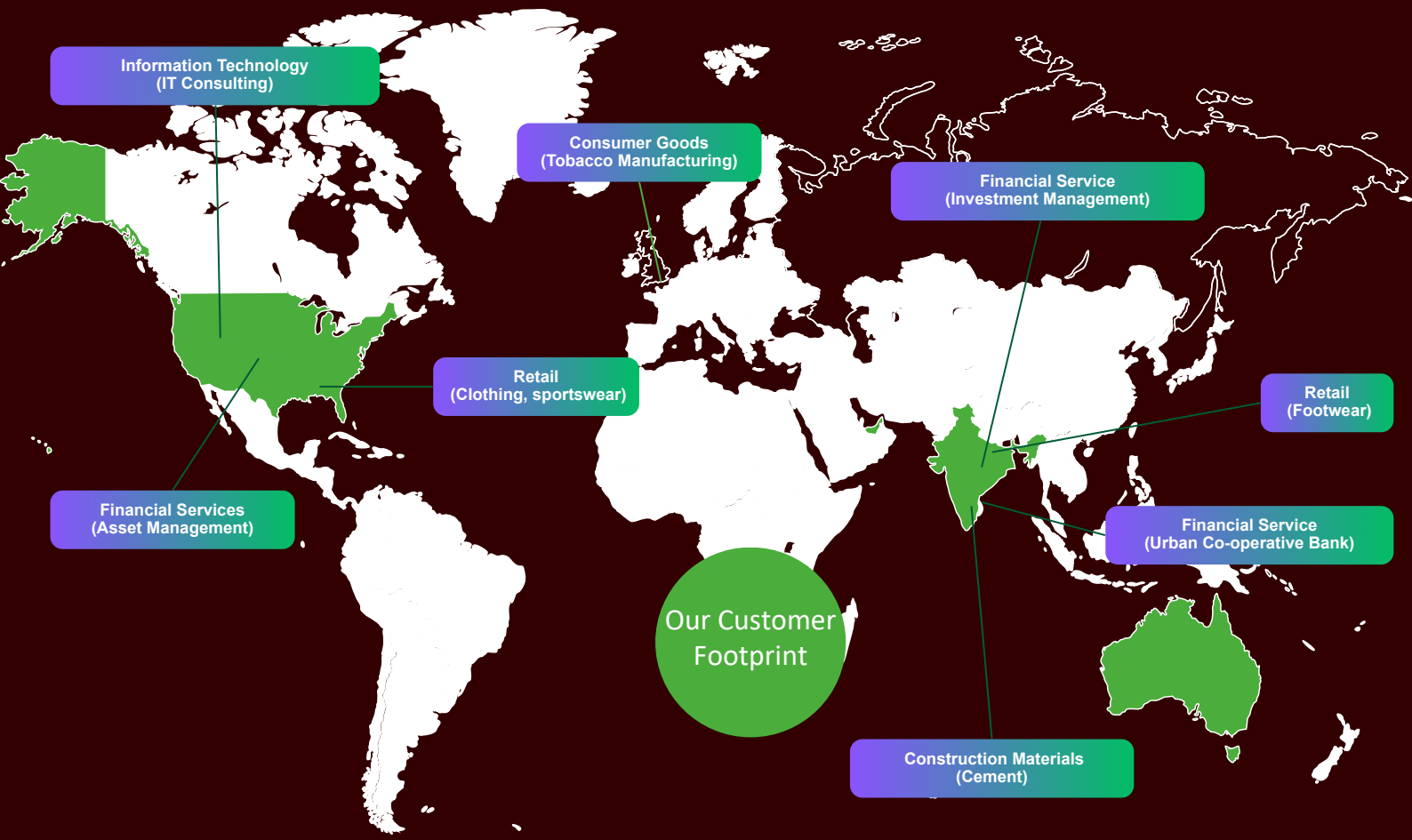
References

- https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries/
- https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/
- https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure
- https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8
- https://www.linkedin.com/posts/vdyachenko_executive-summary-based-on-my-investigation-share-7472221359629185024-ISun/
- https://socfortress.medium.com/fortibleed-global-compromise-of-75-000-fortinet-firewalls-66d99a036e47

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995