Executive Summary

5 active campaigns identified this week targeting Healthcare and Technology sectors across the Americas, Europe, and Asia. **High priority:** Cloud platform attacks (+45%) and ransomware deployments are trending upward. 293 total indicators of compromise (IOCs) identified.

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
ShinyHunters Cloud Data Theft (CAMP.26.003)	Financial	Financial Svcs, Legal/Prof Svcs (US)	Vishing + fake login pages to steal creds; register rogue MFA devices on cloud platforms (Salesforce, Google, etc.)	Review MFA device registrations; train staff on vishing
CrushFTP / TRIDENT Ransomware (CAMP.26.004)	Financial	Tech, Financial, Insurance, Mfg (US)	Exploit CrushFTP vulns; deploy WAVECALL malware + TRIDENT ransomware; rapid lateral movement	Patch CrushFTP immediately; ensure offline backups
UNC6293 Drive-by Web Compromises (CAMP.25.086)	Espionage	Healthcare, Tech, Mfg, Gov (US, EU, Asia, NZ)	Compromise legitimate websites to display fake Microsoft login pages; credential harvesting	Enable Defender SmartScreen; implement passwordless auth
ATOMICPROMPT MacOS Malware (CAMP.25.088)	Unknown	Tech, Mfg, Education, Legal (US, UK)	AI-generated malvertising lures Mac users into running Terminal/cURL commands; bypasses Gatekeeper	Educate Mac users; block untrusted script execution
Iranian TWOSTROKE Espionage (CAMP.25.082)	Espionage	Gov, Telecom (Middle East: Azerbaijan, Turkey)	Targeted phishing delivers C++ backdoor; encrypted C2 over port 443; expanding target scope	Monitor outbound SSL/TLS to unknown domains; email sandboxing

Top 3 Actions This Week

1. **Review MFA Devices:** Audit all critical accounts (especially cloud platforms) for unauthorized MFA device registrations. Remove any you don't recognize.
2. **Train on Vishing:** Brief your team on voice phishing – remind everyone that IT will never call asking for passwords or MFA codes.
3. **Test Your Backups:** Verify backup systems are operational and backups are stored offline where ransomware can't encrypt them.

Threat Metrics

Activity Trends

- ▲ **+45%** Cloud platform attacks
- ▼ **-75%** Ransomware activity
- ▲ **+16%** MacOS malware
- ▼ **-21%** Espionage campaigns

Indicators of Compromise: 293

- 225 Domains
- 14 IP Addresses
- 40 URLs
- 14 Malicious Files

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov)