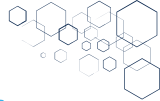


MONTHLY

CYBER THREAT INTELLIGENCE REPORT

APRIL 2026





EXECUTIVE SUMMARY

April 2026 has seen a continued rise in identity-driven attacks, supply chain compromises, and ransomware activity. Cyber threats are becoming more structured, automated, and commercially driven.



Major Cyber Incidents

- France Government Data Breach – Over 11 million users impacted.
- Vercel Supply Chain Attack – OAuth compromise exposed internal systems.
- North Korean Laptop Farm – Insider-style access across 100+ organisations.
- Global Phishing Network – \$20M fraud operation dismantled.
- ADT Data Breach – Identity compromise via SSO.



Emerging Threats & Malware

- AgingFly Malware – Dynamic code execution.
- ZionSiphon – Targets critical infrastructure.
- Payload Ransomware – Double extortion model.
- Osamabinladen Stealer – Credential and data exfiltration.
- Krybit Ransomware – Emerging RaaS threat.



Vulnerability Landscape

Critical vulnerabilities identified across Cisco, Fortinet, Adobe, Chrome, and Apache platforms. Many vulnerabilities exceed CVSS 9.0 and require urgent patching.



Ransomware Activity Overview

- 756 claimed victims in April 2026.
- Top target: United States.
- Top sector: Business Services.
- Active groups include Qilin, LockBit variants, and ShinyHunters.



Key Takeaways

- Identity-based attacks dominate
- Supply chain compromise increasing
- Ransomware evolving rapidly
- Critical infrastructure targeted
- Vulnerabilities remain primary attack vector



System Force I.T.
Secure IT Simplified

RECOMMENDATIONS

Enforce MFA, patch vulnerabilities, deploy EDR, maintain backups, and train staff regularly.

Next Step:

Book your free Monthly Cyber Threat Intelligence Report April 2026.

 01452701355

 www.systemforce.co.uk

 sales@systemforce.co.uk

