VigilIntel

EXECUTIVE THREAT INTELLIGENCE BRIEFING

TLP:CLEAR | PAP:CLEAR

EXECUTIVE THREAT INTELLIGENCE BRIEFING

FEBRUARY 2026

Senior Threat Intelligence Analyst | Strategic Briefing

STRATEGIC LANDSCAPE OVERVIEW

01 / ESPIONAGE

State-aligned espionage dominates the current threat landscape.

02 / INFRASTRUCTURE

Critical exploitation of remote management software is rising.

03 / GEOPOLITICS

Geopolitical events drive targeted reconnaissance and compromise.

04 / VULNERABILITIES

N-day flaws in network tools remain a persistent risk.

UNC6619: GLOBAL ESPIONAGE

37

Nations Targeted

70+ ORGANIZATIONS COMPROMISED

Core Capability

Custom **ShadowGuard** Linux rootkit utilizing eBPF technology for stealth.

Target Sectors

Strategic focus on Finance, Law Enforcement, and Critical Infrastructure.

Access Vector

Sophisticated phishing via mega.nz provides initial network access.

DKNIFE: EDGE DEVICE EXPLOITATION

Persistence

Active Since 2019

Long-standing framework targeting Chinese-speaking users via edge device compromise.

Technique

AitM Operations

Hijacks routers to perform Adversary-in-the-Middle attacks and DNS manipulation.

Payload

ShadowPad & DarkNimbus

Deploys sophisticated backdoors through intercepted Android and Windows updates.

SOLARWINDS WHD: ACTIVE EXPLOITATION

Critical Vulnerability

INITIAL ACCESS

Active abuse of **CVE-2025-26399** RCE flaws. Rapid transition from automated access to manual "hands-on-keyboard" activity.

Persistence

TOOL CHAIN

Abuse of legitimate RMM tools like **Zoho Assist** for persistence. Use of Velociraptor and Cloudflared for redundant C2.

Exfiltration

DATA THEFT

Innovative exfiltration via **Elastic Cloud Bulk API**. Hijacking SIEM infrastructure to manage stolen system information.

CRITICAL VULNERABILITY DISCLOSURES

10.0

Critical / Sandbox Escape

SandboxJS

Multiple flaws allowing full host takeover via arbitrary code execution.

9.9

Critical / Pre-Auth RCE

BeyondTrust

High-impact remote code execution vulnerability in core security platform.

9.1

Critical / Security Flaw

FortiClient EMS

Significant vulnerability in endpoint management server infrastructure.

HIGH

ICS / Configuration Risk

Yokogawa FAST/TOOLS

Weak cryptography and configuration issues affecting industrial control systems.

STRATEGIC RECOMMENDATIONS

Patch Urgently

Update SolarWinds Web Help Desk to version 2026.1 or later to remediate critical RCE vulnerabilities.

Isolate Portals

Remove administrative interfaces from direct internet exposure; enforce VPN or Zero Trust access.

Monitor EDR

Configure alerts for unexpected child processes (cmd.exe, msiexec.exe) originating from WHD wrappers.

Audit Edge

Review router and edge device configurations for unauthorized DNS changes or suspicious traffic redirection.