GN5-1 WP8 T3
Security Threat Landscape

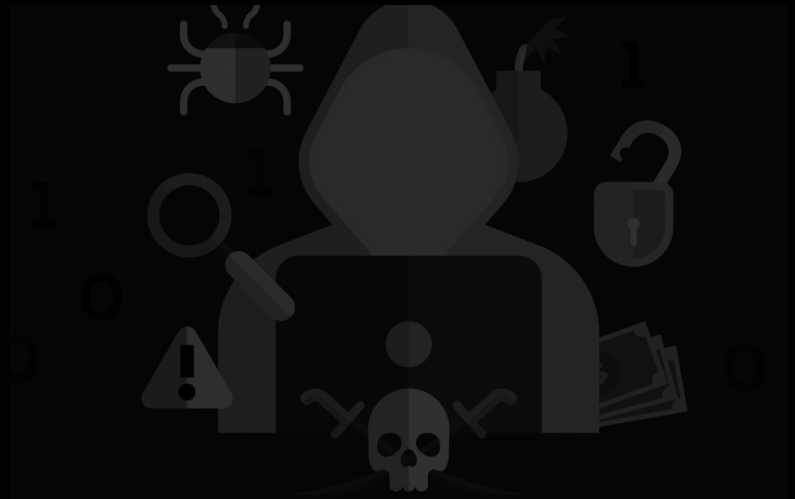
David Heed, Coordinator Sunet security center
GN5-1 WP8 T3 joint-tasklead

Vetenskapsrådet

SUNET

Agenda

- The threat landscape
- Summary of Sunet security center yearbook
- Summary of sector survey of threats and risks
- Summary of Sunet security center activities
- Short updated poll comparison from SIG-ISM Trondheim



Some Sunet Security Center Operational Metrics

- Vulnerability Scans: 100,000 systems scanned monthly, with critical vulnerabilities promptly reported
- Mail Filtering: Over 100 million spam emails blocked annually
- Botnet Surveillance: Monitoring and blocking over 28,000 botnet nodes with the potential to attack connected infrastructure

Key Insights and Emerging Threats

- Evolving Attack Methodologies: Attackers increasingly leverage interactive intrusion techniques, bypassing traditional malware approaches to mimic user behavior, complicating detection efforts
- Targeted Phishing: Phishing attacks have become more sophisticated, with a notable increase in AI-enhanced spear phishing that customizes messages for specific targets, boosting the likelihood of successful breaches
- Software Target Diversity: Attacks now cover a broader range of software, from cloud services to local services, driven by SEO poisoning and social engineering tactics
- AI-Generated Fraud: Attackers use AI to create believable personas and deepfake media, manipulating victims to bypass security protocols.
- Usage of “trusted resources” as Cloud services and storage

Sector-Wide Survey Results (29 responding organisations)

- Top security issues: Spam, phishing, unauthorized access, and malware
- Daily scans and password attacks remain prevalent, with increased attacks on VPNs and email systems
- Rising challenges with user education on risks like USB malware and pirated software downloads.

New and Ongoing Initiatives

- Improved DDoS Resilience: Launch of Sunet CDN to mitigate overloading of local systems
- Enhanced Attack Detection: Future expansion of detection capabilities to meet sector expectations by 2025
- Visualization and Dashboard Upgrades: A more detailed dashboard for data aggregation and client-specific security updates

slido

What threats are relevant to your organisation? (brainstorm with as many as you like)

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

slido

What threats have had an impact on your organisation?

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

slido

How would you like protective DNS service

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

Questions or comments !?