Top Provider Insights – Social Engineering and Edge Appliances

Akria (old Conti) goes after vulnerabilitie in edge services like Cisco and Palo VPN products in August/September. Uses RDP to not draw attention.

Qilin (Agenda) phishing and public facing applications (like FortiGate) and IaaS compromised credentials. Third Party Remote Admin Tools use.

Sinobi is newer Sonic Wall SSL VPNs where reports note many of these services relate to Managed Service Providers to gain network access. Uninstalls and bypasses EDR solutions.

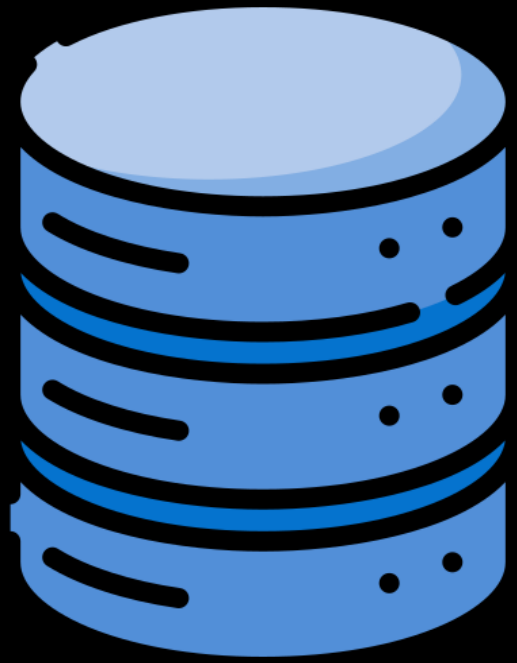
Non RaaS Provider – Social Engineering / AI / DeepFake

ShinyHunters - not a RaaS instead they exfiltrate and wait. Responsible for a lot of high profile breaches, including many of our membership, and is involved in the latest round of Oauth compromises (not the SalesForce breach its self).

Non RaaS Provider – Social Engineering / AI / DeepFake

The massive 'Salesloft Drift' OAuth compromise in September highlighted how the compromise of a single third-party SaaS connector can grant threat actors access to the Salesforce data of numerous large organizations, potentially exposing over a billion records.

Ransomwareless-RaaS – Exfiltration and Extortion with no Encryption



A few new RaaS players with DLS aren't using Ransomware.

CoinbaseCartel new player with no Ransomware & ShinyHunters success has seen an absence of traditional Ransomware.

The Gentlemen: "White Glove" Ransomware

Bespoke Reconnaissance: Conducts deep research map a target's specific security software (AV/EDR) and network layout before the attack.

Bespoke Anti-Security Tooling with emphasis on "Bring Your Own Vulnerable Driver" (BYOVD) Attacks

Tailored Evasion: Develops custom tools designed specifically to bypass the victim's identified security solutions.

Your New IT Contractor – Doesn't report to your Director but to Kim Jong Un

Famous Chollima (DPRK) is successfully placing operators inside companies as legitimate, hired remote IT workers.

Persona: AI-generated headshots, flawless resumes, and keyword-optimized LinkedIn profiles.

Interview: AI-assisted communication and real-time help to pass technical coding challenges.

Payload: AI-aided script and malware development once inside the network.

Crowdstrike "*uses AI at every stage of the attack*"

APT28's AI-Powered Malware "LameHug"

First Live LLM Integration
Qwen 2.5-Coder-32B-Instruct

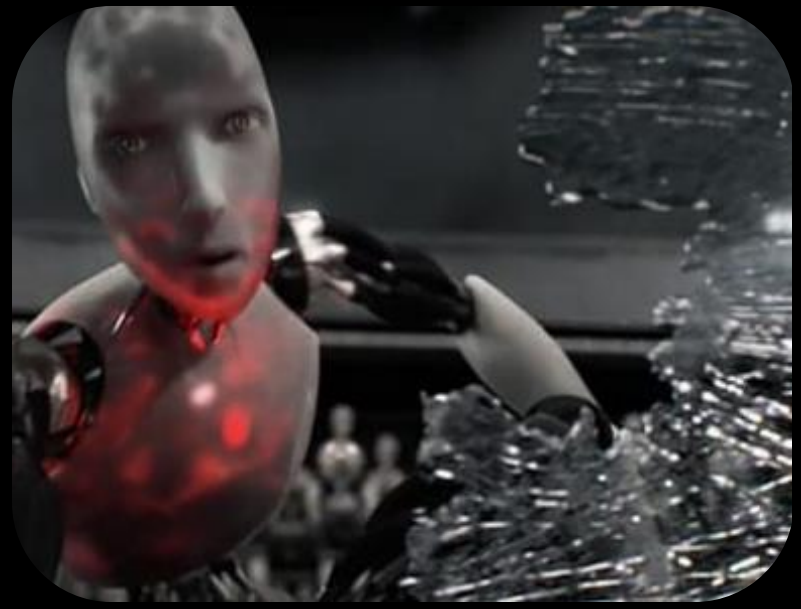
LameHug contains no pre-programmed malicious functions!

July, 2025


FUNKSEC RANSOMWARE
CYBER GROUP

Anthropic Identified Fully-Agentic Attacks After the Fact

Actor targeted 17+ organizations.
Victims included healthcare, emergency services, government, and religious institutions.
Threatened public data exposure instead of traditional ransomware encryption.
Demanded ransoms, some exceeding $500,000.



August, 2025