Cybersecurity in the Age of AI

CYBERTRAP

The Reality of **AI** in Cybersecurity

Stuxnet
Zero Day Exploit

WannaCry
RansomWare

KI
SocialEngineering

DI Dr. René Heinzl

2024 **AI** patent for cybersecurity defense

2022 Austrian Staatspreis for our AI model

2017 Development of own **AI** models

2007 Technology Consulting

The Reality of **AI** in Cybersecurity

Cybersecurity threats are rapidly evolving due to **AI**

Attackers are adopting **AI** to scale, automate, and deceive at levels we've never seen before

Millions of convincing emails are leaving your company's network.

Not because an employee made a mistake,

But because an **AI** has bypassed every security measure.

2024 – The Year of **AI**-Driven Attacks

Examples

AI-Powered
Phishing Campaign

Proofpoint

AI-Automation

Stargazers Ghost
Network

2024 – The Year of **AI**-Driven Attacks

AI-Powered Phishing Campaign

Proofpoint

- AI-Powered Phishing
- Convincing Impersonation
- Massive Scale

2024 – The Year of **AI**-Driven Attacks

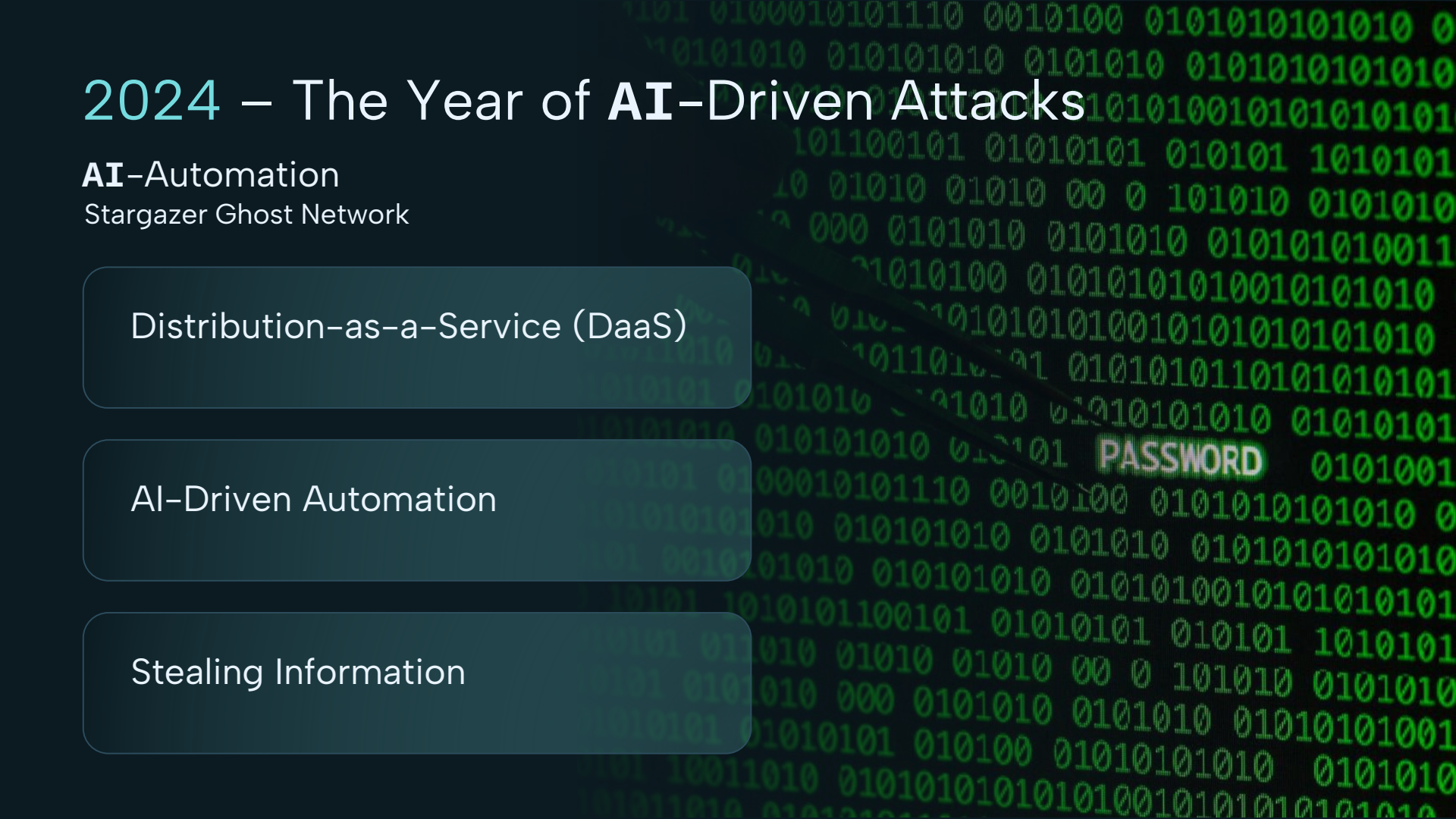
AI-Automation

Stargazer Ghost Network

Distribution-as-a-Service (DaaS)

AI-Driven Automation

Stealing Information



How AI is Transforming Cyberattacks

Speed & Scale

Sophistication

Adaptation

Traditional Cybersecurity vs **AI**-Driven Threats

Traditional Cybersecurity (Static Defenses)	AI-Driven Threats (Adaptive Attacks)
Firewalls rely on predefined rules and signatures	AI-powered attacks adapt in real-time
Fixed and reactive	Dynamic and proactive, constantly evolving
Effective against known threats	Capable of exploiting unknown vulnerabilities
Too slow to respond to rapid changes	Quickly adjusts tactics based on system defenses
Requires human intervention for updates	Automates attack strategies without manual input

Fighting Back with AI – Cybertrap Innovations

Dynamic Traps: Decoys and lures are designed to distract attackers, wasting their time while valuable intelligence is gathered

Skill-Based Response: AI skill module continuously assesses the attacker's abilities and modifies the decoy environment

AI-Powered Adaptation: Our decoy swarm is getting smarter and adjust in real-time, responding to the hacker’s actions and behavior

Our Digital Twin – A Game-Changer

The digital twin **virtualizes** real network assets, but resource-efficient

As hackers attack the twin, our AI **collects** valuable data on their behavior

The twin **evolves** in real-time, feeding attackers false information while protecting the real infrastructure

One Step Ahead – Our AI Strategy

We have **dynamic, AI-driven defenses** that adapt faster than attackers can

Continuous monitoring: The system learns from every attack, becoming stronger over time

The future of cybersecurity relies on **combining human expertise with AI innovation**