

# Ransomware

---

Hochschule für Technik Stuttgart – Aktuelle Themen der IT-Sicherheit

23.01.2026

# Agenda

Entwicklung & Geschichte

Aktuelle Bedrohungslage

Ziele & Motivation

Arten von Ransomware

Case Study: Edu-Ransomware Architektur

Die Phasen eines Angriffs

Gegenmaßnahmen

Forschung & Ausblick

Fazit

## Aktuelle Bedrohungslage

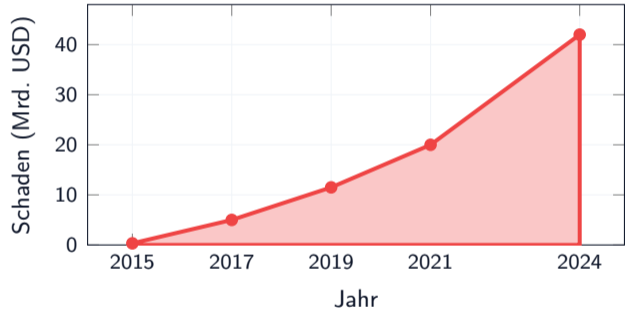
---

## Geschätzte Weltweite Schäden

2017: 5 Mrd. USD

2024: 42 Mrd. USD

**+740%** Anstieg in 7 Jahren

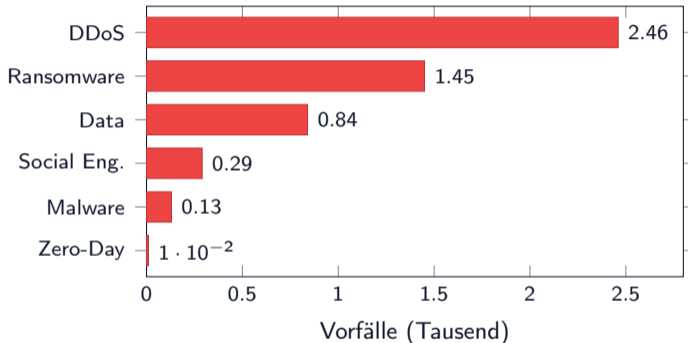


# ENISA Threat Landscape 2024

## Top-Bedrohungen EU:

1. DDoS/RDoS (46,31%)
2. Ransomware (27,33%)
3. Data Breaches (15,87%)
4. Social Engineering (5,37%)
5. Malware (2,45%)
6. Zero-Day (0,11%)

**Ransomware: Zweitgrößte  
Bedrohung**



# Ziele & Motivation

---

## Warum diese Ziele?

### **Finanzielle Motive**

Zahlungsbereitschaft bei kritischen Systemen

### **Kritische Infrastrukturen**

Hoher Druck durch Ausfallkosten

### **Sensible Daten**

Erpressungspotenzial durch Datenleaks

### **Geopolitische Faktoren**

Destabilisierung und Spionage

**Zunehmende Professionalisierung und Organisation**

**Ransomware-as-a-Service (RaaS)** ist eine hochprofessionelle Schattenwirtschaft mit Milliardenumsätzen:

## 1. Access Provider

Spezialisten, die Zugänge zu Netzwerken potenzieller Opfer verkaufen.

## 2. RaaS Provider

Entwickler der Malware. Bieten C2-Infrastruktur und Support gegen Provision.

## 3. Affiliates

Kaufen Zugänge, mieten Malware und führen den Angriff durch.

Die Qualität der Services übertrifft teilweise legale SaaS-Anbieter.

## Beispiel: LockBit 3.0 Bug-Bounty

LockBit hat ein eigenes Prämienprogramm für Hinweise zur Verbesserung ihrer Schadsoftware aufgelegt:

*"Locker Bugs: Any errors during encryption ... that lead to corrupted files or to the possibility of decrypting files without getting a decryptor."*

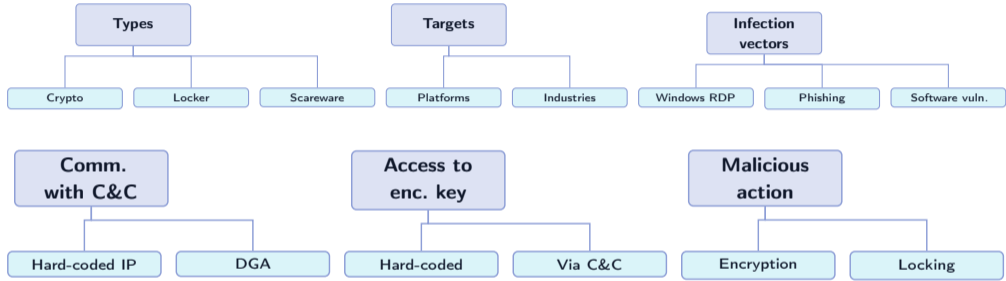
## Wirtschaftliches Risiko

Im Gegensatz zu Banken ("Too big to fail") gilt für Ransomware-Gruppen: **"Too big to prevail"**. Wer zu groß wird, zieht zu viel Aufmerksamkeit der Strafverfolger auf sich.

# Arten von Ransomware

---

# Ransomware Taxonomy



## Projekt-Einblick: Edu-Ransomware

Unsere Ransomware ist eine klassische **Crypto-Ransomware** mit **Double Extortion**.

## 1. Crypto-Ransomware

- Verschlüsselt Benutzerdateien
- Verwendet AES, RSA
- System bleibt funktional
- Wiederherstellung oft unmöglich

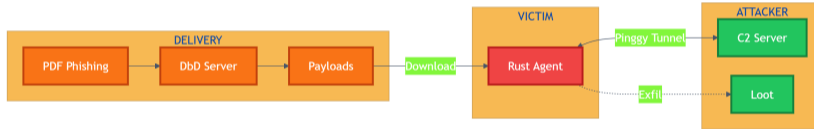
## 2. Locker-Ransomware

- Sperrt Systemzugriff
- Bildschirmsperre
- Keine Datenverschlüsselung
- Einfacher zu beheben

## Case Study: Edu-Ransomware

---

# Projektübersicht



# Technische Architektur

---

# Systemarchitektur & Technologie-Stack

## *Modulare Client-Server-Architektur (Reverse TCP Shell)*

### **Agent (Client)** **Rust**

- **Deployment:** Statische Binary (Windows .exe, Linux .deb)
- **Core-Komponenten:**
  - `main.rs` – Initialisierung, Daemonisierung
  - `evasion.rs` – Ressourcen- & Zeitmanipulationsprüfung
  - `crypto.rs` – AES-256-CTR, atomare Dateioperationen
  - `network.rs` – Raw TCP, Retry-Logik, Protokollparser
  - `extortion.rs` – UI-Manipulation (Wallpaper, Browser)

### **C2-Server (Control)** **Python**

- Multithreaded TCP-Server
- Sitzungsverwaltung paralleler Clients
- Datenaufnahme (Base64-Streams → loot/)
- Interaktive CLI

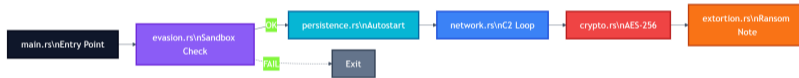
### **Delivery Infrastructure Bash / Python**

- User-Agent-basierte Payload-Auslieferung
- Automatisierter Build- & Konfigurationsprozess

## Die Phasen eines Angriffs

---

# Attack Kill Chain – Übersicht



**Theorie:** Phishing (E-Mail Anhänge, Links), Drive-by-Downloads

## Live Demo: Initial Access Szenario

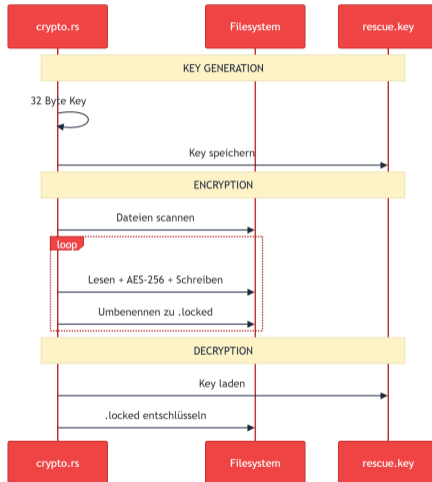
**Szenario:** Mitarbeiter erhält E-Mail mit "Rechnung\_Dez.pdf"

- **Köder:** PDF enthält unscharfes Bild einer Rechnung
- **Trick:** Button "Inhalt entschlüsseln" (Social Engineering)
- **Ergebnis:** Smart-Server liefert Malware aus

# Phase 1: Drive-by-Download Ablauf



# Phase 1: PDF Phishing Technik



**Theorie:** Ransomware installiert sich, prüft auf Sandboxes, etabliert Persistenz.

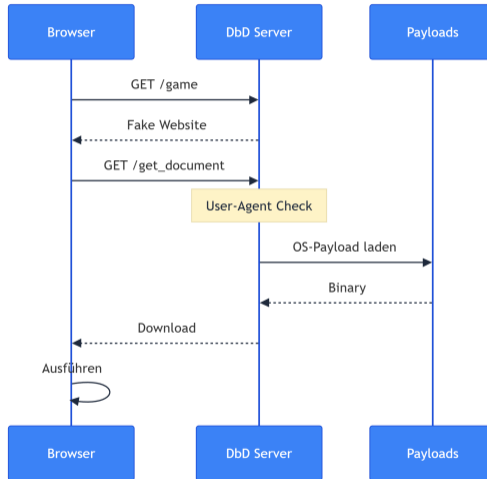
### Projekt-Einblick: Evasion Module

Der Agent prüft beim Start:

- Ist RAM < 3GB?
- Sind weniger als 2 CPU-Kerne verfügbar?
- Sind weniger als 60gb Festplattenspeicher verfügbar?

Falls ja: **Sofortiger Abbruch** mit gefälschter Fehlermeldung.

## Phase 2: Agent Architektur



**Theorie:** Aufbau der Kommunikation, Nachladen von Befehlen, Datendiebstahl.

### Live Demo: Attacker Control

Wir wechseln zum Angreifer-Terminal (C2):

- `[+] New Victim Connected: ID 1`
- Angreifer nutzt `shell`-Befehle zur Erkundung
- **Double Extortion:** `exfil secret.pdf` stiehlt Daten

## Phase 3: C2 Kommunikation



## Phase 4: Encryption (Impact)

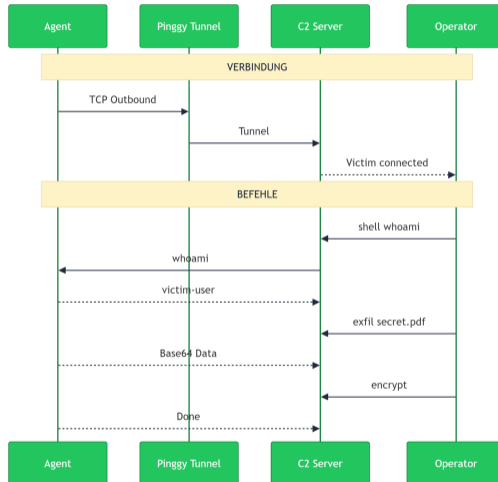
**Theorie:** Starke Verschlüsselung, Löschung von Backups.

### Live Demo: The Panic Mode

Angreifer sendet `encrypt`. Auswirkungen auf Opfer-PC:

- Dateien erhalten Endung `.locked`
- Browser öffnet Lösegeldforderung (Stress)
- Log-File zeigt Verschlüsselung in Echtzeit

## Phase 4: Verschlüsselungsprozess



## Phase 5: Decryption (Recovery)

**Szenario:** Das Lösegeld wurde gezahlt (in der Simulation).

- Angreifer sendet Befehl `decrypt`
- Agent nutzt symmetrischen Key (AES-CTR)
- `.locked` Dateien verschwinden, Originale sind wieder da

# Gegenmaßnahmen

---

## Technische Maßnahmen:

### Backups

3-2-1-Regel: 3 Kopien, 2 Medien, 1 Offsite

### EDR / Antivirus

Verhaltensanalyse in Echtzeit

### Projekt-Reflektion: Warum Evasion?

Herkömmliche AV-Systeme scannen oft statisch. Unsere Ransomware umgeht dies durch:

- Dynamisches Nachladen (keine Signatur beim PDF-Download)
- Sandbox-Checks (verhindert Cloud-Analyse)
- Nutzung von Rust (schwerer zu analysieren)

## Detektionsansätze:

- **Statische Analyse:** Ohne Ausführung
- **Dynamische Analyse:** Sandbox
- **Machine Learning:** Unbekannte Varianten
- **Netzwerk:** Anomalie-Erkennung

## Wichtige Merkmale:

- API-Aufrufe und Systemverhalten
- Datei-/Verzeichnisaktivitäten
- Netzwerkverkehrsmuster
- Verschlüsselungsoperationen

## Sofortmaßnahmen bei Verdacht:

1. **Isolation** betroffener Systeme
2. Identifikation des Ransomware-Stamms
3. Bewertung der Schadenausbreitung
4. Benachrichtigung relevanter Stellen

## Wiederherstellung:

- Aus Backups (wenn möglich)
- Key-Escrow-Mechanismen
- Forensische Analyse
- Systemhärtung vor Neustart

**Keine Lösegeldzahlung** (keine Garantie, finanziert weitere Angriffe)

## Fazit

---

## Erkenntnisse aus der Projektentwicklung:

### Komplexität

Als Anfänger von Null funktionsfähige Malware entwickelt – erschreckend niedrige Einstiegshürde.

### KI-Unterstützung

Entwicklung mit KI-Tools beschleunigt den Prozess erheblich.

### AV-Evasion

Malware-Scanner schlägt nicht an – Agent bleibt unerkannt.

### Fazit

Unser Ziel war es herauszufinden, wie komplex die Implementierung funktionsfähiger Ransomware für Einsteiger ist. Das Ergebnis: **Mit modernen Tools und KI-Unterstützung ist die Hürde erschreckend niedrig.** Selbst gängige AV-Lösungen erkennen unseren Agent nicht.

# Zukünftige Herausforderungen

## Technologische Entwicklungen:

- **KI in Ransomware:** Adaptives Verhalten
- **Quantencomputing:** Bedrohung für Verschlüsselung
- **IoT-Ransomware:** Neue Angriffsflächen
- **Cloud-native:** Angriffe auf Cloud-Infra

## Forschungsbedarf:

- Echtzeit-Schutz, Zero-Day-Erkennung
- Post-Quantum-Kryptographie
- Automatisierte Incident Response
- Internationale Strafverfolgung

- [1] IT-Security Vorlesung, Prof. Dr. Matthias Hamann, WS24/25.
- [2] *The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions* (Razulla et al.)
- [3] ENISA (2024): *Threat Landscape Report 2024*
- [4] *Edu-Ransomware Repository* (GitHub, 2026) – Eigene Entwicklung
- [5] Morato, D.; Berrueta, E.; Magaña, E.; Izal, M.: *Ransomware early detection by the analysis of file sharing traffic.*
- [6] Oz, H.; Aris, A.; Levi, A.; Uluagac, A. S.: *A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions.*