

Ransomware

Anatomie, Netzwerkerkennung und Zero-Loss Recovery

Ihr Name

Ihre Institution

5. Januar 2026

Agenda

Entwicklung & Geschichte
Aktuelle Bedrohungslage
Ziele & Motivation
Arten von Ransomware

Case Study: Edu-Ransomware Architektur
Die Phasen eines Angriffs
Gegenmaßnahmen
Forschung & Ausblick

Entwicklung & Geschichte

Historischer Abriss

Meilensteine:

- **1989:** AIDS Trojan – erster dokumentierter Ransomware-Angriff
- **2005:** Wiederaufleben durch Internet und Kryptowährungen
- **2017:** WannaCry-Ausbruch mit globaler Aufmerksamkeit



Abbildung 1: Entwicklung von Ransomware

Aktuelle Bedrohungslage

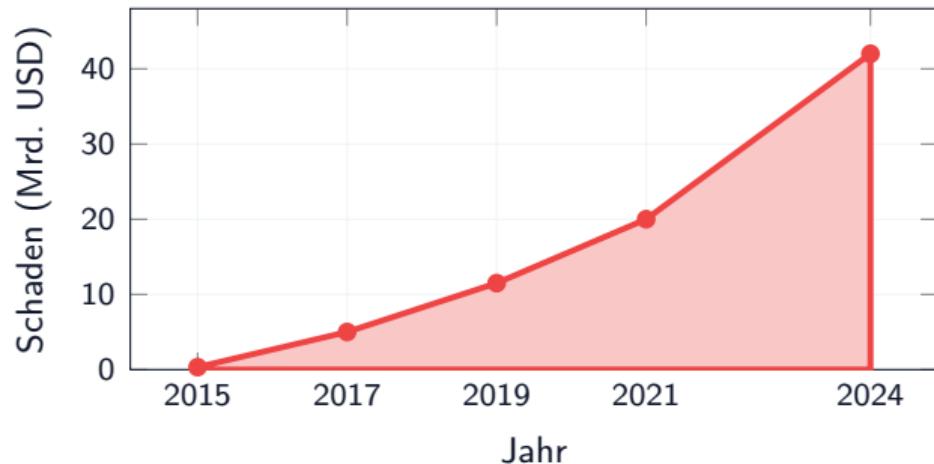
Finanzielle Auswirkungen

Geschätzte Weltweite Schäden

2017: 5 Mrd. USD

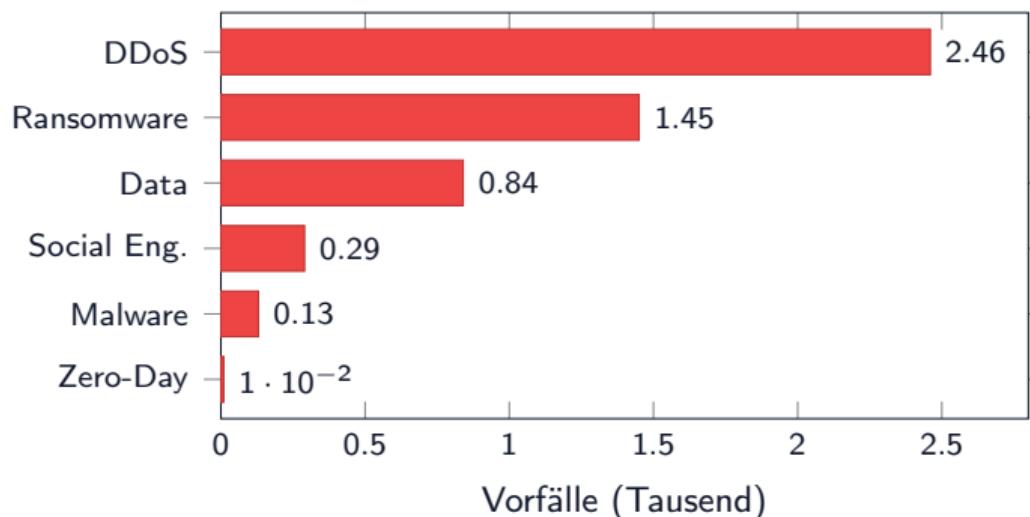
2024: 42 Mrd. USD

+740% Anstieg in 7 Jahren



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

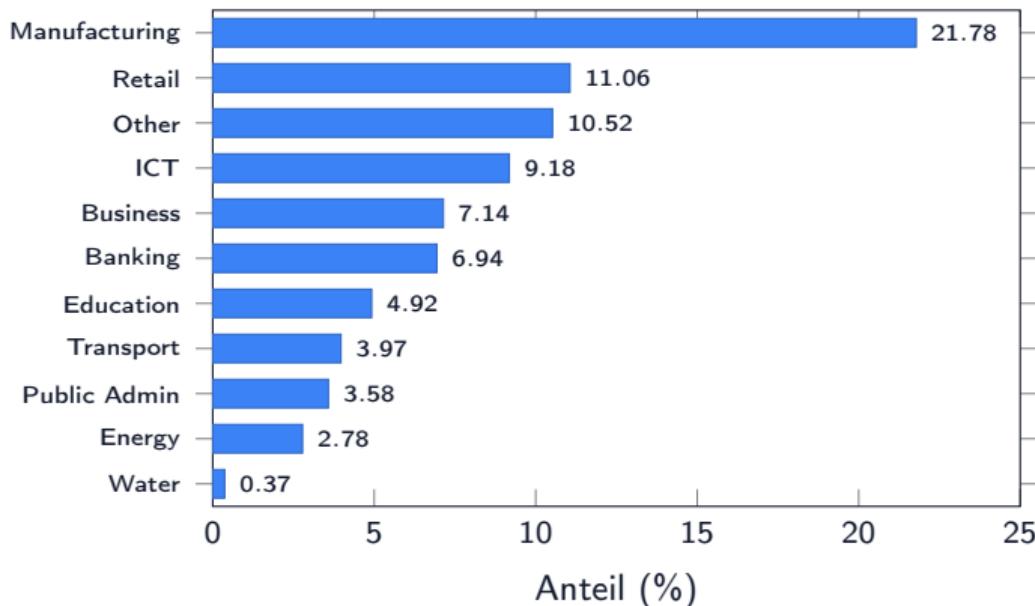
Ziele & Motivation

Am häufigsten betroffene Sektoren

Top 5 Sektoren:

1. Manufacturing (21,78%)
2. Retail (11,06%)
3. ICT Services (9,18%)
4. Business Services (7,14%)
5. Banking/Finance (6,94%)

Industrie und Fertigung am stärksten betroffen



Motivation der Angreifer

Warum diese Ziele?

Finanzielle Motive

Zahlungsbereitschaft bei kritischen Systemen

Sensible Daten

Erpressungspotenzial durch Datenleaks

Kritische Infrastrukturen

Hoher Druck durch Ausfallkosten

Geopolitische Faktoren

Destabilisierung und Spionage

Zunehmende Professionalisierung und Organisation

Warum die Bedrohung bleibt: Die Ökonomie

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.

Professionalisierungsgrad: Beispiel LockBit

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:

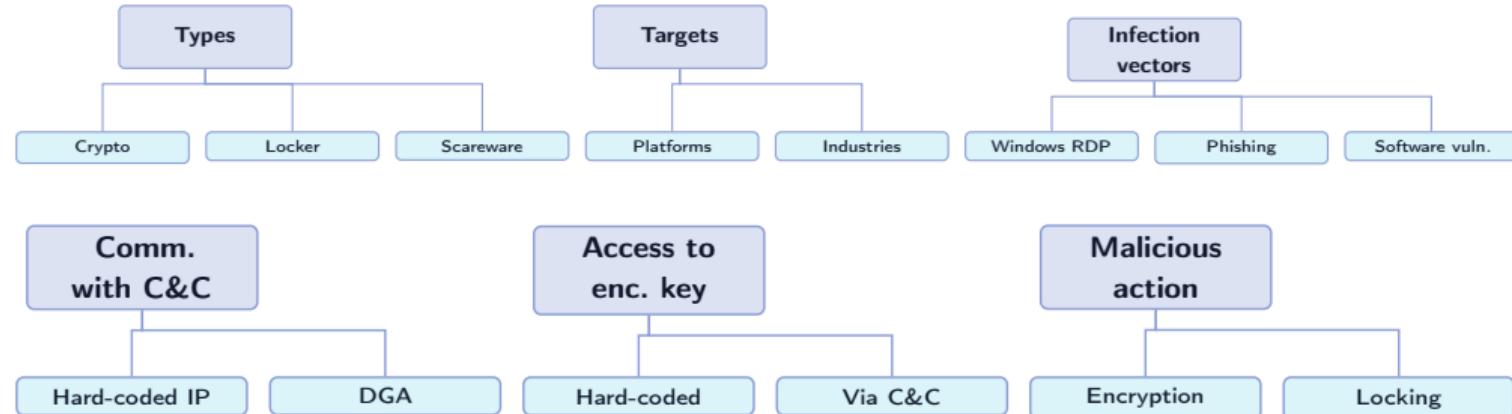
"Locker Bugs: Any errors during encryption ... that lead to corrupted files or to the possibility of decrypting files without getting a decryptor."

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**.

Grundlegende Typen

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 Architektur

Technische Übersicht

Um die Theorie besser verständlich zu machen, haben wir eine Simulation entwickelt.

Komponente A: Agent (Victim)

- Sprache: **Rust** (High Performance)
- Cross-Platform (Win/Linux/macOS)
- AES-256, Sandbox-Evasion, Persistenz

Komponente B: C2-Server (Attacker)

- Sprache: **Python**
- Multi-Threaded TCP Server
- Steuerung, Exfiltration, Key-Mgmt

Modulare Architektur (Agent)

Der Rust-Agent bildet die Kill-Chain durch spezialisierte Module ab:

1. Defense Evasion ([evasion.rs](#))

- Sandbox-Erkennung: RAM <3GB, CPU <2
- Reaktion: Sofortiger Prozessabbruch

2. C2 Channel ([network.rs](#))

- Protokoll: TCP-Loop mit Retry
- Commands: shell, exfil, encrypt

3. Impact Engine ([crypto.rs](#))

- Algorithmus: AES-256-CTR
- Atomic Operations mit [.locked](#)

4. Extortion Logic ([extortion.rs](#))

- User Notification
- Browser-Loop alle 5s

Intelligente Verteilung

- Python-basierter Webserver
- Erkennt OS via User-Agent
- Liefert passendes Binary

Infektionsvektoren

- Phishing PDF: Verschwommene Rechnung
- Drive-by-Download: Fake-Webseiten

Die Phasen eines Angriffs

Phase 1: Distribution & Infection

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 2: Execution & Evasion

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?

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

Phase 3: C2 & Exfiltration

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 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 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)

Forschung & Ausblick

Fokusgebiete:

- 72,8% der Studien: Detektion
- Machine Learning dominiert
- Hohe Genauigkeit bei unbekannten Varianten

- Monitoring von SMB-Protokoll
- Erkennung von Verhaltensmustern
- 99% Erkennung bei <10 Dateien

Weitere Ansätze: Near-Zero-Loss durch Traffic-Wiederherstellung, Moving Target Defense

Funktionsweise:

- Analyse des Netzwerk-Traffics
- Erkennung anomaler Zugriffsmuster
- Aufzeichnung der Dateiinhalte
- Automatische Alarmierung

Vorteile:

- Früherkennung (99% bei <10 Dateien)
- Wiederherstellung ohne Backups
- Minimaler Datenverlust

Fazit

Zusammenfassung

Takeaways aus der Simulation:

Automatisierung

Angriffe sind hochgradig automatisiert (Delivery Server).

Social Engineering

Oft effektiver als technische Exploits.

Double Extortion

Nicht nur Verschlüsselung, auch Datendiebstahl.

Prävention und Awareness sind der beste Schutz.

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, Matthias Hammann, 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