Ransomware

Anatomie, Netzwerkerkennung und Zero-Loss Recovery

Ihr Name

Ihre Institution

2. Januar 2026

Agenda

Entwicklung & Geschichte

Aktuelle Bedrohungslage

Ziele & Motivation

Arten von Ransomware

Case Study: Edu-Ransomware Architektur

Die Phasen eines Angriffs

Gegenmaßnahmen

Forschung & Ausblick

Fazit

Entwicklung & Geschichte

Historischer Abriss

Meilensteine:

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

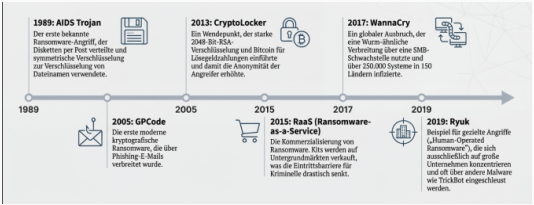


Abbildung 1: Entwicklung von Ransomware über die Jahre

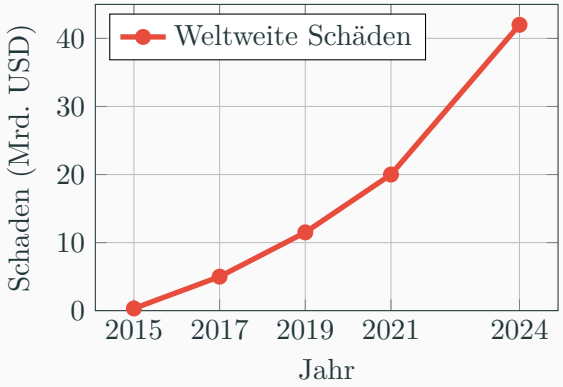
Abbildung 2: Entwicklung von Ransomware über die Jahre

Aktuelle Bedrohungslage

Finanzielle Auswirkungen

Geschätzte Weltweite Schäden

- 2017: 5 Mrd. USD
- 2024: 42 Mrd. USD

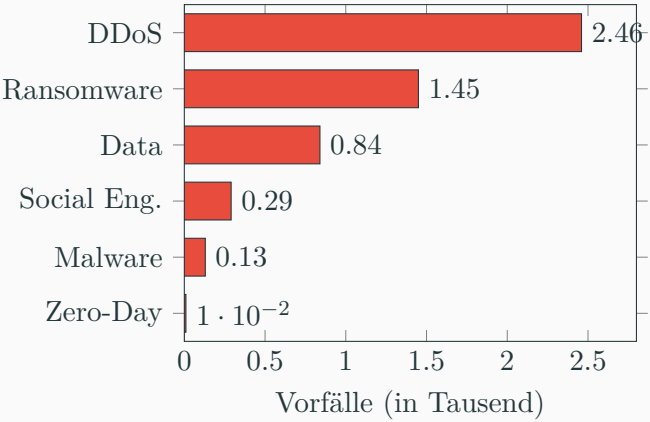


ENISA Threat Landscape 2024: Prime Threats

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



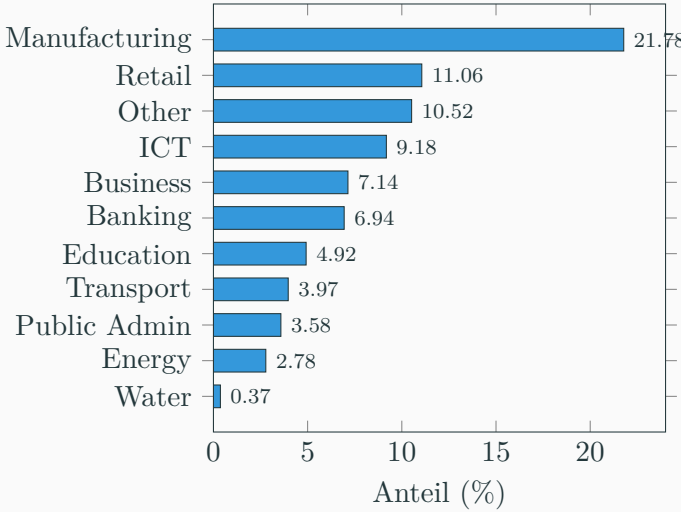
Ziele & Motivation

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

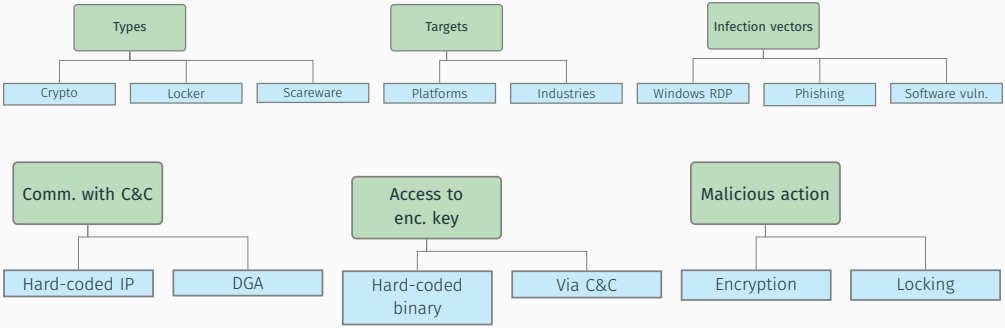
Warum diese Ziele?

- Finanzielle Motive: Zahlungsbereitschaft bei kritischen Systemen
- Kritische Infrastrukturen: Hoher Druck durch Ausfallkosten
- Sensible Daten: Erpressungspotenzial durch Datenleaks
- Geopolitische Faktoren: Destabilisierung und Spionage

Zunehmende Professionalisierung und Organisation

Arten von Ransomware

Ransomware Taxonomy



Projekt-Einblick: Edu-Ransomware

Unsere entwickelte Ransomware ist eine klassische Crypto-Ransomware mit Elementen der Double Extortion (Datenexfiltration vor Verschlüsselung).

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 Theroie besser verständlich zu machen, haben wir eine Simulation enwickelt.

Komponente A: Agent (Victim)

- Sprache: Rust (High Performance, Memory Safety)
- Cross-Platform (Windows/Linux/macOS)
- Features: AES-256 Verschlüsselung, Sandbox-Evasion, Persistenz

Komponente B: C2-Server (Attacker)

- Sprache: Python
- Multi-Threaded TCP Server
- Steuerung, Exfiltration (Data Theft), Key-Management

Modulare Architektur (Agent)

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

1. Defense Evasion (**`evasion.rs`**)
   - Sandbox-Erkennung: Prüft RAM (<3GB) und CPU-Cores (<2).
   - Reaktion: Sofortiger Prozessabbruch zur Tarnung vor Analysten.

2. C2 Channel (**`network.rs`**)
   - Protokoll: TCP-Loop mit Retry-Logik.
   - Commands: Parsing von `shell`, `exfil`, `encrypt`.

3. Impact Engine (**`crypto.rs`**)
   - Algorithmus: AES-256-CTR (Stream Cipher).
   - Atomic Operations: Rename zu `.locked` verhindert Datenverlust bei Absturz.

4. Extortion Logic (**`extortion.rs`**)
   - User Notification: Ersetzt "Panic Mode".
   - Mechanismus: Browser-Loop öffnet Lösegeldforderung alle 5s (Psychologischer Druck).

Delivery Infrastruktur

Intelligente Verteilung:

- Python-basierter Webserver als Delivery-Point.
- Smart Endpoint: Erkennt Betriebssystem des Opfers via User-Agent Header.
- Liefert automatisch passendes Binary (‘.exe‘ für Windows, Elf für Linux).

Infektionsvektoren:

- Phishing PDF: Verschwommene Rechnung mit Fake-Sicherheitshinweis.
- Drive-by-Download: Fake-Webseiten (Gaming, Gewinnspiel, Sicherheitswarnung).

Die Phasen eines Angriffs

Phase 1: Distribution & Infection

Theorie:

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

Live Demo: Initial Access Szenario

Szenario: Ein Mitarbeiter erhält eine E-Mail mit dem Anhang "Rechnung_Dez.pdf".

- **Der Köder:** Das PDF enthält ein unscharfes Bild, das wie eine echte Rechnung aussieht.
- **Der Trick:** Ein Button Ïnhalt entschlüsselnßuggeriert ein technisches Problem (Social Engineering).
- **Das Ergebnis:** Beim Klick liefert der Smart-Server die Malware aus und infiziert das System.

Theorie: Ransomware installiert sich, prüft auf Sandboxes und 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, um Analysten zu täuschen.

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 (‘ls‘, ‘ps‘).
- **Double Extortion:** Befehl `exfil secret.pdf` stiehlt Daten vor der Verschlüsselung.

Theorie: Starke Verschlüsselung, Löschung von Backups.

Live Demo: The Panic Mode

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

- Dateien erhalten Endung `.locked`.
- **Visuell:** Browser öffnet die Lösegeldforderung (Stress-Erzeugung).
- Log-File zeigt Verschlüsselungsprozess in Echtzeit.

Phase 5: Decryption (Recovery)

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

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

Gegenmaßnahmen

Prävention & Detektion

Technische Maßnahmen:

- Backups: 3-2-1-Regel
- EDR / Antivirus: Verhaltensanalyse

Projekt-Reflektion: Warum Evasion?

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

- Dynamisches Nachladen (keine Signatur beim Download des PDF).
- Sandbox-Checks (verhindert Analyse in der Cloud).
- Nutzung seltener Sprachen (Rust binaries sind oft schwerer zu analysieren als C++).

Detektion und Reaktion

Detektionsansätze:

- Statische Analyse: Untersuchung ohne Ausführung
- Dynamische Analyse: Verhaltensbeobachtung in Sandbox
- Machine Learning: Erkennung unbekannter Varianten
- Netzwerkbasierte Detektion: Anomalie-Erkennung im Traffic

Wichtige Merkmale:

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

Incident Response

Sofortmaßnahmen bei Verdacht:

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

Wiederherstellung:

- Wiederherstellung aus Backups (wenn möglich)
- Key-Escrow-Mechanismen
- Forensische Analyse
- Systemhärtung vor Wiederinbetriebnahme

Zahlungsempfehlung: Keine Lösegeldzahlung (keine Garantie, finanziert weitere Angriffe)

Forschung & Ausblick

Aktuelle Forschungslandschaft

Fokusgebiete:

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

Innovative Ansätze:

- REDFISH: Netzwerkbasierte Früherkennung
  - Monitoring von SMB-Protokoll
  - Erkennung von Verhaltensmustern (schnelles Lesen/Schreiben/Löschen)
  - 99% Erkennung vor Verlust von 10 Dateien
- Near-Zero-Loss-Szenario durch Traffic-Wiederherstellung
- Moving Target Defense (MTD)

Zero-Loss Recovery: REDFISH

Funktionsweise:

- Analyse des Netzwerk-Traffics zu Freigaben
- 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:

- Angriffe sind heute hochgradig automatisiert (Delivery Server).
- Social Engineering (PDF) ist oft effektiver als technische Exploits.
- Ransomware ist nicht nur Verschlüsselung, sondern auch Datendiebstahl.

Prävention und Awareness sind der beste Schutz.

Zukünftige Herausforderungen

Technologische Entwicklungen:

- KI in Ransomware: Adaptives, intelligentes Verhalten
- Quantencomputing: Bedrohung für aktuelle Verschlüsselung
- IoT-Ransomware: Neue Angriffsflächen
- Cloud-native Ransomware: Angriffe auf Cloud-Infrastrukturen

Forschungsbedarf:

- Echtzeit-Schutz und Zero-Day-Erkennung
- Post-Quantum-Kryptographie
- Automatisierte Incident Response
- Internationale Zusammenarbeit bei Strafverfolgung

Quellen

- The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions (Razulla et al.)
- ENISA (2024): Threat Landscape Report 2024
- Edu-Ransomware Repository (GitHub, 2026) - Eigene Entwicklung