SLAC 2024

heinlein

Schon gehackt oder wissen wir es nur nicht?

Quiz

Hans Jansen

liblzma Backdoor

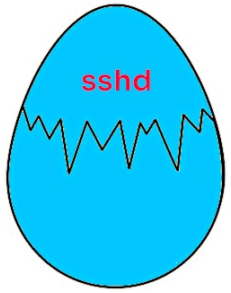
CVE-2024-3094

```
✗ good-large_compressed.lzma
```

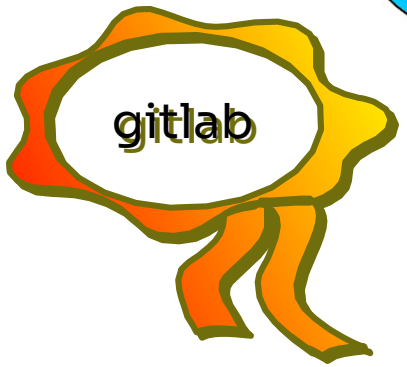
```
before:
real    0m0.299s
user    0m0.202s
sys     0m0.006s

after:
real    0m0.807s
user    0m0.202s
sys     0m0.006s
```

```
diff:
+ gl_path_map='tr "\t \-_" " \t_\-"'
```



Dennis Ens



Lempel-Ziv-Markow-Algorithmus

Quiz - Auflösung

https://research.swtch.com/xz-timeline

Agenda

- Die Lage
- Was bedeutet überhaupt „gehackt“?
- Was wird gehackt?
- Wer sind die Opfer?
- Wie wird angegriffen?
- Beispiel

Die Lage

BSI - Die Lage der IT-Sicherheit in Deutschland 2023

- “Ransomware ist und bleibt die größte Bedrohung“

ENISA – Foresight Cybersecurity Threats for 2030 (Top 5, März 2024)

- Supply Chain Compromise of Software Dependencies
- Skill Shortage
- Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems
- Exploitation of Unpatched and Out-of-date Systems …
- Rise of Digital Surveillance Authoritarianism / Loss of Privacy

Quelle BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html
Quelle ENISA: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary

Was bedeutet überhaupt „gehackt“? 1/2

Formal

- Jemand (Hacker) verschafft sich unbefugt Zugang zu IT-Systemen, verändert oder löscht Daten, zerstört IT-Systeme

Juristisch

- §202a STGB (Ausspähen von Daten),
- §202b STGB (Abfangen von Daten),
- §202c STGB (Vorbereiten des Ausspähens und Abfangens von Daten),
- §303a STGB (Datenveränderung),
- §303b STGB (Computersabotage)

Was bedeutet überhaupt „gehackt“? 2/2

Eine (mögliche) Realität

- Geschäftsprozesse funktionieren nicht mehr
- Kein Zugriff auf die eigenen Anwendungen
- Das Netzwerk „spinnt“, alles ist langsam
- Wir werden zur Malware Schleuder
- Es gibt keine brauchbare Dokumentation
- Die Presse steht vor der Tür und will Antworten
- Die Kunden wollen Antworten
- Die Aufsichtsbehörden wollen Antworten
- Vertrauensverlust
- Alle sind gestresst
- Gefühl von Hilfslosigkeit

Was wird gehackt?

ALLES!

- Webseiten
- IT-Netzwerke und -Systeme
- Lieferketten
- Techn. Produkte
- Prozesse
- Software
- Fahrzeuge & Fluggeräte
- Hacker (-Tools)

Wer sind die Opfer?

Beispiele

- 2021, Accenture: Ransomware; 6TB Daten gestohlen, aus Backups wiederhergestellt
- 2022, Unfallkasse Thüringen: Ransomware; alles verschlüsselt
- 2022, Continental: Erpressung; 7,5GB Daten im Darknet
- 2022, Viasat: APT; Brute Force, Supply Chain, Remote Control
- 2023, Südwestfalen-IT: Ransomware; Zero-Day Lücke, Rechteausweitung
- 2023, Microsoft: Cloud; Rechteausweitung
- 2023, Motel One: Datenabfluss; 6GB Daten im Darknet
- 2023, Ipswitch: MOVEit-Hack; Zero-Day Lücke
- 2024, DENA: Ransomware
- 2024, Bezirkskliniken Mittelfranken: Ransomware; Datenabfluss
- 2024, PSI: Ransomware
- 2024, xz-utils: APT; Social Engineering, Supply Chain, Backdoor (RCE)

Wie wird angegriffen? 1/2

Ransomware

- digitale Erpressung, Ziel ist die Lösegeldzahlung

Malware

- Kurzform von „malicious software“ → schädliche Software
  - Untergruppen „fileless malware“ & „Malware as a service“

Phishing

- Kunstwort aus Password und Fishing, gehört in die Kategorie „Social Engineering“
- Gezielte Aktionen → Spearphishing

Cross Side Scripting

- Kurz „XSS“, Schadcode in vertrauswürdigen Webseiten
- reflection, persistant, DOM

Wie wird angegriffen? 2/2

DoS- und DDoS Angriffe

- Verfügbarkeit von Diensten einschränken,
  - gezielt, reflektiert oder politisch motiviert

SQL-Injection

- Ausnutzen einer Sicherheitslücke zum Einschleusen von SQL Befehlen

Brute Force

- Durchprobieren von Passwörtern

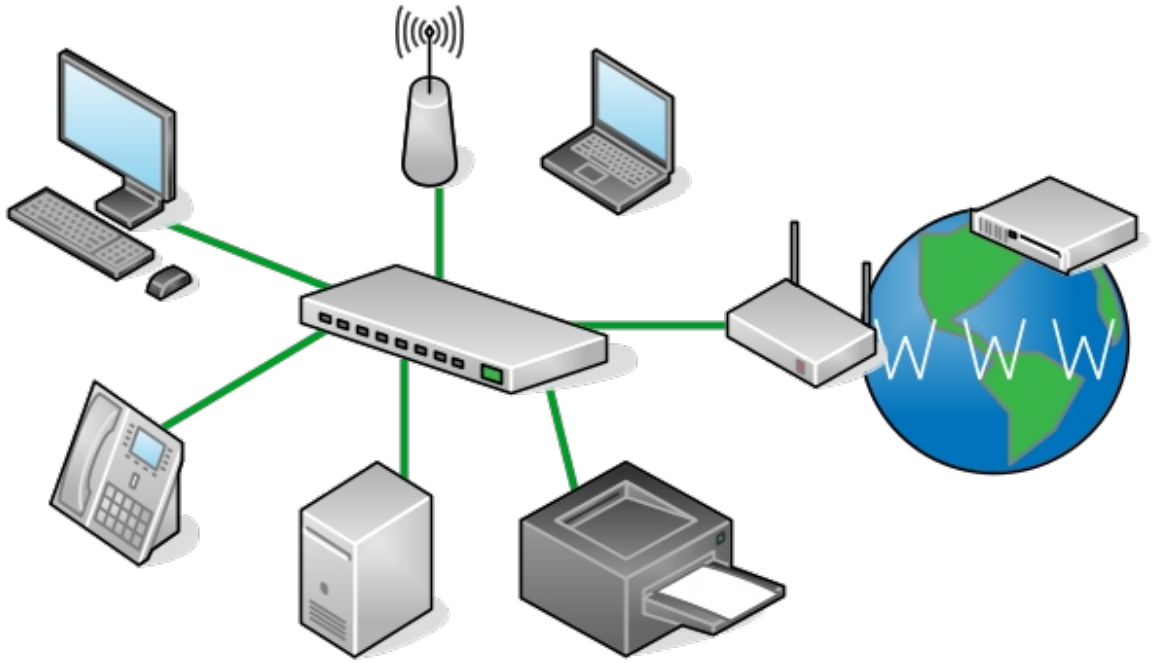
Advanced Persistent Threat

- Zielgerichteter komplexer Angriff auf ein „wertvolles“ Ziel

Beispiel: Ransomware Angriff 1/5

Die Ausgangslage

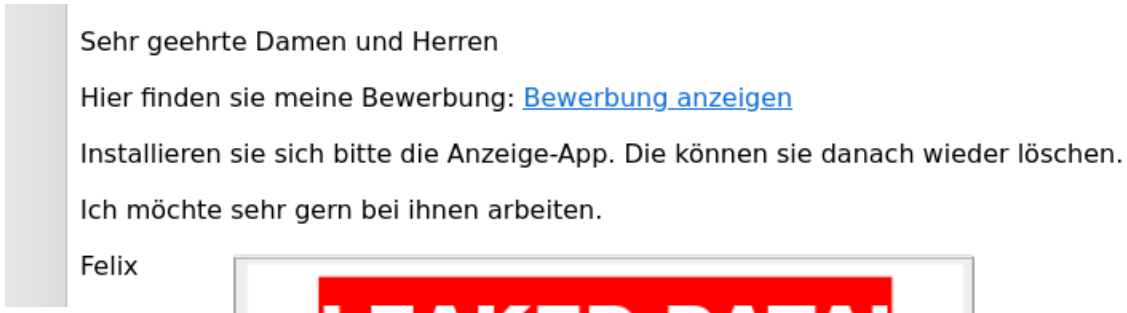
- Kleine Institution
- Ein externer Mail Server
- Ein interner „All-in-One“ Server
- 20 Arbeitsplätze (PCs & Notebooks)
- LAN (VLAN 1)
- WLAN (2x AP, PSK, VLAN 1)
- Multifunktionsdrucker, IP-Telefonie
- DSL-Anschluss mit Firewall
- Kostenfreie AV SW auf den Clients
- „Jede(r) darf Alles“-Berechtigung



Beispiel: Ransomware Angriff 2/5

Der (mögliche) Ablauf

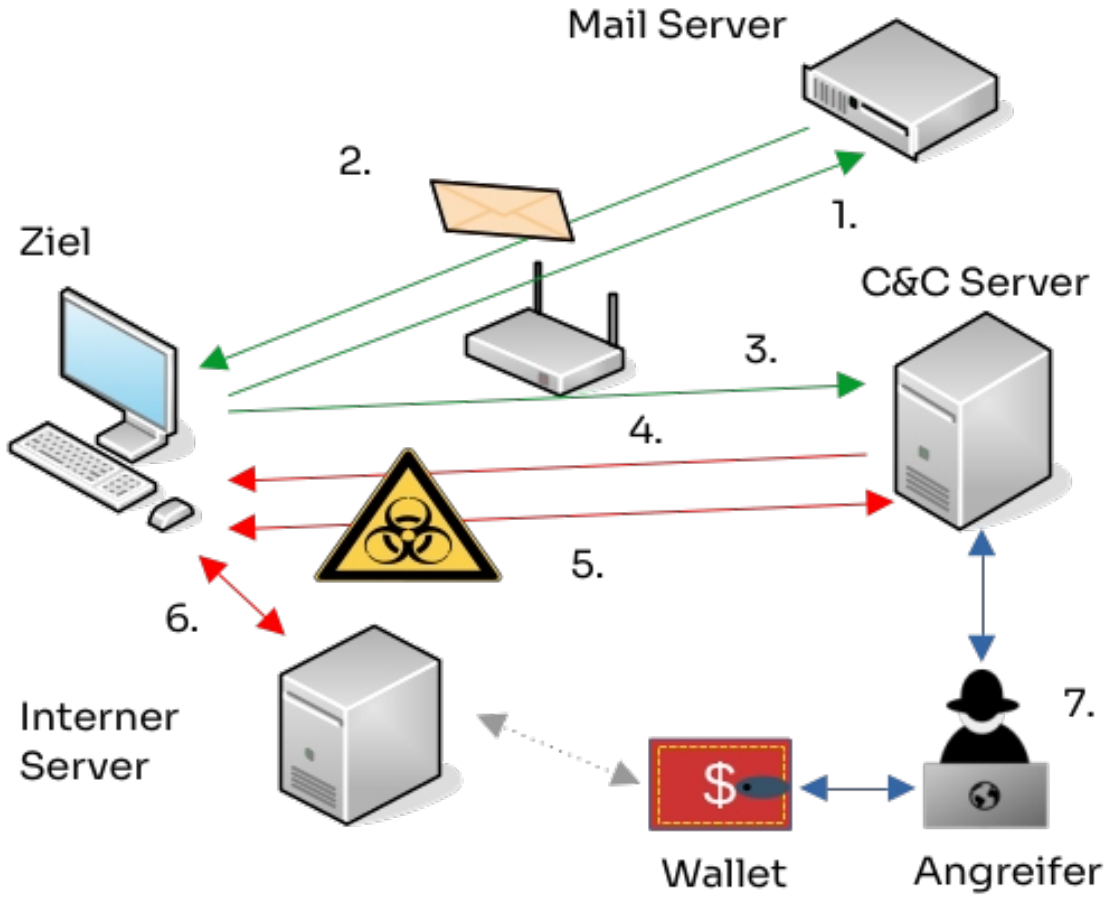
1. Empfang einer „Bewerbungs-Mail“
2. HTML-E-Mail mit einem Link zu „fileshare.me“
3. Es wird eine App zum Anzeigen angeboten
4. App wird installiert und ausgeführt
5. Verbindung zu einem C2-Server wird aufgebaut
6. Die eigentliche Schadsoftware wird nachgeladen
7. Daten des internen Servers werden kopiert
8. Alle Daten hinter Freigaben werden verschlüsselt
9. Backups auf der USB-Festplatte werden verschlüsselt
10. Eine Lösegeldforderung wird platziert



Beispiel: Ransomware Angriff 3/5

Der (mögliche) Ablauf

1. Verbindung zum Mail-Server
2. E-Mail abholen
3. Aufruf von „fileshare.me“
4. Download und Installation der „App“
5. Daten- u. Steuerungskanal C&C Server
6. Zugriff auf internen Server (Freigaben)
7. Kontrolle des C&C-Servers durch Angreifer



Beispiel: Ransomware Angriff 4/5

Was lief hier falsch?

- Es geht eine mutmaßliche Bewerbung auf eine vakante Stelle ein
  → Bewerber bittet um Installation einer App zum Anzeigen der Bewerbung und die
  → App wird installiert

- Alle Mitarbeitenden besitzen Admin-Rechte
  → Der Zugriff auf Daten in Freigaben erfolgt mit den Besitzrechten des Users
  → Installation, Konfiguration u. Deinstallation jeglicher Software ist möglich

- Unzureichende technische Voraussetzungen
  → Uneingeschränkte Rechte
  → Alles ist „ein Netz“
  → Firewall-Schutz unzureichend („Any-Any-Permit“ Regel)
  → Schutzfunktionen in der kostenfreien AV Software zu gering

Beispiel: Ransomware Angriff 5/5

Wie geht es besser?

- Kontrolle behalten!
  → Für das Beispiel hier: Bewerbungsportal bereitstellen (lassen)
- Rechte so vergeben, wie sie zur Aufgabenerfüllung notwendig sind
- Netz in Segmente trennen (Bspw: Clients, Server, Telefonie, WLAN-Gäste)
- Offline-Backups anlegen
- Unterschiedliche Passwörter und Passwort-Manager verwenden
- Sinnvolle Firewall-Regeln für Outgoing-Traffic setzen, Letzte Regel: Blockieren
- Internen DNS-Service mit Reputations-Check für IP Adressen und Domains einrichten
- Ereignisse zentral Protokollieren (Logging) und automatisiert Auswerten
- Klare Prozesse definieren, dokumentieren und vermitteln
- Notfallplan erarbeiten: Was wäre wenn ?
- **IT-Sicherheit ist nicht nur eine Sache der IT-Leute !**

Bleiben wir im Kontakt

Torsten Lange

Tel. +49 30 40 50 51-37
t.lange@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de