Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Real World Threat Intelligence

Tobias Balschun
Tec Lead Cyber Defense Services, balschun@avantec.ch

Agenda

AVANTEC
Competence. Security. Trust.

1. Einleitung
2. Identity Intelligence
3. 3rd Party Risk
4. Vulnerability Intelligence
5. Q&A

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Identity Intelligence

AVANTEC
Competence. Security. Trust.

Fragestellung:

- Gibt es kompromittierte Accounts von Mitarbeitern oder Kunden?

Woher kommen die Daten:

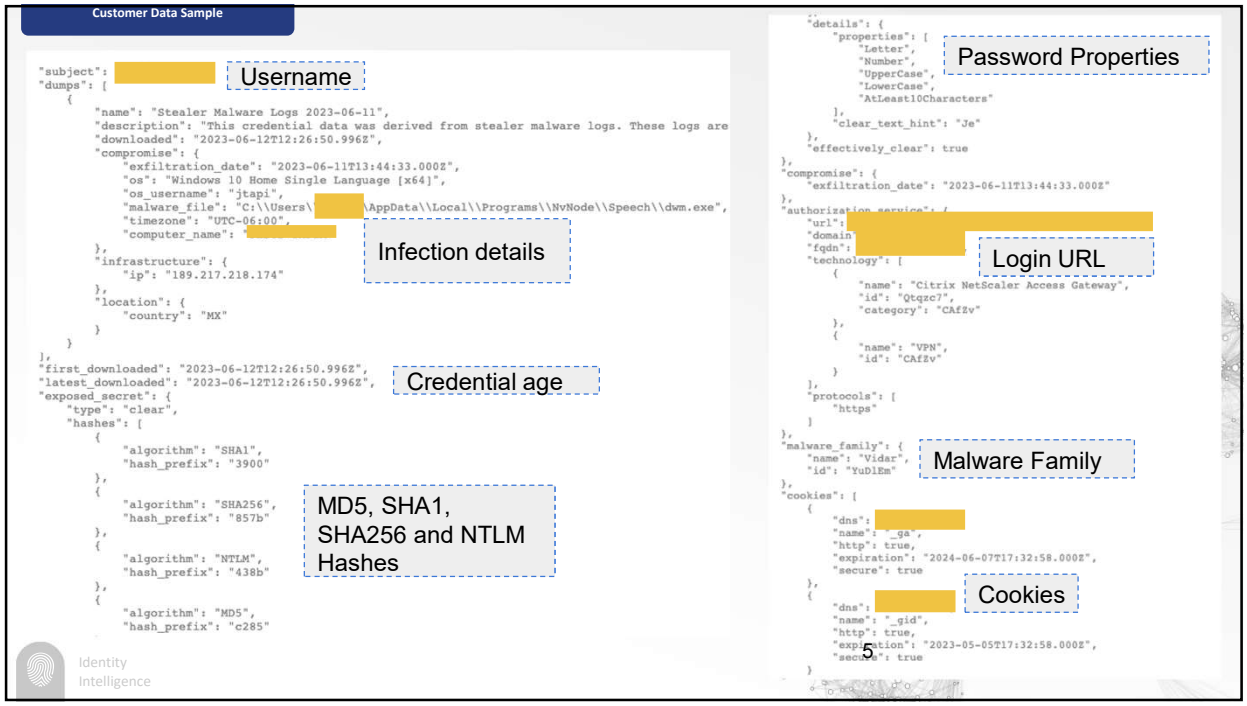
- Hacker-Foren
- Darkweb-Foren
- Malware Stealer Logs
- etc.

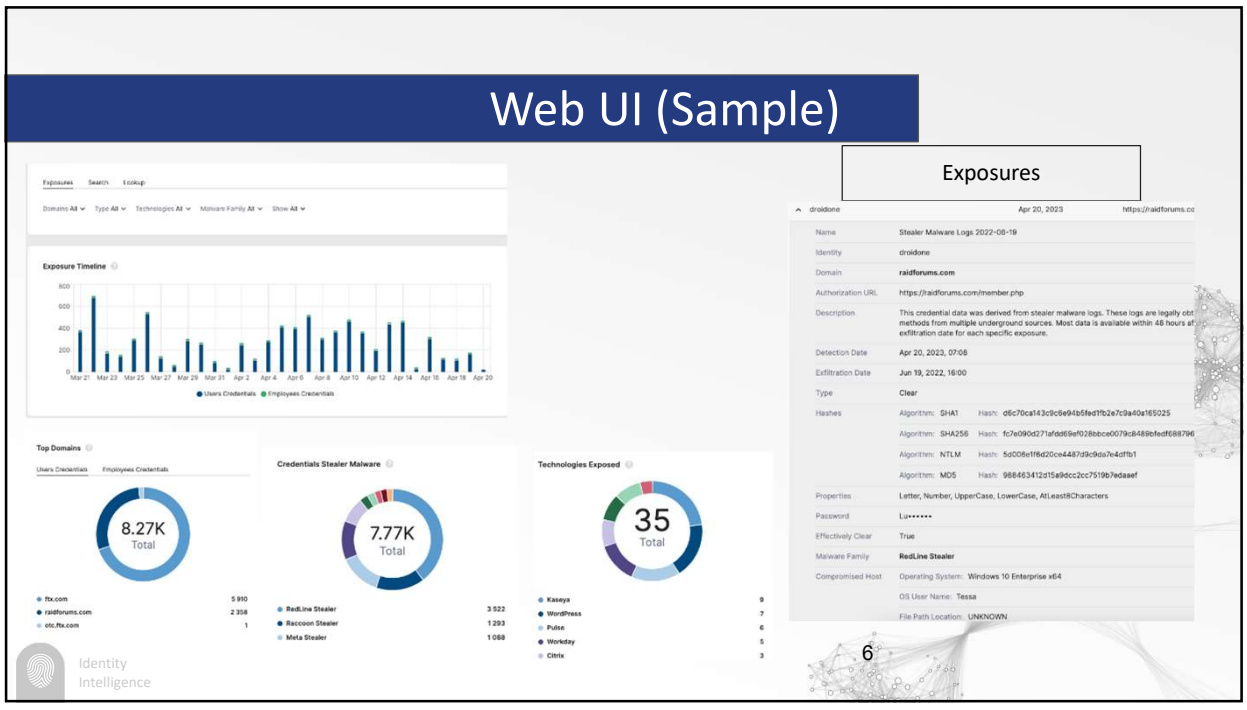
→ Sample Reports verfügbar am Round-Table

Customer Data Sample

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023





AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

3rd Party Risk

- Monitoring von Lieferanten u/o Partner-Unternehmen
  - Früh-Erkennung von Breaches oder anderen Security-Issues
  - Hat das einen Impact auf mein Unternehmen? Müssen Massnahmen eingeleitet werden?
    - VPN Tunnel oder andere Kommunikations-Wege schliessen?
    - Supply-Chain überprüfen?
- Auswahl-Kriterium für zukünftige Partner/Lieferanten?

→ Demo

Vulnerability Intelligence

- Fragestellung
  - Welche Schwachstellen soll ich priorisiert behandeln?
    - PoC Code
    - Threat Actors
    - Erfolgreiche Breaches
  - Gibt es Argumente für eine Down-Time?
  - Gibt es evtl. unbekannte Schwachstellen (noch keine CVE)
- Risiko basierter Ansatz
- Alerts gemäss definierten Watchlists

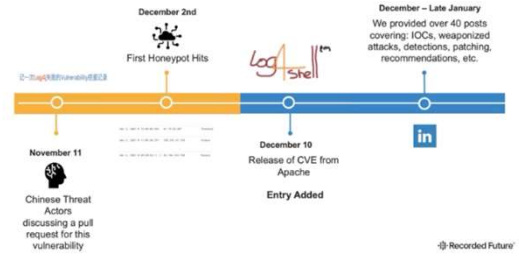
AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

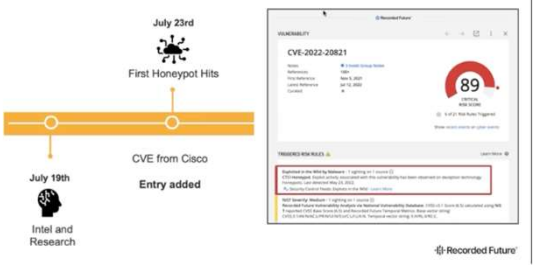
Vulnerability Intelligence

AVANTEC
Competence. Security. Trust.

Log4Shell (CVE-2021-44228)



Cisco IOS XR Software (CVE-2022-20821)



AVANTEC
Competence. Security. Trust.