Ruwac
Industriesauger

INHALT

- Kurzbericht - Axel Runge
- Technische Darstellung des Angriffs – André Sobotta
- Änderungen an der IT und den Prozessen – André Sobotta
- Darknet – André Sobotta
- Änderungen an der IT und den Prozessen – André Sobotta
- Praxistipps zur Prävention

Kurzbericht

- Keine Frage ob, sondern nur wann!
- Ein Fall für den Therapeuten?
- Kann man das eigentlich im Vorfeld organisieren?
- Definitiv ein Geschäftsführer / Gesellschafter Thema
- Können Lösegelder steuerlich geltend gemacht werden?
- Zusammenarbeit mit einer kriminellen Vereinigung?
- Wo steckt das Risiko wirklich?
  - Hardware, Software und Mensch!

Technische Darstellung des Angriffs

IST-Zustand am 10.09.2021 – ca. 06:00 Uhr

- Keine Anmeldung an den Servern mehr möglich
  - keine Telefonie, keine E-Mails, keine Warenwirtschaft, kein Passwortserver etc.
- Linux (VMware-Umgebung) betroffen
- Gesamte Backup-Infrastrukur formatiert und auf Werkseinstellungen zurückgesetzt
- = Szenario: **abgebrannt**

Ruwac Industriesauger

Technische Darstellung des Angriffs

Erste Schritte:

- Das Netzwerk vom Internet getrennt
- Polizei, Datenschutz und BSI informiert und Vorfall gemeldet
- Kontakt mit den Erpressern über das Darknet aufgenommen
- Planung eines IT-Notfallbetriebs
  - Kommunikation: Telefonie, E-Mail
  - Daten: Warenwirtschaft, Anwendungen, Dateiserver

Ruwac Industriesauger

Technische Darstellung des Angriffs

Daten:

- Sicherungskonzept 5 Jahre alt
- Datenstand auf den ext. Backup-Zielen (1-Woche + fehlende Server)
- = **Wir müssen entschlüsseln!**
- Notbetrieb nach 5 Werktagen
- Keine Klarheit zum Angriff

Ruwac Industriesauger

Änderungen an der IT und den Prozessen

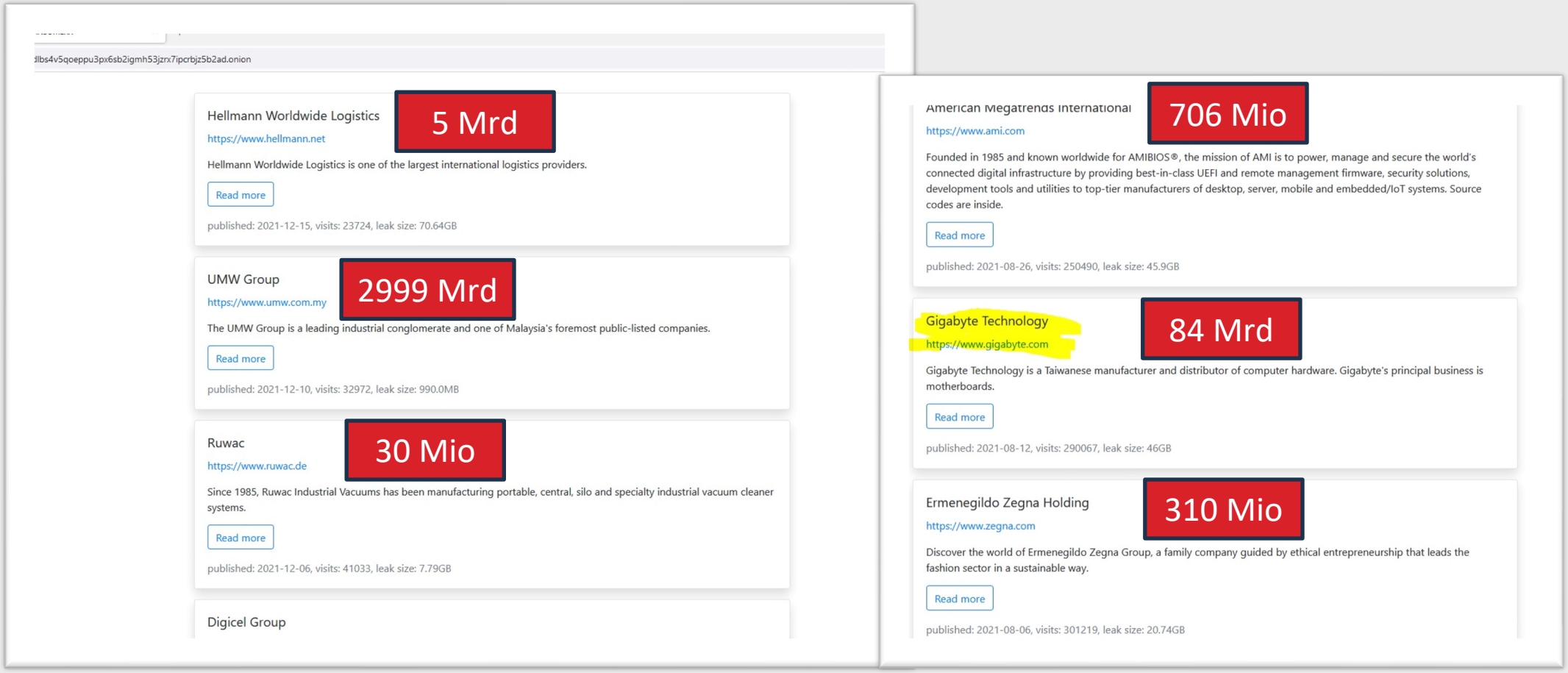
Ruwac Industriesauger

Ergebnis = 2. Angriff

am 01.12.2021

Ruwac Industriesauger

Darknet



Ruwac Industriesauger

Darknet

Ruwac

Offsite, Facebook, LinkedIn, Instagram

[FILELIST]

[Part 1 of 16] [500.0MB] [MD5: d9af201e556ebdff3fdff25c4d8cdacc]
[Part 2 of 16] [500.0MB] [MD5: 7bc491cba125789da0c892fa9bff1e0e]
[Part 3 of 16] [500.0MB] [MD5: d020db8f80945b32ecaba2e216045a3e]
[Part 4 of 16] [500.0MB] [MD5: 8614bade6bcafd10f11a5752163762d8]
[Part 5 of 16] [500.0MB] [MD5: 0d1371514965efdba4cb347441a93ccf]
[Part 6 of 16] [500.0MB] [MD5: dbfadb06acbe1c7e6f69eaab5345e74b]
[Part 7 of 16] [500.0MB] [MD5: 12c44c747f522138653909bea0a4e9e4]
[Part 8 of 16] [500.0MB] [MD5: b9faa9b292d390a9378823d5783f01d2]
[Part 9 of 16] [500.0MB] [MD5: 3218134850b71be15464a1e357983624]
[Part 10 of 16] [500.0MB] [MD5: 947c906d309183b11aa9614de0ad4478]
[Part 11 of 16] [500.0MB] [MD5: 19d8c859152545aca8f11fe23bbe43fa]
[Part 12 of 16] [500.0MB] [MD5: d8618de195c8a0c3e5f3d58ff2c1dbff]
[Part 13 of 16] [500.0MB] [MD5: 74966bb8962dd2c255ce83a35539edc2]
[Part 14 of 16] [500.0MB] [MD5: 596e9944c01cc5faaae304fedf360398]
[Part 15 of 16] [500.0MB] [MD5: a883b9d61d636cdbe86578785cb13c98]
[Part 16 of 16] [473.0MB] [MD5: 61988e4a7f46da1114150d81a56abaa3]

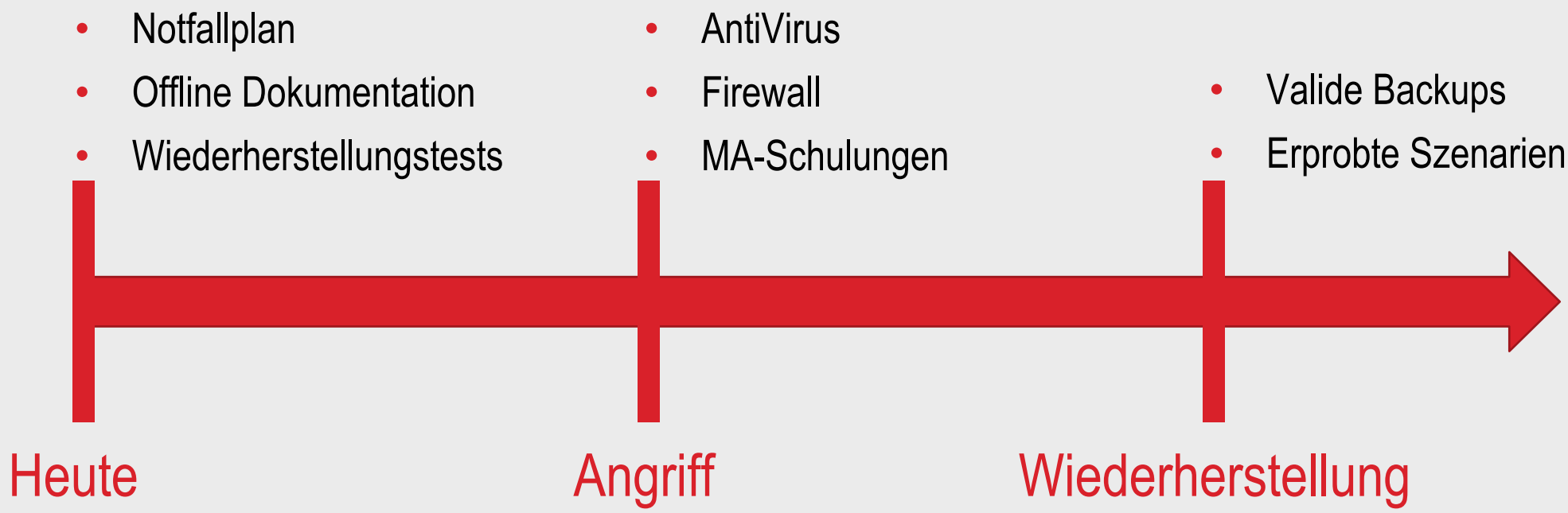
Total leak size: **7.79GB**
Password: **Vm14a2QxVXlVbGhVYWxwU1lteEtUMVJXWkc5WFp3**

Ruwac Industriesauger

Änderungen an der IT und den Prozessen

Ruwac Industriesauger

Praxistipps zur Prävention



Ruwac Industriesauger

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Ruwac Industriesauger