Lagebild IT-Security

Jürgen Schmidt aka ju

ju@heisec.de

Mein Ziel heute

„Kenne deinen Feind“

Sun Tzu by Midjourney

Was haben die gemeinsam?

- ATU
- NZZ
- Bitmarck
- Landkreis Ludwigsburg
- Rheinmetall
- Evotec
- Maxim
- Lürssen
- Stadtwerke Karlsruhe
- ...

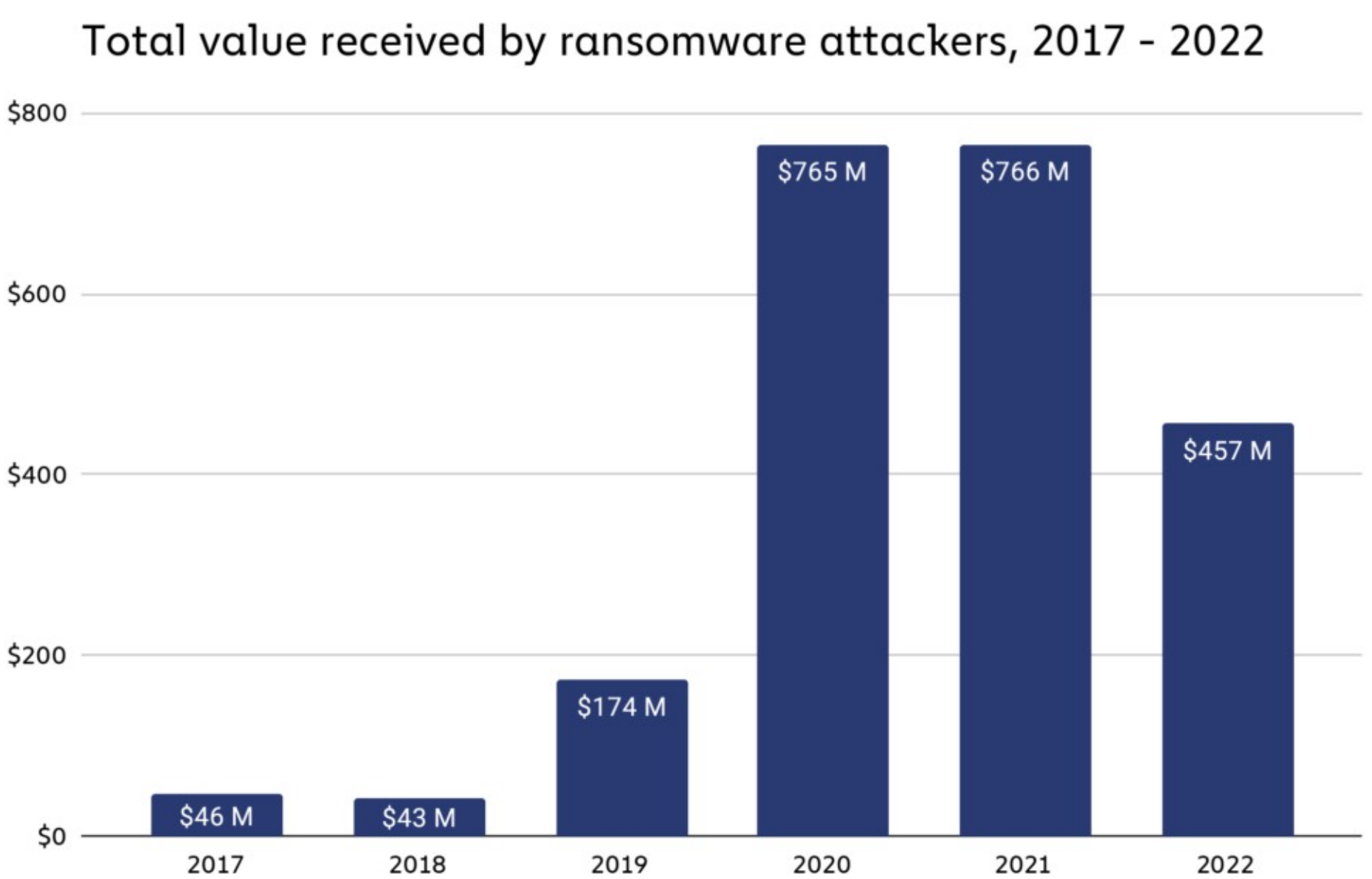
Computersysteme lahmgelegt

Cyberangriffe auf ATU-Kette und Medienportale

19.05.2023 16:04 Uhr

Die Werkstattkette ATU meldet Probleme infolge von Angriffen auf die IT-Infrastruktur. Die Polizei ermittelt. Auch bei Medienportalen gibt es Ausfälle nach Hackerangriffen.

Erpressung – Ransomware



Quelle: Chainanalysis

Die Entwicklung der letzten Jahre

- 2020 + 21 waren Rekordjahre in jeder Hinsicht
- 2022: Verwerfungen durch den Russlands Krieg
- Sinkende Zahlungsbereitschaft / Sanktionen
- Einige große Player sind verschwunden (Conti, REvil, DarkSide, Trickbot), neue schießen aus dem Boden: BlackCat, Basta, Play, Nokoyawa usw.
- 2023 → konsolidiert und „back on track“

Die Mechanik eines Angriffs

Mehrere Stufen –
mit zum Teil unterschiedlichen Akteuren

Initial Access: Einfallstore

- E-Mail → Phishing + Mal-Spam
- Sicherheitslücken in exponierten Diensten
- Eingekaufte Zugänge (Initial Access Broker)
- Neue Mal-Spam-Tricks: OneNote, ISOs, ...
- Vermehrt: Mitarbeiter-PCs im Homeoffice
- Ebenfalls: durch die Hintertür – Lieferketten-Angriffe
- Neu: Angriffe auf 2FA

Ausbreiten und Erobern

„Die Jagd auf den Domänen-Admin“

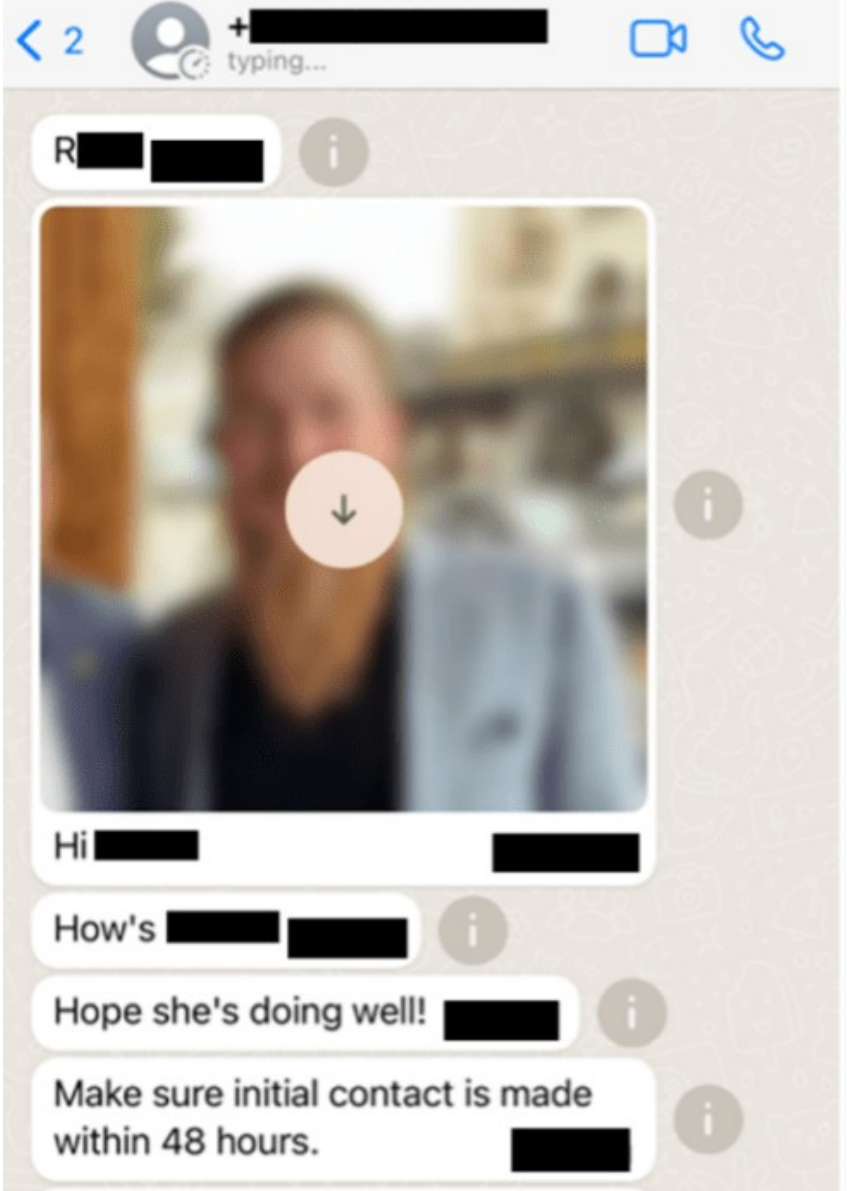
- Rechteausweitung / Privilege Escalation
- Pass the Hash, NTLM Relay, Kerberoasting
- Schwächen im AD → Lateral Movement
- Vermehrt: Einsatz von LOLbins
- Trend: Alternativen zu Cobalt Strike wie Sliver & Anydesk

Impact

- Daten kopieren / exfiltrieren
- Backups löschen oder unbrauchbar machen
- Daten verschlüsselt
- IT lahmgelegt → Lösegeldforderung

Mehrfach-Erpressung

1. Verschlüsselt –> Daten weg, Infrastruktur lahmgelegt
2. Daten kopiert –> Drohung mit Veröffentlichung
3. DDoS-Angriffe –> noch mehr Druck in Verhandlungen
4. Daten genutzt –> Anrufe, Mails an Kunden, Partner



Quelle: Dragos

Die treibende Kraft

Das Cybercrime-Ökosystem

Industrialisierung von Cybercrime

Created by MidJourney

Initial Access Broker (IAB)

QBot

Emotet

IceBot

- Install as a Service
- VPN/RDP- Zugänge
- Credentials

Vermischtes

- DDoS
- Detection Scans
- Exploits / 0days
- ...

Ransomware as a Service (RaaS)

LockBit

Cl0p

Qilin

BlackCat

Alles „As A Service“

- Ransomware as a Service
  - Verschlüsselungs-Software
  - Verhandlungen / „Customer Support“
  - Geldübergabe / -wäsche
  - Tutorials, Workshops usw
- Initial Access Broker
- Phishing, DDoS, Malware, Voice Cloning, ...


Created by MidJourney

Die Akteure

- Dienstanbieter
  - Anschein regulärer „Firmen“
  - Management, Angestellte, HR, 9-5 Jobs, bezahlter Urlaub
  - Code of Conduct

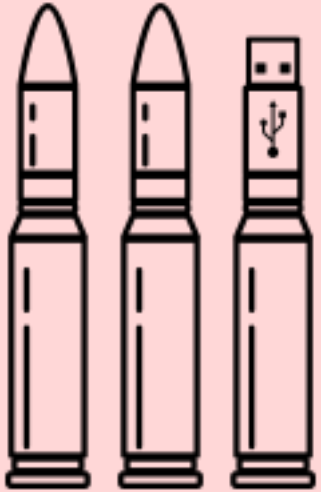
- Angreifer → Affiliates
  - Individuen < ------- > professionelle Teams
  - Einfache Ziele < ------- > Big Game Hunting

RaaS – die Dynamik

- Konkurrenz zwischen den Anbietern
- Affiliates wechseln ihren Anbieter
- Krypto auf hohem Niveau: ECC(Curve25519), AES/ChaCha20
- Einsatz von Rust: BlackCat, Hive, Nokoyawa, …
- Cloud und VMware(ESXi) als Ziele
- N- und 0-Day-Exploits

Cybercrime

Advanced Persistent Threats (APT)



Cybercrime hat aufgeholt

- ✔ Gezielte Angriffe
- ✔ Lateral Movement
- ✔ Hands on Keyboard, LOLbins
- ✔ Kernel-Rootkits, Zero Days, ...
- ✔ Lieferketten-Angriffe

Prognosen zu Cybercrime

- Industrialisierung geht weiter
- Cloud kommt noch stärker in den Fokus
- Einsatz von generativer KI ist ein „Nobrainer“
- Mehr Austausch bzw Zusammenarbeit zwischen Cybercrime und staatlichen Akteuren

APT – aktuelle Entwicklungen

- Russische Aktivitäten dominiert durch den Krieg in der Ukraine
- China: vor allem Spionage
- Nord-Korea
  - Devisen-Beschaffung → Cybercrime (Schwerpunkt Krypto-Währungen und Blockchain)
  - Finanzierung der Spionage durch Cybercrime
- USA, UK & Co – ???

„Was bedeutet das für mich?“

- Die Gefahr nimmt weiter zu – auch und gerade bei KMUs
- Die Täter nutzen Techniken, die vor wenigen Jahren noch zum „James-Bond-Arsenal“ gehörten
- Klassische Schutzkonzepte a la „Antivirus + Firewall“ reichen nicht mehr aus

Der entscheidende Punkt

Cybercrime kann jede(n) treffen!

Genauer

Es wird jede(n) treffen!

Allgemeine Schutzmaßnahmen

„Es wird uns treffen!“

Die Verteidigung

Es gibt keine Wunderwaffe

Gestaffelte Verteidigung

- Bewusstsein → Schulungen
- Gehärtete IT → Updates + Least Privilege
- Identitätsschutz → Zweifaktor-Authentifizierung
- Alarmanlagen → Monitoring, Honeypots
- Sicherungen → gute Backups
- Vorbereitung → Notfallpläne

heise Security Pro

Vernetzen, verstehen, umsetzen –
mit heise Security Pro zu mehr IT-Sicherheit.

https://www.heise.de/heisec-pro

Vielen Dank

Fragen?

ju@heisec.de