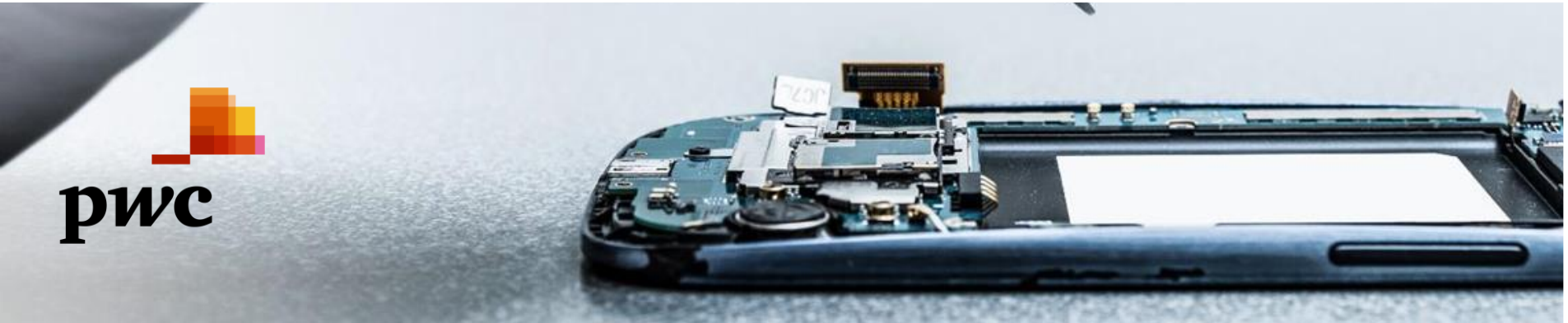
PwC Cyber Security & Privacy

Impulsstatement: Ransomware – Insights

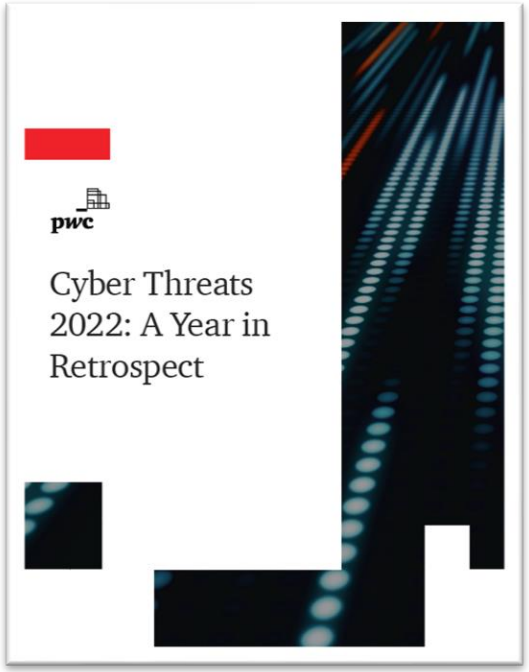
April 2023



Lorenz Kuhlee

Director
Incident Response
Threat Intelligence

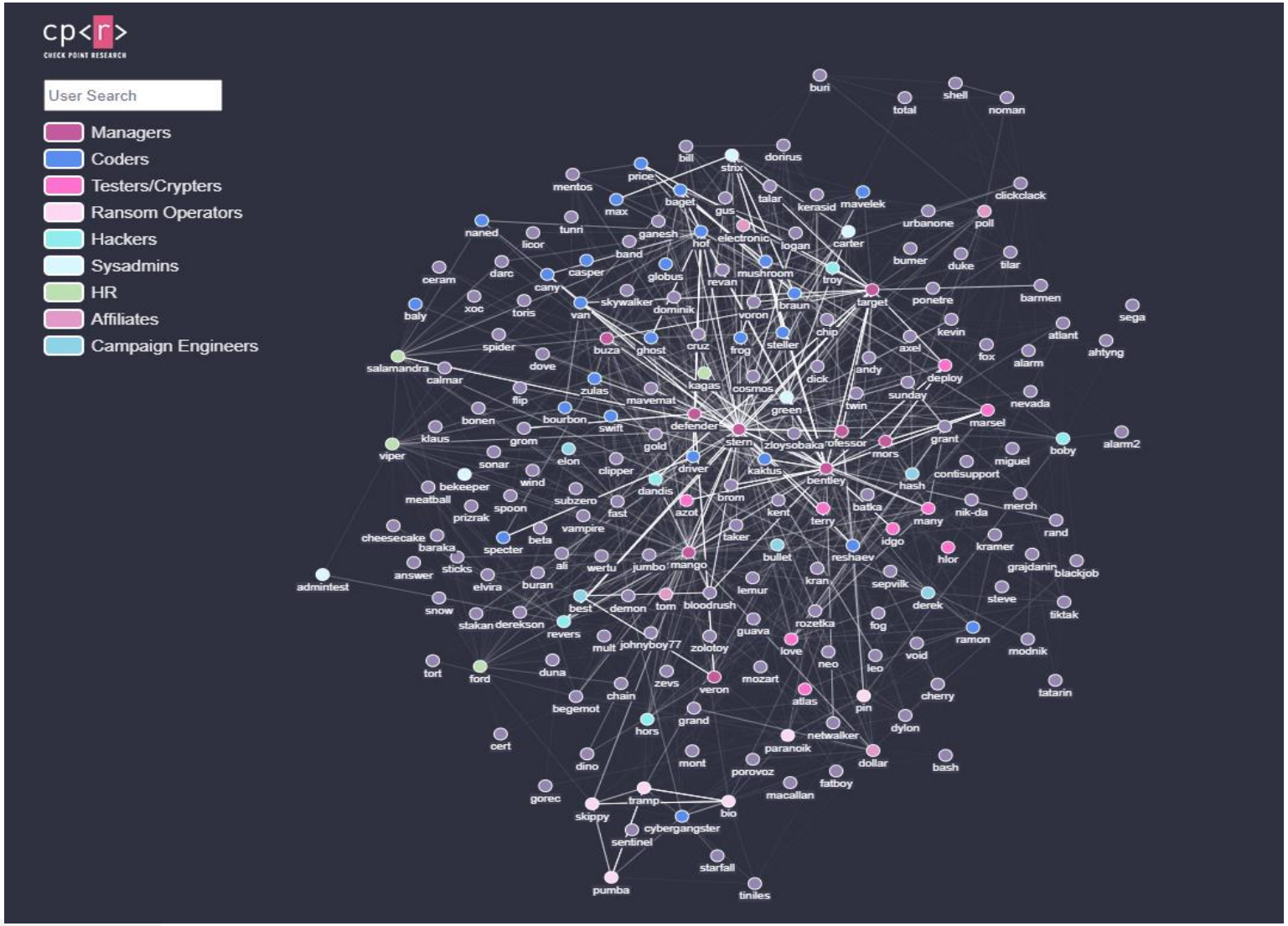
lorenz.kuhlee@pwc.com



https://cloud.email.pwc.com/2022-yir-cyber-threats-report

Realitätscheck

Professionalisierung der Angreifer

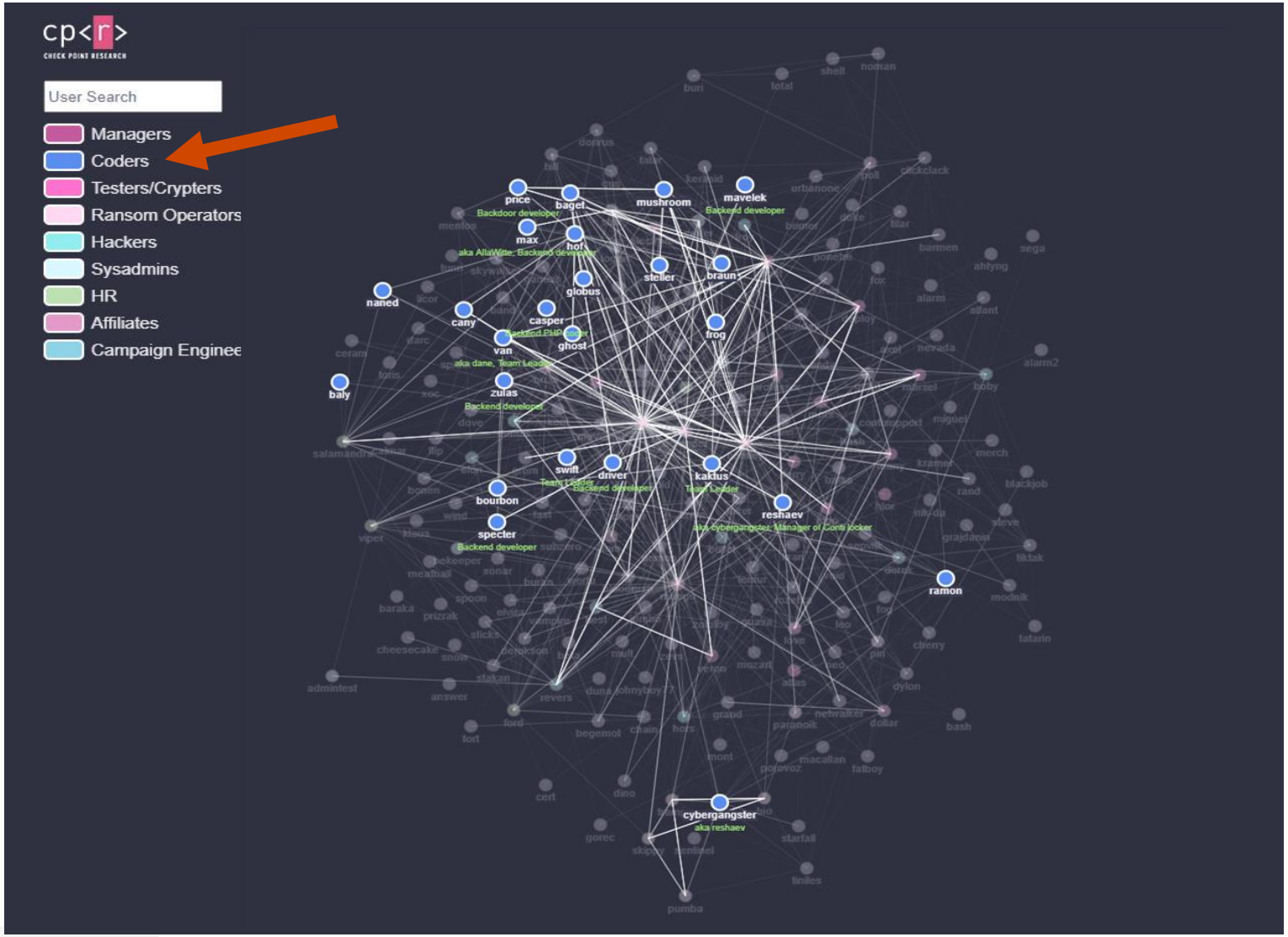


Conti Leaks 2022

- Streit zwischen ukrainischen und russischen Conti Teammitgliedern
- Mitglied hat Informationen geleakt
- Daraus entstand u.a (links) der Zusammenhangsgraph
- Es ist davon auszugehen, dass andere Gruppen ähnlich und sogar überlappend organisiert sind

https://research.checkpoint.com/wp-content/uploads/2022/03/map_index_v2.html

Professionalisierung der Angreifer



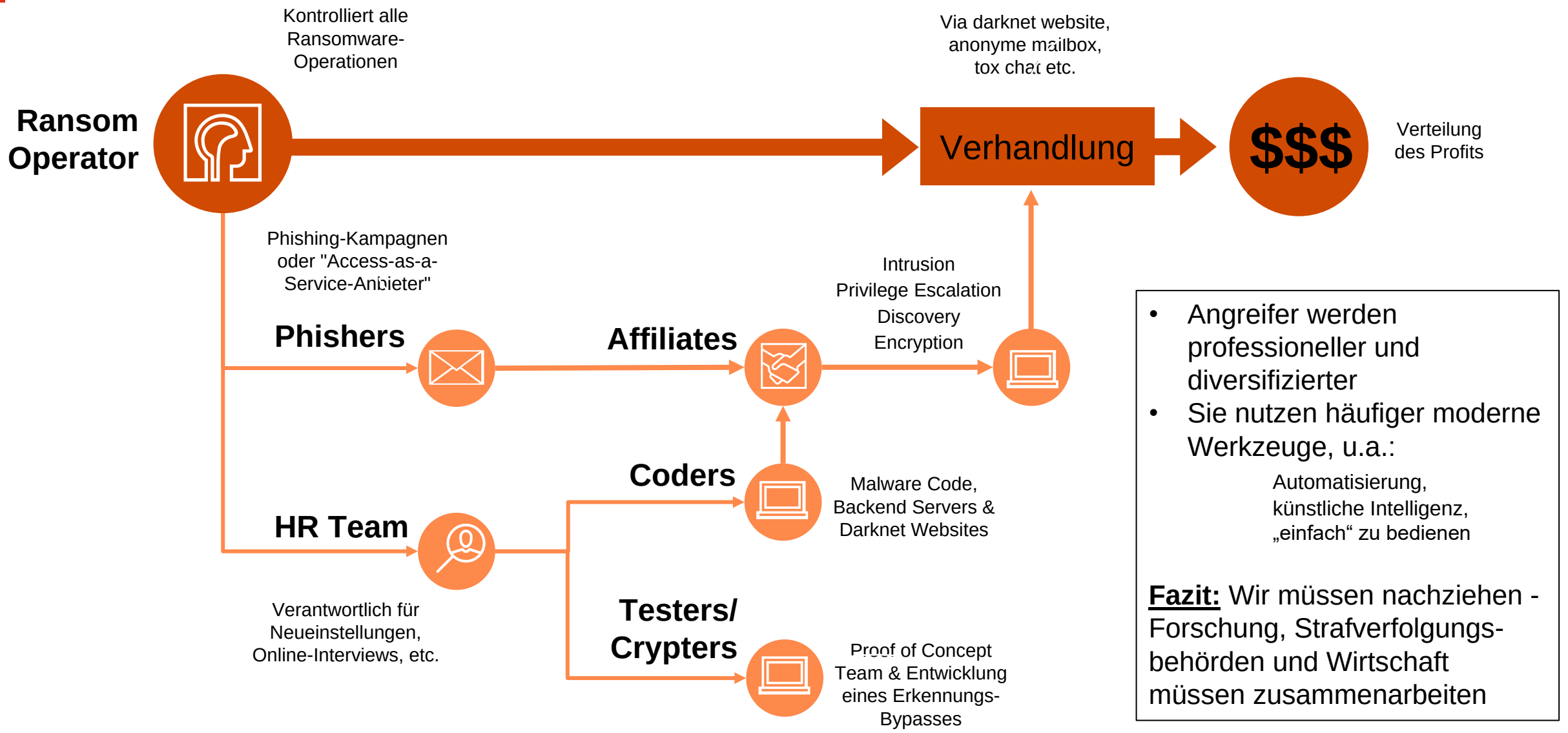
Conti Leaks 2022

- Die Conti Gruppe hatte viele Coders, die den Schadsoftware-Code, den Code für die Backend-Servers und Web-Panels für das Tagesgeschäft pflegte

- Darunter fallen auch viele Hilfstools, wie „TrickBot“, „Bazaar“, „Anchor“, die C&C Infrastruktur und die “lockers” (Ransomware)

https://research.checkpoint.com/wp-content/uploads/2022/03/map_index_v2.html

Organisation eines Ransomware-as-a-Service Angriffs



- Angreifer werden professioneller und diversifizierter
- Sie nutzen häufiger moderne Werkzeuge, u.a.:

  Automatisierung, künstliche Intelligenz, „einfach“ zu bedienen

Fazit: Wir müssen nachziehen - Forschung, Strafverfolgungs-behörden und Wirtschaft müssen zusammenarbeiten

Ransomware Opfer / Top 10 betroffene Sektoren aus 2022

2462

Anzahl der Opfer aus 2022

Professionalisierung von Ransomware-as-a-Services (RaaS) und der Tätigkeiten

LockBit (a.k.a White Janus) dominierte die Aktivität und die Leak-Seiten

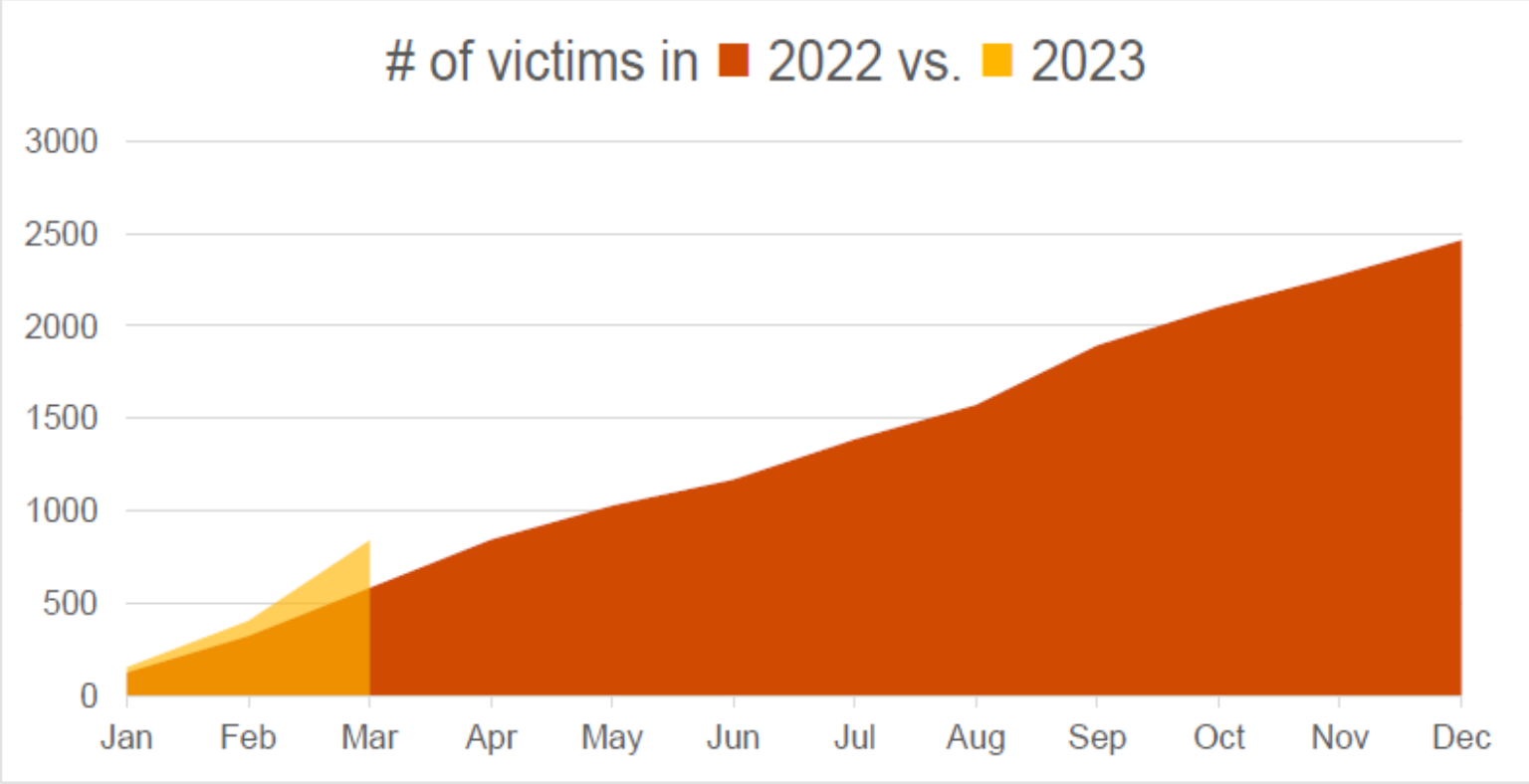
Conti (a.k.a. Blue Cronus) Leaks und Emotet (a.k.a White Taranis) kontinuierliche Aktivitäten über das ganze Jahr

Erweiterter Einsatz von Technologien wie z.B. Bumblebee, IcedID und Qakbot

Top 10 sectors	# victims	% victims
1. Manufacturing	365	15%
2. Construction	248	10%
3. Professional Services	225	9%
4. Retail	203	8%
5. Technology	191	8%
6. Hospitality & Leisure	127	5%
7. Education	125	5%
8. Healthcare	122	5%
9. Government	112	5%
10. Logistics	85	3%

Aktuelle Daten

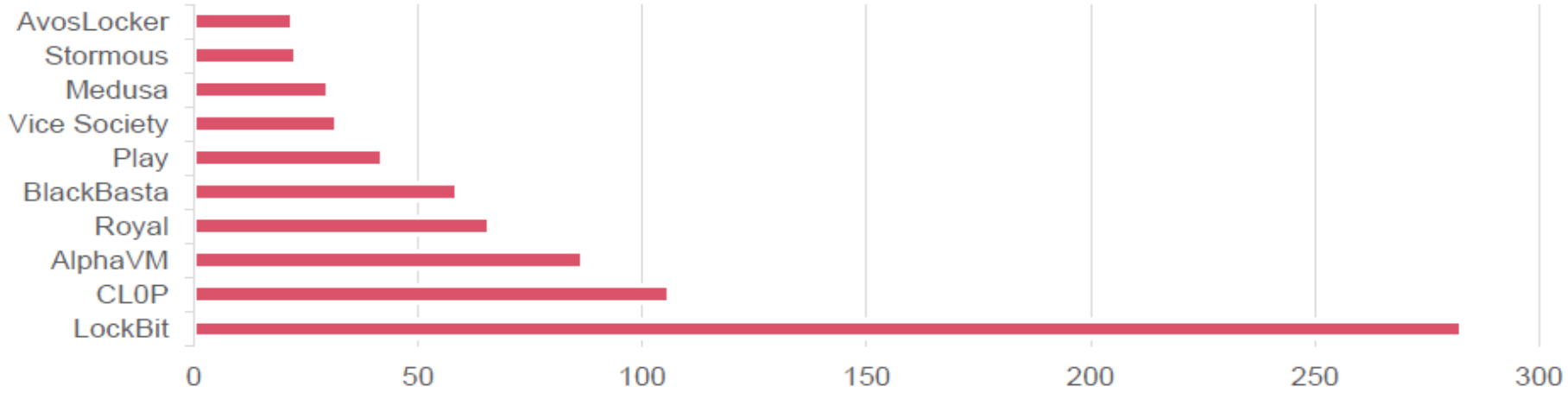
Ransomware



Unsere derzeitige Analyse zeigt, dass in Q1/2023 im Vergleich zu Q1/2022 ein bemerkenswerter Anstieg der geleakten Daten zu verzeichnen ist

Fazit: Anzahl der erfolgreichen Ransomware-Angriffe steigt

Opfer der Ransomware-Gruppen



Anzahl der Opfer in Q1/2023 sortiert nach Top 10 Ransomware-Gruppen

1 Stärkster Zuwachs an Angriffen durch die Gruppe CL0P (a.k.a White Austaras)

2 CL0P Fokus auf Schwachstellenausnutzung von GoAnywhere-Software

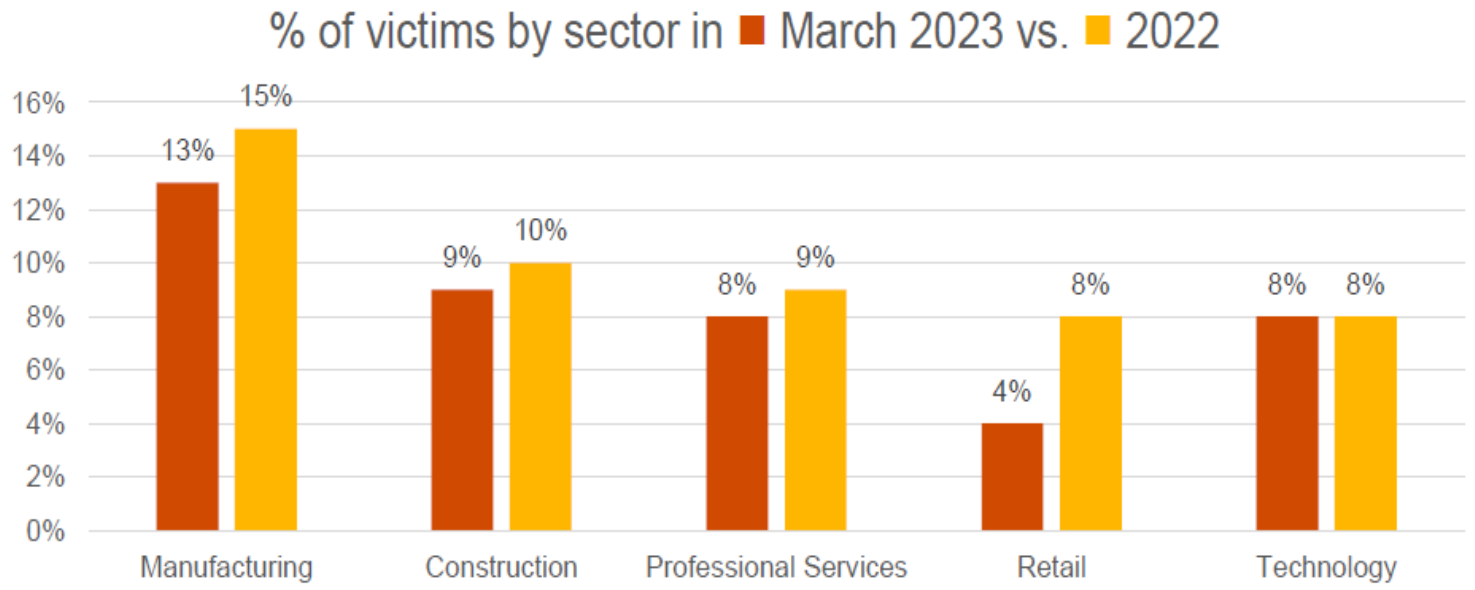
• • • •►

Trend: Ausnutzen von Schwachstellen in verbreiteten Programmen, Angriffe auf die breite Masse (opportunistisch gezielt)

Vergleich der Opferanzahl März 2023 / 2022

- Abwanderung von 8% der Top 5 Sektoren auf weitere Sektoren

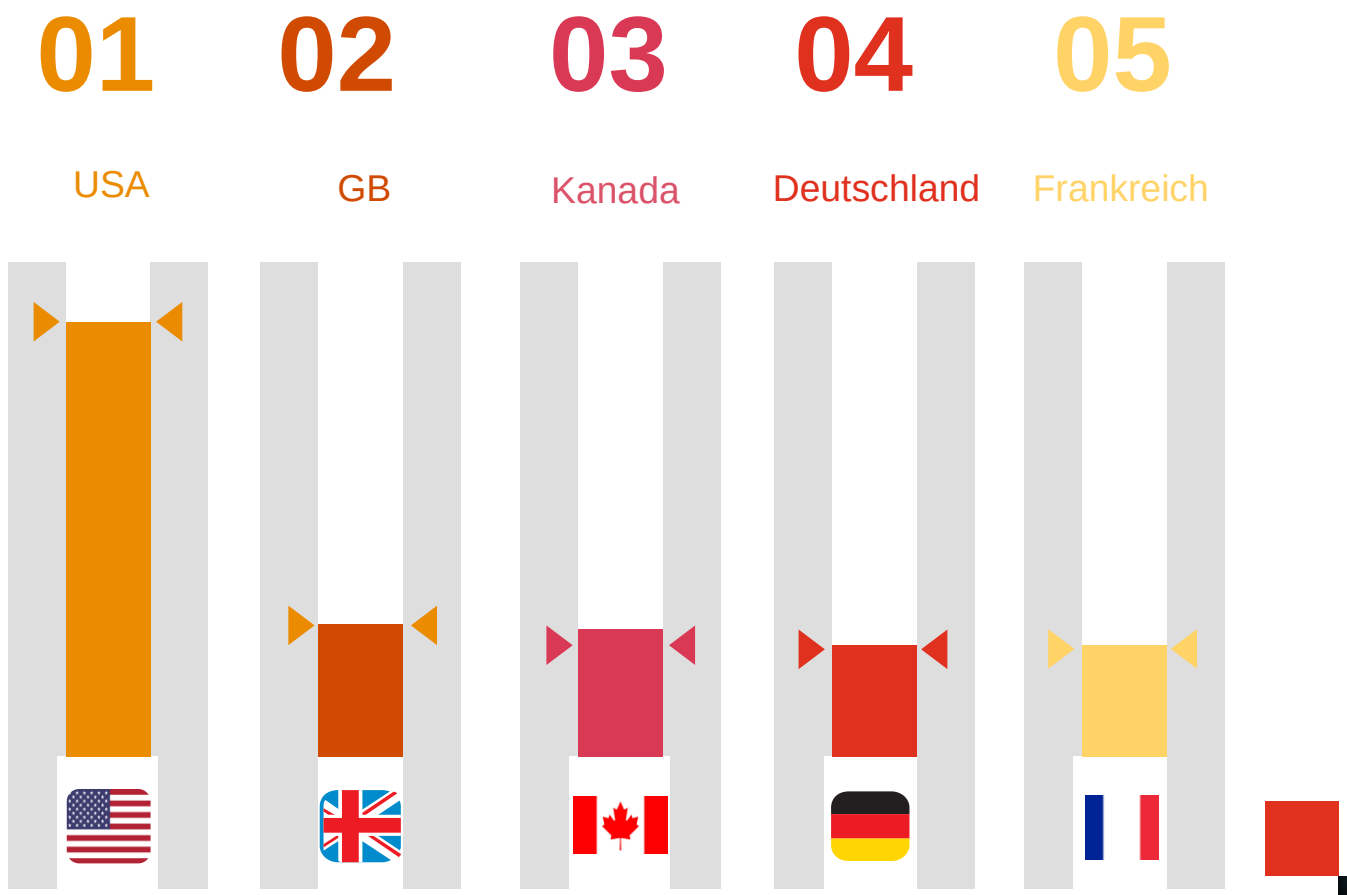
Fazit: Keine branchenspezifischen Angriffe. Angreifer zielen opportunistisch wodurch jeder zum Ziel werden kann und auch wird



Opfer gruppiert nach Länder im März 2023

- USA mit 48% der Opfer größtes Ziel
- Deutschland: Von 6 Opfern im Februar 2023 zu 17 Opfern im März

Fazit: Relativer Anteil bleibt gegenüber den Vormonaten konstant. Die absolute Zahlen steigen jedoch



Nach der Ransomware – zusätzliche Arbeit

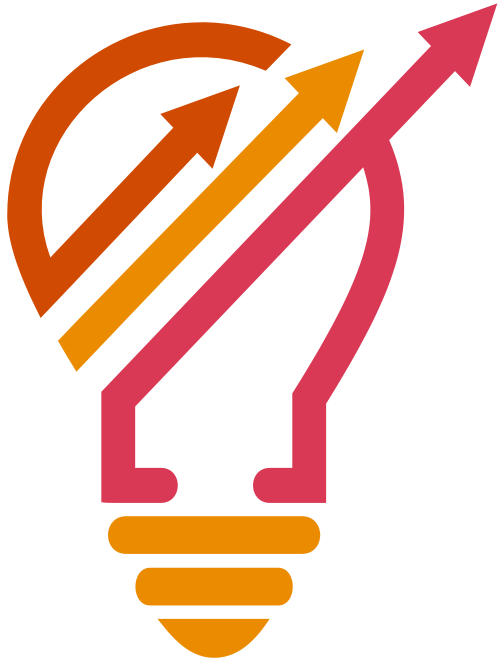
Folgen einer Ransomware sind schlimm genug!

- Beschleunigte Umsetzung der BCM-Maßnahmen
- Rechtliche Maßnahmen können folgen
- Versicherungsaufwand

Vorsicht: *„Die Bewältigung eines erfolgreichen Ransomware-Angriffs ist ein Marathon und kein 100 Meter Sprint“*

Der aktuelle Trend März 2023

- Im Vergleich zum Vorjahr erkennbarer Zuwachs
- 435 Opfer im März im Vergleich zu 250 im Februar und 153 im Januar 2023
- Große Grauzone, Datenlage unklar (bezahlt)
- Verdacht: Es wird weniger gezahlt, dadurch steigen die Angriffe
- Weniger Zahlungen = mehr Leaks
- Ransomware-Gruppen zeigen Vielfalt und Widerstandsfähigkeit
- **ABER FEST STEHT**: Definitiv nicht weniger Angriffe durch geringere Bemühungen der Angreifer!



Sprechen Sie uns an, sollten Sie weitere Fragen haben!

Wir unterstützen Sie gerne:

Vor einem Incident	Während eines Incident	Nach einem Incident
01	02	03

Vielen Dank für Ihre Aufmerksamkeit!