Agentur Cyberschutz

Agentur Cyberschutz

GESAMTKONZEPTE GEGEN CYBERCRIME

ganzheitliche, umfassende IT- und Cybersicherheit

für alle Branchen und Unternehmensgrößen

Agentur Cyberschutz

Oliver HIETZ

- Gründer & Eigentümer Agentur Cyberschutz / Cyber & Crime Versicherungsmakler GmbH
- 26 Jahre Polizeidienst – überwiegend operativer Kriminaldienst
- Konzept der Kriminalistik – täterbezogene Sicht / Prävention nach Täterverhalten
- 2021-2025: stark wachsende Unternehmen mit Partnernetzwerk aus führenden Cyberexperten

Fabian POBER

- Bereichsleiter Darknet Monitoring & Darknet Analyse
- Experte für Cyber Threat Intelligence & Datenleak-Erkennung
- Keynote Speaker & Cybersecurity-Stratege
- Fokus: Darknet-Trends, Ransomware-Analysen & Prävention
- Tätigkeitsschwerpunkt in der DACH-Region

Agentur Cyberschutz

cyber & crime Versicherungsmakler GmbH

cybercrime Komplettschutz

cybercrime Komplettschutz INCIDENT RESPONSE SERVICE TEAM

Agentur Cyberschutz

Cybercrime

Attacken auf IT

Cyberattacken

- zielgerichtete Angriffe
- Unternehmen – kritische IF - Behörden
- Netzwerksicherheitsverletzungen
- Existenzbedrohende Schäden

Werkzeuge / Angriffsvektoren

- IT-Schwachstellen
- Keylogger
- DARKNET Märkte
- Admin Accounts

Ransomware / Extortion
Ransomware / Double Extortion
DDOs
Gesamtschaden: BU – IT - Daten

RAGNAR_LOCKER

DARKNET

- **Kommunikations- und Handelsplattform**
- **Daten- und Schwachstellenverkauf**
- **Cybercrime as a Service - Auftragsattacken**

Social Engineering

CYBER-Betrug- und Erpressung

- Schwachstelle Mensch
- Privatpersonen / Unternehmen
- Breitgefächert / zielgerichtet

Werkzeuge / Angriffsvektoren

- Mail / Tel
- Social Engineering
- Fakemailer / Call – ID Spoofing / Fakeshops

Betrugs- und Erpressungsdelikte (12 MP):

- CEO Fraud / Fake Prs.
- Rechnungsbetrug
- Lieferumleitung
- Phishing – 148a

Agentur Cyberschutz

Ransomware Gangs / „Ragnar Locker“

- IT-Experten / IT-Spezialisten / klass. Hacker
- Einzeltäter – Gruppen - Firmennetzwerke
- Programmieren hochkomplexe Schadsoftware
- zielgerichtete Attacken - CaaS
- Ransomware / DDoS / Datendiebstahl
- **Zielgruppen:** Unternehmen aller Größen und Branchen – Gebietskörperschaften – Behörden – kritische Infrastruktur / Privatpersonen?
- **Länder: Zentraleuropa / USA – insbesondere DACH**

Agentur Cyberschutz

Zielgruppen

Bildungs-einrichtungen
(Schulen, UNIs, Fortbildungen, etc.)

Dienstleister
(Industrie, Klein- und Mittelbetriebe, Einzelunternehmer.)

Behörden
(Gemeinde, Magistrate, Länder, Verwaltungsbehörden)

Versicherungen

Ärzte

Banken

Notare, Anwälte

Handel

Onlinehandel

IT-Dienstleister/ Mailhoster

Soziale Netzwerke
(Facebook, Instagram)

Hotellerie, Tourismus, Fluglinien

Agentur Cyberschutz

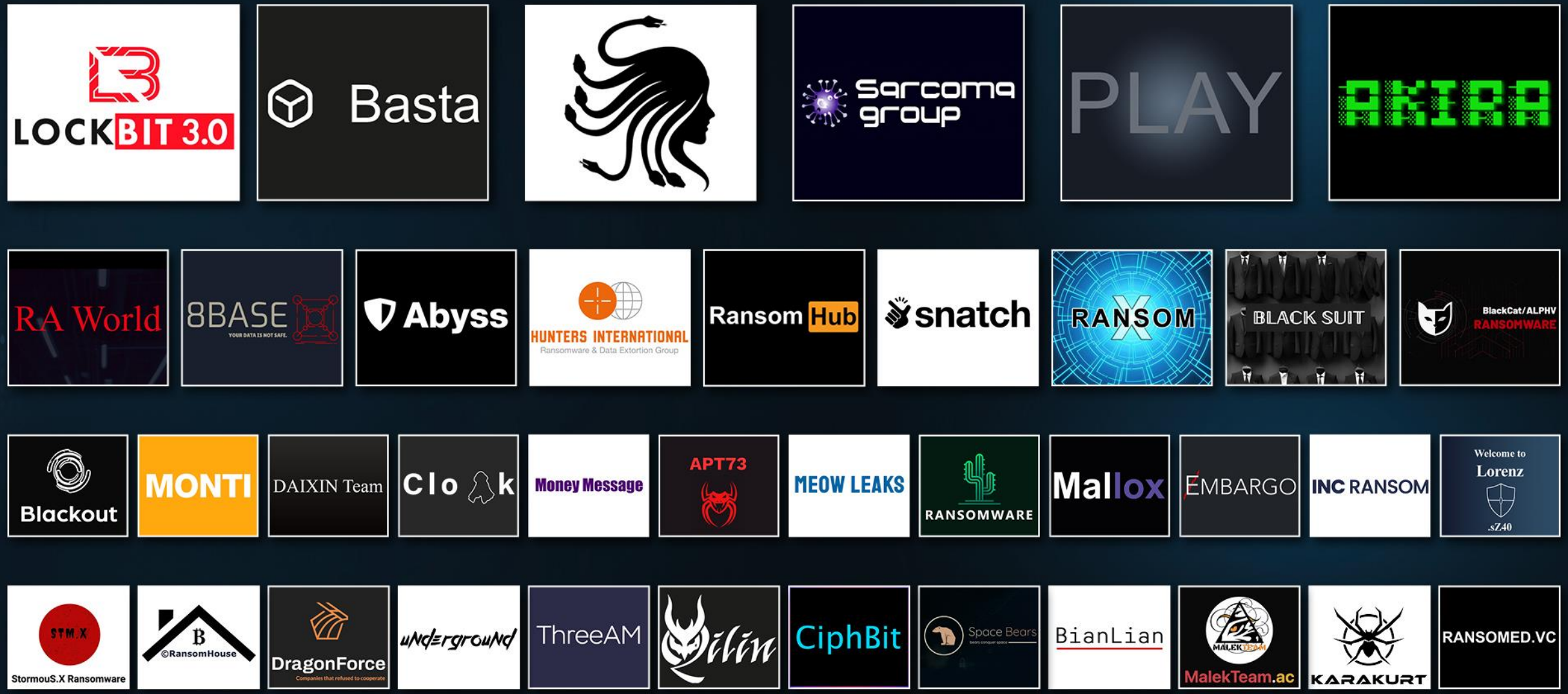
Agentur Cyberschutz Stats

- Weltweit seit 01.01.2022: 18.000 veröffentlichte Opfer mit Datenabfluss
- seit 01.01.2022 – 300 Gruppierungen
- derzeit 90 aktiv
- agieren länder- und branchenübergreifend
- identes Konzept – geringfügige Unterscheidungen

Spezifikationen – Lösegeldbemessung – Affiliate System – Vorverhandlungen

Agentur Cyberschutz

Ransomware Gangs



Agentur Cyberschutz

Tätergruppen

LOCKBIT 3.0

- aktiv seit 2020
- bis zu 60 Opfer / Tag
- bis zu 200 Unternehmen parallel in Verhandlungen
- länder- und branchenübergreifend / keine Spezifikation
- RaaS erkennbar
- Lockbit Affiliate – Pflichten und Rechte
- Lockbit Daten Vendor

LOCKBIT 3.0

Tätergruppen

LOCKBIT 3.0 - Affiliate

- Bewerbungs- und Motivationsschreiben
- Anforderungsprofil / Meldung von anderen Kooperationen
- 1 bitcoin als Pfand / Bürgen
- 20% des Gewinns als Honorar
- Regeln: keine kritische Infrastruktur verschlüsseln / Datendiebstahl erlaubt / keine postsowjetische Länder / medizinische Einrichtungen erlaubt – außer chirurgische Abteilungen, Entbindungsstationen, Kinderspitäler – Datendiebstahl erlaubt

Agentur Cyberschutz

End-Szenarien

Bezahlung des Lösegeldes / meist alternativlos

- Freigabe des Systems
- Datenpaket nicht zum Verkauf freigegeben
- „EHRENKODEX“ – Geschäftsmodell
- BU: 10-14 Tage / Abschluss Schadensfall 1 Monat

Lösegeld wird nicht bezahlt

- Freigabe / Verkauf der Datenpakete im Darknet an Cyberschurken
- löst Social Engineering Tsunami aus
- Betroffene werden Ziele von Betrugs- und Erpressungsdelikte
- BU: 2-3 Monate / Abschluss Schadensfall bis 1 Jahr

Agentur Cyberschutz

Ablauf einer Ransomware Attacke

We have 2TB critical data of this company on our servers.
After time end all data will be publish.
We will be waiting for your suggestions!
We are always happy to offer the best solutions.
Sincerely your team

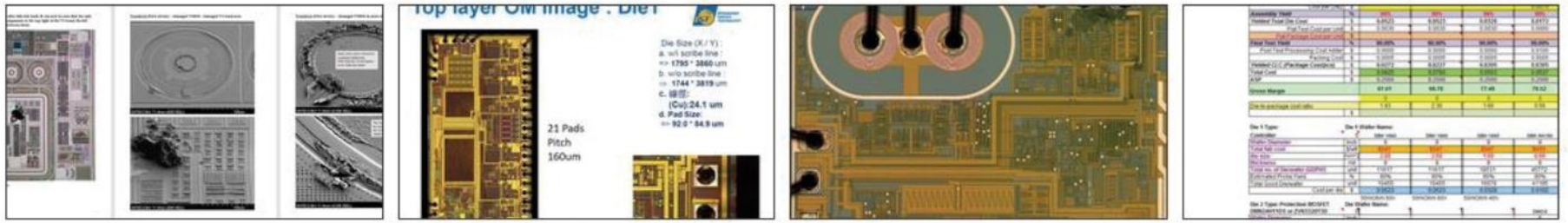
Today you can upload the first part of data.
http://cviru74jqv3yrlrn7iphmoskmskceprafcvqgtqegrxhoppgds3frrqd.onion

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 29 JUN, 2022 22:32 UTC **UPDATED:** 25 JUL, 2022 08:58 UTC

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 10000	$ 15000000	$ 15000000

1-4 of 11



Agentur Cyberschutz

Wie komme ich ins Darknet

- Einstieg über Tor-Browser
- Darknet unsichtbar für Standardbrowser
- Anonymität für Sender und Empfänger
- unkonventionell – keine Clear Adressen
- nicht illegal / nicht strafbar
- kein großes Netz – 35.000 Zielseiten
- Underground Economy – Silk Road

http[:]//3kp6j22pz3zkv76yutctosa6djpj4yib2icvdqxucdaxxedumhqicpad[.]onion (ARVIN CLUB)

Agentur Cyberschutz

Cybercrime as a Service

AlphaBay Marketplace Statistics

Active Vendors:	13945
Registered Buyers:	1028569
Active Listings:	42339

Categories

- Fraud 6200
- Hacking & Spam 1113
- Malware 129
- Drugs & Chemicals 39489
- Services 398
- Security & Hosting 124
- Guides & Tutorials 2969
- Software 800
- Digital Items 1494
- Websites & Graphic Design 19
- Jewels & Precious Metals 25
- Counterfeit Items 700
- Carded Items 49
- Automotive-related Items 15
- Legitimate Items 55
- Other Listings 181

Welcome, **cyber2000**

AlphaBay is **re-opened for business** for the first time exactly 4 years since 2017. Having first **started trading in 2014**, we cultivated a strong connection with the DNM community by being **professional, fair & responsive** when dealing with buyers and sellers alike. By 2017 that alongside our innovations, high security, uptime & ease of use made us **the biggest and most trusted secure anonymous marketplace** ever to have existed. You can read our first public message since 2017 detailing our vision going forward, why we have returned, what has been improved and more answers here.

If the name AlphaBay does not ring a bell and you do not know what this website does or who we are, you should search us up yourself. You can also view our page about AlphaBay here.

AlphaBay has always been a **principle-driven, vision-oriented and community-centered** marketplace. The administration is almost the same as in the 2014-2017 period which means you will find again AlphaBay runs with **mature management, unparalleled security, 24/7 professional & well-trained Staff** and of course unique vision for the future not only for itself but for the darknet market scene too.

If you have any questions about the market refer to FAQ, How-To guides or Support Center. Feedback or suggestions can be directed to the Forum and our Staff members will look into it. We greatly appreciate any feedback you can provide to make the market a better place!

Security & Progress: 50%

- Add public PGP key to profile - [Add PGP Key]
- Enable PGP 2FA (Two-Factor Authentication) - [Enable 2FA]
- Refer a friend and earn up to 25% from escrow profit - [View Referral Code]
- Reach Trust Level 2

Featured Listings

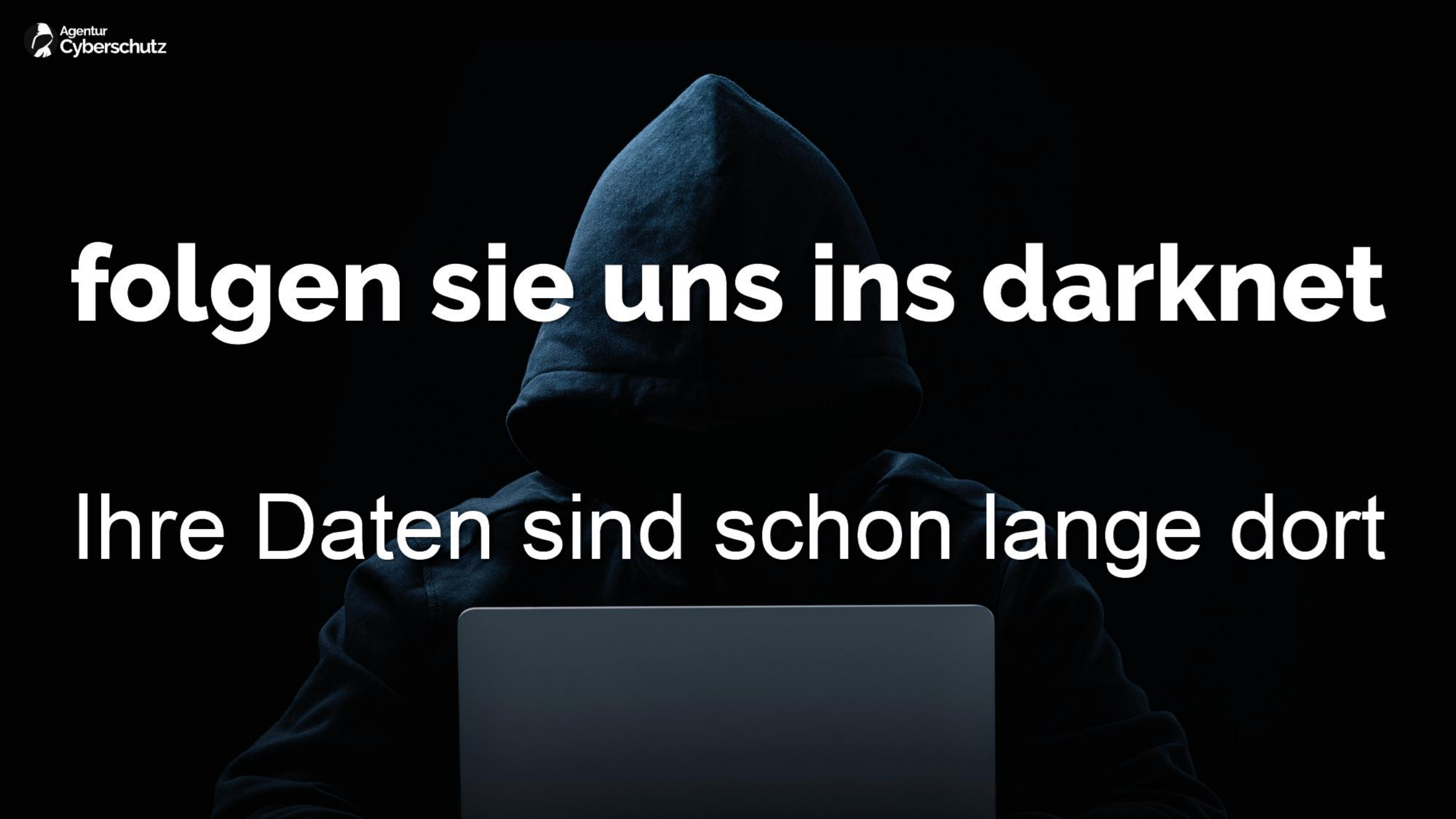
1.64ea ADDERALL b974 30mg x100 countt PROMO

(10 - 1000+ grams) DUTCH MDMA ROCKS - CHAMPAGNE 84%

Raw Colombian Cocaine Untouched 96% Purity *FAST SHIPPING USA

ORIGINAL FORMULA TUCI - COCA ROSA - PINK COCAINE 10 GRAM MINIMUM!

Agentur Cyberschutz



folgen sie uns ins darknet

Ihre Daten sind schon lange dort

Agentur Cyberschutz