Agentur
Cyberschutz

Secutec

Unsere Kooperation zu ihrer Cyber- und IT-Sicherheit

Oliver HIETZ

- Polizeidienst – Kriminaldienst
- Gründer / Eigentümer
  Agentur Cyberschutz GmbH und
  Cyber & Crime Versicherungsmakler GmbH
- umfassendes Gesamtkonzept:
  Cyberversicherung – Voraussetzungen
  Incident Response Service Team

Daniel ROSSGATTERER

- IT-Laufbahn
- Geschäftsführer SECUTEC Österreich
- externe Sicht IT-Security

Agentur Cyberschutz Secutec

Was uns verbindet

- **externe Sicht / klar täterbezogen / praxisnah**
- **Prävention nach Täterverhalten**
- **Schadensfallbetreuung – Hintergrundwissen Täterprofile**

Unsere Kooperation zu ihrer Cyber- und IT-Sicherheit

Agentur Cyberschutz Secutec

Secutec
Cybersecurity Intelligence

- belgisches IT-Security Unternehmen mit Sitz in Antwerpen
- führender Experte auf dem Gebiet von Threat Intelligence
- seit 2021 auch im DACH-RAUM tätig
- Konzentration auf die externe Sichtweise (Tätersicht)
- einzigartige Kombination aus Cyber Threat Intelligence & Bewertung durch Analysten

Agentur Cyberschutz

- Schnell wachsendes, hochspezialisiertes, österreichisches IT-Security Unternehmen
- einer von 3 Exklusivpartner von SECUTEC in der DACH-Region
- einzigartiger Kriminalistik Zugang inkl. DARKNET Intelligence & Investigations
- umfassendes Cyberpräventionskonzept
- ganzheitliches INCIDENT Response Service

Unser einzigartiger Wissensvorsprung für Ihre Cybersicherheit
Wir als Quelle selbst

DARKNET-Analyse & Schadensfall Nachevaluierungen

Ausdruck unseres einzigartigen Kriminalistik Zugangs – Präventionsmaßnahmen nach Täterverhalten und Angriffsvektoren – sind unsere tagtäglichen umfassenden Täter / Opfer Recherchen im Darknet und Nachevaluierungen von Schadensfällen.

Wir vertrauen demnach keinerlei öffentlichen, frei zugängigen Quellen von Medien, Behörden und Interessensvertretungen und können aufgrund unserer tagesaktuellen Datenbasis belegen, dass diese zumeist irreführend und nicht praxisnah sind.

DARKNET-Analyse

- aktive Tätergruppen / Opfer
- weltweite Opferstatistik seit 2022
- DACH-Region Detailreports
- Täterprofiling – Spezifikationen
- Statistiken / Reports

IT-Risikoanalysen

- Überprüfung, Herstellung und Bestätigung von Cyberversicherungsvoraussetzungen
- Feststellung von Schwachstellen und Problemfeldern
- Empfehlungen

Incident Reponse Service Reports

- Auswertung von IT-Forensik Reports
- Angriffsverlauf / Angriffsvektoren
- Verhandlungsverlauf
- Gesamtschadenszusammenstellung
- Nach- und Hochrüsten

Cybercrime

Agentur Cyberschutz Secutec

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 Stats

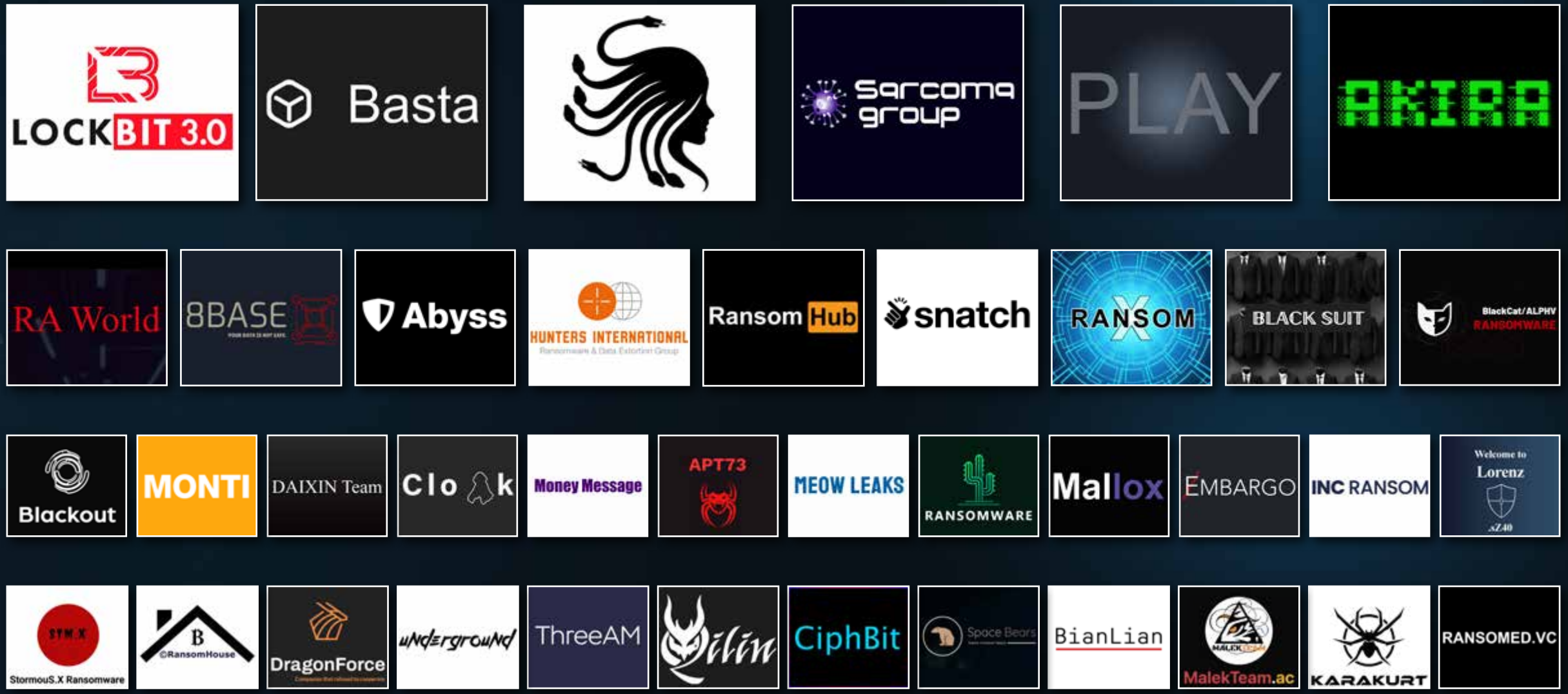
Agentur Cyberschutz Secutec

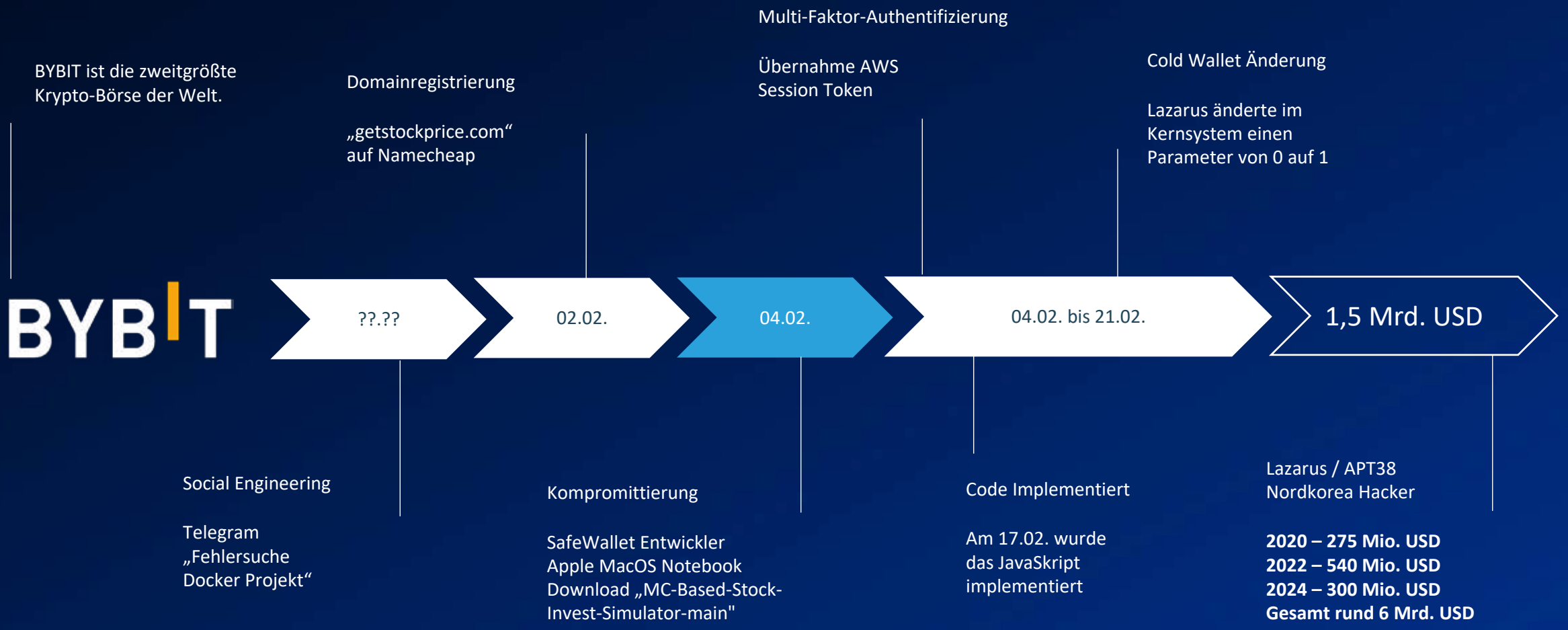
- Weltweit seit 01.01.2022: 18.000 veröffentlichte Opfer mit Datenabfluss
- seit 01.01.2022 – 300 Gruppierungen
- derzeit 90 aktiv
- agieren länder- und branchenübergreifend
- identes Konzept – geringfügige Unterscheidungen

Spezifikationen – Lösegeldbemessung – Affiliate System – Vorverhandlungen

Ransomware Gangs

Agentur Cyberschutz Secutec




BYBIT ist die zweitgrößte Krypto-Börse der Welt.
Domainregistrierung
„getstockprice.com“ auf Namecheap
Multi-Faktor-Authentifizierung
Übernahme AWS Session Token
Cold Wallet Änderung
Lazarus änderte im Kernsystem einen Parameter von 0 auf 1
BYBIT
??.??
02.02.
04.02.
04.02. bis 21.02.
1,5 Mrd. USD
Social Engineering
Telegram „Fehlersuche Docker Projekt“
Kompromittierung
SafeWallet Entwickler Apple MacOS Notebook Download „MC-Based-Stock-Invest-Simulator-main"
Code Implementiert
Am 17.02. wurde das JavaSkript implementiert
Lazarus / APT38 Nordkorea Hacker
2020 – 275 Mio. USD
2022 – 540 Mio. USD
2024 – 300 Mio. USD
Gesamt rund 6 Mrd. USD

Cybercrime aus der Praxis und die Konsequenzen

Case 1 – Lösegeldzahlung trotz Sanktionsverbot

Case 2 – Datendiebstahl aufgrund Vulnerability

Die Welt der Hackergruppen

Agentur Cyberschutz Secutec

Wieviel Prozent
von 100 Unternehmen
könnte einer der besten
Hacker in Europa hacken?

Agentur Cyberschutz Secutec

100%

Schlecht gesicherte Unternehmen in 2 Minuten und 2 Jahre unerkannt.

Sehr gut gesicherte Unternehmen in 2 Jahre und 2 Minuten unerkannt.

Agentur Cyberschutz Secutec

Wirtschaftlichen Hacker Gruppen

Lockbit, BlackCat, Play, …

50-70 professionelle Hacker Gruppe, die Unternehmen angreifen, um Lösegeld zu erpressen.

Die Top Organisation erpressen im Jahr teilweise bis zu 500 Mio. USD Lösegelder.

ZIELE: Lösegeld erpressen von Unternehmen und Organisationen

Politischen Hacker Gruppen

APT28 – FanyBear
- Dt. Bundestag - Angela Merkel
- US Wahlkampf – Hillary Clinton
- OPCW - Syrien, Sergej Skripal

Einheit 74455 – Sandworm
- Ukraine – Stromversorgung
- NTC Vulkan – Software Hersteller

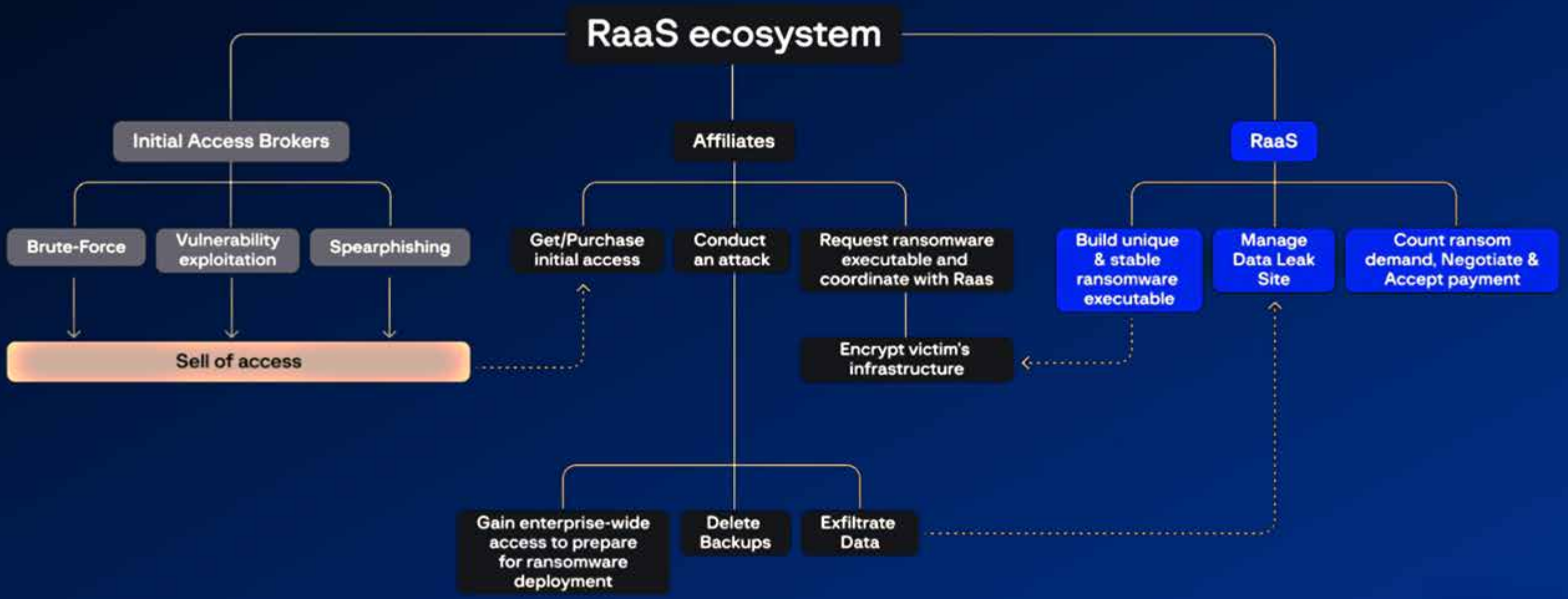
ZIELE: Destabilisierung durch Falschinformationen, Zensur, Durchsetzung Eigeninteressen

Einzeltäter und politisch motivierte Gruppen

Anonymous
Hacktivismus - als Protestmittel, für politische und ideologische Ziele.

NoName057, Killnet
Pro russische Hackergruppen, die gezielt den Westn angreifen.

ZIELE: Politische und Ideologische Ziele erreichen, Privatpersonen


RaaS ecosystem
Initial Access Brokers
Affiliates
RaaS
Brute-Force
Vulnerability exploitation
Spearphishing
Get/Purchase initial access
Conduct an attack
Request ransomware executable and coordinate with Raas
Build unique & stable ransomware executable
Manage Data Leak Site
Count ransom demand, Negotiate & Accept payment
Sell of access
Encrypt victim's infrastructure
Gain enterprise-wide access to prepare for ransomware deployment
Delete Backups
Exfiltrate Data

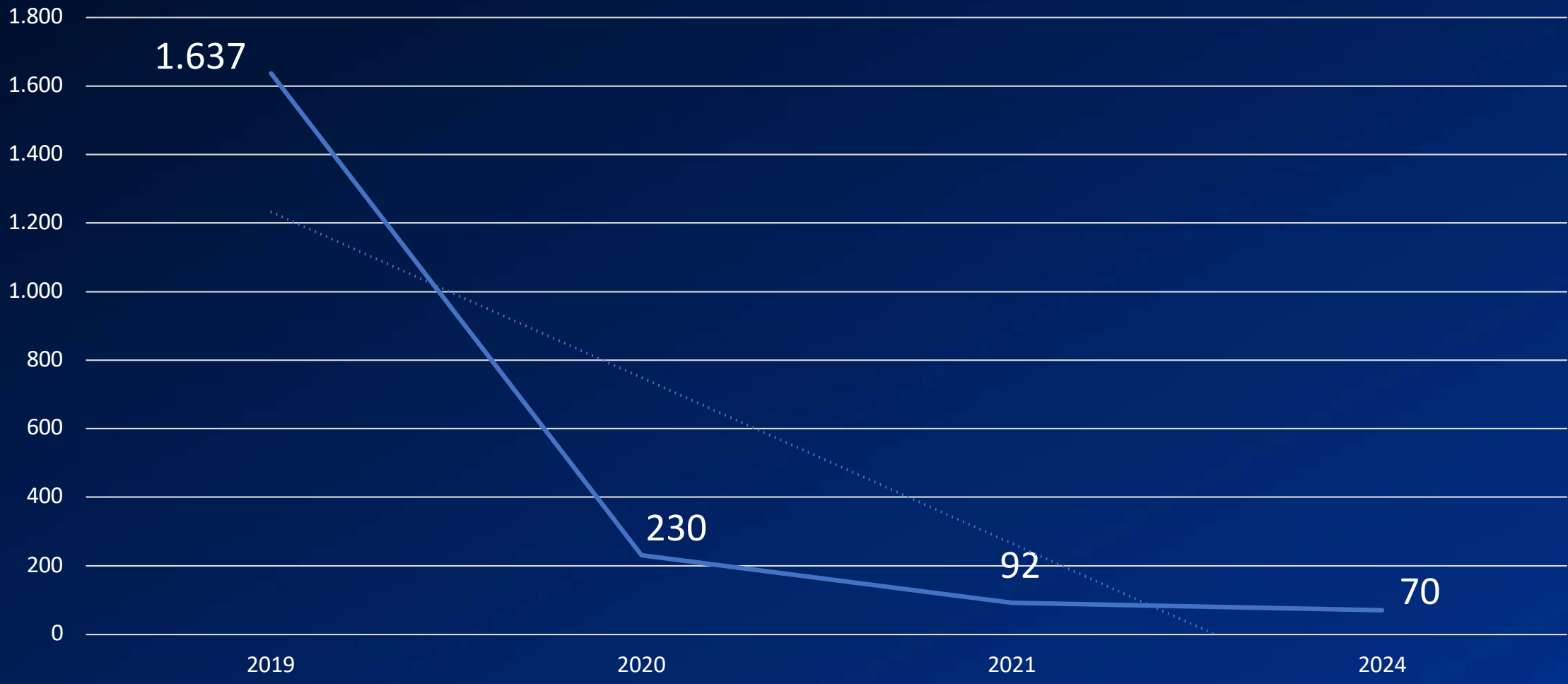
Die Ransomware Attacke

Exfiltieren von Daten
(200GB bis 1 TB)

Backups zerstören
(Index löschen)

Daten verschlüsseln
(4KB einer Datei)

Initial Access via Broker zum Ransomware Deployment (Stunden)



Agentur Cyberschutz Secutec

Angriffsvektoren

Phishing
(Fokus New Domains)

Lösung: SecureDNS

Brute-Force Attacken
(Wellen bei größeren Leaks)

Lösung: Darknet Monitoring

Passwort Stealer/Keylogger
(Private- und Firmengeräte)

Lösung: Darknet Monitoring

Exploit Vulnerability
(Platzierung von Backdoors)

Lösung: Attack Surface Management

Supply Chain Attacken
(Dienstleister, Lieferanten Service Accounts, usw)

Lösung: ASM und Darknet Monitoring

Man in the Middle
(Fokus Rechnungsbelege)

Lösung: SecureDNS, Threat Hunting, M365 Kit

Social Engineering
Deep Fake
(Online, Audio, Video)

M365 Phishing
(Proxy/Cache - Logindaten/MFA)

Lösung: M365 Security Kit

Supply Chain
Service Accounts

Supply Chain
Datendiebstahl

Vulnerability
Backdoor

M365 Phishing
MFA Logindaten

Passwort Stealer
Privatgeräten

Die ersten 48 Stunden nach der Attacke

-Die Server nicht herunterfahren!

-Start der Forensik (Wie, Wer, Was)

-Darknet Monitoring

-Keine Verhandlungen in den ersten 48 Stunden

-Klare Strategie / Organisation (intern/extern)

-Priorisieren der Daten und Systeme

-Isolieren der verschlüsselten Systeme vom Rest

Lösegeld-forderungen

- Decken sich oft mit den liquiden Mitteln.

  Bilanzen sind in vielen Fällen bekannt.

  Start Forderung meist 5-8% vom Umsatz.

- Argumente über nicht liquide Mittel werden

  oftmals mit aktuellen Bankauszügen widerlegt.

Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company's customers will be published on the internet, and the respective country's personal data usage authority will be informed. Moreover, confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID:

Ransome-Note DragonForce

Agentur Cyberschutz Secutec

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. **We work for money and are not associated with politics. All you need to do is contact us and pay.**

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

Link for Tor Browser:
http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion

>>> Use this ID: 39654EB6493411F539654EB6493411F5 to begin the recovery process.

* In order to access the site, you will need Tor Browser, you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1C054B722BCBF41A918E3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.

DO NOT RENAME OR MOVE the encrypted and readme files.

DO NOT DELETE readme files.

--- Important:

If you refuse to pay or do not get in touch with us, we start publishing your files.

16/04/2025 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

DragonForce
Companies that refused to cooperate

Timeline Cybercrime Komplettschutz
INCIDENT RESPONSE SERVICE

Agentur Cyberschutz Secutec

PHASE 1
Die kritischen 48 Stunden

- Krisenstab – INTRO – Täterinfos – Ablauf – Vollmachten
- IT-FORENSIK
- IT-SUPPORT
- Erstmeldungen (DSGVO – Behörden – Polizei)
- Schutzschirm
- Rechtshilfe

Ziele

- Erst-Report
- Erstmeldungen
- Schutzschirm

PHASE 2
EXIT – Systemwiederherstellung

- Erst-Report (Datenabfluss, Angriffsvektor, Back-up)
- Verhandlungsführung
- Sonderfall Lösegeld
- Sanktions- und Embargo-Checks
- Kryptobereitstellung / Zahlung
- System- und Datenwiederherstellung
- Leihgerätschaften / Neuanschaffungen
- DSGVO Obliegenheiten
- PR- Management
- Benachrichtigungen

Ziele

- Exit-Strategie
- Schadenseindämmung
- Systemwiederherstellung

PHASE 3
Nachbearbeitung

- Rechtshilfe – Prozessvorbereitung – Prozessführung
- Gesamtschadenszusammenstellung
- Aufrüsten – Nachevaluierung
- Endreporting

Ziele

- Refundierung des Gesamtschadens
- Eindämmung Reputations- und Imageschäden
- Absicherung / Aufrüstung

Agentur Cyberschutz

tems security

Secutec

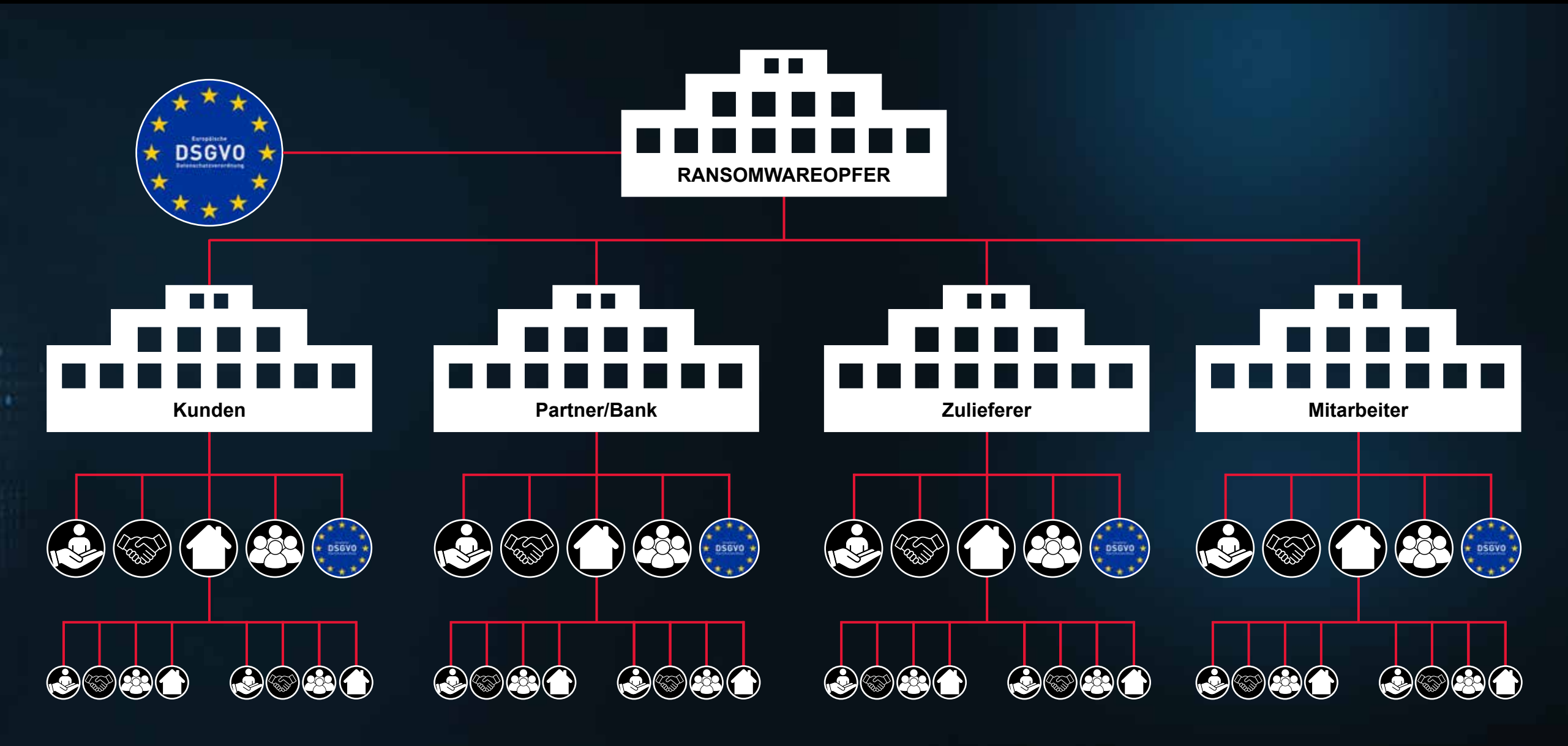
ATB
AZEM I TAUDES I BLÖCH

tems
See the world with Emil

AKIRA - Täterprofiling

- aktiv seit April 2023 / Verbindung zu CONTI
- Angriffsvektoren: VPN, Keylogger, AnyDesk, CVE
- über 320 Opfer mit Datenleck und Veröffentlichung
- Monatsdurchschnitt 25-30 / 1-2 DACH
- DACH-Raum 5%
- Affilate System
- Datenabfluss gering / zweistelliger GB -Bereich
- Lösegeldbemessung nach Jahresumsatz (4 Mio. Rekord)
- Eigenheit: lange Vorverhandlungen / mehrere Monate
- wenig Traffic auf DARKNET Dashboard

Agentur Cyberschutz Secutec



Empfehlungen

Agentur Cyberschutz Secutec

DNS Monitoring

Auch IoT Devices beachten!

Externe Scans Schwachstellen

Aus Sicht eines Cyberkriminellen

Darknet Monitoring

User, Keylogger, VIPs, Keywords

Incident Vorbereitung

Geschäftsleitung nicht vegessen!

Playbook Notfallhandbuch

Hacker Attacke Blackout, usw.

Multifaktor Authentifizierung

Nicht nur mit Bestätigung!

EDR/XDR Virenscanner

Anomalie-erkennung

Backup Konzept und Recovery

Testen nicht vergessen!

Server Logs Backup

Rund 90 Tage für Forensik

Netzwerk Segmentierung

Firewall nicht vergessen!

Keine lokalen Admin Rechte

Nur temporäre Rechte zulassen

Active Directory Tiering Struktur

Eigene User für Server und DC

Passwort Manager

Verwaltung und sichere Passwörter (+Privatnutzung)

SECUTEC Webinar

Agentur Cyberschutz Secutec

„Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence Technologien“

Danke euch, einmal mehr grandios!

Super Webinar, bis bald

🙏

Sehr interessantes und spannendes Webinar!

richtig stark!

Sehr interessanter Vortrag! Vielen Dank.

Einzigartig !!!

💖

Super spannend, herzlichen Dank!!

War sehr Interessant! Danke!

Secutec Webinar – „Darknet, Hacker & Co – Ein Blick hinter die Kulissen von Cyberkriminellen.“

W10.2. = Donnerstag, 30.10.2025 / 08.30 – 10.00 Uhr
Secutec Webinar W10.2 - 30.10.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

W11.1. = Dienstag., 25.11.2025 / 15.00 – 16.30 Uhr
Secutec Webinar W11.1 - 25.11.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

W12.1. = Dienstag, 16.12.2025 / 08.30 – 10.00 Uhr
Secutec Webinar W12.1 - 16.12.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

Agentur Cyberschutz Secutec

Let‘s connect!

Machen wir gemeinsam die Cyber Welt ein Stück sicherer

Agentur Cyberschutz Secutec

Präventiv schützen!

Entwicklung und Expertise in Cyber Threat Intelligence
Technologie in Europa seit 2005.

Hilfe leisten!

Erfahrungen aus hunderten Incident Response Fällen, Verhandlungen und Lösegeldzahlungen.

Agentur Cyberschutz Secutec

Secutec wins exclusive €35 million contract with CCB for delivery of cyber threat intelligence feeds.

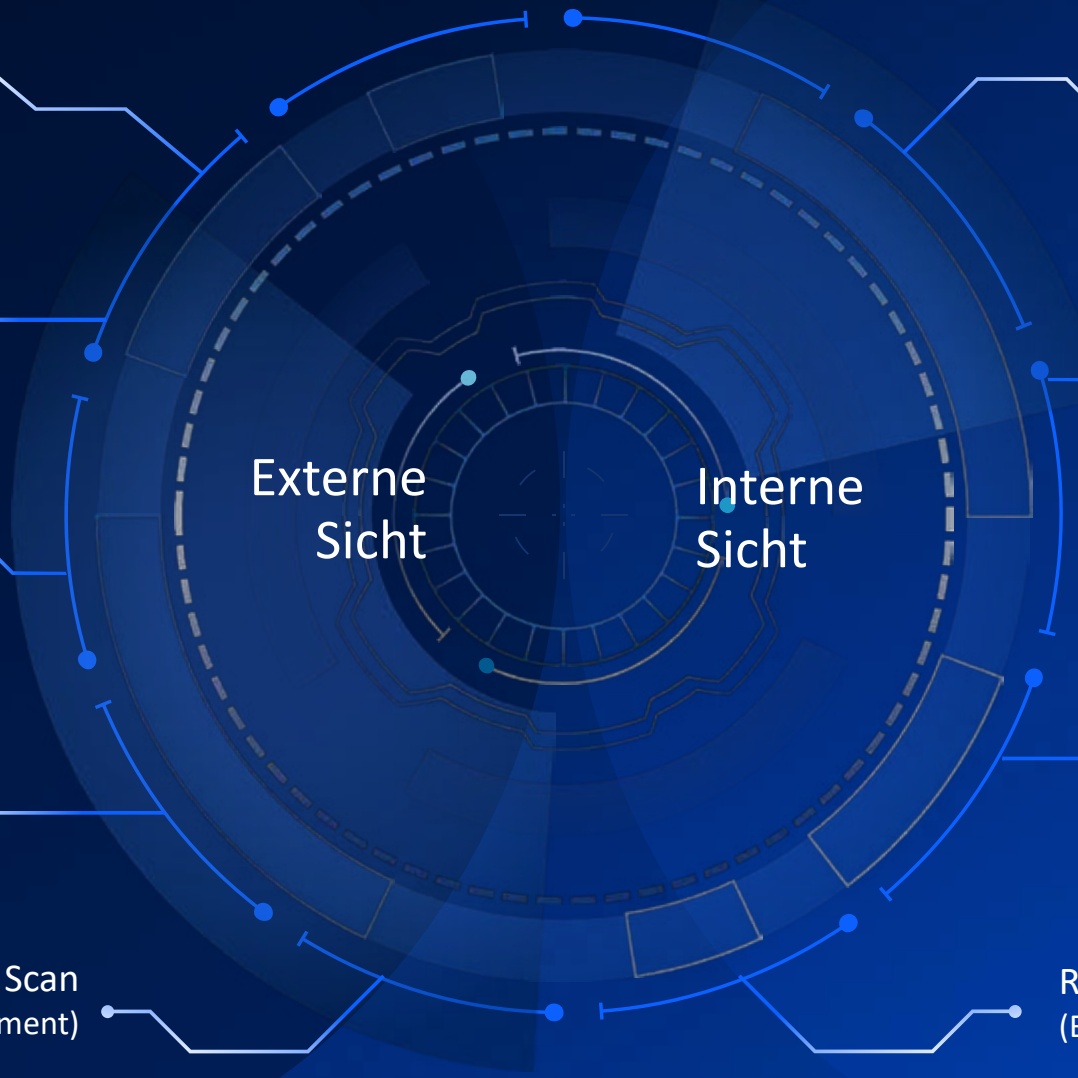
CENTRE FOR CYBERSECURITY BELGIUM

„Secutec weiß, was CTI-Feeds sind und wie man sie effizient einsetzt.“

Miguel De Bruycker, Generaldirektor CCB

SECUTEC Layer (externe Sicht)

Kunde / SOC (interne Sicht)



secureDNS – DNS Monitoring
(Black- und Whitelisting)

secureSIGHT – IP Monitoring
(Active Threat Hunting)

secureSIGHT – Darknet Monitoring
(Professional Darknet Monitoring)

secureSIGHT – M365 Risk Kit
(Phishing Detection / Risk Scan)

secure SIGHT – 24/7 Vulnerability Scan
(Attack Surface Management)

Firewall
(Firewall Segmentierung)

EDR/XDR Virenscanner
(Server und Endpoints)

SOC Log Monitoring
(Monitoring durch SOC/CDC)

Ransomware-sicheres Backup
(Backup-, Test- und Recovery Prozess)

Gesamtkonzept Cyber- und IT-Sicherheit

Agentur Cyberschutz Secutec

Ransomware DDoS

- Umfassend – ohne Lücken und Ausnahmen
- Gegen alle Angriffsvektoren
- Durchgehend – 24/7/52
- Automatisiert + Personaleinsatz
- Intern / extern
- Vorbereitung Schadensfall

Betrug Erpressung

Angriffsvektoren:

- VPN / Fernzugriffe
- CVE
- Keylogger
- Phishing
- M365 Account Hacking
- fehlendes Patchmanagement

Unsere Kooperation zu ihrer Cyber- und IT-Sicherheit

Agentur Cyberschutz Secutec

Secutec
Cybersecurity Intelligence

- **secureDNS**
  24/7 Überwachung aller DNS-Verbindungen inkl. Blocking & Alerting
- **secureSIGHT – Darknet Monitoring**
  aktives DARKNET Monitoring: Darknet, Foren, Chats und Marktplätze
- **secureSIGHT – Active Managed Threat Hunting**
  Permanente Überwachung der nicht geblockten Firewall Logs
- **secureSIGHT – Attack Surface Management**
  permanentes, aktives Monitoring von Domains, Brands und Public IP-Adressen auf Basis eines Vulnerability Scans
- **secureSIGHT – M365 Security Kit**
  leistungsstarke Lösung, die automatisch und kontinuierlich Sicherheitsprüfungen auf Basis anerkannter Best-Practice-Standards durchführt & integrierte M365 Phishing Detection

Agentur Cyberschutz

- **Angebotserstellung**
  Für Testmonate POCs und laufende Services
- **Onboarding**
  Unterstützung und Durchführung des Onboarding-Prozesses
- **Support im laufenden Service**
  Alertings, Unterstützung im laufenden Service bei vermeintlichen Bedienfehlern und diversen, sonstigen Hilfestellungen
- **Regelmäßige Nachbetreuung**
  Nachbetreuung über Webinare, Podcasts, Vorträgen und regelmäßigen Informationsveranstaltungen
- **Zusatzleistungen**
  weitere bis zu 30 Cybersicherheitslösungen inkl. vollwertigen Incident Response Service Team, Cybercrime & Darknet Vorträge und Vieles mehr

Unser Angebot:

Agentur Cyberschutz Secutec

- Webinar
- Cybercrime & Solutions UB – MS Teams
- POCs – Testphasen
- DARKNET Übersichtsreport