
tems
Secutec
Cyber security intelligence

tems

Secutec
Cyber security intelligence

Geert Baudewijns
CEO & Founder

Secutec wurde 2005 gründete mit der Vision, weltweites Wissen über Bedrohungen in einer Technologie zu bündeln.

Wir arbeiten für Behörden und Organisationen weltweit und haben Erfahrung aus über 300 Verhandlungen mit Hacker Organisationen.

- ✓ Führender europäischer Cybercrime Negotiater
- ✓ Organisationen wie Europol, Secret Services, diverse CERTs
- ✓ Cyber-SOC / Forensiker, Analysten, Fraud Spezialisten

tems

Secutec
Cyber security intelligence

secureDNS

Secutec Plattform zur Analyse und effizientem Schutz des DNS-Datenverkehr.

secureSIGHT

Cyber Threat Intelligence Plattform zum permanenten Monitoring von Cyber Risiken.

secureRESPONSE

Hochspezialisierter Incident Response Service von der Forensik bis hin zur Verhandlungsführung mit Hackern.

tems

Secutec
Cyber security intelligence

EXTERNES SECURITY TEAM

Secutec Managed-Services fokussieren auf die Sicht eines externen Angreifers/Hackers.

DNS Security Plattform

Vulnerability Monitoring

Darkweb Monitoring

Active Threat Hunting

Penetration Attack Simulation

Cyber SOC Service

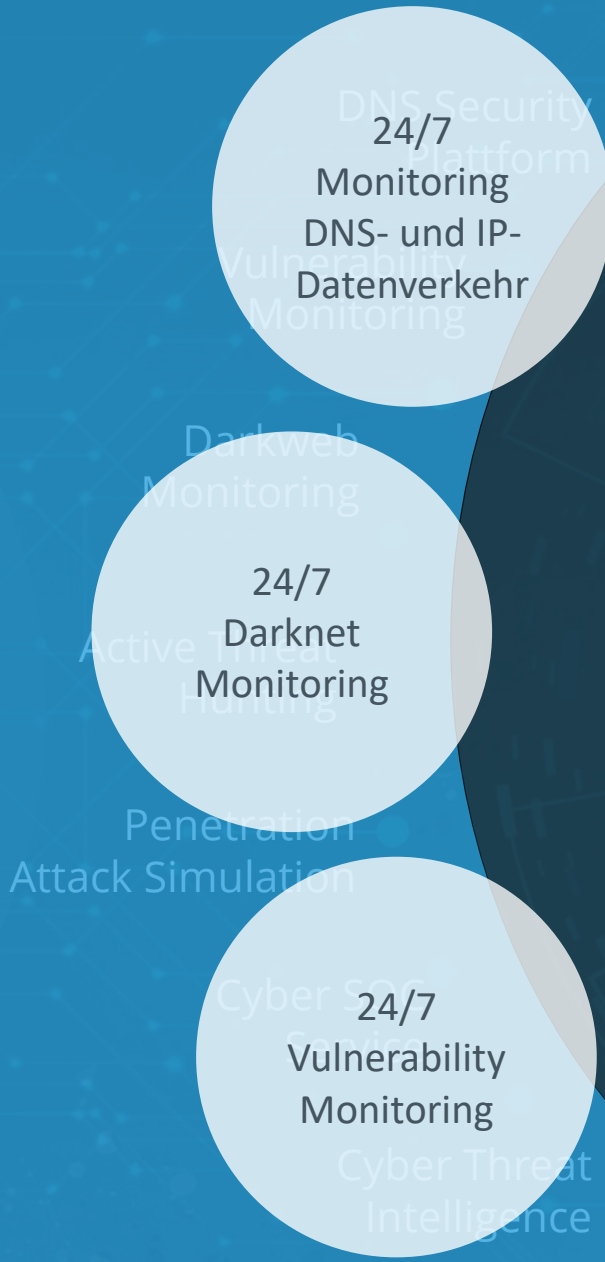
Cyber Threat Intelligence

Ihr IT-Team / Dienstleister haben die interne Sicht auf Ihre Infrastruktur.

EXTERNES SECURITY TEAM

Externe Sicht

Unsere Managed-Services fokussieren auf die Sicht eines externen Angreifers/Hackers.



Interne Sicht

Ihr IT-Team / Dienstleister haben die interne Sicht auf Ihre Infrastruktur.


tems
Secutec
Cyber security intelligence
“Darknet & Co.”

4%

Clear Web

-Internet, wie wir es kennen

-Sichtbar für alle Benutzer

-Erreichbar über Google & Co.

96%

Deep Web

-Zugriffsbeschränkte oder nicht indexierte Webseiten

-Datenbanken, Webseiten und Dienste von Regierungen, Organisationen oder Universitäten

Darknet

-Über “normale” Wege nicht auffindbare Webseiten

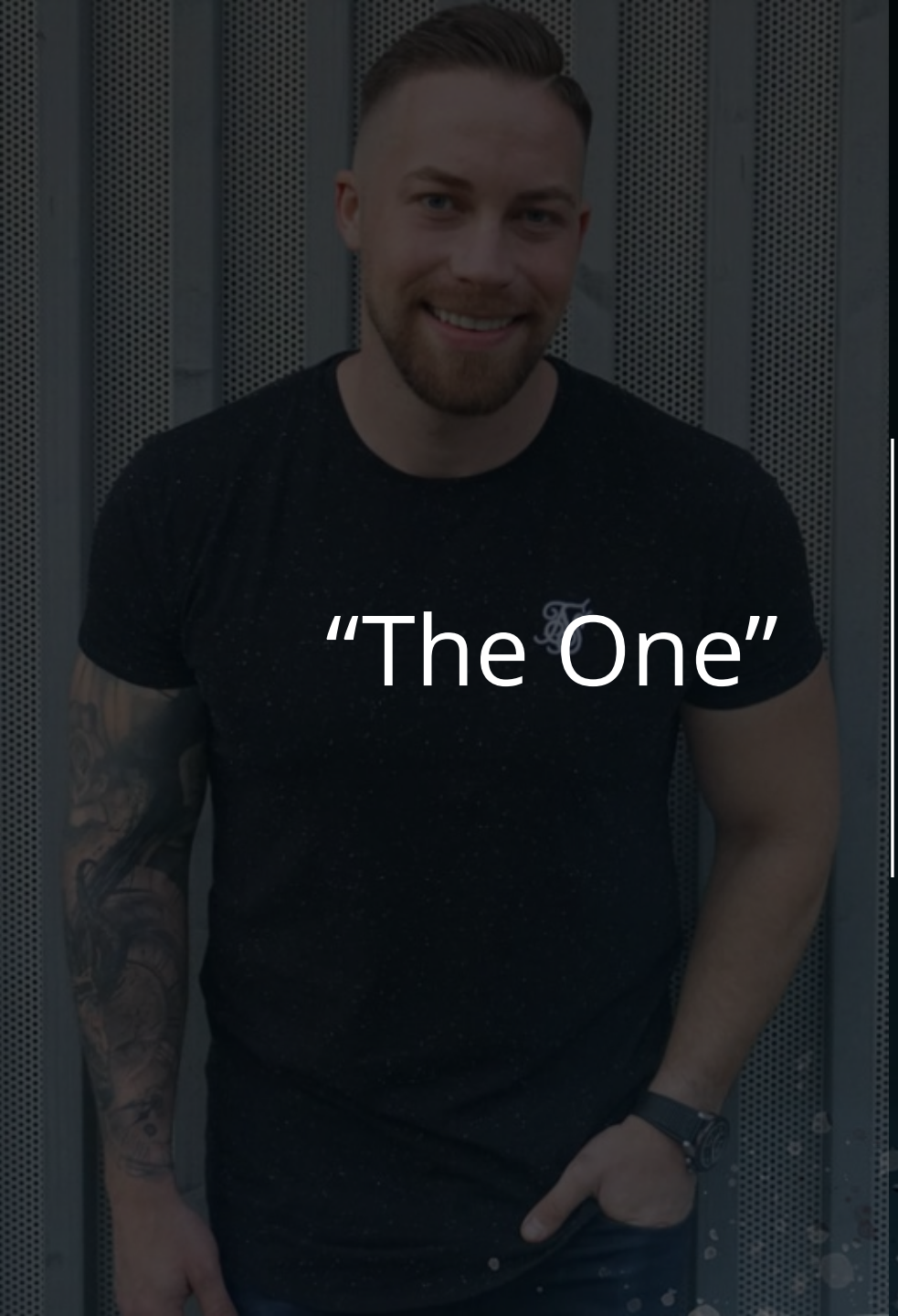
-Verschlüsselte Komminkation

-Betreiber und Besucher möchten anonym bleiben

-Illegaler Inhalt, politischer Protest, geheime Kommunikation

- Russisches Darknet
- Persisches Darknet
- Englisches Darknet
- Chinesisches Darknet

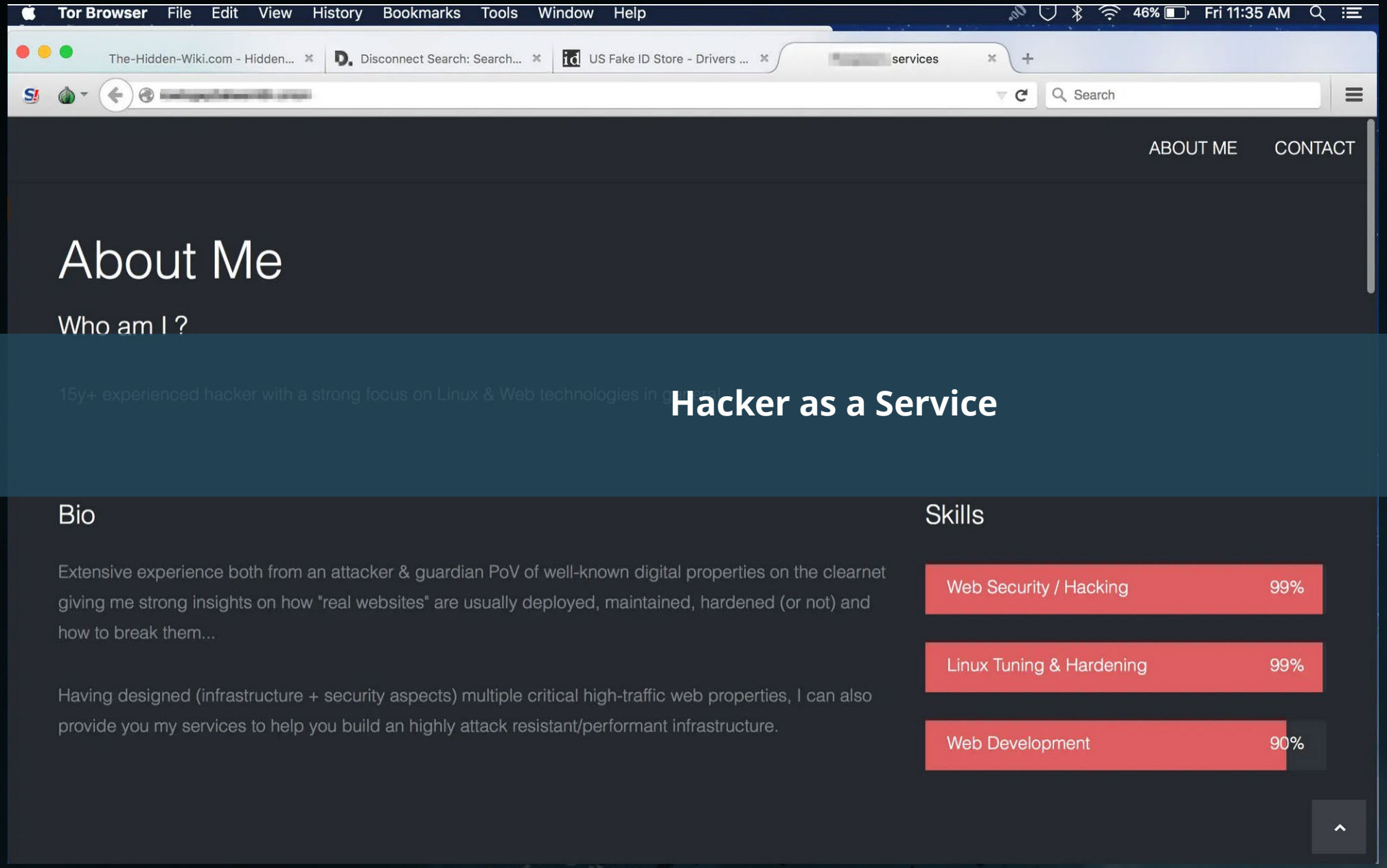
Rund 150 bekannte Schwarzmärkte – 2,2 Mio. tägliche Darknet User



“The One”

Martin Frost
Wall Street Market

- März 2016 bis 02.05.2019
- 100 Mio. Euro Umsatz / 63.000 Angebote
  5.400 Verkäufer / 1,2 Mio. Kundenkonten
- Unterirdisches Rechenzentrum im Cyber Bunker der Kaserne Mont Royal (Rheinland Pfalz)
- Exit Scam am 23.04.2019
  Probleme bei der VPN Verschlüsselung und Bitcoin Transaktionen führten zur Verhaftung durch Europol, FBI und das BKA



Hacker as a Service

Secutec
Cyber security intelligence

Secutec
Cyber security intelligence

Dark Web Hackers

Products | Register | Login

Welcome to the Dark Web Hackers

Have you tried to buy hacking services on the dark web before? Not happy with the results? Only empty promises but no one getting the job done?

Then you should try Vladimir and George, the dark webs most trusted hackers for getting things done.

Unlike others, our prices are not the cheapest, but if we can't do a job, you will get a full refund!

Hacker as a Service

Vladimir

Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up.
I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.
Here you can find a list of my services, if it is not listed, then minimum price will be $600 and we will discuss the final price once you gave me all information and i accept the job.

Secutec
Cyber security intelligence

Hacker as a Service

Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.09353 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.04676 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.02078 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.06755 ฿	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.49361 ฿	1 X Buy now
Other services, final price will be discussed	600 USD = 0.03118 ฿	1 X Buy now
Only additionaly: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.12990 ฿	1 X Buy now

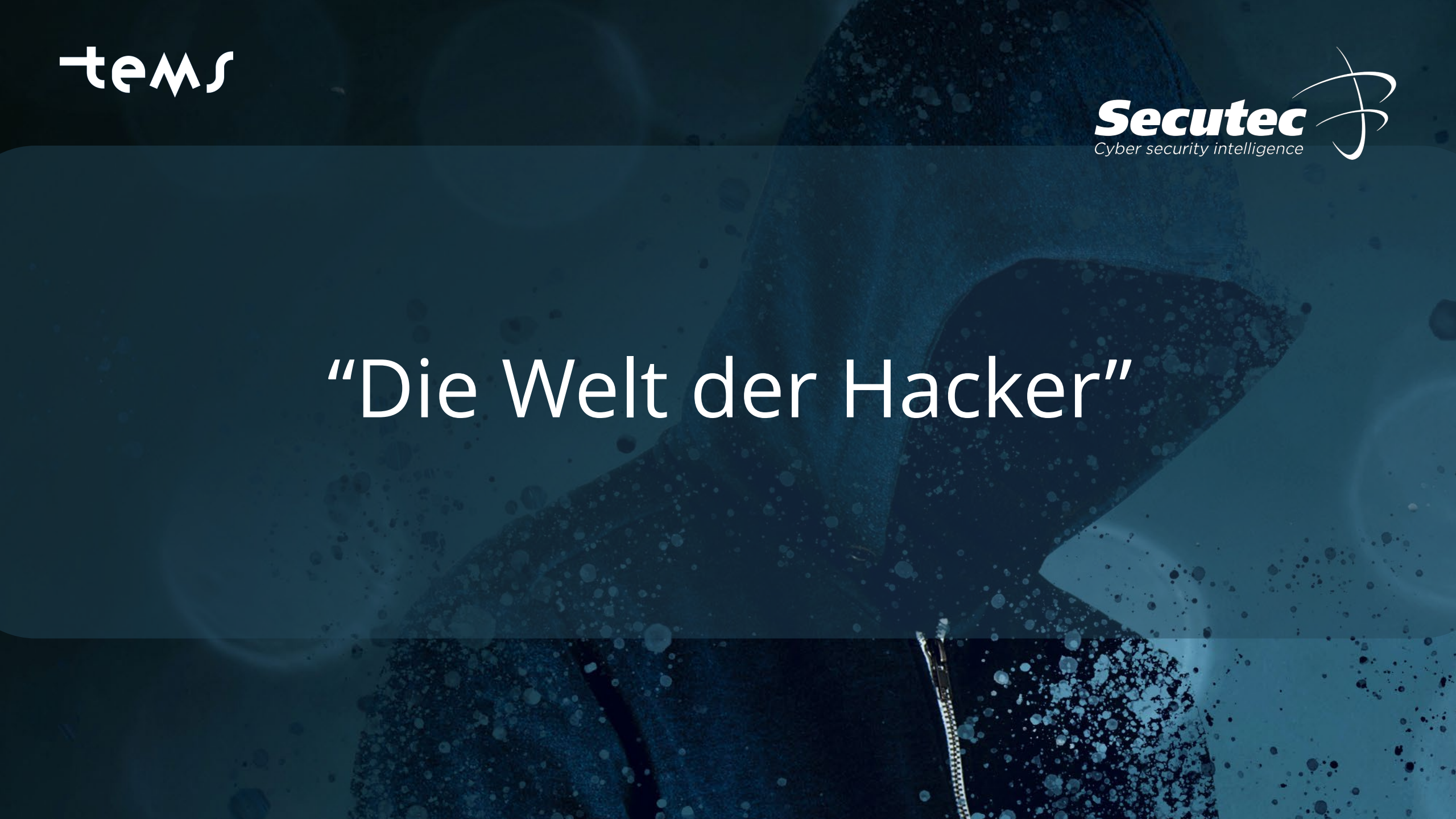
Secutec
Cyber security intelligence

George

Hello, my name is George.
My hacking skills are not as perfect as Vladimir's, but i am really good with social engineering.
And i really like messing with people, i don't care what you want to do to them.
If there is something i can't do then Vladimir will help and teach me for next time.

Hacker as a Service

Product	Price	Quantity
Destroying someones life: Your target will have legal problems or financial problems, proven methods including child porn that always works	1700 USD = 0.08833 ฿	1 X Buy now
Spreading false information about someone on social media, not as life ruining but still nasty	450 USD = 0.02338 ฿	1 X Buy now
Social engineering to get secrets from a person, private or from some employee	450 USD = 0.02338 ฿	1 X Buy now


tems
Secutec
Cyber security intelligence
“Die Welt der Hacker”

tems

Secutec
Cyber security intelligence

Wirtschaftlichen Hacker Gruppen

Lockbit, BlackCat, Play, …

Weltweit 80 professionelle Hacker Gruppe, die Unternehmen angreifen, um Lösegeld zu erpressen.

ZIELE: Lösegeld erpressen

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

Politisch motivierte Einzelhacker und Gruppen

Anonymous
Hacktivismus - als Protestmittel, um politische und ideologische Ziele zu erreichen.

NoName057(16), Killnet
Pro russische Hackergruppen, die gezielt westliche Organisationen angreifen.

ZIELE: Politische und Ideologische Ziele erreichen

Fakten

-Es gibt weltweit rund 80 Hacker Organisationen.

-Der Umsatz der großen Hacker Gruppe
REvil 150 Mio., HIVE 100 Mio.

-Der Zeitraum vom Initial Access bis zur Verschlüsselung wird deutlich kürzer und dauert oft nur 1-2 Wochen.

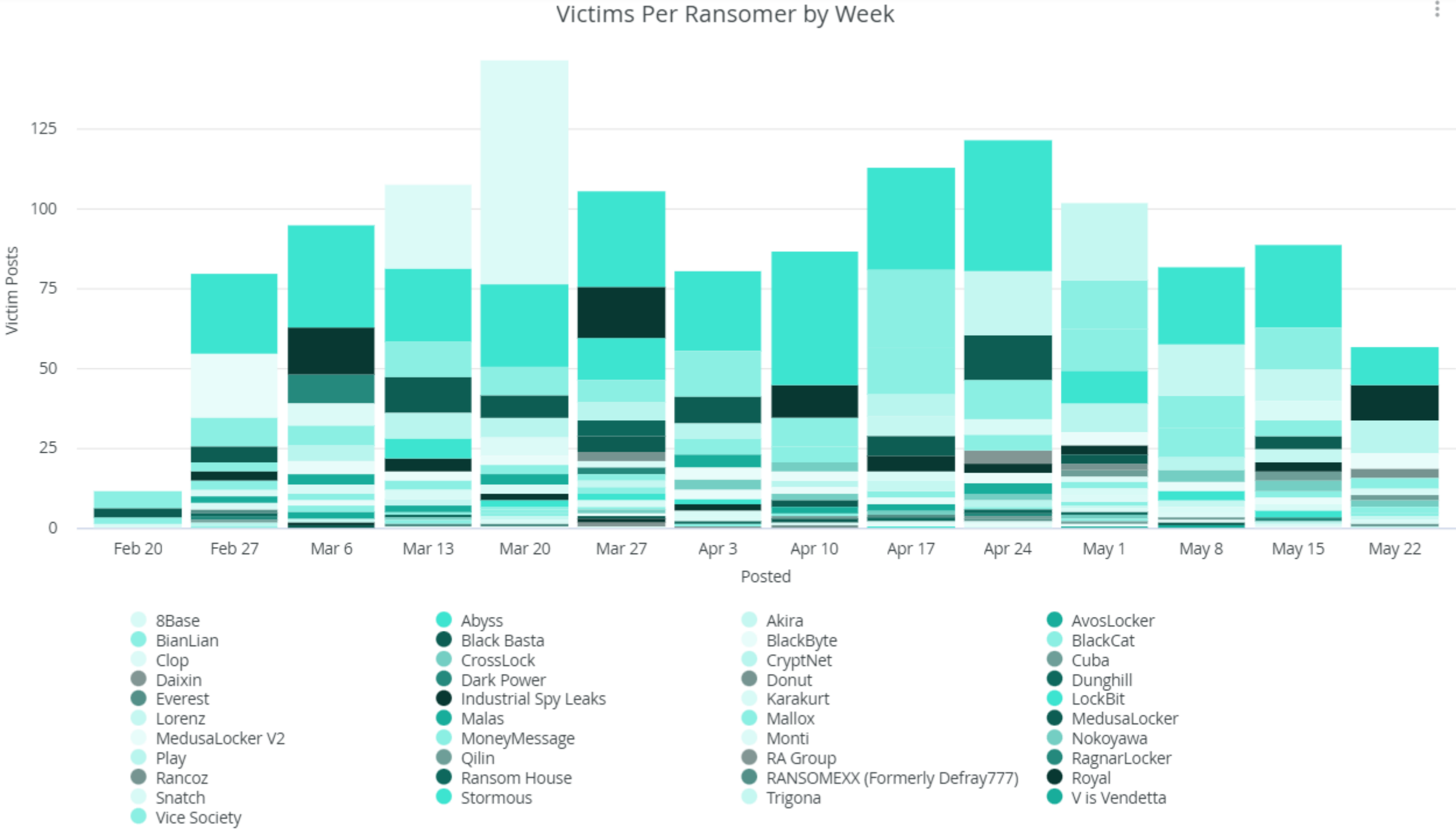
-Für die Verschlüsselung von 100GB Daten benötigt die LOCKBIT 2.0 Ransomware 4 min. 28 Sekunden

1,292

Victim Count

Victim Activity

	Title	Ransomer Name	Posted	Last Observed	Last Updated
1	CentroMed	Karakurt	2023-06-29 00:00...	2023-06-29 05:19...	2023-06-29 05:19...
2	KLGATES.COM	Clop	2023-06-28 22:13...	2023-06-29 00:17...	2023-06-28 22:13...
3	stimgroup.it	LockBit	2023-06-28 17:42...	2023-06-29 05:20...	2023-06-29 05:20...
4	aimtron.com	LockBit	2023-06-28 17:41...	2023-06-29 05:20...	2023-06-28 18:09...
5	ibafrance.fr	LockBit	2023-06-28 17:39...	2023-06-29 05:20...	2023-06-29 05:20...
6	JBCC Corp	Mallox	2023-06-28 09:40...	2023-06-29 05:17...	2023-06-28 07:07...
7	Coachella Valley C...	BlackCat	2023-06-28 08:47...	2023-06-29 05:16...	2023-06-28 10:16...
8	GraphTec	Black Basta	2023-06-28 08:28...	2023-06-29 05:27...	2023-06-28 08:28...
9	SHO	Black Basta	2023-06-28 07:29...	2023-06-29 05:28...	2023-06-28 07:29...
10	TLG_2	Black Basta	2023-06-28 07:28...	2023-06-29 05:28...	2023-06-28 07:28...
11	SANOCHEMIA Ph...	Black Basta	2023-06-28 07:28...	2023-06-29 05:27...	2023-06-28 07:28...


Victims Per Ransomer by Week
Victim Posts
125
100
75
50
25
0
Feb 20
Feb 27
Mar 6
Mar 13
Mar 20
Mar 27
Apr 3
Apr 10
Apr 17
Apr 24
May 1
May 8
May 15
May 22
Posted
8Base
BianLian
Clop
Daixin
Everest
Lorenz
MedusaLocker V2
Play
Rancoz
Snatch
Vice Society
Abyss
Black Basta
CrossLock
Dark Power
Industrial Spy Leaks
Malas
MoneyMessage
Qilin
Ransom House
Stormous
Akira
BlackByte
CryptNet
Donut
Karakurt
Mallox
Monti
RA Group
RANSOMEXX (Formerly Defray777)
Trigona
AvosLocker
BlackCat
Cuba
Dunghill
LockBit
MedusaLocker
Nokoyawa
RagnarLocker
Royal
V is Vendetta

Top Ten Ransomware Groups

	Ransomer Name	Victim Posts
1	LockBit	983
2	BlackCat	360
3	Black Basta	219
4	Royal	202
5	BianLian	181
6	Clop	127
7	Play	121
8	Karakurt	118
9	Vice Society	107
10	Hive	92

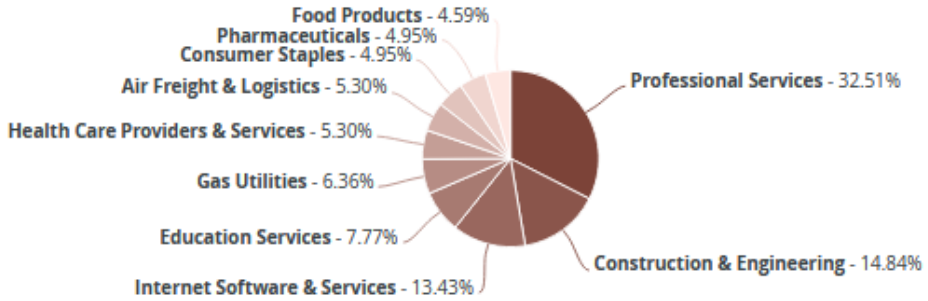

Svalbard
Greenland
Iceland
Sweden
Norway
Russia
Canada
United Kingdom
Belarus
Ukraine
France
Kazakhstan
Mongolia
Spain
Italy
Uzbekistan
Turkey
China
Japan
United States
Morocco
Tunisia
Iraq
Iran
Pakistan
Nepal
Libya
Egypt
Saudi Arabia
Oman
India
Mexico
Cuba
Senegal
Mali
Niger
Yemen
Thailand
Philippines
Sudan
Sri Lanka
Cameroon
Malaysia
Colombia
Kenya
Indonesia
Tanzania
Papua New Guinea
Peru
Brazil
Angola
Bolivia
Madagascar
Namibia
Paraguay
Australia
South Africa
North Atlantic Ocean
South Atlantic
Indian Ocean

Ransomware

Ransomer Name: is any value | Victim Industry: is any value | Victim Country: is any value | Posted Date: 2021/01/01 - 2021/03/31

	Title	Victim Domain	Ransomer Name
1	PRESTIGE MEDICAL GROUP	prestigemedicalgroup.org	Avaddon
2	Ghana National Gas	https://www.ghanagas.com.gh/	Prometheus
3	Henry Brick	henrybrick.com	LV Two
4	DBMSC Steel	www.dbmscsteelfzco.com	Avaddon
5	boggi.com	boggi.com	Ragnarok
6	Consiglio Nazionale del Notariato	www.notariato.it	RANSOMEXX (Formerly Defray777)

Top Ten Targeted Industries



Top Ten Ransomware Groups

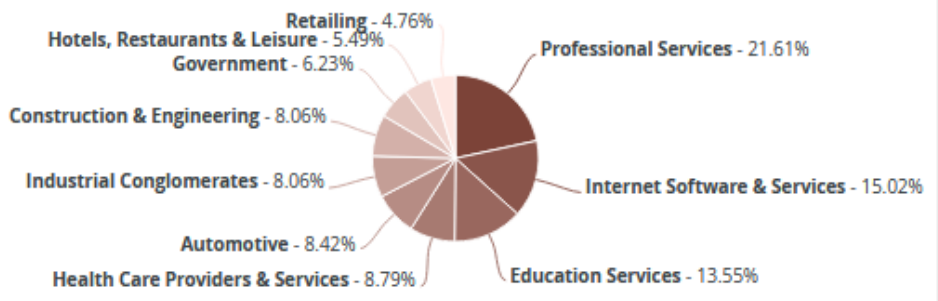
	Ransomer Name	Victim Posts
1	Conti	110
2	DarkSide	87
3	Pysa	72
4	Avaddon	54
5	Sodinokibi	46
6	DoppelPaymer	40
7	Clop	32
8	Nefilim	30
9	Ragnarok	28

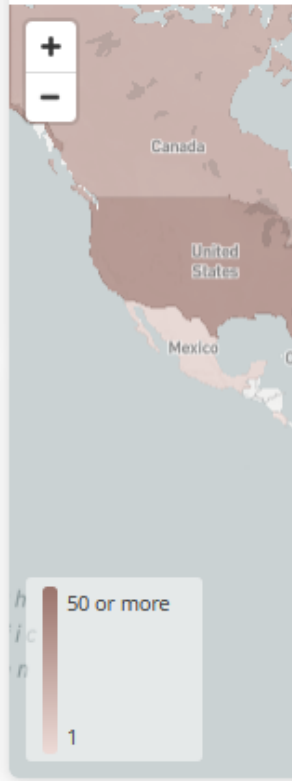
Ransomware

Ransomer Name: is any value | Victim Industry: is any value | Victim Country: is any value | Posted Date: 2022/11/01 - 2023/01/18

	Title	Victim Domain	Ransomer Name
1	carinya	www.carinya.nsw.edu.au	Royal
2	Livingston	www.livingstonintl.com	Royal
3	University of Duisburg-Essen	www.uni-due.de	Vice Society
4	politriz.ind.br	politriz.ind.br	LockBit
5	melody.com.tr	melody.com.tr	LockBit
6	R C Stevens Construction	rcstevens.com	Hive

Top Ten Targeted Industries





Top Ten Ransomware Groups

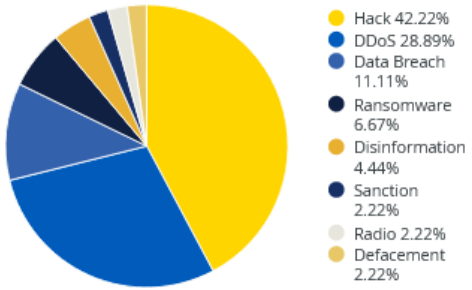
	Ransomer Name	Victim Posts
1	LockBit	113
2	BlackCat	65
3	Royal	63
4	Play	48
5	Karakurt	32
6	Vice Society	30
7	Hive	29
8	Black Basta	26
9	BianLian	25

Aktuelle Hacker Aktivitäten im Russland/Ukraine Konflikt

Ukraine Crisis

10m ago

Attack Types



Possible Threat Actor Locations

The possible location of each threat actor group has been determined either by statements mad...

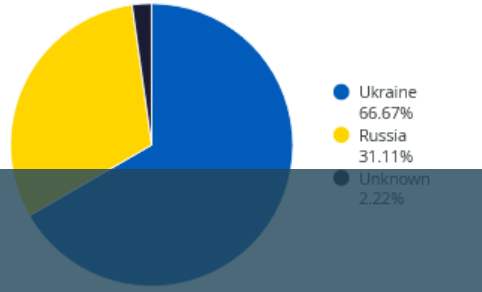
Intelligence Reports and Collab Calls

Last Updated	Title
2022-06-29	Killnet, Kaliningrad, and Lithuania's Transport Standoff With Russia
2022-06-16	Tactical Update, Day 113: Russia's War on Ukraine
2022-05-25	Tactical Update, Day 91: Russia's War on Ukraine

FP Collab Posts

Collab Date	Collab Title
2022-03-24	DOJ Unseals Indictments on Russian Nationals Targeting Energy Sector
2022-03-16	CISA Reports Russian State Sponsored Actors Leverage Vulnerability "PrintNightmare"
2022-03-14	2022 Russian Invasion of Ukraine Update: March 12 - 14, 2022

Threat Actor Affiliation



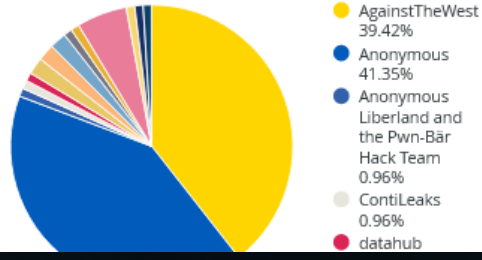
Number of IOCs

No results

Threat Actor Telegram Channels

Name	Support
/CIG/ Telegram | Counter I...	Ukraine
#Армянский_Z_Дворик	Russia
#КНПУ	Ukraine
Борода вещает Z	Russia
Майор и Генерал	Russia
Дети Арбата Z	Russia
В'ячеслав Чаус/ Черніг...	Ukraine
Віталій Бунечко – голо...	Ukraine
Віталій Коваль / Рівнен...	Ukraine
Геннадій Лагута/ Херсо...	Ukraine

Leaks by Groups



IOCs over Time

No results

IOCs

Date	Type of IOC	Event Title	Ioc Value
2022-05-24	sha256	Observation: SaintBear OSINT 2022 [2022-05-24...	c1afb561cd5363ac5826ce7a72f0055b40...
2022-05-24	sha256	Observation: SaintBear OSINT 2022 [2022-05-24...	c83d8b36402639ea3f1ad5d48edc1a220...
2022-05-24	sha256	Observation: SaintBear OSINT 2022 [2022-05-24...	99a2b79a4231806d4979aa017ff7e8b80...
2022-05-24	sha256	Observation: SaintBear OSINT 2022 [2022-05-24...	8ffe7f2eeb0cbfbe158b77bbff3e0055d2...
2022-05-24	sha256	Observation: SaintBear OSINT 2022 [2022-05-24...	9e9fa8b3b0a59762b429853a36674608...
2022-05-24	ip-dst	Observation: SaintBear OSINT 2022 [2022-05-24...	194.31.98.124
2022-03-23	sha256	Observation: DoubleZero Wiper Targets Ukraine...	3b2e708eaa4744c76a633391cf2c983f4a...
2022-03-23	sha256	Observation: DoubleZero Wiper Targets Ukraine...	8dd8b9bd94de1e72f0c400c5f32dcefc11...

hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion 80%

HiveLeaks

BHARBERT

BL Harbert International is a privately-owned construct ion company with U.S. and international operations. He adquartered in Birmingham & USA

Website
www.blharbert.com

Revenue
$974M

Employees
7 611

Encrypted at

5 September 2022

12:16:30

Disclosed at

21 September 2022 19:25:30

Share

Disclosed Links 1 link

hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion 80%

Website
www.isr.tecnico.ulisboa.pt

Revenue
$10M

Employees
57

Disclosed at
2 December 2021 • 19:57:30

MediaMarkt

Founded in 2016 and headquartered in Zurich, Switzerl and, MediaMarktSaturn Retail Group is a retail compan y for consumer electronics

Website
www.mediamarktsaturn.com

Revenue
$240 000M

Employees
53 000

Encrypted at
8 November 2021
00:47:30

Disclosed at
1 December 2021 • 16:26:00

Share

Drake & Scull

Encrypted at

LOCKBIT 3.0

LEAKED DATA

TWITTER
CONTACT US
AFFILIATE RULES
HOW TO BUY BITCOIN
PRESS ABOUT US
MIRRORS

lafondasantafe.com

12D 09h 10m 39s

Each year, La Fonda proves itself of being among the top Santa Fe luxury hotels

Updated: 06 Sep, 2022, 01:51 UTC 38

gavresorts.com.br

14D 11h 11m 23s

GAV Resorts is a company specializing in high-end resorts.

Updated: 06 Sep, 2022, 01:52 UTC 35

pdh.com.tw

11D 22h 57m 35s

Rottley Tile has more than 35 years of experience and professional service team, all kinds of tile questions are happy to answer for you, your inquiries are our honor.

Updated: 05 Sep, 2022, 15:38 UTC 143

monnensenpartners.be

11D 22h 54m 39s

Your partner in accounting, taxation and advice Our accountants and advisors help you with personal and professional growth and work on the well-being and future goals of

Updated: 05 Sep, 2022, 15:39 UTC 168

sbr-zwiesel.de

9D 20h 45m 56s

The company SBR - Stahlbau Regenhütte GmbH - based in Zwiesel is a future-oriented and high-performing medium-sized family company, which manufactures complete

Updated: 05 Sep, 2022, 15:26 UTC 129

finnco.eu

9D 20h 06m 25s

Finnco-altec is a company that operates in the Packaging and Containers industry. It employs 21-50 people.

Updated: 05 Sep, 2022, 14:47 UTC 158

sportscity.com.tw

11D 02h 03m 45s

As a clothing manufacturer for over 30 years, SCI has witnessed the development of the garment industry in Taiwan. We are fully aware that talent is the key to a company's

Updated: 05 Sep, 2022, 14:44 UTC 143

kamut.com

7D 15h 33m 28s

We have three main activities at KEE. We organize the promotion and protection of the KAMUT(R) tradename in the European Union. We also coordinate a research program

Updated: 05 Sep, 2022, 12:14 UTC 173

divultec.pt

11D 19h 20m 55s

www3.comune.gorizia.it

9D 07h 01m 08s

eneva.com.br

13D 19h 37m 32s

floresfunza.com

13D 22h 45m 54s

UNTIL FILES

23H50M02S

PUBLICATION

Deadline: 26 Sep, 2022 15:07:28 UTC

Parrott Sims & McInnis PLLC

parrottsims.com

We are a full-service law firm providing our clients with superior legal services by leveraging our resources and personnel to deliver timely legal advice...

Phone: +1 832-485-6000

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 21 SEP, 2022 15:07 UTC **UPDATED:** 25 SEP, 2022 00:19 UTC

Until the files will be available left

23h 50m 02s

*Download archive *Download files tree

AFFILIATE RULES

Das älteste internationale [Ransomware] LockBit-Partnerprogramm heißt Sie willkommen.

Wir sind in den Niederlanden ansässig, völlig unpolitisch und nur an Geld interessiert.
Wir haben immer eine unbegrenzte Anzahl von Affiliates, genug Platz für alle Profis. Es spielt keine Rolle, in welchem Land Sie leben, welche Sprache Sie sprechen, welches Alter Sie haben, an welche Religion Sie glauben, jeder auf der Welt kann zu jeder Zeit des Jahres mit uns zusammenarbeiten.

Cybergang Lockbit entschuldigt sich für Angriff auf Kinderkrankenhaus

Lockbit-Regelverstoß

Zum Jahreswechsel hat die Lockbit-Cybergang das Entschlüsselungstool für das Krankenhaus kostenlos freigegeben und sich für den Angriff entschuldigt. "Wir entschuldigen uns in aller Form für den Angriff auf sickkids.ca und geben den Decryptor kostenlos heraus. Der Partner, der dieses Krankenhaus angegriffen hat, hat gegen unsere Regeln verstoßen, ist blockiert und ist nicht mehr in unserem Partnerprogramm", schreiben die Cyberkriminellen auf ihrer Darknet-Webseite. Lockbit bietet Ransomware-as-a-Service an, ein kriminelles Geschäftsmodell.

FILES ARE PUBLISHED

Deadline: 29 Nov, 2022 22:26:02 UTC

continental.com

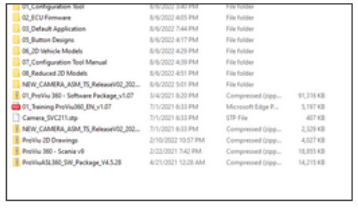
Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 40 million dollars, with a list of stolen files you can read here.

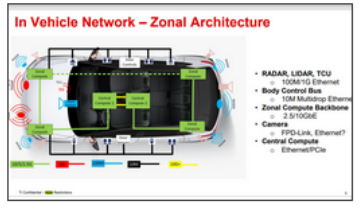
ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 02 NOV, 2022 15:45 UTC UPDATED: 07 APR, 2023 18:37 UTC

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 100	$ 40000000	$ 40000000

1-4 of 4





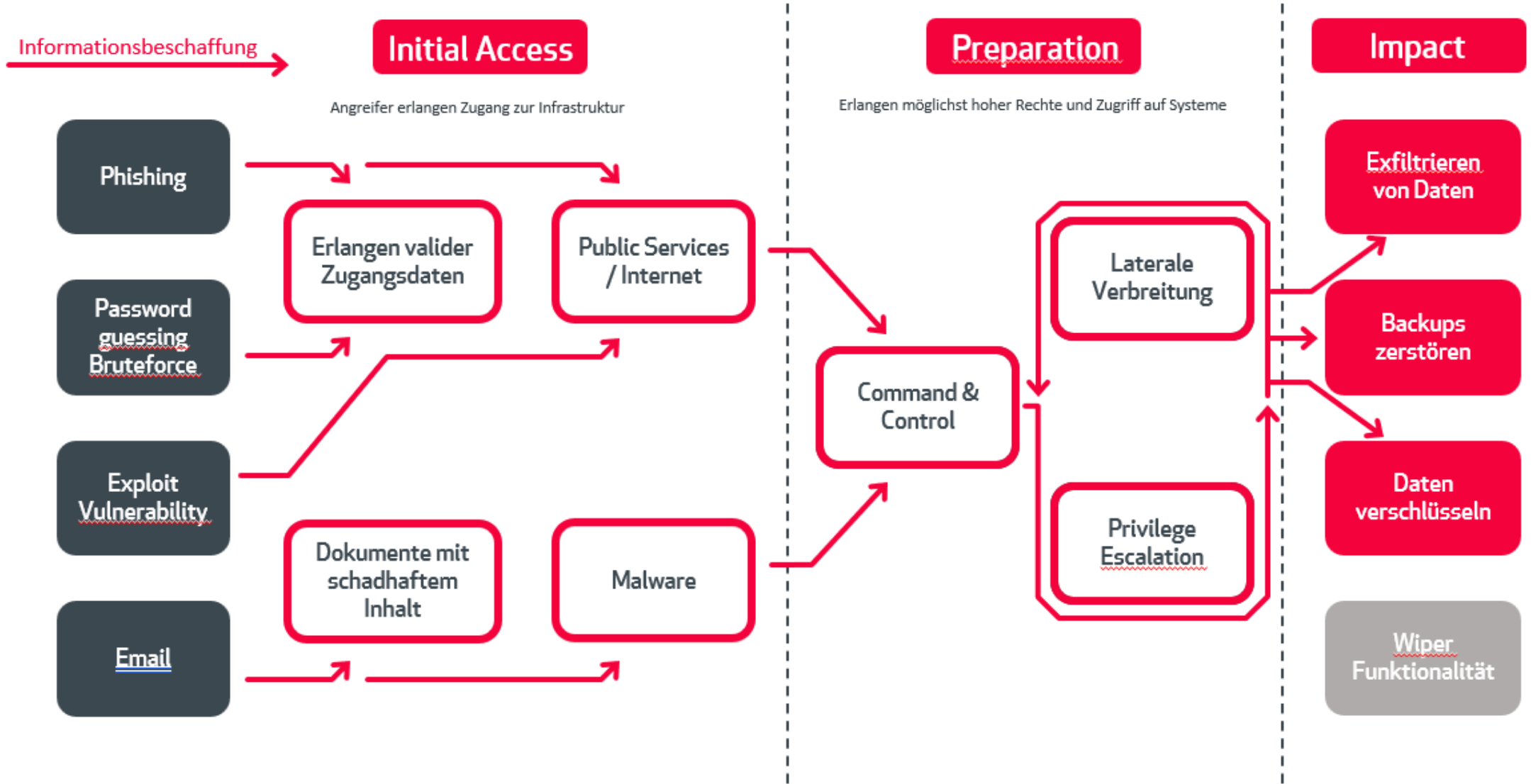
Cyber-Risiken Trends 2023

- Supply-Chain-Attacken
- Deep Fake (KI) / Deep Fake Audio-/Visuals
- Professionelle/Trendy Phishing Attacken
- Geopolitische Konflikte – Wiper Funktionalität
- Cyber-War-Klauseln in Versicherungsverträgen
  Geringe Deckungssummen
- 3,5 Mio. fehlende Cybersecurity Spezialisten


tems
Secutec
Cyber security intelligence
“Ransomware Attacke”

Lifecycle einer Ransomware Attacke

Secutec
Cyber security intelligence




tems
Secutec
Cyber security intelligence
User Session mittels Citrix
Attacke
31.01.
23:18 Uhr
RDP-Anmeldung Domaincontroller
02.02.
Start Daten Exfiltration 124GB über 29 Hosts
03:29 Uhr
04.02.
06:40 Uhr
Auffälligkeiten intern erkannt
Start der internen Alarmierungskette
04.02.
Server lokalisiert
Alle Admin Accounts kompromittiert
2 Standorte mit verschlüsselter VM
Notfallprotokoll gestartet
07:10 Uhr
04.02.
11:04 Uhr
Start Forensik Secutec
04.02.
Hacker RDP-Session vom kompromittieren Server übernommen
Nachmittag
04.02.
Abend
Deepweb Server der Hacker lokalisiert, 124GB gestohlenen Daten retour geholt
04.02.
KIRCHDORFER
GROUP

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

Lösegeld-forderungen

- In vielen Fällen deckt sich die Summe der liquiden Mittel eines Unternehmens mit der Lösegeldforderung der Hacker. Vermutlich sind die Bilanzen in vielen Fällen bekannt. Start Forderung meist 10% vom Umsatz.

- Argumente in der Verhandlung über nicht liquide Mittel werden oftmals mit aktuellen Bankauszügen durch die Hacker widerlegt.

Empfehlungen

-Monitoring des ausgehenden DNS Traffics
Auch IoT Devices beachten

-Externes Schwachstellen Monitoring
Aus Sicht eines externen Angreifers – Darknet/Vulnerabilities

-Vorbereitung auf einen Incident
Es gibt kein 100% Playbook, aber 70%

-Notfall Handbuch und Ransomware Playbook
Unterschiedliche Szenairen (Blackout, Hacker Attacke, ...)

-Multifaktor Authentifizierung
Hier Bedarf es neben dem Passwort eine weiteren Faktor für Hacker

Empfehlungen

-EDR/XDR – Endpoint Detection Response auf Server
Nur “Virenscanner” der next Generation können Gefahren erkennen.

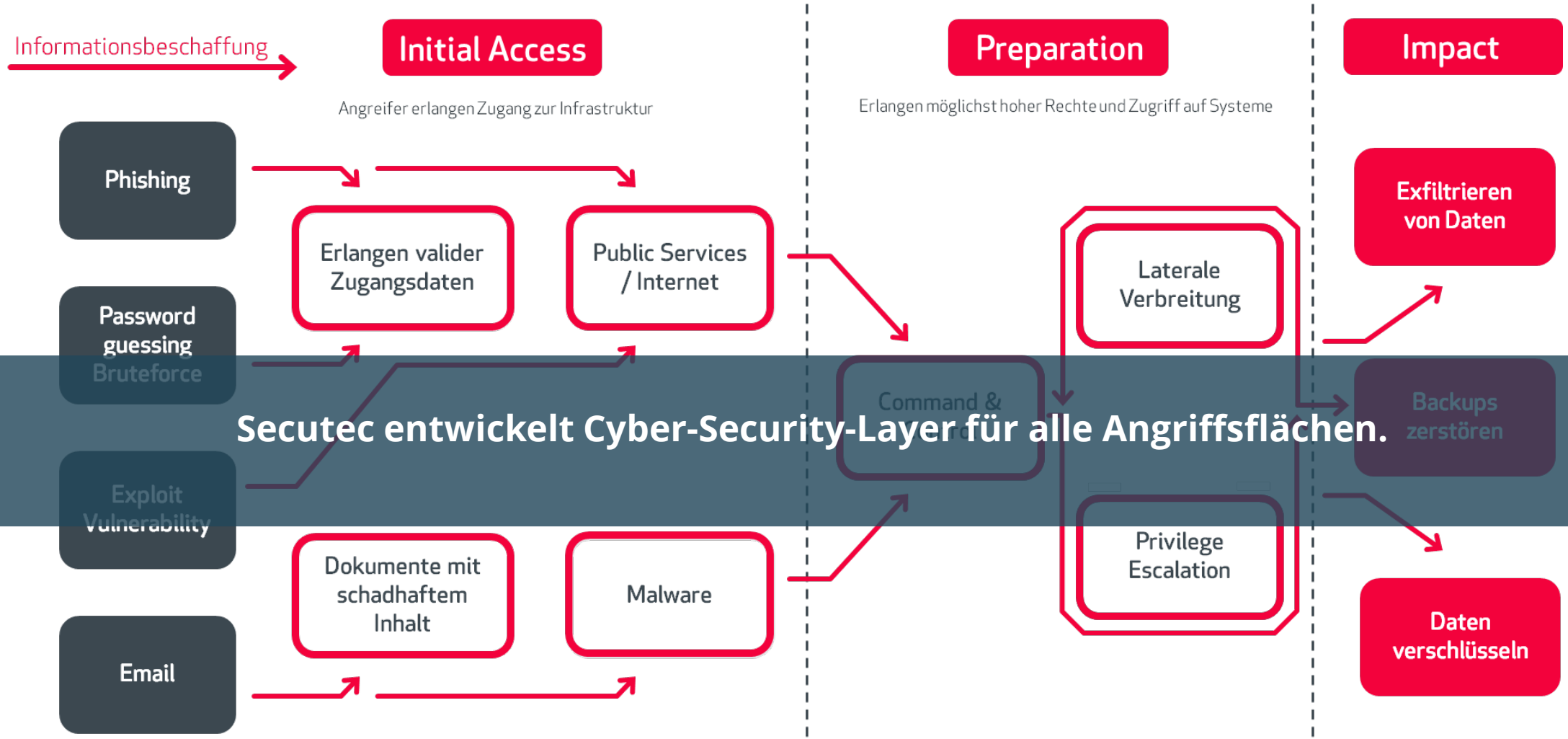
-Alternatives Linux Backup
Hacker gehen in der Regeln den einfach Weg

-Server Logs Backup
Je länger desto besser für die Forensik, min. 90 Tage

-Netzwerk (Mikro)Segmentierung
Netzwerk in kleinere, separate Subnetzwerke unterteilen

-Keine Admin Rechte auf lokalen Geräten
Wenn die Notwendigkeit besteht nur temporäre Rechte zulassen

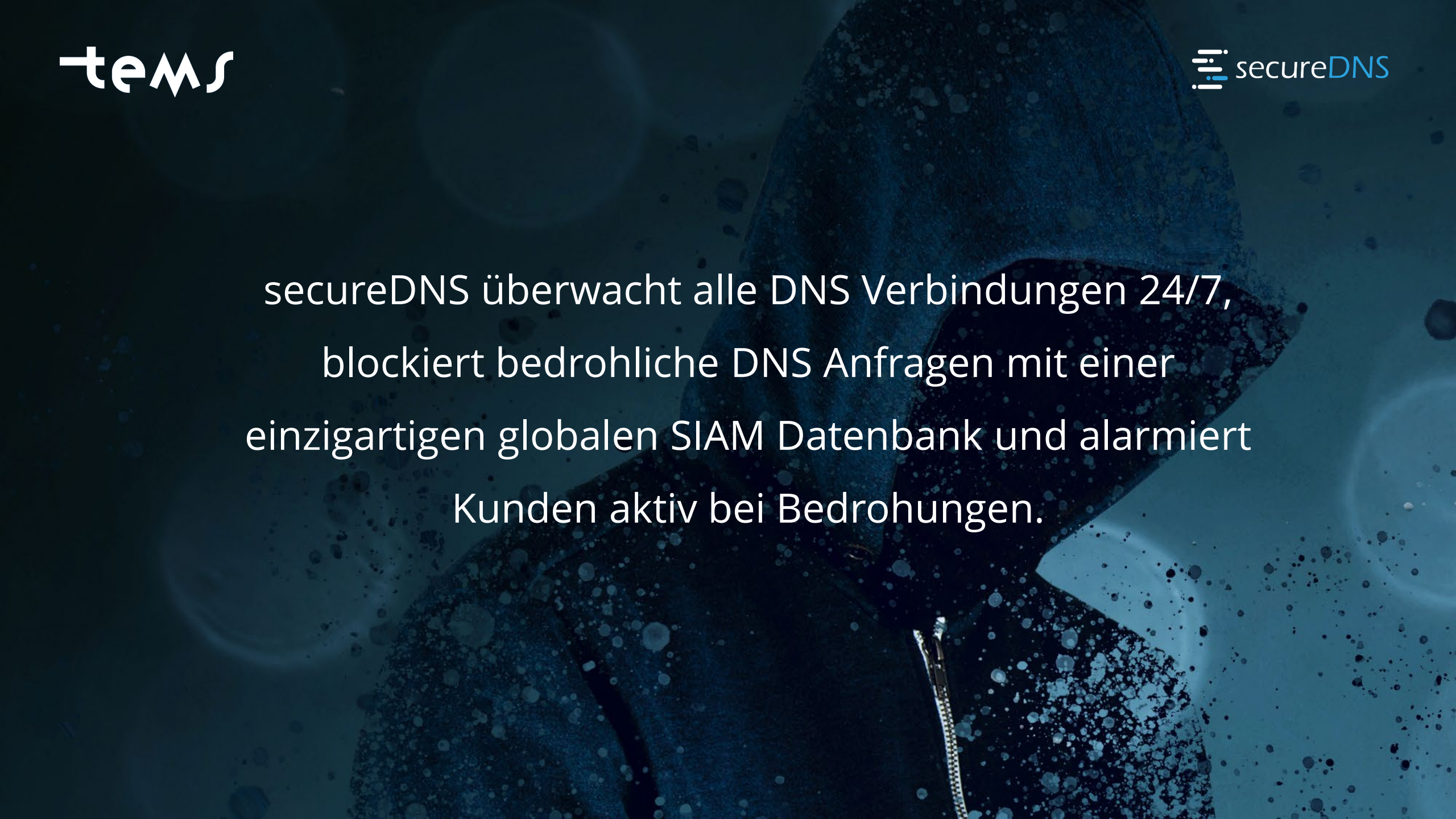
Lifecycle einer Ransomware Attacke

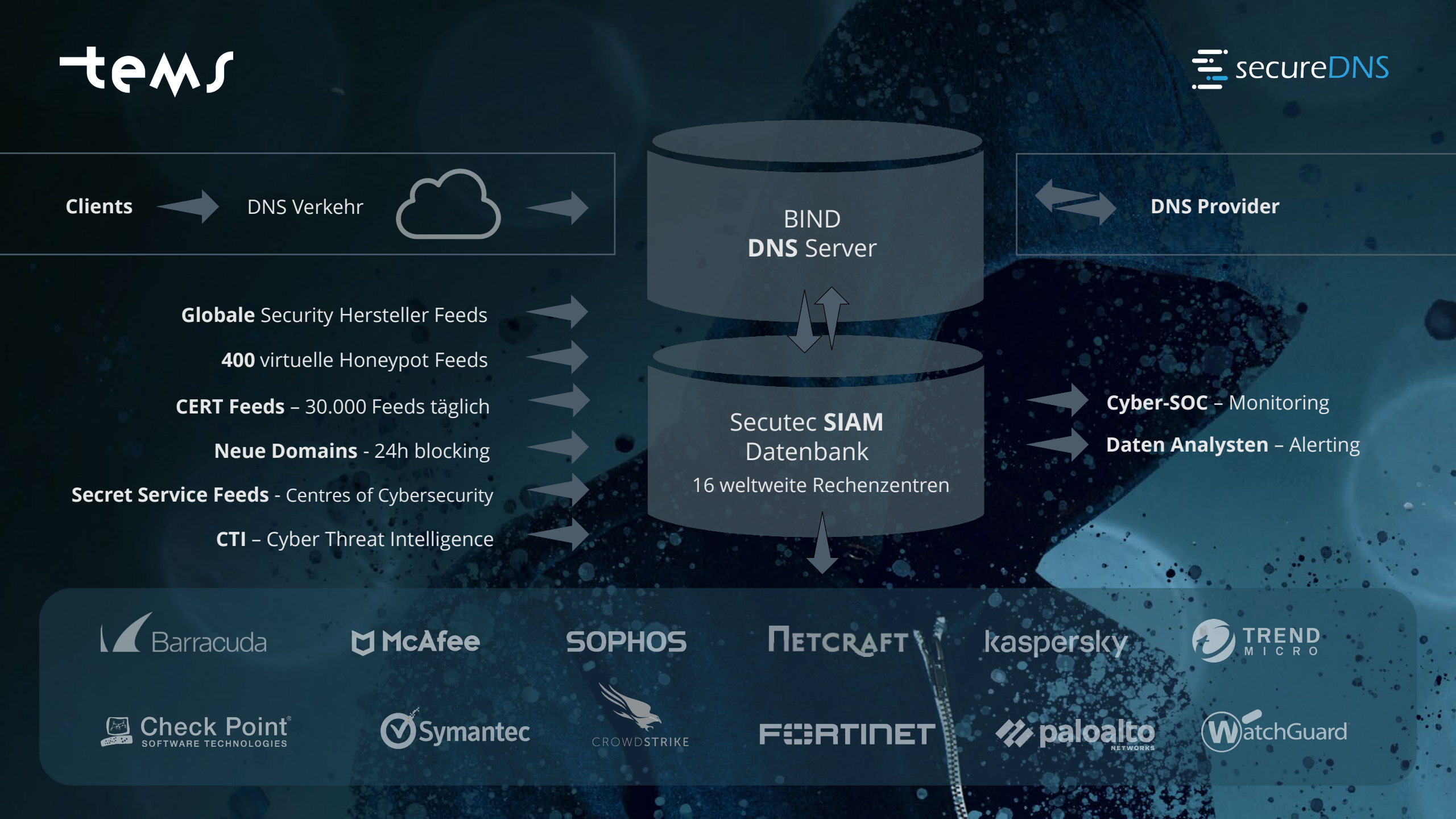


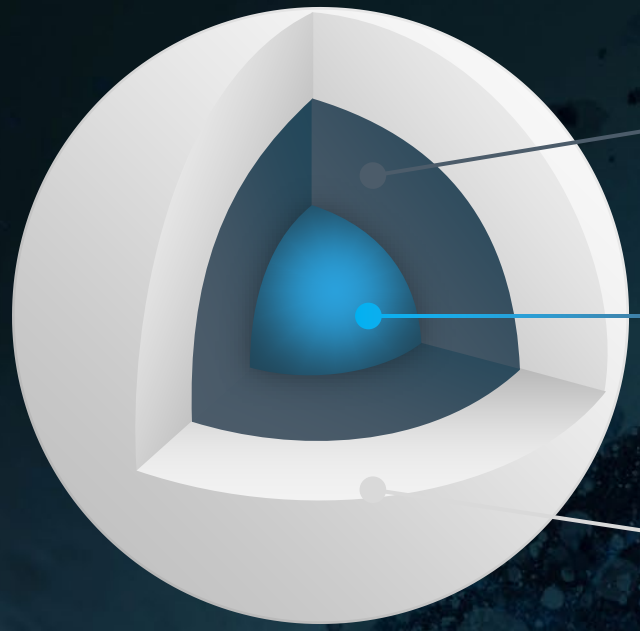
Secutec entwickelt Cyber-Security-Layer für alle Angriffsflächen.

secureDNS

NOCH NIE WAR CYBER-SECURITY EINFACHER


tems
secureDNS
secureDNS überwacht alle DNS Verbindungen 24/7,
blockiert bedrohliche DNS Anfragen mit einer
einzigartigen globalen SIAM Datenbank und alarmiert
Kunden aktiv bei Bedrohungen.


tems
secureDNS
Clients
DNS Verkehr
BIND
DNS Server
DNS Provider
Globale Security Hersteller Feeds
400 virtuelle Honeypot Feeds
CERT Feeds – 30.000 Feeds täglich
Neue Domains - 24h blocking
Secret Service Feeds - Centres of Cybersecurity
CTI – Cyber Threat Intelligence
Secutec SIAM
Datenbank
16 weltweite Rechenzentren
Cyber-SOC – Monitoring
Daten Analysten – Alerting
Barracuda
McAfee
SOPHOS
NETCRAFT
kaspersky
TREND MICRO
Check Point SOFTWARE TECHNOLOGIES
Symantec
CROWDSTRIKE
FORTINET
paloalto NETWORKS
WatchGuard



40% Plattform Technologie

30% Datenbasis und Intelligenz

30% Expertise / Daten Analysten / SOC

Datenbasis

SIAM Datenbank mit
35 weltweite Hersteller
Datenbanken

Hersteller Datenbank ~100MB
Secutec Datenbank 410 GB

Schnelligkeit

Integration von
20.000-30.000 täglichen
CERT Feeds

Einige Stunden
Zeitvorteil gegenüber
Hersteller Datenbanken

Analysten

40 Daten Analysten
überwachen 7x24 Stunden
sämtliche Daten

Kunden bekommen eine
proaktive Information
bei möglichen Bedrohungen

Darknet

Eine Kombination mit
Darknet Monitoring
ist möglich

Secutec überwacht
99% der weltweiten
„bad“ Connections

New Domain

Jede neue Domain
wird innerhalb der ersten
24 Stunden blockiert

Mehr als 22% aller
neu registrierten Domains
werden für Cyberkriminalität
verwendet

False Positive

200 Mio. tägliche
DNS-Requests
werden bewertet

Durchschnittlich
1 x False Positive
pro Monat

Mehrwerte im Vergleich zu anderen Lösungen.

Ganzheitlich

secureDNS
= ausgehender Traffic

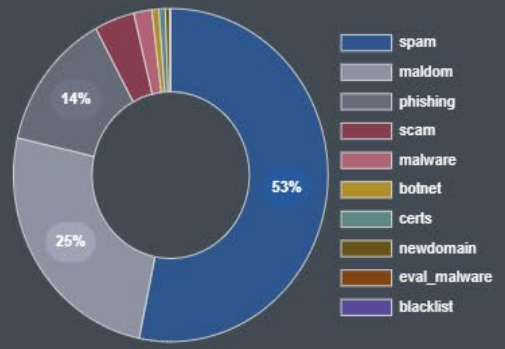
secureSIGHT
= eingehender Traffic
(mehr als 35 CTI Feeds)
+ Clear-Web
+Deep-Web
+Darknet

HOME
News
DATA & REPORTING
Dashboards
Reports
DOCUMENTS
Documents
PARTIES INVOLVED
Users
Organizations

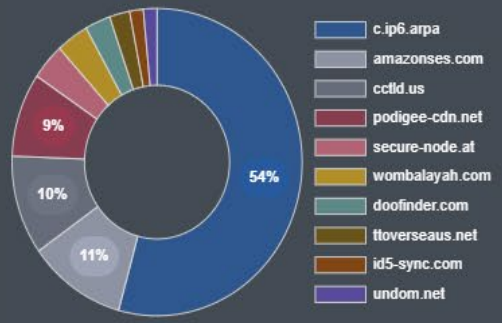
Domain | Query | Category | Public IP | Processes | Users | Computers | Private IP

All requests	Blocked requests	Monitored requests	Blocked botnet requests	Blocked apt requests
512 176	512 176	0	3 668	0

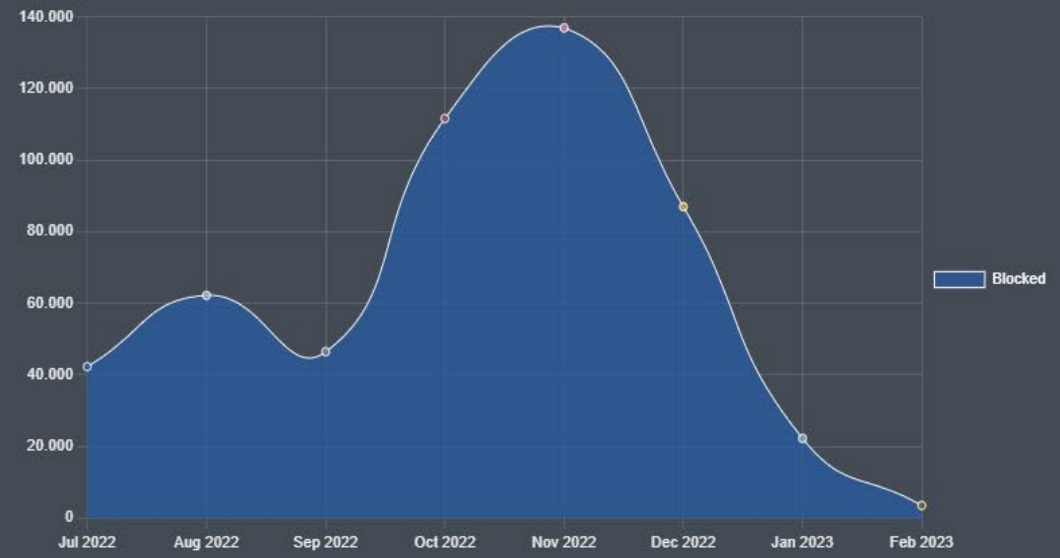
Top 10 categories



Top 10 domains

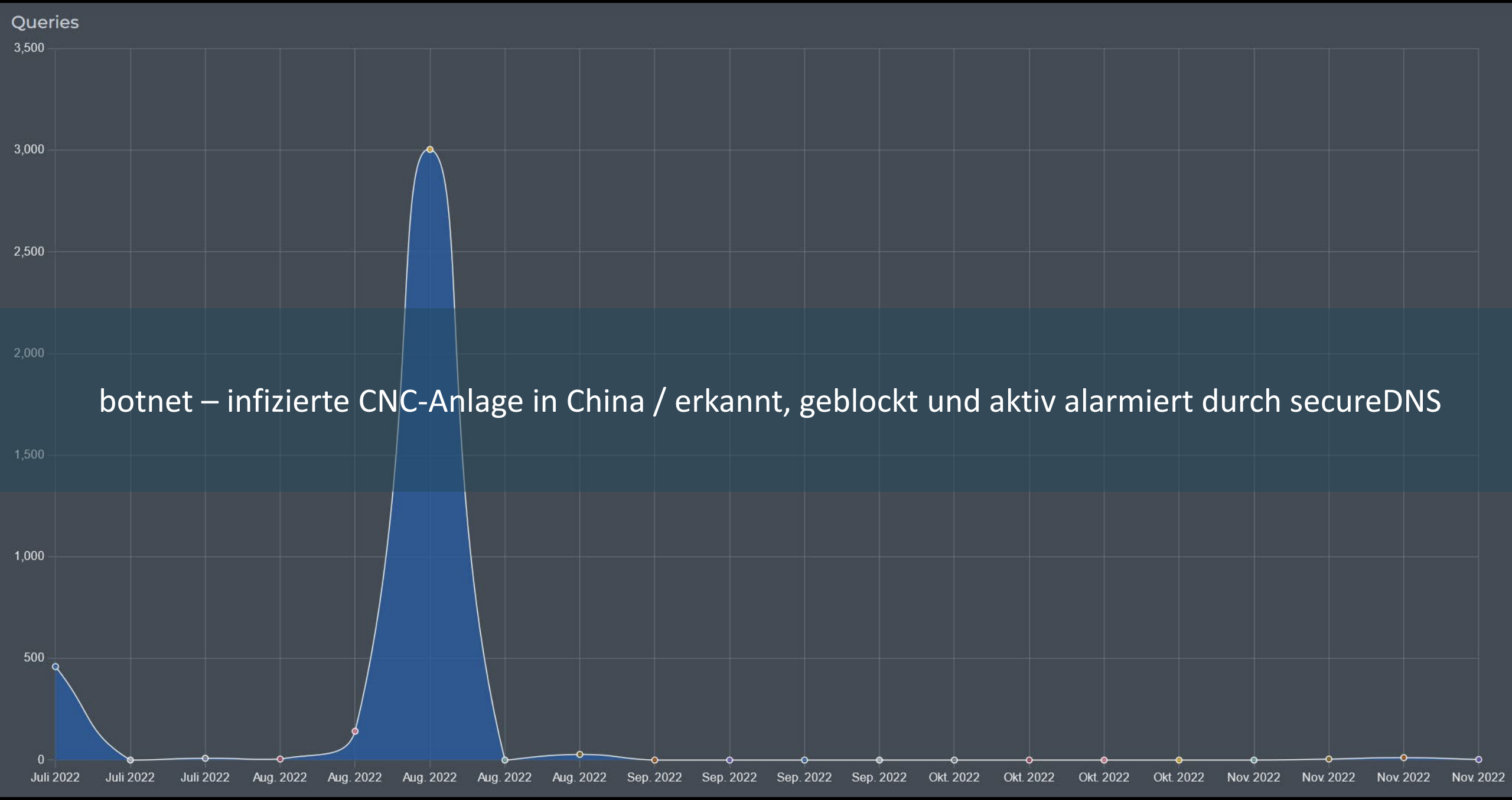


Queries

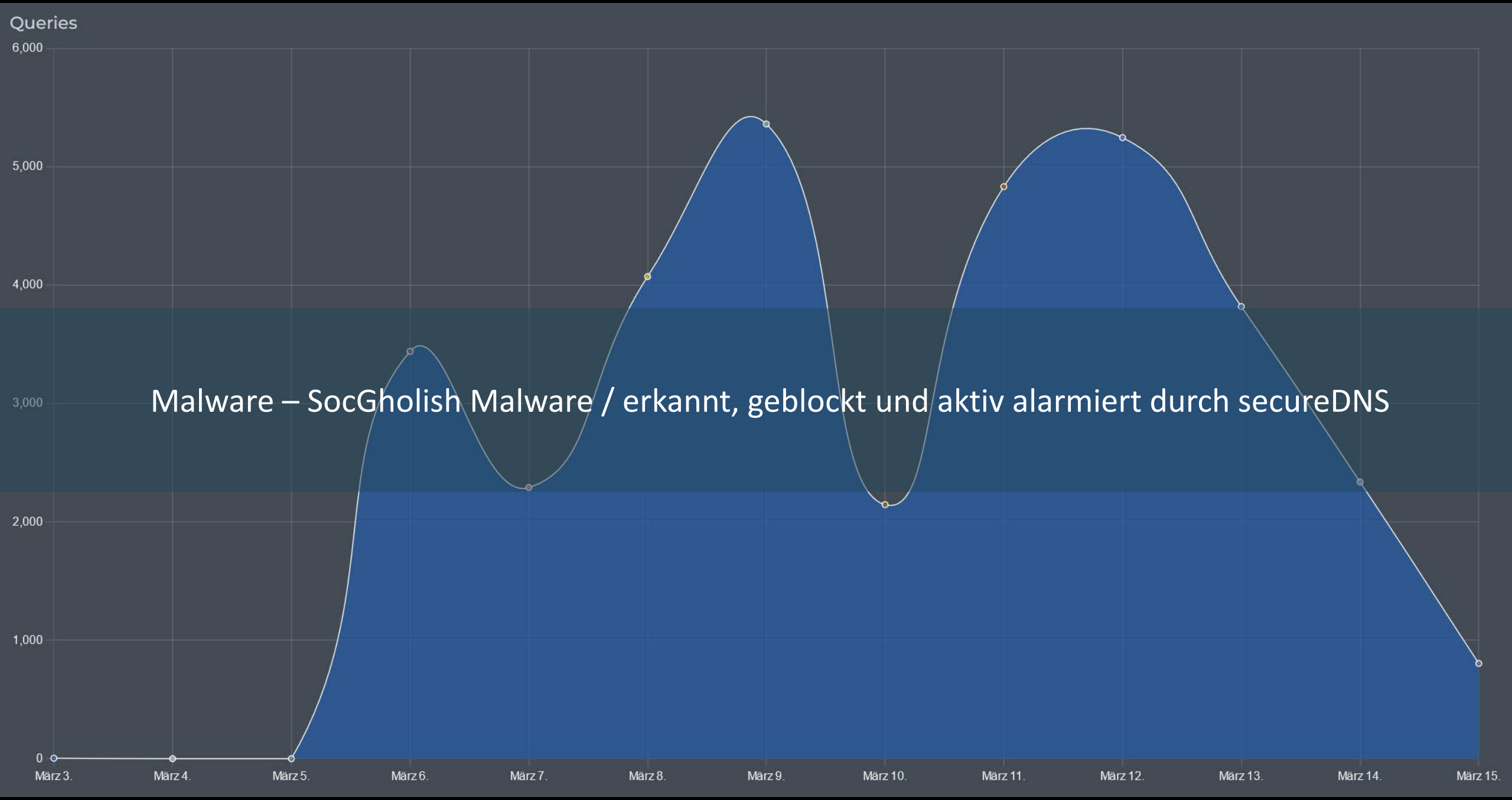


Queries

Date	DNS Category	DNS Query	Client Name	Public IP Address	Site Name	Agent Hostname	Private IP Address	VirusTotal Score	FortiGuard Rating	McAfee Rating	Ticket Number	Whitelisting
02/02/2023 13:39:05	spam	ad.turn.com										Request whitelisting
02/02/2023 13:36:47	spam	ad.turn.com										Request whitelisting
02/02/2023 13:36:47	spam	ad.turn.com										Request whitelisting



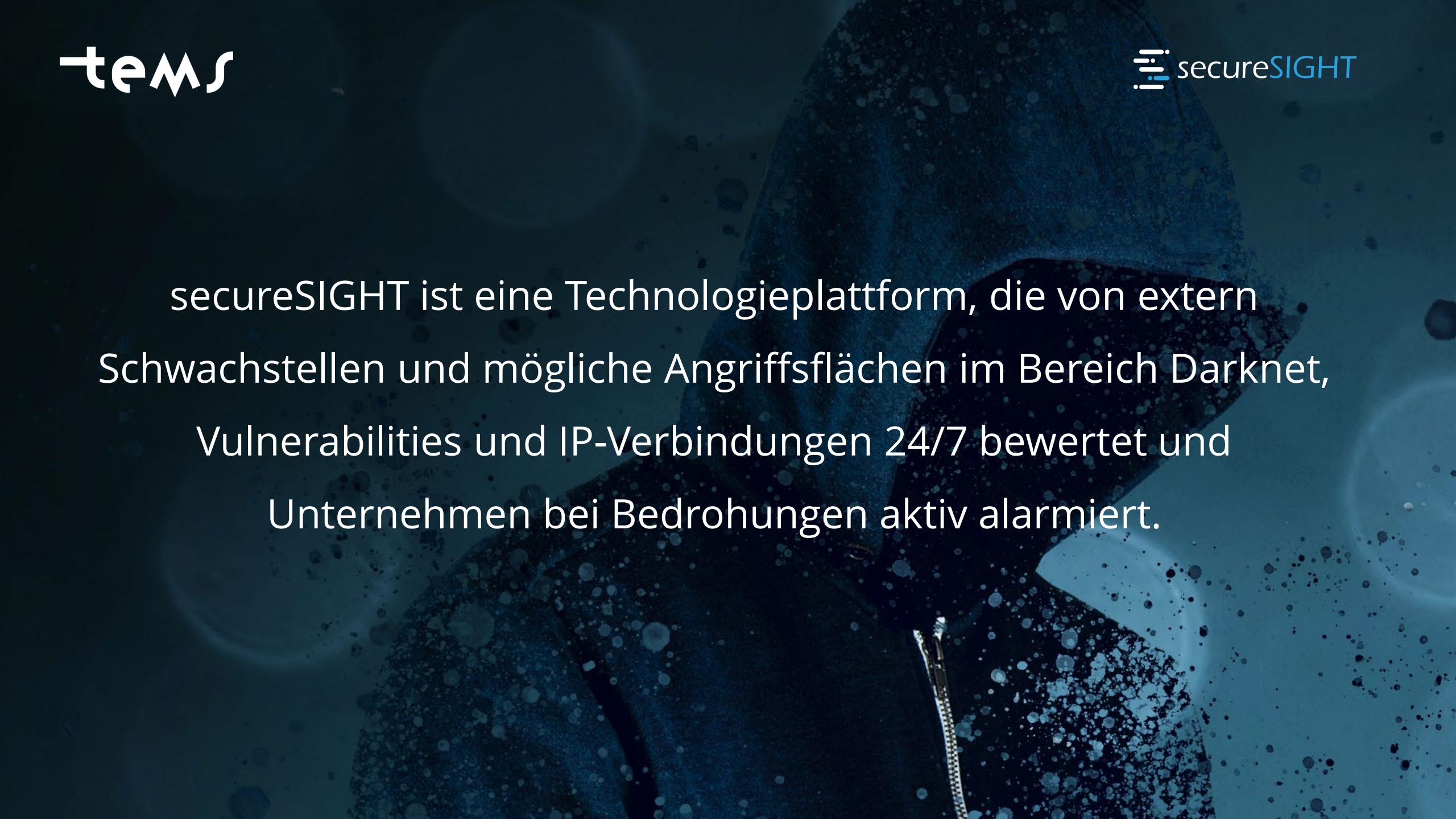
botnet – infizierte CNC-Anlage in China / erkannt, geblockt und aktiv alarmiert durch secureDNS



Malware – SocGholish Malware / erkannt, geblockt und aktiv alarmiert durch secureDNS

secureSIGHT

IHR DIGITALER UNTERNEHMENS FOOTPRINT


tems
secureSIGHT
secureSIGHT ist eine Technologieplattform, die von extern
Schwachstellen und mögliche Angriffsflächen im Bereich Darknet,
Vulnerabilities und IP-Verbindungen 24/7 bewertet und
Unternehmen bei Bedrohungen aktiv alarmiert.

Permanenter Vulnerability Scan

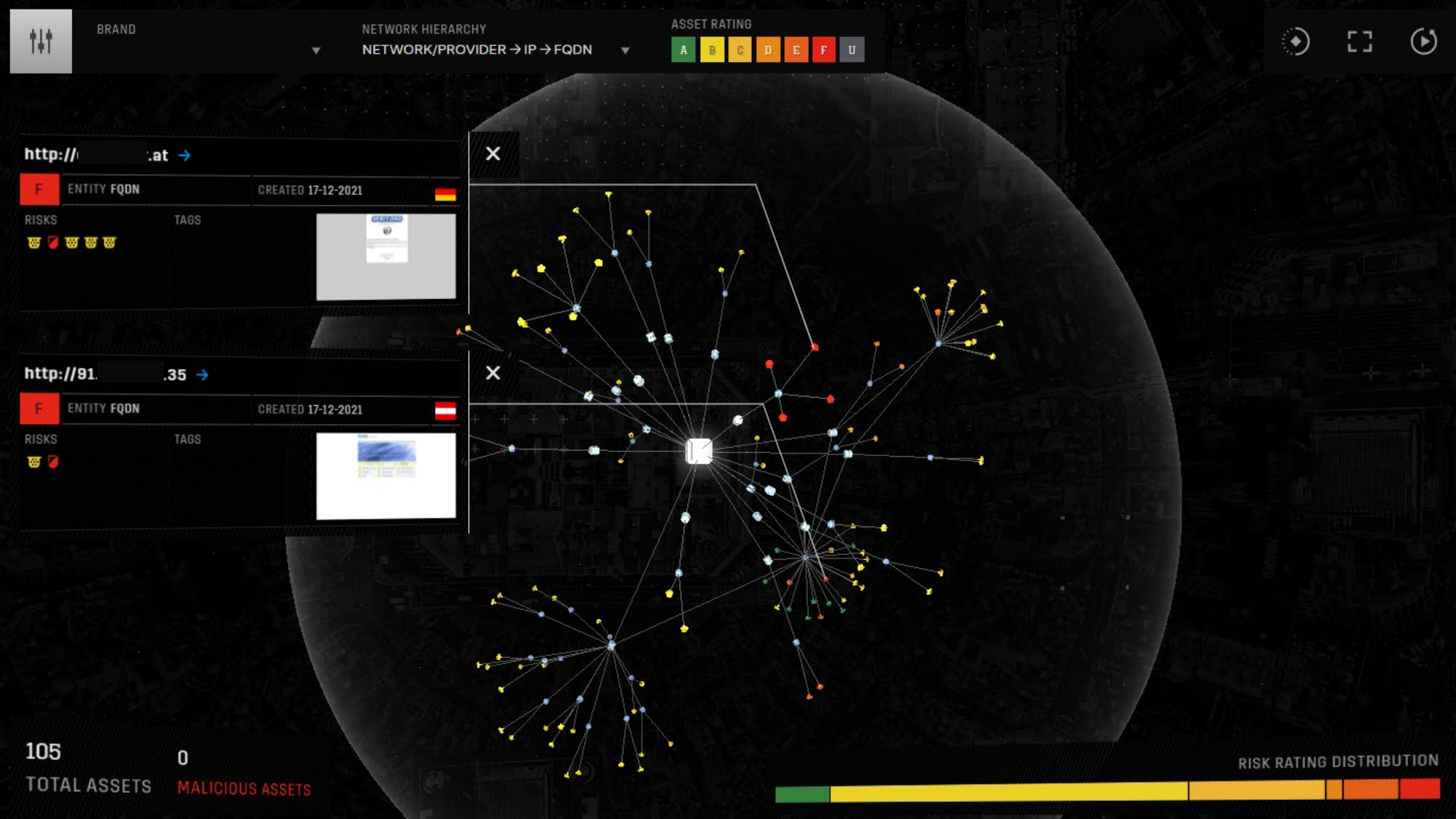
- Externes monitoring möglicher Schwachstellen

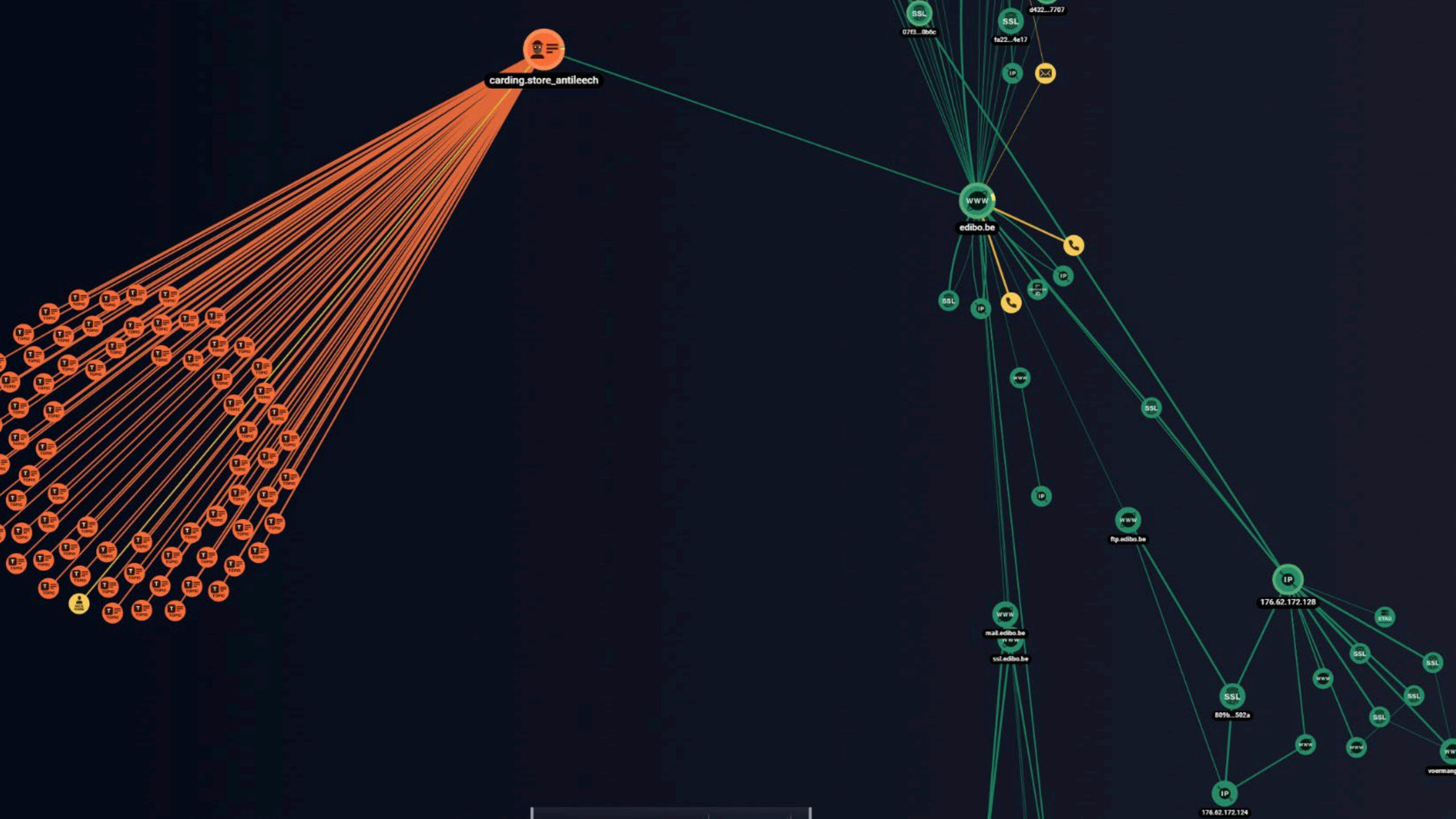
  (Vulnerabilities, Malware, Open-Ports, SSL-Zertifikate, Industrial Control Service, IoT Devices)

- Scanning auch außerhalb bekannter IP-Ranges

- Neubewertung erfolgt alle 24-48 Stunden

- Aktive Alarmierung bei Bedrohungen


BRAND
NETWORK HIERARCHY
NETWORK/PROVIDER → IP → FQDN
ASSET RATING
A B C D E F U
http:// .at
F
ENTITY FQDN
CREATED 17-12-2021
RISKS
TAGS
http://91. .35
F
ENTITY FQDN
CREATED 17-12-2021
RISKS
TAGS
105
TOTAL ASSETS
0
MALICIOUS ASSETS
RISK RATING DISTRIBUTION


carding.store_antileech
edibo.be
ftp.edibo.be
mail.edibo.be
ssl.edibo.be
176.62.172.128
176.62.172.124
07f3...0b6c
fa22...4e17
d432...7707
809b...502a

Managed Darknet Monitoring

- Aktives Darknet Monitoring im Bereich Darknetseiten, Foren, Chats, Marktplätze

- Überwachung von Domains, Benutzerkonten, strategischen Personen, Keyword, Produkten, usw.

- Aktive Suche nach internen und externen Usern mit infizierten Clients (Keylogger, Password Stealer)

- Aktive Alarmierung bei sicherheitsrelevanten Findings

Data for

Data records matching this domain.

Export | Filter | Show Passwords

Corporate Records (408) | Infected Employee Records (17) | Infected Consumer Records (24)

Show 10 entries | Column visibility | Search:

Breach Title	Publish Date	Breach Date	Email	Username	Password	Target Domain	Sighting	Severity	
Russian Password Stealer	2022-04-07	Unknown	philipp.ber		********	proom.de	1	Critical	View Raw Data
Russian Password Stealer	2022-04-07	Unknown	lorenz.bleckenw		********	microsoftonline.com	1	Critical	View Raw Data
Russian Password Stealer	2022-04-07	Unknown	philipp.ber		********	inforxtreme.com	1	Critical	View Raw Data
Russian Password Stealer	2022-04-07	Unknown	philipp.ber		********	auvesy.de	1	Critical	View Raw Data
Russian Password Stealer	2022-04-07	Unknown	philipp.ber		********	fill.co.at	1	Critical	View Raw Data

Field Name	Field value
Email	lorenz.blecke
Domain	
Password	********
Target Domain	microsoftonline.com
Target Url	login.microsoftonline.com
Password Plaintext	********
Severity	Critical
Password Type	plaintext
User Browser	Firefox
Ip Addresses	37.120.155.44
Infected Path	C:\Users\user\AppData\Local\Temp\IXP000.TMP \Gambe.exe.com
User Os	Windows 10 Home 64-bit_(x64) Build: 19041 Release: 2004
Keyboard Languages	deutsch (deutschland) | deutsch (österreich) |
Display Resolution	1536x864
Infected Machine Id	a032631f-438d-43b9-a37c-2c4575adf9f1
User Sys Registered Owner	user
User Hostname	LAPTOP-TQUTJK5E
Infected Time	2021-09-28T14:11:01Z

Active Manged Threat hunting

- 24/7 Überwachung aller IP-Datenverbindungen, die von der Firewall nicht blockiert wurden.

- Aktive Alarmierung bei schadhaften Verbindungen

- Zugang zu TIER1 Netflow Daten der Internet eXchange Knotenpunkte und Kategorisierung dieser Daten

Time (start_time)	_index	src_ip_addr	sr...	src...	prov1.r...	pro...	pro...	prov...	whois.src_...	who...	num_pkts	num_octets	proto	dst_ip_addr	dst...	dst_port	pr...	pro...	pr...	prov1.r...
Sep 11, 2021 @ 08:39:34.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	16	7.3KB	6	176.126.253....	RO	46,303	75	bot	-	gumblar
Sep 11, 2021 @ 08:39:31.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	87	111.3KB	6	176.126.253....	RO	39,827	75	bot	-	gumblar
Sep 11, 2021 @ 04:13:05.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	87	111.2KB	6	185.193.52.1...	RO	45,327	48	bot	-	poseidon
Sep 11, 2021 @ 03:29:11.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	22	23.1KB	6	45.128.133.2...	BE	44,505	75	bot	-	gumblar
Sep 11, 2021 @ 03:29:10.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	28	26.6KB	6	45.128.133.2...	BE	35,861	75	bot	-	gumblar
Sep 11, 2021 @ 03:29:08.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	28	26.6KB	6	45.128.133.2...	BE	37,178	75	bot	-	gumblar
Sep 11, 2021 @ 01:43:09.0...	traffic-ozbe	176.62.171.70	BE	443	-	-	-	-	-	-	3,000	4.3MB	6	118.193.41.1...	HK	39,672	75	bot	-	minerpane
Sep 11, 2021 @ 00:01:21.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	13	7.2KB	6	82.221.131.71	IS	44,502	75	bot	-	gumblar
Sep 11, 2021 @ 00:01:16.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	56	121.1KB	6	82.221.131.71	IS	38,436	75	bot	-	gumblar
Sep 10, 2021 @ 23:25:03.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	15	7.3KB	6	185.193.52.1...	RO	44,215	48	bot	-	poseidon
Sep 10, 2021 @ 23:24:57.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	214	419.5KB	6	185.193.52.1...	RO	33,313	48	bot	-	poseidon
Sep 10, 2021 @ 23:22:30.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	19	23KB	6	185.195.79.1...	TR	37,235	75	bot	-	gumblar
Sep 10, 2021 @ 23:22:29.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	24	26.4KB	6	185.195.79.1...	TR	36,297	75	bot	-	gumblar
Sep 10, 2021 @ 22:02:54.0...	traffic-ozbe	185.59.17.118	BE	443	-	-	-	-	-	-	15	6.7KB	6	195.176.3.20	CH	51,428	75	bot	-	gumblar
Sep 10, 2021 @ 21:47:46.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	35	34.3KB	6	176.126.253....	RO	41,321	75	bot	-	gumblar
Sep 10, 2021 @ 21:47:45.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	31	34.5KB	6	176.126.253....	RO	44,881	75	bot	-	gumblar
Sep 10, 2021 @ 21:25:51.0...	traffic-ozbe	185.162.31.74	BE	80	-	-	-	-	-	-	12	31.8KB	6	5.182.210.216	NL	39,963	75	bot	-	gumblar
Sep 10, 2021 @ 20:57:17.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	27	34KB	6	27.122.59.100	SG	42,305	75	bot	-	gumblar
Sep 10, 2021 @ 20:51:57.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	24	33.9KB	6	185.216.32.1...	BG	36,311	75	bot	-	gumblar
Sep 10, 2021 @ 20:51:55.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	25	34.3KB	6	185.216.32.1...	BG	46,403	75	bot	-	gumblar
Sep 10, 2021 @ 20:44:41.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	23	29.9KB	6	185.195.79.1...	TR	37,019	75	bot	-	gumblar


tems
Secutec
Cyber security intelligence