Generalstaatsanwaltschaft
Bamberg

Cybersicherheit aus der Sicht eines Strafverfolgers

Gegner – Techniken - Strategien

Cybersecurity Day 26.01.2023 – München – Oberstaatsanwalt Christian Schorr

Zentralstelle Cybercrime Bayern

(errichtet bei der Generalstaatsanwaltschaft Bamberg seit dem 01.01.2015)

Aufgaben:

- **Bearbeitung herausgehobener Verfahren der Computerkriminalität**
- Aus- und Fortbildung der bayerischen Justiz
- Zentrale Ansprechstelle für Cyberkriminalität

Zentralstelle Cybercrime Bayern

(errichtet bei der Generalstaatsanwaltschaft Bamberg seit dem 01.01.2015)

Aufgaben:

- **Bearbeitung herausgehobener Verfahren der Computerkriminalität**
- Aus- und Fortbildung der bayerischen Justiz
- Zentrale Ansprechstelle für Cyberkriminalität

- **21 Staatsanwältinnen und Staatsanwälte**
- **4 IT-Referentinnen und Referenten**

Stand 01.01.2023

Zentralstelle Cybercrime Bayern

- **Zentrum zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet (ZKI)**
  - Straftaten gegen die sexuelle Selbstbestimmung (insbesondere „Tauschringe“, kommerzielle Angebote, Kinderpornografie-Foren im Darknet)

- **Taskforce Cyberangriffe auf Unternehmen und Einrichtungen**

– *Cyberangriffe auf Unternehmen, Einrichtungen und Behörden, sowie kritische Infrastrukturen*

– *technische Angriffe unter Einsatz von Schadsoftware*

– *Verstöße gegen das BtMG*

– *Straftaten, die im Darknet begangen werden*

– *Betreiber krimineller Handelsplattformen nach § 127 StGB*

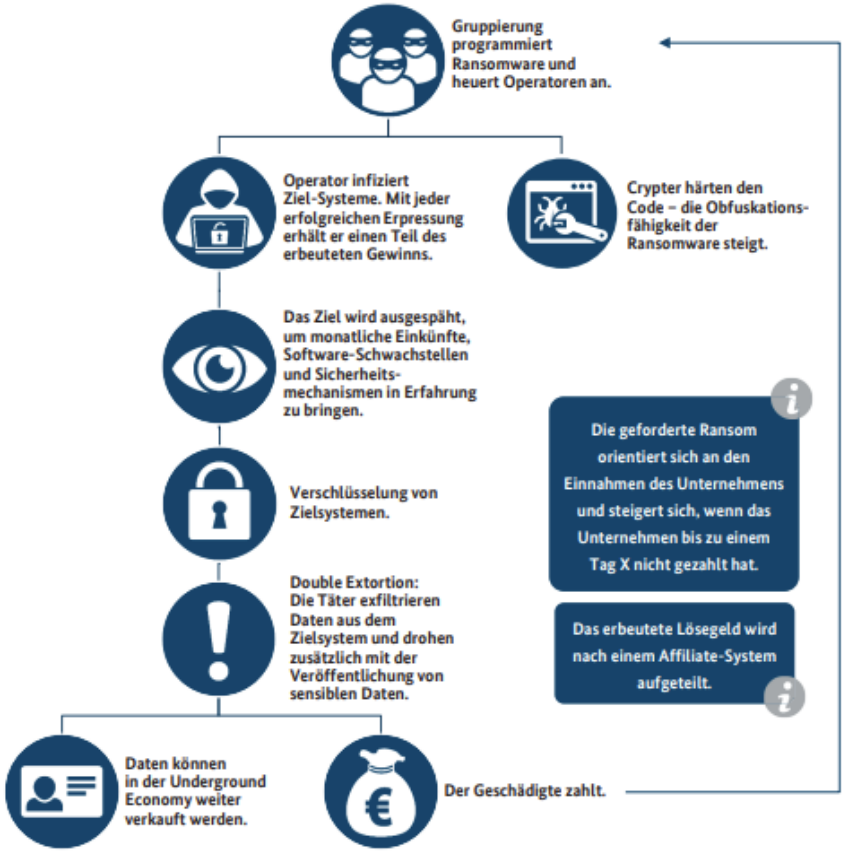
- **Wirtschaftscybercrime I**
  - Wirtschaftsverfahren nach § 74c GVG (seit 01.02.2018), insbesondere Fakeshops (seit 01.10.2022)

- **Wirtschaftscybercrime II**
  - Wirtschaftsverfahren nach § 74c GVG (seit 01.02.2018), insbesondere Cybertrading

Angreifer: Professionelle Täter mit unterschiedlichen Zielen

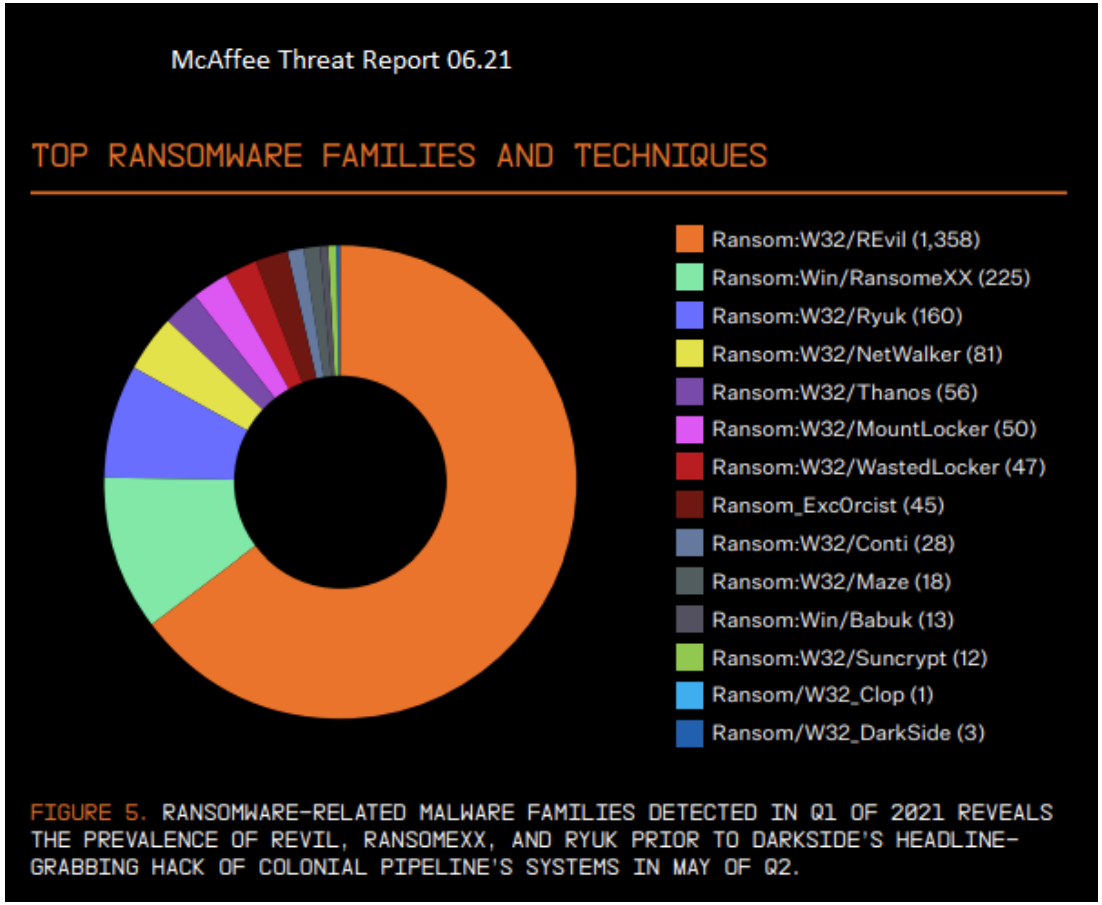
- **Ransomware-Gruppierungen** (Verschlüsselung und Datenabzug)
- APT-Gruppen (Datendiebstahl, Sabotage)
- gewerbliche Industriespione
- **Spearphisher /Fraudster** (EMail-Server)
- Erpresser (DDoS Extortion)

Tendenz: crime-as-a-service



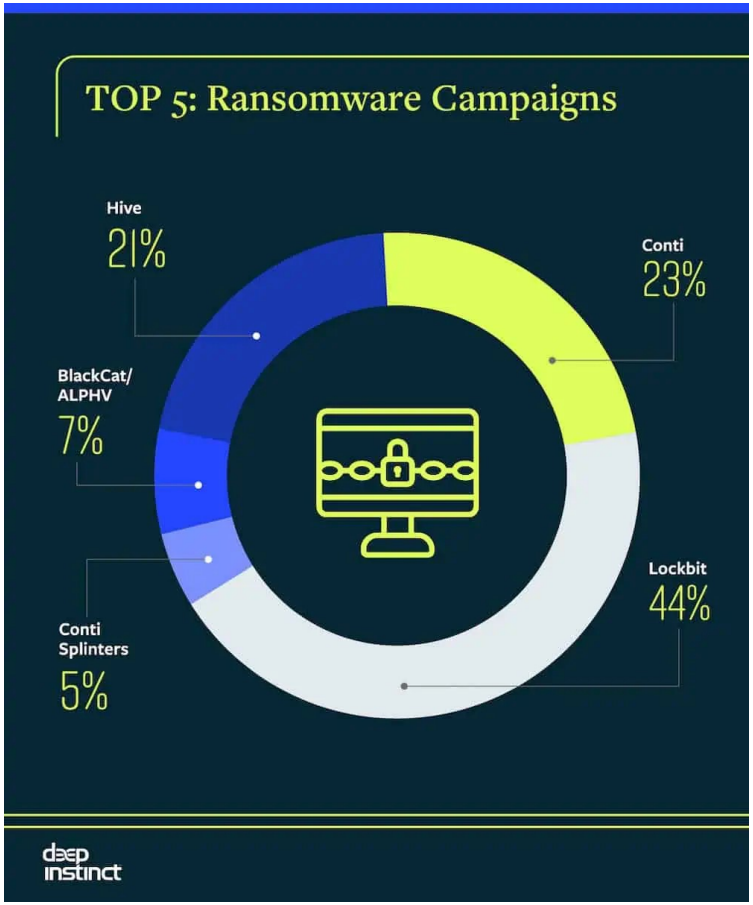
Kriminelle Strukturen

wachsende Anzahl an Gruppierungen…



Kriminelle Strukturen

…die stetig wechseln



Quelle: deep instinct Cyber Threat Report 2022

Affiliate - System

lockbitapt6 tr3a35nygvokja5uuccip4ykyd.onion/conditions

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

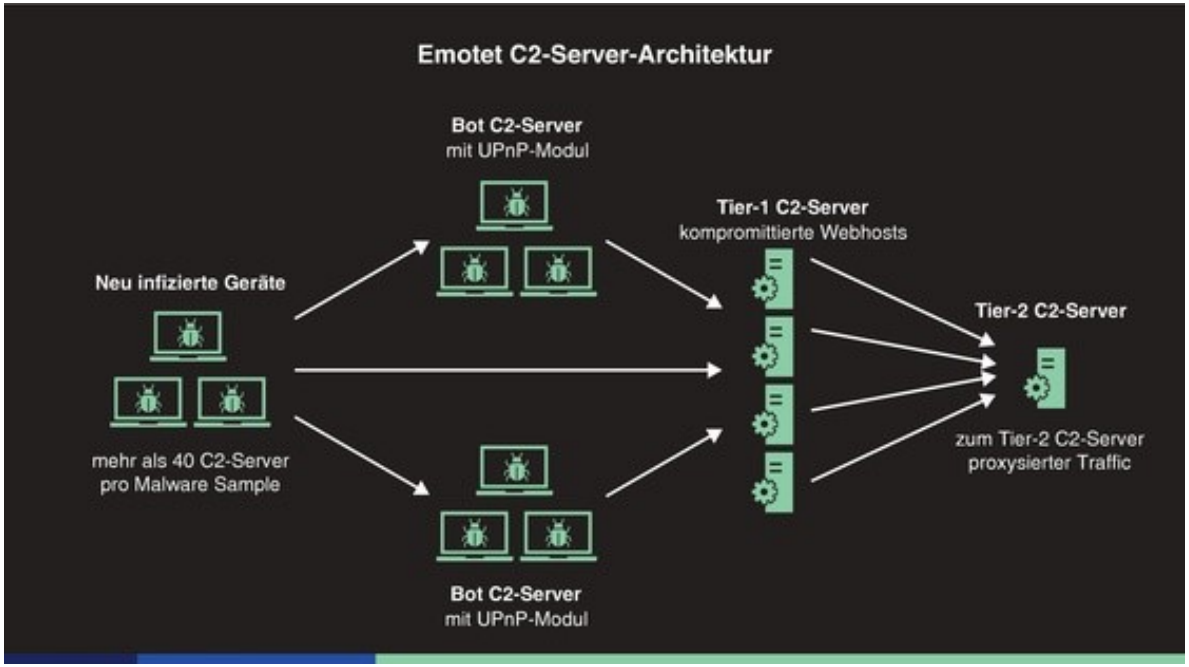
Encryption speed comparative table for some ransomware

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

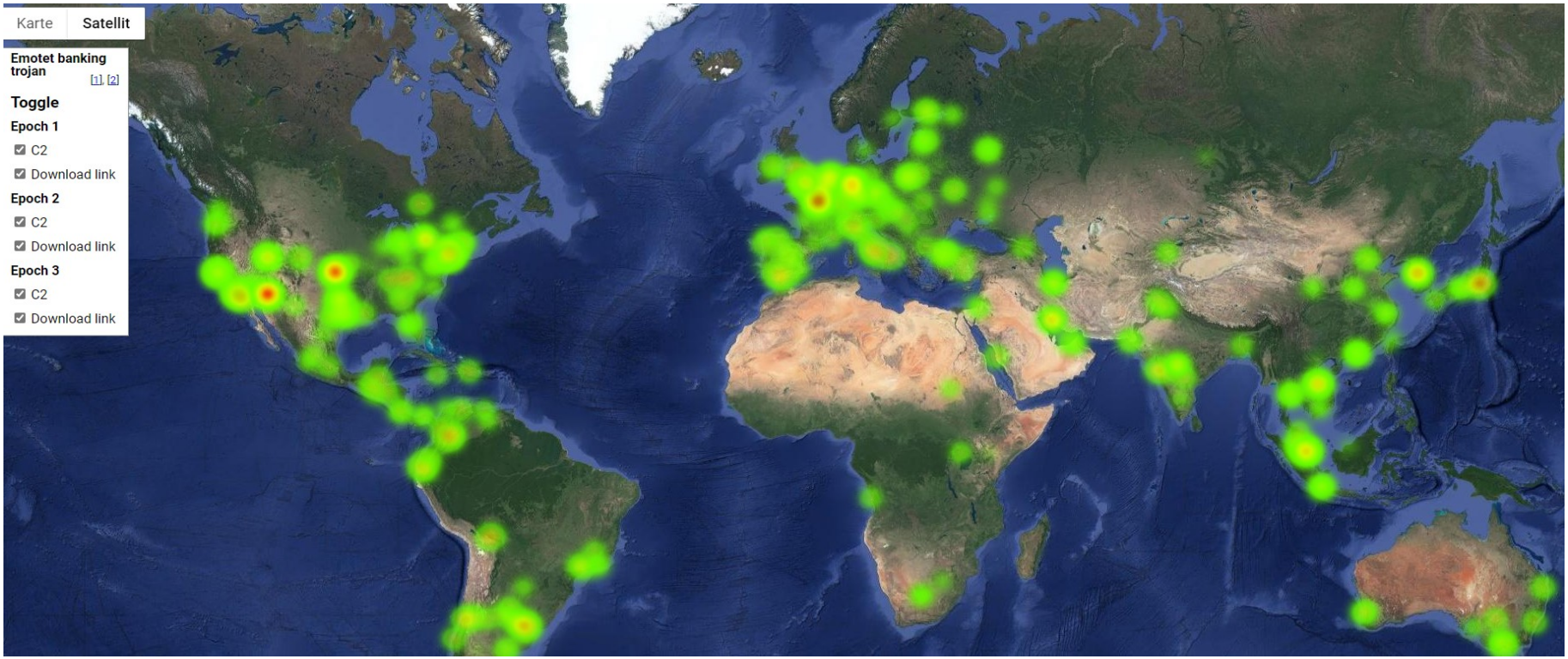
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002

Professionelle Verschleierung

- Benutzung eigener, z.T. komplexer Serverstrukturen (C&C)
- kaskadierend
- schnell wechselnd und weltweit verteilt



Professionelle Verschleierung



Quelle: https://blog.hqcodeshop.fi/archives/471-Data-Visualization-Emotet-banking-trojan.html

Angriffsvektoren

Systeme werden auf die unterschiedlichste Weise angegriffen

- Phishing
- Spear Phishing
- Angriffe auf VPN-Verbindungen (Anstieg der Nutzung durch Covid-19)
- Angriffe auf Client-PCs
- Angriffe über Remote Desktop Port u.ä.
- Angriffe über schwache Passwörter
- Angriffe über bekannte Sicherheitslücken /vulnerabilities (Citrix; Exchange Server, Eternal Blue)
- Supply-Chain-Angriffe (SolarWinds, Kaseya)
- Angriffe auf Frameworks (log4j)

Angriffsvektoren

- **Vorgefertigte Toolkits für Affiliates**
- **Fehlen eindeutiger IOCs aufgrund des Affiliate-Systems**
- **Vielzahl der Tätergruppierungen führt zu Konkurrenz (sowohl „Numbers Game“ als auch „Big Game Hunting“)**
- **Täter nutzen alle Angriffsoptionen aus**
- **Je größer das Unternehmen, desto länger die Erkundung (bis 12 Monate!)**
- **Gezielte Suche nach Backups und sensiblen Daten**

Angriffsvektoren

- **Affiliate – System – Playbooks und Training**

Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM		
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt			
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt			
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt			
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt		2 KB	text
Личная безопасность.txt		1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

Angry Affiliate Leaks Conti Ransomware Gang Playbook

Der Angriff

Aktuelle Beispiele – Ransomware Royal

```
Hello!

    If you are reading this, it means that your system were hit by Royal ransomware
    Please contact us via :
    http://royal2xthig3ou      liqagy6yygk2cdelaxtni2fyad6d      did.onion/fdF7rJ45c

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security
Alas, as a result your critical data was not only encrypted but also copied from yo
From there it can be published online.Then anyone on the internet from darknet crim
and even your employees will be able to see your internal documentation: personal d

    Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ? ) for our pent
covering you from reputational, legal, financial, regulatory, and insurance risks,
To put it simply, your files will be decrypted, your data restoredand kept confiden

    Try Royal today and enter the new era of data security!
    We are looking to hearing from you soon!
```

Angriffe

Jeder kann Opfer werden – aktuelles Beispiel (Ransomware Royal)

- Elektronikunternehmen
- Stahlproduktion
- Auktionen / Finanzdienstleister
- Plastikproduktion
- Textilreinigung
- Nahrungsmittelindustrie
- Private equity
- Produktion Öl / Gas
- Orthopädie-Praxis
- Softwareentwickler
- Restaurantkette

Ermittlungsansätze

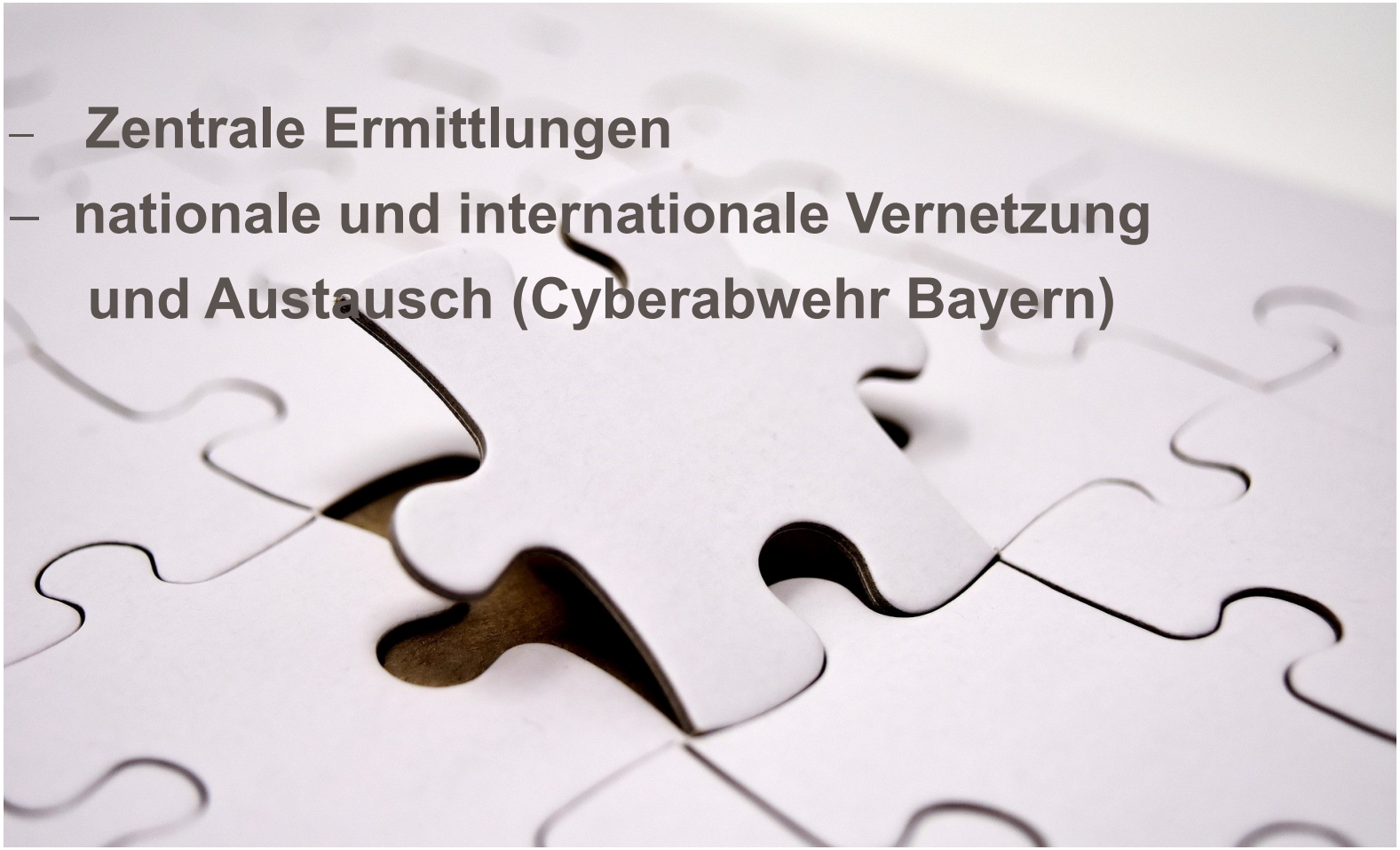
Die wesentlichsten Ermittlungsansätze:

1. technische Ermittlungen im Unternehmen: Einfallstor, digitale Spuren (insb. IPs) -> Problem: Verschlüsselung
2. Kryptoermittlungen nur im Zahlfall möglich; am Einzelfall weniger zielführend
3. Täter-Webseiten sofern ermittelbar und „greifbar“; idR Onion-Domains
4. Analyse der Angreifer-Infrastruktur abhängig von 1.; Zeit- und Ortfaktor; Preservation request; zum Teil komplett verschleiert
5. Täterkontakt technische Mittel; EMail-Beschlagnahme; effektive Verschleierung

Was verspricht Erfolg?

Der Einzelfall in der Regel nicht.

Was verspricht Erfolg?



Was verspricht Erfolg?

Zentrale Ermittlungen

Eine Staatsanwaltschaft ermittelt zentral (in Bayern ermittelt die ZCB so oder so in allen Ransomwarefällen)…

…gemeinsam mit einer Polizeidienststelle bundesweit.

Zusammentragen aller Spuren

Analyse von Strukturen

Auswertung von Daten

Erkennen von Fehlern oder Mustern

Veranlassung notwendiger Rechtshilfeersuchen

zielführende Analyse von Krypto-Zahlungsströmen

Was bedeutet das für Unternehmen?

Jede Strafanzeige zählt.

Strafanzeige – ihre Folgen und Vorteile

- Je schneller Strafanzeige erstattet wird, desto besser (flüchtige Spuren).
- Beweismittel können gesichert und isoliert werden (nicht vernichtet).
- Zusammenarbeit mit der IT des Unternehmens und mit Dienstleistern; idR dadurch Verzicht auf eine amtliche forensische Sicherung möglich. Polizei und Staatsanwaltschaft sind zu Rücksichtnahme auf den Geschädigten verpflichtet.
- Nur geringer Aufwand bei der Unterstützung der Ermittlungen erforderlich
- oft so oder so Meldung an die Datenschutzbehörde erforderlich oder der Vorfall wird anderweitig bekannt (Wall of Shame)
- Unterstützung bei der Bewältigung des Vorfalls

„Der Staatsanwalt achtet darauf, dass die für den Verletzten aus dem Strafverfahren entstehenden Belastungen möglichst gering gehalten und seine Belange im Strafverfahren berücksichtigt werden.“

Prävention vs. Response

Es kann jeden treffen. Prävention ist daher unerlässlich und die beste Waffe gegen die Täter.

Der „worst case“ sollte daher immer gedanklich durchgespielt werden:

Was passiert, wenn nichts mehr funktioniert?

Wie könnte mein Unternehmen dennoch weiterarbeiten?
(Ersatzsysteme, Ausdrucke, Mobiltelefone für Kommunikation)

Wer sind meine Ansprechpartner (Behörden, IT-Dienstleister, Versicherer)

Analyse des bestehenden Systems:

Welche Netze, welche Rechner, welche Maschinen laufen im Unternehmen?

Wie sind diese untereinander verbunden(Netzwerktrennung)?

Sind die Backups mehrfach vorhanden und sicher gegen Verschlüsselung verwahrt(nicht vom Netzwerk aus zu erreichen)?