Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME
COMPETENCE
CENTER

Cybercrime Competence Center (C4)

Ermittlungen

Stand: März 2023

Bundesministerium
Inneres

Bundeskriminalamt

Bundesministerium
Inneres
Bundeskriminalamt

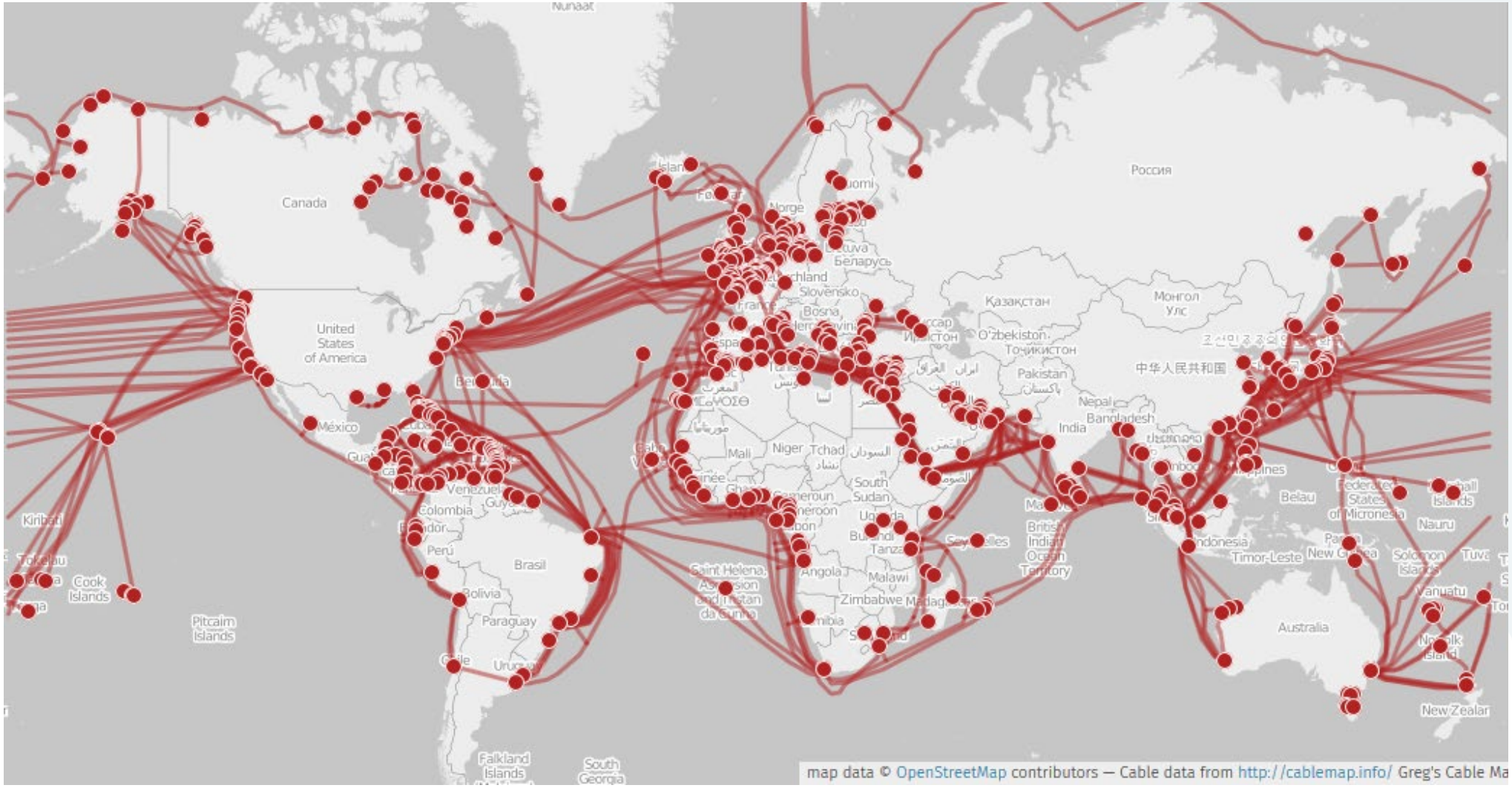
C4
CYBERCRIME
COMPETENCE
CENTER

A Brief History of Cybercr(T)ime

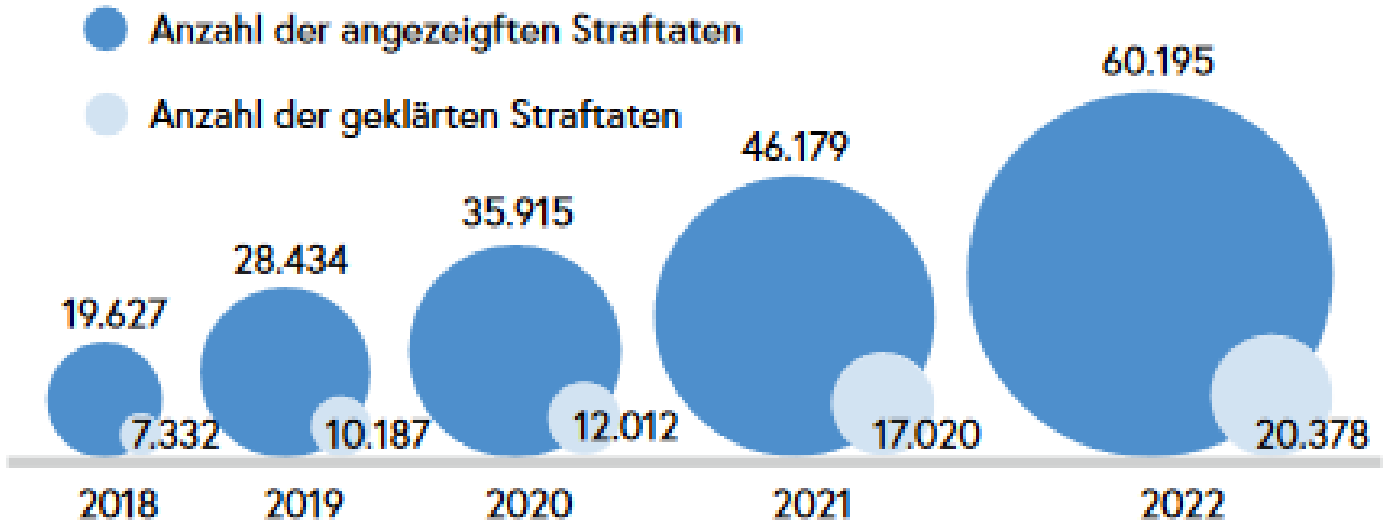
Bundesministerium
Inneres

Bundeskriminalamt

C4
CYBERCRIME
COMPETENCE
CENTER



Entwicklung der angezeigten und geklärten Cybercrime-Fälle von 2018 bis 2022 in Österreich



In der PKS wird im Sinne internationaler Vereinbarungen (in Anlehnung an die Budapester Konvention) eine Einteilung von Cybercrime vorgenommen.

Polizeilicher Zugang:

- **Cybercrime** (im engeren Sinn) (IKT als Angriffsziel)
  - nur mit Computer möglich
  - Vertraulichkeit, Verfügbarkeit und Integrität
- **Cyber-related-crime** (Cybercrime im weiteren Sinn -> „Tatmedium Internet“)
  - Computer/Internet als Tatmittel
  - Delikte existieren auch „in der realen Welt“
- Cybercrime vs. Cybersecurity

Cybercrime im engeren Sinn – rechtliche Abgrenzung

Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)

- Computersystem über das man nicht alleine verfügen darf od. nur zum Teil
- Überwinden einer spezifischen Sicherheitsvorkehrung (Software Sperre – Passwort oder Hardware Sperre – Schließvorrichtung am Gerät)
- Zugang zu personenbezogenen Daten (geheim)
- Daten sind bereits im System abgespeichert (siehe § 119a StGB)
- z.B. Hacking, Brute Force Attacks, Exploits, Social-Media Account
- Achtung: Zugriff (oder Vorsatz) notwendig für die Erfüllung des Tatbestandes!

Missbräuchliches Abfangen von Daten (119a StGB)

- Absichtlich Kenntnis über nicht für ihn bestimmte **Daten** im Wege eines Computersystems verschaffen.
- Daten werden auf dem Übertragungsweg abgefangen (unterschied zu § 118a StGB)
- Daten selber benützt oder jemand anderen zur Verfügung stellt (Vermögensvorteil)
- Mittels Hard. oder Software
- z.B. Trojaner, Sniffing, Men-in-the-Middle, Ausspionieren von Anmeldedaten, um damit kostenpflichtige Datenbank zu benützen

Datenbeschädigung (§ 126a StGB)

- Verändern, löschen, unterdrücken oder unbrauchbar machen von Daten
- z.B. Webseiten-Defacement, Daten von einem fremden USB-Stick löschen
- Achtung! § 125 StGB nur anzuzeigen, wenn der Datenträger dadurch auch tatsächlich unbrauchbar gemacht oder zerstört wird
- Häufiges Beispiel: Ransomware (Verschlüsselung), oft in Verbindung mit § 144 StGB (Erpressung)

Cybercrime im weiteren Sinn

- Delikte i.V. mit **unbaren Zahlungsmitteln** (§§ 241ff StGB)
- **Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses** (§ 123 StGB)
- **Datenverwendung in Gewinn- oder Schädigungsabsicht** (§ 63 DSG (ehem. Art. 51 DSG))
- Delikte nach dem **Urheberrecht** im Zusammenhang mit Software und Internet, z.B. § 78 UrhG – Bildnisschutz (Zivilrechtsweg)
- **Verbotene Inhalte**
  Kinderpornographie
  Nationalsozialistische Inhalte
  Selbstmordforen (§ 78 StGB)

Bundesministerium
Inneres
Bundeskriminalamt

C4 CYBERCRIME COMPETENCE CENTER

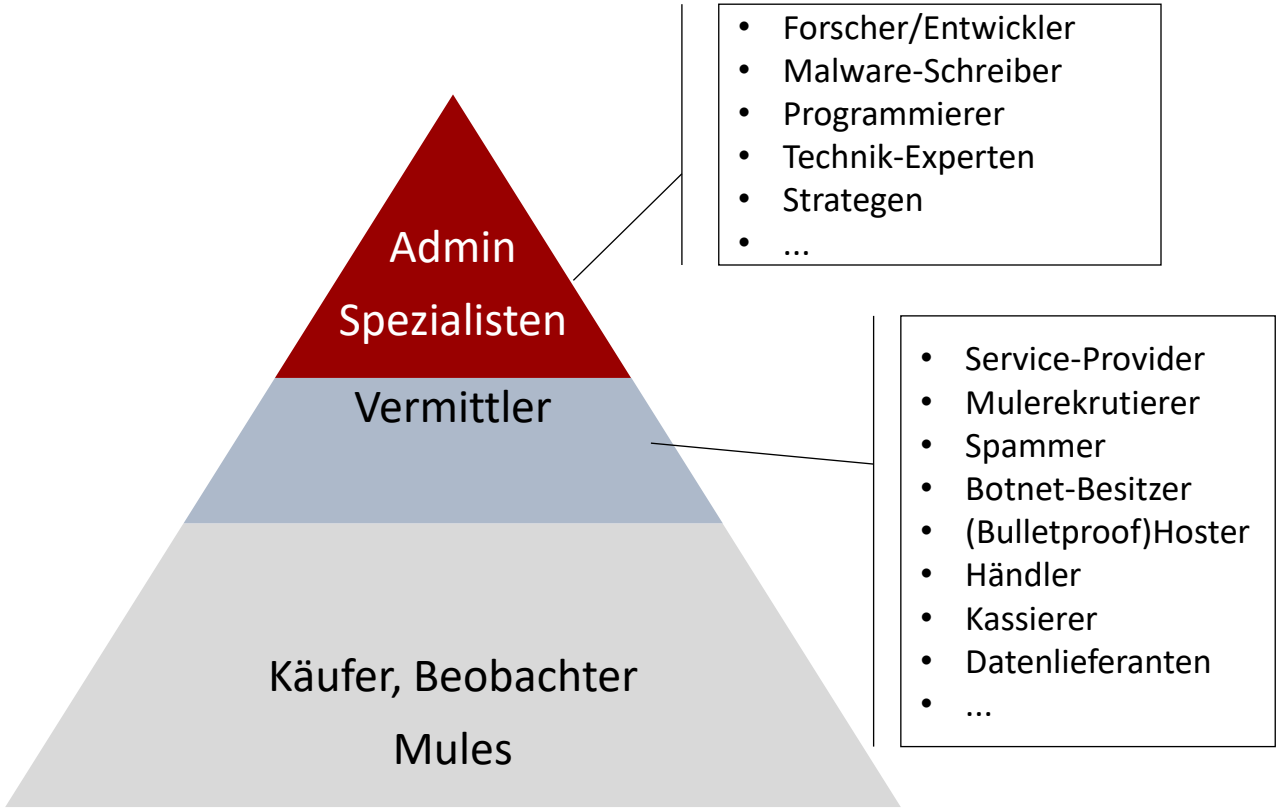
Grundlagen von “organized Cybercrime”

Kriminelle Netzwerke

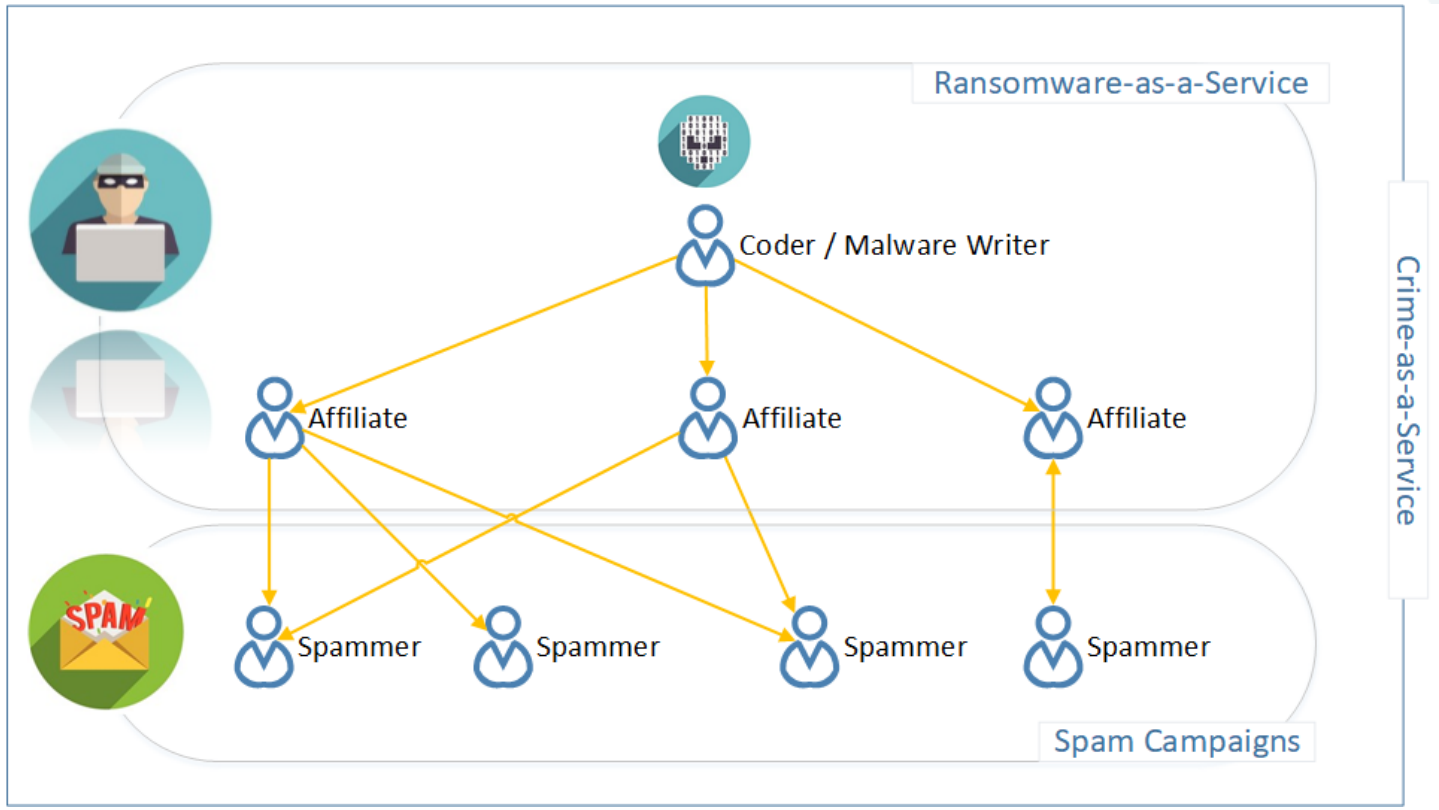
Sind keine **organisierten „Banden“** im traditionellen Sinn:

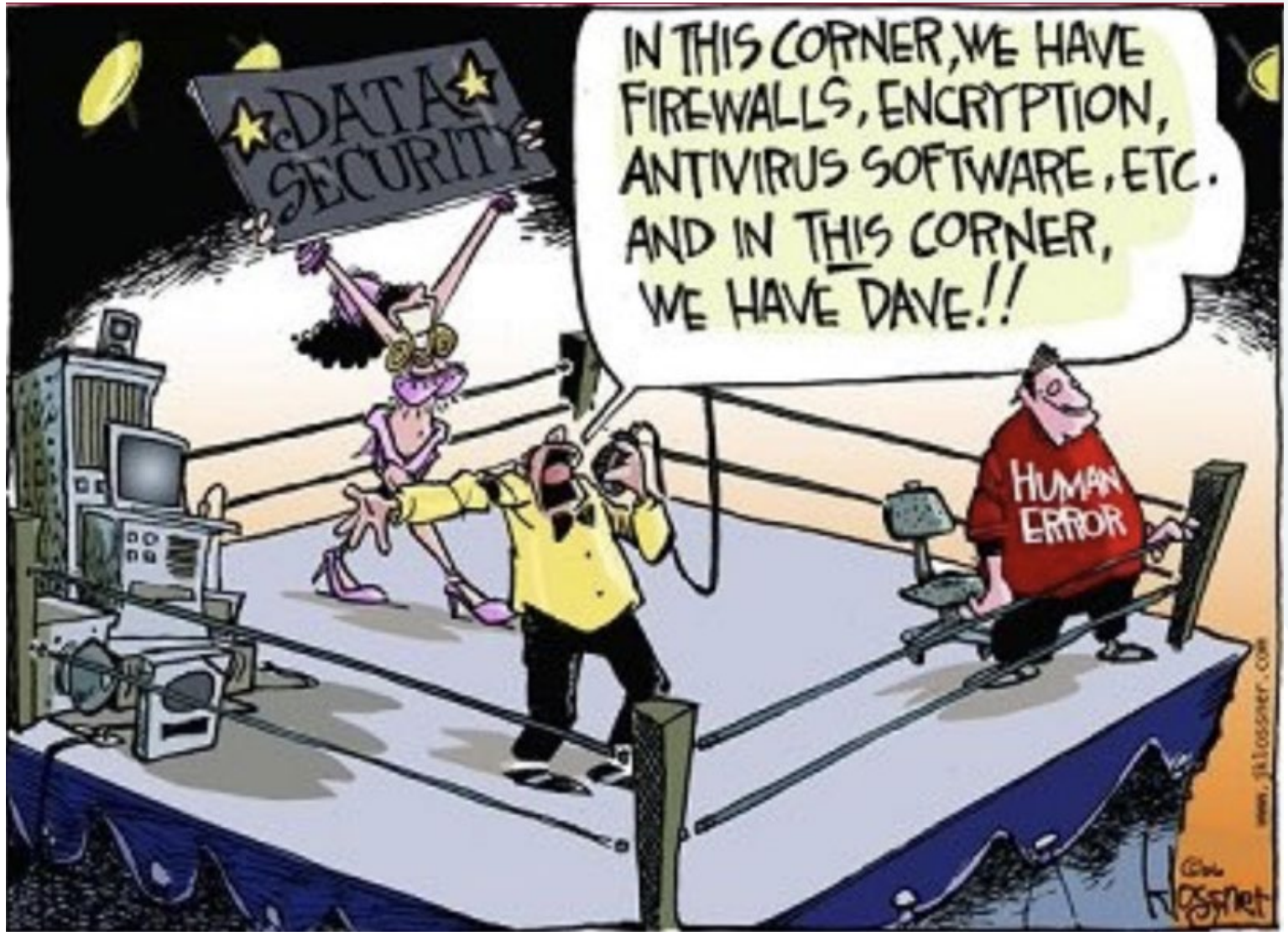
- Sind **arbeitsteilig** und teilweise straff organisiert
- Verfügen vor allem einzeln über enormes **Fachwissen**
- Mitglieder kennen sich i.d.R. **nicht persönlich**
- **Kommunizieren nur online** und anonym (z.B. über Jabber Chat-Server, Telegramm…)
- Sind sehr **dynamisch und kreativ**
- **Zeigen „menschliche Schwächen“**

Cybercrime-as-a-Service



Beispiel: RaaS




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jtlossner.com

Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

CEO/BUSINESS E-MAIL BETRUG (CEO-BETRUG)

CEO-Betrug tritt auf, wenn ein Mitarbeiter, der zur Ausführung von Zahlungen berechtigt ist, dazu verleitet wird, eine gefälschte Rechnung zu bezahlen oder eine nicht autorisierte Transaktion von einem Geschäftskonto vorzunehmen.

WIE FUNKTIONIERT ES?

Die Betrüger, die sich als hochrangige Personen des Unternehmens (z.B. CEO oder CFO) ausgeben, rufen an oder schreiben eine E-Mail.

Sie verfügen über gute Kenntnisse über die Organisation.

Sie verlangen eine dringende Zahlung.

Sie benutzen Begriffe wie: 'Vertraulich', 'Die Firma vertraut Ihnen', 'Ich bin momentan nicht verfügbar'.

Sie nehmen Bezug auf eine sensible Situation (z.B. Steuerprüfung, Fusion, Akquisition).

Der Mitarbeiter wird angehalten, den regulären Autorisierungsprozess zu umgehen.

Instruktionen bezüglich das weitere Vorgehen werden später über eine Drittperson oder über E-Mail bekanntgegeben.

Der Mitarbeiter transferiert Geld auf ein Konto, das durch den Betrüger kontrolliert wird.

Es handelt sich oftmals um internationale Zahlungen, die an Banken ausserhalb Europas gehen.

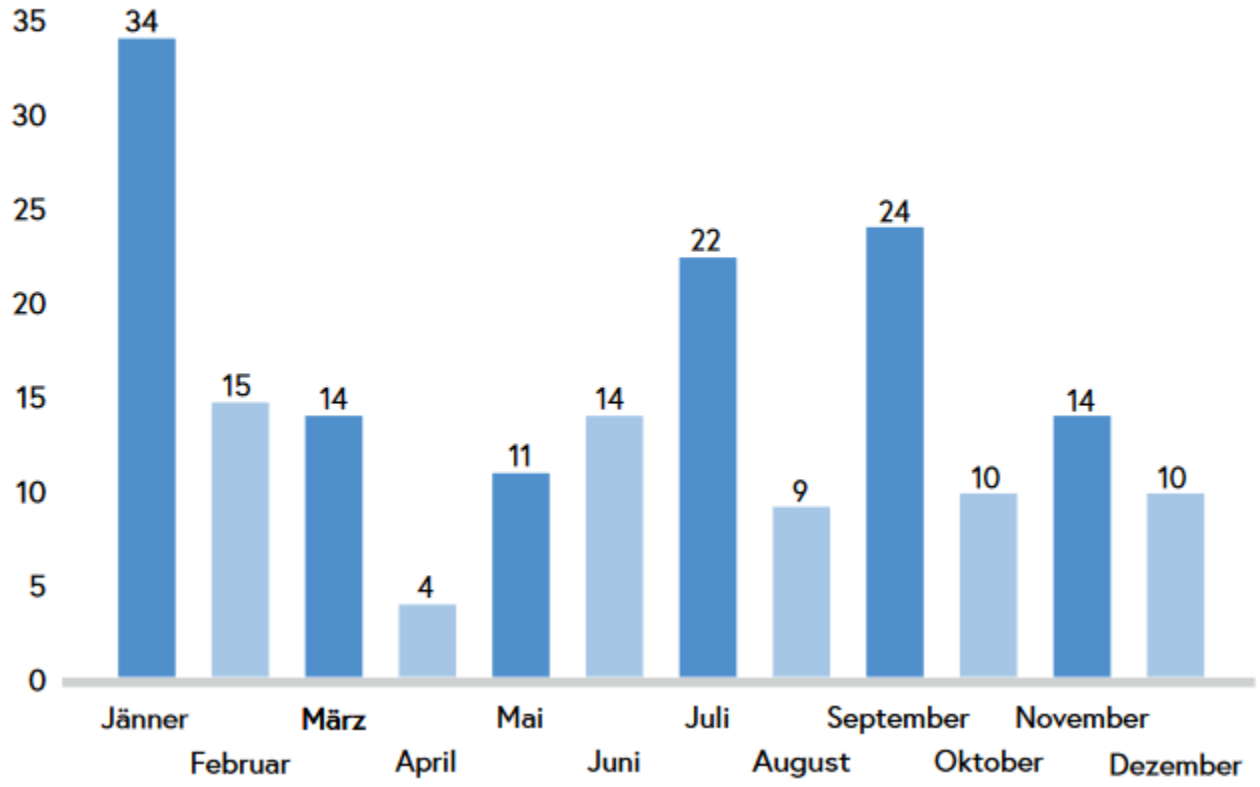
Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

Ransomware

Insgesamt wurden im Jahr 2022 österreichweit 181 Fälle von zur Anzeige gebracht.



Bundesministeriu
Inneres

ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT. – Tor Browser

File Edit View History Bookmarks Tools Help

ALL YOUR FILES HAVE BEEN ×

```
root      /vmfs/volumes# ls
 bb.xlsx.basta     'IDA Freeware 7.6.desktop.basta'   readme.txt
 bcc                kk.txt.basta                      ssd1.pcap.basta
 d1e                ll.txt.basta                      sss.jpeg.basta
 dd.docx.basta      logo.png.basta                    testing.elf.basta
 debugf.py.basta    pp.elf.basta
 ff.doc.basta       pp.txt.basta
root(     :/vmfs/volumes# cat readme.txt
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://                                                          .onion/

Your company id for log in: 01e

root(     :/vmfs/volumes#
ENCRYPTION
Done time: 14.5620 seconds, encrypted: 0.0016 gb
```

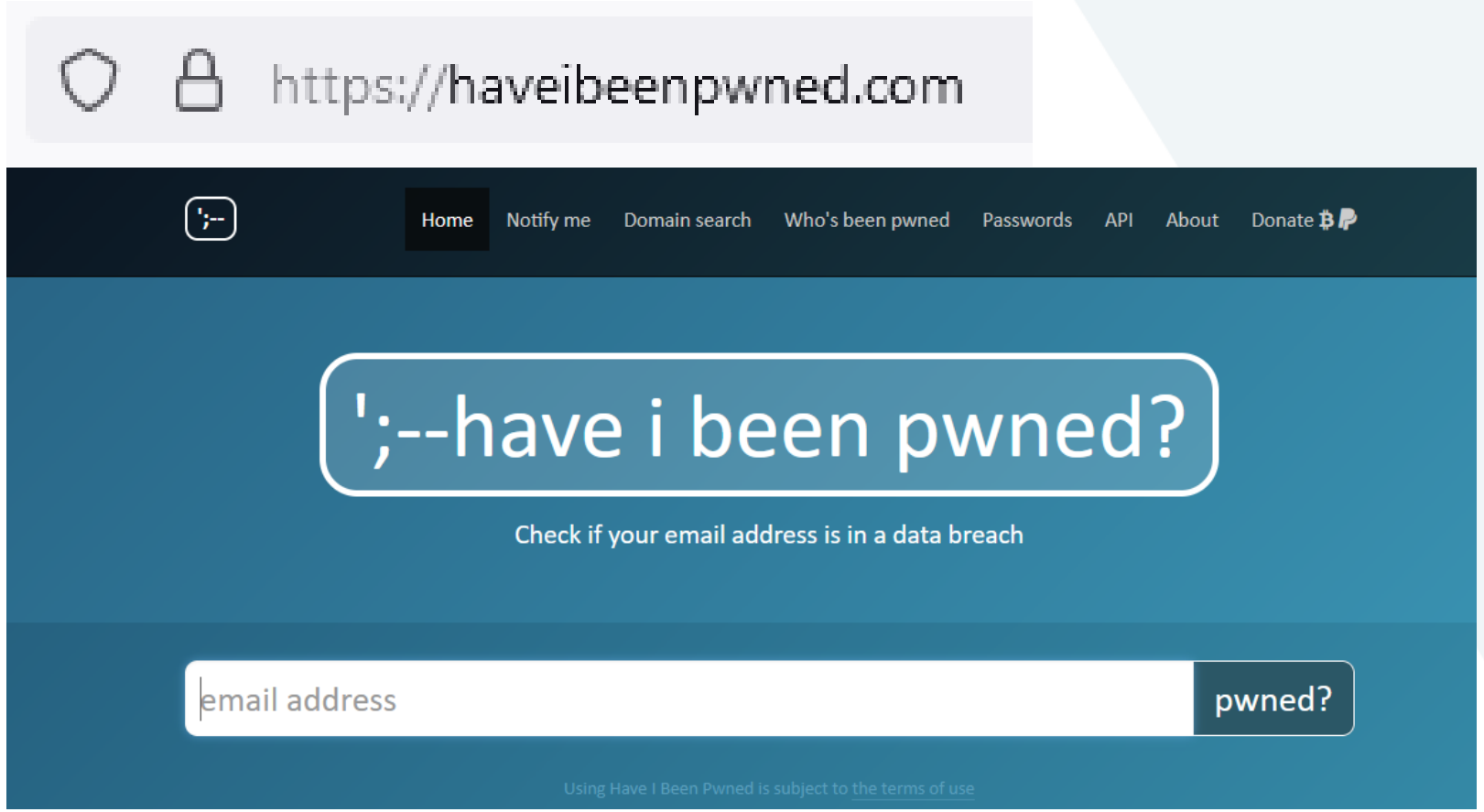
Enter your decryption key here..

Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME
COMPETENCE
CENTER

Phishing


https://haveibeenpwned.com
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
email address
pwned?
Using Have I Been Pwned is subject to the terms of use

Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

https://www.nomoreransom.org/de/decryption-tools.html

NO MORE RANSOM

Partner Über das Projekt Deutsch

Home Crypto Sheriff Ransomware Q&A Tipps zur Vorbeugung **Entschlüsselungs-Werkzeuge**

Straftat melden

Ent-schlüsselungs-Werkzeuge

WICHTIGER HINWEIS: Bevor Sie mit dem Herunterladen und der Problemlösung beginnen, lesen Sie bitte die How-To Anleitung. Stellen Sie sicher, dass Sie die Malware von Ihren System zunächst entfernen, sonst wird Ihr System ständig weiter gesperrt oder wieder verschlüsselt. Jede vertrauenswürdige Antiviren-Lösung kann Sie dabei unterstützen.

Lockbit

Lockbit 3.0 Ransom

Bundesministerium
Inneres

Bundeskriminalamt

C4 CYBERCRIME COMPETENCE CENTER

Aufklärungsarbeit anhand eines aktuellen Falles


THIS HIDDEN SITE HAS BEEN SEIZED
Hive
The Federal Bureau of Investigation seized this site
as part of a coordinated law enforcement action taken against Hive Ransomware.
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
EUROPOL
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE
BKA
CYBERCRIME
BKA
This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the
Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

Wie funktioniert das **Tor**-Netzwerk?

1. Zwiebelverfahren: Tor „verpackt" u.a. die Zieladresse in mehreren „Schichten" und verschleiert sie so.
2. Über zufällige Knotenpunkte (nur vorheriger und nachfolgender Server ist jeweils bekannt) entsteht eine verschlüsselte, nur mit sehr viel Aufwand zurückverfolgbare Verbindung.
3. Mit Tor ist sowohl das Surfen im frei verfügbaren Internet als auch im Darknet möglich.
4. Tor verschlüsselt das letzte Teilstück zum Zielserver nicht, eine Verschlüsselung durch andere Instanzen ist hingegen möglich.

Bundesministerium
Inneres
Bundeskriminalamt

C4 CYBERCRIME COMPETENCE CENTER

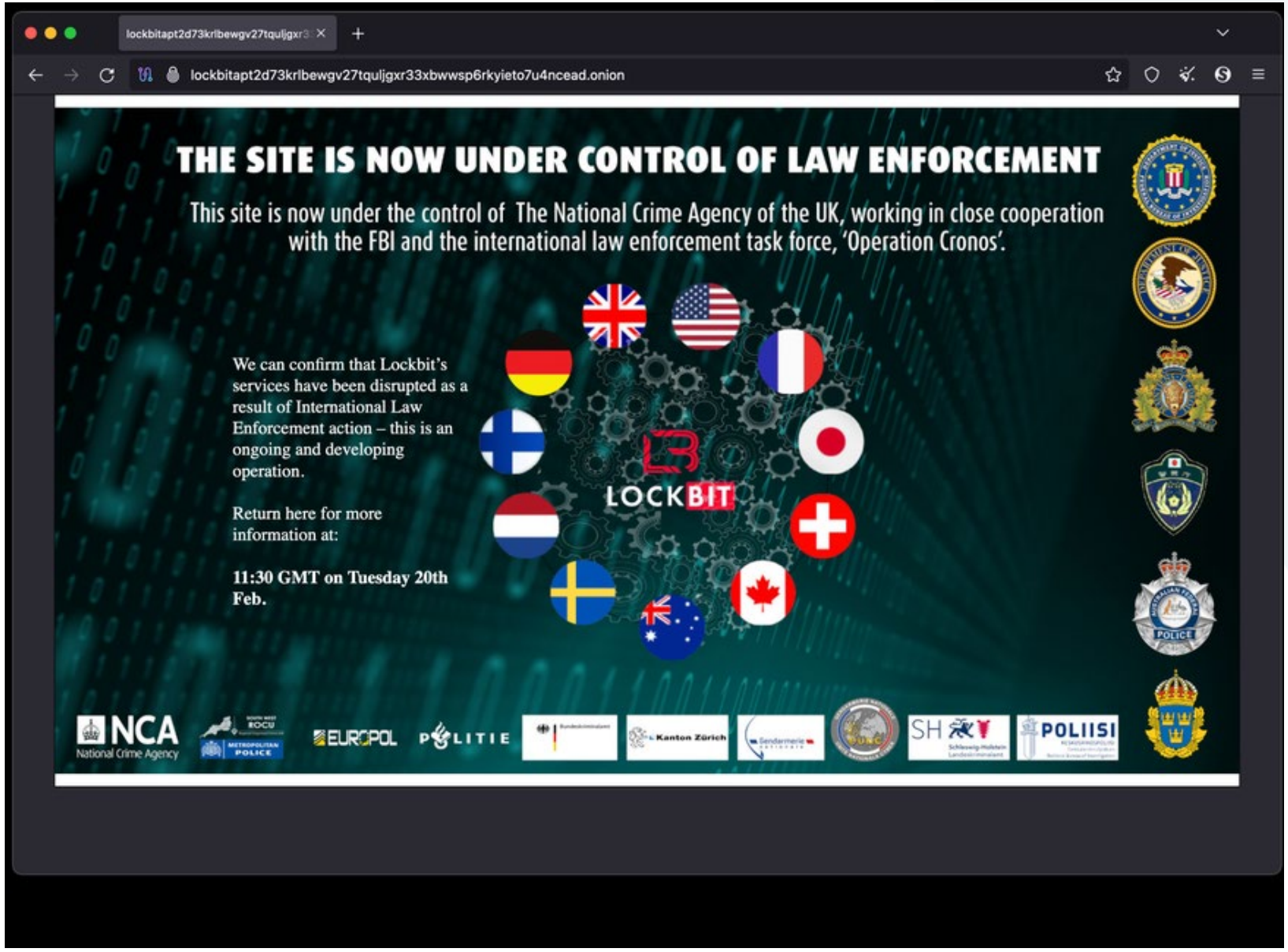
Schwerer Schlag gegen russische Ransomware-Bande LockBit – Schweiz beteiligt

Ermittler haben Teile der Darknet-Infrastruktur der berüchtigten Cyberkriminellen lahmgelegt. Das wissen wir über «Operation Cronos», die gemäss Europol auch Server in der Schweiz betrifft.

Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

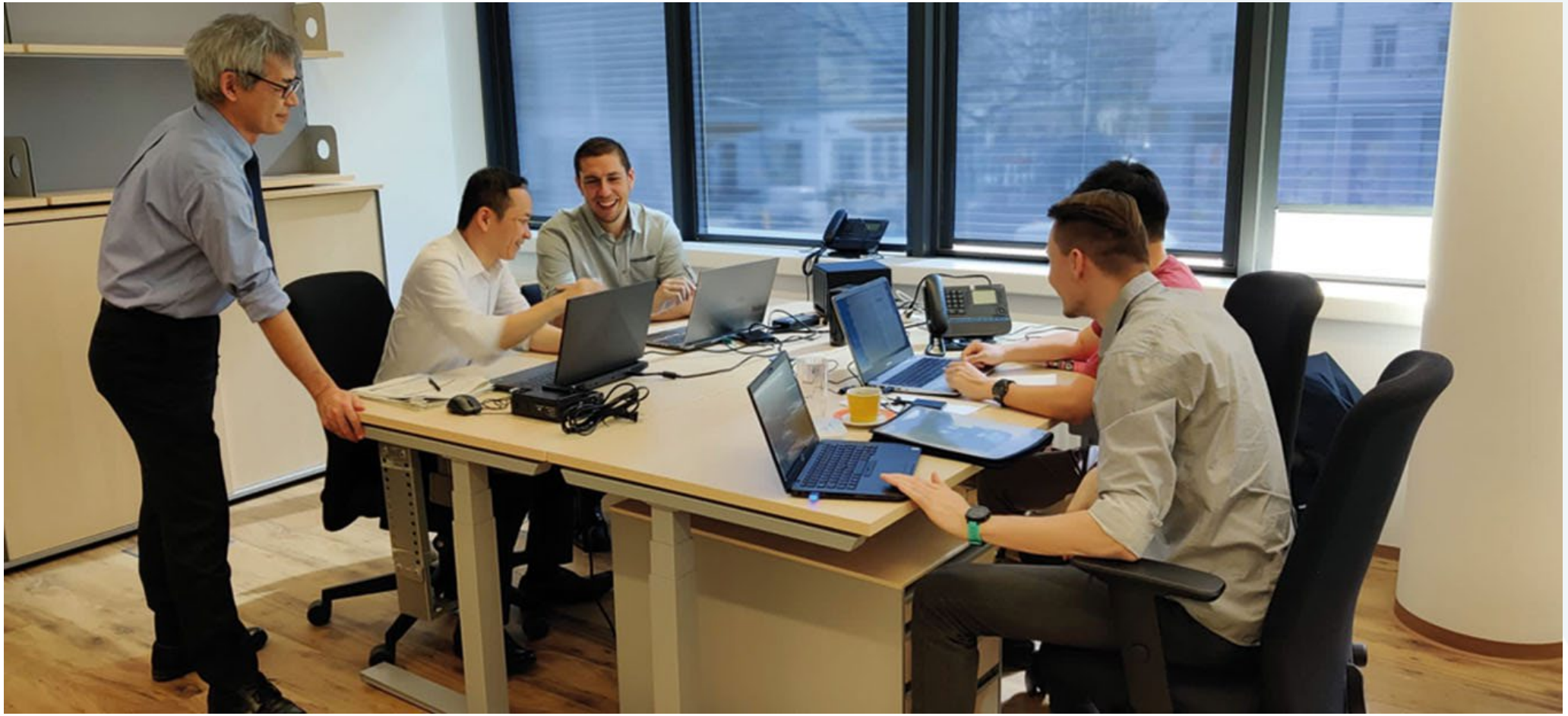


Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME
COMPETENCE
CENTER

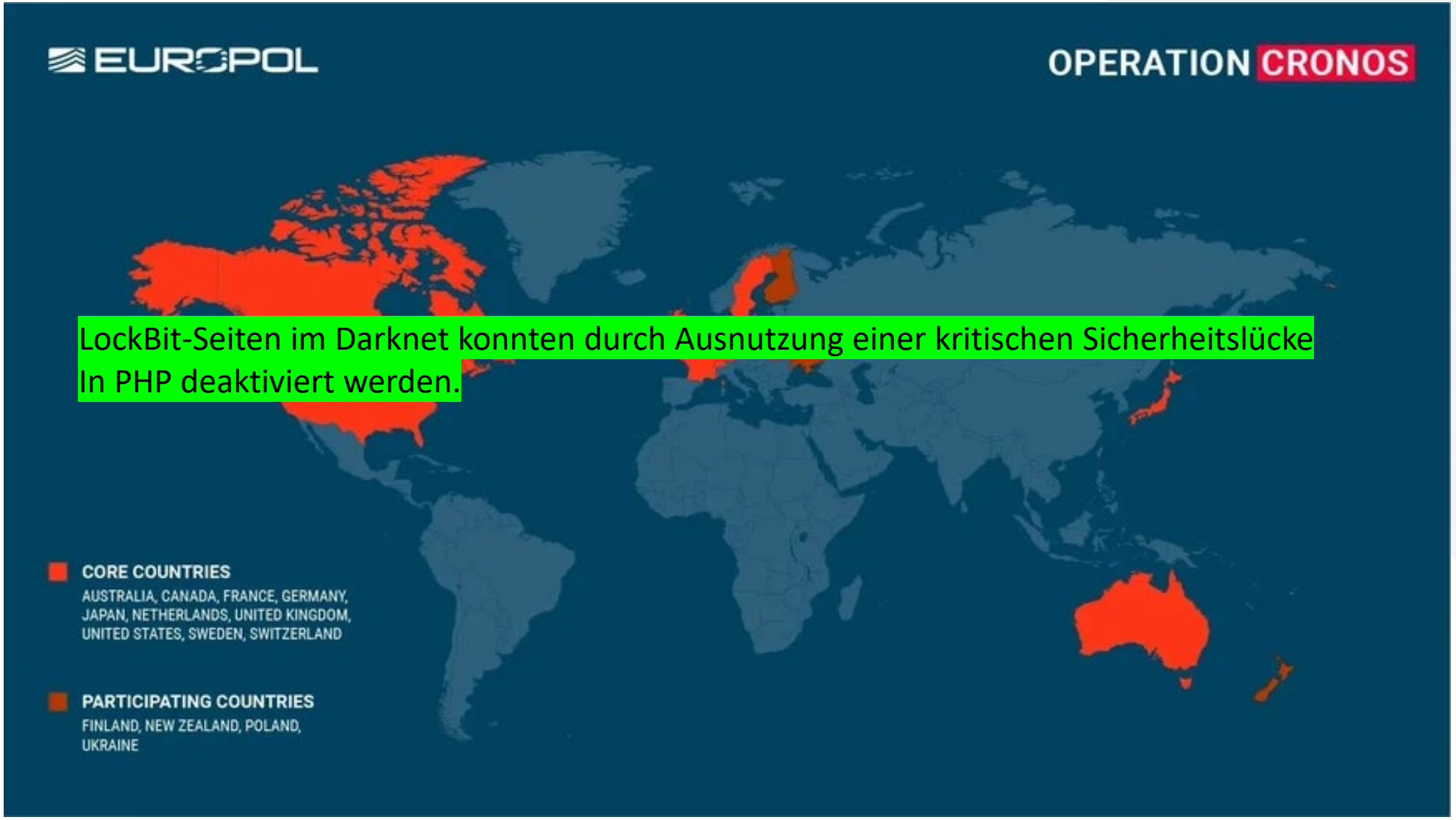
Zusammenarbeit zwischen C4 und japanischer Polizei.



Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME
COMPETENCE
CENTER



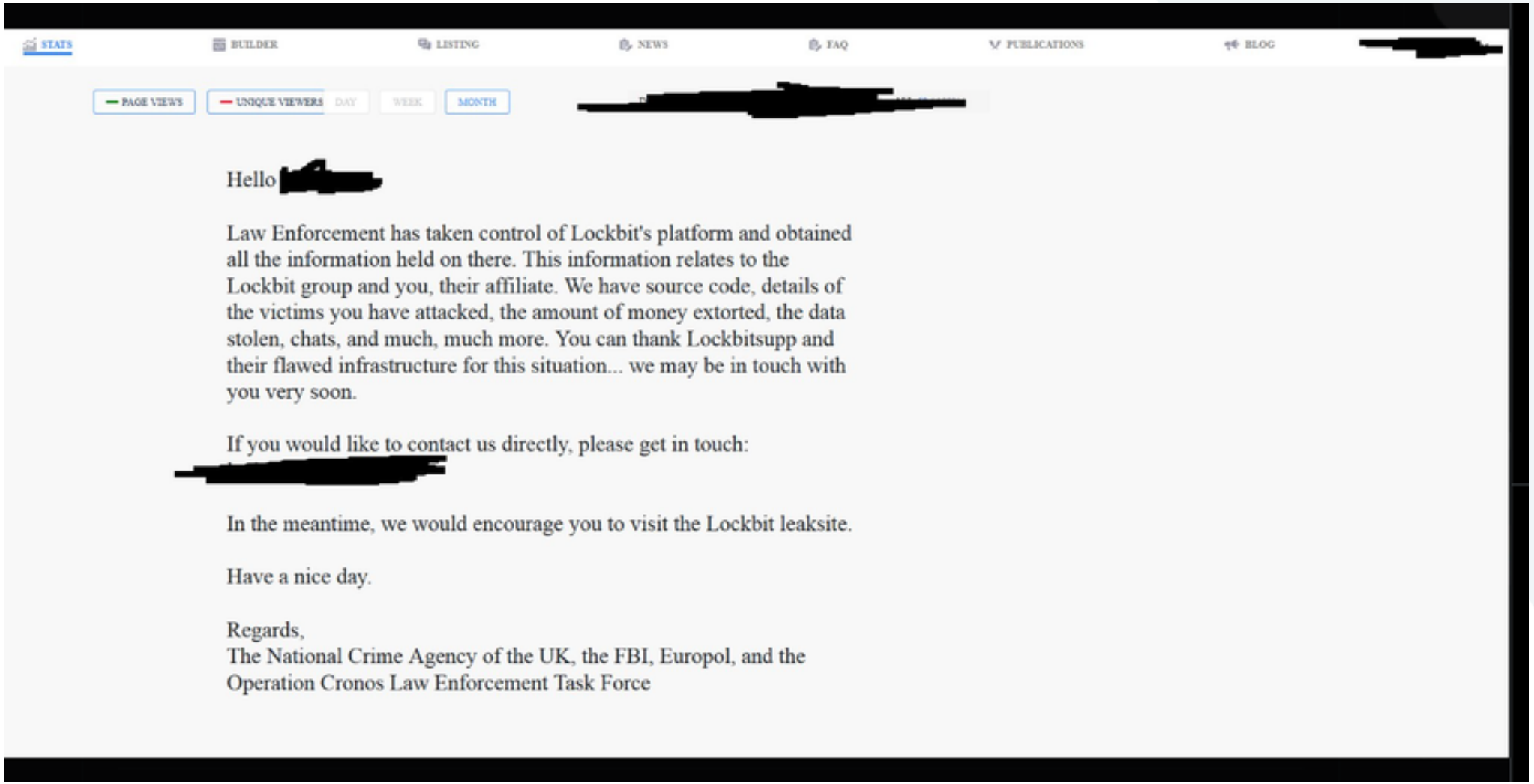
LockBit-Seiten im Darknet konnten durch Ausnutzung einer kritischen Sicherheitslücke In PHP deaktiviert werden.

Bundesministerium
Inneres

Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

Die wichtigsten Punkte im Überblick:


STATS
BUILDER
LISTING
NEWS
FAQ
PUBLICATIONS
BLOG
PAGE VIEWS
UNIQUE VIEWERS
DAY
WEEK
MONTH
Hello
Law Enforcement has taken control of Lockbit's platform and obtained all the information held on there. This information relates to the Lockbit group and you, their affiliate. We have source code, details of the victims you have attacked, the amount of money extorted, the data stolen, chats, and much, much more. You can thank Lockbitsupp and their flawed infrastructure for this situation... we may be in touch with you very soon.
If you would like to contact us directly, please get in touch:
In the meantime, we would encourage you to visit the Lockbit leaksite.
Have a nice day.
Regards,
The National Crime Agency of the UK, the FBI, Europol, and the Operation Cronos Law Enforcement Task Force

Bundesministerium
Inneres

Bundeskriminalamt

Subject: Important Security Notice from Lockbit - Action Required

Dear Valued Affiliate,

We are reaching out to inform you of a recent security incident that may have affected your personal information. Lockbit takes the security of your data seriously, and we are committed to maintaining the highest standards of data protection.

What Happened?
Our team recently detected unauthorized access to our systems, which we believe was carried out by a group known as the NCA. Upon discovering the breach, we immediately launched an investigation with the assistance of cybersecurity experts and have taken steps to secure our network.

What Information Was Involved?
The breach may have involved access to personal information, including names, email addresses, and encrypted passwords. At this time, there is no evidence that any financial information or social security numbers were accessed.

What We Are Doing
In response to this incident, we have:

Implemented additional security measures to prevent future breaches.
Engaged with other operators and cybceriminals to investigate the breach.
Provided free credit monitoring services for 12 months to those affected, to help protect against potential identity theft. You will receive a separate email with instructions on how to activate this service.

What You Can Do
To further protect your information, we recommend the following actions:

- Reset Your Password: Please change your password for your Lockbit account and any other accounts where you use the same or similar passwords.
- Enable Multi-Factor Authentication (MFA): If you have not already done so, we strongly recommend enabling MFA on your Lockbit account and other online accounts. This adds an extra layer of security beyond just a password.
- Monitor Your Accounts: Keep an eye on your account statements and credit reports for any unusual activity.

For More Information
If you have any questions or need further assistance, please do not hesitate to contact our customer support team at support@lock***.com or call us at 1-900-LOCKBIT.

We deeply regret any inconvenience or concern this incident may cause you. Lockbit is committed to continuously improving our security measures and ensuring the integrity and confidentiality of your data.

Sincerely,
The Lockbit Team

C4 CYBERCRIME COMPETENCE CENTER

Bundesministerium
Inneres
Bundeskriminalamt

CYBERCRIME COMPETENCE CENTER

Aktuelle Fälle - Urteile

SN.AT / SALZBURG / CHRONIK

Millionenschwerer Cyberbetrug: Acht und sechs Jahre Haft für zwei Israelis in Salzburg

Nach Mordauftrag an der Ex im Darknet verhaftet

Wegen eines Sorgerechtsstreit soll der Angeklagte, der in Graz vor Gericht steht, einen Mörder für seine Ex-Frau gesucht haben. Dabei hatte er doppeltes Pech: Er fiel auf einen Betrug herein und dem FBI auf.

IT SECURITY

IT der Verkehrsbüro Group nach Cyberangriff noch immer beeinträchtigt

Rückkehr zum Normalbetrieb werde "noch ein bisschen dauern" – Man könne laut Konzernsprecherin aber "alles servicieren"

Bundesministerium
Inneres

Bundeskriminalamt

C4
CYBERCRIME
COMPETENCE
CENTER

Danke für die Aufmerksamkeit!