

**KHK Borries und KHK Huwald**

**LKA 724 Cybercrime**

**ZAC Berlin – Zentrale Ansprechstelle Cybercrime**





Basler Schulnetz gehackt  
Darknet

**Update / Vier Rettungsstellen in Berlin betroffen**  
Cyber-Angriff auf Krankenhäuser als bekannt

Cyber-Partei  
Auf die E-Mails  
Möglich

Cybergang Alpin  
Rüstungen

Heime und Kliniken in Berlin

# Johannesstift ringt weiter mit den Folgen des Cyber-Angriffs

Do 24.10.24 | 18:11 Uhr | Von Yasser Speck

## Cyberangriff auf die dena

Cyberangriff auf die dena-Serverinfrastruktur - dena telefonisch und per Mail nicht erreichbar. IT-Sicherheitsmaßnahmen wurden ergriffen. Die dena-Pressestelle ist über die bekannten Mobilfunknummern erreichbar.

Berlin, den 14. November 2023. Die dena wurde am Wochenende durch einen Cyberangriff attackiert. Dabei wurde die



## Cyberangriff Deutsche Flugsicherung von Hackern angegriffen

Bürokommunikation lahmgelegt: Hacker haben Flugsicherung angegriffen. Die Auswirkungen sind

01.09.2024, 18:23 Uhr

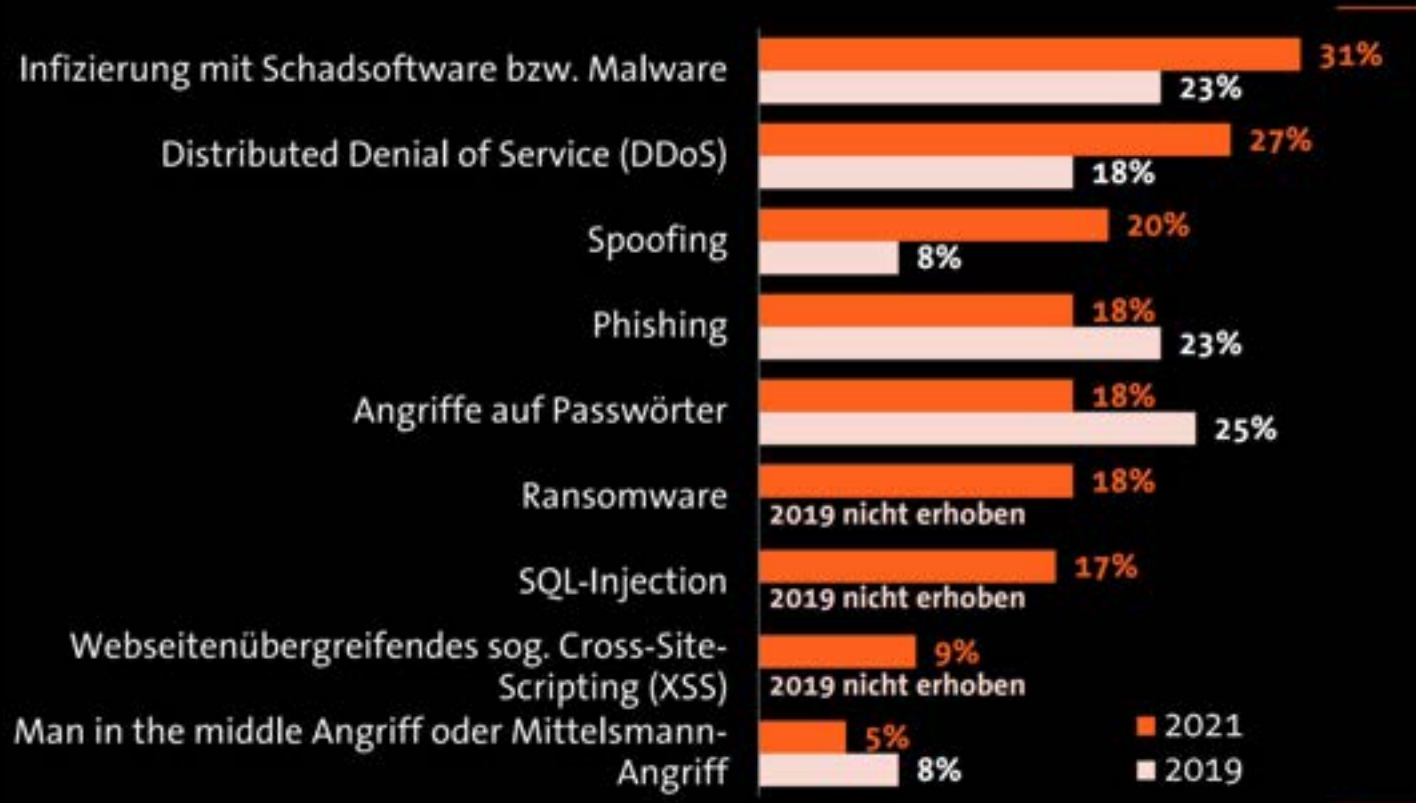
Rettungsdienst

Die Cyber-Experten...

Diakonie, Mariendorfer Weg  
powicz | Bild: imago images/Sch  
stift-Diakonie getroff  
Systeme noch nicht  
t bislang unklar.  
Yasser Speck  
der Johannesstift-Diak  
Systeme dauert immer  
Bedrohungslage und  
schland und andere Län

## Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

**86%**

der Unternehmen einen Schaden verursacht – 2019 waren es erst 70%.

1989

2005

HEUTE

INTERNET

INTERNET 2.0

INTERNET DER DINGE

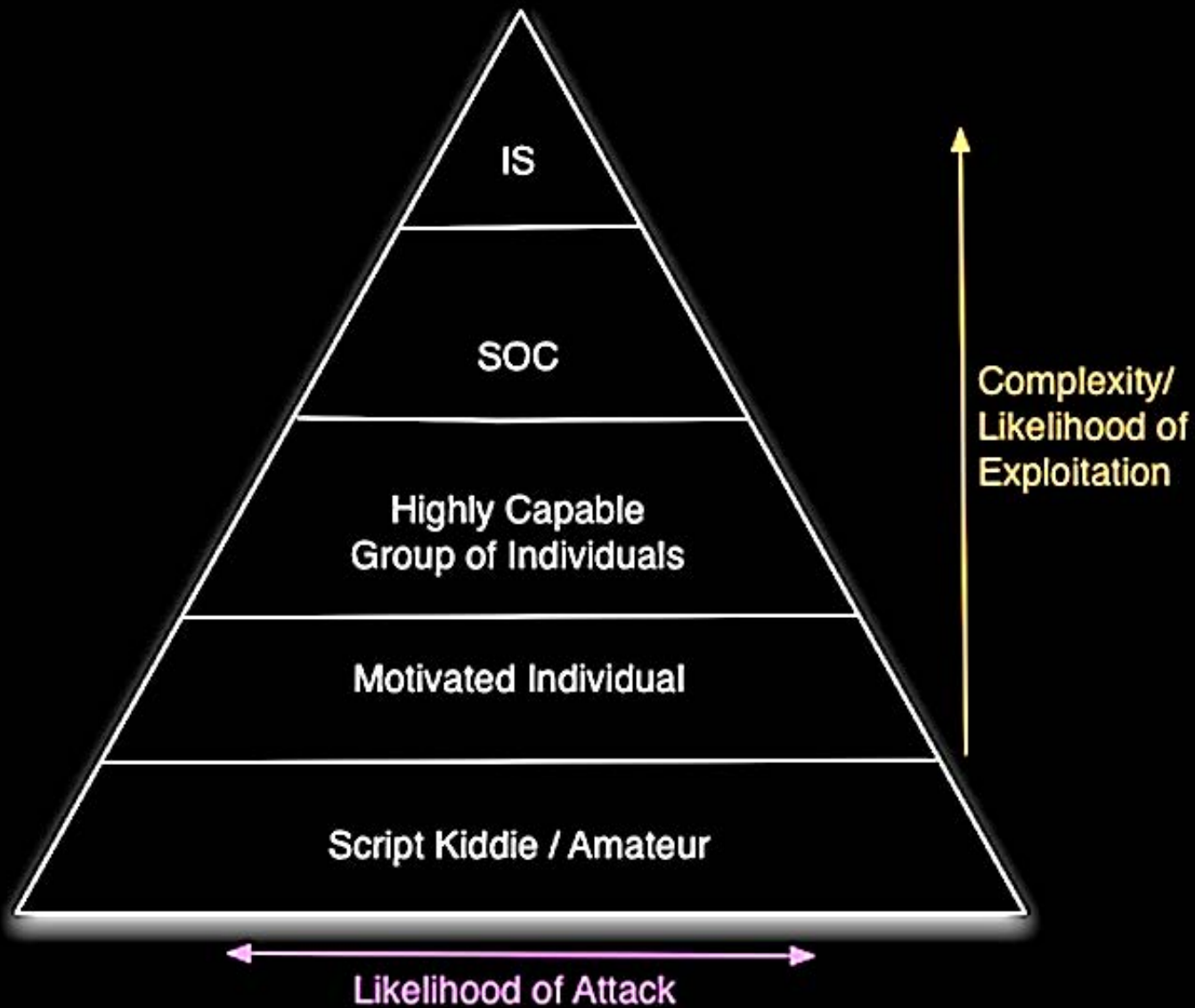
INDUSTRIE 4.0 RELEVANT

- + proprietärer Kram
- + legacy Zeugs
- + mobile Gedöns

Unterscheidung von Angriffszielen in ...

1. Unternehmen, die bereits angegriffen wurden
2. Unternehmen, die bereits angegriffen wurden\*

\* jedoch noch nichts ahnen



IS = Intelligence services

SOC = Serious organized Crime

Welcome to  RansomLook  !

March 25Th, 2025

Currently tracking **413** groups across **1596** relays & mirrors -  
**479** currently online

Got **541** DLS, **819** FS, **214** Chats and **22** Admin/Affiliates  
pages.

Currently tracking **117** forums & markets across **204** relays &  
mirrors - **96** currently online

Currently tracking **284** telegram channels.

There have been **53** posts within the last 24 hours

There have been **636** posts within the month of march

There have been **2412** posts within the last 90 days

There have been **2336** posts within the year of 2025

There have been **20743** posts since the dawn of ransomlook

There are **157** custom parsers indexing posts



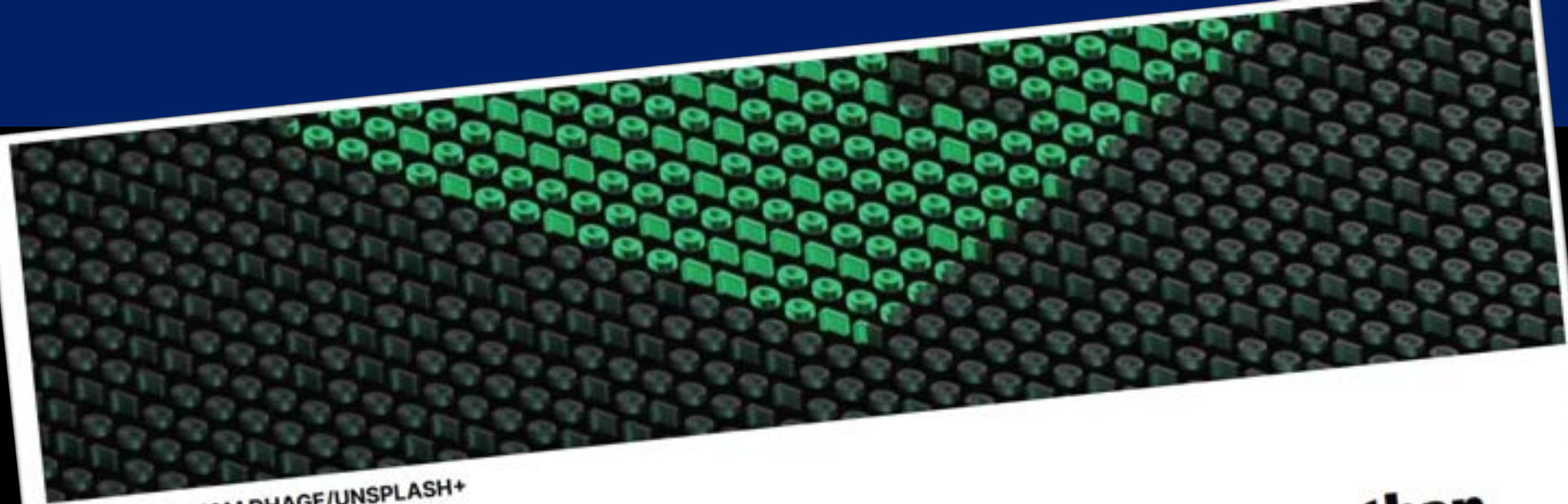


IMAGE: SHUBHAM DHAGE/UNSPLASH+

Jonathan Greig  
August 15th, 2024

## **Ransomware gangs rake in more than \$450 million in first half of 2024**

More than \$459 million was extorted from victims of ransomware attacks in the first half of 2024, highlighting a growing crisis that has affected all organizations from major corporations to local governments and hospitals, according to a new report.

Blockchain research company Chainalysis tracked cryptocurrency payments made to wallets controlled by ransomware actors, finding a \$10 million increase in the amount of money earned from those criminals compared to last year's figure of \$449.1 million.





# ALL YOUR **IMPORTANT FILES** ARE ENCRYPTED!

Any attempts to restore your files with the third-party software will be **fatal for your files!**  
Restore you data possible only buying private key from us.

There is only one way to get your files back:

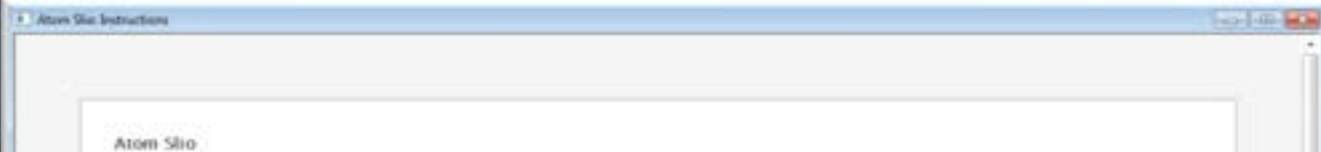


lockbitapt6vx5713eeqjohwgcglmutr3a35nygvokja5uuccip4ykyd.onion

**LOCKBIT 3.0** **LEAKED DATA**  TWITTER  PRESS ABOUT US

- HOW TO BUY BITCOIN
- AFFILIATE RULES
- CONTACT US
- MIRRORS

<b>crowe.com.za</b> 4D 22h 10m 51s Crowe LLP is a public accounting, consulting and technology firm. Crowe uses its deep industry expertise to provide audit services to public and private entities. The firm and its subsidiaries also Updated: 30 Jan, 2024, 11:04 UTC 629	<b>clackamas.edu</b> 16D 11h 33m 43s Clackamas Community College Updated: 30 Jan, 2024, 09:29 UTC 192	<b>ips-securex.com</b> 06h 00m 19s Formed in 1991 and with offices and partners throughout Asia Pacific, IPS Securex has successfully implemented many complex integrated security systems throughout the Updated: 30 Jan, 2024, 07:39 UTC 13931	<b>grimm</b> 9D 18h 16m grimme.dk Updated: 30 Jan, 2024, 11:04 UTC 112
<b>ese.com</b> 13D 03h 07m 52s ESE is the market leader for temporary storage solutions for waste and recyclable materials. We offer a large selection of high-quality products and services, which enable our customers in the Updated: 29 Jan, 2024, 19:07 UTC 622	<b>amenitek.com</b> PUBLISHED AMENITEK Audio, Technology, Video, Computer, Security, and Electrical Systems Installation 14 Williamstown Road Lanesborough, MA 01237 tel (413) 776-0354 fax (413) 776-0355 Updated: 29 Jan, 2024, 18:55 UTC 6409	<b>lyonshipyard.com</b> 7D 19h 54m 31s Lyon Shipyard is a customer focused, family-owned and operated, ship repair facility on the Elizabeth River in Norfolk, VA established in 1928. Lyon Shipyard, Inc. serves as a full service Updated: 29 Jan, 2024, 06:48 UTC 2819	<b>sierrafrost</b> 5D 19h Sierra Front Group has e Cloud Hosting, Event W Hosting, Network Design much more. Updated: 29 Jan, 2024, 06:48 UTC 0
<b>stjohnrochester.org</b> 20h 33m 20s	<b>securinux.net</b> \$ 100000	<b>carsonteam.com</b> PUBLISHED	<b>davidsb</b> PUBLISHED



Atom Silo  
instructions

## WARNING! YOUR FILES ARE ENCRYPTED!

We are AtomSilo. Sorry to inform you that all your files are encrypted. But don't worry, your files are safe. Any forced shutdown or attempts to restore your system will result in permanent data loss. The only way to decrypt your files is to pay for the decryption tool. The price is 0.001 BTC. If you pay within 48 hours, you can get a 50% discount. We only accept Bitcoin payments. You have five days to decide whether to pay or not.

Time started

Survival time : -38

You can contact us with the following email:

Email: [arvan@atomsilo.com](mailto:arvan@atomsilo.com)

If this email can't be contacted, you can find the latest email address:

<http://mhdehvkomeabaa?gsmamk8gn4jgnx1waght5yb5th1k>



## All Of Your Files Have Been Encrypted By XINOF!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, please send an email to [mrpicokins@criptext.com](mailto:mrpicokins@criptext.com)

You have to pay for decryption in Bitcoin. We will provide you with a decryption tool. You have to 48 hours(2 Day) To contact in case of no answer in 6 hours email us. The crypter person username : [mrpicokins@criptext.com](mailto:mrpicokins@criptext.com) your SYSTEM ID is : **458CCEE7**

- Attention!**
- DO NOT pay any money before decrypting the test files.
  - DO NOT trust any intermediaries, they won't help you and will steal your money.
  - DO NOT reply to other emails, ONLY the two emails can help you.
  - Do not rename encrypted files.
  - Do not try to decrypt your data using third party software.

**What is our decryption guarantee?**

- Before paying you can send us up to 3 test files for free (databases, backups, large excel sheets, etc.)

**You only have LIMITED time to get back your files!**

### STOPDecrypter

Settings About

[+] Loaded key for ID: 6se9RalxXF9m70zWmx7nL3bVRp691w4SNY8UCir0  
[+] Loaded key for ID: **D02NfEP94dKuo3faH1wqgo5f9uqRw2Etn2P3VB**

Selected directory: D:\\_Analysis\STOP\rumba\Case0  
Starting decryption...

[+] File: D:\\_Analysis\STOP\rumba\Case0\Chrysanthemum.jpg.rumba  
[+] Decrypted: D:\\_Analysis\STOP\rumba\Case0\Chrysanthemum.jpg

[+] File: D:\\_Analysis\STOP\rumba\Case0\Desert.jpg.rumba  
[+] Decrypted: D:\\_Analysis\STOP\rumba\Case0\Desert.jpg

[+] File: D:\\_Analysis\STOP\rumba\Case0\zeroes.jpg.rumba  
[+] Decrypted: D:\\_Analysis\STOP\rumba\Case0\zeroes.jpg

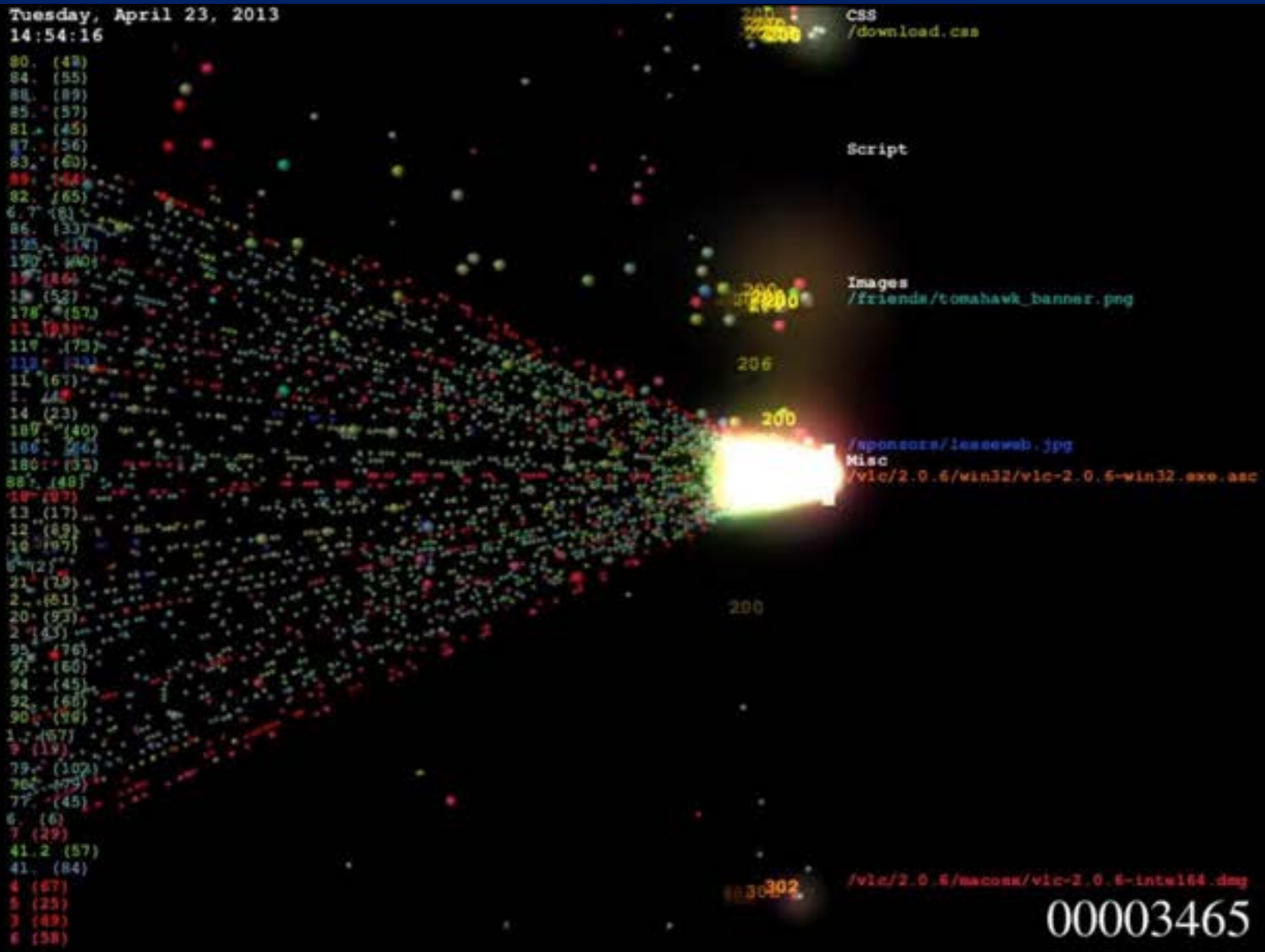
Decrypted 3 files!

Done!

Decrypt







# Medienbericht: Cyberkriminelle spähren angeblich Regierungs-IT aus

Das Informationstechnikzentrum des Bundes warnt Mitarbeiter vor abgegriffener E-Mail-Kommunikation. Die Verantwortlichen wollten jedoch nur sensibilisieren.



(Bild: JARIRYAWAT/Shutterstock.com)

11.05.2023, 00:01 Uhr | Lesezeit: 3 Min. | Security

Von Marie-Claire Koch

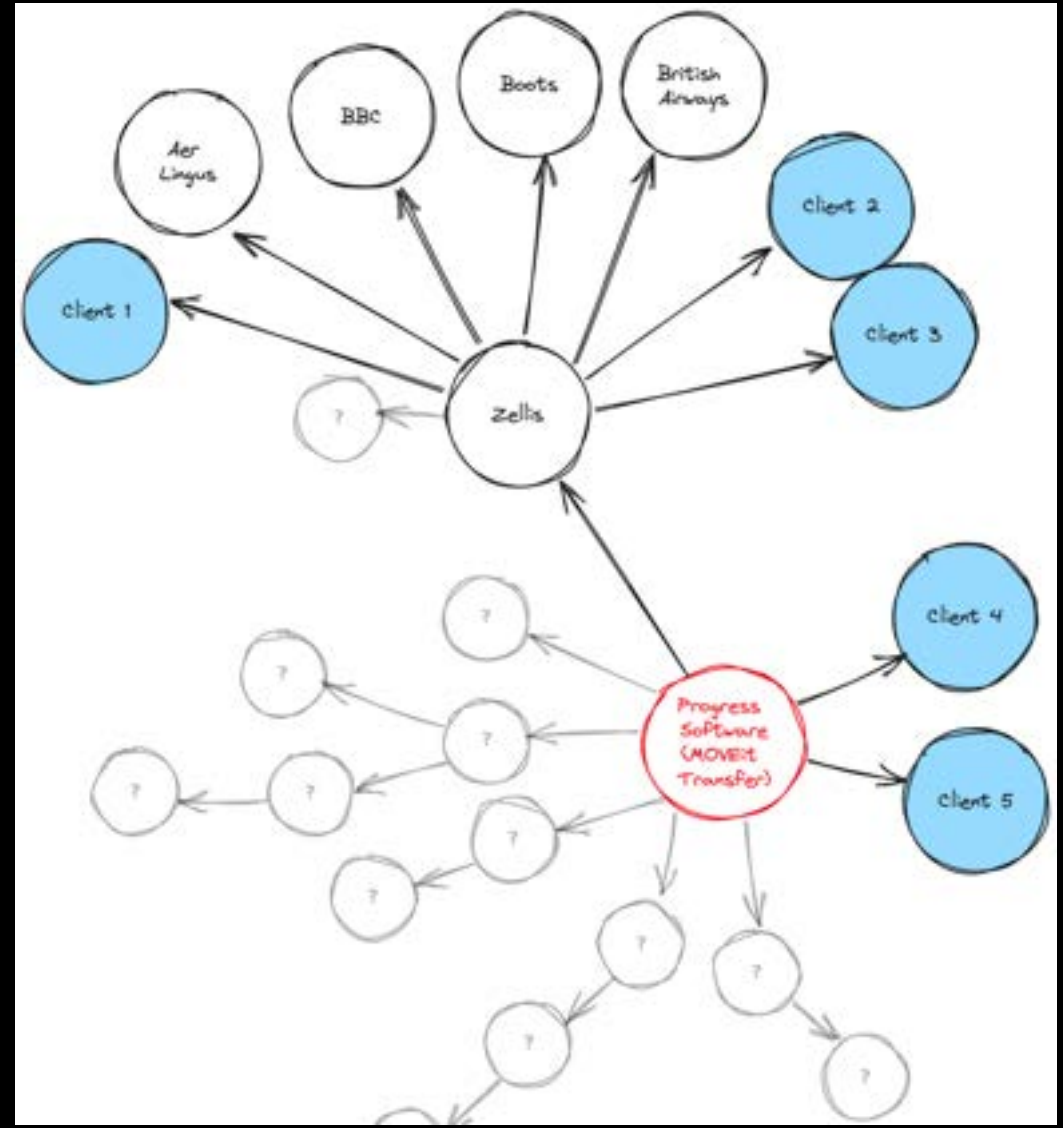
"Unbekannte Hacker" haben Berichten zufolge drei für Ministerien und Behörden arbeitende IT-Unternehmen ausgespäht. Das gehe aus einem Warnschreiben des Informationstechnikzentrums des Bundes (ITZ Bund) von Ende April hervor, das dem Bayerischen Rundfunk (BR) vorliegt. Demnach sollen die Angreifer "sehr wahrscheinlich" die E-Mail-Kommunikation bei den betroffenen Firm

# BR-RECHERCHE: HACKERANGRIFFE AUF DREI IT-DIENSTLEISTER DES BUNDES

Mai 11, 2023 | Hackerangriff aktuell | 0



Wie der Bayerische Rundfunk berichtet, haben unbekannte Cyberkriminelle offenbar drei deutsche IT-Unternehmen angegriffen, die für Bundesministerien und Behörden arbeiten. Das gehe aus einem Warnschreiben des Informationstechnikzentrums Bund (ITZ Bund) von Ende April hervor, das dem BR vorliegt. Laut dem Warnschreiben wurden Daten ausgespäht und sehr wahrscheinlich große Mengen der E-Mail-Kommunikation abgefangen. Die erbeuteten E-Mails enthielten unter anderem personenbezogene Daten, Telefonnummern, aktuelle Projekte, Mailverläufe und angehängte Dokumente. Von dem Hackerangriff betroffen waren die Dortmunder IT-Unternehmen Adesso und M



## MOVEit Transfer Vulnerability: Lack of Supply Chain Visibility Exacerbates Breach

 Risk Ledger  
4,549 followers

June 14, 2023

Once a critical vulnerability has been identified, how long does it take for all affected organisations to realise they might be affected as well and to then investigate, identify if and how they have been impacted, and respond accordingly to mitigate the risk?

## Cyberattac

Wie hoch ist der  
der auf Cyberatt

**28%**

57,7 Mrd. Euro  
Andere  
Schäden

Basis: Alle Unternehmen, die in

## Datendiebstah

Welche der folgende  
Unternehmen gesto

Kommunikationsdate

Zugangsdaten

Geistiges Eigentum z. B. Patent  
aus Forschung

**in Prozent**

Basis: Alle Unternehmen, die in den letzten

## Die psychischen Folgen eines Ransomware-Angriffs sind gravierend

25. Oktober, 2022 05:11

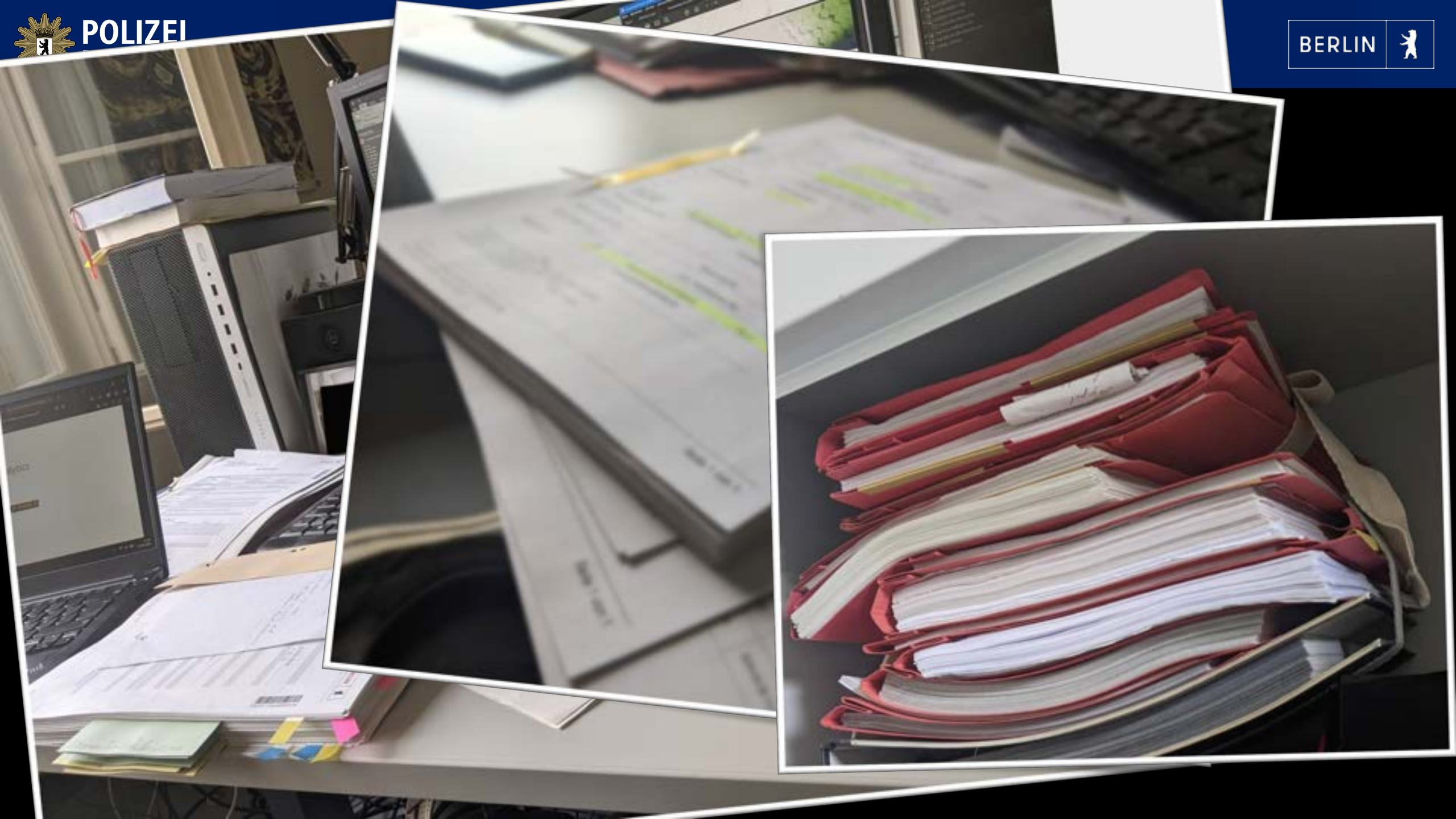


Der Spezialist für Informationssicherheit Northwave hat eine wissenschaftliche Untersuchung zu den psychischen Auswirkungen großer Ransomware-Angriffe gegen Unternehmen durchgeführt. Die Ergebnisse zeigen, welch tiefe Spuren eine solche Krise bei allen Betroffenen hinterlässt.

Zugleich machen sie deutlich, dass es auch nach der Überwindung des Angriffs selbst noch lange dauern kann, bis bei den IT- und Sicherheitsteams wieder Normalität einkehrt.







## 'Operation Endgame' Hits Malware Delivery Platforms

17 Comments

May 30, 2024



Law enforcement agencies in the United States and Europe today announced Operation Endgame, a coordinated action against some of the most popular cybercrime platforms for delivering ransomware and data-stealing malware. Dubbed “the largest ever operation against botnets,” the international effort is being billed as the opening salvo in an ongoing campaign targeting advanced malware

“droppers” or “loaders” like IcedID, Smokeloader and Trickbot.

**THIS WEBSITE HAS BEEN SEIZED**

... seized this site as part of a  
... ALPHV ...



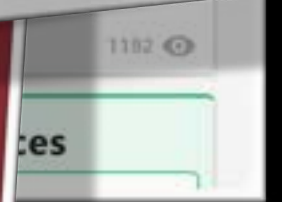
HESSEN

# THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.



2



# LET'S TALK

## GEFÄHRDUNGSLAGE CYBERSICHERHEIT: WIE GUT SIND SIE AUFGESTELLT?

Lars Huwald  
Astrid Frohloff  
Rainer Stock



### Interview mit Olaf Borries

## „Es wird Tätern viel zu häufig leicht gemacht“

Olaf Borries, Kriminalhauptkommissar bei der ZAC – Zentrale Ansprechstelle Cybercrime für die Wirtschaft im Landeskriminalamt Berlin – ist Experte beim Thema Cybercrime. Im Gespräch mit dem KV-Blatt erzählt er, welche Präventionsmaßnahmen Praxen treffen sollten.

Warum sind gerade Arztpraxen beliebte Angriffsziele von Cybercrime? Welche Motivation steckt hinter einem solchen Angriff?

In Arztpraxen werden sehr viele sensible Daten erzeugt und verwahrt, ohne die eine Praxis nicht arbeiten kann und die auch ein hohes Schadenspotential besitzen. Sollten Daten hier abgefließen oder verschlüsselt sein, so ist der Handlungsdruck entsprechend hoch. Als Motiviv sind sehr häufig, besonders im Bereich der Erpressung – Stichwort „Ransomware“ –, finanzielle Interessen zu nennen.



praxis aufzubauen, zum Beispiel durch die Verschlüsselung der Daten. Eine Entschlüsselung erfolgt dann erst gegen die Zahlung eines Lösegeldes. Als Polizei raten wir grundsätzlich davon ab, zu zahlen. In der letzten Zeit kam es immer häufiger dazu, dass die Daten der geschädigten Institution vorher heruntergeladen wurden und es im Falle der Nichtbezahlung zur Drohung der Veröffentlichung der Daten führte. Ein weiterer Bereich – nach unserer Erfahrung nicht so im Fokus bei Arztpraxen – sind so genannte DDoS-Angriffe. Darunter versteht man eine Überlastung von Internetseiten durch massive Anfragen, sodass ein Aufrufen der Seite nicht möglich ist. Dies wird dann überfalls mit Erpressung verbunden.



# VKIU STADT KE SS



> 95%



**KHK Borries und KHK Huwald**  
**LKA 724 Cybercrime**  
**ZAC Berlin – Zentrale Ansprechstelle Cybercrime**

+49 30 4664 972 972  
[zac@polizei.berlin.de](mailto:zac@polizei.berlin.de)



für den harten Kern  
fortlaufendes  
Sicherheitskonzept  
clevere Datensicherungen  
Rollen- und Rechtenkonzepte  
Awareness -> Faktor Mensch  
Notfallpläne

KHK Borries und KHK Huwald  
LKA 724 Cybercrime  
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

+49 30 4664 972 972  
[zac@polizei.berlin.de](mailto:zac@polizei.berlin.de)





## Polizei Berlin - Landeskriminalamt

ZAC – Zentrale Ansprechstelle Cybercrime  
für die Wirtschaft, Behörden und Verbände

Friesenstr. 16  
10965 Berlin

Tel.: 030 - 4664 / 972 972

E-Mail: [zac@polizei.berlin.de](mailto:zac@polizei.berlin.de)

[https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac\\_node.html](https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html)