



Giftige Geschäfte mit Babymilch

AGENDA S. 6 und 7, Kommentar S. 36

Zwanzig Seiten, die den ORF-General den Job kosteten

KOMMUNIKATION Seite 31

Franziska und das Extra-Chromosom

AGENDA Seite 12



SA./SO., 21./22. MÄRZ 2026

ÖSTERREICHS UNABHÄNGIGE TAGESZEITUNG — HERAUSGEGEBEN VON OSCAR BRONNER

€ 3,50 | Nr. 11.258

HEUTE

Isolierte Migrantinnen

In einigen Migrantenfamilien sperren Männer ihre Frauen regelrecht weg. Wie versucht wird, sie aus ihrem Gefängnis zu holen. Seite 9

Digitaler Missbrauch

Collien Fernandes erstattet Anzeige gegen ihren Ex-Mann: Christian Ulmen soll Deepfake-Pornos verbreitet haben. Seite 25, Kommentar Seite 36

Weiterreden in Salzburg

Markus Hinterhäusers Zukunft bei den Salzburger Festspielen ist weiter unklar, es soll noch ein Gespräch mit dem Intendanten geben. Seite 23

ZITAT DES TAGES

„Ich hatte mir das alles viel geschlossener vorgestellt. Das ist ja gar nicht so abgeschottet.“

Besucherin **Rosa Bachmann** bei einer Führung im österreichischen Parlament
AGENDA Seite 10

STANDARDS

Finanzen & Märkte	18, 19
Automobil	20, 21
Zeitgeschichte	22
Szenario, Kino	26, 27
Sport	28, 29
TV & Radio	32, 33
Rätsel, Sudoku	K 9
Wetter	26

Westen:	Süden:	Norden:	Osten:
1 bis 12°	0 bis 10°	3 bis 9°	4 bis 12°



Wie soll das enden?

Während der Krieg der USA und Israels gegen den Iran weitertobt, stehen die Golfstaaten vor den Scherben ihrer Diplomatie. Der Ausgang der Auseinandersetzung ist ungewiss, sicher ist nur: Kein Stein wird in der Golfregion auf dem anderen bleiben. Eine Analyse.

AGENDA Seiten 2, 3, 4 und 5

Ermittler decken riesiges Betrugsnetz im Darknet auf

Wiener Forscher halfen bei Sperrung von 373.000 Domains

München/Wien – Nach fünf Jahren intensiver Ermittlungen haben bayerische Strafverfolgungsbehörden eines der weltweit größten Betrugsnetzwerke im Darknet zerschlagen. Im Rahmen der internationalen „Operation Alice“ konnten rund 373.000 Domains mit kriminellen Inhalten identifiziert und abgeschaltet werden. Die Dimension ist enorm, wie Thomas Goger, Vizeleiter der Zentralstelle Cybercrime Bayern, im STANDARD-Gespräch erklärte: „Wir gehen davon aus, dass wir im Moment deutlich mehr als zwei Drittel aller Seiten im Tor-Netz kontrollieren.“ Das Netzwerk, in dem Darstellungen von Kindesmissbrauch angeboten wurden, diente vor allem dem Vorkassebetrug: Nutzer wurden mit illegalen Angeboten gelockt, erhielten nach der Bezahlung jedoch keine Gegenleistung.

Eine zentrale Rolle bei diesem Ermittlungserfolg spielten Forscherinnen und Forscher des Complexity Science Hub in Wien. Sie analysierten gemeinsam mit internationalen Partnern die Zahlungsströme im Netzwerk und konnten so Verbindungen zwischen tausenden Seiten sichtbar machen. Bezahlt wurde überwiegend mit Bitcoin – doch die vermeintliche Anonymität der Kryptowährung erwies sich als trügerisch. Entscheidend war, dass der Betreiber wiederholt identische Adressen nutzte. So konnten mehr als 440 Kunden identifiziert werden. Die Spur der Geldflüsse führte schließlich zu einem einzelnen Verdächtigen in China, nach dem nun gefahndet wird. (red) Seite 30

Tickets sichern poolbar.at

Poolbar

08.07.-16.08.2026 Feldkirch (AT)



Joss Stone



Babyshambles

11.07.	José González
24.07.	ClockClock
25.07.	Joss Stone
08.08.	HVOB
14.08.	Babyshambles
plus	viele mehr



Dialekt für Flüchtlinge

Kürzlich trat Integrationsministerin Claudia Bauer, vormals Plakolm, mit der Forderung auf, Flüchtlinge müssten künftig nicht nur besser Deutsch, sondern auch regionale Dialekte lernen.

Die Ministerin ist in Walding, im oberösterreichischen Mühlviertel, aufgewachsen. Eine Anfrage beim oberösterreichischen Literaturhaus, dem sogenannten Stifter-Haus, ob in der Mühlviertler Gemeinde Walding der typische regionale Mühlviertler Dialekt gesprochen wird, wird dort prompt und umfassend beantwortet: Das könne man – cum grano salis – mit Ja beantworten; wenn man allerdings ganz spezieller lokaler Dialekt gesprochen wird, lautet die Antwort: eher Nein.

Denn, so die Hüter des Erbes des Dichters Adalbert Stifter: „Ausgeprägte Dialekte sind im Alltag erst zu hören, wenn man über die Bundesstraße 127 in das obere Mühlviertel hinauffährt und man auf einer Seehöhe von 500 m den sog. ‚Saurüssel‘ überwunden hat.“ Es sei aber doch möglich, dass „in der Familie Plakolm noch ein spezifischer Mühlviertler Dialekt gesprochen wird“.

RAU

Flüchtlinge, die also im Mühlviertel den Deutschkurs unter besonderer Berücksichtigung des regionalen Dialekts absolviert haben, könnten sich dann etwa so äußern: „Yallah, habibi, dö Söcköbärn af d'Woad aui teibm!“

Also: „Los geht's, mein Freund, die Schafe (Söcköbärn=Sockenbären) auf die Weide treiben!“

jpi.at

IN ZEITEN WIE DIESEN IST VERTRAUEN DIE HALBE MIETE.

Gerade in unsicheren Zeiten sind JP-Immobilien eine gute Investition.

JP Wir haben was für Sie.

Auf über 373.000 Darknet-Seiten wird seit einigen Tagen dieses Banner angezeigt. Es handelt sich um rund zwei Drittel aller aktiven Seiten im Darknet.

Bisher größter Schlag gegen das Darknet

Auf hunderttausenden Domains wurden Darstellungen von Kindesmissbrauch angeboten. Das Wiener Complexity Science Hub half Behörden in Bayern, den Drahtzieher und über 400 Kunden zu identifizieren.

Reinhard Kleindl

Die bayerischen Strafverfolgungsbehörden deckten nach fünfjähriger Ermittlungsarbeit ein riesiges Betrugsnetzwerk im Darknet auf. Insgesamt über 373.000 Domains, ein großer Teil des aktiven Darknets, konnten im Rahmen der „Aktion Alice“ einer einzigen Quelle zugeordnet werden, wie die bayerischen Behörden am Freitag in einer Pressekonferenz in München bekanntgaben. Es ging dabei um Vorkassebetrug: Kundinnen und Kunden wurden zum Teil Missbrauchsdarstellungen von Kindern angeboten. Reale Missbrauchsbilder dienten als Köder, wer bezahlte, erhielt allerdings nie eine Gegenleistung. Die Domains hatten teils drastische Namen wie „Alice with Violence CP“ oder „Exclusive Baby Sluts CP“. Nicht alle der Seiten versprachen Missbrauchsdarstellungen, manche boten etwa Kreditkartennummern an. Die Server dafür wurden in Deutschland angemietet, zuletzt waren es 105 Stück. Das Netzwerk gab es seit 2019. Die internationale Koordination übernahm Europol.

Operation Alice

„Die weltweite ‚Operation Alice‘ ist ein neuer bedeutender Ermittlungserfolg bayerischer Strafverfolgungsbehörden“, freut sich Bayerns Justizminister Georg Eisenreich. „Sie sind dem Betreiber der Darknet-Plattformen mit innovativen Tools wie dem Dark Web Monitor, einer Suchmaschine für das Darknet, und dem Analyse-Tool Graphsense durch die Verfolgung von Zahlungsströmen auf die Schliche gekommen.“

Die Operation ist das Ergebnis von Ermittlungen, die sich über fünf Jahre erstreckten. „Was die schieren Zahlen angeht, handelt es sich mit den 373.000 übernommenen Darknet-Domains um die mit Abstand größte koordinierte Abschaltung krimineller Inhalte im Darknet weltweit. Wir gehen davon aus, dass wir im Moment deutlich mehr als zwei Drittel aller Seiten im Tor-Netz kontrollieren“, sagt Thomas Goger,

Oberstaatsanwalt der Generalstaatsanwaltschaft Bamberg und stellvertretender Leiter der Zentralstelle Cybercrime Bayern, gegenüber dem STANDARD. Mit dabei war auch das Complexity Science Hub (CSH) in Wien, das das Tool Graphsense beisteuerte.

Illusion von Anonymität

Bezahlt wurde in Bitcoin. Kryptowährungen sind bei kriminellen Geschäften beliebt, weil sie Anonymität versprechen. Doch diese Anonymität ist eine Illusion, wie der Komplexitätsforscher Bernhard Haslhofer vom CSH betont. Er kam vor einigen Jahren bei einem wissen-



Mit diesem Foto fahnden die Behörden nach dem Verdächtigen.
ZENTRALSTELLE CYBERCRIME BAYERN

schaftlichen Vortrag für Interpol mit der Zentralstelle Cybercrime Bayern in Kontakt und startete eine Kooperation, um gemeinsam illegale Plattformen im Darkweb und zugehörige Kryptowährungsströme besser zu verstehen. „Bereits relativ zu Beginn unserer Kollaboration haben wir eine auffällige Plattform entdeckt“, berichtet Haslhofer.

Es handelte sich um die Domain „Alice with Violence CP“. „Wir konnten zugehörige Kryptowährungsadressen extrahieren und die ein- und ausgehenden Zahlungsströme analysieren. Wir haben relativ

schnell erkannt, dass es sich nicht um eine einzige Plattform handelt, sondern um ein Netzwerk zusammenhängender Plattformen.“

Die Forschenden gingen den Zahlungsströmen nach, die jenen bei normalen Verkäufen im Netz ähneln. „Wenn man im normalen Internet etwas zum Verkauf anbietet, dann könnte man im Prinzip auch eine Kontonummer anzeigen, auf die Kunden einzahlen sollen“, erklärt Haslhofer. Das sei heute zwar in der Praxis nicht mehr üblich, funktioniere im Darknet aber nach wie vor so – allerdings mit Kryptowährungsadressen statt Kontonummern.

„Wenn zwei Plattformen im Darkweb dieselbe Bitcoin-Adresse verwenden, dann muss es im Regelfall einen Zusammenhang geben“, erklärt Haslhofer. Einfach sei das Auffinden dieser Zusammenhänge dabei nicht: „Die Betreiber der Darkweb-Seiten generieren ständig neue Adressen, vermutlich, um die Geldflüsse weniger einfach nachvollziehbar zu machen.“

Doch wer eine Seite über einen längeren Zeitraum beobachte, könne diese Adressen sammeln und die Zusammenhänge sehen. „Dieses Beobachten hat eine niederländische Firma durchgeführt, die so etwas wie eine Google-Suche für das Darkweb entwickelt hat. Die Firma indiziert die Darkweb-Webseiten, so wie Google das Web indiziert“, sagt Haslhofer. Das ist außergewöhnlich, denn eigentlich sind Darknet-Seiten durch ein Netzwerk namens Tor geschützt, das Informationen über unzählige Domains umleitet, um so die eigentliche Domain des Nutzers hinter zahlreichen digitalen „Zwiebelschalen“ zu verbergen.

440 Kunden

Diese „Google-Suche“ für das Darkweb öffnete gewissermaßen die Tür für die Forschenden des CSH. „Der Täter hat Kryptowährungsadressen in mehreren Plattformen wiederverwendet. Und das war ein Fehler, weil dadurch die Zusammenhänge zwischen den Plattformen sichtbar wurden“, so Haslhofer.

Den Forschenden um Haslhofer half dabei, dass bei Bitcoin-Zahlungen jede Transaktion transparent dokumentiert ist. Zur Erinnerung: Transaktionen werden in einer sogenannten Blockchain gespeichert, die dezentral verwaltet wird. Zwar sind die Personen hinter den Transaktionen dort nicht unmittelbar erkennbar, aber viel Schutz bietet das nicht, wie die aktuelle Ermittlung zeigt. „Dass Kryptowährungen anonym sind, ist ein hartnäckiger Irrtum“, sagt Haslhofer. Die Bitcoins werden letztlich auf Kryptowährungsbörsen in Euro oder US-Dollar umgewandelt. „Dort kann eine Strafverfolgung ansetzen und einen Personenbezug ausheben“, im Rahmen der geltenden Gesetze mittels Gerichtsbeschluss, wie Haslhofer betont. Auf diese Weise gelang es auch, über 440 Kunden namentlich zu identifizieren, die Geld an die Adressen überwiesen.

Ein einziger Täter

Die Täter-Adressen führten überraschenderweise zu einer einzigen Person in China, nach der nun gefahndet wird. „Ich persönlich bin schon sehr überrascht, dass es wirk-

lich nur eine Person ist. Ich hätte mir gedacht, dass zumindest eine Tätergruppe dahintersteht. Der Verdächtige hat offensichtlich hochautomatisiert gearbeitet“, sagt Haslhofer, der ihn trotzdem für nicht sehr versiert hält. Generell sehe man einen Trend zur Automatisierung in der Cyberkriminalität. Doch auch die Strafverfolgung bediene sich zunehmend automatisierter Methoden. „In diese Richtung muss es wahrscheinlich auch in Zukunft gehen, um da noch mithalten zu können“, sagt Haslhofer. Es zeige jedenfalls, dass Behörden nicht komplett ohnmächtig sind, was Cybercrime betrifft.

Die Arbeit, die für Haslhofer ein Nebenprojekt darstellte, war für diese Ermittlung jedenfalls essenziell. „Unsere Entwicklungspartnerschaften mit TNO und CFLW in den Niederlanden und mit dem Complexity Science Hub und Iknai in Wien haben für diesen Ermittlungserfolg eine zentrale Rolle gespielt“, sagt Thomas Goger. „Nur mit Darkweb Monitor und Graphsense war es uns möglich, überhaupt den Einstieg zu finden und die Zusammenhänge in diesem riesigen Netz zu erkennen.“

WISSEN

Bitcoin und Tor

Hinter Kryptowährungen wie Bitcoin steht die Idee eines Zahlungsmittels, das nicht von Zentralbanken verwaltet wird, sondern bei dem Transaktionen von dezentralen Stellen überwacht werden. Sie werden einer sogenannten Blockchain angefügt, die gewissermaßen ein Protokoll aller bisherigen Transaktionen darstellt und mittels kryptographischer Verfahren gegen nachträgliche Änderung geschützt ist. Nutzerinnen und Nutzer sind dabei zwar anonym, können aber bei der Umwandlung der Kryptowährungen in reales Geld aus-

geforscht werden. Durch das Tor-Netzwerk, das ein Anonymisierungsdienst ist, werden Verbindungsdaten verschleiert. Grob gesprochen wird dabei der Datenverkehr über mehrere eigens dafür bereitgestellte Server umgeleitet, die wie Zwiebschalen die eigentliche Adresse verdecken, um eine Nachverfolgung zu erschweren. Für mehr Sicherheit werden diese Server immer wieder gewechselt. Tor ist die entscheidende Technologie hinter dem Darknet: Es besteht aus Webseiten, die nur über Tor erreichbar sind. (rkl)