Reden in der Eden

„Die unsichere Welt. Unsere Gesellschaft im Spannungsfeld zwischen Desinformation und Computerkriminalität.“

Dr. Cornelius Granig, Unternehmensberater und Sicherheitsexperte

Die unsichere Welt

Unsere Gesellschaft im Spannungsfeld zwischen Desinformation und Cybercrime

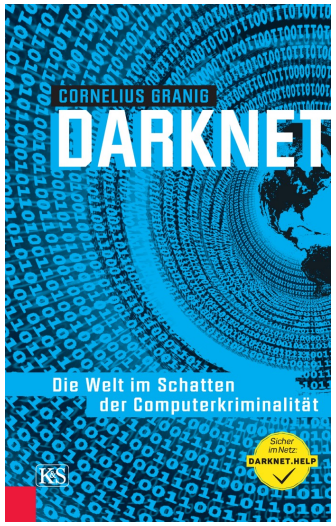
Dr. Cornelius Granig

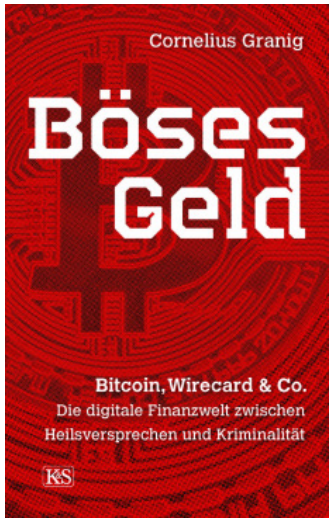
5. September 2024

Cornelius Granig ist ein österreichischer Unternehmensberater und und Buchautor. Er leitet die Taskforce „Journalismus und Medien“ bei **Transparency International** und arbeitet als Aufsichtsrat und Beirat in zahlreichen nationalen und internationalen Organisationen.

Dr. Granig war über ein Jahrzehnt beim Technologiekonzern **IBM** tätig und arbeitete danach als Vorstand von Banken und Versicherungen und als Generaldirektor einer Landesgesellschaft von **Siemens**.

In seinen Büchern befasst er sich mit den Licht- und Schattenseiten der Informationsgesellschaft und der Digitalisierung der Kriminalität, die Justiz- und Polizeibehörden national und international zu schaffen macht.





Fakenews
Rumänien 1963

Der oberste Fakenews-Verbreiter in den 1960ern

General Aleksandr Sakharovsky
Leiter der Auslandsspionage im KGB

Operation „Dragon“

Vier Tage nach dem Attentat auf John F. Kennedy, am 26. November 1963, besuchte der Leiter der KGB Auslandsspionage unangekündigt den rumänischen Schwesterdienst DIE in der rumänischen Hauptstadt Bukarest.

Sein Auftrag von Nikita Chruschtschow lautete, im Rahmen der großen Desinformations-Operation „Dragon“ **den Amerikanern die Schuld am Mord Kennedys zuzuschieben**. Nach der Version der Russen hätte der „eifersüchtige“ amerikanische Präsident Lyndon B. Johnson die Ermordung selbst beim CIA angeordnet.

Diese Darstellung wurde über die Partnerdienste des KGB in Umlauf gebracht, bevor die USA ihre eigene Version der Geschichte hatten, damit die Falschinformationen der Russen schon vorher bekanntund verbreitet waren.

Fakenews
Rumänien 2009

Der israelische Politikberater **Tal Silberstein**, der davor für Adrian Nastase (Sozialisten) und Calin Popescu Tariceanu (Liberale) gearbeitet hatte, unterstützte er Traian Băsescu (Konservative) im rumänischen Wahlkampf.

Erinnerlich blieb nur mehr ein **großes Chaos** über die Vorgänge - und ein bitterer Nachgeschmack.

Unclear contender for face-off with Basescu

With the first round of Presidential elections set for 22 November, the battle has begun over which candidate is likely to face-off against the incumbent Traian Basescu in the second round of voting.

October 2009 - From the Print Edition

As we went to press, Basescu had not yet announced his candidacy, but was widely expected to participate. Backed by the Democratic Liberal Party (PD-L), he has the highest chances of winning.
Basescu attracts about 30 per cent of the vote, against 20 per cent for Mircea Geoana, president of the Social Democrats (PSD) and the same for Crin Antonescu, leader of the National Liberal Party (PNL), according to a poll average. About ten per cent of voters would pick Sorin Oprescu, the mayor of Bucharest.

Fake News
Österreich 2017

Desinformation im Wahlkampf

Desinformation im Wahlkampf

Verhaftung von Beny Steinmetz und Tal Silberstein, 14. August 2017

Wie entstehen Fake News?

Was sind Fake News

„Fake News“ sind falsche Nachrichten, die bewusst geschaffen werden, um Menschen zu manipulieren.

Das können Übertreibungen, Vereinfachungen oder ganz und gar erfundene Berichte sein.

Die Hauptmotivation zur Verbreitung von Fake News ist,

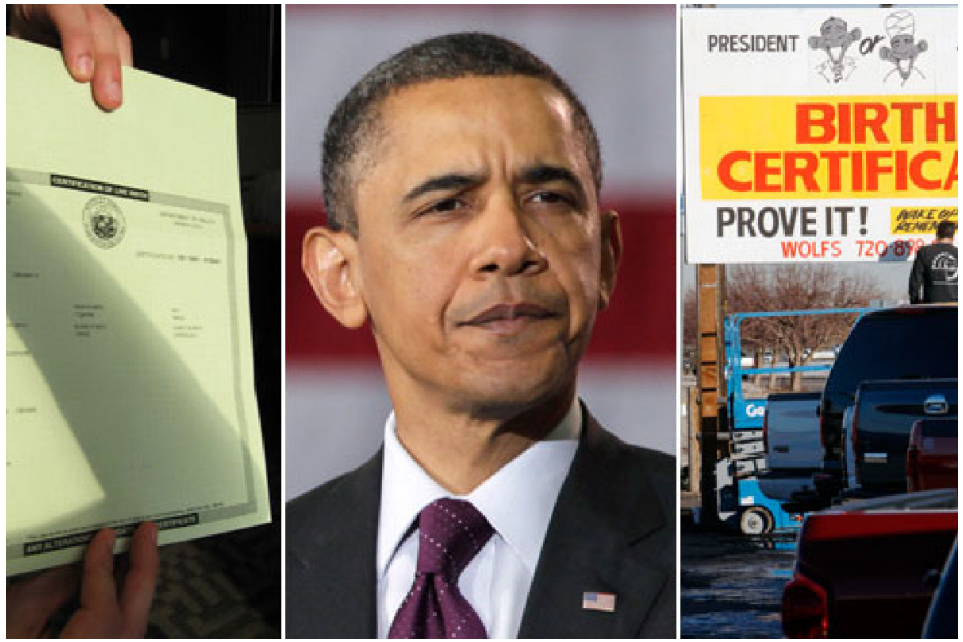
- dass man die Bekanntheit eigener Inhalte erhöht,
- dass man eine wirtschaftliche, soziale oder politische Agenda mit deren Verbreitung verfolgt

Im digitalen Zeitalter ist es **viel einfacher**, Fake News mit großer Reichweite in Umlauf zu bringen, und die **Urheberschaft zu verbergen**.

Zukauf von Fake News im Darknet

Das Schreiben von „Fake News“ kann **ausgelagert** werden – wie beispielsweise in der Operation „Veles“ durch Trump-Unterstützer im Jahr 2016.

140 pro-Trump Webseiten wurden für den US-Wahlkampf aus der nordmazedonischen Stadt Veles heraus betrieben.



Verbreitungsweg - Microtargeting

„Fake News“ nützen häufig Algorithmen für die zielgerichtete Verbreitung.

Diese Vorgehensweise wird „**Microtargeting**“ genannt. Dabei wird versucht, die Inhalte zielgruppengerecht zu variieren.

Der bisher berühmteste Fall ist die Londoner Politikberatungs-Boutique **Cambridge Analytica,** die persönliche Angaben von über 50 Millionen Facebook-Benutzern für die Beeinflussung des US-Wahlkampfes im Jahr 2016 nutzte.

Seither ist die Gewinnung von Daten aus Facebook-Quizspielen nicht mehr erlaubt.

„Fake News“ können von „**Social Bots**“ unterstützt werden. Das sind Algorithmen und keine echten Computerbenutzer, die beispielsweise Nachrichten auf X posten.

Damit solche **digitalen Scheinidentitäten** nach außen hin plausibel auftreten können, benötigen sie Follower und Likes, die über das Darknet für die verschiedenen Social Media Kanäle zugekauft werden können.

Experten vermuten, dass bis zu **25% der X-Nutzer** Bots sind – was der neue Eigentümer Elon Musk massiv bestreitet.

„Spendierte Freunde“ in Österreich, 2011

„Neu ist für uns das Phänomen "spendierte Freunde". Unbekannte Dritte kaufen offenbar "Fake-Fans" in Tausender-Einheiten und widmen sie einer Seite, die ihnen nicht gehört.

Zumindest gemäß unserer bisherigen Recherchen, hat es so etwas bislang auch international noch nicht gegeben.

Auch Facebook war mit so etwas noch nicht konfrontiert.

Es gibt daher auch noch keinerlei Filter, um das zu vermeiden.“
(Team Bundeskanzler, Nov. 2011)

INLAND

Faymanns falsche Fans kommen aus SP-Zentrale

Werner Faymann ließ sich im Internet offenbar von seinen eigenen Leuten bejubeln: Die gefälschten Profile, die auf Facebook den Kanzler unterstützen, sollen in der SPÖ-Zentrale erstellt worden sein - Laura Rudas dementiert das

20. November 2011, 17:32

Die Rolle der Suchmaschinen

Über die vorhin beschriebenen Mechanismen erfahren Fake News im Internet große Verbreitung und werden daher in Suchmaschinen weit oben in den Ergebnislisten angeführt.

Das gilt nicht nur für weit hergeholte Verschwörungs-theorien sondern wird auch für die personenbezogene „digitale Verleumdung“ genutzt.

Der Fall **„Thomas Szekeres“** illustriert, wie schwierig es ist, aus der Maschinerie der Suchmaschinen wieder herauszukommen.

Bedrohung und Fakenews rund um den Ärztekammerpräsidenten

Mangel an Cardion in österreichischen Apotheken!

Soweit wir wissen, ist es äußerst schwierig, Cardion in Apotheken zu kaufen. Dieses Medikament ist selten verfügbar. Ist es so? Und was können Sie österreichischen Bürgern empfehlen?

– Ja, das ist in der Tat so. Cardion wird in begrenzten Mengen produziert und gelang somit einfach nicht in die Apotheken. Der Großteil wird leider ins Ausland verkauft und ein Teil wird von privaten Kliniken aufgekauft.

Daher fällt es gewöhnlichen Menschen wirklich schwer Cardion zu erwerben. DERZEIT KANN DIESES MEDIKAMENT IN UNSERER KLINIK GEKAUFT WERDEN. Zu diesem Zweck können Sie auf unserer Webseite eine Anfrage hinterlassen. Wir haben beschlossen eine kleine Menge dieses Medikaments

RUFMORD-KAMPAGNE

Corona-Leugner bedrohen Ärztekammer-Chef Szekeres

Österreich | 01.09.2020 06:00

Ärztekammerpräsident Thomas Szekeres (Bild: APA/Herbert Neubauer)

Üblen Verleumdungen und beängstigenden Drohungen durch Corona-Leugner ist Ärztekammer-Chef Thomas Szekeres ausgesetzt. Der in der Covid-19-Krise so besonnene Mediziner hat wegen der massiven Rufmord-Kampagne eine Anzeige bei der Staatsanwaltschaft Wien erstattet. Polizeischutz steht im Raum.

Artikel anhören | Teilen

„Über mich ergießt sich eine Flut an Beleidigungen. Ich werden unter anderem als ‚roter Masken-Fetischist' beschimpft", so Szekeres, der wegen seiner mutigen Verteidigung der Pandemie-Maßnahmen ins Visier geraten ist. Anfangs ignorierte der Ärztekammer-Chef die Angriffe. Doch als auf der Leugner-Homepage von einer „Hinrichtungsliste" die Rede war, erstattete der angesehene Mediziner auf dringendes Anraten des Wiener Cyber-Security-Experten Cornelius Granig Anzeige.

Fake News
&
Cybercrime

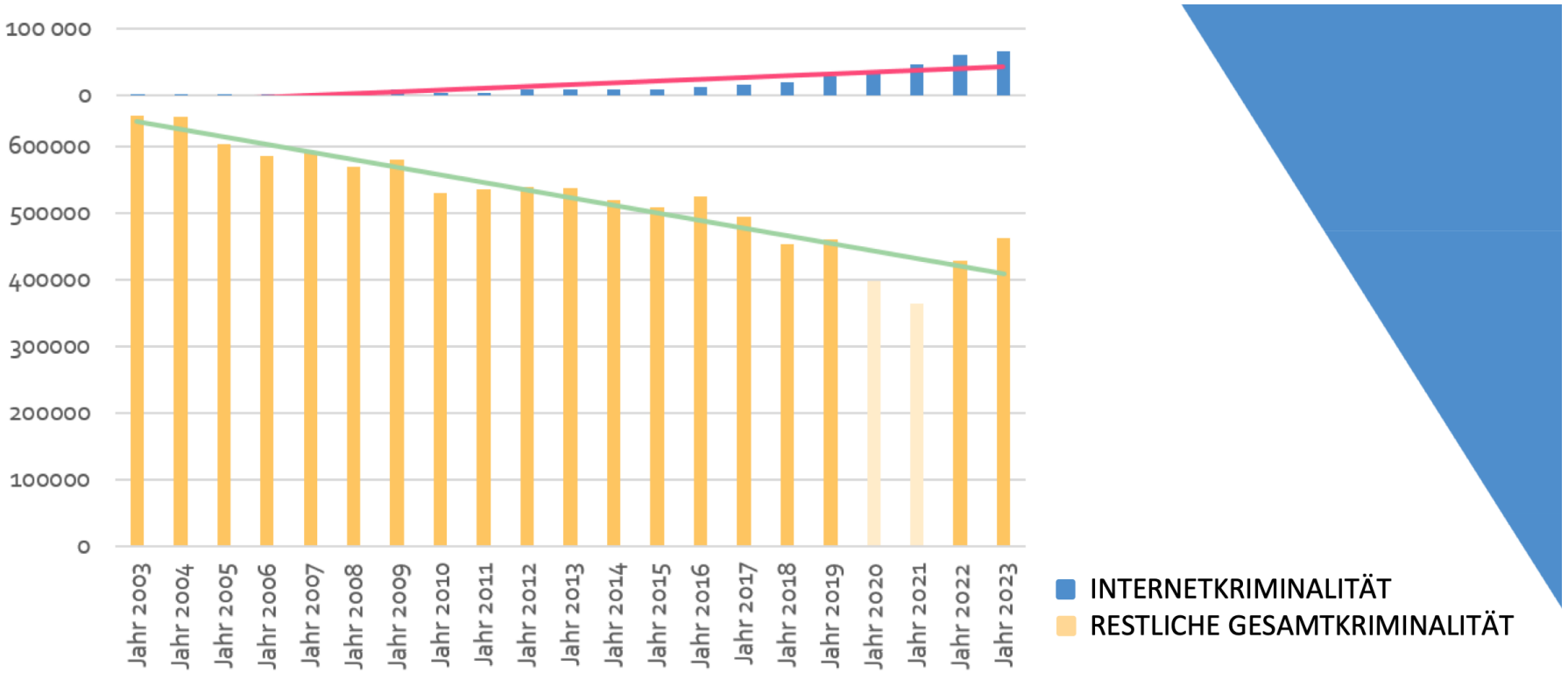
Definition von „Cybercrime“

Als Cybercrime **im engeren Sinne** werden alle Straftaten bezeichnet, bei denen es sich um direkte Angriffe auf Daten oder Computersysteme handelt. Darunter fallen beispielsweise Datenbeschädigung, Hacking oder Denial-of-Service- Attacken.

Cybercrime im **weiteren Sinne** erfasst jene Delikte, bei denen die Informations- und Kommunikationstechnik in der Planungsphase, Vorbereitung und zur Ausführung herkömmlicher Straftaten eingesetzt wird - wie etwa Betrugsdelikte, Kindesmissbrauchsmaterial, Cyber-Mobbing oder Cyber-Bullying. Dabei kann es sich um jede Form von Kriminalität handeln.

Definition: Bundesministerium für Inneres, Deutschland

Kriminalität in Österreich (Anzeigen 2003-2023)



Quelle: Bundesministerium für Inneres, Österreich

Internetkriminalität Österreich (2014-2023)

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2014	8 966	3 660	40,8 %
Jahr 2015	10 010	4 157	41,5 %
Jahr 2016	13 103	5 072	38,7 %
Jahr 2017	16 804	6 470	38,5 %
Jahr 2018	19 627	7 332	37,4 %
Jahr 2019	28 434	10 187	35,8 %
Jahr 2020	35 915	12 012	33,4 %
Jahr 2021	46 179	17 020	36,9 %
Jahr 2022	60 195	20 378	33,9 %
Jahr 2023	65 864	20 818	31,6 %

Quelle: Bundesministerium für Inneres, Österreich

Entwicklung der Computerkriminalität in Österreich

Jährliche **Steigerungsraten im zweistelligen Bereich** bei insgesamt abnehmender Gesamtkriminalität.

66.000 angezeigte Straftaten 2023 in Österreich – innerhalb der letzten 10 Jahre **Zunahme um über 600%.**

Die Gründe dafür liegen häufig in **mangelnder Vorsicht** der Opfer, und Unkenntnis über die Tatbegehungsmöglichkeiten.

Überdies existieren relativ **geringe** Strafdrohungen gepaart mit einer **geringen Aufklärungsquote** (31,6% vs. 52,3% in der Gesamtkriminalität), da die Täter sich erfolgreich im Darknet verstecken und eine internationale Verfolgung schwierig ist.

Die Strafverfolgungsbehörden verfügen über zu **wenige Experten**.

Die größten Bedrohungen

Datendiebstahl durch Innen- oder Außentäter

Ransomware durch der organisierte Cyberkriminelle

Überlastungsangriffe durch Aktivisten

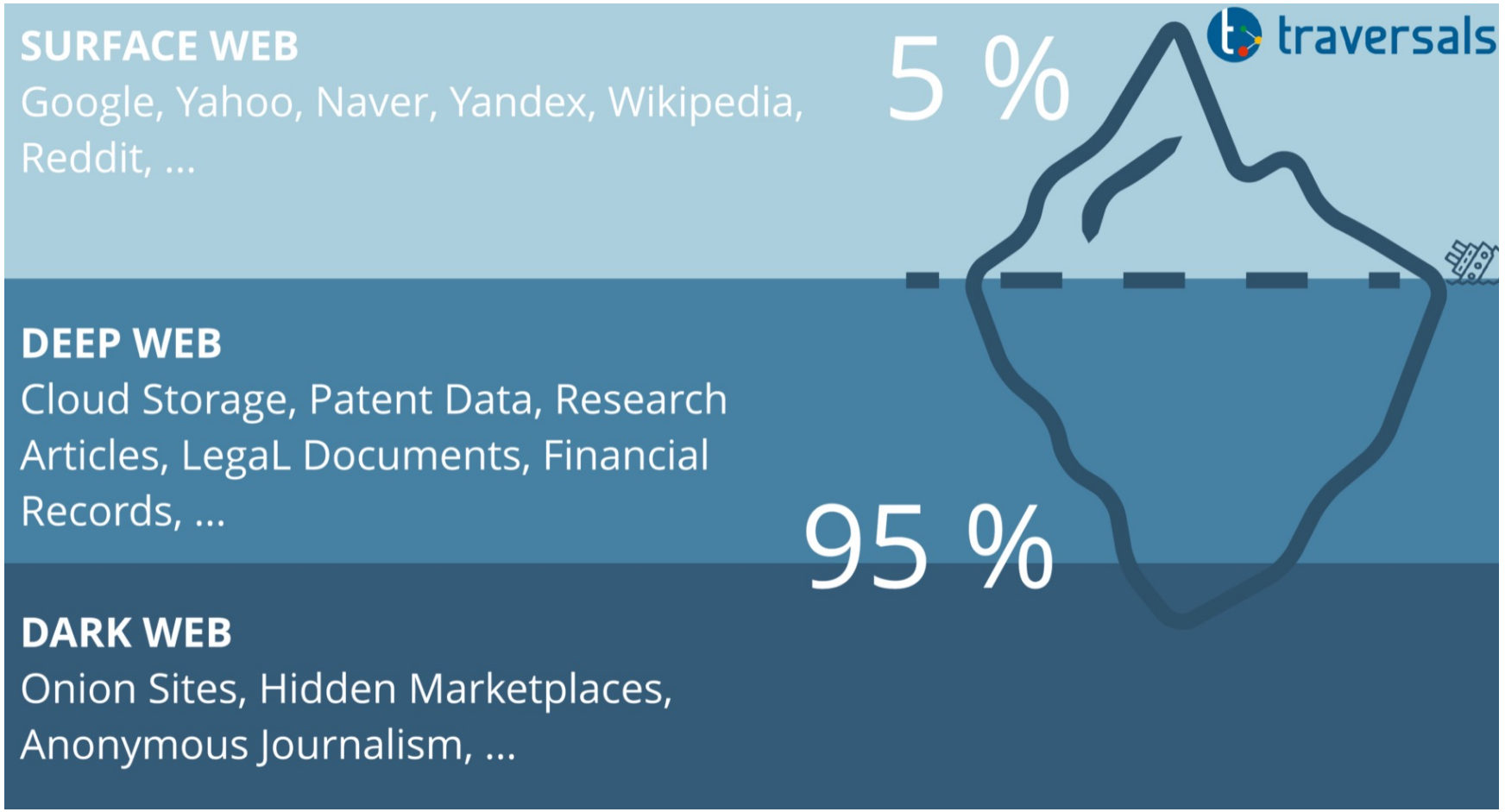
Spionage durch **staatliche Akteure**

Vielfältige **Betrugsmaschen** mit sozialen Tricks

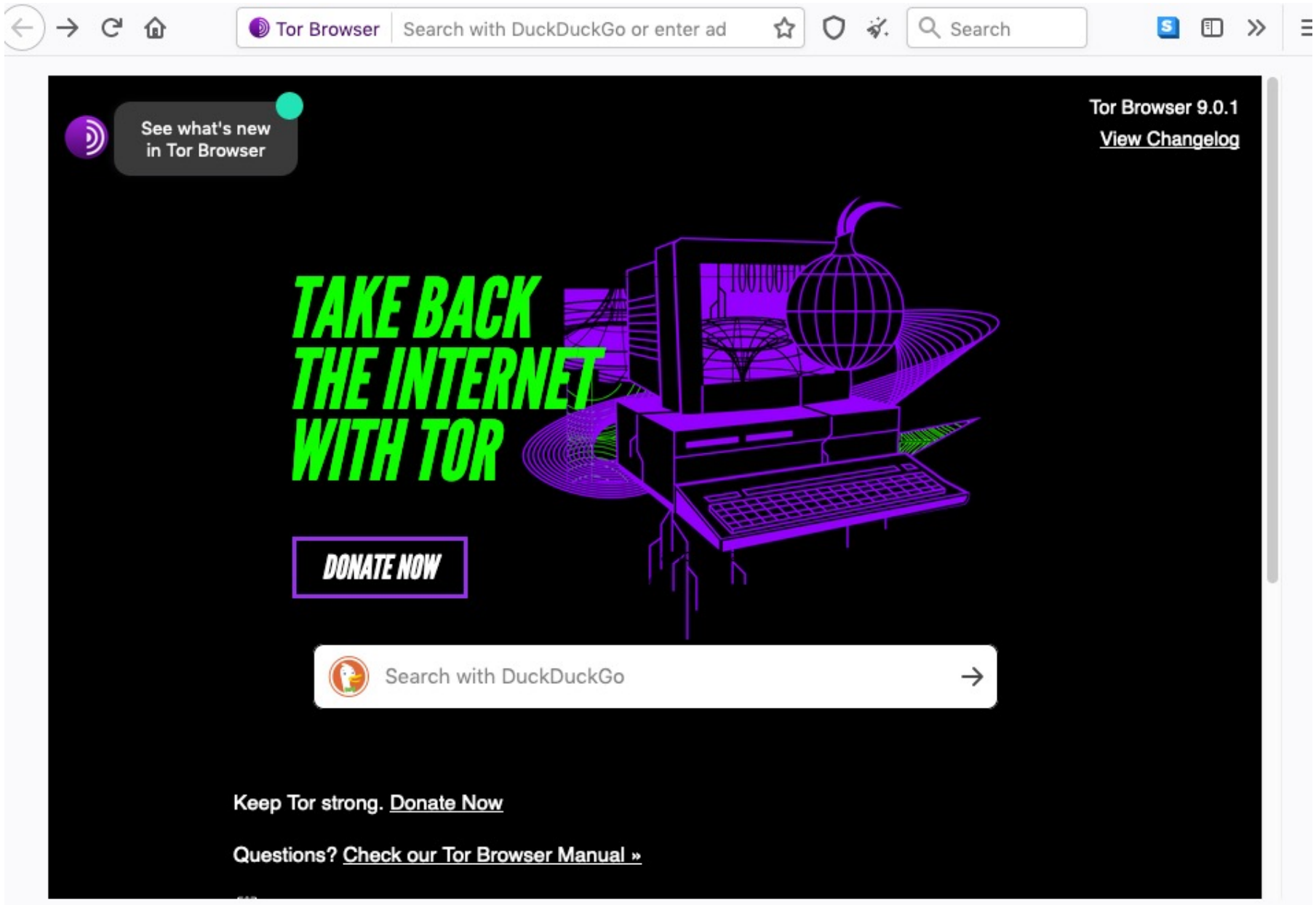
Angriffe über **verbundene Dienstleister und Partner**

Die Rolle des Darknets

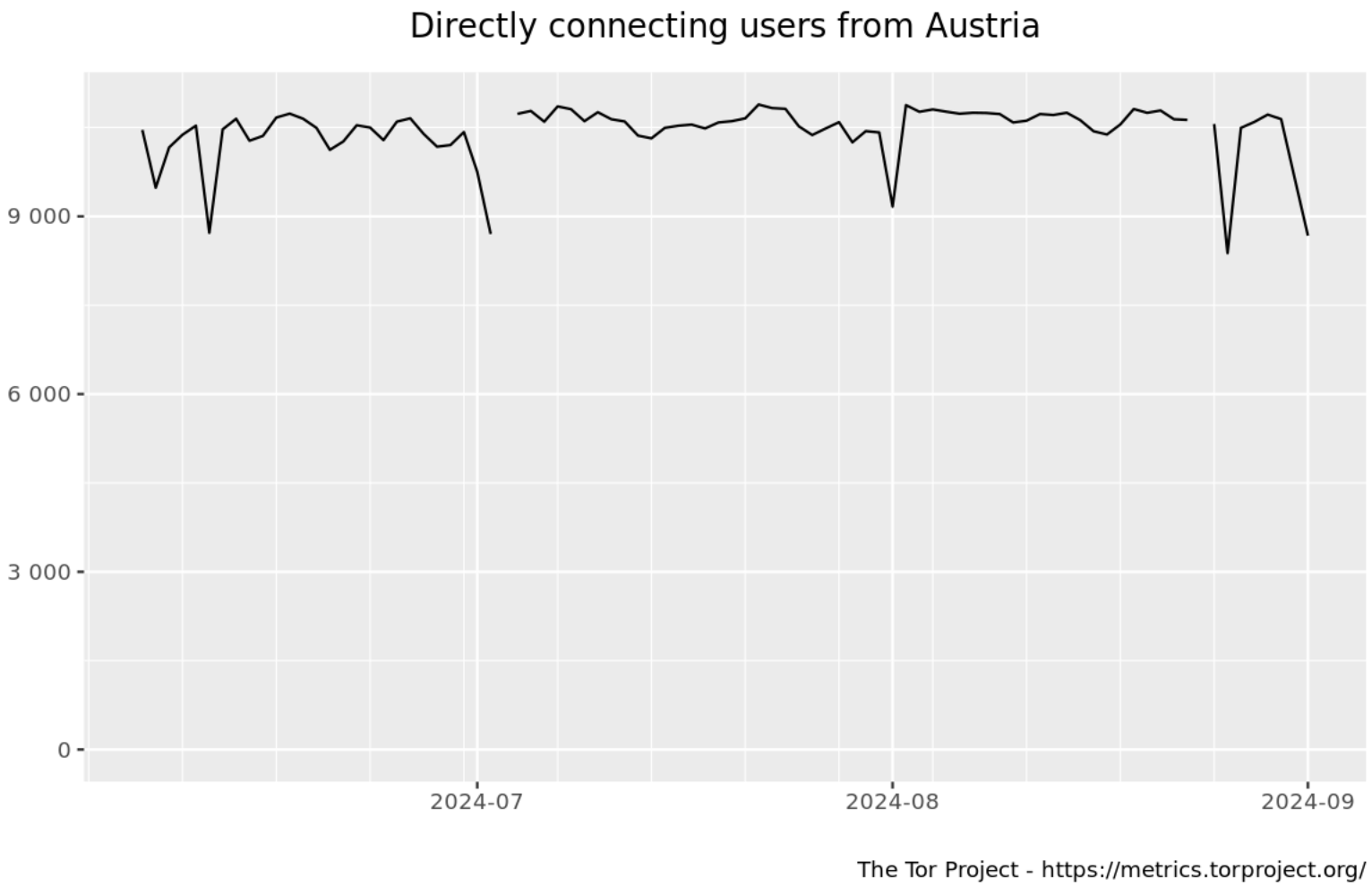
Teile des Internets



Der TOR-Browser

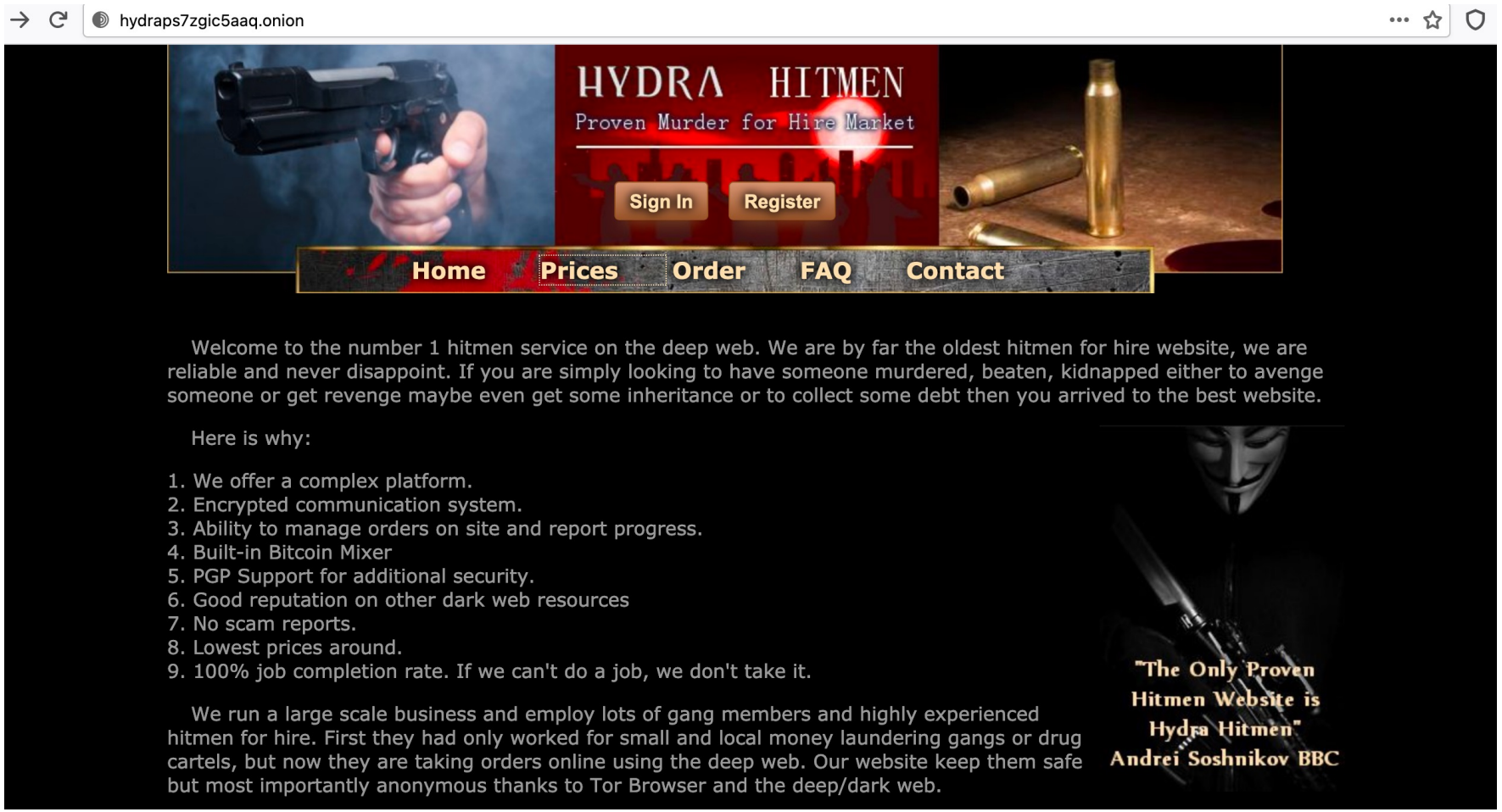


TOR-Benutzer Österreich



„Crime as a Service“ – Zukauf von Kriminalität

Hydra Hitmen – Auftragsmorde, Anschläge



Hydra –Drogenhandel

HYDRA Россия

Поиск... | Москва | 0 BTC | police2021

КАТЕГОРИИ все | Магазины | Товары | Записки | Форум | Обмен | 1 BTC = 46 591 USD / 3 465 352 RUB

› КАТЕГОРИИ

Экстази

Поиск...

Москва

Район/метро...

Цена: От... – До...

Кол-во: г

От... – До...

Тип клада:

- Магнит
- Тайник
- Земляной прикоп
- Снежный прикоп

- Любой

Сортировка: **Рейтинг** | Цена

MDMA (*ecstasy) 260mg (Rolls-Royce|Сердца|Фигуры|Chupa Chups|Пики|Машины)

PokemonGo

Волшебное ассорти на любой вкус! Почувствуй любовь со всем миром! ПРОХОДИТ АКЦИЯ!!

Москва

от **999 руб / 1шт** ★★★★★

Еще экстази от этого магазина:

ОПТ | MDMA (*ecstasy) 260...

от **29 000 руб / 83шт**

Экстази (фиолетовые Maybach) - %СКИДКИ!%

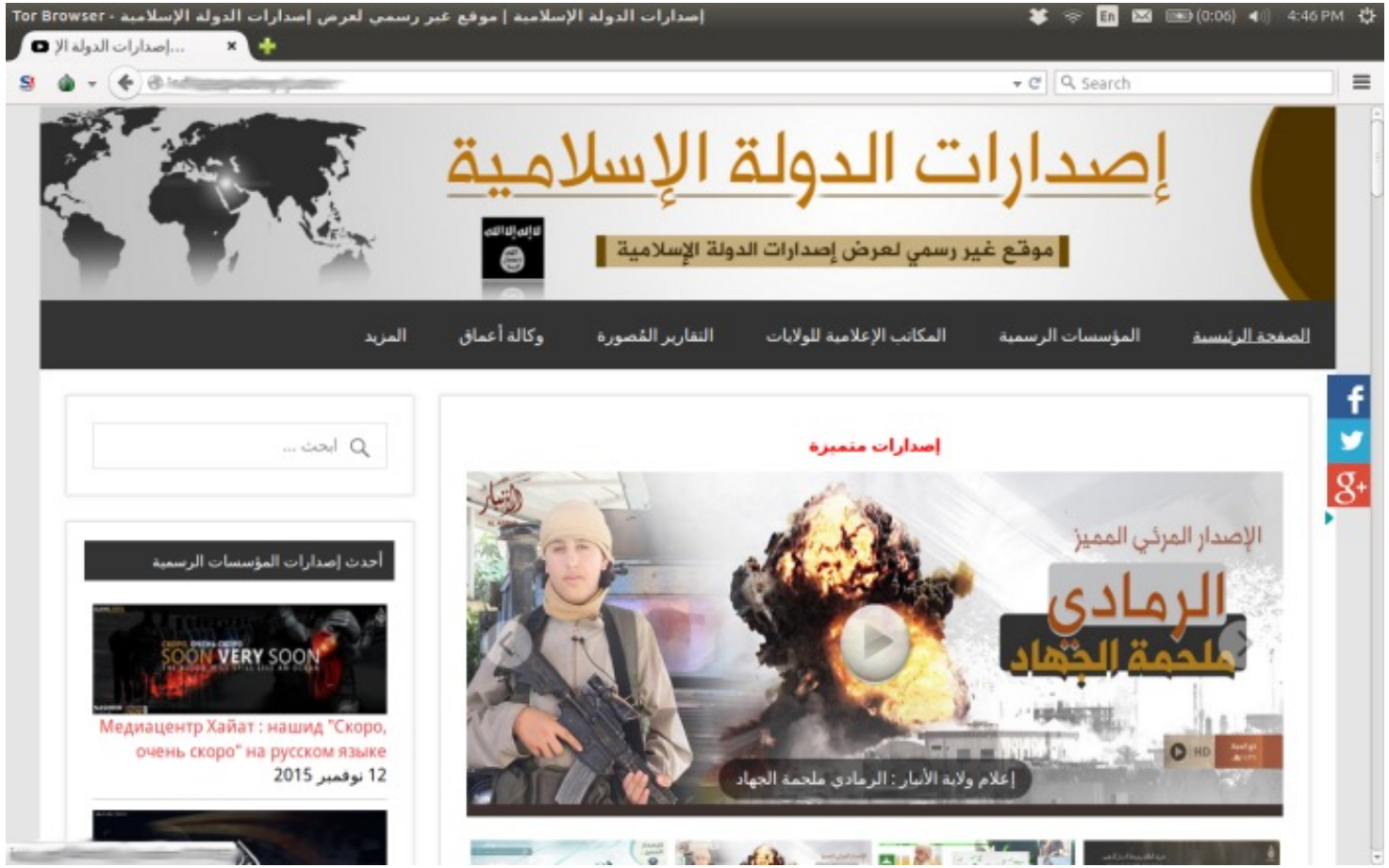
Stuffman

Твоя подруга запомнит эту ночь навсегда! (240mg MDMA)

Москва

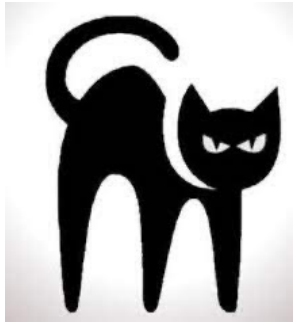
от **9 990 руб / 30шт** ★★★★★

Terrororganisationen erstellen Propagandaseiten und stellen sie auf Darknet-Server, wo sie von allen Beteiligten sicher aufgerufen werden können.



Die Zahl der Angebote im Bereich der Kinderpornographie hat dramatisch zugenommen.

Es ist ein Skandal, der nicht nur Österreichs Kulturlandschaft erschüttert – sogar die amerikanische Oscar-Academy musste sich aktuell damit befassen. Wie am Freitag bekannt wurde, wird sich der Wiener Schauspieler Florian Teichtmeister (43) im Februar vor Gericht wegen mutmaßlicher Beschaffung und des Besitzes kinderpornografischen Materials verantworten. Er zeigt sich geständig, im Zeitraum von Februar 2008 bis August 2021 aus dem Darknet 58.000 derartige Mediendateien heruntergeladen zu haben, die Behörden stellten 22 Datenträger sicher.

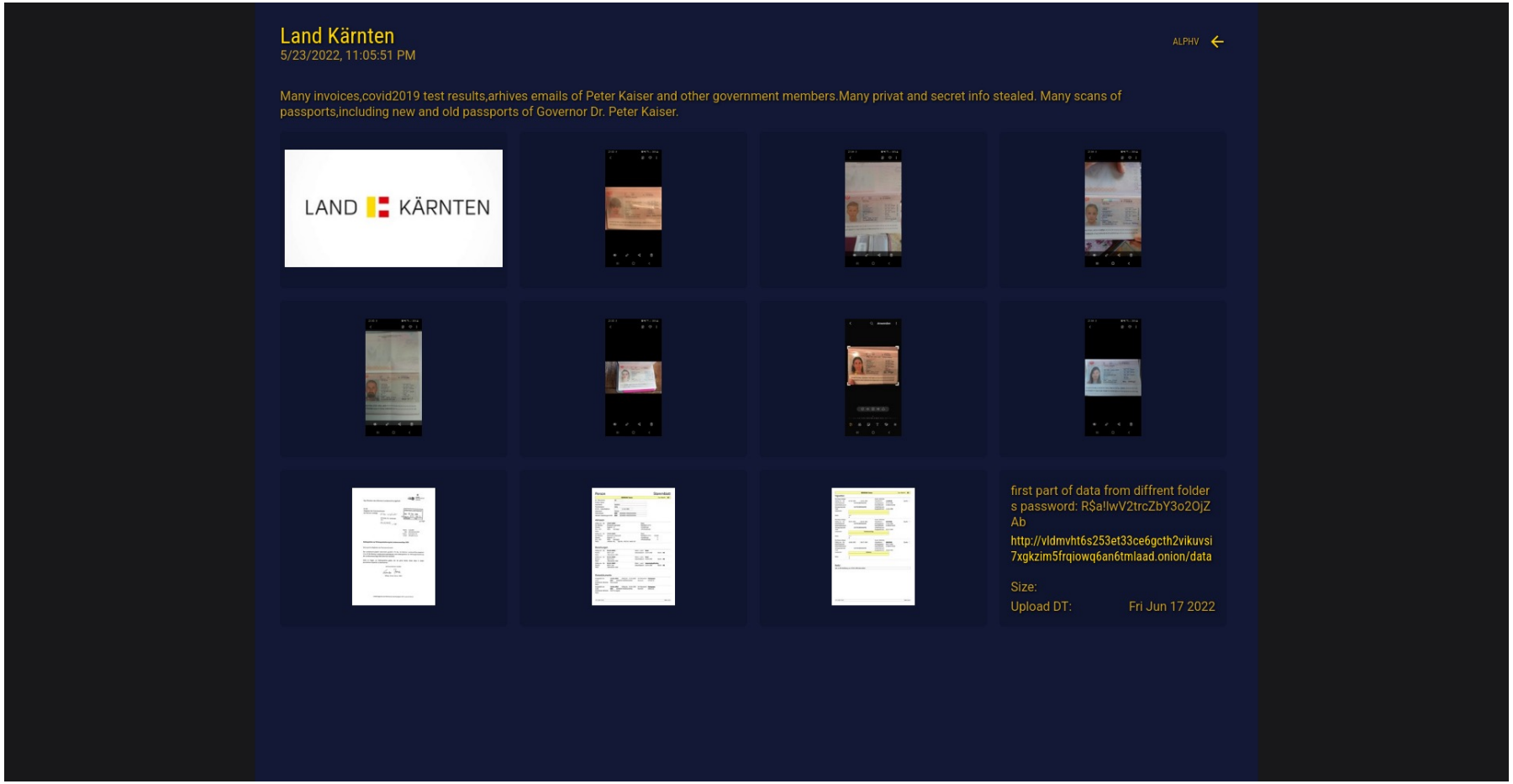


Beinharte Erpressung durch organisierte Cyberkriminalität

Blackcat/ALPHV gelang über ein Phishing-Mail in das Netzwerk der Kärntner Landesregierung:

- Einen Monat lang wurden **Daten kopiert**
- Anschließende **Verschlüsselung** der Systeme
- Nach Zahlungsverweigerung **Datenveröffentlichung**
- Nach weiterer Zahlungsverweigerung **DDOS-Angriffe**
- Daten als Basis für die Verbreitung von **Fakenews**

Blackcat – Angriff auf das Bundesland Kärnten



Suche nach den Tätern

Systeme von Blackcat wurden vom FBI in Zusammenarbeit mit anderen Polizeibehörden übernommen / stillgelegt.

Die Angreifer sind weiterhin unbekannt – für Hinweise, die zu deren Ergreifung führen, ist eine **Belohnung von 10 Millionen Dollar** ausgelobt.

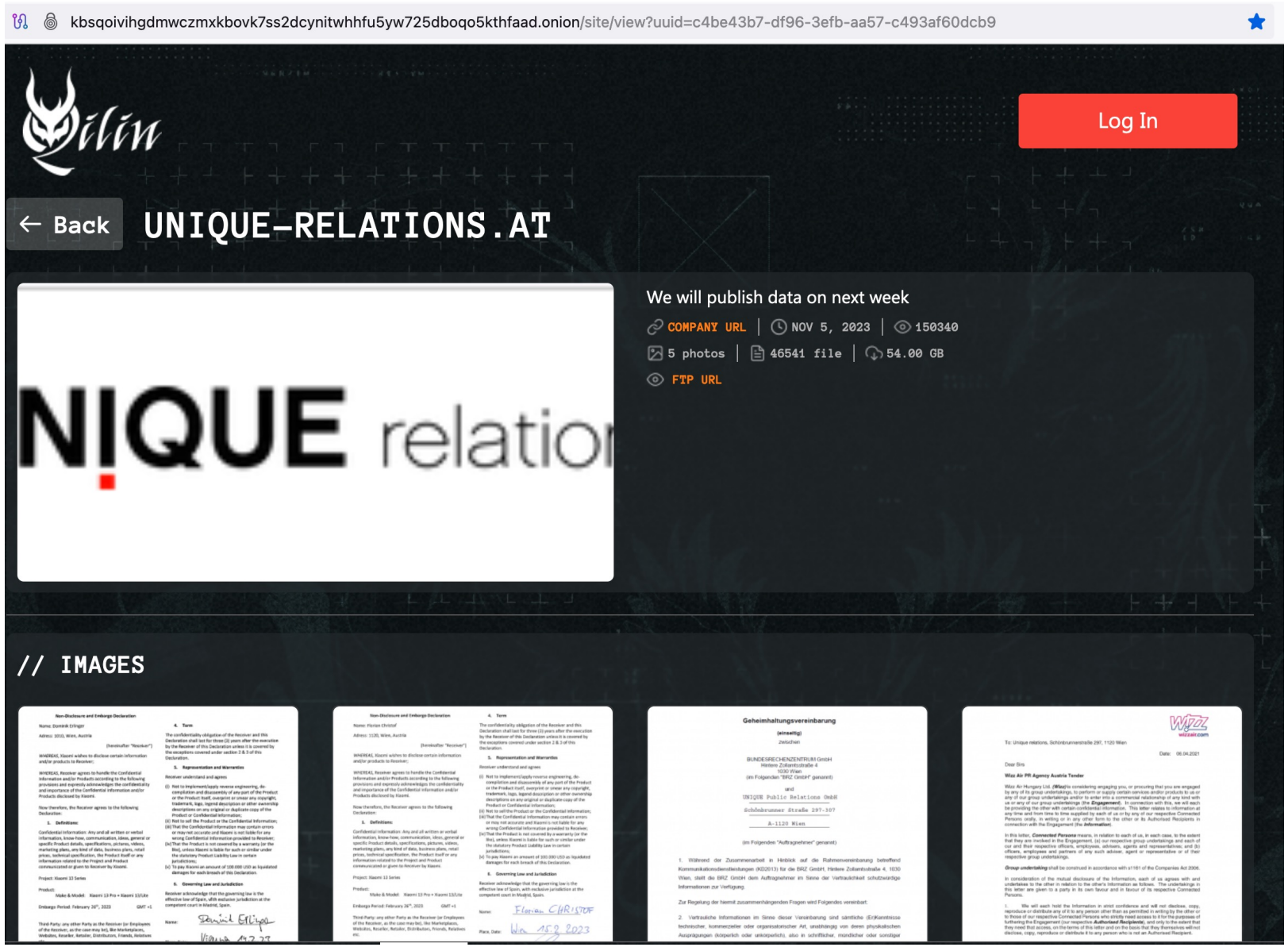
REWARD FOR INFORMATION: ALPHV/BLACKCAT RANSOMWARE AS A SERVICE – REWARDS OF UP TO $15 MILLION

REWARD OF UP TO $15 MILLION

NAME: ALPHV/Blackcat Ransomware as a Service (RaaS)
NATIONALITY: Various (Unknown)
CITIZENSHIP: Various (Unknown)

The U.S. Department of State is offering a **reward of up to $10,000,000** for information leading to the identification or location of any individual(s) who hold a key leadership position in the Transnational Organized Crime group behind the ALPHV/Blackcat ransomware variant. In addition, a **reward offer of up to $5,000,000** is offered for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in ALPHV/Blackcat ransomware activities.

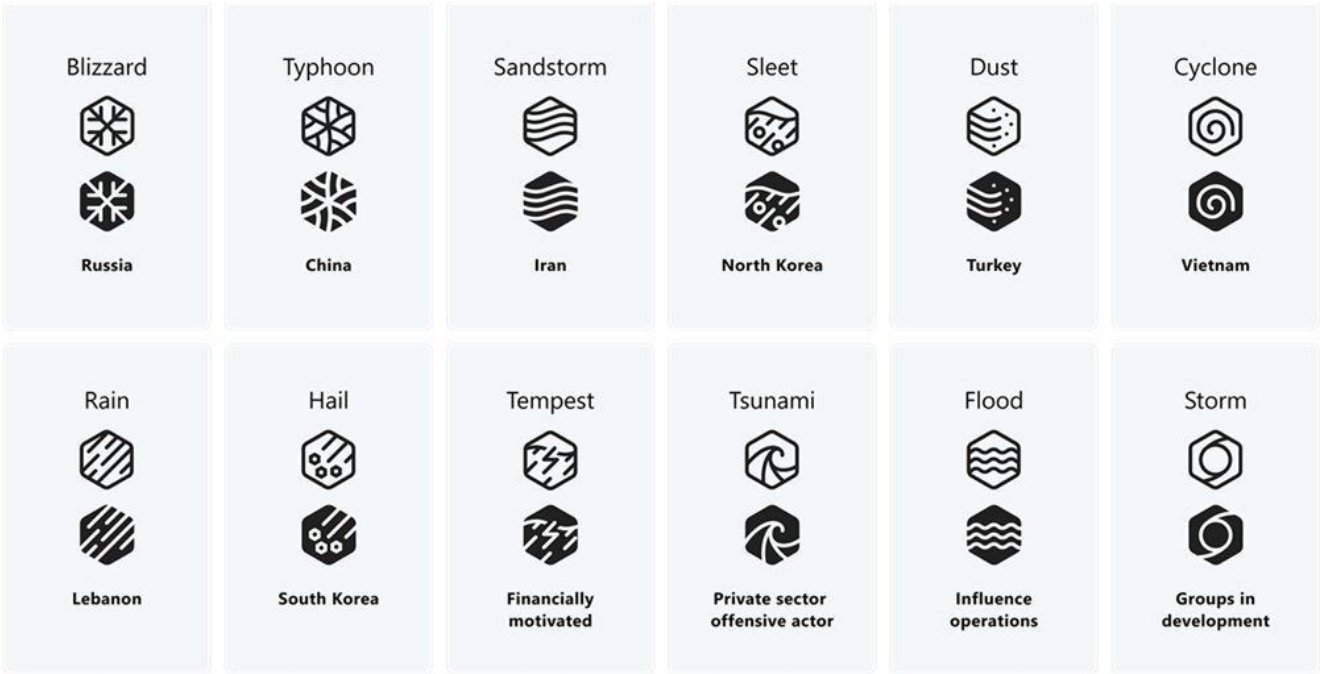
Angriff auf Unique Relations



Wer sind die Angreifer – und: woher kommen sie?

Microsoft verwendet inzwischen wetterbezogene Namen zur Klassifizierung von Hackergruppen.

Blizzard (Russland), Taifun (China), Sandstorm (Iran), Sleet (Nordkorea) sind die aktivsten Länder – die „Big Four“ in der Computerkriminalität.



Denim Tsunami: Gefährlicher Akteur aus Österreich

Denim Tsunami (früher: Knotweed / Subzero) bezeichnet eine österreichische Hack-for-Hire-Gruppe, vor der **Microsoft warnt**.

Österreichische Staatsanwälte arbeiten noch immer an diesem Fall, während das über 250 Mio. Euro werte Unternehmen sich damit verteidigte, ein irregeleiteter junger Mitarbeiter, hätte die gefährliche Software nur „ausprobiert“.

Die österreichischen Datenschutz-Aktivisten von epicenter.works haben dazu eine Anzeige bei der Polizei eingebracht.

Die wichtigsten Angriffswege

Die meisten Angriffe werden auf folgenden Wegem durchgeführt:

- Phishing Mails
- Verseuchte Memory-Sticks
- Social engineering
- Eindringen über verbundene Einrichtungen (Supply chain attacks)

Von: "UniCredit Austria AG." <webmaster@juniagut.de>
Datum: 5. August 2023 um 15:15:48 MESZ
Betreff: #UniCredit.Ticket : BA010631052. 05.08.2023

Bank Austria
Member of UniCredit

Sehr geehrter Kunde,

in Ihrem Konto wurde kürzlich ungewöhnliche Aktivitäten festgestellt .

Um nachzuweisen dass Sie der Eigentümer dieser Aktivitäten sind ,

müssen wir einige Informationen überprüfen .

Klicken Sie bitte auf den untenstehenden Link um die Aktualisierung zu starten .

Kundenbereich

Mit freundlichen Grüßen

© Ihr Bank Austria Team

Empfehlungen für mehr Computersicherheit

Oberstes Prinzip:

Sicherheit
ist
Chefsache!

Von der Spitze der Organisation muss der Anstoß für die Verstärkung der Sicherheitsmaßnahmen kommen:

- Krisenmanagementstrategie
- Klarheit über die eigene Datenverarbeitung
- Monitoring der Zulieferer, Partner und verbundenen Organisationen
- Abschluss einer Cyberversicherung
- Nutzung des „Cyber Insights Report“

In Zusammenarbeit mit dem Universitätsinstitut für Sicherheitsforschung und Krisenmanagement entwickelt.

Periodische Information über Cybergefahren, kriminelle Akteure und Fake News zur Gefahreneinschätzung – maßgeschneidert für Unternehmen, deren verbundene Einrichtungen, Partner und Lieferanten.

Daten dafür kommen aus der Analyse des Clearweb, Deepweb- und Darknet und aus Informationen von Strafverfolgungsbehörden, Journalisten und Universitäten.

CYBER INSIGHTS REPORT

K-ADVISORS

Kontakt

Kontakt

Dr. Cornelius Granig

CEO

K-ADVISORS

E-Mail: cornelius.granig@kadvisors.at

Mobil: +436643369013

CYBER INSIGHTS REPORT

K-ADVISORS