

Cybercrime aus polizeilicher Sicht

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

I Bedrohungslage und Phänomene

Eric Fischer, Kriminalkommissar



**CyberCrime
Competence
Center
Sachsen**

Agenda

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

Was ist Cybercrime?

Rolle der Polizei?

Phänomene und Trends

Was ist Cybercrime?

LANDES-
KRIMINALAMT



POLIZEI
Sachsen



Welche Arten von Cyber-Angriffen gibt es?



- Angriffe auf die Vertraulichkeit von Daten
- Angriffe auf die Integrität von Daten bzw. IT-Systemen z.B. durch die Manipulation von Informationen, Software oder Schnittstellen
- Angriffe auf die Verfügbarkeit von Daten oder IT-Diensten z.B. durch einen Denial-of-Service-Angriff

Warum sind Cyber-Angriffe möglich?



Rolle der Polizei bei Cybercrime?

LANDES-
KRIMINALAMT



POLIZEI
Sachsen





I Strafverfolgung

- I Aufklärung einer Straftat und die Ermittlung von Tatverdächtigen
- I Erhebung des objektiven und subjektiven Tatbefundes
 - I objektiv - Beweismittel (Daten, Screenshots, Daktyloskopische Spuren, DNA, Auskünfte von Providern und Geldinstituten)
 - I subjektiv - Zeugenvernehmung, Beschuldigtenvernehmung

I Gefahrenabwehr

- I Warnmeldungen zu aktuellen Phänomenen
- I allgemeine Prävention

Rolle der Polizei

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

- Cybercrime Competence Center Sachsen – SN4C
 - Gegründet 2014
 - Aktuell ca. 90 Spezialisten
 - IT-Analysten
 - IT-Ermittler
 - IT-Forensiker

Aktuelle Phänomene

LANDES-
KRIMINALAMT



POLIZEI
Sachsen



Phishing



- Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln".
- Phishing-Betrüger fälschen z.B. **E-Mails** und **Internetseiten** und finden immer wieder neuen Weg, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heran zu kommen – die Nutzer geben ihre Daten einfach freiwillig preis. (unbemerkt)
- Das „knacken“ von Passwörtern ist somit nicht erforderlich.

Phishing



Transaktionscode: 796225571181

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

Guten Tag Carsten [REDACTED]

es wurde eine verdächtige Zahlung getätigt in Höhe von 79,99 EUR an Zalando GmbH (paypal@zalando.de).

Unser System hat eine verdächtige Transaktion festgestellt welche eventuell nicht von Ihnen getätigt wurde. Als Schutzmaßnahme haben wir Ihr Konto vorübergehend eingeschränkt. Wenn Sie Ihr Konto weiterhin wie gewohnt nutzen möchten, bitten wir Sie Ihre Daten erneut zu verifizieren.

Sie haben für diese Verifizierung 24 Stunden Zeit, ansonsten sind wir aus datenschutzrechtlichen Gründen gezwungen Ihr Konto dauerhaft zu deaktivieren.

Sollten Sie diese Zahlung selbst veranlasst haben, bitten wir Sie diese erneut auszuführen. Die Transaktion wird unter Umständen nicht in der Übersicht angezeigt.

Wir bitten um Ihr Verständnis! <https://is.gd/sfbccc>
Klicken, um Link zu folgen

Identität bestätigen

Verkäufer

Zalando GmbH

Versanddetails

Der Verkäufer hat keine Versanddetails angegeben.

Mitteilung für Verkäufer

Vielen Dank für die Bestellung, Carsten!

Beschreibung	Stückpreis	Anzahl	Betrag
Nike Free Gr. 42 - schwarz	79,99 EUR	1	79,99 EUR
Artikelnr. 1HTCPC1R5			
	Versandkosten		0,00 EUR
	Versicherung - nicht angeboten		---
	Summe		79,99 EUR
	Zahlung		79,99 EUR

Zahlung gesendet an paypal@Nike.de

Copyright © 1999-2016 PayPal. Alle Rechte vorbehalten.
PayPal (Europe) S.À r.l. & Cie, S.C.A. Société en Commandite par Actions
Sitz: 22-24 Boulevard Royal, L-2449 Luxembourg RCS Luxembourg B 118 349

Phishing?




Suche

- Ungelesen 11
- Favoriten
- Freunde & Bekannte 9
- Unbekannt 2
- Bestellungen NEU
- Weitere Ordner
- Papierkorb
- Spam
- Gesendet
- Entwürfe
- Allbecon
- Deleted Messages
- gesendet
- Sent Messages
- Ordner hinzufügen
- E-Mail-Postfach hinzufügen

Ungewöhnliche Aktivitäten in Ihrem Konto

Von: service@paypal.de

 **PayPal**

Sehr geehrte/r Kunde,

aufgrund der neuen Datenschutz-Grundverordnung (DSGVO) des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die am 25. Mai 2018 in Kraft getreten ist, muss PayPal (Europe) seine AGB aktualisieren und eine Verifizierung aller Kundendaten durchführen.

Da Sie die Verifizierung bisher noch nicht in Ihrem Nutzerkonto durchgeführt haben und wir auch weiterhin den Schutz ihrer Daten gewährleisten müssen, fordern wir Sie dazu auf den Verifizierungsprozess innerhalb von 24 Stunden nach Erhalt dieser E-Mail durchzuführen.

<https://i.imgur.com/f5/f50ba5ea04.png>

Verifizierung durchführen

Falls wir Abweichungen in Ihren Angaben feststellen sollten, wird sich ein Support Mitarbeiter mit Ihnen in Verbindung setzen. Bitte führen Sie die Verifizierung schnellstmöglich durch und helfen Sie uns dabei Ihre Daten in Zukunft noch besser zu schützen.

Mit freundlichen Grüßen
PayPal-Sicherheitsteam

Diese PayPal-Benachrichtigung wurde an Sie gesendet, gesendet, weil Sie in Ihren E-Mail-Einstellungen unter "Neues von PayPal" den Erhalt aktiviert haben. Um diese Einstellungen zu ändern, klicken Sie [hier](#). Änderungen werden innerhalb von zehn Tagen wirksam.

Copyright © 1999-2019 PayPal. Alle Rechte vorbehalten. PayPal (Europe) S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Eingetragener Firmensitz: 22-24 Boulevard Royal, L-2449 Luxembourg RCS Luxembourg B 118 349.

WEB.DE Club Vorteile

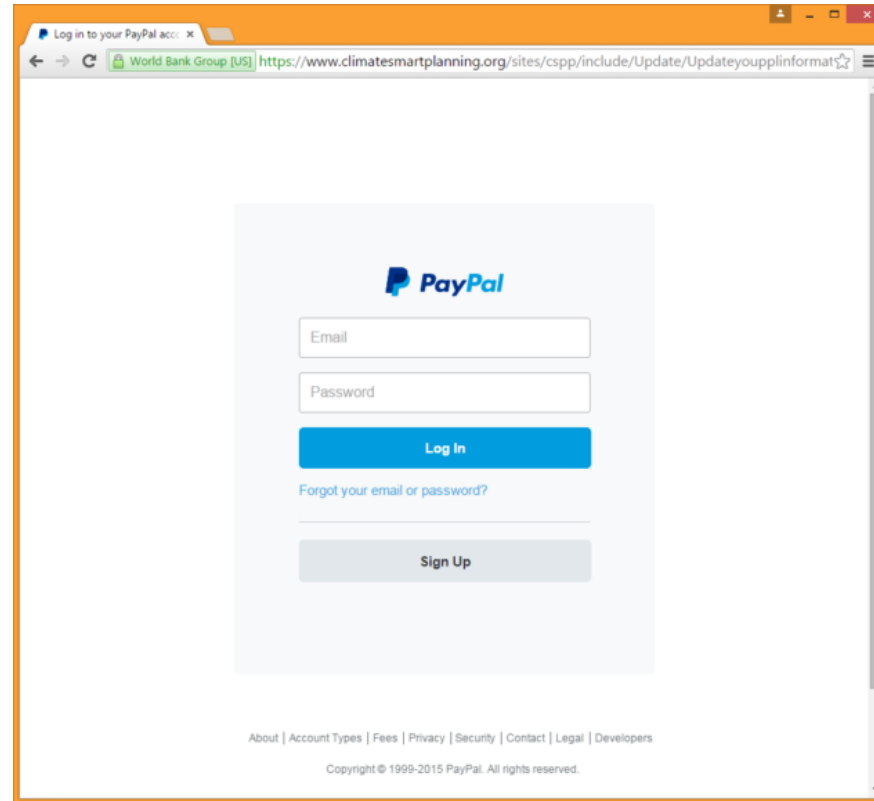
Hilfe

Einstellungen

Sofortantwort hier schreiben ...

<https://deref-web-02.de/mail/client/iNeWUTQMq4/dereferrer?redirectUrl=http://185.203.117.87/index.php?ref=msorptrt>

Phishing



Phishing?



Received-Details

Die Received-Zeilen sind in umgekehrter Reihenfolge (in der Reihenfolge ihrer Eintragung) sortiert.

1. Eintrag (Zeile 2):	from paypal.com ([89.34.111.117]) (authenticated) by <u>conuserg-12.nifty.com</u> with ESMTMP id x3BEmgw0008865 for <[REDACTED]>; Thu, 11 Apr 2019 23:48:43 +0900
Absender:	paypal.com
Absender IP-Adresse:	89.34.111.117
Absender (from):	paypal.com
Empfangen von:	conuserg-12.nifty.com
Empfangen mit:	ESMTMP
Empfangszeit:	11.04.2019 14:48:43 UTC
Zeit bis zum Empfang:	Nicht verfügbar
Empfangen für:	[REDACTED]
Warnung:	Der Absender ist möglicherweise nicht korrekt.
Hinweis:	Die Hostnamen stimmen überein.
2. Eintrag (Zeile 1):	from conuserg-12.nifty.com ([210.131.2.79]) by mx-ha.web.de (mxweb010 [212.227.15.17]) with ESMTPTS (Nemesis) id 1N8YLd-1gsPGL1twH-014WHR for <[REDACTED]>; Thu, 11 Apr 2019 16:48:57 +0200
Absender:	conuserg-12.nifty.com
Absender IP-Adresse:	210.131.2.79
Absender (from):	conuserg-12.nifty.com
Empfangen von:	mx-ha.web.de
Empfangen von (erw.):	mxweb010 [212.227.15.17] (Nemesis)
Empfangen mit:	ESMTPTS
Empfangszeit:	11.04.2019 14:48:57 UTC
Zeit bis zum Empfang:	14 Sek.
Empfangen für:	[REDACTED]
Hinweis:	Dieser Eintrag wurde vom Mailserver Ihres Providers erstellt.
Warnung:	Der Absender ist möglicherweise nicht korrekt.

Phishing?



56 engines detected this file

60c89ed8266335257535538ae329cfed8fd06e338afd07dc709b7debdea4ec1e

656c22d21d8d50e47a25a4d3327800da.virus

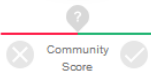
overlay peexe

1.39 MB

Size

2019-03-24 20:55:51 UTC

18 days ago



DETECTION

DETAILS

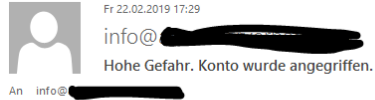
RELATIONS

BEHAVIOR

COMMUNITY

Acronis	! Suspicious	Ad-Aware	! Trojan.GenericKD.30969350
AegisLab	! Trojan.Win32.Cycler.l2bS	AhnLab-V3	! Win-Trojan/Unruy.1355704
ALYac	! Trojan.GenericKD.30969350	Antiy-AVL	! Trojan[Clicker]/Win32.Cycler
Arcabit	! Trojan.Generic.D1D88E06	Avast	! Win32.Unruy-AA [Trj]
AVG	! Win32.Unruy-AA [Trj]	Avira	! TR/Crypt.XPACK.Gen
Baidu	! Win32.Trojan-Clicker.Cycler.a	BitDefender	! Trojan.GenericKD.30969350
Bkav	! W32.DownloaderV2MT26G.Trojan	CAT-QuickHeal	! Trojan.Mauvaise.SL1
ClamAV	! Win.Downloader.Unruy-6804088-0	CMC	! Trojan-Clicker.Win32.CyclerIO
Comodo	! TrojWare.Win32.TrojanSpy.BZub.~IP@f8...	CrowdStrike Falcon	! Win/malicious_confidence_100% (D)
Cybereason	! Malicious.21d8d5	Cylance	! Unsafe

Sextortion



Hallo!

Wie Sie vielleicht bemerkt haben, habe ich Ihnen eine E-Mail von Ihrem Konto aus gesendet.
Dies bedeutet, dass ich vollen Zugriff auf Ihr Konto habe.

Ich habe dich jetzt seit ein paar Monaten beobachtet.
Tatsache ist, dass Sie über eine von Ihnen besuchte Website für Erwachsene mit Malware infiziert wurden.

Wenn Sie damit nicht vertraut sind, erkläre ich es Ihnen.
Der Trojaner-Virus ermöglicht mir den vollständigen Zugriff und die Kontrolle über einen Computer oder ein anderes Gerät.
Das heißt, ich kann alles auf Ihrem Bildschirm sehen, Kamera und Mikrofon einschalten, aber Sie wissen nichts davon.

Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre Korrespondenz.

Warum hat Ihr Antivirus keine Malware entdeckt?
Antwort: Meine Malware verwendet den Treiber.
Ich aktualisiere alle vier Stunden die Signaturen, damit Ihr Antivirus nicht verwendet wird.

Ich habe ein Video gemacht, das zeigt, wie du befriedigst dich... in der linken Hälfte des Bildschirms zufriedenstellen,
und in der rechten Hälfte sehen Sie das Video, das Sie angesehen haben.
Mit einem Mausclick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden.
Ich kann auch Zugriff auf alle Ihre E-Mail-Korrespondenz und Messenger, die Sie verwenden, posten.

Wenn Sie dies verhindern möchten, übertragen Sie den Betrag von 336€ an meine Bitcoin-Adresse
(wenn Sie nicht wissen, wie Sie dies tun sollen, schreiben Sie an Google: "Buy Bitcoin").

Meine Bitcoin-Adresse (BTC Wallet) lautet: 15mWFjVymAdqimVim2f1UgX6oSD4TYeGLE

Nach Zahlungseingang lösche ich das Video und Sie werden mich nie wieder hören.
Ich gebe dir 48 Stunden, um zu bezahlen.
Ich erhalte eine Benachrichtigung, dass Sie diesen Brief gelesen haben, und der Timer funktioniert, wenn Sie diesen Brief sehen.

Eine Beschwerde irgendwo einzureichen ist nicht sinnvoll, da diese E-Mail nicht wie meine Bitcoin-Adresse verfolgt werden kann.
Ich mache keine Fehler.

Wenn ich es herausfinde, dass Sie diese Nachricht mit einer anderen Person geteilt haben, wird das Video sofort verteilt.

Schöne Grüße!

Sextortion

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

Von: Marcelle Keel [mailto:marcellekeel@bipw.cia-us-govn.ga]

Gesendet: Montag, 18. März 2019 20:50

An:

Betreff: Central Intelligence Agency - Case #91235847

Case #91235847

Distribution and storage of pornographic electronic materials involving underage children.

My name is Marcelle Keel and I am a technical collection officer working for Central Intelligence Agency.

It has come to my attention that your personal details including your email address [REDACTED] are listed in case #91235847.

The following details are listed in the document's attachment:

- Your personal details,
- Home address,
- Work address,
- List of relatives and their contact information.

Case #91235847 is part of a large international operation set to arrest more than 2000 individuals suspected of paedophilia in 27 countries.

The data which could be used to acquire your personal information:

- Your ISP web browsing history,
- DNS queries history and connection logs,
- Deep web, onion browsing and/or connection sharing,
- Online chat-room logs,
- Social media activity log.

The first arrests are scheduled for April 8, 2019.

Why am I contacting you ?

I read the documentation and I know you are a wealthy person who may be concerned about reputation.

I am one of several people who have access to those documents and I have enough security clearance to amend and remove your details from this case. Here is my proposition.

Transfer exactly \$10,000 USD (ten thousand dollars - about 2.5 BTC) through Bitcoin network to this special bitcoin address:

3PWs1Man6a7rt28uK4jdamYxku2kjSBA

You can transfer funds with online bitcoin exchanges such as Coinbase, Bitstamp or Coinmama. The deadline is March 27, 2019 (I need few days to access and edit the files).

Upon confirming your transfer I will take care of all the files linked to you and you can rest assured no one will bother you.

Please do not contact me. I will contact you and confirm only when I see the valid transfer.

Regards,

Marcelle Keel

Technical Collection Officer

Directorate of Science and Technology

Central Intelligence Agency

Business Email Compromise



- Vortäuschung einer persönlichen Beziehung zum Opfer
 - Man-in-the-Middle-Attack
 - CEO-Fraud
 - Betrügerische Rechnung
 - Account Compromise (tatsächlicher Hack)
 - Datendiebstahl (Ziel: Personalabteilung)

CEO-Fraud (Betrügerische Chefmail)



CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge von Unternehmen. Mit fingierten **E-Mails** und Zahlungsanweisungen werden illegale Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen Automobilzulieferer getroffen.

Der deutsche Automobilzulieferer Leoni ist um rund 40 Millionen Euro betrogen worden, **wie das Unternehmen am Dienstag selbst bekanntgegeben hat** [↗](#). Die Angreifer nutzten dabei offenbar eine als Chef-Trick oder CEO-Fraud bekannt gewordene Masche, um sich Zugriff auf die Zahlungen zu sichern.

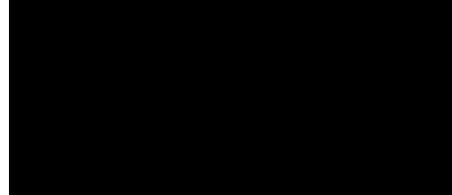
<https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html>

CEO-Fraud



From: G [REDACTED] B [REDACTED] [mailto:iphoneiosoffice@aol.com]
Sent: Wednesday, May 23, 2018 12:32 PM
To: A [REDACTED]
Subject: Banküberweisung.
Was ist unser Kontostand? Können wir heute 48 Tausend zahlen?
Grüße,
G [REDACTED] B [REDACTED].
Von meinem iPhone gesendet

...
From: A [REDACTED], B [REDACTED]
To: 'G [REDACTED] B [REDACTED]'; iphoneiosoffice@aol.com
Sent: Wed, May 23, 2018 12:22 pm
Subject: RE: Banküberweisung.
ja, können wir
B [REDACTED] A [REDACTED]
Verwaltungsbeauftragte



...
Von: G [REDACTED] B [REDACTED] [mailto:iphoneiosoffice@aol.com]
Gesendet: Mittwoch, 23. Mai 2018 14:15
An: A [REDACTED], B [REDACTED]
Betreff: Re: Banküberweisung.
Bank: Barclays Bank Plc.
Name: [REDACTED]
IBAN: GB [REDACTED]
SWIFT CODE: BUKBGB22
Bank Address: [REDACTED].United Kingdom
Senden Sie mir die Zahlungsbestätigung, wenn sie abgeschlossen ist.
Grüße,
G [REDACTED] B [REDACTED].
Von meinem iPhone gesendet

...
Von: G [REDACTED] B [REDACTED] [mailto:iphoneiosoffice@aol.com]
Gesendet: Mittwoch, 23. Mai 2018 17:24
An: A [REDACTED], B [REDACTED]
Betreff: Re: Banküberweisung.
Ist die Zahlung abgeschlossen?
Grüße,
G [REDACTED] B [REDACTED].
Von meinem iPhone gesendet

Betrügerische Rechnung



Di 05.06.2018 08:55

Dr. [REDACTED] <cpelaez@tarmexico.com>

Rechnungszahlung 55254273

An [REDACTED]

Guten Tag,
[REDACTED]

ich hab versucht Sie telefonisch zu erreichen.
Leider waren Sie nicht da. Ich hab um Rückruf gebeten.
Da ich aber nicht den ganzen Tag im Büro sein werde, möchte ich Ihnen gerne sagen,
dass ich schon enttäuscht bin, dass die versprochene Zahlung noch nicht angekommen ist.
Ich bitte Sie, die Zahlung bis Dienstag zu tätigen, die Rechnung ist unter dem folgenden Link
verfügbar.

>>> <http://chris-dark.com/Zahlungserinnerung/Bezahlen-Sie-die-Rechnung-Nr02996/>

Wir bedanken uns für Ihr Vertrauen und wünschen Ihnen weiterhin viel Erfolg.
[REDACTED]

Digitale Erpressung mittels Verschlüsselungstrojanern



Ransomware



- 2017: Deutsche Bahn durch Ransomware befallen
- 2018: sächsische Autohauskette durch Emotet + Ransomware befallen
- 2019: Ransomware befällt Norsk Hydro
- 2019: Trägergesellschaft Süd-West des DRK durch Ransomware offline

Die Zentrale Ansprechstelle Cybercrime (ZAC)

LANDES-
KRIMINALAMT



POLIZEI
Sachsen

Kontakt:

LKA Sachsen

Neuländer Straße 60, 01129 Dresden

Telefon: 0351 855 3226

E-Mail: zac.lka@polizei.sachsen.de



Danke für Ihre Aufmerksamkeit!

