

Wiederkehrendes Phishing

Beispiele für E-Mails oder Mitteilungen, die mit diesem oder einem ähnlichen Wortlaut immer wieder versendet werden:

Bitcoin-Erpressung (deutsch)	2
Ich beobachte dich	2
Es geht nur um ihren Ruf / Sie müssen zusammenarbeiten / Du bist gehackt	3
Ich weiß, „...“, das ist dein Passwort	4
Hallo ...,	5
Bitcoin-Erpressung (englisch)	6
Hi, stranger!	6
Bestell-Bestätigungen	7
Im Namen von Amazon	7
Im Namen von PayPal	8
Im Namen von Apple / App store / iTunes	9
Zoll-Kundendienst	10
Meistens mit Bezug auf DHL	10
EMOTET	11
Viruswarnung	13

Bitcoin-Erpressung (deutsch)

ICH BEOBACHTE DICH

Hallo ...

Entschuldigung, aber ich mochte Sie warnen. Ich hatte dein Foto, ich verfolge dich seit einigen Tagen, jetzt weiß ich alles.

Dein Freund rat dir, Schwefelsäure auf dein Gesicht zu gießen, aber ich will nicht, aber ich brauche wirklich Geld. Ich schlage vor, Sie zahlen mir 750 Euro und stornieren meine Bestellung. Wenn ich kein Geld von dir bekomme, muss ich meinen Job machen. Sie haben genau 72 Stunden. Ich akzeptiere nur Bitcoins. Bitcoin ist anonym, niemand wird wissen, wie viel Sie mir bezahlt haben.

Bitcoin-Adresse: ...

(Kopieren Sie die Adresse und senden Sie die Details)

Wenn Sie nicht wissen, wo Sie Bitcoin kaufen können, geben Sie „Bitcoin kaufen“ in die Google-Suchmaschine ein.

Und folgen Sie den Anweisungen.

Wenn ich Geld von Ihnen erhalte, sende ich Ihnen ein Foto und ein Video dieser Frau.

Denken Sie daran, die Zeit läuft ab!

Was sind meine Regeln?

Ich habe 3 Regeln

Wenn Sie diese Nachricht teilen, wird Ihr Ruf ruiniert.

Wenn Sie nicht bezahlen, wird Ihr Ruf ruiniert.

Wenn Sie versuchen, mich auszutricksen, wird Ihr Ruf ruiniert.

Ich gebe Ihnen ab diesem Moment nicht mehr als 50 Stunden Zeit, um den Deal abzuschließen.

Verschwenden Sie nicht Ihre Zeit. Ich kann nicht aufgespürt werden und niemand kann dir helfen, also denke nicht, dass dir jemand helfen kann, wenn du dich beschwerst.

ES GEHT NUR UM IHREN RUF / SIE MÜSSEN ZUSAMMENARBEITEN / DU BIST GEHACKT

Schönen Tag,

Wer bin ich?

Ich bin ein professioneller Pentester und habe Ihr System infiziert, als Sie eine Website für Erwachsene besucht haben ...

Ich habe Ihre Aktivität seit mehr als 1 Monat überprüft.

Worüber rede ich?

Mit meiner Malware kann ich auf Ihr System zugreifen. Es ist ein Multiplattform-Virus mit versteckter VNC. Es funktioniert unter iOS, Android, Windows und MacOS. Es ist verschlüsselt, so dass Ihr AV es nicht erkennen kann. Ich reinige seine Signaturen jeden Tag.

Was habe ich?

Ich könnte Ihre Kamera einschalten und alle Ihre Protokolle speichern.

Ich habe alle Ihre Kontakte, Social-Media-Daten und Chats mit Ihren Freunden, Kollegen, usw.

Ich habe Informationen gesammelt, die Ihren Ruf ruinieren können.

Ich habe ein Video mit deiner Masturbation und dem Video, das du gesehen hast. Es ist schrecklich ...

Was will ich?

Ich werde diese Aufzeichnung veröffentlichen und Ihr Leben wird zerstört, wenn Sie nicht 1000 Dollar mit Bitcoins bezahlen.

Verwenden Sie diese Bitcoin-Adresse : ...

Wie kannst du mich bezahlen?

Verwenden Sie Google, um zu erfahren, wie Sie Bitcoins kaufen und ausgeben.

Was sind meine Regeln?

Ich habe 3 Regeln

Wenn Sie diese Nachricht teilen, wird Ihr Ruf ruiniert.

Wenn Sie nicht bezahlen, wird Ihr Ruf ruiniert.

Wenn Sie versuchen, mich auszutricksen, wird Ihr Ruf ruiniert.

Ich gebe Ihnen ab diesem Moment nicht mehr als 50 Stunden Zeit, um den Deal abzuschließen.

Verschwenden Sie nicht Ihre Zeit. Ich kann nicht aufgespürt werden und niemand kann dir helfen, also denke nicht, dass dir jemand helfen kann, wenn du dich beschwerst.

ICH WEIß, „...“, DAS IST DEIN PASSWORT

Ich weiß, „...“, das ist dein Kennwort.

Ich bin dir nicht vertraut, und voraussichtlich interessierst du dich, warum du diese E-Mail erhalten hast, richtig?

Lass es mich verständlich machen.

Ich habe einen Virus auf der Seite mit Videos für Erwachsene (sexueller Inhalt) gepostet. Mehr noch, hast du diese Website aufgerufen, um mit sich zu spielen (du weißt, was ich meine).

Während du die Videos angesehen hast, hat dein Internet-Browser das Skript für den Fernzugriff geladen, und ich habe Zugriff auf deinen Bildschirm und deine Kamera erhalten. Klarerweise habe ich entschieden aufzunehmen, was du siehst und tust))

Es stellte sich eine wunderbare Collage aus den Videos heraus, man kann dich da deutlich sehen. Es gibt nun ein Doppelbildschirm-Video mit dir und den Pornofilmen, die du ansiehst hast)) Ich möchte bemerken, du hast befremdliche Bevorzugungen. Lass es uns das Video, das ich aufgenommen habe, vor deinen Bekannten in sozialen Netzwerken und Messengerdiensten geheim halten.

Wenn ich du wäre, würde ich nicht wollen, dass meine Verwandten und Bekannte mich auf so unangenehmen Weise sehen.

Was kannst du machen, um dies zu verhindern?

Ich bin der Meinung, dass 600 euro eine passende Summe für meine neutrale Position sind.

Hier ist meine Bitcoin-Geldbörse: ...

Schaue dich in Google, wie man mit dieser Währung zahlen kann. Ich glaube, sieben Tage sind genug, um die Zahlung zu machen, in anderen Fall sei nicht beleidigt auf mich.

Denken Sie daran, ich habe Ihnen nur 7 Tage gegeben!

HALLO ...,

Durch eine Sicherheitslücke in deinem System konnte ich unbemerkt einen Virus auf deinem Gerät installieren.

Aufgrund dieses Virus hab ich kompletten Zugriff auf dein System. Ich hab versteckt auf deiner Festplatte Kinderpornos gespeichert, sowie ein Sicherheitskopie deiner persönlichen Daten(z.B Deine Anschrift und Bankdaten),Fotos & Videos erstellt.

Solltest du mir nicht glauben hier ein Parr Beispieldaten:

Name: ...

Geburtsdatum: ...

Adresse: ...

PLZ / Stadt: ...

Bank: ...

IBAN: ...

Als du dich das Letzte mal selbstbefriedigt hast, hab ich mithilfe des Virus ein Video aufgezeichnet. Auf diesem Video ist zusehen, wie du masturbierst, ich hab durch gekonnte Bearbeitung das Video verändert, das man im Vordergrund siehst, wie Du masturbierst und im Hintergrund/„Deinem Bildschirm“) Sieht man wie Du dir Kinderpornos anguckst. Du und ich wissen das es sich dabei um ein „Fake“ handelt., Aber stell dir vor was passiert, wenn ich das Video veröffentliche, es an die Polizei weiterleite. Die Polizei wird eine Hausdurchsuchung bei dir durchführen und wird die gespeichert Kinderpornos finden, du wirst ein verurteilter Kinderschänder sein.

Deine Freunde und Familie werden sich von dir abwenden, du wirst dein Job verlieren. Niemand wird etwas mit dir zutun haben wollen.

Als du diese E-Mail geöffnet hast, hat Sicht automatisch ein Timer gestartet.

Du hast ab jetzt 72 Stunden zeit 750€ in Bitcoin an die nachfolgende Bitcoin Adresse(„Bitcoin Wallet“) zu zahlen: ...

Sollte die Zahlung in dieser Frist nicht eingehen, wird das Video automatisch veröffentlicht, es wird deine Freunde und Familie weitergeleitet und außerdem wir anzeige bei der Polizei erstattet.

Solltest du aber wie gefordert zahlen, wird sich das Video automatisch Löschen, die Kinderpornos werden von deiner Festplatte gelöscht und du wirst nie wieder von mir Höhren.

Wenn du nicht weißt, wie du an Bitcoins kommst bzw. Wie du das kaufen kannst, ich helfe dir gerne bei. Es ist ganz einfach, du gehst einfach auf google und suchst nach einen der beiden Sätze“Wie Kauf ich Bitcoins“ oder „How to Buy Bitcoins“

... das ist kein Scherz, solltest du die 750€ nicht bezahlen werde ich deine leben zerstören.

Ich werde nicht aufhören bis du alles verloren hast und als Kinderschänder abgestempelt bist, es liegt in deiner Hand.

Bitcoin-Erpressung (englisch)

HI, STRANGER!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy (you know what I mean).

While you were watching video clips,
My trojan started working as a RDP (remote desktop) with a key logger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people), and the second part shows the recording of your webcam.

What should you do?

Well, I think \$565 (USD dollars) is a fair price for our little secret.
You will make a bitcoin payment (if you don't know, look for „how to buy bitcoins“ on Google).

BTC Address: ...
(This is CASE sensitive, please copy and paste it)

Remarks:
You have 2 days (48 hours) to pay. (I have a special code, and at the moment I know that you have read this email).

If I don't get bitcoins, I will send your video to all your contacts, including family members, colleagues, etc.
However, if I am paid, I will immediately destroy the video, and my trojan will be destruct someself.

If you want to get proof, answer „Yes!“ And resend this letter to yourself.
And I will definitely send your video to your any 19 contacts.

This is a non-negotiable offer, so please do not waste my personal and other people's time by replying to this email.
Bye!

Bestell-Bestätigungen

IM NAMEN VON AMAZON

... für bestellte Produkte unterschiedlicher Hersteller. Als Absende-Adresse ist meistens die Domain des jeweiligen Herstellers angegeben.

[Meine Bestellungen](#) | [Mein Konto](#) | [Amazon.de](#)

amazon.de

Bestellbestätigung
Bestellung # 304-...

... - Ihre Bestellung war erfolgreich!

Aufgrund der Annahme, dass es sich bei dieser Bestellung um einen autorisierten Zugriff handelt haben wir die Bestellung als ausstehend markiert und Ihr Konto vorerst eingeschränkt.

[Stornieren](#) Sie die unauthorisierte Buchung und heben Sie die Kontoeinschränkung auf.

Bestellübersicht

Bestellnummer # 304-...

Aufgegeben am xx.xx.2020

Zustellung: Bestellung ausstehend	Die Bestellung geht an: Deutschland
Maßnahme: Stornierung	
Bestellung stornieren	



[Produktbeschreibung ...](#)

Verkauft von: Amazon EU S.à.r.l.

EUR

IM NAMEN VON PAYPAL

... für bestellte Produkte unterschiedlicher Hersteller.

PayPal

Transaktionscode: 0-...

Sie haben eine Bestellung über, EUR an ... AG gesendet

Vielen Dank für Ihre Bestellung bei ... AG. Das Geld wird erst dann von Ihrem Konto abgebucht, wenn die Bestellung von ... AG verarbeitet wurde. Ihr Guthaben wird hierfür immer vorrangig vor anderen Zahlungsquellen wie Bankkonto oder Kreditkarte verwendet.

Probleme mit Ihrer Zahlung?

Falls Sie nicht transaktions.

Zahlung gesendet an ... @com

Lassen Sie es uns umgehend wissen

Händler

... AG
... @com

Mitteilung an Händler

Sie haben keine Mitteilung eingegeben.

Beschreibung	Stückpreis	Anzahl	Betrag
Artikelnr.	€...,... EUR	1	€...,... EUR
		Zwischensumme	€...,... EUR
		Summe	€...,... EUR

Probleme mit Ihrer Zahlung?

Ab dem Datum der Transaktion haben Sie 180 Tage lang Zeit, um auf der Seite „Konfliktlösungen“ ein Problem zu melden.

Bitte antworten Sie nicht auf diese E-Mail. Diese Mailbox wird nicht überwacht. Wenn Sie Hilfe benötigen, loggen Sie sich in Ihr PayPal-Konto ein und klicken Sie auf **Hilfe**.

Anstelle unserer HTML-E-Mails können wir Ihnen Benachrichtigungen auch als Reintext zusenden. Wenn Sie Ihre Optionen für E-Mail-Benachrichtigungen ändern wollen, loggen Sie sich in Ihr Konto ein und klicken Sie unter „Mein Profil“ auf **Einstellungen**.

Copyright © 1999-2020 .Alle Rechte vorbehalten.
PayPal (Europe) ...

IM NAMEN VON APPLE / APP STORE / ITUNES

App Store		Steuerrechnung	
Rechnungseingang			
DATE		BILLED WITH	TOTAL
...tag, xx. ... 2020		KREDITKARTE	xx.xx €
ORDER ID	DOCUMENT NO.		
T...	8...		
App Store	TYPE	PURCHASED FROM	PRICE
ABBILDUNG	In-App Purchase	iPhone	...,... €
		TOTAL	...,... €
<p>Probleme mit dieser Transaktion? Wenn Sie diese Transaktion nicht autorisiert haben, Klicken Sie auf den Link unten, um Ihre Bestellung zu stornieren oder eine vollständige Rückerstattung zu erhalten:</p> <p>Melden Sie ein Problem, verwalten Sie die Zahlung oder stornieren Sie Ihre Bestellung ></p>			
 Deutschland Copyright © 2019 Apple Inc. Alle Rechte vorbehalten			

Zoll-Kundendienst

MEISTENS MIT BEZUG AUF DHL

Sehr geehrter Kunde,

Ihr DHL-Paket Nr. ..., versandt am 22.09.2020, wird bearbeitet. Damit wir Ihr Paket liefern können, werden dem Importeur die Mehrwertsteuernkosten erneut in Rechnung gestellt.

Nach den geltenden Zollbestimmungen ist jede Einfuhr aus einem Land außerhalb der Europäischen Gemeinschaft mit einem Handelswert von mehr als 22 EUR unabhängig von der Art der Waren steuerpflichtig *.

*Artikel 134-I und II-1 ° des CGI: GESETZ Nr. 2012-1510 vom 03. Mai 2017 – Art. 68 (V) Die Validierung des Paysafecard-Guthabens für die Zahlung von Zollgebühren ist gültig.

Um die Zustellung Ihres Pakets für Ihre Heimatadresse zu ermöglichen, bitten wir Sie, Ihre nicht bezahlten Zollgebühren zu regulieren, indem Sie die folgenden Schritte ausführen, um die Zustellung Ihres Pakets abzuschließen.

1. [Kaufen Sie eine Paysafecard PIN-Code online \(50 EUR\)](#)
2. Senden Sie den PIN-Code (16 Ziffern) an folgende Adresse.

[dhl @ postoffice-fees .com](mailto:dhl@postoffice-fees.com)

Grüße,
Zoll-Kundendienst

EMOTET

Typische Formulierungen, die Sie alarmieren sollten sowie Beispiele für E-Mails, deren alleiniger Zweck die Verbreitung von Emotet oder ähnlicher Trojaner ist.

Betreff: - RE:

- Sofortmeldung
- Anfrage (mit Kundennummer und Namen Ihres Unternehmens)
- AW: Bezugnahme auf Ihr Unternehmen / Ihre Dienstleistung

E-Mail-Text:

Die Texte sind i. d. R. kurz, können in deutscher oder englischer Sprache verfasst sein und verweisen (nur) auf angehängte Dokumente (Rechnungen, Word-Dokumente).

- Anbei erhalten Sie Ihre angeforderten Informationen für Ihre Unterlagen
- Im Anhang dieser E-Mail erhalten Sie Informationen zu Ihrem Vertrag
- Alle Angaben entnehmen Sie bitte dem angehängten angeforderten Dokument
- Eine Dokumentation befindet sich im Anhang
- In der Anlage das SEPA Formular und die neue Rechnungsanschrift
- Your statement ist attached (Ihre Abrechnung ist angehängt.) und/oder
- Please remit payment at your earliest convenience (Bitte überweisen Sie die Zahlung baldmöglichst.)

Dringlichkeitshinweis:

- Bei Rückfragen oder Reklamationen erwarten wir eine Kontaktaufnahme innerhalb von zwei Werktagen

Anhang:

- RechnungsDetails_tt_mm_2020_... .doc
- GmbH_2020-mm.doc



Guten Morgen ...,

Bitte Sofortmeldung zu Frau ... siehe Anhang . Den AV bringe ich morgen, die I beantragt.
Vielen Dank

...

Von ...(Gerät) gesendet.

 RechnungsDetails... 228 KB

Sehr geehrte ...,

Wie telefonisch besprochen, sind wir gerade auf der Suche nach einer Glas- und Rahmenreinigung (beidseitig inkl. Falze, Außen- und Innenverglasung) für mindestens die Front unseres Haupteinganges (siehe blaue Markierung). Präferieren würden wir die Reinigung des gesamten Gebäudes wie bereits im vergangenen Jahr abgewickelt. (...) zu der Herausforderung. Die Reinigung müsste spätestens am ..., den tt.mm.2020 erfolgen muss, da wir am ... einen ...

 GmbH... 229 KB

... oder ...

In der Anlage das SEPA Formular und die neue Rechnungsanschrift.

Mit freundlichen Grüßen,

... service

 RECH... 229 KB

Viruswarnung

Einblendungen mit diesen oder ähnlich lautenden Texten (i. d. R. Im Browser als Overlay über einer Webseite) geben vor von Microsoft initiiert zu sein:

**Windows wurde aufgrund verdächtiger Aktivitäten blockiert
Bitte aufhören und den PC nicht schließen**

Anmelden

http: www. winhelpde .club

Die Verbindung zu dieser Webseite ist nicht sicher.

Nutzername:

Passwort:

[Abbrechen](#) | [Anmelden](#)

Authentifizierung erforderlich

http: www. win-firefox-help-jp .club ich ersuche Ihren Benutzernamen und Ihr Passwort. **Warnung: Passwörter werden nicht an die Webseite gesendet, die Sie gerade besuchen. Website Edition: „Ihr Computer ist gesperrt, um Ihren Computer sicher zu machen, Hotline-Nummer**

Nutzername:

Passwort:

[OK](#) | [Stornieren](#)

Das System ist schwer beschädigt, gefunden (4) virus!

Wir haben festgestellt, dass es ein beschädigtes Betriebssystem 37,2% und enthält (4) Viren!

Fast 80% der Computer sind infiziert. Ihr computer wurde auch gehackt!

Wenn Sie das Virus jetzt nicht entfernen, kann dies Systemdateien, Daten, Anwendungen usw. beschädigen.

Sie müssen tun (Schritt für Schritt):

Schritt 1: Drücken Sie die Taste Herunterladen und jetzt kostenlos laden!

Schritt 2: Wählen und öffnen Sie die Anwendung, um die Systeme wiederherzustellen!

4 Minuten 51 Sekundenschnelle [HERUNTERLADEN >>]