

[Spam] Hohe Gefahr. Konto wurde angegriffen.

Eine Betrügernachricht an meine spezielle E-Mailadresse (nur für Newsgroups) landete, in meinen Postfach. Hier geht es nur um Lügen, Drohungen und eine handfeste Erpressung ...

Besten Dank, Betrüger!

Hier ist der gesamte geistige Durchfall zu lesen:

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 Mausklick 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 325€ 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!

... gelesen, gelacht! 🤪

Ein angeblicher Zugriff auf „Ihrem Konto“ würde im E-Mailheader ganz anders aussehen und das trifft auch für die „Benachrichtigung“ zu. Einfach eine fremde E-Mailadresse als Absender anzugeben erfordert kein Fachwissen.

Die Nachricht wurde direkt von der IP-Adresse: [138.122.29.242](#) an den MX-Server der Domain zugestellt.

Die Betrügernachricht ist nur ein Lügenkonstrukt mit Nötigung und Erpressung. (Siehe: [§240 StGB](#), [§253 StGB](#))

Sehr interessant aus der Artikel auf Heise.de: „[Porno-Erpresser-Mails: 17-jähriger Tatverdächtiger in Bremen verhaftet](#)„

So wie es aussieht ist hier jede Menge kriminelle Energie dabei.

[spam,betrug,nötigung,erpressung](#)

From:
<https://www.remo-web.de/> - **remo-web.de**

Permanent link:
https://www.remo-web.de/doku.php?id=blog:spam_hohe_gefahr_konto_wurde_angegriffen

Last update: **2019/03/17 16:52**



