Über Drohmails.

(Von E. Noldus.)

Eine lästige Begleiterscheinung der Kommunikation per e-Mail ist der Empfang von Datenmüll, der die verschiedensten Formen annehmen kann. Von Billigkrediten bis Potenzpillen reicht die Bandbreite dieser ungewollten Zuschriften. Interessant sind Drohmails, die mit einer Erpressung verbunden sind. Wir geben hier einige Beispiele und daran anschließend einige Hinweise, wie man mehr über die Hintergründe dieser Art von Mails erfahren kann.

Drohmail vom 13. 5. 2021

Freut mich, dich kennenzulernen! Wir setzen uns mit Ihnen in Verbindung, um Sie über unsere Enttäuschung zu informieren. Ich habe vor ein paar Monaten auf das Gerät zugegriffen, mit dem Sie im Internet surfen, und verfolge seitdem die Internetaktivität.

Der Grund für den Zugriff war, dass ich vor einiger Zeit von einem Hacker den Zugriff auf mein E-Mail-Konto gekauft habe (es ist heutzutage ziemlich einfach, solche Dinge online zu kaufen). So konnte ich mich problemlos in Ihr E-Mail-Konto einloggen (kontakt@afd-ob.de). Eine Woche nach dem Anmelden habe ich bereits eine Trojaner-Malware auf dem Betriebssystem aller Geräte installiert, die mit Ihrer E-Mail verbunden sind. Tatsächlich war es überhaupt nicht schwierig. (Vielen Dank, dass Sie dem E-Mail-Link in Ihrem Posteingang problemlos folgen.) Die cleveren Tricks sind alle überraschend einfach. (^^) Mit der Software können Sie alle Ihre Geräte (z. B. Mikrofon, Camcorder, Tastatur) steuern.

Ich habe Ihre persönlichen Informationen, Daten, Fotos und den Browserverlauf bereits auf meinem Server heruntergeladen und gespeichert. Ich habe Zugriff auf alle Ihre Messenger-, Social Media-, E-Mail-, Chat-Verlaufs- und Kontaktlisten. Mein Virus arbeitet auf Treiberebene und aktualisiert die Signatur kontinuierlich, sodass sie von der Antivirensoftware nicht erkannt wird. In ähnlicher Weise verstehen Sie jetzt, warum dieser Brief von Antivirensoftware nicht erkannt wurde. Während Sie Ihre Informationen sammeln, befinden Sie sich auf einer Website für Erwachsene. Ich habe festgestellt, dass ich ein großer Fan bin. Sie scheinen es wirklich zu mögen, Pornoseiten zu besuchen und aufregende Videos anzusehen, während Sie enorme Freuden ertragen. Zufälligerweise ist es mir gelungen, Ihre obszöne Szene aufzunehmen, also habe ich mehrere Videos montiert, die zeigen, wie Sie masturbieren und Ihren Höhepunkt erreichen.

Wenn Sie der Meinung sind, dass es eine Lüge ist, stellen Sie sicher, dass alle Ihre Videos mit nur wenigen Mausklicks mit Ihren Freunden, Kollegen und Verwandten geteilt werden können. Für mich gibt es kein Problem mit dem öffentlichen Zugang. Selbst wenn Sie den Geschmack Ihres Lieblingsvideos berücksichtigen, möchten Sie ein solches Video nicht öffentlich machen. (Sie wissen, was ich meine) Wenn es an die Öffentlichkeit geht, könnte es eine echte Katastrophe sein. Also lasst uns hier handeln.

Bitte überweisen Sie mir 1500 Euro (der Betrag, der Bitcoin zum Wechselkurs zum Zeitpunkt der Überweisung entspricht). Wenn Sie die Übertragung erhalten, löschen Sie alle diese obszönen Videos. Danach vergessen wir uns sauber und versprechen, schädliche Software auf Ihrem Gerät zu stoppen und zu entfernen. Ich werde behalten, was ich gesagt habe. Angesichts der Tatsache, dass ich Ihr Profil und Ihren Datenverkehr für eine Weile überprüft habe, ist dies ein fairer Deal und sollte ziemlich billig sein. Wenn Sie nicht wissen, wie Sie Bitcoin kaufen oder übertragen können, können Sie es finden, indem Sie mit einer beliebigen Suchmaschine suchen. Meine Bitcoin-Brieftasche ist 19dRnjdXfyLtVJQqppYAq6bjRQzB5SGRC4 . Geben Sie 48 Stunden (2 Tage um genau zu sein) ab dem Moment, in dem Sie diese E-Mail öffnen. Bitte unterlassen Sie die folgenden Handlungen. *

Antworte mir. (Weil ich diese E-Mail in Ihrem Posteingang erstellt und auch eine Antwortadresse erstellt habe.) * Ich habe versucht, die Polizei oder andere Sicherheitsdienste zu kontaktieren. Sprich auch nicht mit deinen Freunden. Wenn ich feststelle, dass ich spreche, wird Ihr Video veröffentlicht. (Ich kontrolliere alles in Ihrem System, daher glaube ich nicht, dass es so schwer zu erkennen ist.) * Ich versuche, mich zu finden.

Alle Kryptowährungstransaktionen sind anonym und absolut bedeutungslos. * Neuinstallation oder Zerstörung des Betriebssystems auf dem Gerät. Dies ist auch sinnlos, da alle Videos bereits auf dem Remote-Server gespeichert sind. Das Folgende sind Dinge, über die Sie sich keine Sorgen machen müssen. * Ich kann die Überweisung nicht erhalten. —— Seien Sie versichert, dass wir alle Ihre Aktionen verfolgen und Ihnen zeigen, sobald Ihre Übertragung abgeschlossen ist. (Meine Trojaner-Malware verfügt über eine Fernbedienungsfunktion wie TeamViewer.) * Ich kann Ihr Video auch dann freigeben, wenn Sie die Übertragung abgeschlossen haben. »Vertrau mir. Ich werde Ihr Leben nicht komplizierter machen, und wenn Sie es nur teilen möchten, sollten Sie diesen Brief nicht senden! Mach alles fair!

Und noch etwas ... lassen Sie sich in Zukunft nicht in die gleiche Situation verwickeln!

Drohmail vom 24. 7. 2021 02:56

Von no-reply@xn--sueocelestepago-0qb.com

Betreff Zahlung von Ihrem Konto

An kontakt@afd-ob.de

Grüße!

Ich muss Ihnen schlechte Nachrichten mitteilen.

Vor ungefähr einigen Monaten habe ich Zugriff auf Ihre Geräte erhalten, die Sie zum Surfen im Internet verwenden. Danach habe ich begonnen, Ihre Internetaktivitäten zu verfolgen. Hier ist der Ablauf der Ereignisse: Irgendwann Vorher habe ich Zugang zu E-Mail-Konten von Hackern erworben (heute ist es ziemlich einfach, so etwas online zu kaufen).Offensichtlich habe ich es problemlos geschafft, mich in Ihr E-Mail-Konto einzuloggen kontakt@afd-ob.de

Wenn Sie Zweifel haben, kann ich ein paar Mausklicks machen und alle Ihre Videos werden an Ihre Freunde, Kollegen und Verwandten weitergegeben. Ich habe auch überhaupt kein Problem damit, sie öffentlich zugänglich zu machen. Ich denke, das möchten Sie wirklich nicht, wenn man die Besonderheiten der Videos bedenkt, die Sie sich gerne ansehen. (Sie wissen genau, was ich meine) es wird eine wahre Katastrophe für Sie verursachen.

Lassen Sie es uns so regeln: Sie überweisen mir 1500 EUR (in Bitcoin-Äquivalent zum Wechselkurs zum Zeitpunkt der Überweisung), und sobald die Überweisung eingegangen ist, werde ich all dieses schmutzige Zeug sofort löschen. Danach werden wir uns vergessen. Ich verspreche auch, alle schädliche Software von Ihren Geräten zu deaktivieren und zu löschen.

Vertrauen Sie mir, ich halte mein Wort. Dies ist ein fairer Deal und der Preis ist ziemlich niedrig, wenn man bedenkt, dass ich schon seit einiger Zeit dein Profil und deinen Traffic checke. Im Falle, Wenn Sie nicht wissen, wie Sie die Bitcoins kaufen und übertragen sollen, können Sie jede moderne Suchmaschine verwenden.

Hier ist meine Bitcoin-Wallet: 1PEerGK1e5R1JTiiNYAnrAdR9eN9BRSgYj

Sie haben weniger als 48 Stunden ab dem Zeitpunkt, an dem Sie diese E-Mail geöffnet haben (genau 2 Tage).

Ein Informationsschreiben vom 25. 7. 2021.

Hallo

Ihr DE65062006047IN-Paket wird verarbeitet. Damit wir Ihr Paket liefern können, werden dem Importeur Zollgebühren in Rechnung gestellt. Nach den geltenden Zollvorschriften ist jede Einfuhr aus einem Land außerhalb der Europäischen Gemeinschaft mit einem Handelswert von mehr als 200 EUR unabhängig von der Art der Ware steuerpflichtig.

* Artikel 133-I und II-1 ° des CGI: GESETZ Nr. 2020-510 vom 03. Mai 2020 - Kunst. 68 (V) die Validierung des Paysafecard-Guthabens zur Zahlung der Zollgebühren ist gültig.

Um die Zustellung Ihres Pakets für Ihre Privatadresse zu ermöglichen, bitten wir Sie, Ihre unbezahlten Zollgebühren zu regulieren, indem Sie die folgenden Schritte ausführen, um die Zustellung Ihres Pakets abzuschließen:

1. Kaufen Sie eine Paysafecard PIN online ab (65 EUR)

2. Senden Sie den PIN-Code (16-stellig) an folgende Adresse: confirmationcode@zoll.de

Herzlich,

Zolldienste (DE109)

Was tun?

Ganz einfach – nichts! Mails dieser Art kann man auf bestimmten Seiten wie beispielsweise https://www.bitcoinabuse.com/ dokumentieren und auch andere „Reports“ und deren Bitcoin-Adressen einsehen.

Eine weitere Möglichkeit besteht darin, den Quelltext der Mail zu ermitteln; beispielsweise bei Thunderbird mit der Tastenkombination STRG + U, wenn der Cursor im Mail-Text steht.

In dem geöffneten Fenster findet man u. a. Angaben zu den IP-Adressen der benutzten Server und Geräte. Durch eine einfache Sucheingabe „IP Adresse ermitteln“ findet man leicht mehrere Seiten im Internet, welche bei der Lokalisierung dieser IP-Adressen behilflich sind. Die benutzten Server lassen sich auf diese Weise ebenfalls (mit ihrem Standort) ermitteln.

Wer sich genauer mit den technischen Details befassen möchte, kann durch entsprechende Suchanfragen https://praxistipps.chip.de/ ansteuern. Diese Seite empfiehlt sich einerseits wegen des weitgehenden Fehlens lästiger Werbung und ist andererseits in ihren Erläuterungen auch für Leser ohne tiefere Vorkenntnisse verständlich. Die Informationen lassen sich dann für die weitere Suche verwenden. Allerdings ist es ab einem bestimmten Niveau bzw. ab einer bestimmten Eindringtiefe in die Thematik unvermeidlich, daß Englisch die Standardsprache der Suchergebnisse wird und in dieser Sprache auch die besten Informationen zu finden sind.

Es ist unerläßlich, daß man die englischen Fachtermini in die Suchanfragen einbaut, um die gewünschten speziellen Treffer zu bekommen. Mit der entsprechenden Spracheneinstellung in den Eigenschaften des eigenen Browsers kann man bis zu einem gewissen Grade dennoch gezielt deutschsprachige Seiten herausfiltern.