Spam, Phishing & Co

Guido Bunsen

„Sicher“ unterwegs im Internet

Du musst deinen Feind kennen, um ihn besiegen zu können.

Sunzi, chinesischer Philosoph und Stratege, ca. 500 vor Christus in der Zeit des Königreichs von Wau (Die Kunst des Krieges. Hrsg: Clavell, J., München 1988)

Angriffsziele

Geld, Passworte, Kontrolle des Rechners

- Vermeintliche Anlagetipps
- Regierungsnahe Person, hoher Militär, Witwe von … hat X Mio. $ und kommt alleine nicht an das Geld.
- Das Konto (E-Mail, Cloud-Dienst, Bank, Paketdienst, …) läuft ab …
- Anhang der E-Mail, oder Webseite enthält Schadsoftware

Beispiel E-Mail

From: "Rosana K. Batista"<anower@nzgroupbd.com>
To: Undisclosed recipients:;
Date: Tue, 12 Jan 2016 22:15:44 -0800
Message-ID: <6504fe2c02bc474f9d2da9ef42cc6a2a@rwthex-w2-a.rwth-ad.de>
Return-Path: anower@nzgroupbd.com
Subject: Purchase Order #P77868 11-1-2016

Hi,

Please find attached our Purchase Order. Confirm price and availability.
(PLZ SHIP TODAY)
Advise tracking number and Invoice as soon as you get it.
Any comments please contact me.
Would like to thank you for your friendship, support & business throughout 2015.
It has been a pleasure working with you !

Rosana K. Batista
Purchasing Department
cid:image001.jpg@01CC5085.C5D2A2D0
Aviation Parts Executive Inc.
1170 NW 51st St.
Fort Lauderdale, Florida 33309
PH (954)493-5018 EXT. 120
FAX (954)493-6519

Website: www.aviationpartsinc.com

Der Anhang mit PDF-Dokument fragt nach PW

Merkmale einer Phishing-Mail

- Grammatik- und Orthografie-Fehler
- Mails in fremder Sprache
- Fehlender Name
- Dringender Handlungsbedarf
- Eingabe von Daten
- Aufforderung zur Öffnung einer Datei
- Links oder eingefügte Formulare
- Bisher noch nie E-Mails von der Bank erhalten oder k
- Mailheader

- Quelle: https://www.verbraucherzentrale.nrw/link1129939A.html

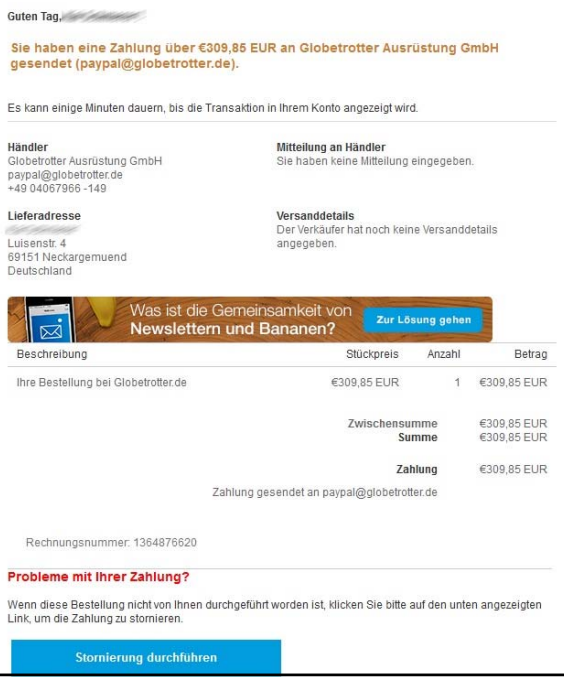
Wirksame Abwehrmaßnahmen

- Sicherheitsbewusstsein / Awareness
- Aktueller Virenscanner
- Aktuelle Updates (Betriebssystem, Anwendungssoftware wie z.B. Java, Adobe)

- Spam- und Virenfilter für E-Mails am Hochschuleingang

- Surfen über den Web-Filter (https://doc.itc.rwth-aachen.de/display/Proxy)

Beispiel 2



Guten Tag,

Sie haben eine Zahlung über €309,85 EUR an Globetrotter Ausrüstung GmbH gesendet (paypal@globetrotter.de).

Es kann einige Minuten dauern, bis die Transaktion in Ihrem Konto angezeigt wird.

Händler
Globetrotter Ausrüstung GmbH
paypal@globetrotter.de
+49 04067966 -149

Mitteilung an Händler
Sie haben keine Mitteilung eingegeben.

Lieferadresse
Luisenstr. 4
69151 Neckargemuend
Deutschland

Versanddetails
Der Verkäufer hat noch keine Versanddetails angegeben.

Beschreibung	Stückpreis	Anzahl	Betrag
Ihre Bestellung bei Globetrotter.de	€309,85 EUR	1	€309,85 EUR

Zwischensumme €309,85 EUR
Summe €309,85 EUR

Zahlung €309,85 EUR

Zahlung gesendet an paypal@globetrotter.de

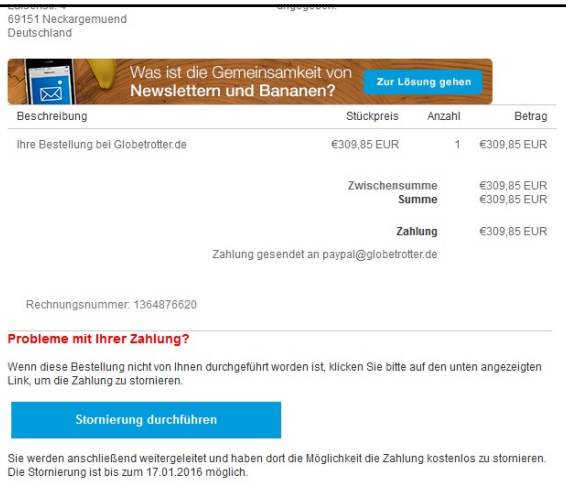
Rechnungsnummer: 1364876620

Probleme mit Ihrer Zahlung?

Wenn diese Bestellung nicht von Ihnen durchgeführt worden ist, klicken Sie bitte auf den unten angezeigten Link, um die Zahlung zu stornieren.

Stornierung durchführen

Beispiel 2



69151 Neckargemuend
Deutschland

Beschreibung	Stückpreis	Anzahl	Betrag
Ihre Bestellung bei Globetrotter.de	€309,85 EUR	1	€309,85 EUR

Zwischensumme €309,85 EUR
Summe €309,85 EUR

Zahlung €309,85 EUR

Zahlung gesendet an paypal@globetrotter.de

Rechnungsnummer: 1364876620

Probleme mit Ihrer Zahlung?

Wenn diese Bestellung nicht von Ihnen durchgeführt worden ist, klicken Sie bitte auf den unten angezeigten Link, um die Zahlung zu stornieren.

Stornierung durchführen

Sie werden anschließend weitergeleitet und haben dort die Möglichkeit die Zahlung kostenlos zu stornieren.
Die Stornierung ist bis zum 17.01.2016 möglich.

Der Aufwand für den Angreifer ist deutlich höher
Quelle: zdnet.de, silicon.de

HRK zum Thema IT-Sicherheit

HRK Hochschulrektorenkonferenz
Die Stimme der Hochschulen

Rundschreiben zum Thema IT-Sicherheit der HRK im Okt. 2014 an alle Rektoren

„ … So kommt es zum Beispiel seit geraumer Zeit zu massiven Angriffen ausländischer Nachrichtendienste auf die internen informationstechnischen Systeme wissenschaftlicher Einrichtungen mit allen dort vorhandenen Daten. Dabei sind nicht nur Institute der Hochtechnologie, sondern auch geisteswissenschaftliche Einrichtungen betroffen. …“

Professor Dr. Dr.h.c. Horst Hippler, Präsident der Hochschulrektorenkonferenz

Weitere Merkmale

- Vorab umfangreiche Recherchen zum sozialen Umfeld des „Targets“
- Aufwändige Phishing-E-Mails
  - Spezielle „passende“ Absenderdomains
  - Inhalt oder Anfrage zu konkreten Forschungsinhalten mit Bezug zum Empfänger
  - Schadsoftware die noch unbekannte Sicherheitslücken ausnutzt (Zero-Day-Exploits)
- Häufung von Aktivitäten vor Internationalen Konferenzen
- „Politikberater“
- Auch Geisteswissenschaften oder Landwirtschaftliche Fakultäten sind betroffen
- „… nicht nur Institute der Hochtechnologie“

Zusammenfassung

- Kenne Deine Gegner
- Vorsicht bei unbekannten Absendern und unerwarteten E-Mails und nicht nur bei diesen
- Aktuelles Betriebssystem mit aktuellen Updates
- Aktueller Virenscanner mit aktuellen Virenmustern
- Surfen über Web-Filter
- Fragen Sie ihren Administrator …
- IT Sicherheit ist ein Orgathema. Sicherheit braucht einen Prozess.

Vielen Dank
für Ihre Aufmerksamkeit