"Passwortklau" (Phishing)

Die derzeit (2024) gefährlichste Form von Internet-Kriminalität ist "Phishing". Das Wort kommt von Englisch "Fishing", also "fischen" oder "angeln". Laut "Bitcom" beträgt der Schaden, den Phishing alleine im Jahr 2022 in Deutschland angerichtet hat, über 200 Milliarden Euro.

Da wichtige Daten heutzutage immer mit Passwörtern geschützt sind, muss man dazu zuerst das Passwort eines Benutzers, der Zugriff hat, ergaunern. Hat man das Passwort, kann man die Daten abgreifen und weiterverkaufen. Bei wichtigen Firmendaten ist es inzwischen üblich, sie zu verschlüsseln, und den Schlüssel nur gegen Lösegeld herauszurücken.

Meistens beginnt der Angriff mit einem Mail, mit einer SMS oder einer Nachricht in einem sozialen Medium. Man wird aufgefordert, auf einen Link zu klicken, oder einen Anhang (Attachment) zu öffnen. Wir wollen uns beide Möglichkeiten getrennt ansehen.

Ziel für einen Phishing-Angriff ist meistens nicht eine bestimmte Person, sondern man sucht nach dem DAU", dem "Dümmsten anzunehmenden User". Die Idee dahinter ist, dass es in den meisten Organisationen viele Mitarbeiter gibt, die Zugang zu wertvollen Daten haben. Es ist also ausreichend, irgendeinen Mitarbeiter hereinzulegen, es ist egal, welchen. Man versendet daher das Phishing-Mail an möglichst viele Mitarbeiter und hofft, dass mindestens einer darauf hereinfällt.

Zuerst wird dann der Computer des "DAU" übernommen, und von dort verbreitet sich der Schädling über das Netzwerkkabel meistens auf die anderen Computer der Firma.

Phishing mit einem Anhang (Attachment, Dateianhang)

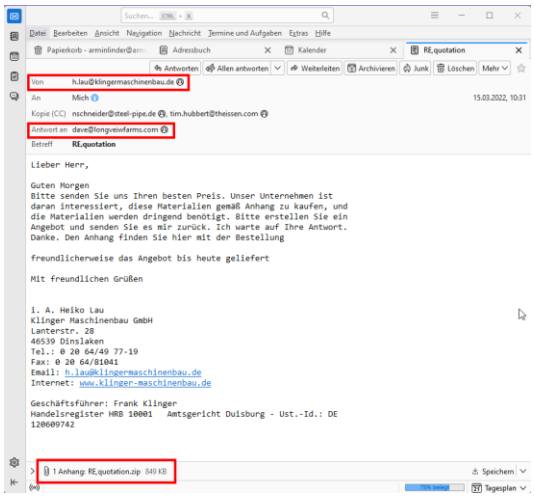
Die Vorbereitung des Tricks besteht darin, eine schädliche Datei zu erstellen. Das ist nicht weiter schwierig, wenn es sich um eine Datei handelt, die ausführbare Programme enthalten kann.

Gefähliche Apps: .vbs, .com, .ps, .exe, .cmd, .bat, .ipa, .oat

Dateien mit diesen Endungen enthalten direkt Apps (Programme), die allein dafür geschaffen wurden, Schaden anzurichten. Es gibt solche Dateien für jedes Betriebssystem. Unter Windows sind vor allem .exe Dateien extrem gefährlich.

Für Windows sind besonders häufig: .vbs, .ps und .exe. Für Apple-Computer .ipa, und für Android-Computer .oat. Das sind einige Bespiele, es gibt noch viele weitere.

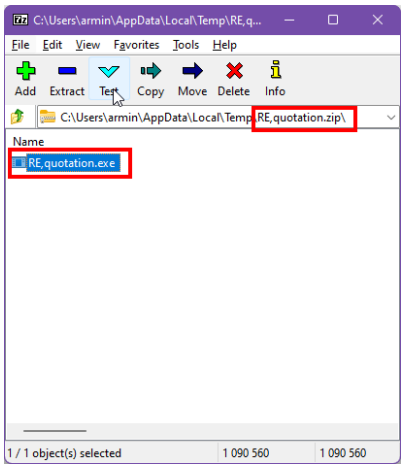
Daneben existieren für jedes Betriebssystem auch noch zahlreiche "Bundle" oder "Container" Formate, in denen man gefährliche Apps verstecken kann. Häufig verwendet werden .zip (alle Betriebssysteme), .msi (Windows), .aab (Android) und .ipcc (Apple).



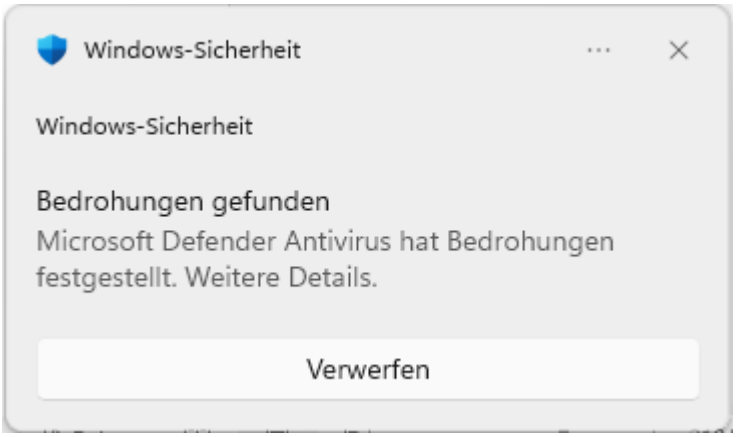
Dieses Phishing-Mail bekam ich am 15.3.2022. Ein bisschen drüber nachdenken hilft. Es kommt also angeblich von einer Firma Klinger Maschinenbau in Dinslaken. Die "von" Adresse ist eigentlich OK, @klingermaschinenbau, aber E-Mail Adressen lassen sich ganz leicht fälschen. Trotzdem ist mir diese Firma völlig unbekannt, warum sollten die bei mir etwas bestellen wollen? Also Vorsicht, und weiter mitdenken. Die Antwort soll an eine andere Firma @loongfeiwfarm gehen. Das macht keinen Sinn, abgesehen davon ist da ein Schreibfehler drinnen, es soll wohl "longviewfarm.com" heißen. Dann kommt der lange Text. Er verspricht mir Geld, man will etwas bei mir kaufen. Dann baut er Druck auf, die Materialien werden dringend benötigt, ich soll nicht lange nachdenken, und den Anhang öffnen. Und dann ist im Textkörper auch noch ein grober Fehler.

Der Anhang besteht aus einer .zip Datei, das ist eine von denen, die oben als "möglicherweise gefährlich" aufgelistet ist. Der Name der Datei macht überhaupt keinen Sinn.

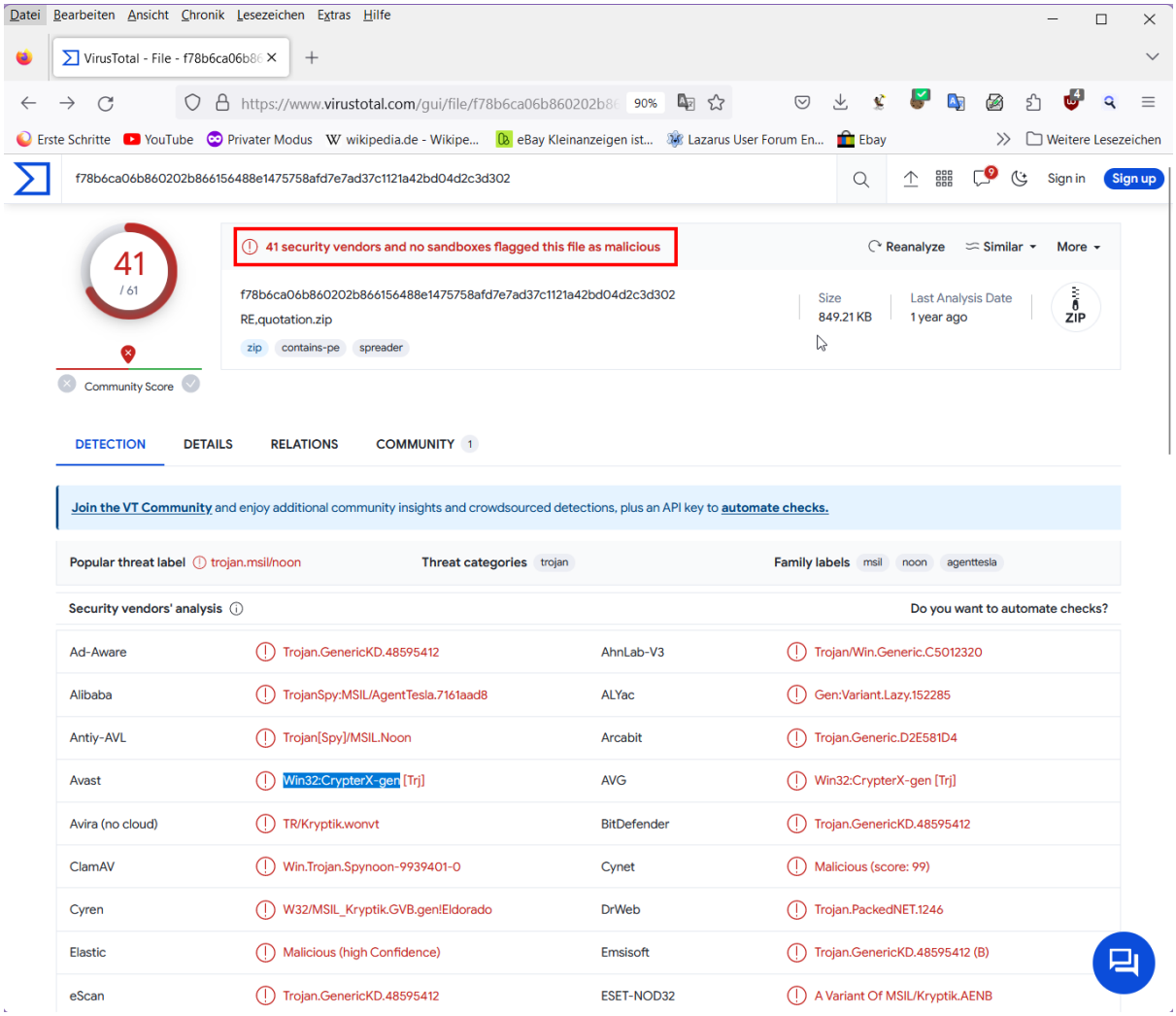
Ich habe sie dann NICHT angeklickt, sondern mit einem speziellen Werkzeug (7-Zip) geöffnet. In ihr versteckt sich eine der als extrem gefährlich bezeichneten .exe Dateien.



Ich führe diese Datei natürlich auf keinen Fall aus, aber ich möchte schon wissen, was sich in ihr versteckt. Ich schicke sie daher zur Untersuchung an einen Online-Virenscanner. Bereits als ich sie aus dem .zip herausnehmen möchte, schlägt der Windows Virenwarner an.



Also enthält die Datei, wie schon vermutet, ein Virus. Um die sie noch genauer zu untersuchen, lade ich die .zip Datei daher bei www.virustotal.com hoch. Das Untersuchungsergebnis kommt sofort, und es ist wie erwartet:



Die Datei ist bei 41 verschiedenen Antiviren-Herstellern als schädlich bekannt. Ich führe sie also auf keinen Fall aus, sondern lösche die infizierte Datei sofort.

Gefährliche Office-Dateien: .doc, .xls, .ppt

Ein verbreitetes Beispiel für gefährliche Dateien sind alle Dateien, die mit Microsoft Office zusammenhängen, weil alle Office-Produkte eine kleine Programmiersprache (Visual Basic for Applications, VBA) enthalten. Die ist eigentlich dafür gedacht, besonders "intelligente" Dokumente zu erstellen. Sie kann aber auch leicht dafür genützt werden, Schaden anzurichten. Die immer noch weit verbreiteten "alten" Office-Dateiformate (.doc, .xls und .ppt) sind im Zweifelsfall gefährlich.

Microsoft hat in den neusten Office-Versionen endlich Maßnahmen ergriffen, das zu unterbinden. Die moderneren Versionen von Word, Excel und Powerpoint (.docx, .xlsx, .pptx) können technisch keinen Programmcode mehr ausführen und sind daher generell nicht gefährlich. Man muss allerdings genau aufpassen: die fast gleich aussehenden Dateien .docm, .xlsm und .pptm können Makros ("Programme" enthalten, und sind daher möglicherweise gefährlich.

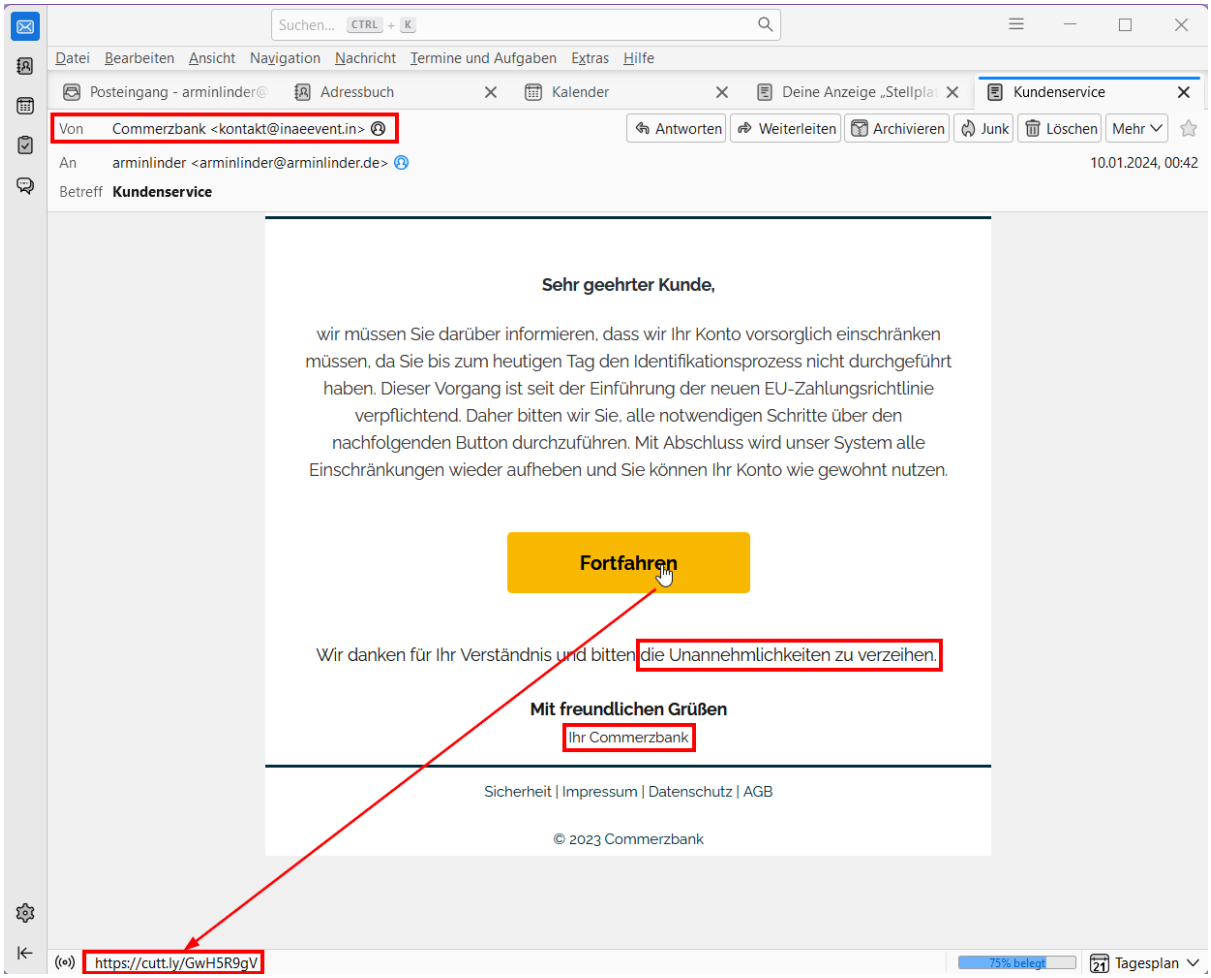
Gefährliche Dokumente: .pdf

.pdf Dateien sind sehr beliebt, aber auch sehr gefährlich, weil auch sie kleine Programme (JavaScript, .js) enthalten können.

Daneben lassen sich in.pdf Dateien praktisch alle oben aufgelisteten gefährlichen Formate einbauen, sowie auch Links zu gefährlichen Webseiten.

Gefährliche Verknüpfungen ("Links")

Am 10.1.2024 bekam ich diese Nachricht. Sie kommt angeblich von einer bekannten Bank (Commerzbank). Wieder wird Druck aufgebaut. Ich habe angeblich etwas falsch gemacht ("den Identifikationsprozess nicht durchgeführt"). Das ist wichtig, es ist eine Vorschrift der EU. Deswegen wird mein Bankkonto eingeschränkt, ich kann z.B. kein Geld mehr abheben. Dann kommt ein Versprechen: ich soll auf den gelben Button klicken, und das Problem lösen. Danach kann ich sofort wieder auf mein Konto zugreifen.



Das mache ich natürlich nicht. In der Regel passieren dann drei Dinge:

- Der kriminelle Absender weiß, dass ich Mails lese, und so doof bin, auf verdächtige Buttons zu klicken. Er verkauft diese Information im Darknet, und ich bekomme noch mehr solche Mails.
- Nach dem Klick bekomme ich meistens (ich habs nicht ausprobiert) entweder eine perfekt gefälschte Kopie der Commerzbank-Internetseite, in die ich meine Konto- und Zugangsdaten eingeben soll. Der kriminelle Angreifer speichert sich diese Daten, und benützt sie, sich auf der richtigen Commerzbank-Seite anzumelden. Oder ich komme auf eine Seite mit Werbung für allerlei wertlose Produkte und dubiose Geldanlagen (meistens irgendwelche Bitcoin-Börsen).

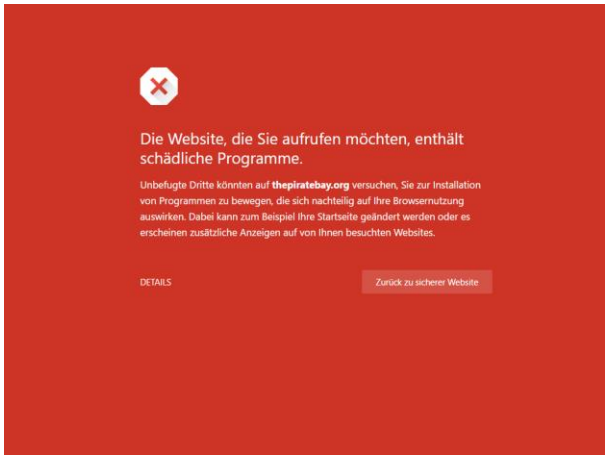
Und, hätte ich erkennen können, dass das Mail eine Fälschung ist? Klar, und es wäre kinderleicht gewesen.

- Im "von" Feld, in dem der Absender steht, steht zwar "Commerzbank", aber die dahinter angegebene E-Mail Adresse kommt ganz sicher nicht von der Commerzbank, sondern von einer unbekannten Firma "inaeevent.it". Wäre die Adresse wirklich von der Commerzbank, dann müsste sie …@commerzbank.de heißen.
- Schiebe ich die Maus über den Button (nicht klicken! Nur den Mauszeiger draufschieben) erscheint links unten die Adresse, zu der ich gelangen würde, wenn ich klicken würde. Ich würde zur Webseite "cutt.ly" geleitet werden, und nicht zur Commerzbank. Deren Webseite ist "commerzbank.de".
- Der Text ist – im Unterschied zu früher – fast fehlerfrei, aber nur fast, er enthält zwei Fehler. Banken bitten nie um Verzeihung, und die korrekte Unterschrift für die Commerzbank wäre "Ihre Commerzbank". Richtige Angestellte der Commerzbank würden keine solchen Fehler machen.
- Solche Mails werden regelmäßig im Namen aller großen Deutschen Banken gesendet, ich habe schon welche gesehen von der Hypovereinsbank, der Deutschen Bank, der Sparkasse, der Targo-Bank und vieler anderer mehr. Banken versenden deswegen NIE solche Mails. Sie rufen an, oder schicken einen Brief per Post. Bei wirklich wichtigen Dingen wird man gebeten, mit einem Ausweis in die Bank zu kommen.
- Und zuletzt: ich habe gar kein Konto bei der Commerzbank 😊

Gefährliche Webseiten: .html, .js

Auch Webseiten (.html) können Programmcode enthalten (JavaScript, .js). Im Web ist die Situation besonders unangenehm, weil das Anzeigen besonders cooler Webseiten, wo viele hübsche Effekte drauf sind, ohne JavaScript gar nicht möglich ist. Man kann JavaScript also nicht einfach ausknipsen.

Um das Surfen im Web für den Anwender so ungefährlich wie möglich zu machen, werden die Browser so gut es geht abgesichert gegen Webseiten, die "bösartige" JavaScript Programme verbreiten.



Wenn eine Webseite dafür bekannt ist, schädliche Programme zu verbreiten, bekommt man eine deutliche Warnung.

Viele bösartige Webseiten versuchen deswegen, den Benutzer dazu zu bringen, die Warnung zu übergehen. Sie behaupten zum Beispiel, dass ein besonders cooles Spiel, das natürlich nichts kostet, nur dann läuft, wenn man die Sicherheitsabfrage wegklickt und weiter die Seite aufruft.