Hoaxe, Malware und CEO-Fraud

Tom Gries | Berlin | Oktober 2023

Dokumenten URL:	http://docs.tx7.de/TT-SE8
Autor:	Tom Gries <TT-SE8@tx7.de>
	@tomo@chaos.social
Lizenz:	Creative Commons BY-NC-ND
Version:	7.0.0 vom 20.10.2023

Hoaxe (Fake News)

Ein Hoax - ursprünglich ein „Jux“ oder „Scherz“ – ist eine Falschmeldung. Der Begriff wird heute nur noch selten verwendet - er ist in den letzten Jahren durch „Fake News“ abgelöst worden.

Einige Beispiele:

1. McDonalds Kaffee
2. Verbrannte Zigarren
3. SULFNBK.EXE (auf den nächsten Seiten)

Hoaxe (Fake News)

Hallo ihr Lieben!

bitte mal Systeme checken... das ist kein Fake oder Scherz! Nach einer Warnung vor einem "schlafenden Virus" habe ich diesen Virus auf meinem Rechner gefunden und jetzt gelöscht - ohne ihn zu öffnen! Er wird wohl von vielen Virenprogrammen nicht erkannt und aktiviert sich zu einem späteren Zeitpunkt.

Er verbreitet sich durch Emails, infiltriert C:\Windows\command und löscht - wenn er sich aktiviert - alle Dateien/Ordner auf der Festplatte.

Ich bitte alle, die in den letzten Monaten von mir eine Mail bekommen haben, ihn zu suchen und ggf. zu löschen. Dabei wie folgt verfahren:

Hoaxe (Fake News)

Ist der Rechner infiziert erscheint die Datei im Ergebnisfeld. AUF KEINEN FALL ÖFFNEN! (durch Doppelklick oder ausführen) sondern wie folgt verfahren:

[…]

Dann auf jeden Fall noch den Papierkorb leeren. Wenn die Datei gefunden wurde, alle Empfänger/Innen von E-Mails der letzten Monate informieren.

Diese Virenwarnung hab ich auch von anderen bekommen. Ich hatte den Virus auch. Also bitte ernst nehmen und weiterleiten.

Habe den Virus eben gelöscht!!!! Unter Garantie habt ihr den auch! Also seht nach. Geht ganz schnell!

Hoaxe (Fake News)

1. Der Adressat wird aufgefordert, die "Warnung" an möglichst viele Menschen weiterzuleiten.

2. Der Betreff enthält etwas reißerisches (z. B. "Virus Warnung").

3. Die Wirkung des Virus wird sehr drastisch dargestellt und beinhaltet Dinge, die ein Computer-Virus gar nicht kann (z.B. Hardware beschädigen).

4. Als Quelle wird gerne eine namhafte Firma oder Organisation genannt, um die Glaubwürdigkeit zu verbessern (a.k.a. False Authority Syndrome). Bei diesen Firmen finden sich jedoch keine Hinweise auf eine solche Warnung.

5. Es wird mit Aktualitätsangaben wie "gestern" oder "am Freitag" gearbeitet, die keinen Bezug zu einem bestimmten Datum haben. Man erkennt so nicht, wie alt die Meldung tatsächlich schon ist.

Hoaxe (Fake News)

Bekannte Malware

Jahr	Name	Wirkung	Schadenshöhe
2017	Wannacry	Ransomware	
2010	Stuxnet	Vermutlich zur Spionage (genauer Zweck bis heute unbekannt). Es waren überwiegend iranische Industrieanlagen betroffen.	
2004	Sasser	Nutzte Sicherheitslücke in XP aus. Befallene Rechner schalteten sich in unregelmäßigen Abständen aus. Ein 17-jähriger aus Niedersachsen.	
2003	SQL_Slammer	Verbreitete sich innerhalb von 10 Minuten auf mehr als 70.000 Rechner. Nutzte eine Sicherheitslücke des MS SQL Servers.	
2001	Nimda	Weltweite Verbreitung innerhalb von 22 Minuten. Versendete sich selbst an alle Outlook Kontakte.	590 Mio. USD
2001	Code Red	Kaperte Computer und missbrauchte diese für Angriffe.	2,6 Mrd. USD
2000	I love you (Lovebug)	Email-Wurm. Überlastete Mailserver. Anhang sah aus wie eine Textdatei.	10 Mrd. USD
1999	Melissa	Versendete sich selbst an Outlook Kontakte.	1,1 Mrd. USD

CEO-Fraud (Fake President Fraud)

CEO-Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden. Den CEO-Fraud gibt es schon länger. Einen ähnlichen Hack hat Kevin Mitnick bereits 1992 angewandt, um sich den MicroTac Source Code von Motorola zu beschaffen.

Anruf bei Alicia von Motorola: "Hi Alicia, ich wollte eigentlich Pam anrufen, aber sie scheint schon im Urlaub zu sein. Das ist sehr ärgerlich, sie hatte doch vergangene Woche versprochen, mir noch den Source Code des MicroTac Ultra Light bereitzustellen. Kannst du mir helfen?"

Das Besondere an dieser Masche ist, dass die Täter sehr gut vorbereitet sind und ein ganz bestimmtes Ziel im Auge haben.

CEO-Fraud (Fake President Fraud)

Die Täter kundschaften ihr Ziel im Vornherein genau aus. Über Soziale Medien, wie Xing, LinkedIn, Facebook und Co. lassen sich besonders gut personenbezogene Daten herausfinden. Die Täter wissen ganz genau, wen sie am besten kontaktieren, um die größten Chancen auf eine schnelle Überweisung zu haben.

Ein bekanntes Beispiel für einen erfolgreichen CEO-Fraud liefert die **Firma LEONI**. 40 Millionen Euro erbeuteten sich die Täter über "betrügerischer Handlungen unter Verwendung gefälschter Dokumente und Identitäten sowie Nutzung elektronischer Kommunikationswege".

Die meisten Angriffe dieser Art werden mit gefälschten Emails durchgeführt. Wie das geht, haben wir bereits gesehen.

Anmerkungen oder Fragen?