# Schurkenstaaten-Hacker aus der Sicht der Cybercommander

Ich schreibe hier nicht „hacker behind monitors hacks servers, cyber security“ und den Namen einer Agentur, die so ein Foto verkauft hat, sondern die Billigversion, die sogar besser ist und von mir stammt: „ransomware computer malware –ar 16:9 –chaos 100 –s 750“

Die Jerusalem Post schreibt über pöhse Schurkenstaaten, die was mit cyber machen: „Rogue states using fake GPT content to hack governments – ex-IDF cyber chief – Former IDF Unit 8200 cyber commander says that all cyber attacks and defenses are getting better with AI.“ Das hört sich natürlich spannend an, zumal wenn es mit „exclusive“ gelabelt ist.

Wie funktioniert das? Die „Hacker“ schießen mit der Schrotflinte aka Ransomware und hoffen, dass sie irgendwas treffen. *„According to public information, around 10%-15% of hacked victim companies pay the ransom,” when hacked with ransomware, while „some give up on the data and some get the data back using backups.“*

Wait a minute. Warum zahlt überhaupt irgendjemand etwas? Weil sie kein Backup haben? Kann mir das jemand erklären?

Jetzt haben wir onlinedurchsuchungsähnlich die zentrale Frage: Wie kommt die Malware auf einen Rechner?

*Ransomware almost always starts with a human factor. You get a 'phishing' email which looks very reliable. You open the link and they send in the ransomware. Phishing has gotten much more personalized.“ – „It includes the correct person's name and job title using a phishing auto-generated tool, and from GPT and other tools.*

Wait a minute again. E-Mails werden nicht verschlüsselt, sondern als Postkarte geschrieben? So was beantworte ich gar nicht. Ist doch ganz einfach. Und Mails, die mich nicht persönlich anreden, schreddere ich sofort – das ist alles zu 100 Prozent Spam. Ich beurteile doch Post nicht phänotypisch, ob die *reliable* ist. Kennt übrigens jemand noch KorrNews, mit dem man in Kombination mit Hamster im Header herumpfuschen konnte? (Chor im Hintergrund singt den Refrain in Fis-Moll: Usenet! Usenet! Usenet!)

Dann die Pointe des Ex-Cybercommanders, die niemand erwartet: Man klickt auf einen Link *and they send in the ransomware*. So einfach ist das also. Was ist aber mit den Muttern und Clawsmailern? Die dürfen beim Phishing nicht mitspielen, weil ihre Software das nicht erlaubt.

Ich habe mich ein bisschen umgeschaut: Linux ist nicht davor gefeit. Aber: *Der Systemzugang erfolgt über ein ZIP-Archiv, das eine bösartige Java-Image-Datei enthält.* Ein Attachment also, das man erst entzippen müsste. (Wer verschickt denn heute noch zip-Dateien?) Und dann Remote. Wenn ich aber mit der Schrotflinte schieße, woher kenne ich das Betriebssystem des zufälligen dümmsten anzunehmenden Opfers?

Ich schrieb 2010: „Werbemails sind ein lukratives Geschäft. Obwohl man einen Bedarf nicht unbedingt erkennen kann, wenn wahllos allen Menschen, die jemals eine E-Mail-Adresse irgendwo im Internet veröffentlicht haben, angeboten wird, ihren Penis zu verlängern, auch wenn sie zufällig weiblich sind – das Geschäftsmodell funktioniert. Es lebt jedoch nicht von einer Krankheit, einem Lebensgefühl oder einer Sucht wie

bei psychotropen Substanzen, sondern ausschließlich von der Dummheit vieler Internetnutzer. Zahlreiche empirische Studien wie etwa die der Anti-Abuse Working Group haben belegt, dass rund die Hälfte aller Nutzer Spam-Mails öffnen, häufig unter Missachtung der einfachsten Sicherheitsregeln.“

Was uns der Ex-Cyberkommandant sagen will: Die KI kann helfen, fehlerfreie E-Mails zu schreiben. Der Rest bleibt wie vorher. Man schreibt also nicht mehr: „Dies ist zu informieren, dass Sie Ihre E-Mail-Adresse beigefügt Zu einem Ticket-Nummer (SP338-634) gewann den Preis Sum Von 750.000,00 (Sieben hundertfünfzigtausend nur) Gewinnspiel in einer E-Mail-Programm am 31. März. 2008.“ Sondern:
*ChatGPT: Gerne, hier ist der korrigierte Satz: „Ich möchte Sie darüber informieren, dass Ihre E-Mail-Adresse mit der Ticket-Nummer SP338-634 den Preis in Höhe von 750.000,00 (siebenhundertfünfzigtausend) in einem E-Mail-Gewinnspiel am 31. März 2008 gewonnen hat.“*

Also bei elektronischen Postkarten immer schön aufpassen! Zu Risiken und Nebenwirkungen fragen Sie Ihren Cyberkommandanten.

ransomware computer malware –ar 16:9 –chaos 100 –s 750