

WERDEN WIR BALD EIN CYBERCRIME-UNICORN SEHEN?

Auf der Jagd nach dem ersten, illegalen Milliarden-Dollar-Tech-Startup



Zunächst einmal, was ist ein Tech-"Unicorn"?

Ein Unicorn ist ein nicht börsennotiertes Privatunternehmen, das auf mehr als eine Milliarde Dollar geschätzt wird.

Okay, einige dieser cyberkriminellen Banden machen richtig viel Geld.

Uber receipt \$44.32
Ransomware \$300

Ich begann mich zu Fragen, ob es in der Tat Cybercrime-Unicorns gibt.

Mit Malware wird bereits seit langer Zeit Geld verdient. Doch nun ist es anders, dank Bitcoin! So kommen Kriminelle auch an ihr Geld, ohne ihre Identität preiszugeben.

Aber es gibt eine Wendung...

Bitcoin-Register sind öffentlich. Wir können sehen, wie viel Geld bewegt wird. Aber wir wissen nicht, wer es bewegt.

Bitcoin-Register sind öffentlich. Wir können sehen, wie viel Geld bewegt wird. Aber wir wissen nicht, wer es bewegt.

Jedem Ransomware-Opfer wird eine eindeutige Bitcoin-Wallet zugewiesen, was sehr clever ist: Eine der größten Gruppen transferierte das Geld immer an eine zentrale Wallet.

Jedem Ransomware-Opfer wird eine eindeutige Bitcoin-Wallet zugewiesen, was sehr clever ist: Eine der größten Gruppen transferierte das Geld immer an eine zentrale Wallet.

So werden schließlich Hunderte von Millionen steuerfreier Gewinne bald dazu führen.

DAS ERSTE CYBERCRIME-UNICORN

So einfach ist es aber nicht.

Einen Ausstieg zu finden ist aber für Kriminelle nicht einfach. Sie werden niemals an die Börse gehen.

Und es ist nicht ganz einfach, an das Geld zu kommen, ohne erwischt zu werden.

Die Akteure kaufen Prepaid-Karten und verkaufen sie dann auf Ebay.

Und dann gibt es noch Online-Poker...

Sie spielen, um zu verlieren... an Mitglieder ihrer Bande.

So begannen sie Bots zu verwenden, die realistisch spielten und dennoch verloren, aber nicht so offensichtlich.

Aber die Pokerseiten greifen ein.

Warum können wir sie nicht aufhalten?

Unsere Sicherheit ist sehr effizient, aber wir können nicht einfach alles aus dem Internet blocken.

AKTIVIEREN SIE KEINE MAKROS!

Deswegen müssen User nach wie vor geschult werden.

Prävention bedeutet auch, Backups richtig zu erstellen, damit eine Wiederherstellung möglich ist, selbst wenn das Schlimmste passiert.