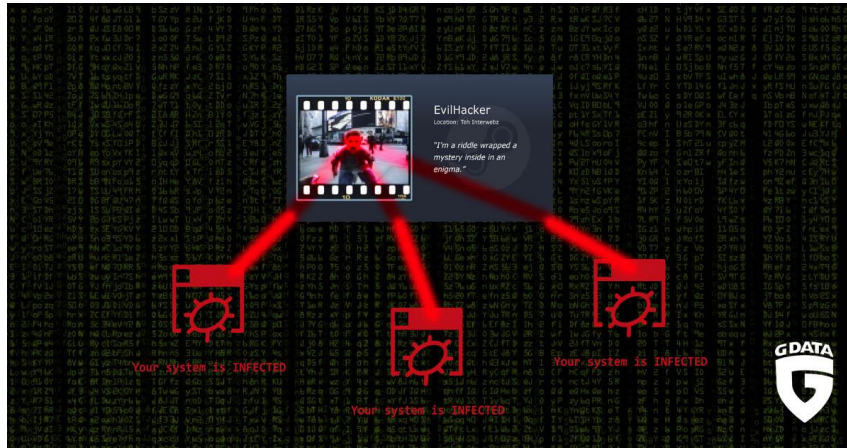


Neue Bedrohung: Malware per Steam-Profilbild

Bochum (Deutschland), 09. Juni 2021

Eine neu entdeckte Art der Malware-Verteilung nutzt Profilbilder auf der beliebten Spiele-Plattform „Steam“. Der schädliche Code ist in den Bilddateien versteckt und wird von einem anderen Schadprogramm entschlüsselt und geladen.



Dass sich Schadsoftware in Bilddateien verstecken lässt, ist nichts Neues – doch dass eine öffentliche Spiele-Plattform wie Steam effektiv als Downloadserver missbraucht wird, hat zumindest G DATA Malware-Analyst Karsten Hahn in dieser Form auch noch nicht gesehen. Zwar wird diese Art der Malwareverteilung bisher nicht aktiv genutzt, aber es ist offensichtlich, dass Kriminelle derzeit aktiv an der Methode arbeiten und diese verfeinern.

„Steam ist eine beliebte Spiele-Plattform mit einer riesigen Anzahl an Accounts. Die manipulierten Profilbilder sind zwar bereits auf Steam zu finden, die Downloader befinden sich aber noch in einer Testphase. Es ist nur eine Frage der Zeit, bis die Malware auch aktiv eingesetzt wird. Für Steam ist es schwierig, derartig manipulierte Bilder ausfindig zu machen“, sagt Karsten Hahn, Malware Analyst bei G DATA CyberDefense AG.

Dabei muss ein Nutzer noch nicht einmal Steam oder irgendeine andere Spiele-Plattform installiert haben oder dort ein Konto besitzen. Sobald der passende Downloader, der sich etwa in einem Mailanhang verbergen kann, gestartet wird, lädt er die Bilddatei herunter und extrahiert den darin versteckten Schadcode.

Diese Methode hat für Kriminelle einige Vorteile, da sie auf diesem Weg ihren Schadcode schnell und effektiv bereitstellen können. Für Nutzer macht es keinen großen Unterschied – sie können sich weiterhin zum Beispiel durch Vorsicht und Skepsis im Umgang mit Dateianhängen vor Schadsoftware schützen.

Mehr Informationen und technische Details finden sich im englischsprachigen Beitrag auf dem G DATA TechBlog: <https://www.gdatasoftware.com/blog/steamhide-malware-in-profile-images>

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299