

# FortiNet Overblocking bei Chocolatey

FortiNet neigt zu False Positives was Chocolatey angeht.

Trifft mal die nuspec des chocolatey Pakets, mal das [install.ps1](#) - wer weiß was da noch kommt. Zum Glück gibts ein live URL Rating, das zwar Ewigkeiten braucht, aber immerhin animierte Ladebalken hat. Auf den Timer ist kein Verlass.

Verdammte Schlangenölsoftware.

## Funktionsumfang ist nicht eingeschränkt

Für normale Paketupdates ist der Funktionsumfang nicht eingeschränkt, üblicherweise trifftts keine Pakete, sondern nur Chocolatey selbst.

Sprich: Chocolatey wird sich nicht selbst aktualisieren können, wohl aber all die Pakete, die man schon drin hat.

Nice to know für die choco-upgrade-all-at\* Pakete. Wollte ich so halt mal für alle aufgeschrieben haben.

Immer wenn ich irgendeinen Schlangenölsoftwarenamen in Google eintippe, dann ist der erste Vorschlag "... false positive" oder "...rerating" ☐ - Google kennt mich.

Die AV-Hersteller sind es derart gewöhnt solche fluten an False-Positive Mails zu erhalten dass man das sicher irgendwie social engineeren kann. Hat das wer schon mal probiert? Einfach die eigene Ransomware als False Positive bei ein paar AV-Herstellern melden?

---

Version #4

Erstellt: 2022-05-11 06:18:59 UTC von Konstantin

Zuletzt aktualisiert: 2022-05-11 06:51:50 UTC von Konstantin