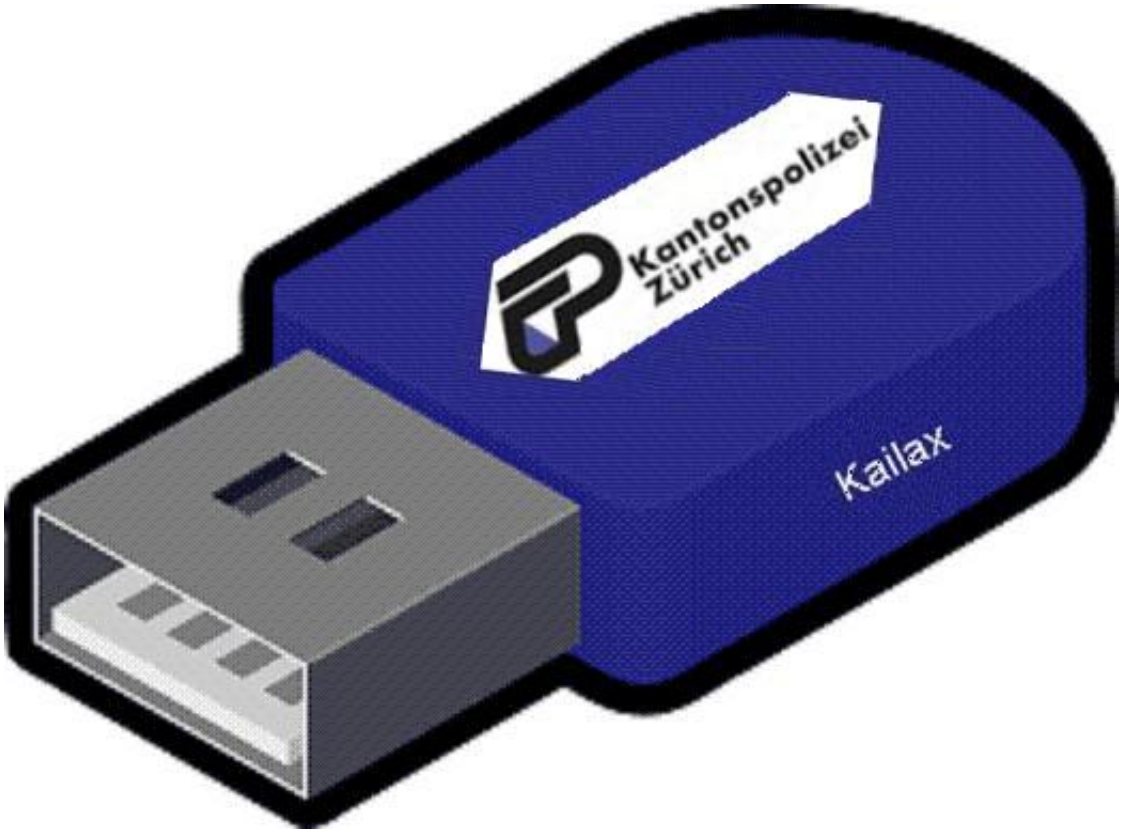
Kailax Unlocker in Zürich

1. März 2017

Der «Kailax Unlocker» ist ein USB-Stick, der unbemerkt Windows-Computer infizieren kann (Windows Vista 7, 8, 8.1 oder Windows Server 2008 resp. Server 2012, 32 und 64-bit). Auf einem infizierten Computer kann beliebige Software installiert und ausgeführt werden.

Über Kailax ist nur wenig bekannt. Die Website www.kailax.com umfasst lediglich die Geschäftsadresse des Unternehmens (eine Adresse in Singapur). Nach Angaben des Herstellers, der sich in E-Mails abwechselnd Max und Nir Levy nennt, wird der «Kailax Unlocker» in siebzig Ländern eingesetzt. Das Holländische Büro Jansen & Janssen verfolgte den Ursprung des «Kailax Unlockers» und der Personen Max und Nir Levy durch eine Analyse von Domain-Namen. Der «Kailax Unlocker» scheint israelischen Ursprungs zu sein. Nir (Max) Levy gehörte dem israelischen Geheimdienst an und arbeitet jetzt für das Unternehmen Mhyli.



Aus WikiLeaks-Dokumenten ist ersichtlich, dass das italienische «Hacking Team» Interesse zeigte, den «Kailax Unlocker» in sein Sortiment aufzunehmen. Die Kommunikation von «Hacking Team» und Max / Nir Levy zeigt, dass der «Kailax Unlocker» als Black Box daherkommt. Käufer wissen nicht, wie er funktioniert und was er mit Servern in Israel kommuniziert.

Bernhard Weder von der Kantonspolizei Zürich machte nach dem Kauf des «Remote Controlled System» die Firma «Hacking Team» in einem Mail auf «Kailax Unlocker» aufmerksam. Offenbar hatte die Kantonspolizei Zürich den «Kailax Unlocker» bereits vor dem Jahr 2015 erworben und

getestet. Weder im Protokoll des Regierungsrates des Kantons Zürich (Sitzung vom 2. September 2015, Interpellation Nr. 199 der Kantonsräte Markus Bischoff, Beat Bloch und Jörg Mäder betreffend Staatstrojaner) noch im Bericht der Geschäftsprüfungskommission vom 19. Mai 2106 zur Beschaffung und den Einsatz von «GovWare» kommt der «Kailax Unlocker» auch nur mit einer Silbe vor.

Es ist gut möglich, dass die Kantonspolizei Zürich beim Evaluieren eines Trojaners auf den «Kailax Unlocker» gestossen ist, er wird z. B. von Gamma Group verwendet. Der «Kailax Unlocker» kann auch verwendet werden, um selbst geschriebene Programme auf einen fremden Rechner zu laden. Es ist daher möglich, dass der «Kailax Unlocker» immer noch von der Kantonspolizei Zürich eingesetzt wird. Auf jeden Fall hätten die Antwort des Regierungsrats auf die Interpellation und der Bericht der GPK den «Kailax Unlocker» offenlegen müssen.

Wikileaks Mails