

On the StrongPity Waterhole Attacks Targeting Italian and Belgian Encryption Users

Archived: 2026-04-05 14:20:49 UTC

Thursday 6 October 11:30 - 12:00, Red room

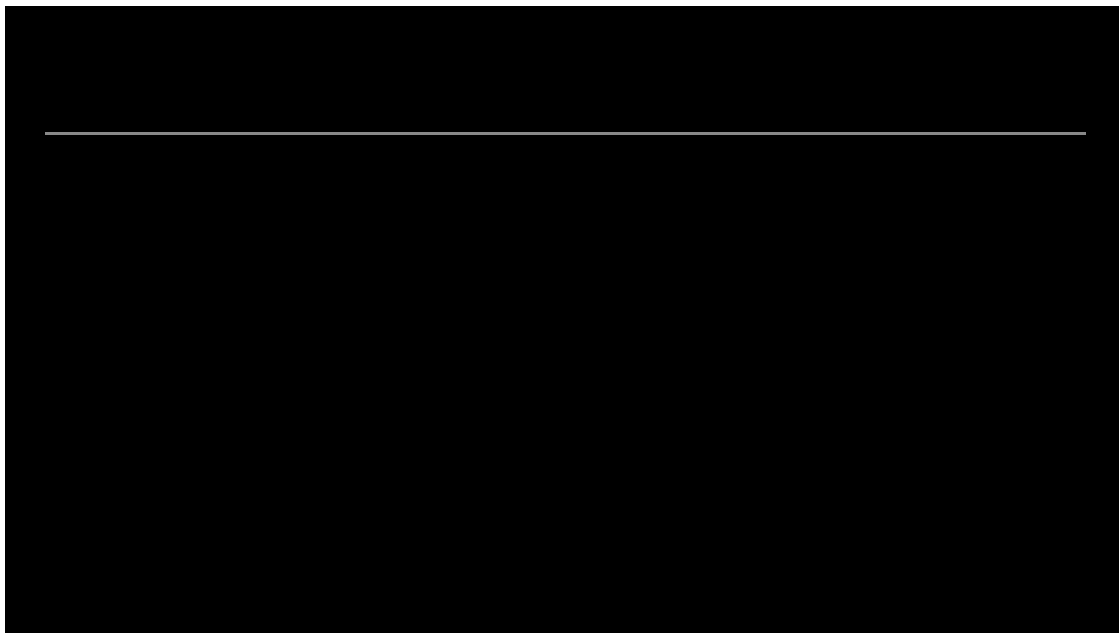
Kurt Baumgartner (Kaspersky Lab)

Encryption has brought with it the promise of self-controlled privacy. And not only have encryption advocates developed effective encryption software and shared it over open source channels, but computer users are taking the time to learn its use and install these software packages in higher numbers than ever.

Along with this increased adoption of encryption technologies came the attention of cyber-espionage actors this summer. Even with what seemed to be a narrow focus, they were willing to attack anyone with an interest in downloading one of a couple of open source encryption installers. Watering holes and poisoned installers are the name of the game here. As with the Darkhotel worms we saw arbitrarily spreading across Asian nations, watering holes affect arbitrary targets as well. In this case, European nations were hit with watering holes affecting large numbers of systems in Italy and Belgium, and other countries as well.

We will describe the watering holes and the time frame of activity, examine how far these attacks reached throughout Europe over the summer, and present some characteristics of the malware used by an actor we call StrongPity.

Click [here for more details about the conference](#).



Source: <https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users>