Cryptokiller Aracı

written by Mert SARICA | 8 September 2015

Geçtiğimiz haftalarda, kullanıcıların ve kurumların oldukça başını ağrıtan Cryptolocker zararlı yazılımı üzerinde çalışırken, işletim sistemine Cryptolocker zararlı yazılımının bulaştığını tespit edip, işlemi (process) durduran Cryptokiller adında bir araç hazırladım.

Windows 7 Enterprise SP1 (x86)'de test ettiğim bu aracı 5 farklı Cryptolocker zararlı yazılımı üzerinde test ettikten sonra yeni bir salgın başlamadan önce herkesin kullanımına sunma kararı aldım.

İlerleyen zamanlarda bu aracı kaynak kodu ile birlikte burada yayınlayacağım. Bu sayede aracı ihtiyaçlarınıza göre iyileştirme/geliştirme imkanınız olacaktır.

Aracın Kısıtları:

1. Cryptokiller aracı, Cryptolocker zararlı yazılımı sisteme bulaşmadan önce sistem üzerinde çalışıyor olması gerekmektedir.
2. Cryptolocker'ı tespit etmek için sistem üzerinde en az bir dosyanın Cryptolocker tarafından şifrelenmesi gerekmektedir.
3. Aracın yönetici yetkisi ile çalıştırılması gerekmektedir.
4. 32 bit Windows işletim sistemi üzerinde çalışmaktadır.
5. Sistem üzerinde Python 2.7 ve Winappdbg modülünün yüklü olması gerekmektedir.

Aracı "hidden" parametresi ile çalıştırdığınız taktirde (cryptokiller.exe hidden) GUI olmadan çalışabilmekte ve gerçekleştirdiği işlemlerlerle ilgili bilgileri C:\Cryptokiller klasörü altına kayıt etmektedir.

Araç ile ilgili gelişmelerden haberdar olmak için https://www.mertsarica.com/cryptokiller adresini ziyaret edebilirsiniz.

Uyarı: Crytokiller, POC olarak geliştirdiğim bir araçtır bu nedenle hataları/eksikleri olabilir. Aracı prototip olarak düşünmeli ve bunu göz önünde bulundurarak kullanmanızı öneririm.

İndir (Windows 7 Enterprise SP1 x86'da test edilmiştir.)

Güncelleme (19.11.2015): Cryptokiller aracının kaynak kodu yayınlanmıştır.

ENGLISH

While I was working on a Cryptolocker malware that targeted Turkish users, I decided to create a POC tool called Cryptokiller (tested on Windows 7 Enterprise SP1 x86) which is able to detect and stop the infection and also kills the infected process. I tested it on 5 different Cryptolocker malwares.

I will share the source code of Cryptokiller soon so you will be able to modify it for your needs.

Limitations:

6. Cryptokiller must be running on the operating system before the infection.
7. Cryptokiller is able to detect & kill the Cryptolocker process after at least one file is encrypted by Cryptolocker.
8. It must be run must under an account with administrator privileges.
9. Supports only 32 bit Windows 7 at the moment.
10. Python 2.7 and Winappdbg module must be installed on the system.

You can run Cryptokiller without GUI by running it with “hidden” parameter. (cryptokiller.exe hidden). You will find the log file inside C:\Cryptokiller folder.

Warning: Cryptokiller is POC tool. It may have bugs/issues so keep in mind.

Download (Tested on Windows 7 Enterprise SP1 x86)

Update (19.11.2015): Source code of Cryptokiller tool released.

POC Video: Cryptokiller vs 5 Cryptolocker Malwares
