DeepSec 2017 Talk: How To Hide Your Browser 0-days: Free Offense And Defense Tips Included – Zoltan Balazs

Posted on **October 09,2017** by **sanna**

There is a famous thought experiment described in the book *A Treatise Concerning the Principles of Human Knowledge*. It deals with the possibility of unperceived existence; for example does a falling tree in the forest make a sound when no one is around to hear it? Given the many reports and mentions about zero-day exploits, the question might be rephrased. Does a zero-day exploit cause any effects when no one is able to detect its presence? Before we completely get lost in philosophy, the question has a real background. Zoltan Balazs wants to address the issue of zero-days in his DeepSec 2017 presentation. The idea seems somewhat contrary to intuition – protecting exploits from being disclosed.

> Zero-day exploits targeting browsers are usually very short-lived. These zero-days are actively gathered and analyzed by security researchers. One example is when Ahmed Mansoor was targeted by an iOS 0-day exploit. The Citizen Lab analyzed the 0-day exploit, and Apple patched the vulnerability within days. Whoever targeted Mansoor, lost a precious 0-day exploit worth hundreds of thousands of dollars.
>
> In my research, I propose a solution for law enforcement, 0-day brokers, and advanced attackers to protect their browser exploits. The key step is to establish key agreement between the exploit server and the victim browser. After a shared key is set up, attackers can encrypt the real exploit with AES. It is recommended to encrypt both the code to trigger the exploit and the shellcode. This idea was first published by me, and quickly adopted by exploit kit developers in-the-wild.

We recommend attending this talk, because it definitely opens a whole lot of questions for discussion, technical and philosophical.

Image not found
http://blog.deepsec.net/wp-content/uploads/2017/09/Zoltan_Balazs_pic_new.jpg

Zoltan (@zh4ck) is the Chief Technology Officer at MRG Effitas, a company focusing on AV testing. Before MRG Effitas, he had worked as an IT Security expert in the financial industry for 5 years and as a senior IT security consultant at one of the Big Four companies for 2 years. His main expertise areas are penetration testing, malware analysis, computer forensics and security monitoring. He released the Zombie Browser Tool that has POC malicious browser extensions for Firefox, Chrome and Safari. He is also the developer of the Hardware Firewall Bypass Kernel Driver (HWFWBypass) and the Sandbox tester tool to test Malware Analysis Sandboxes. He has been invited to give presentations worldwide at information security conferences including DEF CON, Hacker Halted USA, Botconf, AusCERT, Nullcon, Hackcon, Shakacon, OHM, Hacktivity and Ethical Hacking. Zoltan passed OSCE recently, and he is very proud of it.

Posted in:Conference | Tagged:0day,AES,DeepSec,Defence,Talk | With 0 comments