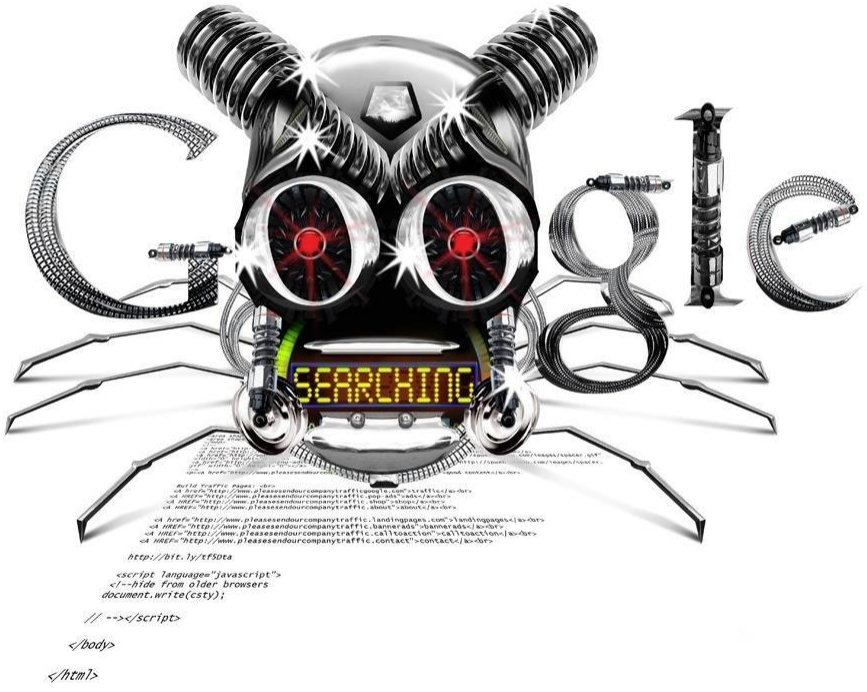
How Zero-Day Exploits Are Bought & Sold

By **occupytheweb** 01/15/2015 10:07 pm



Credits:

Occupytheweb

https://creator.wonderhowto.com/occupythewebotw/

Most of you already know that a zero-day exploit is an exploit that has not yet been revealed to the software vendor or the public. As a result, the vulnerability that enables the exploit hasn't been patched. This means that someone with a zero-day exploit can hack into any system that has that particular configuration or software, giving them free reign to steal information, identities, credit card info, and spy on victims.

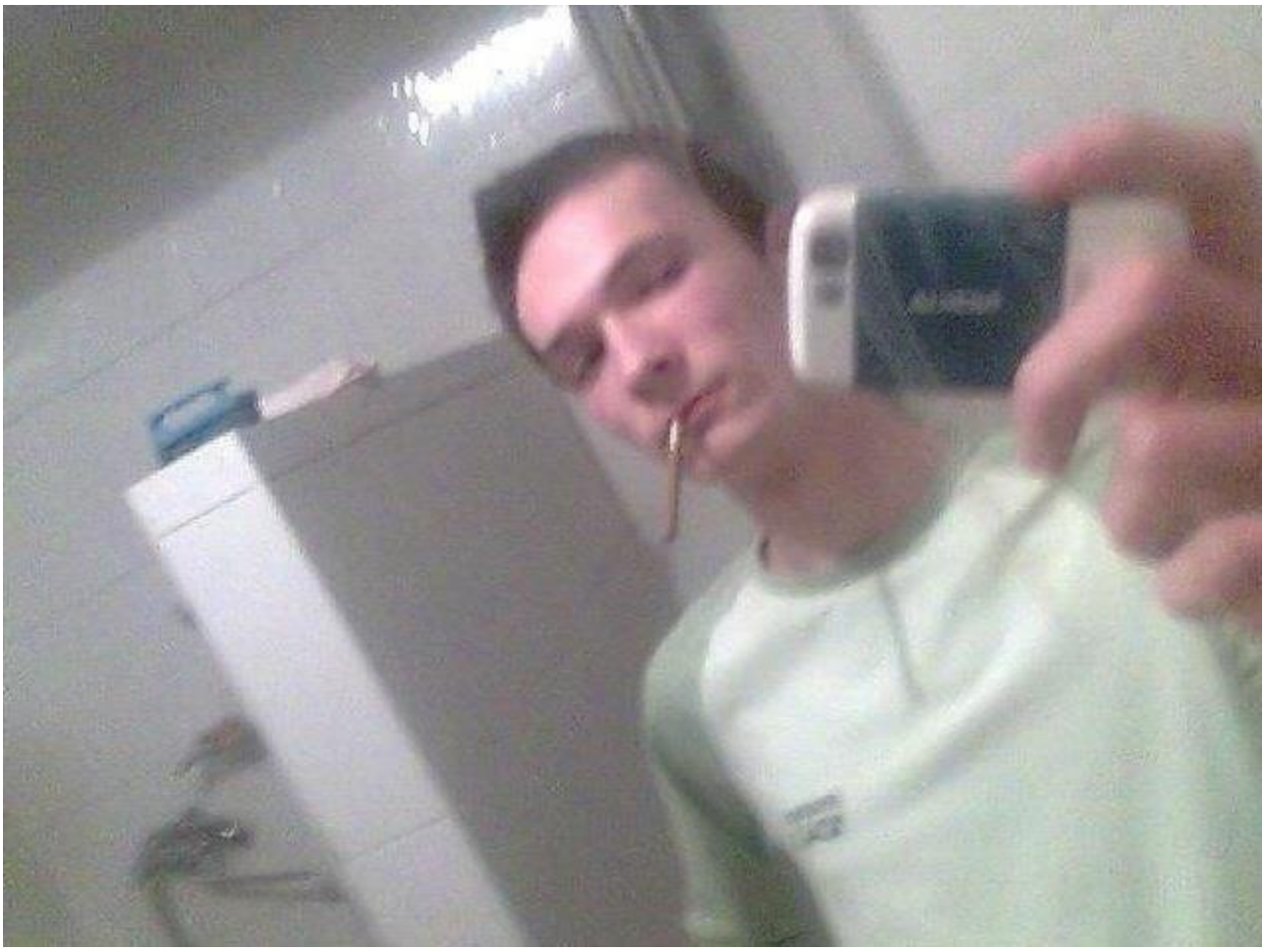
Software Developers

Zero-days may be developed by security researchers and sold to the software developers. Many of these firms have programs to reward researchers for finding flaws in their products. Probably the most generous is Google, who rewarded $150,000 for a successful hack of their Chrome OS at Pwnium. Normal non-competition bounties top out at $15,000 to $20,000. You can see who has won rewards here

For more information on zero-day bounties and their rewards, see my previous guide.

Black Markets

There are a number of black markets where you can buy or sell zero-day exploits. Some of the most active are in Russia. The selfie below is of Andrey Hodirevski, the man believed to run one of the most successful black markets in Russia for zero-days and other exploits.



Andrey Hodirevski, aka Helkern. *Image via Brian Krebs*

Unfortunately, unless you can speak Russian fluently, your chances of completing a transaction there is very low. In order to maintain the safety of these black markets, purveyors will not do business in English or any other language other than Russian.

Speaking and writing that language is the first hurdle you need to overcome to gain their trust. There will be more hurdles, but unless you are a native Russian speaker, you won't get very far. (Believe me, I've tried; for good reason, they are very cautious.)

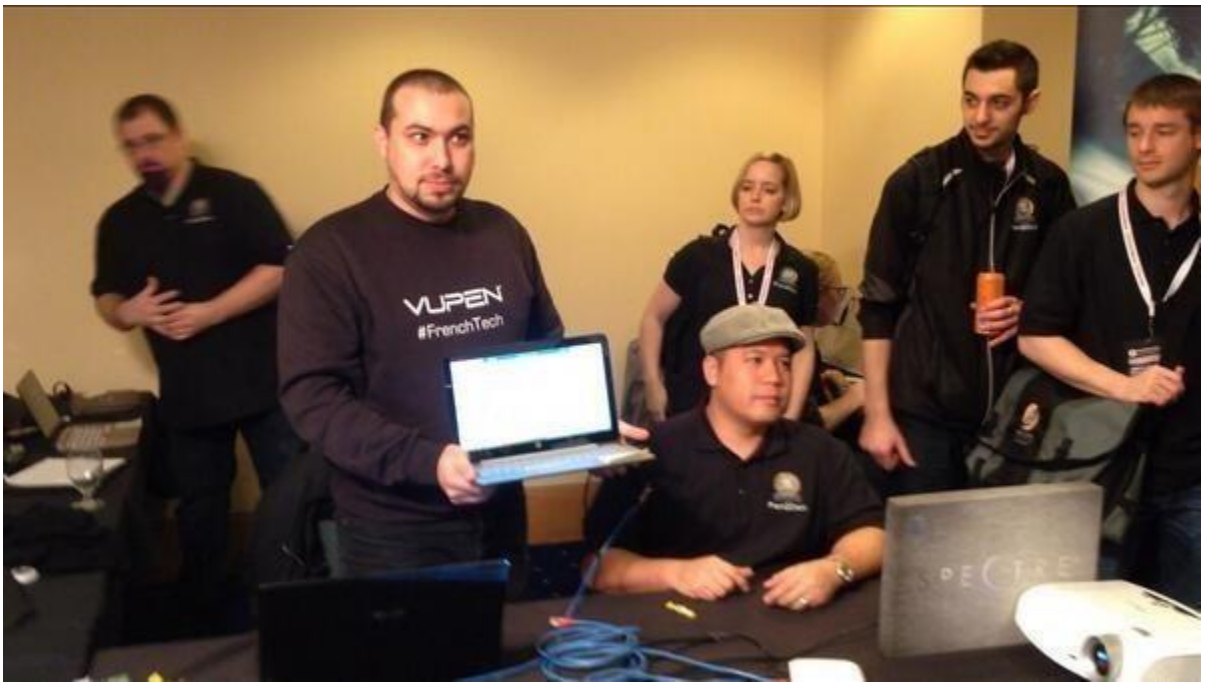
If you can actually get into these markets, zero-day exploits sell for very reasonable prices. Reportedly, the exploit used against Target last year sold for just $1,200.

National Governments

For those of you with advanced skills, or aspiring to advanced skills, there is a highly developed and pricey market for selling zero-day exploits to national militaries and spy

agencies. Of course, they use these for cyber warfare and espionage on each other, and sometimes even their own citizens.

One such firm, Vupen of France, develops and sells zero-day exploits for millions of dollars each. It was recently revealed that Vupen has a contract with the U.S. National Security Agency (NSA) to sell them zero-day exploits. Reportedly, you can't even see their catalog for less than an entry fee of $3M. Now that is tidy business to aspire to.



Vupen pwns Google Chrome at CanSecWest. *Image by Jerome Segura/Twitter*

As cyber security and cyber threats become increasingly important, hacker skills become increasingly valuable. There are now numerous marketplaces, including the software developers themselves, where you can sell your exploits.