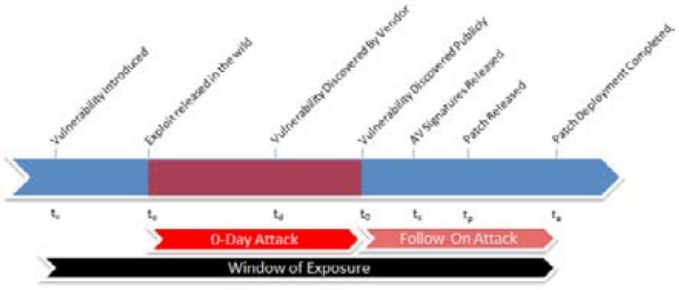
Paolo Passeri

A 0-Day Attack Lasts On Average 10 Months « Hackmageddon.com

(But in some cases may remain unknown for up to 2.5 years). A couple of days ago, two Symantec Researchers have published an interesting article ("Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World") reporting the study of 0-Day Attacks between 2008 and 2001. They have analyzed 300 million files collected by 11 million hosts (a representative subset of the hosts running Symantec products) between March 2008 and February 2011.

These files were extracted from the the WINE environment (Worldwide Intelligence Network Environment, a platform for repeatable data intensive experiments aimed to share comprehensive field data among the research community) and correlated with three additional sources: the Open Source Vulnerability Database (OSVDB), Symantec's Threat Explorer (the company database for the known malware samples) and an additional Symantec data set with dynamic analysis results for malware samples.

The purpose of the research was to execute a sort of automatic forensic analysis aimed to go back in time to look for 0-day attacks carried on during the analyzed period. The results are disarming.



The researchers were able to find 18 vulnerabilities exploited before disclosure, among which 11 were not previously known to have been deployed in 0-day attacks. Based on the data, a typical zero-day attack lasts on average **312 days**, but in some cases may remain unknown for up to **2.5 years** (think to what it means to have the enemy inside the gates for such a long time).

Just to confirm that 0-days are the cradle of targeted attacks, the data show that most zero-day attacks affect few hosts, with the exception of a few high-profile attacks (Do you remember Stuxnet?). Moreover, after vulnerabilities are disclosed, the volume of attacks exploiting them increases by up to **5 orders of magnitude** (the number of variants increases "only" by up to 2 orders).

And this is not a mere coincidence since apparently the cyber criminals watch closely the vulnerability landscape, as exploits for 42% of all vulnerabilities employed are detected in field data **within 30 days** after the disclosure date.

A terribly worrying landscape, even considering a theoretical point of weakness of the research, that is the fact that the sample could be considered self-

consistent referring only to malware strains collected by Symantec customers.

Like this:

Be the first to like this.