Catching the hackers in the act

A BBC article[1]

Summary

Cyber-criminals start attacking servers newly set up online about an hour after they are switched on, suggests research.

About 71 minutes after the servers were set up online, they were visited by automated attack tools that scanned them for weaknesses they could exploit. Once the machines had been found by the bots, they were subjected to a constant assault by the attack tools.

The servers were accessible online for about 170 hours to form a cyber-attack sampling tool. They were given real, public IP addresses and information that announced their presence online. Also, they were configured to superficially resemble a legitimate server. Each one could accept requests for webpages, file transfers and secure networking. The servers' limited responses did not deter the automated attack tools, or bots, that many cyber-thieves use to find potential targets. A wide variety of attack bots probed the servers seeking weaknesses that could be exploited had they been full-blown, production machines.

During the experiment: 17% of the bots were scrapers that sought to suck up all the web content they found, 37% looked for vulnerabilities in web applications the servers might have been running, 10% checked for bugs in web applications the servers might been running, 29% tried to get at user accounts using brute force techniques that tried commonly used passwords, and 7% sought loopholes in the operating system software the servers were supposedly running. These were typical patterns for these automatic bots, they used similar techniques to those that have been seen before and they are a good guide to what organisations should do to avoid falling victim.

Criminals often have different targets in mind when seeking out vulnerable servers, there had been times when a server compromised by a bot was passed on to another criminal gang because it was a bank, government or other high-value target. Once an adversary has got to a certain level in an organisation you have to ask what will they do next?

Opinion

By reading it, I feel more exposed to hackers. I didn't know how persistent they are working because of the automatic process they use. I guess my computer have been attacked for one of those bots, but fortunately I haven't had big problems because of them. From now I will be more careful about them, especially because I've heard about some malicious mails that are in the university's mail platform.

New Words

Thin

Query

Thwart

Sought

phishing

Gangs

seeded

spoof

[1] (September 2, 2017). Catching hackers in the act. BBC News. Technology. Taken from: http://www.bbc.com/news/technology-40850174