PHYS.ORG

Targeted 'malvertising' reveals move towards more sophisticated hacks

October 28 2014, by Eerke Boiten And Julio Hernandez-Castro

Credit: AI-generated image (disclaimer)

At the recent Information Security Solutions Europe conference, former White House cybersecurity adviser Howard Schmidt claimed that most security threats may be persistent, but are not as "advanced" as their common acronym APT (Advanced Persistent Threat) suggests.

In too many cases, Schmidt explained, major security breaches occur because hackers are able to exploit well-known vulnerabilities. These are software flaws that expose security holes, for which manufacturers released a patch to fix the problem – only for IT administrators to fail to act and apply them. It's the equivalent of pushing on an open, unlocked door.

For the vast majority of successful attacks, he is probably right.

Sometimes these security holes are unknown until they are revealed to be the basis of an attack. These so-called zero-day exploits are researched and traded in a global marketplace, through both official channels and the black market. This is estimated at a few hundred exploits per year for some of the largest software vendors, and it can be many months before these are patched.

Unpatched vulnerabilities are a problem for some companies more than others. Microsoft, for example, releases updates every month on "patch Tuesday", while others like Oracle and Cisco release updates less frequently.

But it's certainly likely that a lack of attention or competence among those responsible for keeping systems secure is what makes the majority of cyberattacks possible. However, that doesn't necessarily mean it also causes the most damage.

No help if you won't help yourself

The second Kent Cybercrime Survey in January 2014 investigated the attack vectors and countermeasures employed in a representative sample of 1,500 UK internet users. Around 20% of those who had been attacked in the past 12 months were still not applying basic internet hygiene and good practice. Defending against internet attacks is a little like avoiding a tiger: there's no need to outrun it, only to outrun others also trying to escape. Total security is unlikely to be achievable, but "enough" security is required to prevent hackers going for easy targets and the path of least resistance.

For example, do the many people and organisations still running Windows XP and Internet Explorer 6 represent many victims of cyber attacks? Both have long since been declared end of life and unsupported, which means no new security updates for newly discovered flaws. Or it may just be that the stakes are rising, with malware writers deliberately targeting more profitable victims rather than just the low-hanging fruit.

Taking a harsher line

A look at the approach by banks to internet fraud hints that this may be the case. Banks have always compensated their customers for any money lost through malware attacks or card fraud – presumably to encourage the uptake of online banking and so the massive potential savings the banks stood to gain from closing branches. But there has been a change of heart, as a bakery business in Surrey found out last year.

The firm's computer was infected with a piece of malware that circumvented the antivirus software and installed a keylogger. As they had not installed the bank's recommended additional protection software the bank refused to cover the £19,600 stolen, claiming customer's negligence. This is disgraceful behaviour from the bank, but it's likely we'll see further examples of it in the future.

Follow the money

There's worrying evidence of increasingly sophisticated and well targeted attacks. Imagine you are a cybercriminal, tired of compromising thousands of computers without being able to transform that into cash. Every attack slightly increases the probability you will be caught, so a lower profile with fewer, more profitable targets is a better long-term strategy. You want wealthy victims and you want to know how wealthy they are – this is called price discrimination in economic theory, and it maximises profit.

This is where targeted advertising comes in. The cynical view of "big data" is even that personalised adverts are its main application – to serve you "ads that make you feel queasy", as Sir Tim Berners-Lee has said. Advertisers will queue up to pay to display their wares to internet users whose profiles have been suitably analysed for suitability to their products.

Unfortunately the world of cybercriminals and malware has spotted this too. One instance of this has been dubbed Operation Deathclick by security company Invincea. In this case specialised malware is written that impersonates targeted advertising, aimed at US defence industries, probably to steal trade secrets. This malvertising, taking advantage of lax verification by the companies that serve up adverts embedded in web pages, these micro-targeted attacks are able to reduce the criminal's visibility by being active only for short times, in varying locations and with different signatures. Consequently, they stand a much better chance of hitting only their intended victims, and evading law enforcement.

Clicking on ads had never been considered to be a good security practice – many implement "drive-by" attacks that surreptitiously download malware or do so by disguising it as something legitimate. When there are so many routes into your computer that not even seasoned security professionals are immune, it is obvious that average users will feel more than perplexed.

So with that in mind, it's really not fair to blame the victim.

Organisations such as banks profit handsomely from transferring their operations to the internet – and are thus more able to invest in crime prevention. If they fail to do so, sooner or later we'll all find our digital pockets picked.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Targeted 'malvertising' reveals move towards more sophisticated hacks (2014, October 28) retrieved 17 April 2024 from https://phys.org/news/2014-10-malvertising-reveals-sophisticated-hacks.html