The attack almanac

Published on 20 January 2009

By Iftach Ian Amit

"E-crime is not random – it follows world events and seasonal trends. So adopting an anticipatory security strategy can help close vulnerabilities"*E&T* investigates this claim.

Traditional enterprise security methods are caught in a vicious cycle. Cyber-criminals take the initiative to set the strategy of attacks, the security vendors try frantically to catch-up once an attack is underway, and meanwhile the online malevolents have moved on to bigger and badder strikes, leaving the security sector scrambling to keep pace.

Technology continues to advance, but the methodology deployed creates a cycle of inadequacy that will not be broken until security vendors reinvent their strategies to not just follow where the cybercriminals lead, but anticipate their moves. By analysing the latest attacks, security providers are able to discern trends in e-crime activity, and then develop a solution patch or signature to prevent their customers from being affected by similar attacks in the future.

'MalWeb' is the natural evolution of malware in the Web 2.0 world. Different from malware, which is created and packaged in one central place and then distributed in its final form via the Web, MalWeb is created in the browser only when it is triggered. The complexity of Web 2.0 has lent MalWeb its most important capabilities: working in the same media and form as legitimate code, which gives it enough power to take advantage of system-level vulnerabilities simply by running on the same Web browsers and add-ons already existing in Web 2.0.

Anticipating the next step requires security researchers to dig deeper into attacks, analysing not only the surface of the final attack vector, but delving into the methodology, strategy and implementation of the attack. This approach enables researchers to build a holistic model of how e-crime operates – the business model, as it were, of participating parties, and also the tools used. Taking into account additional features such as localisation, specialisation for specific markets, focus on corporations-versus-consumers, and local and global events, completes the picture, enabling researchers to provide a detailed anticipatory service model, delivering products and roadmaps for future attacks – and even attack technologies.

Time of year

Cyber-criminals are highly skilled at taking into account seasonal and event-based browsing in order to most effectively target the largest base of victims. These events include elections, regulatory changes, financial crises, and its effect on prices etc, as well as holidays and ensuing shopping and travel.

Like legitimate marketers, cybercriminals improve their 'market penetration' by ensuring they infect relevant legitimate websites to reach the highest customer base possible at any given time. Research conducted by Aladdin's Attack Intelligence Research Centre (established to provide business intelligence around evolving threats, predict future trends in Internet security, and uncover the inner workings and effects of the business of e-crime) shows that predictions based on specific events and trends have had a high success rate materialising into actual attacks, bringing legitimate sites to be compromised in direct correlation to current events. Tested scenarios include political events, the rise of new pop stars, and holiday shopping.

For instance, about a week before the 2008 US presidential election, visitors to Barack Obama-related sites were serving-up approximately 360 separate instances of Malweb, while McCain-related sites followed with 230 instances.

After Obama's victory, email accounts around the world were overwhelmed with spam inviting users to watch the acceptance speech, only to download a cleverly-named Trojan and RootKit, monitoring the victim's passwords to banking websites and sending the information back to cybercriminals in the Ukraine.

A similar Trojan installed itself on the machines of users supposedly opening screenshots of Republican vice-president nominee Sarah Palin's Yahoo account, which was hacked before the election.

As well as opportunistic events, savvy cyber-criminals work to calendar fixtures that provide a hook for their ambits going forward. Ongoing events (holiday packages, cheap flights, cheap local fuel prices), retail-related events (Christmas, back-to-school,

Thanksgiving, and Black Friday – the Friday after Thanksgiving in the US, which is the beginning of the traditional holiday shopping season), and sporting tournaments (Olympics, Wimbledon, football and rugby World Cups), and general news (political conflict, disasters, etc), celebrity gossip (Britney's comeback, Angelina Jolie, TV's 'Big Brother') are the driver for choosing sites to be used as launchpads for the next wave of e-crime attacks.

But this also means that cyber-criminals are, to a degree, very predictable, and such intelligence helps in the fight against them. To predict where the next attacks will take place, a security organisation need look no further than the front page of a newspaper, or perhaps a teenager's favourite blog, to spot the trends in media popularity that precede an attack.

Online trend-watch services, such as Google Zeitgeist, or search patterns correlating to current events and trends, can provide an avid marketer or a sociology researcher plenty of information and insight on what people are searching for, and watching, on the Web; but the same statistics are also used by cyber-criminals to find their next attack targets. By correlating search patterns and current trends, attackers are able to reach large portions of the Internet-browsing population with targeted attacks on sites relevant to current fads.

Translating Google Zeitgeist statistics into target attack points is simple, leading to more targeted and effective e-crime than ever before, and enabling cyber-criminals to extend their portfolio of breached sites.

The skills needed to compromise such sites and serve malware to unsuspecting users has been dramatically reduced with the introduction of basic attack toolkits, or even 'Malweb-as-a-service' for a low monthly fees. Service exchanges provide traffic for 'advertising' purposes, with the advertisement serving Malweb and bringing in much higher revenue that a legitimate advertisement.

Another popular method of attack is as simple as hacking a site so a user simply clicks 'Next' several times inside a mass-attack application that has been updated with the latest SQL injection attack vector. Creating the actual Malweb is simple, using tools that, in some cases, fall short of their legitimate counterparts, but in other cases surpass them in terms of report granularity and control, provided to manage the unsuspecting victims.

Iftach Ian Amit is director of security research for the Content Security Business Unit at Aladdin Knowledge Systems

Further information:

www.aladdin.com/airc

IET Technical and Professional Network

http://kn.theiet.org/communities/itsecurity/index.cfm

Comments

All comments

You need to be registered with the IET to leave a comment. Please log in or register as a new user.