ANTICIPATORY SECURITY AND CURRENT AFFAIRS: CONNECTING THE DOTS

Traditional security methods are caught in a vicious cycle. The attacker takes the initiative to set the strategy of attacks, the security companies try desperately to catch up once the attack is underway, and meanwhile the attacker has moved on to bigger and badder attacks, leaving security in the dust and scrambling to catch up. While technology continues to advance at a truly remarkable rate, the methodology employed creates a cycle of inadequacy that will not be broken until security providers reinvent their strategy to not just follow where the cybercriminals lead, but anticipate their moves to block attacks that haven't yet been launched.

By analysing the latest attacks, security providers are able to see trends in the e-crime industry and develop a solution patch or signature to prevent customers from being affected by similar attacks in the future. Anticipating the next step will require 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, participating parties, and the tools used in the final attacks. 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 roadmaps for future attacks and attack technologies.

Cybercriminals are highly skilled at taking into account seasonal and event-based browsing in order to most effectively target the largest customer base. These events include elections, political changes, rules and regulations, the current financial crisis and its effect on prices, etc, as well as holidays and ensuing shopping and travel. Like legitimate marketers, cybercriminals improve their "market penetration" by making sure they infect relevant legitimate websites to reach the highest customer base possible at any given time. Research conducted by the Attack Intelligence Research Center (AIRC) shows that predictions based on specific events and trends have had a high success rate materialising into actual web attacks, bringing legitimate sites to be compromised and serve malweb in direct correlation to current events. Tested scenarios

Security providers must reinvent their strategy to not just follow where the cybercriminals lead, but to anticipate their moves to block attacks that haven't yet been launched.

Ian Amit reports

In order to provide effective protection against future attacks, security measures must incorporate the e-crime business strategy into their core methodologies, instead of waiting for the attack launch and then building protection.

include the US presidential elections, the rise of pop stars, and holiday shopping.

Approximately one week before the US presidential election, visitors to Obama-related sites were serving up approximately 360 separate instances of malweb, while McCain followed with 230 instances of malweb from sites bearing information on the Arizona senator. After Obama's election, users worldwide were overwhelmed with a flood of spam e-mails 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 VP nominee Sarah Palin's Yahoo e-mail account, which was hacked several months before the election.

Ongoing events (vacation packages, cheap local gas prices), retail-related events (Christmas, back-to-school, Black Friday) and world events (Olympics, World Cup, political conflict) and general news, celebrities and gossip (Angelina Jolie, soccer scandals) are the driver for choosing sites to be used as launch pads for the next e-crime attacks. In order to predict where the next attacks will take place, a security organisation need not look further than the front page of the newspaper, or perhaps their teenager's favourite blog to spot the trends in media popularity that precede an attack. Online trend watch services such as Google's Zeitgeist, 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 cybercriminals 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 today's fads. This leads to more targeted and effective e-crime than ever before, allowing cybercriminals to expand their portfolio of breeched sites with alarming success.

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

Looking forward to the coming year, it is already apparent that certain trends will dominate the e-crime scene. The failing global economy has already garnered much attention by legitimate users and cybercriminals alike, and will continue to be a popular topic for points of attack. In addition to dictating which websites will be targeted for malweb, the economy will generate increased growth in e-crime due to higher profitability than legitimate businesses. Cybercriminals will not only increase the amount of malweb attacks, but bring on additional headcount to manage and execute these attacks. The appeal of a somewhat steady income stream and work-from-home situations would be seen as a temporary means to survive the problematic job market. This temporary job would appeal not only to the more obvious and already thriving technology sector, but also from the management and financial sectors that would find better and more efficient ways to increase revenues in the still untapped resources of corporate and financial data. Anyone who can access and analyse this data will be a welcome addition to any cybercrime organisation.

While the global interest in the down economy gives researchers a pretty good idea of one area of upcoming attacks, it is essential for researchers to stay on top of current trends and make predictions about the direction of future e-crime activities. It is only by being proactive that companies and individuals will be able to prevent the significant effects of e-crime. Current affairs will continue to dominate the direction of cybercrime in the same way that newspapers, magazines and retailers boost sales by capitalising on significant events and interests. Building on basic business strategy, cybercriminals will continue to target and profit from the hottest sites that draw the most traffic and interest correlating to seasonal and local events and trends rather than blanket attacks on generic or less relevant sites. It is the responsibility of the researcher to maintain awareness of these trends to predict where they will occur and advise companies of how to build security technology to prevent these attacks before they are enacted. Security must break out of the box of static patterns, site restrictions, reputation or selective scanning of content if companies have any hope of protecting their data and users. In order to provide effective protection against future attacks, security measures must incorporate the e-crime business strategy into their core methodologies, instead of waiting for the attack launch and then building protection. ■

Ian Amit is Director of Security Research at Aladdin Knowledge Systems