Explosion in Advanced Evasion Techniques and APTs Is Costing Businesses Millions

infosecurity-magazine.com/news/explosion-in-advanced-evasion-techniques-and-apts

April 1, 2014

With the average cost of a data breach to an organization coming in at upwards of $1 million, it's imperative to take a realistic tack when it comes to understanding and thwarting AETs, according to a Vanson Bourne study, commissioned by McAfee.

Nearly 40% of IT decision-makers do not believe they have methods to detect and track AETs within their organization

AETs, first discovered in 2010 by network security specialist Stonesoft (acquired by McAfee last year), are methods of disguise used to penetrate target networks undetected and deliver malicious payloads. Using AETs, an attacker can split apart an exploit into pieces, bypass a firewall or IPS appliance, and once inside the network, reassemble the code to unleash malware and continue an APT attack. The prevalence of these techniques has risen significantly since 2010, with millions of combinations and modifications of network-based AETs having been identified to date.

The report found that more than one in five security professionals admit their network has been breached (22%), and out of those, nearly 40% believe that AETs played a key role. However, the scope of the AET threat is often widely underestimated – the report shows that respondents believe there are less than 500,000 of them. In reality, there are an estimated 800 million known AETs. And less than 1% are detected by other vendor's firewalls.

"The simple truth is that AETs are a fact of life. It's shocking that the majority of CIOs and security professionals severely underestimated that there are 329,246 AETs, when in fact the total of known AETs is approximately 2,500 times that number or more than 800 million AETs and growing," said Andrew Blyth, a professor at the University of South Wales who has studied the prevalence and impact of AETs, in a statement.

Recent high-profile data breaches have demonstrated that criminal activity can still evade detection for long periods of time. Survey respondents acknowledged this.

“We are no longer dealing with the random drive-by scanner that is just looking for obvious entryways into your network,” said John Masserini, vice president and chief security officer at MIAX Options. “In today's interconnected world, we are dealing with adversaries who spend weeks or months studying your public facing network footprint, looking for that one small sliver of light which will allow them to gain a foothold into your networks. AETs are that sliver of light.”

Nearly 40% of IT decision-makers, however, do not believe they have methods to detect and track AETs within their organization, and almost two-thirds said that the biggest challenge when trying to implement technology against AETs is convincing the board they are a real and serious threat.

“Many organizations are so intent of identifying new malware that they are falling asleep at the wheel toward advanced evasion techniques that can enable malware to circumvent their security defenses,” said Jon Oltsik, senior principal analyst for the Enterprise Strategy Group. “AETs pose a great threat because most security solutions can’t detect or stop them. Security professionals and executive managers need to wake up as this is a real and growing threat.”

The stakes are high and getting higher: respondents whose organizations had experienced a network breach in the past twelve months estimate the average cost to the business to be $931,006. Australia, which reported a lower number of breaches at 15%, indicated a much higher average cost per breach at $1.5 million. The cost to American respondents also exceeded $1 million on average. The hit to the financial services sector was the hardest, with estimated cost to be over $2 million per breach globally.