BIZCOMMUNITY

A practical guide to advanced threat detection

By Fred Mitchell

22 Sep 2016

It's a message that has been beaten to death: as security technology evolves so do attacks become more sophisticated. It's a vicious, somewhat symbiotic, lifecycle that seems to have no end in sight. And by golly is business doing its best to stay one step ahead of threats that are more diverse, more refined, more numerous and more targeted than ever before. To fight these onslaughts companies are adopting security technology to proactively safeguard their operations.

If you consider the above, it seems businesses have quite a fight on their hands; however, throwing products at the problem without maximising its potential is definitely not the silver bullet. In order to strengthen your defence against advanced attacks you must address two important questions: how can I maximise my existing security investment; and what other technologies and approaches will deliver more comprehensive and effective protection moving forward?

Whichever way you look at it, positive and effective steps must be taken to defend yourself against advanced attacks.

Step one: Know your enemy

To understand the scale of today’s advanced threats it’s important to understand how serious it is. Many organisations have made the fundamental mistake of underestimating the scale of risk, whereas others have over-reacted. The problem is that in both cases organisations don’t trust their existing security system. Often so many alarms go off that companies become complacent or overreact completely and out of context that precious resources are destroyed to prevent potential security breaches.

Organisations must have a clear understanding of not only the threat landscape, but also its specific vulnerability profile within the size, scope, and nature of their operations. Here are a few issues to consider when assessing your vulnerability posture:

• Traditional, mass-market cyber attacks such as spyware, botnets, SQL infections and phishing still need to be dealt with and traditional security software such as anti-virus, firewalls and intrusion prevention are an excellent line of defence.

• New advanced threats are emerging. For example, polymorphic threats continuously change, making it impossible for traditional signature-based security defences to detect it. Blended threats employ multiple attack vectors (paths and targets) and multiple types of malware to disguise the attack, confuse security analysts, and increase the likelihood of a successful data breach.

• Malware is dramatically on the rise and are often successful: many threats today are encrypted via SSL (also known as HTTPS or TLS) therefore hiding malware from many solutions. Encrypted SSL traffic now represents 15-25% of all outbound web traffic and up to 40% of production web traffic but 80% of defence-in-depth systems do not inspect encrypted traffic, according to Gartner.

Ransomware forms part of malware and four million samples were identified in the second quarter of 2015, indicating an upward trend, according to Security Magazine.

• Mobility adds a new dimension to advanced threats and represents a growing percentage of overall traffic. According to CIO Magazine there are over 1 million malicious and high-risk Android apps currently in circulation.

• The window of opportunity for advanced threats is wider. It takes only seconds, minutes, or hours to compromise targets while breaches can take weeks, months, or years to discover.

Step 2: Measurement and tracking

Now you need to determine whether additional threat detection and protection is required. The key is measurement and tracking by establishing metrics that will evaluate the effectiveness of your security solutions and measure it constantly. Start by measuring your success against malware, this will provide you with an understanding of how your employees are interacting with the web. Also, make sure you know when systems are infected, and which ones.

A 'Potentially Infected Clients report, which is typically available through malware protection systems, will tell you how many devices have needed remediation over a period of time and importantly what systems that are attempting to send out confidential or proprietary information. Also, assess how many applications are running on your network and whether they have been approved. The more applications you have the higher likelihood that you'll be victimised by an advanced threat, many applications contain vulnerabilities that attackers can exploit remotely.

Step 3: A network-based approach

Visibility particularly if its network based is vital for an effective defence against advanced threats. The more visibility you have into your network traffic at all phases of the lifecycle, the more you can analyse, understand, control, and remediate issues and incidents.

With network-based anti-malware tools you get full visibility into all inbound traffic, you can analyse it and filter out malicious content before it arrives at the endpoint, and you can increase coverage and catch more malware (by using multiple anti-malware engines at the network level). Important network-based anti-malware tools provide:

• Visibility into SSL traffic. SSL encryption protects the privacy of network-based communications but it can also be used by hackers to mask advanced threats.
• Proxying all network requests will guarantee that threats aren't able to tunnel its way into your network.
• Whitelisting, therefore, maintaining a registry of approved files that have been granted permission by an administrator.
• Malware scanning to block the black listed threats. The combination of a good secure web gateway appliance and a content analysis system with malware scanning and whitelisting can block all known threats, sources and signatures and direct truly unknown content for malware analysis

Step 4: Implement a complete defence solution

Piecemeal solutions aren't the answer. Many forward-looking enterprises are implementing a lifecycle defence that integrates security solutions to provide more effective attack detection, response and prevention. This shift requires an integrated approach that not only blocks known exploits but also tells you the how, what, where, when and why of advanced targeted attacks and security breaches. This is then coupled with end-to-end visibility of data exfiltration and malware infiltration on the network.

For example, many companies are implementing multiple web access logs – using multiple protocols (HTTP, HTTPS, streaming media, SOCKS, etc.) With a lifecycle defence, they can implement a variety of standard web access context logs, provide full capture data, and tune additional security logs to vector in on what might try to hide in the ocean of data.

Lastly, lifecycle defence leverages the network effect by sharing threat intelligence from enterprises and users worldwide.

ABOUT FRED MITCHELL

Fred Mitchell is the Business Unit Division Manager: Symantec at Drive Control Corporation (DCC)
- A practical guide to advanced threat detection - 22 Sep 2016
- Effective information governance essential to managing data growth - 21 Sep 2015

View my profile and articles...