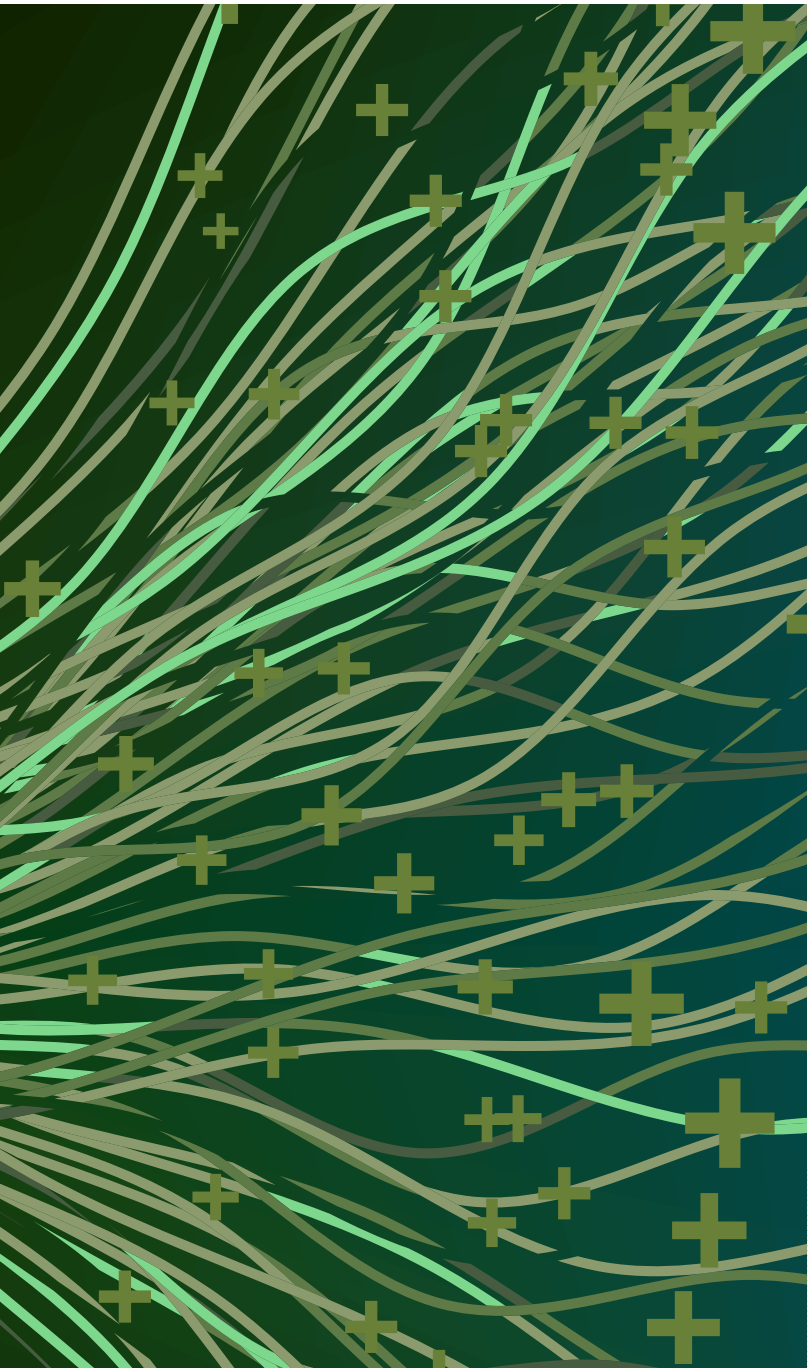
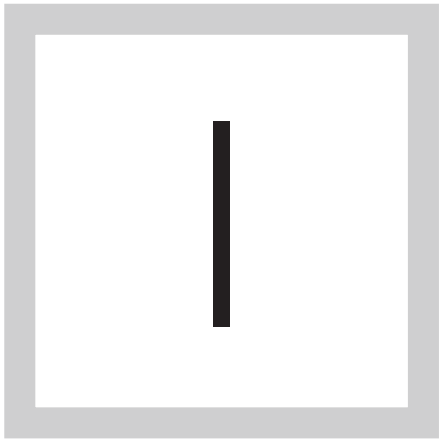


E-Guide

TARGETED ATTACKS: DETECTION AND CONTAINMENT

TechTarget | SearchSecurity



T'S NOT ENOUGH anymore to keep the network secure through patching and updates. Network segmentation and continuous monitoring are essential too.

TARGETED ATTACKS: DETECTION AND CONTAINMENT

Michael Cobb

Enterprise networks no longer consist of just desktop computers and a few local area network servers; now it includes employees' laptops, smart phones, tablets and other mobiles devices, plus file, data, and mail servers, kiosks, supervisory control and data acquisition systems, and so on. Many networks extend into the cloud and virtual environments and interact with third-party systems and the Internet of Things.

As recent data breaches show, enterprise IT pros are failing to secure all these endpoints; too many still believe that they can trust their internal networks and users. Their defenses focus on trying to prevent attacks. Firewalls, email filtering, antivirus software (AV) and VPNs are still the four most widely deployed security technologies, yet hackers still routinely compromise endpoints sitting on even the mostly heavily protected networks. Cybercriminals are creating new malware and attack techniques faster than endpoint security solutions can be updated. According to Panda Security, a

quarter of all malware samples ever recorded were produced in 2015, with around 230,000 new malware samples discovered every day.

PATCHING AND UPDATING ARE NOT ENOUGH

Ensuring devices and endpoints are patched and running up-to-date AV software will always be a key security control, but given the myriad variety of devices, applications and users that an enterprise has to support, it has to be just one of many. Preventative technologies not only miss too many attacks, they don't have the ability to identify and remediate ongoing exploits. Security teams need a strategy that can protect key resources and data even when perimeter defenses have been breached and the network compromised.

Network segmentation can greatly improve the protection of data held on today's more open networks by limiting the scope of a compromise. Segmenting internal networks allows access to critical information to be restricted to only those individuals or applications that have a valid and trusted requirement to access it. It also means that additional security controls can be deployed only on segments that warrant them, reducing unnecessary costs while ensuring sensitive areas are well protected.

Home

Targeted attacks: Detection and containment

Segmentation can limit an attacker's ability to move around a network, but without the ability to discover successful infiltrations many organizations will only learn of an attack after valuable data has been stolen. Once an attacker has breached a network's preventative defenses they are very good at reducing the footprint of their activities in order to evade detection. According to the 2015 Trustwave Global Security Report, 81% of victims did not detect the breach themselves and the median length it took to detect a breach was 86 days.

CONTINUOUS MONITORING ALSO ESSENTIAL

To detect sophisticated and targeted attacks, enterprises need to continuously monitor network activity and actively search for unusual behavior. For an attacker to extract data, at some point they have to act differently to a genuine and trustworthy user, so monitoring systems that learn behavior patterns of users, devices, and services can spot actions that are out of character and indicate a possible attack. For example, the Anthem breach could have been picked up fairly early on because the attackers submitted database queries remotely to obtain the PII records—certainly unusual behavior.

Of course for monitoring tools to pick up on malicious activity there has to a baseline of what's normal, across activities that span multiple environments.

IBM's InfoSphere Guardium, Splunk Cloud or Solutionary's cloud-based ActiveGuard Security and Compliance platform are a few products that can create a baseline and provide a unified view of on-premises and cloud activity, generating alerts when an activity falls outside of an expected bandwidth.

AUTOMATION IS AN ESSENTIAL PART OF FUTURE SECURITY

The attack surface of a modern enterprise is too great for prevention-based technologies to ever be 100% effective, yet so many organizations assume they are and tend to base their security strategies and spending on these technologies. While prevention technologies are important, enterprises desperately need to deploy tools that can automatically detect and respond to threats. This proactive approach can reduce the time between the initial compromise and its discovery and remediation, thus reducing the extent of the damage.

Michael Cobb, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS). Mike has a passion for making

IT security best practices easier to understand and achievable. His website www.hairyitdog.com offers free security posters to raise employee awareness of the importance of safeguarding company and client data, and of following good practices.

Home

Targeted attacks: Detection and containment

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.