On any given day, infrastructure attacks can account for approximately 15 percent of global Internet traffic; and many of these new attacks fall into the class of APTs (Advanced Persistent Threats) which evade today’s perimeter defenses and host-based security solutions. Research shows that virtually every organization continues to suffer from successful exploits. One study found, on average, that enterprises experienced 102 successful attacks per week in 2012, as compared to 72 in 2011 and 50 in 2010, with the average resolution time growing to 24 days per attack versus 18 in 2011, and an average cost of $591,780 over that time. The magnitude of financial impact is not surprising since a recent investigation found a single command and control system had over 750 networks actively “calling home” with confidential data. Experts warn that more than $1 Trillion has been lost to APTs, with more intellectual property losses in the last few years than since the Internet became mainstream.

Traditional security approaches are not effective against this new breed of attack. APTs are built to circumvent existing perimeter and endpoint defenses with 94% of organizations unaware that these attacks were operating inside their networks, often for months.

The success of attacks is due to the progressively sophisticated nature of the attacks and attackers. Historically, the majority of attacks were generated by “script kiddies” trying to see what they could do; now, the profile of an attacker is that of a well-funded criminal organization, hacktivists, or operatives from hostile nation-states, motivated to steal information for financial gain, inflict damage or political advantage.

Concurrently, APT attacks are expanding from high-profile and high-value targets like government research labs, system integrators, and critical infrastructure, to large enterprises and even mid-sized businesses. These attacks are often focused on exfiltrating core intellectual property or financial data, and either reselling the data on the gray market or using the information for specific financial gains.

The New Security Reality - Attackers are Already Operating INSIDE the Network

Today’s global, connected economy requires that organizations open themselves up to employees, contractors, partners, vendors, and even customers, in order to provide access to the organization’s resources, from wherever they are, using whatever device they have, so they can conduct business. This operational

WHY APTs BYPASS TRADITIONAL SECURITY

Loss of perimeter means numerous alternative channels and many more vulnerable targets

- Attacks via 3rd party managed services
- Social engineering and direct attacks of employees with weak security practices
- Exposure at airports, hotels, cafes
- Infection via USB devices
- Compromise of VPN access bypassing perimeter security
- Exposed corporate devices – printers on open WiFi
- Open Ethernet ports in shared areas

New attack vectors drive multi-pronged infection and compromise

- Phishing + drive-by downloads
- Customized malware
- Social engineering
- Password attacks
- Exploitation of zero-day vulnerabilities

4 Center for New American Security, 2013
necessity has resulted in the disappearance of the perimeter, requiring a new way of thinking about how to secure an organization’s network and assets.

Unfortunately, this loss of perimeter facilitates APT attacks, providing a much larger attack space and improving their chances of penetration. The new threat landscape necessitates that organizations base their approach to security on the assumption that multiple attacker profiles are already operating IN their network. Research shows that 81% of organizations have experienced a data breach as a result of negligent or malicious employees or other insiders.\(^5\)

The headlines are also increasingly filled with more and more examples where attackers have meticulously targeted an individual organization over long periods of time to get at their most critical assets.

**New Threats require New Approaches…**

**Introducing Advanced Threat Deception™ from Shadow Networks**

Shadow Networks has taken a new approach that leverages disruptive technology to help organizations protect their network and resources from attackers under the assumption that they are already successfully operating INSIDE the customer network. Applying patented network virtualization and a software-defined networking (SDN) architecture, Shadow Networks is able to cost-effectively create operationally realistic systems that can scale up to represent very large infrastructure targets. These Shadow Networks deceive attackers to help organizations hide critical assets and ultimately understand the elusive intent of the advanced malware and attackers.

Shadow Networks’ ShadowBox™ is an appliance that introduces large-scale simulated hosts and networks (akin to creating a large network neighborhood around your key assets), without impacting the performance of the actual enterprise network. These simulated Shadow Networks and Shadow Hosts are a mix of high-interaction realistic hosts meant to deceive attackers and hide valuable network resources, while simultaneously acting as bait with low-interaction simulated hosts for maximum coverage. ShadowBox provides key functionality to weed out and contain sophisticated attacks such as APTs.

**Now, with Shadow Networks’ ShadowBox, organizations finally have a way to:**

**Hide and Protect** – ShadowBox is able to replicate networks at sufficient scale and fidelity to be able to attract and convince attackers they are operating within a legitimate network environment, effectively hiding actual resources from discovery and attack. These simulated networks can operate side-by-side with or in front of your real network resources, making it extremely difficult for attackers to tell the difference between them.

Since the “shadow” infrastructure is running real applications, including customer “Gold Images”, it can simulate “real” hosts and their behaviors. As a result, organizations are able to obfuscate their most critical resources, dynamically cloaking resources and networks by creating so many targets that it’s not clear which assets the attackers should focus on.

**Bait and Detect** – Shadow Networks has virtual Shadow Hosts within ShadowBox and deceptive agents that entice attackers to attack these “decoy” resources instead of the real ones. It may be that a few systems have slightly weaker security postures – for example, they may look as if they are unpatched machines vulnerable to attack. As soon as anyone attempts to connect to these Shadow Hosts, ShadowBox will detect and start monitoring the activity. Because the resources are “decoys,” the organization can be confident it’s not legitimate traffic. And because the organization sets the “Gold Image” or policies around the Shadow Hosts, there is no concern over false positives created by users who change settings, add applications or behave unpredictably.

**Contain and Inspect** – ShadowBox leverages its patented SDN capabilities to trap and contain attacks in a virtualized dynamic quarantine, recording all activity as the attack plays out in a deceptive Shadow Network, while preventing malware from spreading to other systems in the real customer network. Instead of eliminating malware upon detection, attacks are safely removed from the customer network, then contained and recorded, so the organization can understand the ultimate intent of the attack. This information supports real-time and post-attack forensics, enabling the organization to determine the best course of action to effectively protect their assets from further attacks.

The combination of unique capabilities of Shadow Networks provide the most innovative and extensive APT detection and mitigation today, effectively complementing the perimeter and host security solutions you already have deployed, and establishing a safety net for catching the APTs that have made their way past your defenses.

To learn more, visit us at www.shadownetworks.com or contact us at info@shadownetworks.com.

\(^5\) Trend Micro and the Ponemon Institute, “The Human Factor in Data Protection.”