Phishing attacks, the cause of 95 percent of cybersecurity-related data breaches and financial loss, continue to evade security defenses. Detecting and protecting from these attacks is complicated by the fact that the attacks are often multi-vector, meaning that they impact email, web, and network traffic. Further complicating defense, these attacks are dynamic, hackers often launch and shut down phishing sites and payloads in a matter of hours to evade detection.

**PHISHING ATTACK VECTORS**

Attacks often start by tricking a victim into unknowingly downloading malware that is hidden in an email file attachment or on a web page. Once the victim’s device is infected, a hacker can gain access to their network and systems. From there, the attacker can establish communication with external phishing sites to exfiltrate data and download more malware, further infecting systems to achieve their malicious objectives. To protect from attacks, organizations need phishing security solutions that can detect and block threats across all attack vectors, including email, web, and network.

**PHISHING SITES AND CAMPAIGNS ARE DYNAMIC**

When executing phishing campaigns, hackers often first compromise trusted websites and email servers, or establish imposter websites and email accounts—weeks or even months in advance of a planned attack. After setting up a phishing site, hackers launch and shutdown attacks in a matter of hours. The dynamic nature of phishing sites makes legacy security defenses that mostly rely on threat intelligence extracted from active, launched attacks, less effective.
EARLY VISIBILITY INTO PHISHING SITES AND CAMPAIGNS

To protect from phishing attacks, cybersecurity solutions, including email, web, and network defenses, need early insight into phishing sites before campaigns launch and attacks are active. Fortifying defenses with security technology that hunts for malicious sites before attacks launch, during the weeks and months hackers are establishing or compromising websites in preparation of launching an attack, can provide the early visibility and threat indicators necessary to protect from impending attacks. Arming email, web and network cyberdefenses with early insight into phishing sites and payloads enables these defenses to more effectively detect and block phishing email, malicious web downloads, attacker movement through your network, command-and-control communication and data exfiltration to external sites. With early visibility to phishing sites and payloads before attacks launch, security defenses can prevent cyber breaches.

AREA 1 HORIZON™ ANTI-PHISHING SERVICE

Area 1 Security offers an anti-phishing cloud service that stops email, web, and network phishing attacks that other security technologies miss. Area 1’s innovative technology crawls the web continuously and proactively, discovering phishing campaigns and infrastructure before attacks launch. On average, we detect malicious sites and payloads a full 24 days before industry benchmarks.

By proactively hunting for new phishing infrastructure as it’s set up, Area 1 Security has early visibility into phishing sites, payloads, malware, and compromised servers before campaigns launch. The resulting insight and threat information powers the Area 1 Horizon anti-phishing service to detect and block phishing threats that other security technologies miss. The service is easy to deploy and integrates with existing email, web, and network security infrastructure to provide an added layer of anti-phishing protection that effectively stops attacks.
Backed by top-tier investors, Area 1 Security is led by security and data analytics experts from NSA, USCYBERCOM, Cisco/IronPort and FireEye, who realized the pressing need for a proactive solution to targeted phishing attacks. Area 1 Security is working with organizations that implement the most sophisticated security infrastructures. These companies include F500 banks, insurance providers, retail organizations, and health care providers. Our mission is to preempt and stop targeted phishing attacks at their very outset and significantly improve the customer’s cybersecurity posture.

To learn more, please visit www.area1security.com.

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, Palo Alto Networks’ game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization’s most valuable assets.

Find out more at www.paloaltonetworks.com.