AREA 1

COMPANY
S&P 100 Consumer Goods Leader

PRODUCT
Household & Personal Products

PRODUCT
Area 1 Horizon

CHALLENGE

Malicious Links and Business Email Compromise Phishing Attacks

RESULTS

Multibillion-dollar global company is now protected against email and web-based phishing attacks.

- Eight million targeted phishing attacks blocked in one year
- BEC attacks targeting senior executive and board members blocked
- IT team no longer needs to spend time "tuning" email security rules and blocklists

CUSTOMER STORY

Defeating a Fortune 500 Company's Cloud Email Threats

BACKGROUND

Throughout its successful, multi-decade long history, the confidential subject of this case study has always strived for advancing technology to address the needs of its consumers worldwide.

In a pivotal example of its commitment to innovation and growth, and to modernize its collaboration companywide, the company successfully migrated to G Suite. In doing so, the company initially elected to rely on its existing information security infrastructure to keep the business safe from cyber threats.

However, as technologies and industries evolve, the risk of cyberattacks that could lead to a data breach or system disruption also evolves - and increases. Particularly for an S&P 100 company that serves customers around the world, such attacks can inflict major operational downtime, brand harm, significant cost, and government investigations and fines.

CHALLENGE

The information security team recognized that the most significant cyber risk is email-borne threats: it was time to prioritize a project to defend against these attacks.

Of greatest concern were end users clicking on malicious links or falling for business email compromise (BEC), with high potential for theft of funds and information.

According to the FBI, phishing attacks through BEC emails alone have cost companies over $12 billion during the last five years.

Although the company relied on industry-known email and web security technology to protect it from phishing attacks, **the team found itself frequently "tuning" the security gateways and adding rules to block messages after attacks got through. Therefore, executives and end users worried their email was not secure.** While the IT team can control software updates, they can't control which links end users click on or whether they fall for a BEC email. The team recognized the need for technology to better defend the company against malicious links and phishing attacks.

SOLUTION

The company worked with Area 1 Security to bring the attacks to a halt. Area 1's innovative technology continuously and proactively crawls the web, discovering phishing campaigns and infrastructure before attacks launch. **On average, the solution detects malicious sites and payloads a full 24 days before industry benchmarks.** The resulting early insight and threat information empowers Area 1 Horizon™ anti-phishing service to detect and block phish that other defenses miss, adding a layer of protection against attacks.

To evaluate effectiveness, Area 1 Horizon was deployed with the company's Gmail instance. The Area 1 service is automated, operationally simple, and cloud-based, so it required no new on-site equipment.

The Area 1 service successfully detected and blocked substantial numbers of phishing emails, including credential harvesting and BEC attacks. In one incident, an email sent to the CFO that appeared to be from the CEO, requesting a transfer of funds, was detected and blocked before it reached the CFO's inbox, averting potential financial loss.

In addition to protecting against phishing email, Area 1 Horizon also includes a recursive DNS service that protects against web-based attacks. The company successfully deployed the Area 1 recursive DNS service with their Windows DNS server to block end-user access to phishing sites. The Area 1 service is updated hourly with newly discovered phishing domains to maximize protection.

RESULTS

Area 1 Horizon is now operational company-wide, protecting this Fortune 500 leader against email and web-based phishing attacks. Over the past year, the service processed 375 million email messages and stopped upwards of eight million targeted phishing attempts. The multitude of stopped attacks includes credential harvesting threats that spoof brands such as Outlook, Paypal, UPS, and Apple; links resolving to sites or files with malicious payloads; and email attachments with embedded malicious code or links.

The CIO noted that fewer phishing emails land in inboxes, and the IT team no longer needs to spend time "tuning" email security rules and blocklists.

Also, the IT team is now better able to provide specific metrics and reporting to the Board about the number of emails processed and malicious messages caught, demonstrating the effectiveness of cyber defenses.

Area 1 Security's preemptive, comprehensive, targeted phishing protection has helped improve productivity, and significantly reduced cybersecurity risk.

ABOUT AREA 1 SECURITY

The industry's most comprehensive anti-phishing solution, Area 1 Horizon identifies threat campaigns, attacker infrastructure, and delivery mechanisms to give an advance warning to stop targeted phishing attacks during the earliest stages of an attack cycle.

Backed by top tier investors, Area 1 Security is led by security and data analytics experts coming from NSA, USCYBERCOM, Cisco/IronPort, and FireEye who realized a pressing need for a proactive solution to targeted phishing attacks. Area 1 Security works with some of the most sophisticated organizations in the world, including F500 banks, insurance companies, and health care providers, to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture, and change outcomes.

Learn more and get in touch with us for a free preview:
INFO@AREA1SECURITY.COM