

Social Engineering Protection Appliance™

Powered by Cyveillance
January 2011

EXECUTIVE SUMMARY

The explosion of personal information in cyberspace available from sources such as professional and personal networks is fueling the newest breed of highly sophisticated and targeted social engineering attacks. The fear that a highly customized email can easily evade existing email security measures and compromise the enterprise is keeping information security professionals up at night.

This breed of cyber threats is carefully planned and executed for network infiltration or corporate espionage. Attacks can result in the loss of core intellectual property, sensitive information, customer data, loss of business productivity, and undermine customer trust. In recent months, social engineering attacks have successfully compromised government agencies, defense contractors, and many leading corporations.

While companies go to great lengths to protect corporate data and systems, employees often are not as guarded with their personal information. Gaining access to employee names, titles and trusted associates is as easy as conducting searches on social networking sites. Sophisticated social engineering threats are highly personalized and designed to acquire information from an individual or individuals who have access to high value information or systems. Armed with research about a company, its systems and its employees, credible looking emails are delivered to employees who most likely will be unable to detect the insidious nature behind what appears to be a legitimate emailed request.

According to a study by the Center for Strategic and International Studies and security software firm McAfee, the average cost for the downtime associated with a cyber attack is 6.3 million dollars a day. While costs associated with downtime are well understood, the impact on national security and industry competitiveness are much greater and harder to quantify.

Companies need to supplement existing email security systems with a targeted solution to address these rapidly evolving and evasive attacks. **The Social Engineering Protection Appliance™ offers the industry's first appliance focused on rapid detection and protection against new forms of social engineering attacks.**

ANATOMY OF A CUSTOM SOCIAL ENGINEERING ATTACK

Even companies with significant resources to spend on security are not immune to social engineering attacks. Companies such as Google, Adobe Systems, ExxonMobil made headlines in 2010 as their security was breached and intellectual property compromised.

According to a report from the Christian Science Monitor, ExxonMobil, ConocoPhillips and Marathon oil were victims of a highly targeted cyber attack. This attack was launched in 2008 and designed to obtain highly valued "bid data" detailing the quantity, value, and location of oil resources. Executives at these companies were tricked by socially engineered emails delivering malware. While the attacks originated in 2008, the attacks were not detected and reported to the companies until 2009.

"Posting of personal, corporate and governmental information in publicly accessible social environments on the Internet has created a deep repository of artifacts that can be mined and analyzed to uncover confidential matters."

*Andrew Walls -Gartner
"Everyone's a Spy:
Mining Social Media
for Security Intelligence"*

CUSTOMIZED SOCIAL ENGINEERING ATTACK VECTORS

Sophisticated social engineering attacks such as the ones mentioned earlier can utilize a number of strategies to infiltrate an organization as described below.

STEP 1: SYSTEMS VULNERABILITY ASSESSMENT

An email campaign may solicit information for the purpose of understanding the best way to infiltrate an organization's network. The attacker may canvass a number of employees within the same organization in an attempt to mine the most accurate internal intelligence. Usually, email campaigns of this nature are sent to a small number of employees to avoid detection from spam filters. Once the required information has been collected, the attacker can develop highly customized malware to exploit software, anti-virus, and other system weaknesses for use in a zero day exploit.

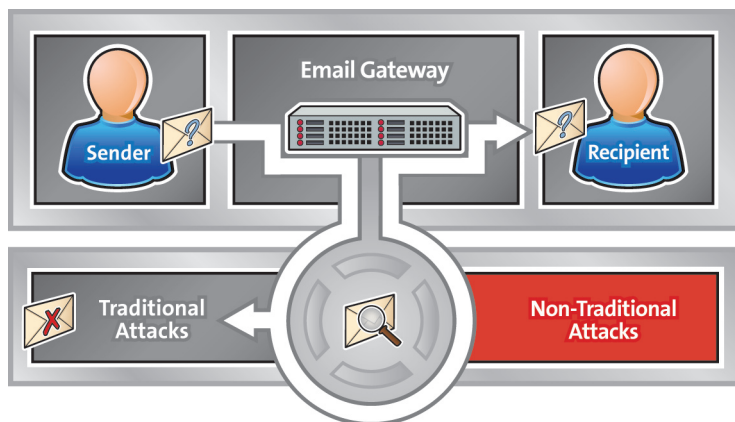
STEP 2: IDENTIFY HIGH VALUE EMPLOYEES

Criminals conduct research on individuals with access to desired intelligence or systems. Social networking sites or other publicly available data sources provides a wealth of information on a company's employees. Knowing how to approach key individuals may not be a one step process. In the Operation Aurora attack, social engineering emails were sent to determine working relationships between employees. By understanding these relationships, hackers better qualified their targets and increased the odds of delivering an email that wouldn't raise any suspicions. A clever hacker could steadily build a knowledge base and "fly under the radar" by soliciting small pieces of corporate information from various individuals.

STEP 3: INITIATE FINAL ATTACK

The final step in this process utilizes the data collected to craft a highly customized email to evade detection and obtain the desired information. The request may utilize attachments, poisoned links to deliver malware on a target web page, or the request for information may be contained in the body of the email. Once the email recipient unknowingly either provides the information or clicks on a link, the damage is done without the recipient's knowledge. As recent headlines have shown, the attack can take months or longer to be detected.

SOCIAL ENGINEERING ATTACK VULNERABILITY



ILLUSTRATION

The hypothetical example described below exposes the vulnerability most individuals have to social engineering attacks.

THE TARGET

Dan Jones is a senior executive at a Fortune 500 company. Dan keeps in touch with his professional network using LinkedIn, but his wife and children use Facebook to keep in touch with their friends.

EXPOSURE

A quick web search on Dan Jones provides the following information:

Dan's LinkedIn profile - Dan has a robust network of colleagues and trusted business associates.

Business article - A quotation from Dan in a business article reveals his name, company, title and his focus within the organization.

Charity fundraiser for school article - The family ran a 5K together. Family names, ages of children, name of school and race times are referenced in the article.

RESEARCH PHASE

A hacker from outside of the United States has been looking for a way to infiltrate an organization with desired intellectual property. While he was reading the news, he sees the business article quoting Dan. He begins to research Dan.

His research yields valuable information that can be used to craft a very personalized email message. The LinkedIn profile gleans professional contact information. The charity fundraiser

article provides information about his family. He then cross references this information with Facebook data to obtain even more information on Dan and his family. At the conclusion of his research, the hacker has not only obtained the required information to craft a personalized message to Dan, but he also been armed with additional information to penetrate his company.

THE ATTACK

Dan receives an email message from a former colleague. He worked with this former colleague many years ago and had posted a recommendation for his work on LinkedIn. The email joked about his race time and inquired about how things were going with work and the family. He provides a link to pictures of his family on Facebook. When Dan clicks on the link, he is taken to the Facebook picture of his friend and a Trojan (malware) is delivered stealthily. He replies to his friend with an email, but never receives a response back. The message soon fades from his memory, but the damage has been done.

TRADITIONAL EMAIL SECURITY DETECTION CHALLENGES

Traditional email security is highly effective at stopping spam, mass phishing attacks, and viruses found in attachments. When new attacks are discovered, security experts analyze and identify the signature associated with the attack to ensure that this signature is detectable in the future. Email security systems rely heavily upon signature based scanning methods. This prevents known attack signatures from reaching the intended recipient. An August 2010 study by Cyveillance revealed that it took antivirus vendors 2 to 27 days to catch the new malware threats. Even the most popular antivirus solutions detect less than half of the latest malware threats and target URLs are not analyzed.

Mass phishing and spam attacks are often detected rapidly based on the sheer volume of the email sent. The perpetrators of these attacks realize that there is an inherent latency associated with updating signature files, so attacks of this nature continue.

Since sophisticated social engineering attacks are characterized by low volume and are highly customized, traditional email security is not sufficient at detecting and thwarting these targeted social engineering attacks.

SOCIAL ENGINEERING PROTECTION APPLIANCE

SEPA's advanced real-time inline detection scans messages for suspicious indicators and key organization-specific parameters to protect against new forms of social engineering attacks. The following section provides an overview of SEPA.

When an email is sent only the sender knows whether the email was legitimate or sent for illicit use. As a result, all incoming email must be inspected and evaluated for security threats.

The first step of email security defense is a traditional email gateway. Traditional email security inspects emails for known signatures and is optimized for stopping spam, mass phishing attacks, and infected attachments.

SEPA works with traditional email gateway systems to add a critical layer of protection. Once an email has passed through the email gateway, SEPA performs a deep inspection of both email content and context to determine whether the intent of the sender is malicious.

SEPA goes beyond just the content contained in the email itself to also protect against poisoned web links. Embedded web links are traversed and the destination web pages are evaluated for malicious behavior using cutting edge heuristic and behavioral analysis.

A comprehensive protection strategy requires updates based on constantly evolving live cyber threats occurring in the wild. Cyveillance Global Threat Intelligence provides real-time integration with Cyveillance's cloud-based cyber intelligence to provide protection against web links distributing malware, hosting phishing attacks, command and control botnet servers, botnet drop sites, malicious IP addresses running rogue DNS servers and open proxies, etc.

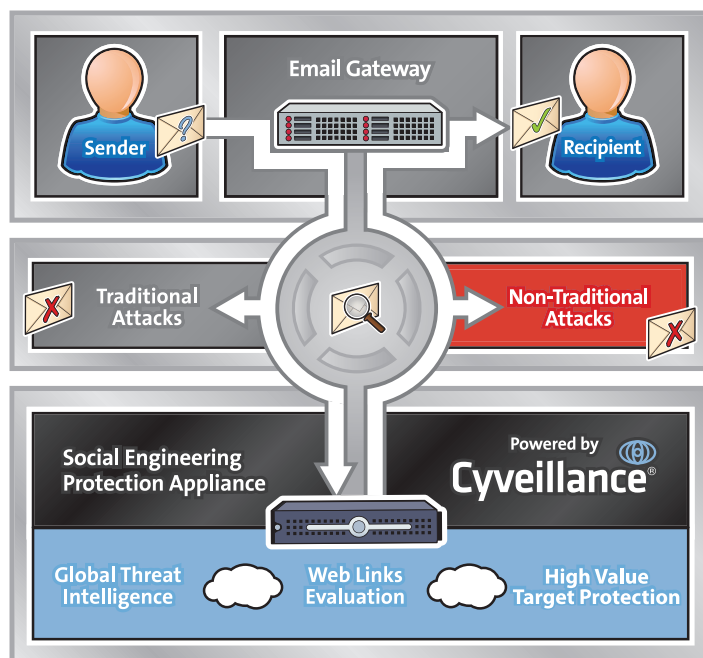
SEPA's core social engineering attack detection capabilities may be further enhanced, through Cyveillance Professional Services, to protect individuals with access to critical assets or sensitive information. These individuals are high value targets for hackers and require an additional layer of protection.

SEPA's High Value Target Protection service begins with a red team exercise to discover the cyber-footprint, including social networks, of a particular individual to know what information can be used against them. This intelligence is then utilized by SEPA to enhance detection and protect against targeted attacks which specifically leverage the publicly available information for a given high value target. The unique ability to correlate individual specific cyber footprints with SEPA's advanced detection capabilities provides a highly effective defense against targeted attacks.

FEATURES

- **Real-time Inline detection** - Scans for suspicious indicators and key organization-specific parameters using advanced algorithms, behavioral analysis and Cyveillance Global Threat Intelligence.
- **Rapid Response** - Adaptive technology platform and rapid configurability
- **Seamless integration into existing email security** - Rapidly integrates with existing email security systems
- **Rules-based Workflow** - Configurable rules ensure appropriate actions are taken based on threat classification
- **Adaptable Threat Categories** - Comes preloaded with social engineering classification tags.
- **Web-based GUI** - Provides users control over algorithm configuration, email review, and appliance management.
- **Powerful, Self-Learning Technology** - Ensures that the technology is updated to catch the latest threats.
- **Easy to operate and administer** - Leverages existing skill sets of IT staff.

SOCIAL ENGINEERING PROTECTION APPLIANCE™ Starts where Traditional Methods Stop



SUMMARY

The newest highly targeted social engineering attacks are difficult to detect with conventional email security systems. In order to address this vulnerability, a new solution is required to fill this security gap.

The Social Engineering Protection Appliance™ works with existing email security systems to provide inline real-time comprehensive protection against sophisticated social engineering attacks. Since threats are constantly evolving, powerful configuration tools enable administrators with the ability to respond to zero- day threats rapidly. SEPA's advanced cyber security technology has been built using patented and proprietary technologies developed and in use by Cyveillance, Inc. for over a decade ensuring a high degree of stability for mission critical environments.

ABOUT CYVEILLANCE

Cyveillance, a world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals and their interactions, enabling its customers to preserve their reputation, revenues, and customer trust. Cyveillance serves the Global 2000 and OEM Data Partners – protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and service providers that include AOL and Microsoft. Cyveillance is a QinetiQ Company. For more information, please visit www.cyveillance.com or www.qinetiq-na.com.

Copyright © 2012 Cyveillance, Inc. All rights reserved. Cyveillance is a registered trademark of Cyveillance, Inc. All other names are trademarks or registered trademarks of their respective owners.

BENEFITS

- Protect against infiltration attempts, espionage and cyber criminals
- Protect intellectual property sensitive information and customer information
- Preserve revenue, business productivity and client trust

Cyveillance, Inc,
2677 Prosperity Avenue Suite 300
Fairfax, Virginia 22031
888.243.0097
www.cyveillance.com
info@cyveillance.com