AREA 1

WHACK-A-PHISH?

Why “Tuning” Email Security Is a Losing Game

It's striking how security vendors claim you can "tune" leaky email defenses. Whether those defenses are provided by a secure email gateway (SEG) or included with Office365 or Gmail, trying to patch the breach after you've been attacked is like bringing a bandaid to a knife fight.

The typical scenarios are execs or end users unhappy with the volume of phishing email hitting inboxes — or worse, a breach that occurs due to a phishing email. Your security team scrambles to react to the incident and prevent brand damage and financial loss to the business.

Then, only after the fact, your vendor tells you to update to the latest release and "tune" the email security configuration in an evidently ineffective and certainly expensive solution, to prevent follow-on attacks. Really?

TUNING IS AN ENDLESS DO-LOOP

Unfortunately, no amount of "tuning" can turn back time and prevent phish from being clicked on, causing harm, and perpetuating this miserable cycle. Tuning may help defend from a repeat attack of the same phish, but tuning is fundamentally ineffective against the attack that evaded your defenses to begin with. The damage is done. The vendor says "tune it." The attacks keep coming. The cycle continues.

Also, the rate at which threat actors launch phishing campaigns, new domains, URLs, accounts and payloads is accelerating. Over one million new phishing sites are established every month. Attacks launch and shut down in hours. Manually analyzing missed phishing email and tuning email security rules and policies has become a never-ending and ineffective solution for dealing with increasingly agile and sophisticated phishing attacks.

For example, the graph below tracks daily malicious phish evading defenses at one of our typical large enterprise customers. The "spikes" represent high-volume malicious phish days — those days that, without advanced phishing technical controls, the security team finds itself scrambling to react to incidents and unhappy execs.

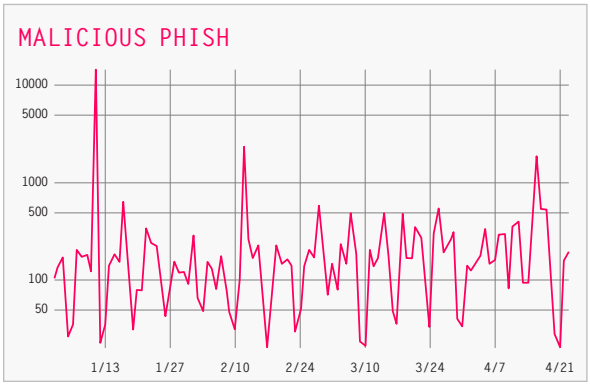

FIG 1: Daily Malicious Phish detections at an Area 1 F500 customer. Without an advanced Anti-Phishing solution, these campaign spikes will consistently drive incident response and manual tuning of defenses.

TUNING TRADITIONAL GATEWAYS AFTER THE FACT DOESN'T WORK.

PLAYING WHACK-A-PHISH IS A WASTE OF YOUR TIME — AND MONEY

Each tuning episode is resource-intensive. Tuning requires security experts to analyze the evasive phishing email, identify malicious characteristics, and manually update email security rules and policies to block a follow on attack.

Here's just a small sample of tuning methods typically employed, and how threat actors respond to defeat tuning:

Attack Type	Typical Manual Tuning Method on the Secure Email Gateway	Modified Attacker TTPs to Bypass Tuning
BEC attack – Display name spoof **E.g. oren@gmail[ ][ ].com instead of the actual exec email oren@area1[ ][ ].com**	Add imposter sender addresses to block list: display name "from", envelope "from" and "reply-to".	Create new email addresses with same Display names
BEC attack – Domain spoof	Add header envelope domain name to block list	Use an alternate sending domain, typo-squatted differently
BEC attack – domain lookalike spoof	Add lookalike domain name to block list	Register new domain name, still resembling proximity to the parent domain
BEC attack – business relevant message content	Create content filters to check for specific words	Modify message text or add spurious text below the eye line to confuse regular expression based content filters
Malicious link in message body	Add URL to block list	Create new URL, use URL shortener, embed URL in attachment
Malicious link in message body leading to payload	Isolate URL link	Credential harvester attack with no active content to execute
Malicious link in message body leading to credential harvester	Isolate URL link, render uncategorized URLs in Read-Only mode	Compromise trusted site to host credential harvesters
Malicious file attachment	Add file hash to block list	Modify file slightly to defeat hash detection
Malicious sending IP	Add sending IP to block list	Initiate same campaign from a different IP; or use ISP networks where subscriber emails can come from separate IP addresses
Brand impersonation attack	Check for SPF / DMARC records on incoming messages and warn on incorrect records	Impersonate domain through typosquatting, use SPF / DMARC compliant providers (eg: Google, Microsoft) to send campaigns out

FIG 2: This is just a sampling of typical techniques used to tune and how they get bypassed by attackers easily.

As an example, recent high profile breaches within Equifax and Capital One immediately prompted bad actors to register hundreds of proximity and new domains related to their breach settlements.

These domains will be used in varying stages and in different campaigns, and there is little chance for anyone to keep up with the specific phishing campaign in play and tune themselves out of those attacks using custom rules in their Secure Email Gateways.

EQUIFAX-RELATED

eligibilityequifaxdatabreach[ ].com
equaifaxbreachsettlement[ ].com
equalfaxbreachsettlement[ ].com
equfaxsettlementbreach[ ].com
equiafaxbreachsettlement[ ].com
equifaxbeeachsettlement[ ].com
equifaxbeechsettlement[ ].com
equifaxberachsettlement[ ].com
equifaxbreachhsettlement[ ].com
equifaxbreachseattle[ ].com
equifaxbreachseattlement[ ].com
equifaxbreachsettiement.net
equifaxbreachsettleemnt[ ].com
equifaxbreachsettlement.us
equifaxbreachstatement[ ].com
equifaxbreachswttlement[ ].com
equifaxbreadsettlement[ ].com
equifaxbreah[ ].com
equifaxbreahcsettlement[ ].com
equifaxbreechsettement[ ].com
equifaxbreechsetttlement[ ].com
equifaxbrreachsettlement[ ].com
equifaxbrwachsettlement[ ].com

CAPITAL ONE-RELATED

capitalonebreachsettlement[ ].com
capitalonefatcs[ ].com
capitalonefaacts[ ].com
capitalsourcingsolutions[ ].com
capitalonebreech[ ].com
capitalonefats[ ].com
capitalonefaccts[ ].com
ccapitalonefacts[ ].com
capitalonesecuritybreach[ ].com
capitalonefscts[ ].com
capitaloneclaim[ ].com
capitalonefavts[ ].com
capitalonegacts[ ].com
capitalnefacts[ ].com
capitalonefacrs[ ].com
capitalonfacts[ ].com
capitalonehack[ ].com
capitalonecompromised[ ].com
capitalonefacs[ ].com
capitalonehacked[ ].com
capitalonnefacts[ ].com
capitaloneacts[ ].com
capitalone-holding[ ].com
capitalonrfacts.[]com

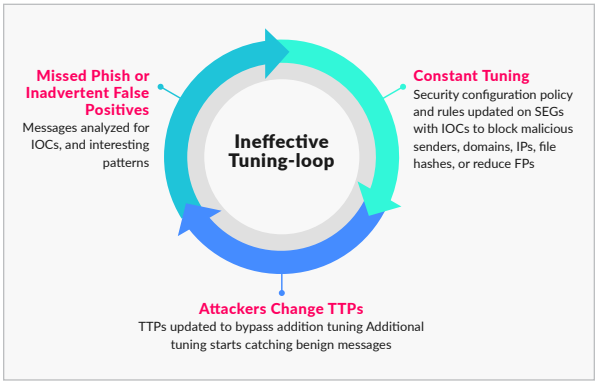

FIG 3: Never ending whack-a-phish loop

This never ending and ineffective tuning loop takes precious time and resources from security teams, along with impacting legitimate business activity as well. Manually tuning is also known to cause an increase in false-positive detections of malicious email and is plagued by human error, creating even more work for security teams.

FORWARD-LOOKING SECURITY TECHNOLOGY

Protection from modern phishing attacks requires a new approach to security.

Traditional email security defenses rely on knowledge of yesterday's active attack characteristics, such as reputation data and threat signatures, to detect the next attack, and therefore can't defend against modern phishing attacks that continually evolve.

What's needed is forward-looking security technology that is aware not only of yesterday's active phishing payloads, websites, and techniques—but also has insight into the threat actors' next moves. Which sites and accounts are they compromising or establishing for use in tomorrow's attacks? What payloads and techniques are they preparing to use in those attacks? Where are they prodding and probing before an attack?

Forward-looking security technology that proactively monitors and analyzes threat actor activity reveals phishing campaigns and infrastructure that are under construction. It can dynamically analyze suspicious web pages and payloads. And it can continuously update analysis and detection models as threat-actor tactics evolve.

Effective protection from modern attacks requires that email security defenses be armed with early visibility into emerging phishing campaigns and infrastructure, and that they use predictive, real-time analysis techniques that can detect new, previously unseen malicious payloads and links — **before** they hit your in-boxes. Not after the fact.

ONLY WITH FORWARD-LOOKING ADVANCE protection and analysis techniques can email security defenses automatically adapt, detect and block modern attacks before the damage is done.

The next time your SEG vendor tells you to "tune" an ineffective, reactive technology, talk to Area 1 to learn about how we protect our customers by delivering the only preemptive, performance-based phishing defense in the industry.

About Area 1 Security

Area 1 Security is the first to bring accountability to cybersecurity. Backed by top-tier investors, Area 1 Security is led by security, Artificial Intelligence, and data analytics experts who created a preemptive solution to stop phishing, the number one cause of cyber attacks.

Area 1 Security works with organizations worldwide, including Fortune 500 banks, insurance, and tech companies, and healthcare providers to realign their cybersecurity posture for combating the most significant risks, protecting customer data, and stopping attacks before they happen. Area 1 Security is a recipient of Inc. Magazine's "2018 Inc.'s Best Workplaces" in America. To learn more about Area 1 Security, visit **www.area1security.com**, join the conversation at **@area1security** or follow the **blog** for the latest industry news and insights on how to stop phishing.

▸ Learn More INFO@AREA1SECURITY.COM