theemaillaundry

Exchange Office 365 G Suite

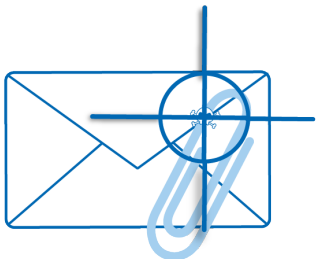
FULL-STACK EMAIL SECURITY

MALWARE IMPERSONATION SPEAR-PHISHING

Dynamic Defense

Powered by Industry-Leading

Threat Intelligence



Attachment Detonation

THE MOST POWERFUL SANDBOX IN THE INDUSTRY

Unknown attachments - including password protected documents - are analyzed in a cross matrix of OS's, programs, and applications for malicious content and behavior.

Impersonation Detection

KNOW WHO YOU'RE REALLY TALKING TO

Domain names, display names, message headers, and content, are all inspected for impersonation tactics, defending against impersonation attacks like CEO fraud.

Advanced URL Defense

CLICK WITH CONFIDENCE

URLs, linked landing pages, and source code are extensively examined for credential harvesting, fake login pages, and other phishing indicators.

91%

OF CYBER ATTACKS START WITH A PHISHING EMAIL

KEY FEATURES

- Cloud-based service - no hardware or software to maintain or install
- Real-time protection from advanced threats
- Unknown attachments are detonated in a sandbox
- Linked landing pages are analyzed to determine intent
- Unknown links are rewritten for time-of-click protection
- Spam and viruses are blocked
- Easy-to-use centralized admin console
- Gray-mail management
- Outbound email scanning
- Email spooling during server downtime

theemaillaundry

Exchange Office 365 G Suite

SANDBOXING TAKEN TO THE NEXT LEVEL

GET PROTECTED

ATTACHMENT DETONATION

Intelligent

multi-vector, multi-stage, & multi-flow

Cross Correlation

The Email Laundry's Attachment Detonation detects more zero-days and unknown malware than all other sandboxes in the security industry combined. Attachments are detonated on over 200 virtual machines in a cross-matrix of operating systems, programs, and applications to detect zero-day exploits and never-before-seen malware.

CATCHES MORE ZERO-DAYS THAN THE REST OF THE INDUSTRY COMBINED

Exploit Detection

Cyber criminals are constantly developing new tactics to gain access to an organization's network in order to steal money and/or data. Unknown exploits like WannaCry and Petya have demonstrated how damaging zero-day exploits can be for organizations. With over 80 file types supported, attachments are opened in a virtual environment, including current and old versions of operating systems, programs, and applications. This enables The Email Laundry to detect and quarantine these never-before-seen attacks.

Password-Protected Attachments

To evade detection by signature and heuristic-based AV engines, attackers commonly password protect their malware-laden attachments, usually including the password in the message body so that the recipient can still gain access. Attachment Detonation overcomes this tactic by scanning both the text and images in the message body, along with using a directory of commonly-used passwords, enabling for the attachment to be opened virtually.

KEY FEATURES

- Detects never-before-seen malware and ransomware
- Unknown attachments are detonated on over 200 virtual machines to observe their behavior
- Even password-protected documents can be detonated if considered to be potentially malicious
- Over 80 file types supported

theemaillaundry

Exchange Office 365 G Suite

KNOW WHO YOU'RE REALLY TALKING TO

GET PROTECTED

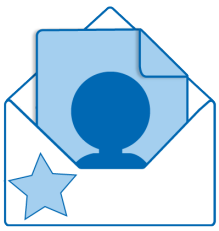
IMPERSONATION DETECTION

PREVENT

SOCIAL ENGINEERING ATTACKS LIKE

CEO FRAUD

Social Engineering attacks like Business Email Compromise (BEC), CEO-fraud and Whaling, use email to masquerade as a high-raking exec, like a CEO or CFO,with the objective of manipulating the recipient into making wire transfers or other transactions involving money and/or data. Impersonation Detection delivers real-time protection against these attacks by utilizing a specifically-designed set of filters, algorithms and machine-learning, to identify all variations of impersonation emails like typo-squatting domains and friendly display names.



Friendly Display & Usernames

Mobile Devices have now overtaken desktops and laptops in terms of email usage, with nearly 70% of email being read on mobile devices. Consistent with this trend, attackers regularly exploit the fact that mail clients on smart phones obscure the full email address of the sender, showing just the sender's Display Name. Simply by having the same display name, an email sent from any email address can appear to come for a trusted source known to the recipient.

Impersonation Detection cross-references both the display name and the username on an incoming email with the list of users at the recipient organization, to determine if a match is found.

Sounds-Like & Looks-Like Domains

Typosquatting has been a popular technique used by cyber criminals for years. By registering a domain name very similar to that of the recipient's organization or an organization familiar to them, attackers can send email appearing to come from a co-worker, or a trusted third party. Spotting the difference between exampledomain.com and exampeldomain.com is extremely difficult for a busy recipient.

Impersonation Detection compares the sending domain name with the recipient domain, and trusted sending domains for similarities, both visually and phonetically.

IMPERSONATION ATTACKS HAVE CAUSED OVER $12.5 BILLION IN LOSSES

KEY FEATURES

- Stops targeted impersonation attacks like whaling, CEO fraud (BEC), & W2 fraud
- Detects emails from "looks-like" and "sounds-like" versions of your domain name
- Protects against spoofed display name & spoofed username attacks
- Email tagging to identify emails from external sources
- CEO fraud algorithms analyze key aspects of the message headers and body to determine authenticity

theemaillaundry

Exchange Office 365 G Suite

CLICK WITH CONFIDENCE

ADVANCED URL DEFENSE

EXTENSIVE

URL & LINKED LANDING PAGE

ANALYSIS

Protecting against phishing and spear-phishing attacks, Advanced URL Defense goes beyond traditional URL inspection by dynamically analyzing links found in the message body, or in an attachment, along with their landing pages. Links are followed to their final destination, even when attackers use sophisticated techniques such as multiple redirects, shortened URLs, or hijacked URLs, to avoid detection. Any files found at the destination URL are detonated to determine if they contain malicious code.

Phish Vision

Phishing attacks commonly contain links to fake login pages for well-known websites such as Office 365, Google Docs, and Dropbox, in an attempt to steal an employee's login credentials. Phish Vision utilizes artificial intelligence to compare the logos and text on these sites with numerous other factors such as its IP address to determine authenticity.

Click Protection

To evade traditional email security services, attackers will regularly wait until an email has been delivered before weaponizing the landing page behind a link. Advanced URL Defense rewrites unknown links allowing them to be checked in real-time as a user clicks on them. Users will be denied access to webpages found to be malicious after delivery.

Newly Existing Domains

Real-Time Blacklists (RBLs) rely on new domain registration lists published by the registrars. These lists are usually released every other day, leaving a 24-48 hour window where new domains and new URLs are unknown to RBLs and the spam filters that use them. Cyber criminals exploit this by launching email attacks immediately after registering a new domain.

The 'NED' look-up allows The Email Laundry to identify domains registered in that initial period, enabling detection of even the first email in a new attack.

76% OF ORGANIZATIONS REPORT BEING VICTIMS OF A PHISHING ATTACK

KEY FEATURES

- Blocks emails containing malicious links in the message body and in attachments
- Unknown links are rewritten to offer time-of-click protection
- Linked landing pages and extensively analyzed to determine their intent