GreatHorn

SPEAR PHISHING REPORT

JANUARY 2017

Today's attackers are smart.

They impersonate your users. They register lookalike domains, write compelling content, and trick your employees into giving up access to their credentials, granting illicit access to your sensitive data, and even into authorizing fraudulent financial transactions. Every week, every month, every year, the number, scope, and damage inflicted by data breaches increases, and despite millions of dollars invested into the cybersecurity industry, large scale breaches just keep coming.

The volume, sophistication, and cleanup costs associated with highly targeted social engineering attacks continue to rise, but detection and defense strategies haven't evolved accordingly.

Attackers have gained an advantage over organizations relying on misguided tactics and outdated tools to defend themselves. IT leaders continue investing billions in perimeter-based security solutions and training to make it as difficult as possible for hackers to gain entry into their networks, but these integrations are complex, highly expensive, and ultimately ill-suited to address the most effective low-volume, hyper-targeted types of attacks that we see today.

The key to stopping these attacks is not "more tools," but rather a shift in mindset. One of the trends we see is that bolstering detection capabilities is more effective when coupled with automated response capabilities and preventive controls, which allow security teams to spend their time understanding and preventing threats categorically rather than being buried in the noise of day-to-day alerts. Statistically, we see that machine-driven security coupled with appropriate end-user engagement at the moment of threat identification reduces security professionals' operational workloads by nearly 90 per cent.

This focus yields even stronger results when not only detection but also response is driven by policy rather than manual action. As information security and IT staff shifts to become a more analytical role, the ability to narrow the time between incident and remediation is key to preventing a major financial or data loss event.

There's no one-size-fits-all point solution.

Attackers are always looking for an edge, and the prominence of social engineering techniques and spear phishing attacks proves that when the rewards are large enough, criminals are willing to invest considerable time into research and development of non-technological threats that will simply bypass yesterday's security infrastructure.

Stopping spear phishing attacks isn't as simple as pushing a button; the sheer volume of these attacks, coupled with the size of the attack surface and IT/Security resource constraints, makes it impossible to mitigate risk solely via human intervention, no matter how much you try to train your end users. A true defense-in-depth strategy for protecting against these attacks requires unified visibility and control, coupled with risk-appropriate automation, across an organization's entire communications infrastructure.

Authentication frameworks can help, but they aren't a silver bullet - and many organizations implement them unevenly, or not at all.

SPF, DKIM, and DMARC aren't necessarily "simple" to implement, but they are a free and essential component of email security that's particularly helpful in preventing brand damage by preventing outbound phishing attacks via impersonation, as well as reducing inbound spear phishing attacks. Even if these frameworks don't stop 100% of attacks, organizations shouldn't miss this low-hanging-fruit opportunity to add a layer of security to their email landscape.

Security can't afford to ignore user experience.

Employee security awareness training efforts have increased over the years, but are often typified by ill-attempted compliance tick-box initiatives that largely waste time and resources. Making end users more cognizant of cybersecurity certainly can't hurt, but "most secure" and "easy to use" are not phrases traditionally found together, and high-stress, deadline-oriented work environments (an apt description for almost all enterprises these days) create situations where employees will either access, transfer or work with data outside even the most thoughtful cybersecurity strategy. Rather than trying to shame and then coach employees, IT leaders should be looking to create a frictionless information security strategy – one that is natively integrated into the workflows of ordinary users and which complements rather than conflicts with technology-centric security investments.

We are at an interesting moment in the evolution of communication technology.

As legacy email technologies are being replaced by their modern, cloud-native successors, new platforms that merge messaging, collaboration, and filesharing are seeing widespread adoption. Where once information technology teams discussed the risks of cloud applications and so-called "shadow IT," entire organizational units are bringing new infrastructure online in minutes, deploying it to improve their efficacy and ability to interact across traditional business lines.

In many ways, we are witness to the beginnings of a shift away from cloud as a means of reducing costs, and towards a new future where the mechanisms of discussion and collaboration will inform not only where we interact, but how.

Unsurprisingly, email remains at the heart of the modern enterprise communication landscape, and given this integral role in core business operations, it is no surprise that the adoption rate of email security technology is nearly 100%. In spite of this deep investment in security, however, the rate of data breach that can be attributed to email security failures is stunningly high; 93% of breaches begin via targeted attacks on executives that originate from business email compromise attacks (BEC) and other forms of threats that legacy technologies cannot detect. In aggregate, those attacks account for over $3.1B in damage annually – a figure revised upward by nearly 30% since 2015 alone.

Why does email continue to be a viable attack vector, and what can organizations do to secure it?

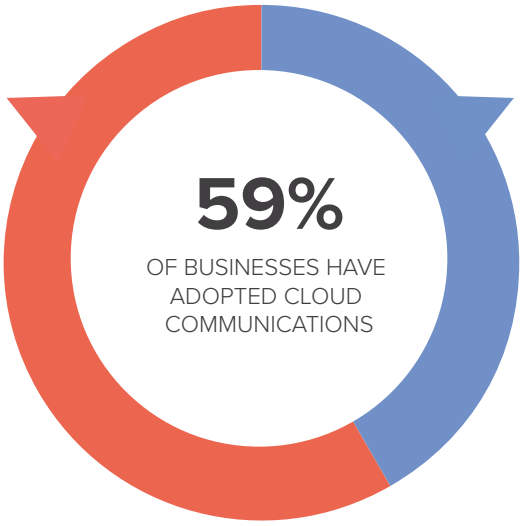
The widespread adoption and interconnection of cloud services plays a significant role. The level of enterprise workloads in the cloud is expected to reach 60% by mid-2018; one in three enterprises now run all their applications in the cloud, and more than half of those who don't are on their way to doing so. The data that moves through these platforms is changing: core business information is now being exchanged over infrastructure that legacy security models cannot account for, especially in the communication space, where gateways and static threat detection are at odds with the systems that business users rely upon.

35%

Office 365

"The number of commercial Office 365 customers has surpassed 70 million monthly active users, and seats grew by 57%."

Source: Microsoft



Source: The Bitglass 2016 Cloud Adoption Report

25%

G Suite

"Google's popularity is higher among smaller companies, approaching a 50% share of companies with revenues less than $50 million."

Source: Gartner

In addition, cybercriminals are becoming increasingly sophisticated (and successful) in their attacks, recognizing that the convergence of non-technical users and externally hosted systems creates an opportunity to use deception and social engineering to extract financial and data gains from companies. Highly targeted, low-volume spear phishing attacks are responsible for 90% of security breaches, and despite the high success rate, cloud email providers and secure email gateways don't protect against these types of payload-free attacks.

In order to effectively secure email in this increasingly connected environment, security professionals must implement a comprehensive security strategy that encompasses all services that touch the company's communications infrastructure. This multilayered threat landscape includes the services that an organization controls directly - such as internal mailboxes - as well as external partners, and third-party services that send mail on an organization's behalf.

What we see today as the systematic set of interaction points between executives, trusted partners, and vendors (email, chat, CRM, web, social, etc.) is incredibly dynamic; one of the challenges facing security teams is thinking not in terms of point solutions for technologies, but rather in terms of the hub-and-spoke model of infosec. This is a view in which data (the hub) is accessed by myriad platforms and products (spokes); security that exists at the center of the model and protects against types of threats becomes a scalable center, whereas products that focus on the deficiencies or vulnerabilities of spoke-level technologies is commoditized at best, and distracting at worst.

Effectively securing the email attack surface requires a risk-management approach to your entire security landscape. By implementing security where it will have the highest return-on-investment — in other words, by identifying the types of risks that most often lead to large or frequent breaches or loss within your industry or across the market as a whole, and automating the detection and remediation of those threats within your email infrastructure — it is possible to interweave security into the systems that most need protection.

"Attackers are striking even more effectively with spear phishing and highly-focused business email compromise (BEC) scams ... these emails are so convincing that they can even bypass the secure email gateway."

– SANS Institute Report, Guarding Beyond the Gateway: Challenges of Email Security (January 2016)

GreatHorn

THE GREATHORN DATA CLOUD

GreatHorn's automated policy-driven engine leverages machine learning to analyze a growing data set comprised of millions of analyzed emails and over 3.5 terabytes of enterprise mailbox data.

GreatHorn's Inbound Email Security platform is focused on detecting modern attacks that operate by exploiting user trust rather than through the delivery of malware or via the transmission of insecure URLs. By natively integrating with cloud email providers like Google and Office 365, the platform is able to perform realtime analysis of message authenticity, based on both authentication data such as SPF, DKIM, and DMARC as well as contextual analysis of mail transmission pathways, sender IPs, domain "look-alike" attack vectors, and indicators of message or domain spoofing.

With hundreds of millions of emails analyzed every week, the breadth and scope of data with which GreatHorn detects threats enables our customers to benefit from the early identification of emerging attack trends, and increases threat intelligence over time.

9 MONTHS OF DATA FROM 2016

91,500 MAILBOXES UNDER PROTECTION

56,513,652 UNIQUE EMAILS ANALYZED

653,447 DOMAINS ANALYZED

773,410 RISKS IDENTIFIED

GreatHorn

SPEAR PHISHING BY THE NUMBERS

Spear phishing attacks are highly customized emails that appear to be from legitimate, well-known sources.

Attackers are increasingly relying on these kinds of highly targeted, non-payload attacks. Rather than trying to fool a message recipient into clicking an unsafe URL or opening a malicious attachment, these low-volume, highly-targeted attacks exploit trust and leverage pressure tactics to trick users into taking action that will put their organizations at risk.

490,557

DISPLAY NAME SPOOFS

An attacker identifies the "friendly" name of a known contact (typically a first and last name) and uses it as the display name in order to fool the recipient into thinking the message came from a trusted source.

44,726

DIRECT SPOOFS

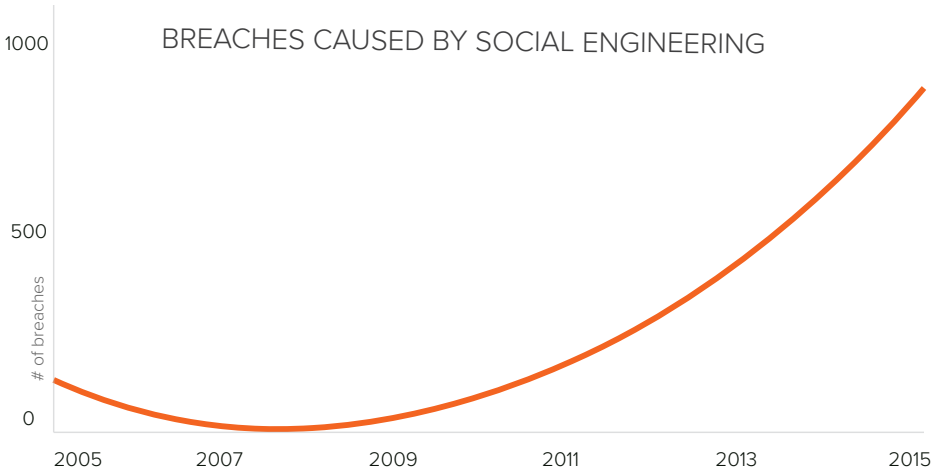
An attacker rewrites SMTP mail headers to send mail with the From:, Return-Path:, and other key email fields manipulated to appear as though a user inside of your domain sent the message.

2,334

DOMAIN LOOKALIKES

An attacker either registers or spoofs a domain name that looks similar to one your organization actually uses, and then sends mail from the faked domain to users inside your real domain.

These types of social engineering attacks continue to result in rising numbers of data breaches - and rising costs.



Source: Verizon 2016 Data Breach Investigation Report

THE AVERAGE CONSOLIDATED TOTAL COST OF A DATA BREACH IS

$4,000,000

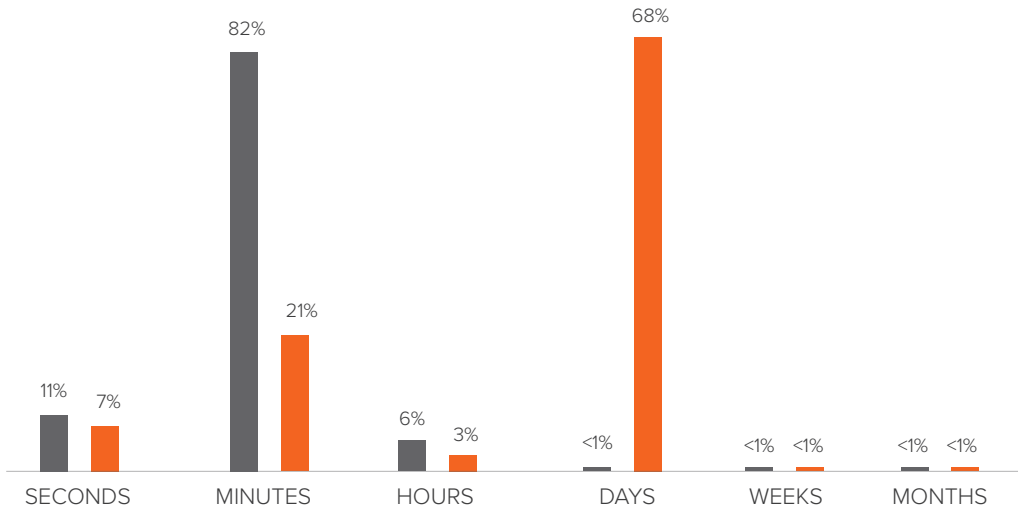
... up from $3.8M in 2015

Source: 2016 Ponemon Institute Cost of a Data Breach Study

Protecting against spear phishing at scale requires automation - not manual intervention.

As attackers move faster and utilize more sophisticated strategies, the windows of time to compromise and exfiltration are shrinking; unfortunately, time to detection is concurrently *increasing* as overburdened security teams struggle to sift through increased volumes of data and potential threats.

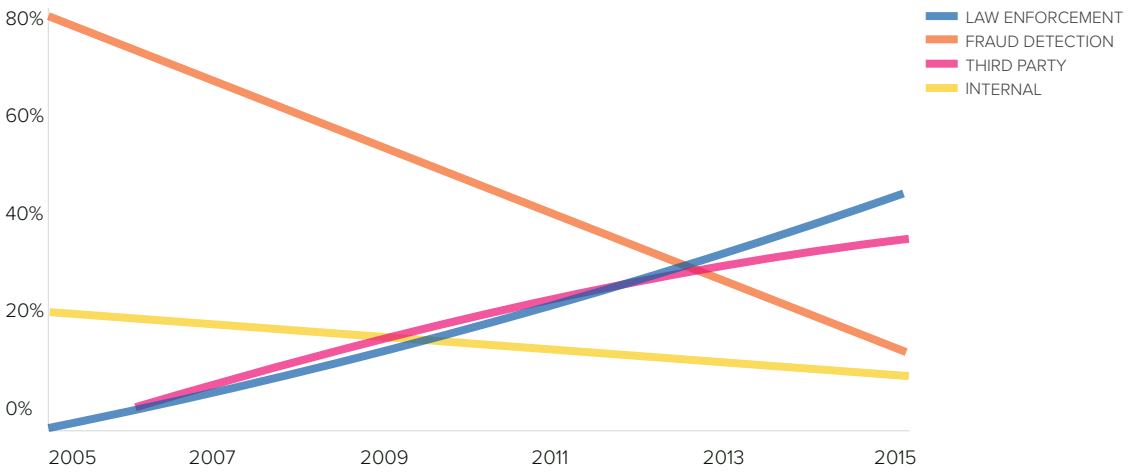
TIME TO **COMPROMISE** AND **EXFILTRATION**



Source: Verizon 2016 Data Breach Investigation Report

As a result, many organizations are notified of a breach by external parties, like law enforcement and third-party partners. The number of breaches discovered internally or through fraud detection methods has declined steadily over the past ten years, and in 2015, less than 20% of breaches were detected via each of these channels.

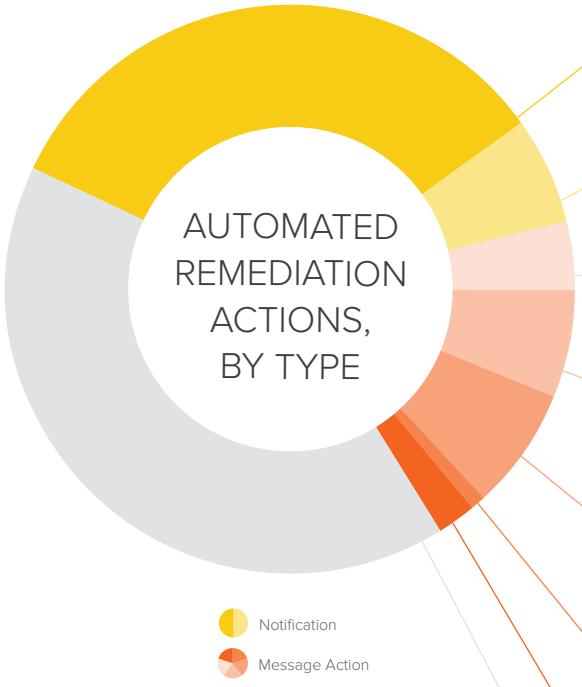
BREACH DISCOVERY METHODS OVER TIME



Source: Verizon 2016 Data Breach Investigation Report

Bolstering detection capabilities is more effective when coupled with automated response capabilities.

GreatHorn enables users to monitor, manage, and create policies, which operate autonomously to protect mailboxes against inbound threats in real time. Policies are combinations of focusing conditions such as attack types, email recipients, senders, content keywords, etc., along with automated actions taken by GreatHorn in response to email events flagged by policies.



33% ALERT ADMIN

Sends a notification email to the administrator when a policy is violated; often used to provide a permanent record of potential threats.

6% ALERT USER

Sends a notification email to the recipient of an email that was identified as a policy violation.

4% ADD WARNING BANNER

Adds a warning message to the top of an email, informing the recipient that the email has been flagged as a potential threat and to proceed with caution.

6% ADD LABEL / CATEGORY

Adds a specified label (Google Apps) or category (Office 365) to an email; often used to provide a browser-based notification to recipients that an email may represent a threat without fully removing it from their inbox.

7% MOVE TO FOLDER

Removes an email from the recipient's inbox and places it in a specified folder; if the folder does not exist, it is created on a per-user basis at the time of the policy application.

1% QUARANTINE

Places an email in a specified Quarantine Folder and requires the intended recipient to review and release the email before replying, clicking links, or opening attachments.

2% MOVE TO TRASH

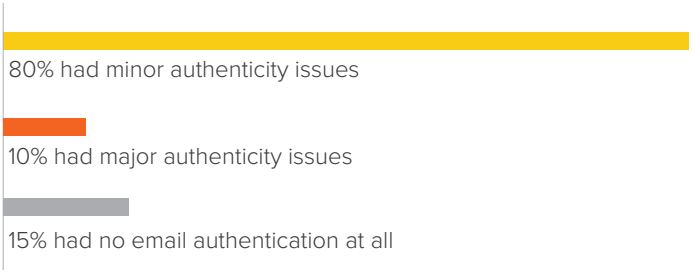
Removes an email from the recipient's inbox and moves it to the Trash.

41% NO ACTION

Email authentication frameworks are an essential (and free!) component of email security - but are often incompletely implemented, or not configured at all.

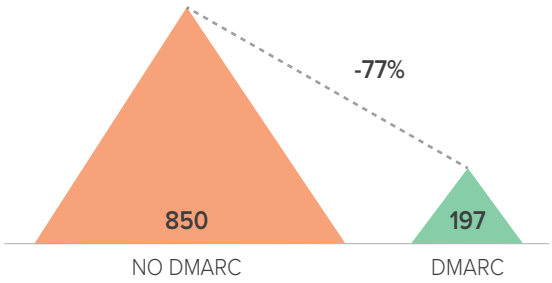
GreatHorn "fingerprints" every sender and recipient whose mail is analyzed by our security platform. Based on these digital fingerprints, authentication and sender anomalies - unexpected patterns of data transmission - can be separated from consistent but expected mail configuration issues. When combined with a robust data set that spans hundreds of millions of senders and messages, authenticity can be used as a major component of risk identification.

OVER 9 MONTHS OF EMAIL TRAFFIC:



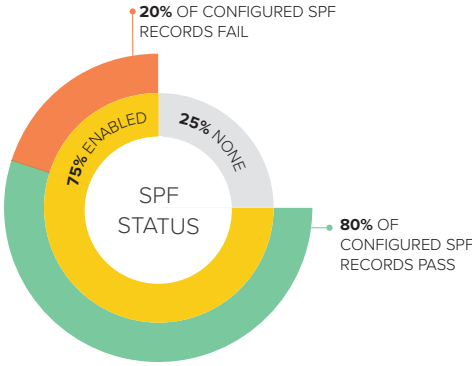
While SPF, DKIM, and DMARC can be incredibly helpful at preventing outbound phishing attacks - where your organization's brand is impersonated to consumers and business partners - it can be difficult to rely on them for protecting against inbound spear phishing attacks (also known as business email compromise or whaling attacks). However, the value of email authentication is clear even under inbound circumstances: within our dataset, organizations with correct and complete authentication records received less than a third of the W2 threats that those without DMARC protection received.

NUMBER OF W2 THREATS RECEIVED

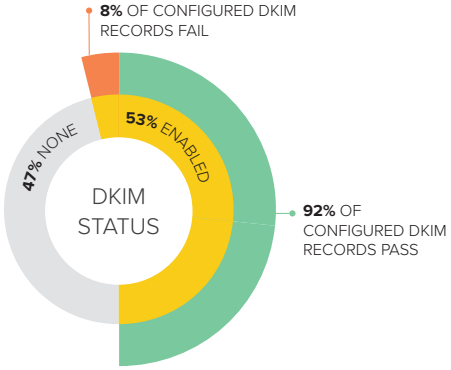


TYPES OF AUTHENTICATION FRAMEWORKS

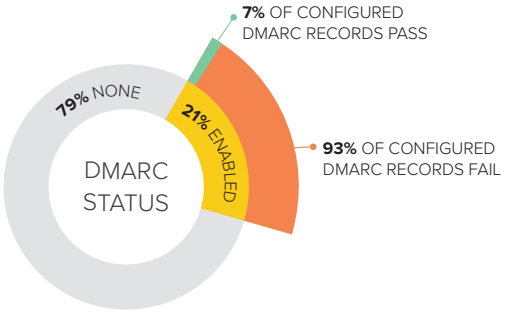
SPF, or Sender Policy Framework, defines what IP addresses are allowed to send on behalf of a domain.



DKIM, or DomainKeys Identified Mail, provides crytographic proof that a message was sent from a specific sender, and that it was not modified in transit to the recipient.



DMARC, or Domain-based Message Authentication, Reporting, and Compliance, checks for alignment between the apparent sender of a message and its SPF and DKIM headers, along with instructions to recipients on handling messages that display misalignment.



ABOUT GREATHORN

Attacks on cloud email, chat, and collaboration tools are responsible for more than 90% of all data breaches. GreatHorn helps companies secure these platforms and communicate with confidence. Built on a foundation of unique intelligence, automation, and cloud-native technology, GreatHorn deploys in minutes, reducing risk and simplifying compliance through a combination of realtime monitoring and policy-driven response.

Cloud-Native

GreatHorn is natively integrated with the world's most popular cloud email platforms - including Google Apps and Office 365 - and provides seamless protection across all devices, clients, and networks.

Rapid Deployment

Deploying GreatHorn takes 15 minutes, and doesn't compromise your organization's existing security and compliance programs by requiring you to change MX records or BCC / copy mail to an untrusted server. You'll start seeing data within minutes of deployment.

Fully Automated

GreatHorn's unique Policy Engine allows you to identify and remediate potential threats 24/7, 365 days a year, instantly removing threats from user mailboxes and alerting security staff, and is compatible with Secure Email Gateways - no additional technology required.

Continuous Protection

With hundreds of millions of emails analyzed every week, the breadth and scope of data with which GreatHorn detects threats and removes false positives is unmatched; insights across the GreatHorn Data Cloud continuously increase threat intelligence.

We are headquartered in Belmont, Massachusetts. To learn more or get in touch:

www.greathorn.com

info@greathorn.com

800-604-2566