REPORT

Q4 2018
Email Fraud & Identity Deception Trends
Global Insights from the Agari Identity Graph™

AGARI

© Copyright 2019 Agari Data, Inc.
The New Realities of Email-Based Fraud & Identity Deception

For all the buzz generated by social media, mobile texting and new messaging platforms, email remains the single most popular and important communications and collaboration tool in modern day life. But email has a gaping security flaw: the ability for anyone to send an email claiming to be someone else.

The Devil is in the Emails

The lack of built-in authentication has opened businesses up to a growing number of phishing, business email compromise (BEC) attacks. The price tag: $12.5 billion and counting. While attacker tactics are growing more sophisticated and ingenious with each new day, they all bare a few similar traits. Almost all email attacks leverage some form of identity deception such as domain spoofing, lookalike domains or complex display name deception techniques combined with social engineering tactics to manipulate recipients into coughing up login credentials or making fraudulent wire payments by making them believe they’re reacting to a trusted source.

Target: Your Customers; the Lure: Your Brand

Just as with many attacks facing businesses, there are no malware-infected attachments to detect, nothing in the email’s code to raise a red flag. Instead, these filchers leverage identity deception and social engineering tactics to exploit the relationships targets have with the brands they know and trust.

KEY FINDINGS:

- **Display Name Deception** was the clear attacker technique of choice for BEC attacks
- **54%** of attacks leveraged impersonated brands in the display name, with Microsoft and Amazon being the brands of choice
- The most comprehensive DMARC adoption snapshot revealed an unprecedented 51% increase in raw DMARC policies over a three month period (though not always with a benevolent intent)
- With a **76% DMARC reject rate**, the US Federal Government is the standout sector for DMARC adoption, followed by Finance and Technology

---

Inside this Report

In this report, we look at trends in email fraud and advanced email attacks against businesses (inbound) and those targeting their customers through domain spoofing and phishing (outbound). The statistics presented here reflect data captured within the Agari Identity Graph from July 1st, 2018 through October 31st, 2018, as well as publicly-available DNS information that can provide a broader context to these trends and what they may mean to businesses and their customers.

Agari is in a unique position to illuminate advanced email attack activity, as our products are deployed in enterprises across the globe as the last line of defense behind secure email gateways or other email security controls. Instead of focusing on email content and infrastructure reputation like most email security solutions, Agari solutions harness advanced machine learning techniques to focus on people, known relationships, and predictable human behavior to detect and stop email-based threats. Agari also has the broadest view into email authentication traffic, commanding the largest volume of domains undergoing DMARC authentication on behalf of customers and email senders.
Table of Contents

Inbound Attack Trends
- The Language of Deceit 6
- Angle of Attack: Display Name Deceptions Dominate 8
- Vertically Challenged: Top Attack Modes by Industry 10
- Fraudsters’ Go-To Disguise: Microsoft is #1 Most Impersonated Brand 11

Outbound Attack Trends
- Best Defense: The Largest Snapshot of DMARC Adoption Rates Ever 16
- Hitting the Sweet Spot: More Domains, Highest Enforcement Levels Win 18
- Parked Domains & Lookalike Factories: Not all DMARC Adoption Rates Are Equal 20
- DMARC Global Sector Analysis 21
- Large Sector Analysis: US Government is a Standout 24
- Enforcement Rates Compared: The Agari Advantage 26
- A Fast Start for BIMI Adoption 27
- A Closing Note: The Importance of DMARC and a Reject Policy 28

About this Report
About Agari Cyber Intelligence Division 29
Inbound Attack Trends
The Language of Deceit

With rising cybercrime representing a serious threat to individuals, businesses and governments, it’s vitally important to establish a consistent set of terms to describe the different challenges that make up this threat. Not every email scam is a “phishing attack,” for instance.

To address this need, Agari has developed a classification system for cyber threats—a threat taxonomy—that breaks down common email-based attacks in terms of how they are carried out, and what the perpetrators aim to achieve. This taxonomy will help readers understand the terms used in this report and what they mean to email security.

Because email fraud centers around identity deception, or the impersonation of trusted senders in order to con recipients, we start with the method by which the impostor impersonates the trusted sender’s email account—making it appear as if the emails the impostor is sending are originating from the trusted party.

For more information about the Agari Threat Taxonomy, see: [agari.com/taxonomy](http://agari.com/taxonomy)
Generally speaking, we observed three primary ways in which cybercriminals impersonate an email account:

**LOOKALIKE DOMAINS AND DOMAIN SPOOFING:** With Lookalike domains, the cybercriminal registers a domain that is very similar to the legitimate domain they’re seeking to impersonate. Lookalike domains are distinguished from domain spoofing, in which the attacker uses the actual email address of the impersonated identity in the From header (e.g. “Company Customer Service” <noreply@company.com>). Email authentication standards, such as DMARC, can be used by a domain owner to prevent spoofing of their domain, but are still not adopted widely by all businesses. Domain spoofing is addressed in Part 2 of this report.

**DISPLAY NAME DECEPTIONS:** The cybercriminal inserts the name of the impersonated individual or brand into the “from” field within Gmail, Yahoo or other free cloud-based email platform. These are also known as a “friendly from” attack.

**COMPROMISED ACCOUNT ATTACKS:** The cybercriminal sends targeted requests from an account that’s already been compromised—assuming the identity and the actual email account of the impersonated individual or brand, which is the most dangerous threat of all.

Different types or classes of attacks will entail different elements of this taxonomy.

A business email compromise (BEC) attack, for instance, can involve an imposter who aims to impersonate a trusted individual or brand using a lookalike domain, display name deception or in the worst cases, a compromised legitimate account, leveraging sophisticated social engineering tactics to send highly personalized attacks. Impersonated individuals may be executives within the target’s own company, or an outside vendor or partner company. A BEC attack targeted and uses a con with no URL or attachment.

By comparison, a phishing attack may use any identity deception technique and send more broad-based messages meant to fool someone into clicking on a malicious link that captures their username and password. When attacking businesses, display name deception is the tactic of choice for cybercriminals seeking to impersonate the email account of a trusted individual or brand.
Angle of Attack: Display Name Deceptions Dominate

When attacking businesses, display name deception is the tactic of choice for cybercriminals seeking to impersonate the email account of a trusted individual or brand.

Imposter Syndrome

During July 2018 through Oct 2018, Agari data indicates 62% of all identity-deception based attacks leveraged display name deception aimed at impersonating a trusted individual or brand (typically an outside vendor, supplier or partner.) This aligns with long-term findings, with display name deception remaining the preferred tactic over lookalike domains and simple domain spoofing.

Breaking this down further, attackers demonstrated a strong preference for impersonating trusted brands versus individuals (54% vs. 8%, respectively). Perhaps this indicates the ease of impersonating generalized email notifications or departmental email vs. the risk that a fraudulent message from a known individual may quickly be spotted.
In either scenario, display name deceptions can be hard for many email systems to detect. For instance, add-on modules designed to enhance detection of attacks on a company’s own top executives can miss attacks designed to impersonate anyone else, whether it’s a trusted lawyer to the company or the electronic document signing system they use.

A successful account takeover not only affords fraudsters the ability to impersonate the account’s owner, but it also gives them access to all of the individual’s contacts, historical emails to craft more targeted cons and more. With a growing marketplace for stolen email login credentials on the dark web, it’s feared this form of attack will become more prominent in coming months.

The data also shows 3% of attacks stemming from compromised accounts that were involved in an Account Takeover. While the percentage of compromised account attacks is small relative to other techniques, this represents a serious vulnerability for the company involved.
Vertically Challenged:
Top Attack Modes by Industry

In most cases, trends align in terms of the forms of identity deception perpetrated against businesses. But there is some variation by industry.

As you can see in the chart below, manufacturing and logistics/transportation industries experienced a disproportionate percentage of attacks leveraging lookalike domains during the third quarter. Transportation businesses captured in the Agari Identity Graph include major airlines. While it’s unclear why attackers would find more success with lookalike domains in these industries, it’s possible the high-value targets they seek are more deskbound than other businesses, making display name deceptions a little harder to pull off.

However, it’s also worth noting that both manufacturing and food processing see the highest number of display name deception attacks impersonating specific individuals of any industries. And when it comes to display name attacks impersonating brands, broadcasting and media see the highest overall volumes within the Agari customer base, followed by manufacturing, education and healthcare.
Fraudsters’ Go-To Disguise: Microsoft is #1 Most Impersonated Brand

It’s true: Microsoft appears to work magic for cybercriminals seeking to impersonate the company’s multitude of sub brands across all forms of attack. But Amazon isn’t far behind.

Maybe it’s OneDrive, Office 365, or just Microsoft as a whole. Whatever the case, fraudsters overwhelmingly impersonate some unit of this major brand when launching email-based attacks. And that’s true whether an attack is targeting personnel at any level of a business or key executives. But on that score, attack preferences deviate from there.
Below is a prototypical example of an attack that leveraged the Microsoft brand and coincidentally bypassed the protections of Microsoft Office 365 Exchange Online Protection:

**Brand Impersonation Attack Example: Microsoft**

![Example Email]

Can’t DMARC Authentication Help?

It’s worth noting that every one of these brands have a DMARC authentication policy of Reject, which would protect their domains from spoofing. Display Name Deception attacks bypass any DMARC authentication controls, and, it seems apparent virtually all secure email gateways. While these brands have taken steps to eliminate their own domains from being spoofed, cybercriminals as still using display name deception to execute phishing and advanced email attacks.

When it comes to targeting employees overall, email attackers impersonate Microsoft 35.87% of the time, followed by Amazon at 26.79%. Think Amazon Web Services (AWS), A9 and even Amazon Prime. Bank of America rounds out the top three impersonations for this broad audience, whether it’s targeting the finance department or the general employee base.
For attacks targeting high-value executive targets, it’s Microsoft by a mile—accounting for 7 out of 10 brand impersonations. Dropbox is a distant second, followed by United Parcel Service (UPS). File sharing services such as Dropbox or OneDrive are a common impersonation targets because they can link to a file with embedded malware and are common within many companies, lowering user scrutiny of the message.

As an example, Agari blocked a targeted Office 365 “Update” email specifically directed at a Chief Intellectual Property Counsel for a major manufacturing firm. For this attack, the attacker’s goal was likely to sit in stealth to silently harvest corporate assets, potentially a company audit report or new corporate M&A activity.

Brand Impersonation Attack Example: Microsoft

<table>
<thead>
<tr>
<th>Brand</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>70%</td>
</tr>
<tr>
<td>Dropbox</td>
<td>10%</td>
</tr>
<tr>
<td>UPS</td>
<td>5%</td>
</tr>
<tr>
<td>VISA</td>
<td>3%</td>
</tr>
<tr>
<td>Amazon</td>
<td>2%</td>
</tr>
<tr>
<td>CHASE</td>
<td>2%</td>
</tr>
<tr>
<td>FedEx</td>
<td>2%</td>
</tr>
<tr>
<td>IRS</td>
<td>1%</td>
</tr>
<tr>
<td>PNC</td>
<td>1%</td>
</tr>
</tbody>
</table>
In most attacks involving these or the rest of the Top 10 most impersonated brands, phishing scams are likely aimed at credentials harvesting, in hopes of hijacking accounts from which to launch more highly-targeted attacks of all kinds, including wire fraud based BEC schemes. Leveraging the vulnerability email gateways have in detecting and mitigating display name deception, attackers attempted to exploit the relationship employees have with trusted major technology and financial brands.

A case in point was the carefully crafted Amazon brand impersonation sent to an AWS admin for a software/SAAS company. This credential phishing attack was especially pernicious given the dependence many enterprises place on web and compute services provided by AWS.

**Brand Impersonation Attack Example:**
**AWS Credential Phishing**

Welcome to Amazon Web Services

Hello,

You have been given access to the AWS Management Console for the Amazon Web Services account ID ending in 4782. You can get started by using the sign-in information provided below.

Sign-in URL: [https://target-prod.signin.aws.amazon.com/console](https://target-prod.signin.aws.amazon.com/console)

User name: [REDACTED]

Your initial sign-in password will be provided separately from this email. When you sign in for the first time, you must change your password.

Sincerely,

Your AWS Account Administrator

**KEY FINDINGS:**

- **Display Name Deception** was the clear attacker technique of choice for BEC attacks
- **54%** of attacks leveraged impersonated brands in the display name, with Microsoft and Amazon being the brands of choice
- When targeting executives and high-value targets at organizations, **Dropbox replaced Amazon as the second-most impersonated brands**
- Compromised accounts continue—the most difficult to address—accounted for **3%** of attacks
Outbound Attack Trends
**Best Defense:**
The Largest Snapshot of DMARC Adoption Rates

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an open standard email authentication protocol that helps businesses protect their brands and domains from being used to send fraudulent phishing emails. In the broadest snapshot ever of 283 Million Internet domains, we break down the state of DMARC implementation worldwide.

**The Domain Spoofing Challenge**

DMARC gives brands the ability to help email receiver systems recognize when an email isn’t coming from a specific brand’s approved domains, and gives the brand the ability to tell the email receiver systems what to do with these unauthenticated email messages. Policy settings include monitor “p=none,” instructing the email receiver system to allow the email to be delivered anyway; “p=quarantine”, which places in the email in the spam folder, and “p=reject,” which blocks the email from ever reaching the inbox. When enforcement policies are set properly, DMARC helps ensure only authorized senders can use an organization’s domain name in emails, and has been shown to drive down phishing rates impersonating brands down to near zero.

For more information on DMARC and the benefits of adoption see: agari.com/dmarcguide
During the analyzed period, Agari captured an unprecedented view into the state of DMARC adoption rates and enforcement policies by crawling the entire public Internet domain space representing over 283 million domains, generating a snapshot of DMARC implementation rates worldwide. Agari took a snapshot in July, 2018, followed by a snapshot of the data in October, 2018.

KEY FINDINGS:

- **Increased Adoption:** In our examination of more than 283 million domains, Agari identified 3.5 million domains with valid DMARC records in July. That count rose to 5.3 million domains in October, representing a 51.4% gain in DMARC record observances.

- **The Vast Majority of Records Belong to .coms:** Internet domains tied to business and ecommerce contain DMARC records. Interesting to note that the category most associated with brand impersonation—.edu domains—have the fewest number of domains with DMARC records of all sectors.

- **Significant Growth Observed in Strongest Enforcement Setting:** The bulk of the changes are generated by domains for which DMARC policies have been changed to the highest possible enforcement level, “p=reject”. This category of policies nearly tripled from under 400,000 to 1.1 million from July to October.

- **But Not All DMARC Domains Send Email:** As we’ll discuss in more detail later on, none of this means that several hundred thousand emailsending domains have suddenly become more secure. On the contrary, any number of domains could have been registered in bulk and simply had reject policies assigned.
Hitting the Sweet Spot: More Domains, Highest Enforcement Levels Win

An early avenue of investigation into our dataset was to get a read on how vendors and DMARC service providers are helping organizations use DMARC to protect their domains from email impersonation scams. The size of our dataset offers a unique view into the number of domains for which vendors have established DMARC records as well as how many of those records have been set to the highest enforcement level (p=reject). This combination of data points offers a snapshot of market share and success rates for each of these vendors.

Unprecedented Insight into Vendor Standing

As a shorthand to determining a market share figure, we tabulated the number of times specific well-known DMARC implementation vendors were specified as a recipient of reporting feedback via DMARC. The “rua” field that accepts an email address to receive aggregate DMARC data reports is a good proxy for this calculation. With this email address, the DMARC vendor typically accepts, parses, and visualizes the data on behalf of the customer. We included active vendors with more than 1000 domains reported.
The following table shows a basic ranking of top vendors, corresponding to the number of domains that specify that vendor in the rua field. We then applied a second filter indicating the all-important percentage of domains at the highest possible DMARC enforcement policy (p=reject) for each vendor, which is the policy level that will block phishing messages.

**KEY FINDINGS:**

- **Enforcement rates vary widely by vendor.** Having a high enforcement rate should be a key criteria for selecting a vendor. Enterprises with hundreds or thousands of domains should consider vendors who have both high numbers of domains and enforcement rates.

- **Higher Quantities Can See Lower Enforcement Rates:** Mid-tier vendors tend to struggle with the ratio of domains they service and what percentage of those records they succeed at converting to the highest enforcement policies. That's true whether the total universe of domains they service is numerous or sparse.

- **The Goldilocks Ratio:** Category-leading vendors achieve that perfect combination of a large number of domains serviced across a wide range of industries matched with high levels of top enforcement policy implementation.
Parked Domains & Lookalike Factories:
Not all DMARC Adoption Rates Are Equal

It’s important to note that not all domains with DMARC records are intended to send email and ensure an authentic stream of communications.

Agari observed many examples of dubious or tangential use of DMARC configurations, which goes a long way to explain the growth in raw policies we witnessed in Q3 2018. For example, during the course of our analysis, Agari tracked substantial movement among domain registrars or domain monetization companies which, as a matter of business process, configured DMARC records. For example, one firm, Team Internet, registered over 100,000 incremental domains over the course of the analyzed period, all of which had DMARC records. Another registrar based out of Russia, snbox.ru, registered over 300,000 new domains, all set to a p=reject policy. Many of these domains were very similar (or lookalike) domains to common and well-known brands, such as the Internet bandwidth site “speedtest” or the popular gaming site “Kongregate.” Our hypothesis is that for these domain monetization firms, it’s likely best practice to ensure that domains of this ilk do not end up on takedown sites, IP reputation blacklists or being used by cybercriminals in phishing scams, hence the strategy to assign a DMARC reject policy to the domain.
DMARC Global Sector Analysis: Fortune 500

As we have done in the past, we looked at publicly available adoption data for the Financial Times Stock Exchange 100 (FTSE 100), and Australian Securities Exchange 100 (ASX 100) to gauge adoption trends among prominent global organizations across geographies.

Our additional research indicates that, across the board, the largest corporations around the world have in fact made strides with email authentication. However when considering the prevailing proportion of “no record” and “monitor-only” policies, the state of implementation is leaving their customers, business partners and brand vulnerable to phishing and the losses associated with email fraud.

Almost 87% percent of the Fortune 500 are vulnerable to phishing, leaving their customers, employees and brand name exposed to a fraud. The Fortune 500 are the largest, most well-known and most trusted companies in the United States. Unfortunately, DMARC adoption is dangerously low within the Fortune 500, enabling malicious actors to abuse that trust and leaving corporations unprepared to prevent it.

DMARC Adoption – Almost half (49% percent) of the Fortune 500 have not published any DMARC policy. This is, however, an improvement over the previous year, in which two-thirds (67%) of the Fortune 500 had no DMARC policy.

Quarantine Policy – Only five percent have implemented a Quarantine policy (Spam folder)

Reject Policy – Only 8 percent have implemented a Reject policy (Blocked). This is an increase of over 3 percent from the previous period.
DMARC Global Sector Analysis:
FTSE 100

The Financial Times Stock Exchange 100 Index, more commonly known as the FTSE 100, is a share index of the top 100 companies listed on the London Stock Exchange (LSE) and is seen as the ‘goto’ reference for those seeking an indication on the performance of the major companies listed in the United Kingdom.

Adopting the same methodology as referenced from the Fortune 500 analysis, it reveals that, similarly to the United States, the majority of the top 100 United Kingdom public companies do not have a DMARC record for their corporate domain. The lack of implementation of DMARC within an organization exposes the business not only to the potential for fraud but also a data breach, and all the public reputational and financial penalties that are associated with an incident, while simultaneously eroding the faith that employees and customers have in the brand.

DMARC Adoption - Over half (56 percent) of the Financial Times Stock Exchange 100 have not published any DMARC policy, which represents an 11 percentage point increase over the previous period.

Quarantine Policy - Only one percent have implemented a Quarantine policy (Spam folder). This percentage is unchanged from last year.

Reject Policy - Only nine percent have implemented a Reject policy (Blocked).
DMARC Global Sector Analysis: ASX 100

The ASX 100 is Australia’s stock market index, representing its top 100 large and mid-cap securities.

With just under a third of Australian businesses having taken, at a minimum, the first step in adopting DMARC to combat the threat of digital deception, it is evident that a high level of education still needs to be undertaken in this market.

**DMARC Adoption** – Almost two-thirds (60 percent) of the Australian Securities Exchange (ASX 100) have not published any DMARC policy.

**Quarantine Policy** – Only one percent have implemented a Quarantine policy (Spam folder).

**Reject Policy** – Only seven percent have implemented a Reject policy (Blocked), which doesn’t amount to an increase from last year’s 3% reject rate.
Large Sector Analysis: US Government is a Standout

An additional avenue of analysis from an overall DMARC adoption trend perspective was to examine public DNS records for primary corporate and government website domains of large organizations with revenues above $1B.

We compared these statistics to the United States government domains, which were the subject of a high level, top-down mandate in 2017 to implement security controls, with DMARC enforcement being a key component. As the chart below shows, when viewed from a DMARC policy attainment perspective, the US Government could be the poster child for a sector-wide DMARC implementation success story. When looking at DMARC enforcement (or domain policies with a p=reject or block configuration), the US Government is the clear leader with 76% of its in-scope domains at an enforcement policy.
The reject or enforcement policy ensures that mailbox providers block any malicious emails from spoofing an organization’s brand or domain name. It’s telling that the government’s progress far outpaces dominant business-to-consumer sectors such as retail and healthcare, for example, which depend on a trusted communication channel to their customers. The Finance industry, which has the highest adoption and reject other than the U.S government, was an early adopter of DMARC and has historically been a top target for initial phishing attacks. Yet, in only one year, driven by the BOD 18-01 mandate, the US federal government was able to far surpass all other sectors.

For more information on the BOD 18-01 and a detailed analysis of federal agency progress and policy attainment, see: [agari.com/fedreport](http://agari.com/fedreport).
Enforcement Rates Compared:
The Agari Advantage

To see how enforcement rates across industries compared with those of Agari customers, we looked at the data from the Agari Email Threat Center.

The Threat Center provides real-time aggregate DMARC statistics from Agari customer data, which is the largest set of detailed DMARC data in the world based both on email volume and domains. In effect, given Agari’s broad customer base, the Agari Email Threat Center can consolidate and aggregate all DMARC statistics from the domains of top U.S. banks, social networks, healthcare providers, major government agencies and hundreds of other organizations. It analyzed more than 571 billion emails over 16,000 domains in Q3 2018.

Using the same industry grouping cohorts presented in the previous section, we compared the respective enforcement levels for each vertical category with Agari customers. Matching the larger industry dynamics we reported, the government sector (heavily weighted towards US government) took top prize for enforcement levels within the Threat Center rankings. Following this sector, healthcare and technology were tied as the next-ranked vertical for the percentage of domains at enforcement.

Notably, Healthcare as a vertical moved from the lowest enforcement rate in the Threat Center to this second-ranked position. It’s notable that following much publicized Binding Operational Directive (BOD) 18-01 which sheparded in the DMARC attainment process for the US government, the Health Care ISAC issued a companion “pledge” for member organizations to similarly adopt the standard.

Percentage of Domains at Enforcement

Note: The Threat Center tracks authentication statistics across active domains belonging to Agari’s customers. Passive or defensive domains that don’t process email will not be reflected in the totals. Overall, as indicated previously, the Agari reject rate across all industries in the global domain snapshot is 82%.

More Resources:
To see detailed industry authentication statistics and trends, visit agari.com/threatcenter
For more information on the NH-ISAC DMARC pledge and healthcare adoption, visit agari.com/healthreport
For the latest on US Government adoption and BOD 18-01, visit agari.com/fedreport
A Fast Start for BIMI Adoption

Brand Indicators for Message Identification (BIMI) is a standardized way for brands to publish their brand logo online. It lets the logos be easily incorporated into messaging and social media applications. BIMI does this with built-in protections that safeguard the brand, application providers, and consumers from impersonation attempts.

For instance, a bank could use BIMI to display its logo next to its messages—providing brand exposure as well as an assurance to recipients that the message really did come from that bank. BIMI will work only with email that has been authenticated through DMARC standard and for which the domain owner has specified a DMARC policy of enforcement (so only authenticated messages can be delivered).

Based on our Q3 dataset, Agari determined that BIMI adoption reflected 48 distinct brands or email-sending domains. Given the promise of the proposed standard, which delivers free brand impressions to organizations combined with the boost in email trust, we expect this figure to grow in subsequent quarters.

For more information on BIMI, visit brandindicators.org

Oct 2018 DMARC Domain Snapshot
A Closing Note: The Importance of DMARC and a Reject Policy

The importance of a well-configured DMARC enforcement policy with a p=reject blocking policy on all domains cannot be overstated.

Below is an example of a customer experience over the course of Q3 2018. This customer, a global, publicly traded ecommerce firm, was receiving a tremendous volume of phishing and unauthenticated emails—at times more than 100 million per day impersonating its brand. These emails were being viewed by existing and potential customers, spoofing the company domain in the “From:” header of emails.

At the end of the day on September 26th, 2018, the customer implemented a DMARC Reject policy, resulting in millions of spoofed messages that were no longer being delivered. Specifically, in the days following the configuration change, 99% of fraudulent/unauthenticated messages were immediately blocked, unviewed by the intended victims.
About this Report

This report contains metrics from data collected and analyzed by the following sources:

**Inbound Threat Data:**
For inbound threat protection, Agari uses machine learning—combined with knowledge of an organization’s email environment—to model good or authentic traffic. Each message received by Agari is scored and plotted in terms of email senders’ and recipients’ identity characteristics, expected behavior, and personal, organizational, and industry-level relationships. For the attack categorization analysis, we leveraged anonymous aggregate scoring data that automatically breaks out identity deception-based attacks that bypass upstream SEGs into distinct threat categories, such as Display Name Deception, Compromised Account, and more.

**Global Domain Snapshots:**
For broader insight into DMARC policies beyond what we observed in email traffic targeting Agari’s customer base, we obtained and analyzed two large snapshots, representing virtually all the publicly accessible domains in DNS over the course of Q3.

<table>
<thead>
<tr>
<th>DATE OF SNAPSHOT</th>
<th>SNAPSHOT 1</th>
<th>SNAPSHOT 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF SNAPSHOT</td>
<td>JULY 2018</td>
<td>OCTOBER 2018</td>
</tr>
<tr>
<td>TOTAL DOMAINS CRAWLED</td>
<td>245,146,357</td>
<td>283,237,541</td>
</tr>
<tr>
<td>RAW DMARC POLICIES OBSERVED</td>
<td>3,293,505</td>
<td>5,315,514</td>
</tr>
</tbody>
</table>

Over the course of this period, our base domain list increased by 38 Million, mostly in newly detected country code top-level domain (CCTLDs.) These snapshots will form the basis for trend tracking in subsequent reports.
Agari Threat Center:

The Agari Threat Center continually aggregates anonymized DMARC reporting data that we track over our customer domains in several industry sectors. Over the period of this report, over 576 trillion emails were visible to the Agari Threat Center, traversing over 14,200 top level and subdomains. Visit agari.com/email-threat-center/ to explore authentication results across various verticals and timeframes. To maintain complete confidentiality, the Threat Center database does not store company-specific information of any kind. Threat Center data is primarily representative of business to customer (B2C) email for the countries and industries in which we have significant market penetration.

In order to compare and contrast the global DMARC insights provided by our domain snapshots with the data tracked by Agari, we grouped public data into corresponding vertical categories represented in the Agari Threat Center. Note that for other analysis, such as the Fortune 500, US federal government, and large industry sections, we obtained the domain names from public sources and determined DMARC authentication status using Agari lookup tools.
About Agari Cyber Intelligence Division

The Agari Cyber Intelligence Division (ACID) is the only counterintelligence research team dedicated to worldwide BEC and spearphishing investigation. ACID supports Agari’s unique mission of protecting communications so that humanity prevails over evil. ACID uncovers identity deception tactics, criminal group dynamics, and relevant trends in advanced email attacks. Created by Agari in 2018, ACID helps to impact the cyber threat ecosystem and mitigate cybercrime activity by working with law enforcement and other trusted partners.

Start with a Free Assessment of Your Email Environment

Get a free, personalized audit of your organization’s inbound and outbound email security posture including:

- Comprehensive breakdown of identity-based attacks bypassing your email gateway
- DMARC authentication trends
- Identification of phishing using your domains
- Discovery of services sending email on your behalf
- Recommendations to improve deliverability and security

Sign Up agari.com/freeaudit

Visit the Agari Threat Center

To see up-to-date global and sector-based DMARC trends across the Agari customer base, go to: agari.com/threatcenter