AGARI CYBER
INTELLIGENCE DIVISION

REPORT

Q1 2020

Email Fraud & Identity Deception Trends

Global Insights from the Agari Identity Graph™

agari
by HelpSystems

Executive Summary

Why attack hardened computer systems when it's so much easier to hack human nature? The tactics employed in phishing attacks, business email compromise (BEC) scams, and other advanced email threats continue to shape shift, pummeling US businesses with attacks that lead to more than $700 million in losses each month. As the latest quarterly analysis from the Agari Cyber Intelligence Division (ACID) affirms, the success of these attacks is growing less dependent on technical prowess, and more on sophisticated forms of identity deception and advanced social engineering techniques. As infuriating as it may be, the brilliantly simple, expertly-crafted email messages used to dupe corporate employees into surrendering sensitive information, revealing login credentials, or paying for fraudulent invoices or gift cards grow more effective by the day.

62% of BEC Scams Target Gift Cards During the Holiday Season

Gift cards continue to be the preferred cash-out method in BEC scams, accounting for 62% of such attacks from October through December 2019. Possible seasonal patterns have emerged in the types of gift cards requested. Google Play narrowly retained its status as the #1 most requested gift card, dropping from 27% share to 16%, while cards from Target, BestBuy, Sephora, and other retailers saw major increases in demand. Attackers may be capitalizing on office gift giving to launder stolen cards through physical goods rather than through traditional channels such as cryptocurrency exchanges. During the last two weeks of the year, BEC attacks were also 63% lower than the average seen during the rest of the quarter—indicating scammers go on holiday, too. SEE MORE ▶

Employee-Reported Phishing Attacks Saddle SOCs With 60% False Positives

While tools that enable employees to report suspected phishing attacks can provide crucial data on attack modalities, the sheer volume of reports often swamp Security Operations Centers (SOCs) with more incidents to triage, investigate, and remediate than they can handle. Our Q1 2020 ACID Phishing Response Survey of large organizations across six industries reveals that this problem is compounded by the fact that 60% of those employee-reported incidents turn out be false positives. But organizations implementing advanced phishing response workflows to identify the full scope of phishing attacks report the detection and remediation of 44X more emails related or similar to those manually submitted by employees. SEE MORE ▶

Despite Gains in DMARC Adoption, 85% of Fortune 500 Remain Vulnerable

DMARC adoption rates climbed 83% over the course of 2019, with 11,698,125 domains identified with recognizable DMARC policies worldwide. Yet while encouraging, this represents just a tiny fraction of a total universe of more than 366 million domains globally. And despite some measured progress, 85% of the Fortune 500 remains vulnerable to cybercriminals seeking to hijack their domains for use in phishing-based brand impersonation scams that put their customers, partners, investors, and the general public at risk of significant financial damage. SEE MORE ▶

Inside This Report

The statistics presented in this report reflect information captured via the following sources from October through December, 2019:

Active defense engagements with cyber threat actors to **collect intelligence** about emerging BEC tactics and targets

Data extracted from **trillions of emails** analyzed and applied by Agari Identity Graph™

DMARC-carrying domains identified among **366 million+ domains** crawled worldwide

Analysis of incident data from SOC professionals at **six large companies** spanning multiple industries

ACID is the only counterintelligence research team dedicated to worldwide BEC and spear-phishing investigations and the identity deception tactics, criminal group dynamics, and other relevant trends behind today's most advanced email threats. Created by Agari in 2018, ACID helps to mitigate cybercriminal activity by working with law enforcement and other trusted partners.

Table of Contents

Employee Phishing and Business Email Compromise Trends

KEY FINDINGS

Gift cards were the preferred cash-out mechanism in **62%** of all BEC scams during the fourth quarter of 2019, up from **56%** during the previous quarter.

Google Play remained the most-requested gift card in BEC attacks, but cards from eBay, Best Buy, Sephora and other retailers selling physical goods rose during the holiday season.

As attacks impersonating trusted brands continued to decline, **32%** of advanced email attacks now spoof specific individuals, compared to just 12% in the first half of 2019.

Imposter Syndrome

68% of Attacks Impersonate Brands or Individuals, But Tactics Are in Flux

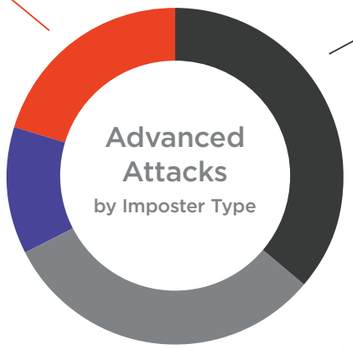
Cybercriminals continuously modulate the identity deception tactics they use in phishing and BEC scams to optimize attacks netting the best results. In keeping with recent trends, attacks impersonating specific individuals climbed 10% during the fourth quarter of 2019, accounting for 32% of all advanced email threats—bringing these attacks in closer parity with those impersonating trusted brands. While the drivers behind these shifting dynamics may vary, the upward trajectory of business losses they generate remains stubbornly recalcitrant.

The Deception Proves the Rule

Today, 68% of all phishing attacks employing identity deception techniques use display names meant to fool recipients into believing they're from a known and trusted brand or individual.

In the aggregate, this highlights the outsize role display name deception plays in a growing number of advanced email attacks. But the exact balance of these deceptions is far from static.

From October through December, 36% of all phishing attacks impersonated a well-known brand in the initial email, down 6% from the previous quarter. But those impersonating individuals accounted for 32% of all attacks. That's up from just 12% in June—a 2.6X increase in only six months.



20%
Look-alike Domain

From: LinkedIn <noreply@liinkediin.com>
To: Jan Bird <jan.bird@gs.com>
Subject: Diana has endorsed you!

36%
Display Name Deception (Brand)

From: Chase Support <chase@gmail.com>
To: Tom Frost <ffrost@amazon.com>
Subject: Account Disabled

12%
Compromised Account

From: Raymond Lim <rlim@contoso.com>
To: Cong Ho <cho@contoso.com>
Subject: PO 382313

32%
Display Name Deception (Individual)

From: Patrick Peterson <Patrick Peterson [hackyjoe@gmail.com]>
To: Cong Ho <cong@agari.com>
Subject: Follow up on Invoice Payment

The Method to Their Madness

Generally speaking, current trends in identity deception tactics support observations shared in our Q4 2019 report. At the time, we noted that rising levels of phishing emails impersonating trusted individuals, combined with a lower percentage of attacks masquerading as well-known brands, may portend a period of heightened risk from savvier, social engineering-based attacks.

That's because scams masquerading as brands are typically linked to credentials-harvesting attacks, while those impersonating individuals are largely associated with more sophisticated BEC scams. This is especially true when perpetrators are seeking gift cards as the cash-out method. After all, companies don't typically ask an admin or rank-and-file employee to purchase gift cards outside of regular procurement processes—people (and their imposters) do.

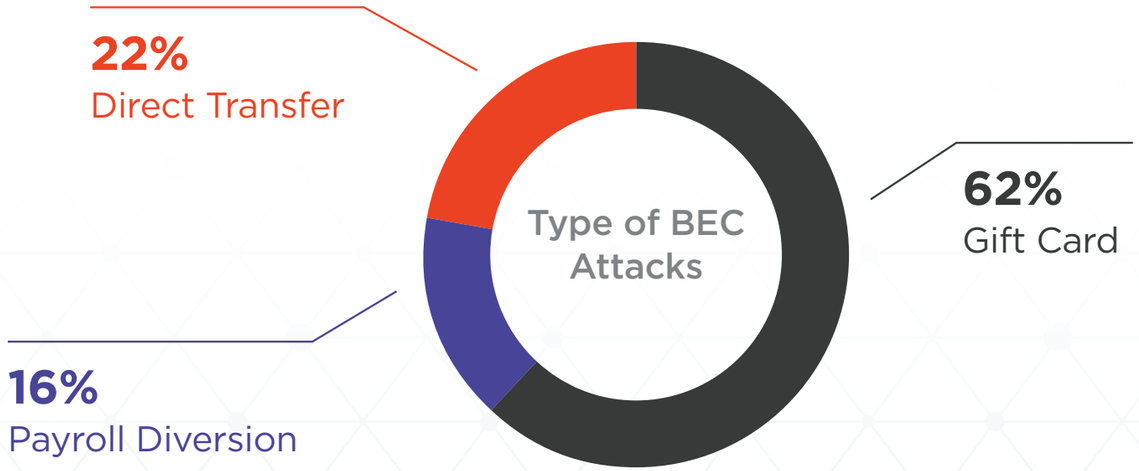
BEC Breakout Session

Gift Card Cash-Outs Gain Traction (and Twists) During the Holiday Season

While an email scam that successfully manipulates corporate employees into wiring payment on a fraudulent invoice may net more loot per attack, gift cards remain BEC's biggest cash cow.

It's easy to see why. Since the ruse involves asking an employee to purchase gift cards for colleagues, victims are much less likely to inform others about the request—especially during the holiday season. Perpetrators are free to phish multiple targets within the same organization, boosting the size of their potential bounty. And it's nearly impossible to track down gift cards, let alone recover the proceeds stemming from them.

During the last three months of 2019, gift cards were requested in 62% of all BEC scams, compared to 56% during the previous quarter, which is hardly surprising given the season. As the same time, the percentage of schemes seeking direct wire transfers rose to 22%, up from 19% quarter-on-quarter, while payroll diversions slid nearly 9% during the same period.



Numbers Game: Looking for a $700 Million-a-Month Solution

During the last three months of 2019, the average dollar amount for gift cards requested in BEC scams reached just over $1,600, compared to more than $55,000 for attacks seeking wire transfers. To put these numbers into perspective, companies have lost $26 billion to BEC in all its forms in just the last three years, according to the FBI. That's $700 million in business losses each month. As the Association of Financial Professionals reports, wire transfers account for roughly 43% of those losses. With gift card scams making up most of the rest, it's clear this particular approach is dependent on reach, volume, and attack tempo.

Amount Requested Per BEC Attack Type

BEC Attack Type	Average	Quarterly Change	Median	Quarterly Change	Minimum	Maximum
Gift Card	$1,627	+3%	$1,200	+20%	$250	$10,000
Wire Transfer	$55,395	+5%	$28,350	+13%	$2,550	$680,456

It's not like wire transfer schemes are growing less costly, either. Though modest on a quarter-over-quarter basis, even incremental increases in the average amounts requested in these crimes are troubling.

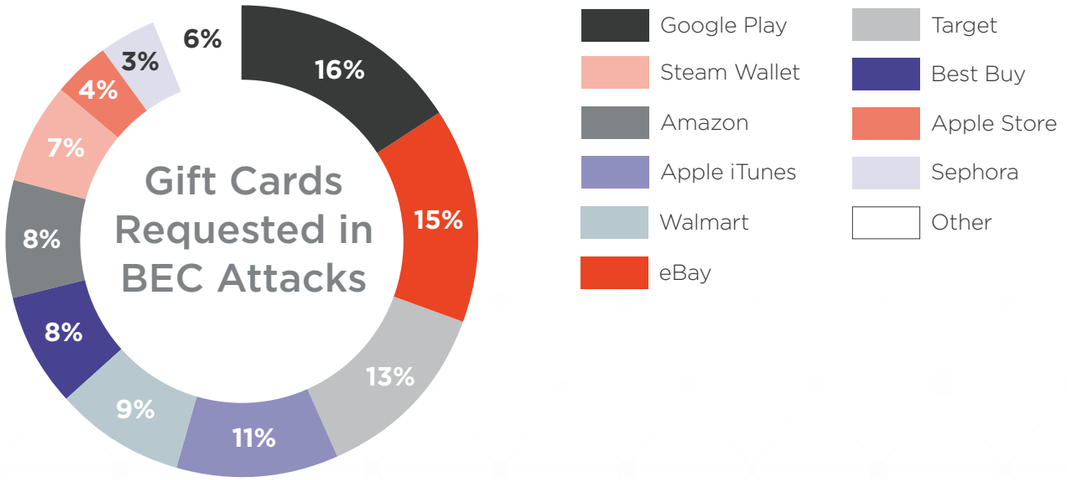
In recent months, ACID analysts have uncovered vexing developments in attack strategies. Where once fraud rings might seek to defraud a business with bogus invoices, they are now infiltrating email accounts within one organization to attack organizations throughout its entire supply chain ecosystem in attacks we have named Vendor Email Compromise (VEC).

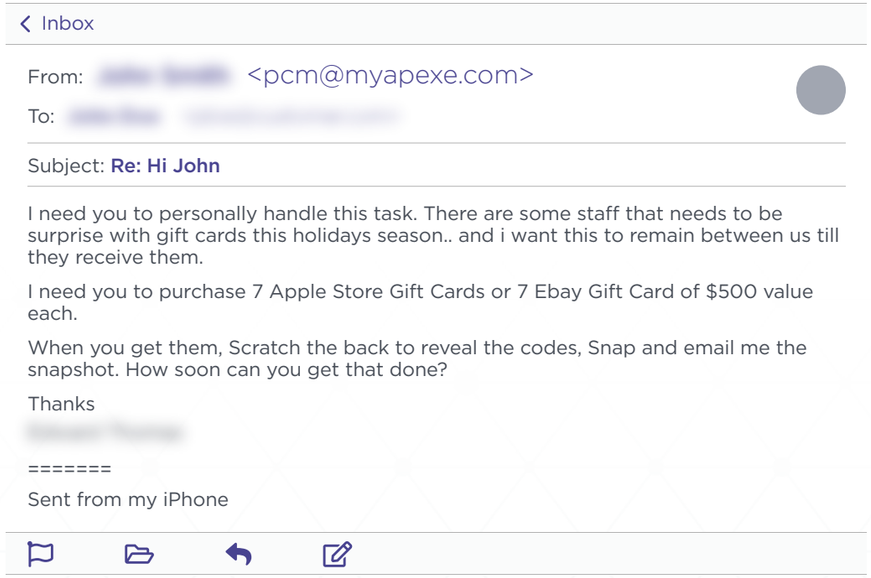
Threat actors within a cybercrime ring we call Ancient Tortoise, for instance, work to compromise aging reports from accounts payable teams and then launch attacks on the company's entire customer base using fraudulent invoices or requests for changes to payment details.

Gift Card Cash-Out Requests Do the Holiday Shuffle

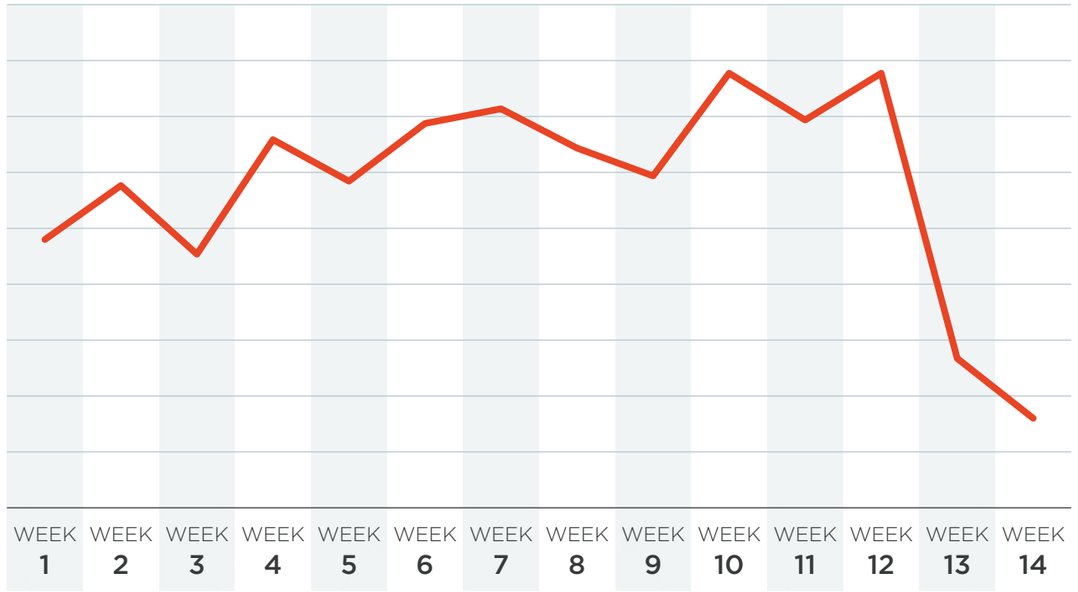
Given the holiday season, an increased emphasis on gift cards as the preferred method for cash-outs makes perfect sense. There were also some notable shifts in the types of cards sought by fraudsters.

Google Play narrowly retained its status as the most requested gift card in BEC schemes, but its share dropped from 27% to just 16%. Requests for gift cards from eBay nearly tied Google Play (16%), while cards from Target (13%), Walmart (9%), and BestBuy (8%) all saw significant increases in demand. Seasonal timing and the fact that these online retailers sell physical goods suggests scammers may have been looking to launder proceeds from stolen gift cards through tangible merchandise, rather than through traditional channels such as cryptocurrency exchanges.





Bad Santa Hits the Brakes: BEC Attacks Drop 63% in Q4's Final Weeks



The shuffled mix of gift cards requested in BEC scams wasn't the only thing in flux during Q4. The cadence of BEC scams that have long targeted specific times and days within the workweek also took on a seasonal turn. During the weeks leading up to Christmas and New Year's, attacks fell 63% from the average seen during the rest of the quarter. With many employee targets out of the office, scammers either sought out other avenues of attack, or took some holiday downtime of their own.

Nearly 60% of BEC Scams Use Free Webmail, But Roadrunner Hits a Wall

One of the things that makes BEC attacks so outrageous is that they can wrest billions in ill-gotten gains with very little effort or overhead. In the vast majority of cases, the culprits use free or temporary webmail accounts to launch their malicious campaigns. During the fourth quarter of 2019, for instance, our data shows 57% of all BEC emails were sent from an easily-acquired webmail account.

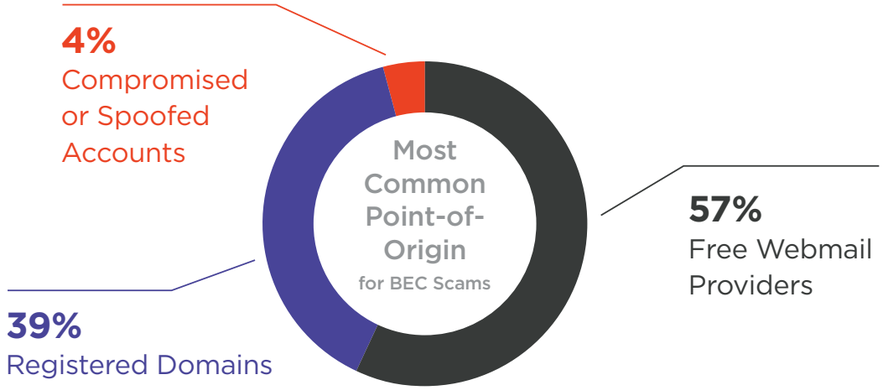
Gmail remains the most weaponized email platform for BEC scammers the world over. But this past quarter, the number of attacks launched from longtime fraud-ring favorite Roadrunner has fallen off a cliff—dropping from 23% of all attacks to just 3% in 90 days.

Reality Czech: Email Fraudsters Are Switching Up Webmail Providers

In a first for this tracking index, BEC scams exploiting familiar webmail brands like Gmail, Roadrunner, as well as Earthlink (10%), and Virgin Media (9%), are suddenly being joined by a booming number of email schemes launched from Czech-based webmail platforms with names like Seznam.cz (8%) and Email.cz (4%), and Post.cz (2%).

Lookalike Domains Locked And Loaded for New BEC Attacks

Today, 39% of BEC campaigns are launched from email accounts hosted on a domain registered by the attacker. While there is usually a cost associated with registering a domain, the ability to create a more legitimate-looking email address is worth it for some. Meanwhile, 4% of BEC emails are sent from compromised email accounts, which are notoriously difficult for most business targets to detect.



Gmail	35%	1	7	Email.cz	4%
Earthlink	10%	2	8	Roadrunner	3%
Virgin Media	9%	3	9	Post.cz	2%
Seznam.cz	8%	4	10	Tutanota	2%
Naver	5%	5	11	Other	17%
AOL	4%	6			

Phishing Response Trends

KEY FINDINGS

60% of employee-reported phishing incidents are false positives, representing a significant waste of valuable time for SOC analysts who must triage, investigate, and remediate reported incidents that pose no threat to the organization.

Organizations with automated phishing response processes detect **44X** the number of similar malicious messages exclusively reported by employees.

Organizations with continuous detection and response (CDR) capabilities informed by real-time threat intelligence collectively interdicted at least **3,500** latent threats that would have otherwise gone undetected post-delivery.

Phishing Response Obstacles Multiply

Employee-Reported Phishing Attacks Leave SOCs Scrambling

In a world where cybercriminals send 3 million phishing emails every minute of the day, it's unrealistic to believe there won't be a single employee who takes the bait. Worldwide, as many as 94% of all corporate data breaches may begin this way, according to Verizon's 2019 Data Breach Investigations Report (VDBIR). Juniper Research estimates business losses stemming from data breaches hit $3 trillion worldwide this past year, and could top $5 trillion in 2024. Unfortunately, the same tools businesses are putting in place to mitigate this threat may only be magnifying it.

Fast Trigger Fingers: Slower Response Times, Higher Breach Costs

According to Ponemon Institute, businesses currently stand a 28% chance of suffering at least one data breach some time during the next 24 months. To help blunt the impact of phishing attacks that can lead to a breach, most large organizations provide employees tools to report suspect emails at the push of a button. But the avalanche of incident reports often ends up burying Security Operations Centers (SOCs) with more than they can handle. As a result, triage, forensics, remediation, and breach containment grow more time consuming—and more costly. Unless they find ways to automate these processes, businesses face a losing battle against an endless barrage of email attacks.

Inside the ACID Q1 2020 Phishing Incident Response Survey

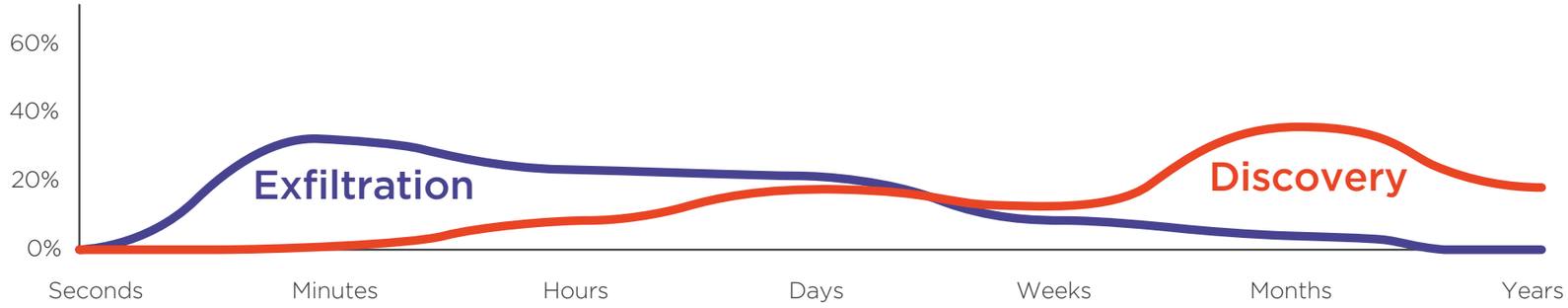
This quarter, ACID researchers interviewed SOC professionals at large companies with operations spanning a cross-section of industries—including retail, high-tech, healthcare, agriculture, construction, and energy. The objective of this quarter's survey was to gain insights on reported incident volumes, false positive rates, and the impact of automation on the investigation and remediation of email threats from October through December 2019. This section of the Q1 2020 Email Fraud and Identity Deception Trends Report highlights our analysis of these conversations.

Employee-Reported Incidents: 60% False Positives

Employees at all participating companies in our Q1 2020 phishing response survey have the ability to report suspected phishing attacks. Collectively, SOC analysts at these organizations had to triage, investigate, and remediate 2,765 employee-reported incidents during the fourth quarter of 2019. Unfortunately, an average of 6 out of every 10 suspected phishing emails submitted by employees is ultimately determined to be non-malicious. Nonetheless, SOC analysts must still dedicate a significant amount of time triaging these innocuous messages. Related ACID research spanning more than 200 companies in the US and UK recently found that on average, it can take more than 7 hours to remediate a false positive.

Breachonomics

Automation Grows Critical to Reducing Time-to-Containment



Source: 2019 Verizon Data Breach Investigations Report

Every minute spent investigating false negatives means actual phishing emails are left undetected, increasing the likelihood of a data breach with each passing moment. According to the 2019 Verizon Data Breach Investigations Report (DBIR), phishing is directly implicated in more than a third of all data breaches, and a factor in up to 94% of them.

On average, these breaches result in data exfiltration within minutes or hours—while it often takes months before they're discovered. For US-based companies, the costs associated with breaches now average $8.19 million per incident, with a 14.8% probability of falling victim to a breach within the next year, according to Ponemon Institute.

When asked about their approaches to addressing these risks, survey participants cite automation as central to reducing the time it takes to mitigate reported phishing incidents and contain breaches. In some cases, the ability to streamline the processes involved in remediating email threats can be cut down to a few minutes, versus the days, weeks, or months reported in the VDBIR. With less time spent fielding reported incidents, SOC analysts are able to focus on more important initiatives.

The Automation Index

44X More Threats Detected Than Manual Reporting Processes Alone

In addition to streamlining the remediation of reported phishing incidents, organizations in our survey report that automated phishing response detects 44x more email threats than manual reporting alone.

Out of an aggregated pool of 2,765 verified malicious emails reported during the fourth quarter of 2019, automated phishing response processes identified 45,294 additional email threats that were either similar or directly related to those reported by employees. According to these organizations, this form of automation limits the potential blast radius of phishing campaigns while producing further reductions in the time required to contain breaches.

Number of Malicious Phish Reports	Number of All Similar Messages Found	Number of All Malicious Similar Messages Found	Discovery Factor
59	24,178	11,956	203
208	3,100	2,338	11
1,250	112,229	9,958	8
885	163,261	11,205	13
1	123	1	1
362	21,552	9,836	27
		Average Discovery Factor	44

Continuous Detection and Response
Thirty-Five Hundred Additional Email Threats Neutralized

According to survey participants, continuous detection and response (CDR) technologies enhanced with shared threat intelligence identified 3,500 additional malicious messages beyond those detected through automated phishing response alone.

Generally speaking, CDR technologies identify latent threats that have evaded detection through dormant payloads, new impersonation techniques, or "time-bombed" URLs that redirect post-delivery. By analyzing company-wide email metadata, these technologies forensically recognize and remove email threats from all inboxes automatically.

According to survey participants, augmenting CDR with shared, real-time threat intelligence vetted by a network of cross-industry SOC experts increases their ability to neutralize emerging threats that would otherwise go unrecognized. During the fourth quarter of 2019, more than 90% of the malicious emails identified through intel-enhanced threat detection were automatically deleted or quarantined.

Consumer Phishing and DMARC Trends

KEY FINDINGS

The number of domains with DMARC records surged **83%** over the past year, but they only represent a small fraction of the total universe of domains worldwide.

85% of the Fortune 500 remains at risk of seeing their brands hijacked for use in email-based brand impersonation scams targeting their customers, partners, investors, and the public.

BIMI continues to gain traction, with **2,338** domains possessing an associated record, reflecting a **46%** increase in just 90 days.

DMARC Adoption Snapshot

The Industry's Largest Ongoing Study of Adoption Rates Worldwide

In our latest quarterly snapshot of more than 366 million Internet domains, we assess the state of DMARC implementation from October through December 2019. For the full year, adoption rose 83%, to 11,628,125 domains with recognizable DMARC policies worldwide. But given the total universe of domains, most organizations remain defenseless against fraudsters seeking to pirate their domains to launch phishing-based brand impersonation scams targeting their customers, partners, and the general public.

Why DMARC is Critical to Brand Protection

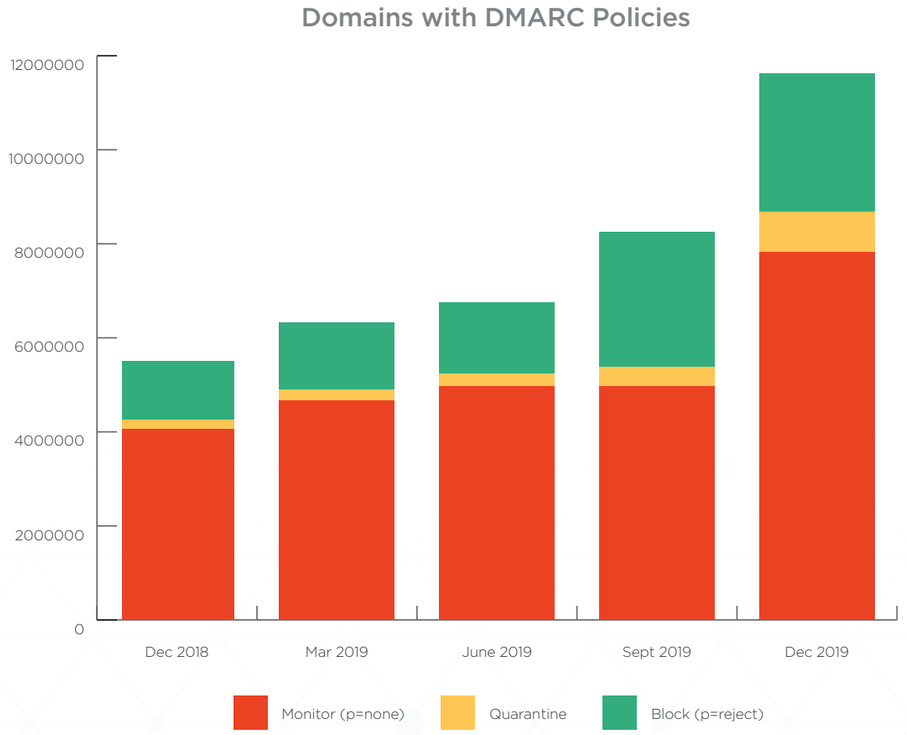
Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an open standard email authentication protocol that gives brands control over who is allowed to send emails on their behalf. Put simply, DMARC enables email receiver systems to recognize when an email isn't coming from a specific brand's approved domains, and gives the brand the ability to tell email receiver systems what to do with these unauthorized email messages.

Full Enforcement Required to Prevent Impersonation

Failure to implement DMARC at its highest enforcement level, *p=reject*, leaves brands at risk of reputational damage from fraudsters using their domains to launch phishing attacks. These domains may also be blacklisted by receiver systems, or experience reduced deliverability rates for the brand's own legitimate email messages, resulting in costly disruptions to their email-based marketing and revenue streams.

Brands looking to deploy DMARC are advised to begin with a *p=none* enforcement policy and work up to the *p=reject* policy through a well-defined DMARC implementation plan. When enforcement policies are set properly, DMARC has been shown to drive phishing-based impersonations to near zero.

For more information on DMARC adoption and its benefits, visit **www.agari.com/dmarc-guide**



DMARC Breakout Session

US, Germany Continue to Dominate in DMARC Adoption

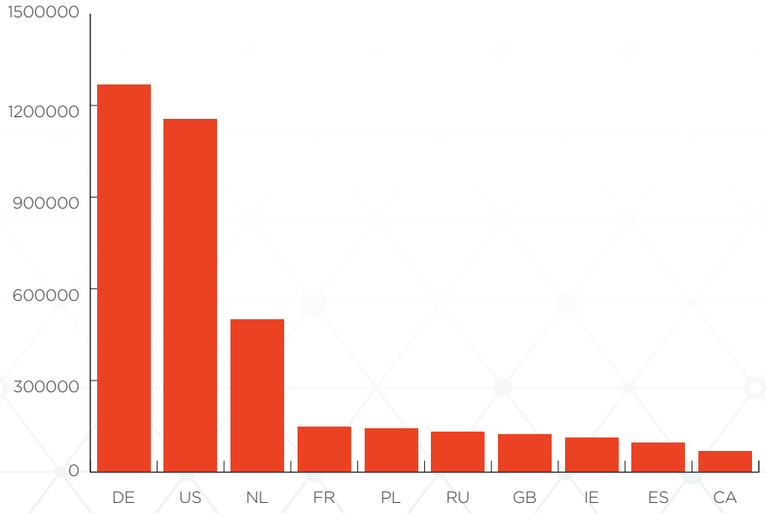
As part of our quarterly reports, ACID examines the state of DMARC adoption by key geographies. As measured by domains for which a country code can be validated, this data encompasses roughly 50% of our total pool of analyzed domains worldwide.

US Tops in DMARC Policies at *p=reject*

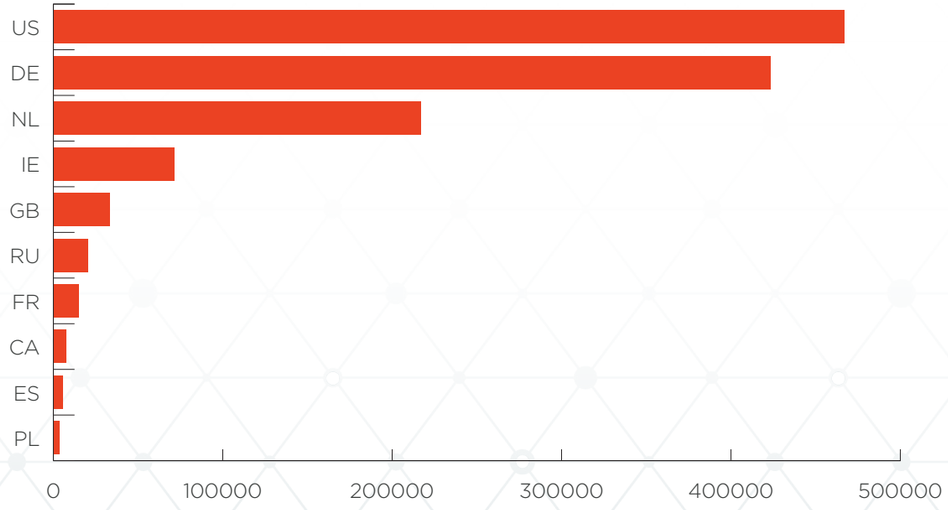
While the United States continues to trail Germany in country-coded domains assigned DMARC records, a higher percentage (40.4%) of its domains with established DMARC records are set to the *p=reject* enforcement level needed to protect against email-based brand impersonation scams.

In contrast, Germany continues to lead all geographies in registered domains with established DMARC records, and the vast majority of domains for which a country code can be correlated. However, most DMARC records here are at the default, monitor-only setting (65% set to monitor only; 33.4% set to *p=reject*).

Top 10 Countries with DMARC Policies



Top 10 Countries with DMARC Policies at *p=reject*



DMARC Adoption Trends Among the World's Largest Companies

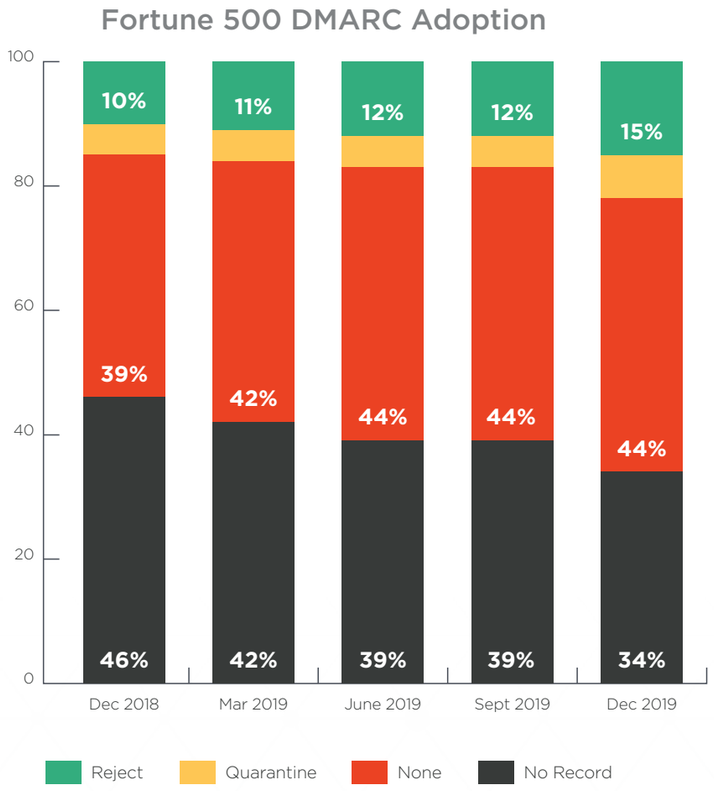
This quarterly assessment of publicly available DMARC adoption data captures trends for the Fortune 500, Financial Times Exchange 100 (FTSE 100), and the Australian Securities Exchange 100 (ASX 100), from October through December 2019.

Each chart in this section offers a snapshot of adoption trends among some of the world's most prominent organizations. It's important to note that even companies that have assigned DMARC records to their domains are not truly protected unless they are set to a level of enforcement. The sizable proportion of "no record" and "monitor only" policies highlights the fact that these organizations can still be impersonated in phishing campaigns that put their customers, partners, investors, and the general public at risk of serious financial harm.

Fortune 500: DMARC Adoption Edges Up, But 85% of Companies Remain Unprotected

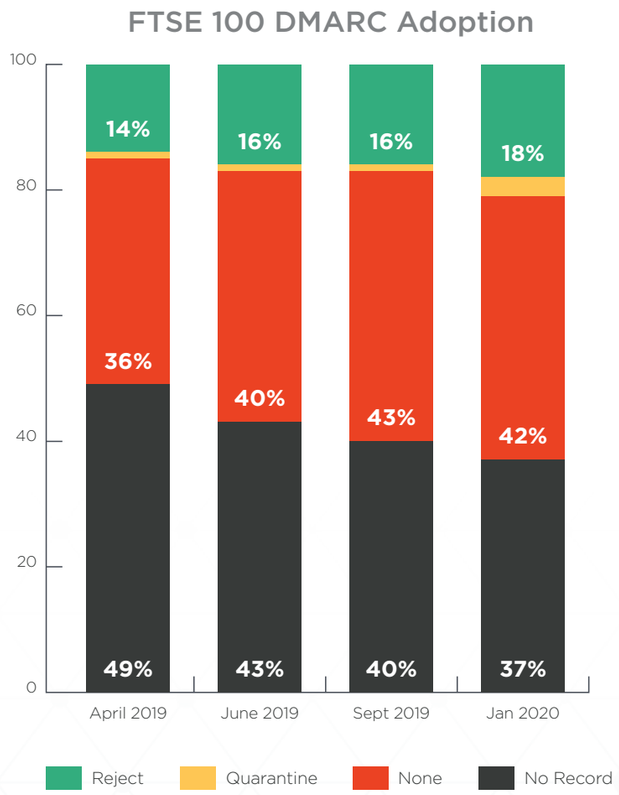
Only 15% of Fortune 500 companies have a DMARC record set to the *p=reject* enforcement policy required to prevent cybercriminals from impersonating their brands in phishing attacks. That's up just 5% from December 2018, leaving 85% of the Fortune 500 unprotected.

It is worth noting that the percentage of Fortune 500 companies without a DMARC record assigned to any of their domains dropped 12% in 2019, from 46% to 34%. However, 44% of those that have adopted DMARC have yet to set an enforcement policy.



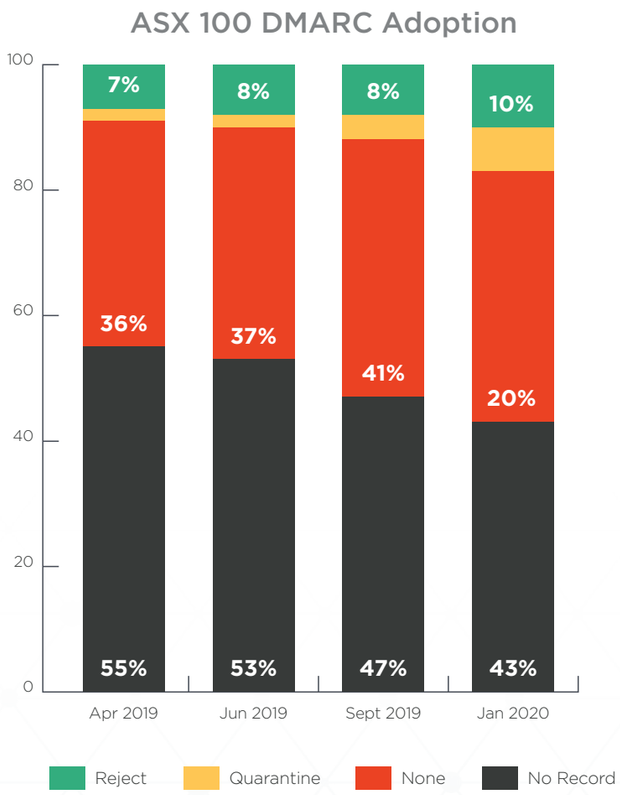
FTSE 100: Progress Made, But 82% of Companies Continue to Put Customers at Risk

In the fourth quarter of 2019, only 18% of the UK's FTSE 100 companies were fully protected by email authentication—up just 2% during the final three months of the year. While the number of domains with DMARC records rose 22% year-over-year, most do not yet have an enforcement policy set. As it stands now, 82% of FTSE 100 companies do not yet have protections in place to block fraudsters from impersonating their brands in email attacks targeting customers.



ASX 100: Only 1 in 10 Companies Are Fully Protected From Brand Impersonation

Just 10% of Australia's ASX 100 companies have implemented DMARC with the reject policy needed to prevent cybercriminals from hijacking their brand identities in phishing attacks. On a brighter note, the percentage of companies that have at least taken the first step toward defending their brands by assigning DMARC records to their domains rose 13% in 2019. But vast majority of companies with DMARC records have yet to set an enforcement policy.



DMARC Adoption by Industry Vertical

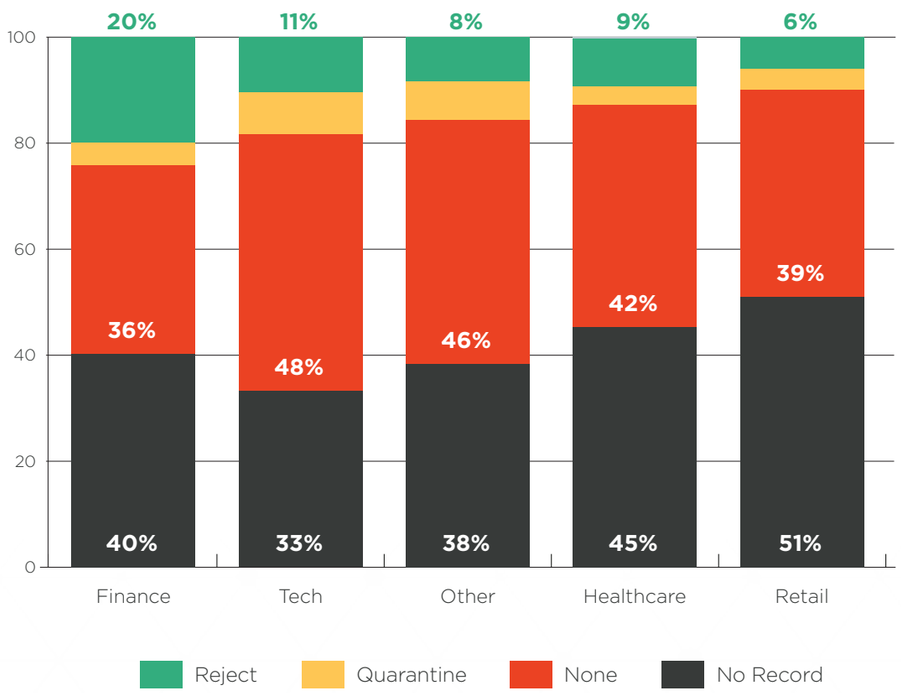
Our quarterly analysis of DMARC adoption across key industry verticals is based on public DNS records for primary corporate website domains of large companies with revenues above $1 billion.

As captured in stats from the fourth quarter of 2019, measured progress continues to be made across all verticals in our index. Though much work remains, the percentage of domains without DMARC records dropped 10% to 15% in some industries over the last year.

Finance remains the industry champion in terms of DMARC implementations set at a *p=reject* enforcement level, with nearly 20% of all companies protected against impersonations that put their customers, partners, and the public at large at risk.

But the healthcare industry saw the greatest gains this year, doubling the rate of enforcement. Today, nearly 1 in 10 companies in this sector have put protections in place to stop fraudsters from commandeering their brand identities in phishing attacks—up from just 5% during the same quarter last year. Yet despite this progress, 90% of all healthcare companies remain at risk.

DMARC Policy and Enforcement Trends for Key Industries



The Agari Advantage: Industry Enforcement Comparison

Data in the Agari Email Threat Center enables us to understand how enforcement rates across industries compare with those of Agari customers.

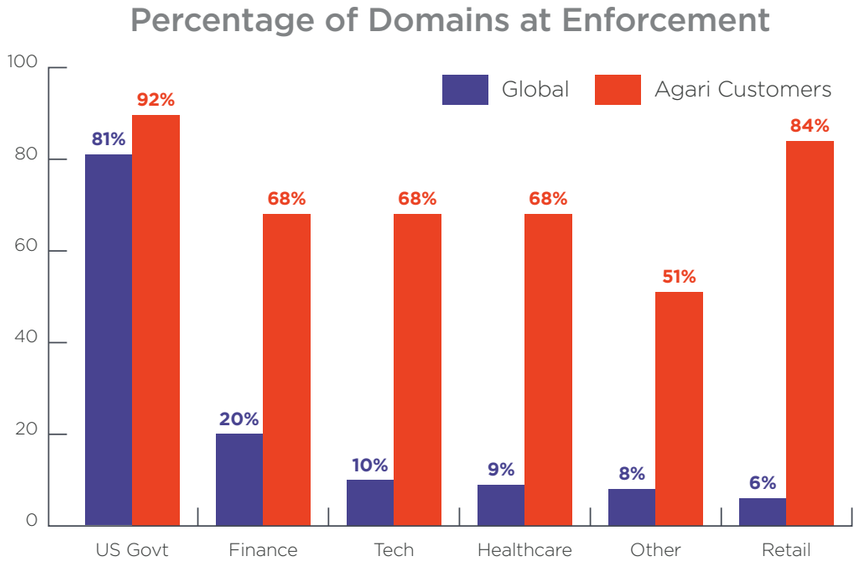
Aggregating real-time DMARC statistics from the domains of top banks, social networks, healthcare providers, major government agencies and thousands of other organizations, the Agari Email Threat Center is the largest set of detailed DMARC data in the world both in terms of email volume and domains. To generate real-time threat intelligence, the Agari Email Threat Center analyzed more than 350 million emails from more than 20,500 domains from October through December 2019.

Retail Rocks DMARC Enforcement, But Government Still Rules

During the fourth quarter of 2019, Agari clients in Retail rallied to once again overtake Healthcare in DMARC adoption at *reject*—rising 17% in just 90 days.

Cybercriminals are increasingly targeting retailers as they expand the number of online channels from which they market merchandise. It's clear retailers want to be prepared for a barrage of attacks during 2019's all-important holiday shopping season. For comparison, just 6% of retailers worldwide have implemented DMARC at full enforcement, putting Agari's Retail clients 78% ahead of the sector as a whole.

It's worth noting, however, that Government still outpaces all other sectors in implementing full enforcement for DMARC-enabled domains.



Note: The Agari Email Threat Center tracks authentication statistics across active domains belonging to customers of Agari. Passive or defensive domains that do not process email will not be reflected in the totals.

Brand Indicators Adoption

BIMI Adoption Skyrockets Nearly 10X Since March 2019

Brand Indicators for Message Identification (BIMI) is a standardized way for brands to publish their brand logos online with built-in protections that safeguard the brand from spoofing.

Capital One, eBay, Groupon, and Aetna are just a few of the brands that use BIMI to display their logo next to their email messages—enhancing brand presence as well as the ability for brands to control the logo that is displayed. BIMI will work only with email that has been authenticated through the DMARC standard and for which the domain owner has specified a DMARC policy of enforcement, so only authenticated messages can be delivered.

Q4 Snapshot: 46% Growth in BIMI Brand Adoption

As of December 2019, an impressive 1,389 domains added BIMI records along their top level domains, and any number of subdomains, during the preceding three months. That's a 46% increase from 949 logos during the second quarter of this year—and 10X more than the 130 logos seen in March.

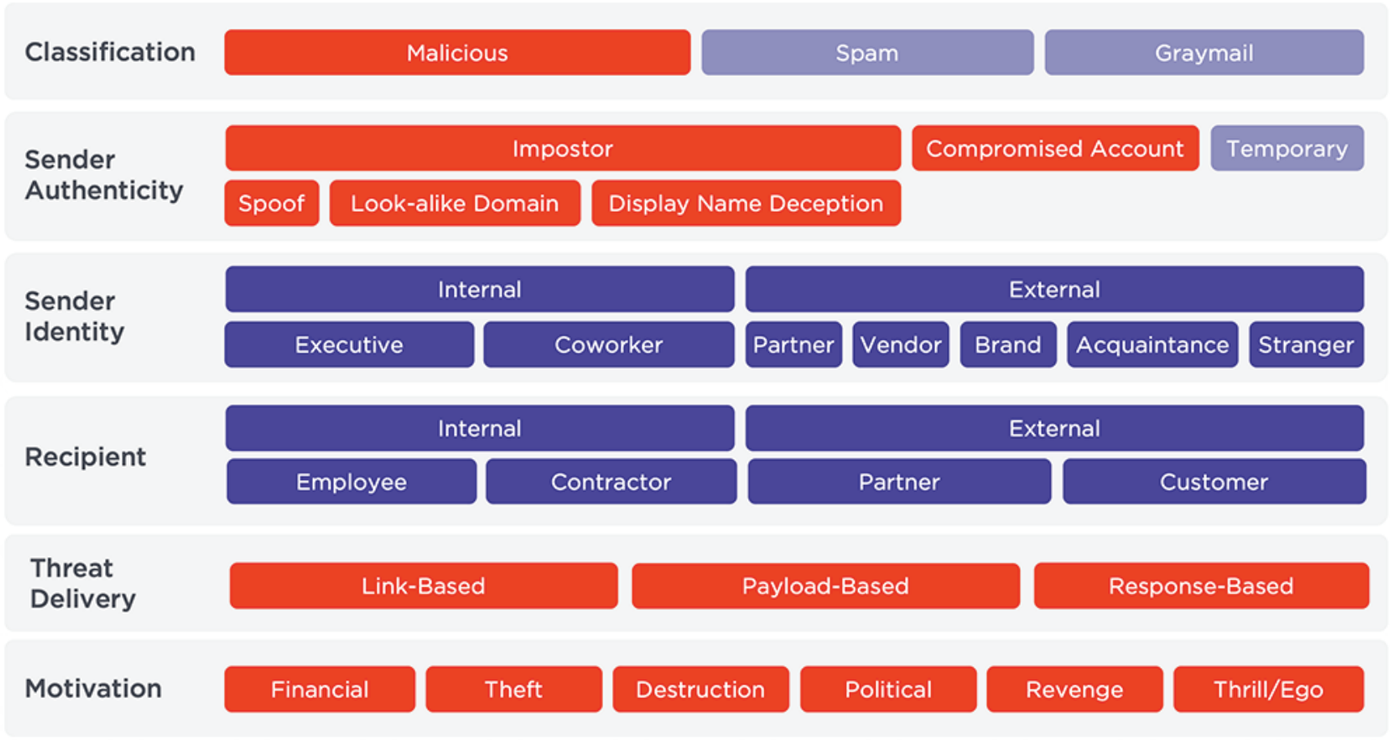
It's worth noting that smaller brands make up a significant portion of these increases, as larger number of organizations seek to leverage the tremendous brand presence BIMI affords their logos by displaying them prominently within email clients. This, combined with the BIMI pilot from Google set to launch early this year, will only accelerate growth among a larger number of brands seeking to avoid being outpaced by rivals.

Because of its ability to help increase brand exposure and visibility even while protecting against brand impersonations, it may soon be considered a "must-have" for brand email campaigns everywhere.

About This Report

Taxonomy of Advanced Email Threats

ACID has established 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 helps readers understand the terms used in this report and what they mean to email security.



The metrics and data analyzed in this report are collected from the sources indicated below.

Aggregate Advanced Threat Protection Data

For inbound threat protection, Agari uses machine learning—combined with knowledge of an organization's email environment—to model good, legitimate 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 Secure Email Gateways (SEGs) into distinct threat categories, such as display name deception, compromised accounts, and more. See section on "Taxonomy of Advanced Email Attacks" on the preceding page.

Phishing Incident Response Trends

This report presents results from a survey of six large organizations in a cross-section of industries conducted by Agari in December 2019.

Global DMARC Domain Analysis

For broader insight into DMARC policies beyond what we observed in email traffic targeting Agari's customer base, we analyzed 366 million domains, ultimately observing 11,628,125 domains with recognizable DMARC policies attached. This constantly updated list of domains serves as the basis for trend tracking in subsequent reports.

About Agari Cyber Intelligence Division

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. ACID has conducted more than 12,000 active defense engagements with threat actors since May 2019. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Learn more at acid.agari.com

About Agari by HelpSystems

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity. Agari was acquired by HelpSystems in May 2021.

Learn more at www.agari.com

AGARI CYBER
INTELLIGENCE DIVISION

Discover How Agari Can Improve Your Current Email Security Infrastructure

As your last line of defense against advanced email attacks, Agari stops attacks that bypass other technologies—protecting employees and customers, while also enabling incident response teams to quickly analyze and respond to targeted attacks.

Get Free Trial **www.agari.com/trial**

View the 2020 Presidential Campaign Email Threat Index

To see the latest information on which candidates have implemented email security for their campaigns, visit: **www.agari.com/election2020**

Visit the Agari Threat Center

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

Calculate the ROI of Implementing Agari

To discover how much money you can save by adding Agari to your email security environment, visit: **www.agari.com/roi**

agari
by HelpSystems

hds-rp-1021-79d