AGARI

Agari Global DMARC Adoption Report:

Open Season for Phishers

Executive Summary

Based on Agari research of public DNS records, 92 percent of all Fortune 500 companies have left their customers and business partners unprotected from phishing and other forms of email attacks that impersonate their corporate email domain. A similar pattern has emerged around the world with the FTSE 100 and the ASX 100. Cybercriminals exploit this vulnerability by sending billions of emails per year claiming to be from these companies.

Digital deception emails trick users into clicking on websites that steal their passwords, install ransomware or con unsuspecting victims into sending money. This type of fraud represents billions of dollars in losses per year and is completely preventable if organizations adopt an open standard called DMARC (Domain-based Message Authentication, Reporting & Conformance).

When a company implements DMARC, there are three levels of policies that can be applied to their domains:

Monitor (None) – Unauthenticated messages are monitored but still delivered to the inbox

Quarantine – Unauthenticated messages are moved to the “Spam” or “Junk” folders

Reject – Unauthenticated messages are blocked and not delivered to any folder

Shockingly, the largest corporations around the world have by-and-large not implemented the DMARC standard, leaving their customers, business partners and brand vulnerable to digital deception and the losses associated with email fraud:

Fortune 500

DMARC adoption – Two-thirds (67 percent) of the Fortune 500 have not published any DMARC policy. Only four Fortune 500 industry sectors have a majority DMARC adoption rate: business services (60 percent), financials (57 percent), technology (55 percent) and transportation (53 percent).

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

Reject Policy – Only five percent have implemented a Reject policy (Blocked).

FTSE 100

DMARC adoption – Two-thirds (67 percent) of the Financial Times Stock Exchange 100 have not published any DMARC policy.

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

Reject Policy – Only six percent have implemented a Reject policy (Blocked).

ASX 100

DMARC adoption – Almost three-quarters (73 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 three percent have implemented a Reject policy (Blocked).

DMARC ADOPTION ANALYSIS

Phishing has become a pervasive threat in the United States and around the world. The impact of these threats has been felt by both businesses and government, alike. If organizations implement DMARC, they could protect against these attacks; yet more than two-thirds have not implemented any DMARC policy and more than 90 percent remain vulnerable to impersonation of their corporate email domains. The cybercriminals have responded by ramping up phishing activity to take advantage of this vulnerability. Between October 2014 and June 2016, the number of new, unique phishing sites has increased by more than 1000 percent.

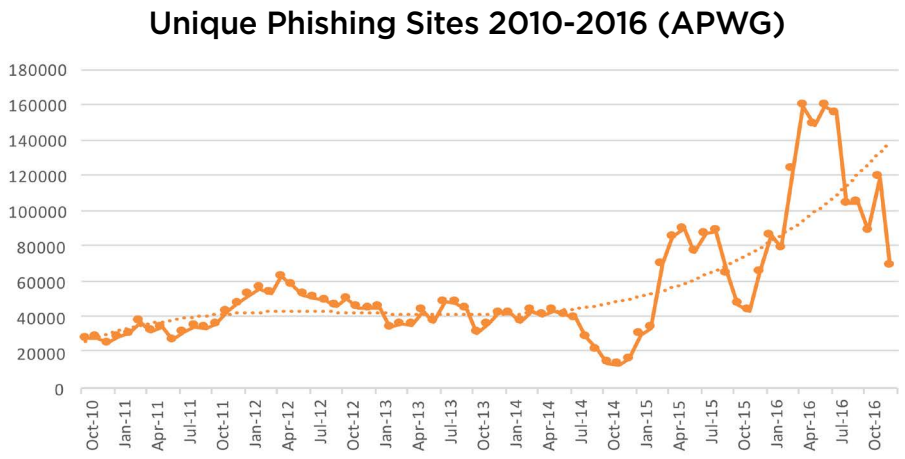


Figure 1 - Unique Phishing Sites From 2010-2016 from Anti-Phishing Working Group

DMARC Adoption in the Fortune 500

Methodology

On July 21st, 2017, Agari analyzed Fortune 500 companies to determine their corporate domains and industry sectors. This list of domains was surveyed through the Agari DMARC Record tool to determine if the domain had deployed a DMARC record in its DNS – and if so, what was its policy.

Analysis

More than 90 percent of the Fortune 500 are vulnerable to digital deception, 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 America. Unfortunately, DMARC adoption is dangerously low within the Fortune 500, enabling malicious actors to abuse that trust and leaving corporations unprepared to prevent it.

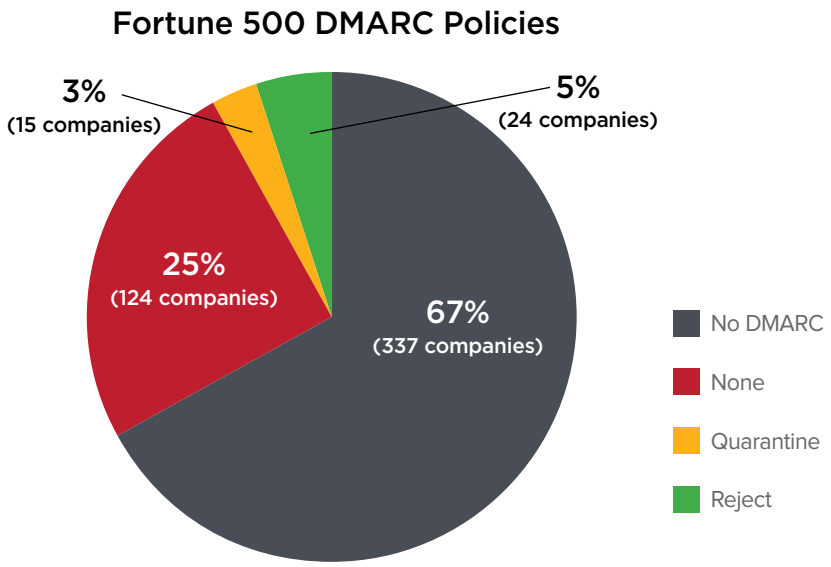
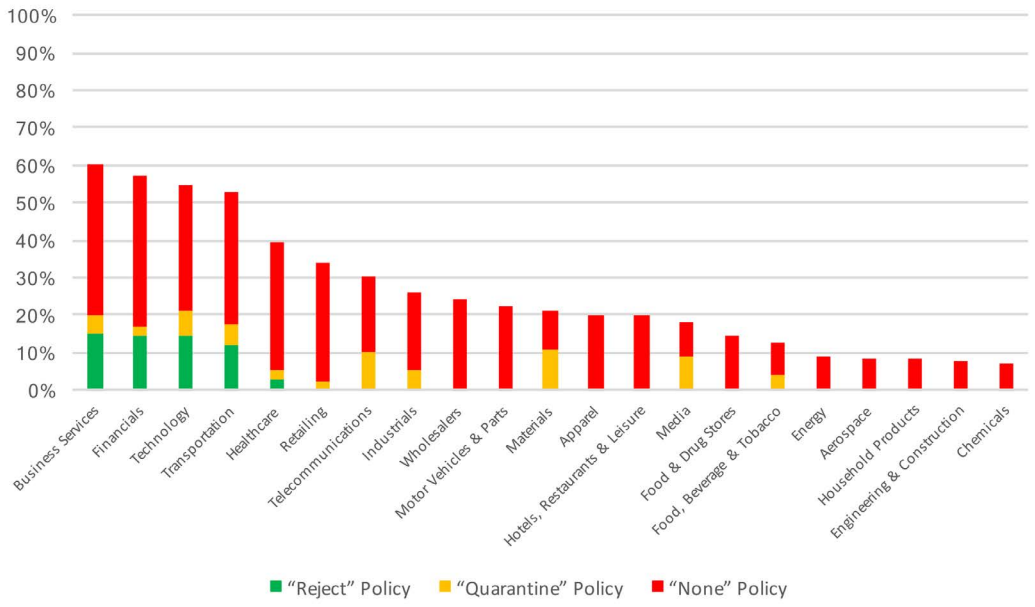


Figure 2 – Fortune 500 DMARC Adoption (7/21/2017)

More than two-thirds of the Fortune 500 (337 companies) do not have a DMARC record on their corporate domain. Of the remaining third, 124 companies have a Monitor (None) policy, which monitors for DMARC abuse, but does not prevent it. Fewer than 10 percent of the Fortune 500 have deployed a DMARC policy to prevent digital deception; 15 companies (three percent) have a Quarantine policy and 24 companies (five percent) have a Reject policy.

Interestingly, only four industry sectors have achieved a majority adoption rate: business services (60 percent), financials (57 percent), technology (55 percent) and transportation (53 percent). The full list of DMARC adoption by industry sector follows along with a per-sector percentage breakdown:

Fortune 500 DMARC Adoption Rate by Policy (Corporate Domains)



Fortune 500 DMARC Adoption – Number of Companies by Sector

Sector	No DMARC Policy	Monitor (None) Policy	Quarantine Policy	Reject Policy
Business Services	8 (40%)	8 (40%)	1 (5%)	3 (15%)
Financials	36 (43%)	34 (41%)	2 (2%)	12 (14%)
Technology	19 (45%)	14 (34%)	3 (7%)	6 (14%)
Transportation	8 (47%)	6 (35%)	1 (6%)	2 (12%)
Healthcare	23 (60%)	13 (34%)	1 (3%)	1 (3%)
Retailing	31 (66%)	15 (32%)	1 (2%)	0
Telecommunications	7 (70%)	2 (20%)	1 (10%)	0
Industrials	14 (74%)	4 (21%)	1 (5%)	0
Wholesalers	22 (76%)	7 (24%)	0	0
Motor Vehicles & Parts	7 (78%)	2 (22%)	0	0
Materials	15 (79%)	2 (10%)	2 (11%)	0
Apparel	4 (80%)	1 (20%)	0	0
Hotels, Restaurants & Leisure	8 (80%)	2 (20%)	0	0
Media	9 (82%)	1 (9%)	1 (9%)	0
Food & Drug Stores	6 (86%)	1 (14%)	0	0
Food, Beverage & Tobacco	21 (88%)	2 (8%)	1 (4%)	0
Energy	52 (91%)	5 (9%)	0	0
Aerospace	11 (92%)	1 (8%)	0	0
Household Products	11 (92%)	1 (8%)	0	0
Engineering & Construction	12 (92%)	1 (8%)	0	0
Chemicals	13 (93%)	1 (7%)	0	0

Certainly, it is interesting to note that business services, financials, technology and transportation have a majority adoption rate; these are seemingly the sectors most likely to be targeted by phishing attacks. Business services include payment processors and credit card companies, which are frequently spoofed in phishing campaigns. The same can be said for financials, such as banks and stock portfolios. Technology companies are a logical early adopter of new technology. Finally, transportation includes both shipping and airlines, which are both frequently spoofed to deliver malicious attachments disguised as tracking numbers and reservations.

It may seem these corporations are aware of the threat of digital deception and have taken appropriate counter-measures. However, even among these early adopters, the majority of their deployments are "p=none," which does nothing to prevent these attacks. DMARC adoption is of little use, unless organizations move to a Quarantine or Reject policy.

Analysis into DMARC adoption by the US Government falls outside the scope of this research, but bears mention because of a recent letter to the Department of Homeland Security by Senator Ron Wyden. In the letter, Sen. Wyden notes:

"Industry-standard technologies exist, and are already used throughout the private sector and even by a few federal agencies, which, if enabled, would make it significantly harder for fraudsters and foreign governments to impersonate federal agencies."

Sen. Wyden is referring to DMARC, writing in his letter:

"Other federal cyber security leaders such as the National Institute for Standards and Technology (NIST) and the Federal Trade Commission (FTC) strongly recommend DMARC. A few federal agencies, including the FTC, the Federal Deposit Insurance Corporation, and the Social Security Administration have taken the initiative by enabling DMARC. Moreover, they have configured it in the most strict "reject" mode so that email service providers can automatically reject phishing emails impersonating their agency. Unfortunately, most agencies, including DHS, have still not enabled DMARC or configured it in the strongest setting."

In fact, according to recent research conducted by the **Global Cyber Alliance**, 1180 out of 1315 (90 percent) government domains have not implemented DMARC.

DMARC Adoption in the FTSE 100

Analysis

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 'go-to' 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 US, more than two-thirds (67 percent) of the top 100 UK listed 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.

Of the remaining 33 companies, only six have implemented DMARC's Reject policy, which protects customers and employees from potential exposure to fraudulent and malicious messages as even the most sophisticated spoof email can be detected and blocked from reaching its intended inbox. Twenty-six of the organizations have a Monitor (None) policy in place, which monitors for abuse, but does not prevent it.

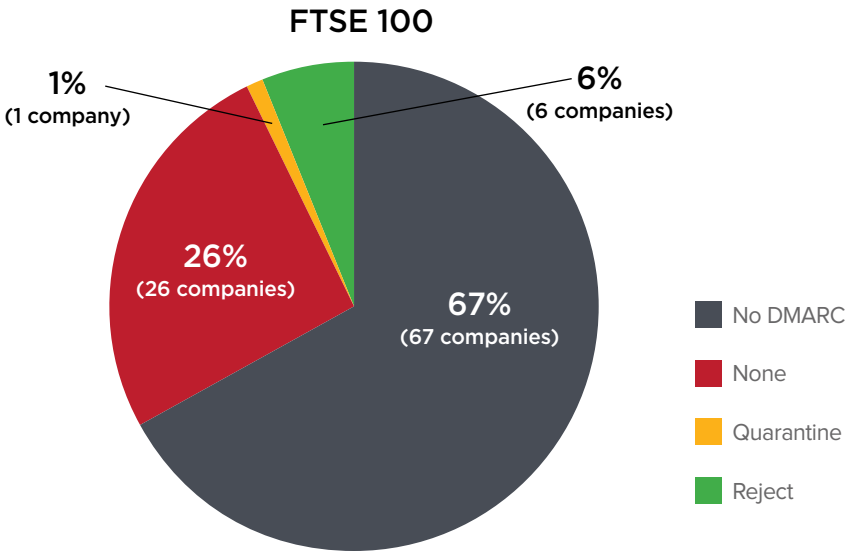


Figure 3 - FTSE 100 DMARC Adoption

The pharmaceutical industry sector has the highest adoption rate at 100 percent (although they are all still in DMARC Monitor mode), followed by financial services at 42 percent, energy & utilities at 38 percent and retail and telecommunications both at 33 percent. However, financial services has both the most overall companies with a DMARC record and the most at "Reject."

The full list of DMARC adoption by industry sector follows:

FTSE 100 DMARC Adoption – Number of Companies by Sector

Sector	No Policy	Monitor (None) Policy	Quarantine Policy	Reject Policy
Real Estate & Property	3 (75%)	0	0	1 (25%)
Financial Services	13 (59%)	5 (23%)	1 (4%)	3 (14%)
All Other	15 (63%)	7 (29%)	0	2 (8%)
Pharmaceuticals	0	3 (100%)	0	0
Energy & Utilities	5 (62%)	3 (38%)	0	0
Retail	8 (67%)	4 (33%)	0	0
Telecommunications	2 (67%)	1 (33%)	0	0
Mining	5 (71%)	2 (29%)	0	0
Manufacturing	3 (75%)	1 (25%)	0	0
Media	3 (100%)	0	0	0
Hospitality & Entertainment	4 (100%)	0	0	0
Building	6 (100%)	0	0	0

The majority of industry sectors with a high adoption rate are those with large consumer customer bases, which are frequently spoofed in phishing campaigns. This indicates that these companies have taken proactive steps to counteract the increasing threat of digital deception.

Enterprises (and the US Government) could look to the UK Government for the positive and forward thinking move they have taken toward improving security for both the UK government and its citizens. As of October 1, 2016, the UK's Government Digital Services (GDS), a part of the Cabinet Office, mandated that all central Government departments need to adopt DMARC as standard for all services using the .gov.uk domain.

During the Chancellor of the Exchequer's National Cyber Security Strategy announcement in November 2016, he referenced one case of more than 50,000 fraudulent emails from an account named "taxrefund.gov.uk" which were being sent to the unsuspecting British public daily. This spoofed domain has now been shut down thanks to the use of the DMARC protocol.

The same effect can be achieved across enterprises.

DMARC Adoption in the ASX 100

Analysis

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

Almost three-quarters (73 percent) of the ASX 100 companies do not have a DMARC record in place for their corporate domain. This represents a higher proportion of Australian companies that have not sought to adopt any level of email authentication protocols through DMARC compared to both the US and the UK.

Of the remaining 27 companies, 23 have taken the first step in implementing DMARC by setting up the Monitor (None) policy, which instructs the server to authenticate the incoming email via DMARC, but takes no action based on the results, ultimately delivering the email to the recipient. Just three organizations have adopted a Reject policy, meaning that emails that fail DMARC authentication are not delivered to the intended email inbox.

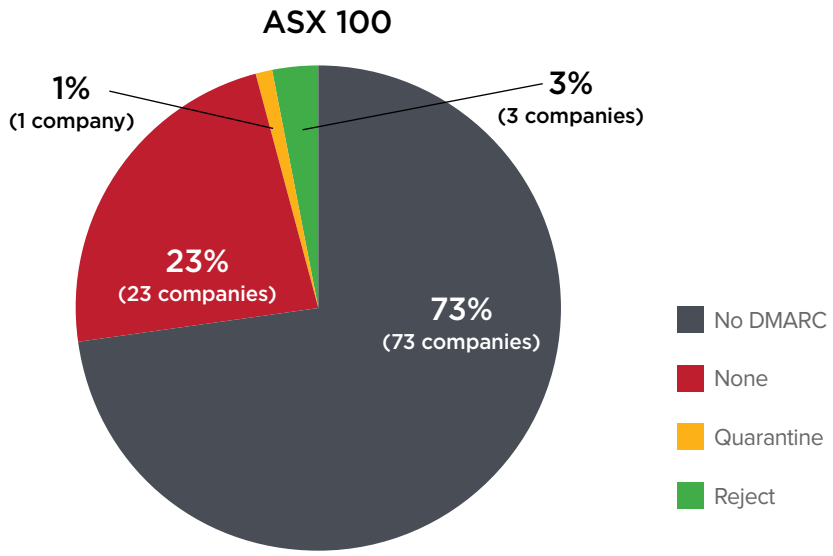


Figure 4 - ASX 100 DMARC Adoption

The information technology sector has the highest adoption rate at 100 percent (although they are all still in DMARC Monitor mode), followed consumer staples at 40 percent and financial services at 35 percent, while consumer discretionary has 27 percent adoption.

The full list of DMARC adoption by industry sector follows:

ASX 100 DMARC Adoption – Number of Companies by Sector

Sector	No Policy	Monitor (None) Policy	Quarantine Policy	Reject Policy
Utilities	3 (75%)	0	0	1 (25%)
Industrials	9 (82%)	1 (9%)	0	1 (9%)
Consumer Discretionary	8 (73%)	2 (18%)	0	1 (9%)
Materials	16 (80%)	3 (15%)	1 (5%)	0
Information Technology	0	3 (100%)	0	0
Consumer Staples	3 (60%)	2 (40%)	0	0
Financial Services	13 (65%)	7 (35%)	0	0
Healthcare	6 (75%)	2 (25%)	0	0
Energy	4 (80%)	1 (20%)	0	0
Real Estate	8 (80%)	2 (20%)	0	0
Telecommunication Services	3 (100%)	0	0	0

Similar to the UK, the majority of industry sectors with a high adoption rate are those with large consumer customer bases, which are frequently spoofed in phishing campaigns. With just over a quarter 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.

A BRIEF HISTORY OF EMAIL AUTHENTICATION

DMARC emerged from an experiment piloted by Yahoo! and PayPal in 2007 that was designed to prevent account credential phishing. Before DMARC, there were two email authentication protocols, “Sender Policy Framework” (SPF) and “Domain Keys Identified Mail” (DKIM). SPF utilizes DNS to specify which mail servers are authorized to send email for the domain listed in the envelope or “bounce” address. SPF is therefore able to authenticate the envelope sender, but does nothing to authenticate the sender contained in the “From: header” of the message. Since end users don’t see the envelope sender, it’s far more important to authenticate the “From: header,” which they do see.

DKIM uses cryptographic authentication. A hash of the message is digitally signed using a private key known only to the sending email server. This signature rides around in a special message header, and can be verified using the signer’s public key, which is stored in the signer’s DNS. DKIM is actually quite easy to deploy so long as your mail server or Email Service Provider supports it. Unfortunately, there’s a misconception that DKIM is difficult to deploy, or that deploying DKIM will cause receivers to block your email if the signature fails validation. Neither of these are true.

The “Domain-based Message Authentication, Reporting & Conformance” (DMARC) protocol seeks to advance these previous standards by comparing the envelope sender authenticated by the SPF check and the signing entity authenticated by the DKIM signature back to the sender listed in the “From:” header. Known as “identifier alignment”, this identifier comparison is what enables DMARC to authenticate the “From: header” of an email message.

PayPal and Yahoo! were successful in their DMARC pilot program. Criminals could no longer send fraudulent PayPal messages to Yahoo! mail users. Next came a working group of email industry experts including Google, Yahoo!, Bank of America, PayPal, Agari, and a number of other companies interested in scaling up the Yahoo!/PayPal experiment. The goal was to allow anybody on the Internet to control the use of their domain in the “From:” header of email messages. This group was known as MOOCOW, or Messaging Operational Overlay Coalition Of the Willing.

After many months of discussion, debate, and compromise, Microsoft, AOL, Google, and Yahoo! deployed the first working receiver implementations of what came to be known as DMARC in January 2012. Since then, many senders and receivers have implemented this crucial email control, often with the help of a vendor such as Agari. In March 2015, DMARC was detailed in an informational Request for Comments as RFC-7489. Since then, a number of additional consumer mailbox providers have implemented the standard, and most major Secure Email Gateway vendors have incorporated parts of the standard into their services and appliances.

DMARC is designed to be deployed in stages. Companies generally start in “monitor mode” using what’s known as a “p=none” policy. This will provide feedback about servers using the domain name in the “From:” header of the email messages they send. The domain owner uses this information to make adjustments to their SPF and DKIM configurations until all of their legitimate mail sources are properly authenticated. At this point, the policy can be tightened to “p=quarantine”, which sends authenticated messages to the recipient’s spam folder or even “preject”, which causes the message to be blocked outright.

According to DMARC.org, DMARC is designed to:

- Minimize false positives.
- Provide robust authentication reporting.
- Assert sender policy at receivers.
- Reduce successful phishing delivery.
- Work at Internet scale.
- Minimize complexity.

Finally, it is important to realize that DMARC must also be deployed on the receiver side, by email service providers. Currently, the major email service providers, Microsoft, AOL, Google and Yahoo! have deployed DMARC, but smaller email service providers or a self-hosted email server may not provide the same level of protection.

A Practical Deployment of DMARC

Agari is uniquely positioned to share its insight into the practical applications of DMARC deployments because so many of its users are early adopters of DMARC. The following charts provide an anonymized view of Agari dashboards to highlight the positive impact of DMARC. Together, Agari and DMARC are preventing digital deception.

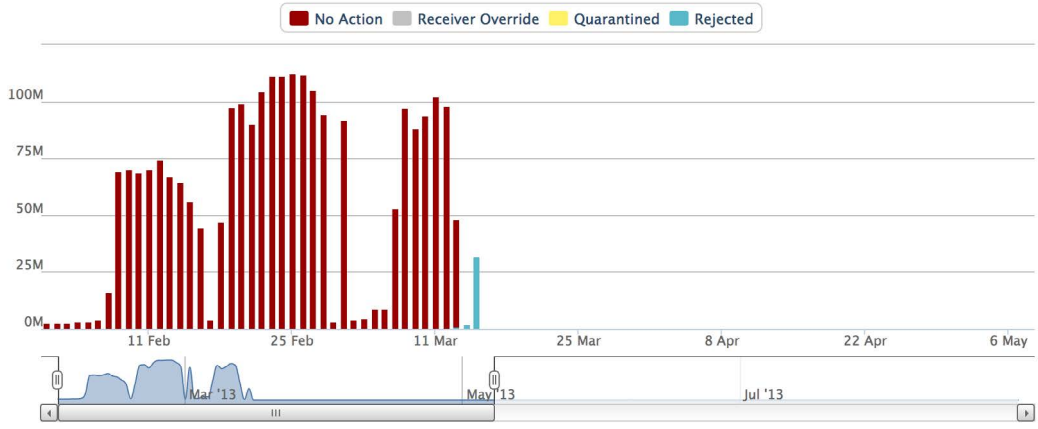


Figure 5 – DMARC Pre and Post Reject

As shown in Figure 5, the Agari client was receiving a tremendous volume of unauthenticated emails – at times more than 100 million per day. These are emails that were spoofing the domain in the "From:" header. Shortly after March 11, 2013, the client implemented a DMARC Reject policy, resulting in millions of spoofed messages that could no longer be delivered. As a result, by the end of that March, these messages all but ceased – the perpetrators realized there was no benefit to continue their campaign when every message was rejected.

Following this same customer's journey, let's fast forward a few years.

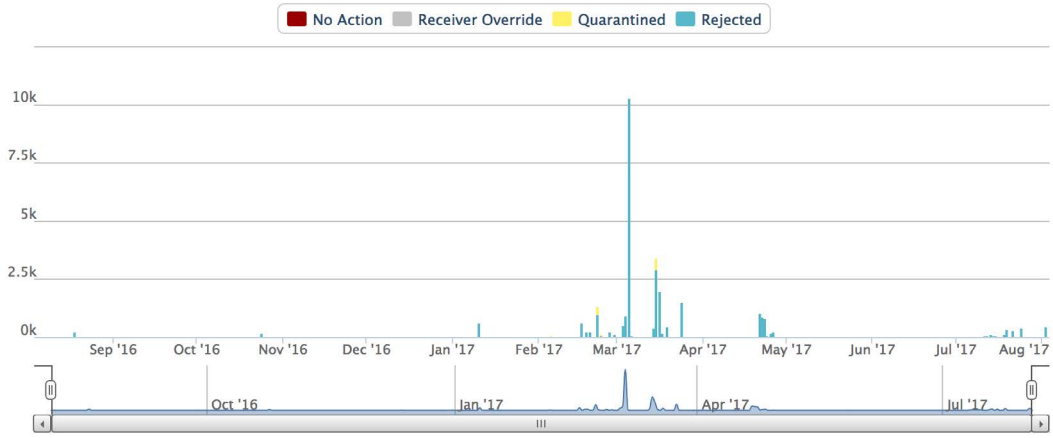


Figure 6 – DMARC Reject

Figure 6 demonstrates that these spoofed messages have been all but eliminated. In most cases, there are simply no messages that are attempted to be sent. However, every so often, a new campaign may emerge, as seen in March of 2017. Even in this instance, the volume of messages sent is only 10,000, which seems insignificant compared to the initial 100 million. Again, these messages are rejected and the campaign drops off, as attackers turn their attention to more vulnerable targets elsewhere. DMARC is so effective at preventing these campaigns that the bad guys literally give up trying.

Finally, let's switch gears to observe the gradual deployment of DMARC from Monitor (None) to Quarantine, to Reject.

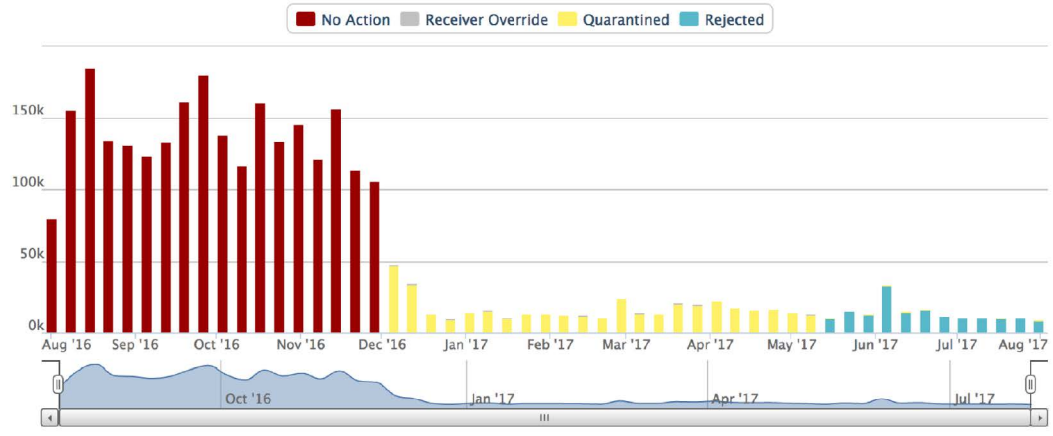


Figure 7 – DMARC Monitor (None), Quarantine and Reject

Figure 7 demonstrates another client's gradual adoption of tighter DMARC policies, precisely as DMARC was designed to be deployed. The initial volume of unauthenticated mail surpassed 100,000 to 150,000 messages per day, which was cut dramatically to 50,000 or less once a Quarantine policy was implemented. After another six months, this is tightened further to a Reject policy, which practically eliminates the volume of unauthenticated email.

Based on the Agari research, many organization find themselves in the first stage of DMARC implementation and unable to progress to quarantine and reject policies. The reason for this is that larger organization have to first identify who is sending email on their behalf and get them to authenticate the email they are sending before changing the policy. Agari is the leading solution to help large organization with the analytics, workflow and services to move to more effective policies, maintain email governance and prevent ongoing brand abuse.

CONCLUSION

Corporations and governments around the world are woefully unprotected against phishing. From the Fortune 500 to the FTSE 100 and the ASX 100, the majority of organizations have not deployed DMARC, and for those that do, the majority maintain a monitor-only "p=none" policy that doesn't protect anyone. These organizations and their customers remain vulnerable to domain spoofing and phishing attacks.

The logical early adopters of DMARC were the original high-value targets of phishing: payment processors, credit cards, banks, shipping and airlines. However, all organizations should be concerned with domain name spoofing to protect their brand reputation and trust.

Deploying a DMARC policy where p=none is simple, but it is only the first step. Organizations must Quarantine, Reject and maintain strong email governance to reap the benefits of DMARC.

To Create or Look Up a DMARC Record:
https://www.agari.com/resources/tools/dmarc/

About Agari

Agari, a leading cybersecurity company, is trusted by leading Fortune 1000 companies to protect their enterprise, partners and customers from advanced email phishing attacks. The Agari Email Trust Platform is the industry's only solution that 'understands' the true sender of emails, leveraging the company's proprietary, global email telemetry network and patent-pending, predictive Agari Trust Analytics to identify and stop phishing attacks. The platform powers Agari Enterprise Protect, which help organizations protect themselves from advanced spear phishing attacks, and Agari Customer Protect, which protects consumers from email attacks that spoof enterprise brands. Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is backed by Alloy Ventures, Battery Ventures, First Round Capital, Greylock Partners, Norwest Venture Partners and Scale Venture Partners. Learn more at http://www.agari.com and follow us on Twitter @AgariInc.