AGARI

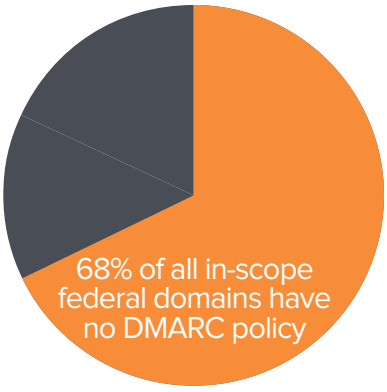
Agari U.S. Federal Government DMARC Adoption:

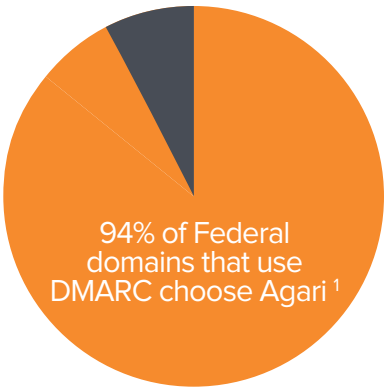
DHS Mandates DMARC for Email Security

Executive Summary

On October 16, 2017, the U.S. Department of Homeland Security issued a Binding Operational Directive (BOD) 18-01 that mandates the implementation of specific security standards to strengthen email and web site security. As part of this directive, all federal agencies that operate .gov email domains must implement a DMARC monitoring policy (p=none) within 90 days. Furthermore, all federal agencies must move to a reject policy (p=reject) by 1 year.

Based on Agari research of public DNS records, 68% percent of all US Federal Government domains do not have a DMARC policy, leaving their constituents unprotected from phishing and other forms of email attacks that impersonate their agency email domains. Due to a lack of an enforcement policy on an additional 20% of domains, almost 90% of federal domains provide no protection against unauthenticated email. Cybercriminals exploit this vulnerability by sending billions of phishing emails per year claiming to be from these government agencies.





[1] Based on the set of 1106 US government domains that a.) are subject to BOD 18-01 and b.) send aggregate data to a 3rd party DMARC vendor.

Email Abuse on Federal Agency Domains

Phishing continues to be a pervasive threat in the United States and around the world.The impact of these threats has been felt specifically by government agencies. Beyond the high-profile targeted attacks that have made headlines, criminals are executing phishing attacks leveraging the brand name of agencies. Indeed, over the last six months, Agari has seen an amplification of attacks against our Federal customers. As the following chart indicates, on the email-sending and defensive domains that we monitor, 25% of email volume was malicious or failing authentication. Almost 90% of our Federal domains were targeted by domain abuse.

Agari Email Trust Network

Agari Protected	Threat Volume	Threat Rate
336.41 M Total Emails	85.56 M Malicious Emails	25.43% Malicious Emails
400 Total Domains	358 Domain Targeted	89.5% Domain Targeted

DMARC Adoption in the Federal Government

Aside from the DHS mandate issued earlier this week, the DMARC standard has been previously cited as a key control to help agencies reduce the likelihood that their domains and brand will be used in an attack. These recommendations came from government bodies including:

FISMA: DMARC (and email authentication) is evolving into a key metric that impacts the FISMA scorecard against an agency.

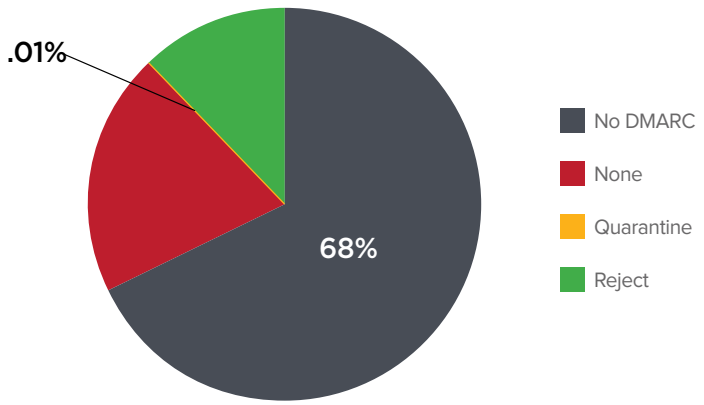
NIST: NIST recommends using DMARC authentication tools to provide protection against phishing (SP 800-177, Trustworthy Email, Section 4.6).

FTC: The FTC recommends wider implementation of DMARC to combat phishing attacks (Staff Perspective, March 2017).

Despite these recommendations, DMARC adoption has been extremely low, enabling malicious actors to abuse that trust and leaving agencies unprepared to prevent it.

On November 7th, 2017, Agari analyzed over the 1106 US government domains subject to the the DHS directive to determine if which domains had deployed a DMARC record in its DNS – and if so, what was the policy. The dataset was provided to Agari by representives of the US government.

DMARC U.S. Federal Domain Adoption and Policies



DMARC adoption – More than 65% government agency domains (1064) do not have a DMARC record on their domains. It's notable that this low adoption rate trails what Agari has recently reported for the commercial sector, where two-thirds (67 percent) of the have not published any DMARC policy.

None Policy – 20% of in-scope federal domains have a none (Monitor) policy. This policy monitors for authentication abuse, but does not prevent it. When combined with the number of domains without any DMARC policy, close to 88% of in-scope of federal agency domains are vulnerable to digital deception, leaving their constituents and email recipients exposed to phishing and fraud. The 'none" policy is the minimal level that that Federal agencies need to implement by the 90 day deadline.

Quarantine Policy – Less than 1% (only 5 domains) were at the initial level of enforcement, or a Quarantine policy (which sends messages that fail DMARC tests into the spam folder).

Reject Policy – 12% (132 domains) have implemented a Reject policy to block messages that fail authentication. Of these domains at a Reject policy, almost 72% of them were so-called defensive domains, which do not send mail. As per the DHS mandates, government agency domains need to be at Reject policy within one year.

Clearly, some agencies are aware of the threat of digital deception and have taken appropriate counter-measures. A few federal agencies, including the US Postal Service, the US Department of Health and Human Service, and the Social Security Administration (among others) 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. However, among other early adopters, a significant number 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.

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.

About DMARC

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 an agency 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. The DHS directive mandates a policy of “none” as a minimum by the 90 day deadline.

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

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

For more information on the DMARC standard, see www.agari.com/dmarc-guide/

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.

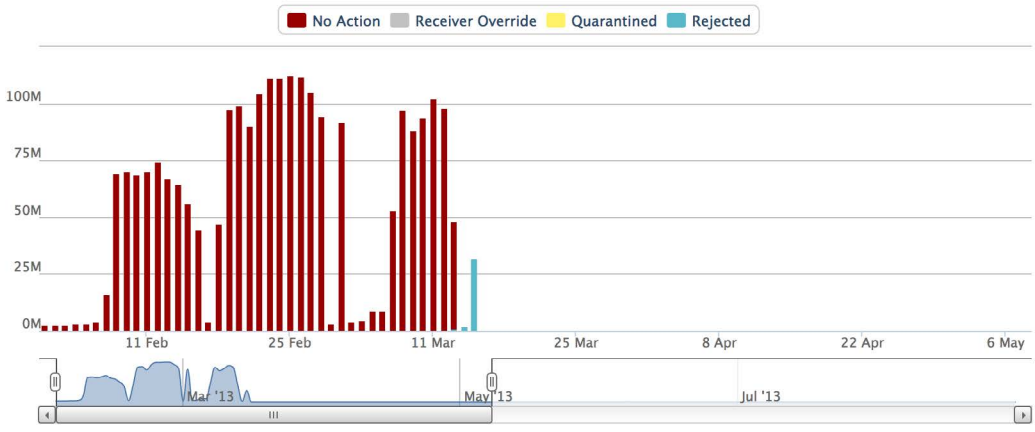


Figure 5 – DMARC Pre and Post Reject

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.

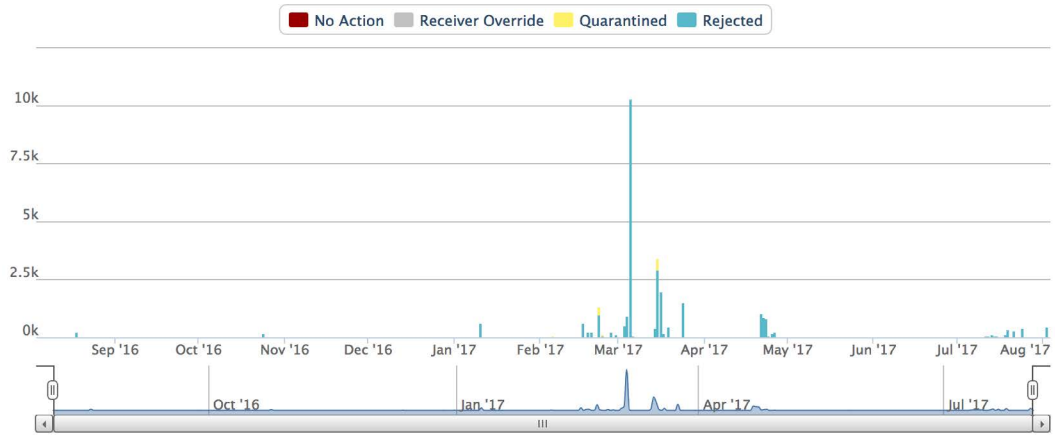


Figure 6 – DMARC Reject

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.

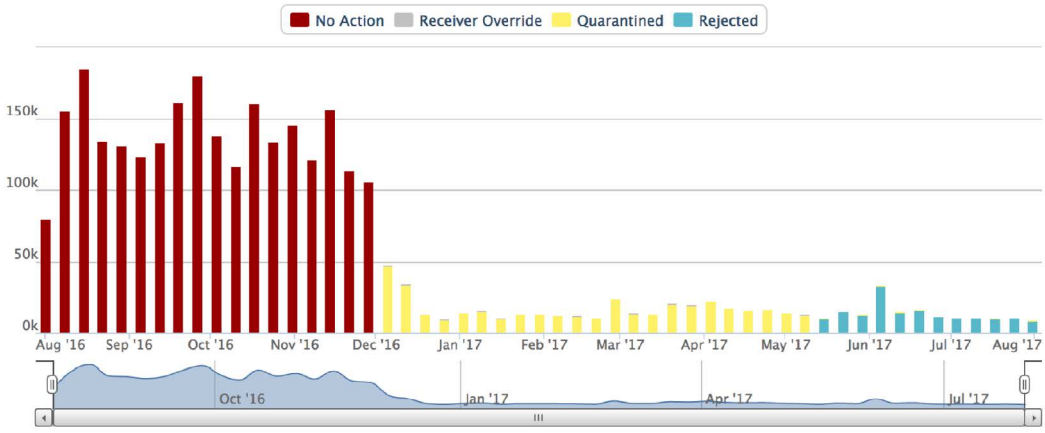


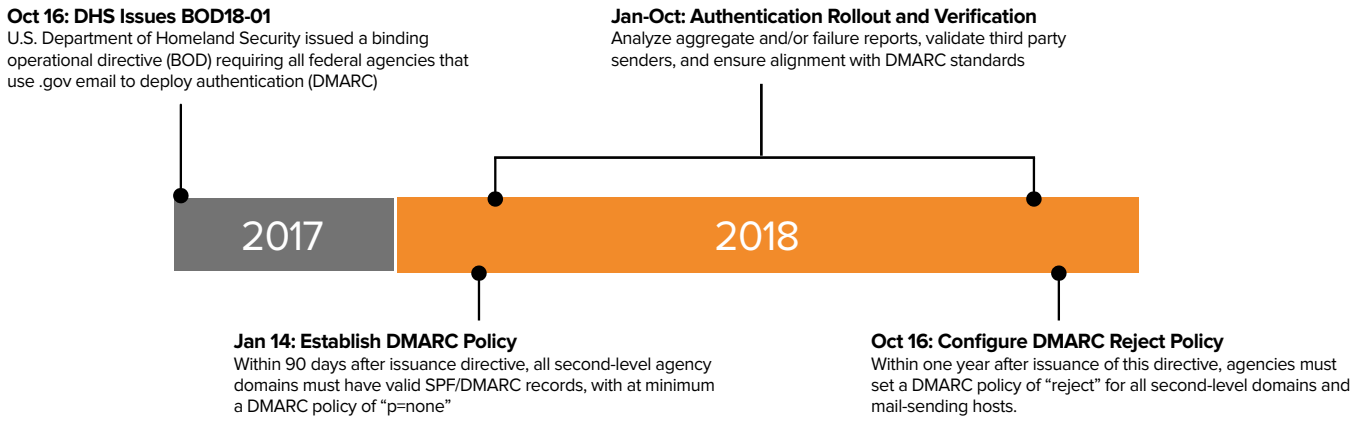
Figure 7 – DMARC Monitor (None), Quarantine and Reject

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 organizations 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

The logical early adopters of DMARC were the original high-value targets of phishing: payment processors, credit cards, banks, shipping and airlines. However, government agencies should be equally concerned with domain name spoofing to protect their reputation and safeguard their citizens. The recent mandate by the Department of Homeland Security for all agencies to implement DMARC on .gov domains underscores this fact.



The analysis in this paper has shown that federal agencies are woefully unprotected against phishing. Almost 68% of federal agencies' domains currently do not have a DMARC policy. For those that do, the majority maintain a monitor-only "p=none" policy that doesn't protect their constituents. These agencies and their email reciipients remain vulnerable to domain spoofing and phishing attacks. Deploying a DMARC policy where p=none is simple, but it is only the first step. To fully protect against phishing threats against both the federal government and the public at large (and maintain strong email governance), federal agencies must ultimately move to Quarantine and Reject policies.

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.