AGARI

DMARC Adoption Update for Healthcare

Special Edition for NH-ISAC

May 2018

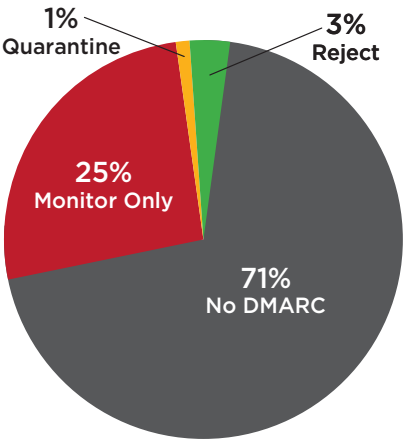
On May 10, 2018, Agari conducted an update to our ongoing tracking of DMARC adoption trends, examining public DNS records for primary corporate website domains of global healthcare/pharmaceutical companies with revenues above $1B. Our key findings:

Negative trends:

- *Poor overall adoption:* The overwhelming majority of healthcare organizations still do not have a DMARC record published
- *Ongoing lack of enforcement:* Most organizations with records don't take action against fraudulent emails

Positive trends:

- *Adoption increased:* More organizations than ever established an initial DMARC record and set up monitoring policies
- *Enforcement rates doubled:* "Getting to Reject' ensures mailbox providers block any malicious emails from spoofing your brand



Healthcare Industry DMARC Adoption

DMARC adoption – Currently, 71% of large healthcare organizations (390) do not have a DMARC record on their domains. It's notable that this low adoption rate trails what Agari has previously reported for the commercial sector at large, where two-thirds (67 percent) of Fortune 500 have not published any DMARC policy on their domains.

None Policy (Monitoring) – 25% of healthcare organizations 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, we can conclude that almost 92 percent of healthcare organizations are vulnerable to domain abuse, leaving their customers and email recipients exposed to phishing and email fraud.

Quarantine Policy (Enforcement) – Approximately 1 percent (8 organizations) implemented a Quarantine policy, which redirects messages failing authentication to the configured spam folder.

Reject Policy (Enforcement) – 3% (16 organizations) have implemented a Reject policy to block messages that fail authentication. This is the ideal state as it protects criminals from spoofing an orgnization's brand.

While the number domains at enforcement level (Quarantine and Reject) is relatively low, the 9 month trend is encouraging, as shown in the following table.

Enforcement Changes on Healthcare Domains Over 9 Months

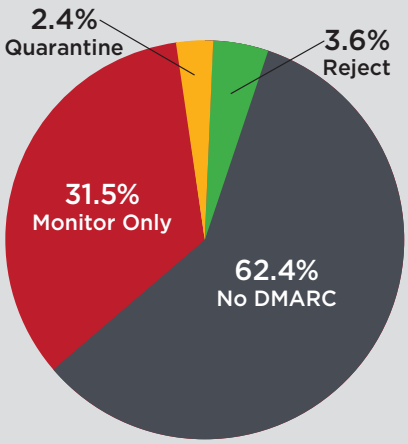
	Domains at Quarantine		Domains at Reject	
May 2017	2	Bruker Corporation, Sharp HealthCare	5	Aetna Inc., Flex , Geisinger Health System, HealthNow New York, Inc., Houston Methodist
Nov. 2017	6 200% ▲	Bruker Corporation, **Gilead Sciences, Inc., Kettering Health Network,** Sharp Healthcare, **Sun Pharmaceutical Industries Ltd, Tampa General Hospital**	8 33% ▲	Aetna Inc., **Blue Shield of California**, Flex, Geisinger Health System, HealthNow New York, Inc., **Horizon Blue Cross Blue Shield of New Jersey**, Houston Methodist, **Spectrum Health**
May 2018	8 33% ▲	**baycare.org**, bruker.com, **childrens.com**, ketteringhealth.org, **pfizer.com**, **primehealthcare.com**, sharp.com, sunpharma.com	16 100% ▲	Aetna Inc., Blue Shield of California, **cerner.com**, Flex, Geisinger Health System, HealthNow New York, Inc., Horizon Blue Cross Blue Shield of New Jersey, Houston Methodist, **merck.com**, **priorityhealth.com**, **rpsweb.com,** Spectrum Health, **synthes.com**, **texashealth.org**, **tgh.org**, **unitedhealthgroup.com**

NH-ISAC Spotlight: An Update on the DMARC Pledge

On October 16th, 2017, the Department of Homeland Security (DHS) directed all federal agencies to implement better security protocols on government emails and websites by implementing DMARC. That same week, Jim Routh, Chairman of the NH-ISAC, issued a letter enlisting NH-ISAC members to take a "pledge" to implement DMARC. Below is an excerpt from that request:

> *I am asking you to make a pledge to implement DMARC in 2018 on behalf of your organization in an effort to dramatically improve cyber resilience for healthcare. I implemented DMARC three years ago for my enterprise and we continue to get a 10% lift in click-through rate for all external emails each year as a key indicator of the increase in trust from our members.*

For more information on the pledge, see https://www.surveymonkey.com/r/JCKLCYD



NH-ISAC DMARC Adoption as of May 2018: Low, but still outpacing the larger Industry

On a percentage basis, the membership of the NH-ISAC is ahead of the superset of large healthcare organizations when it comes to implementing DMARC.

In keeping with the larger trend, the majority (62.4%) of NH-ISAC members have no policy at all. However, this represents a 9% improvement over the industry at large that we analyzed.

Focusing on rest of the NH-ISAC member organizations that do have a DMARC policy, the distribution of policies is fairly similar from a Monitor and Quarantine policy perspective. The percentage of domains at the all-important Reject policy – 3.6% – for the first time exceeds that for the larger healthcare sector (3%). This translates to 12 NH-ISAC organizations, versus 16 in the global data set.

These improvements notwithstanding, the overall adoption numbers are low for NH-ISAC, especially considering the security risk of fraudulent or otherwise unauthenticated email traversing healthcare domains. Given the vital role the Healthcare and Public Health sector serves in the nation's critical infrastructure, embracing DMARC controls within this ecosystem is a logical step to eliminate domain spoofing as a phishing technique for patients and consumers.

Take the NH-ISAC DMARC Pledge: **nhisac.org/DMARC-pledge**
Create or look up a DMARC record **agari.com/resources/tools/dmarc/**
Contact Agari to help protect your customers with DMARC: **agari.com/contact-us**

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, machine learning-based Agari Identity Intelligence 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.