VALIMAIL
TRUST YOUR EMAIL

DOMAIN SPOOFING DECLINES AS PROTECTIVE MEASURES GROW

VALIMAIL EMAIL FRAUD LANDSCAPE
WINTER 2020

EMAIL: THE FRONT LINE OF CYBERCRIME

The battle against phishing rages on. Estimates from the FBI peg losses due to just one type of email-based attack, the business email compromise (BEC), at $1.7 billion in 2019 alone. Other sources have noted that 83% of email attacks are brand impersonations and another 6% are impersonations of people, meaning nearly 90% of all email attacks rely on deceptive sender identity (i.e. spoofing). And meanwhile, email remains the single largest vector for initiating cyberattacks of all kinds, as many studies have shown over the years and IBM Security recently confirmed.

In this battle, DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a front-line defense — and it's working. DMARC gives domain owners visibility into what services (and which bad actors) are sending email "from" their domains. When configured properly (with an enforcement policy), it prevents email spoofing. Once at enforcement, a domain can only be used by authorized senders. Email attackers are then forced to rely on other, easier-to-detect impersonation techniques — or they move on to other targets. In fact, Valimail has observed that the number of attempts to spoof a domain typically drops to zero or near zero within a few months after that domain moves to DMARC enforcement.

Evidence from Valimail shows that the use of DMARC is growing. And, despite relatively low rates of configuring it with enforcement policies (which actually stop spoofing), DMARC is having a noticeable, positive effect on reducing exact-domain spoofing globally.

KEY FINDINGS

Nearly 1 million domains globally now have DMARC records

70% growth in DMARC records in the past year, and 180% growth over two years

Only 13% of all DMARC records are configured with enforcement policies

23% of billion-dollar companies' domains are at enforcement

1% of global email volume, at a minimum, is sent using a spoofed domain

The United States remains the largest source of spoofed email by volume

Vietnam, Russia, China, and India continue to have a high proportion of spoofs among email originating from those countries

Domains without DMARC enforcement are spoofed at 3.93x the rate of domains with DMARC enforcement

"80% of the world's inboxes do DMARC checks on inbound email, enforcing domain owners' stated policies."

THE GROWTH OF DMARC ON TWO FRONTS

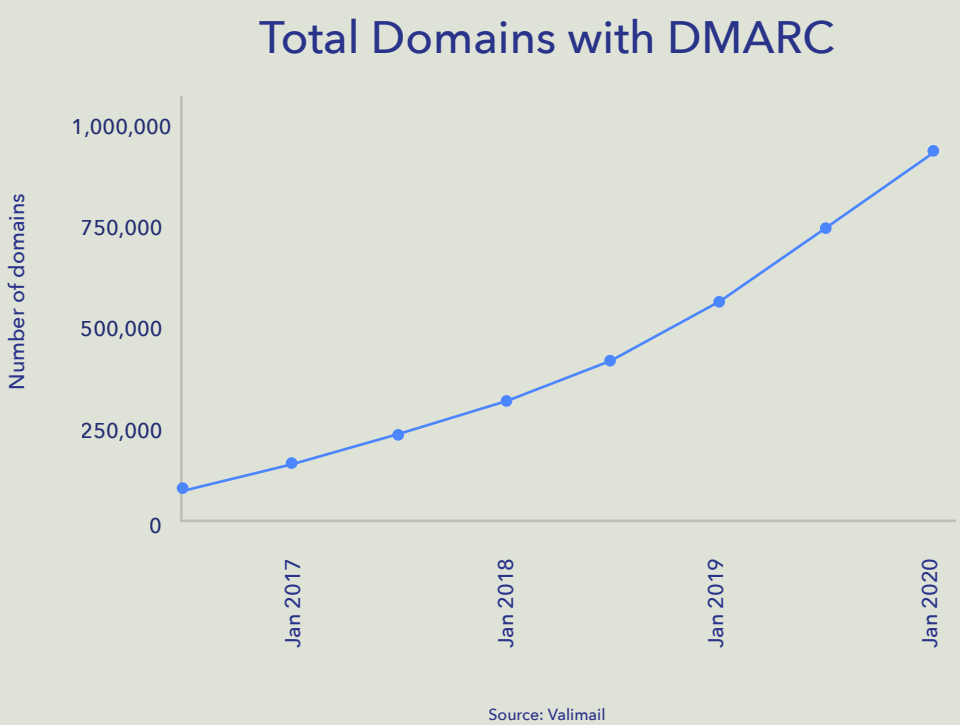
Given its benefits, it's no surprise that the growth of the DMARC standard has been impressive.

One the receiving side, major email receivers have been supporting the standard for years now. Valimail data has shown for several years that about 80% of the world's inboxes (including virtually all U.S.-based email providers) do DMARC checks on inbound email messages, enforcing the domain owner's stated policies. Our data from analysis of DMARC reports shows that proportion remained consistent in the second half of 2019.
.

However on the sending side, more and more domain owners are waking up to DMARC's potential. As of the start of 2020, nearly one million domains — 933,973 to be exact — have published DMARC records.

That's an increase of 70% over one year prior, and a more than 180% increase over two years ago.

Note: Valimail's analysis counts organizational domains only. Unlike some other reports on DMARC's market penetration, we are not including subdomains in these totals.

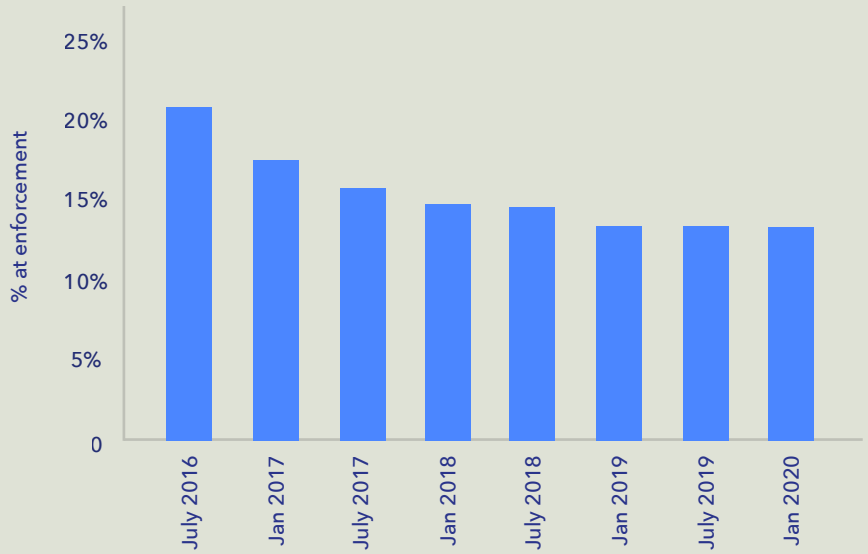


Source: Valimail

DMARC ENFORCEMENT RATES

Merely publishing a DMARC record is not sufficient to protect a domain against spoofing, however. Domain owners must also configure an enforcement policy (one that directs mail receivers to quarantine or reject non-authenticated email, with no exceptions for subdomains). If they don't do so, then mail receivers will not take any particular actions on email that appears to come from the domain but which fails authentication.

Percent of DMARC records at enforcement



Source: Valimail

The syntax of DMARC is simple, and in principle it's easy to set an enforcement policy simply by adding "p=quarantine" or "p=reject" in the proper place in the domain's DMARC record. However, domain owners who do this without first carefully auditing their email environments run into trouble. If you don't properly authorize all the services that you want to send email on your behalf (e.g. a corporate payroll system, or mailing list manager) then the enforcement setting will tell mail servers to reject messages from those senders. Such authorization is done through SPF and/or DKIM, two other email standards that let domain owners specify which senders are allowed to send "as" them.

As a result, the best practice is to start in monitor mode (a policy of "none," indicated by "p=none" in the DMARC record), which allows you to collect detailed, daily reports from mail servers about exactly which senders are authenticating and which ones are not.

Unfortunately, that's as far as most domain owners get. Valimail's analysis shows that of the 933,000 organizational domains with DMARC, just 13% are at enforcement.

Worse, that percentage has generally declined over time, although it has remained level in the past twelve months. The inescapable conclusion: Interest in DMARC is growing, but DMARC expertise is not keeping pace.

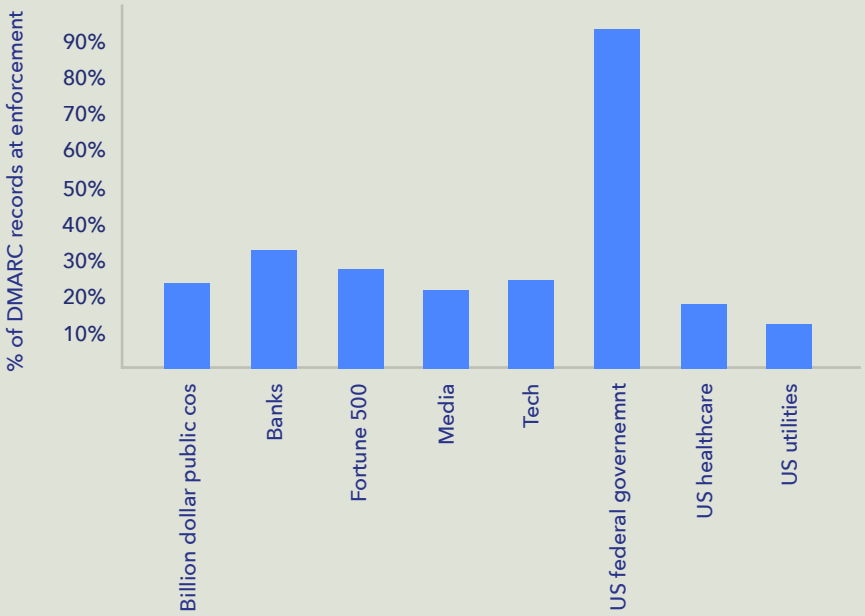
INDUSTRY ANALYSIS

The majority of the 933,973 domains with DMARC are owned by small companies, small nonprofits, or individuals. Perhaps companies with large IT budgets can do better at deploying DMARC and getting to enforcement?

The answer: A little bit — but it depends on the industry. Among billion-dollar publicly traded companies (globally), almost 52% of these companies' primary domains have DMARC records. But of those with DMARC, only 23% are at enforcement — significantly better than the global average of 13%, but not an order of magnitude better.

Other industries have similar or slightly better rates of success at getting to enforcement: Global banks and financial services companies 33%, Fortune 500 companies 28%, global tech

Enforcement success rates by category



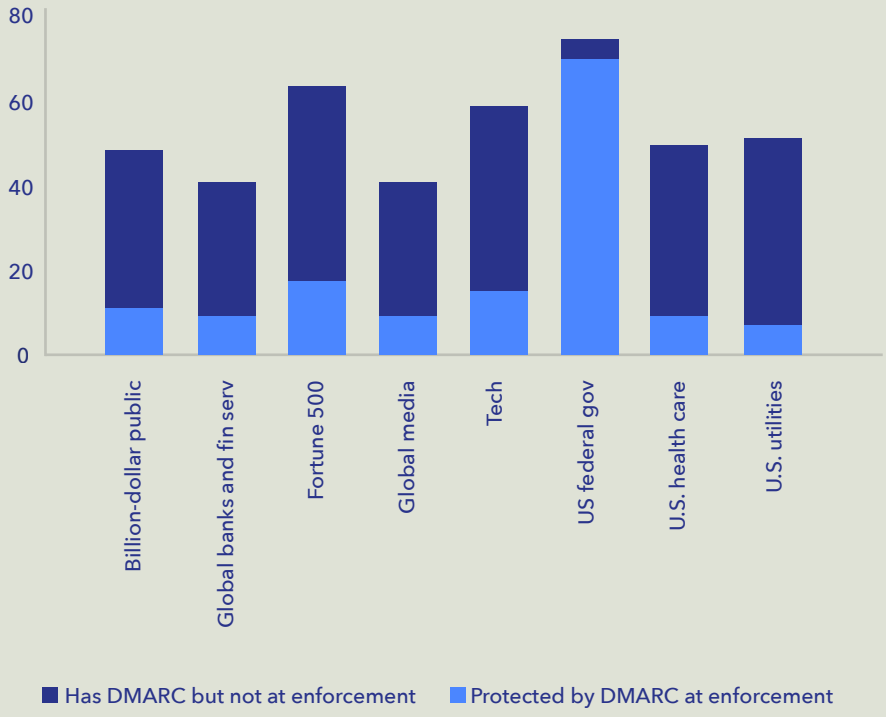
Source: Valimail

companies 24%, and global media companies 22%. Somewhat lower on the scale are U.S. healthcare providers with 18% and U.S. utilities with 13%. (Note: all categories were limited to $1B+ revenue companies, except for media companies, which included $500M+ revenues.)

The only standout category is the set of U.S. federal government domains, of which 79% have DMARC records. Of those DMARC records, 93% are at enforcement. These are remarkably high figures — a tribute to the success of a 2017 directive from the Department of Homeland Security, BOD 18-01, which mandated DMARC at enforcement for most executive branch domains by January 2018. At the time that BOD 18-01 was issued, fewer than 20% of government domains had DMARC and almost none were at enforcement. Although the mandate was unfunded, several things about it favored success: It was clearly worded, included specific guidance for agencies to follow, and was coupled with tools that agencies could use to check their status and interpret DMARC data.

Despite the fact that almost no industry has a better than 25% success rate in getting DMARC records to enforcement, some industries are doing better at protecting themselves, simply because they have a larger proportion of domains attempting DMARC.

DMARC status by category



Source: Valimail

For instance, 67% of Fortune 500 companies have deployed DMARC, and about a quarter of those are at enforcement. This means that almost 20% of the Fortune 500 are now protected from impersonation by DMARC at enforcement. Global tech companies have taken a similarly aggressive approach to DMARC deployment, so 15% of these domains are protected.

But global media companies lag: Only 43% of this category has a DMARC record, and with a success rate of 22%, this means that just 10% of this category's domains are protected.

THE RATE AND SOURCES OF SPOOFING

Valimail's data shows a slow decline in the rate of email spoofing through exact-domain impersonation over the past several years. In the last year it's remained roughly level at about 1% of all email volume authenticated by Valimail. This is significantly down from 2.3% in the first half of 2018, and 5% in 2017.

One thing to note is that, as Valimail's customer base has grown, so too has the number of domains at enforcement that we manage.

To put this another way: The domains that Valimail manages have a much, much higher rate of enforcement than the global average — and indeed our customers' enforcement success rate is far higher than that of every private sector industry.

Since domains at enforcement are less likely to be spoofed (fraudsters give up on spoofing a domain once they notice that spoofing no longer works), we have observed that the rate of fraudulent activity for a domain almost always declines towards zero within a few months after a domain gets to enforcement.

In fact, comparing the volume of fraudulent email during H2 2019, Valimail found that domains without DMARC enforcement were spoofed 3.93x more often compared with domains at DMARC enforcement.

Additionally, the domains that Valimail manages include some high-volume senders of legitimate mail, further skewing the statistics.

The result: The true global rate of fraud for unprotected domains is almost certainly higher than what is shown in this dataset, as it is drawn from a subset of Valimail-managed domains. However, from this dataset we can get a reasonable picture of where in the world fraudulent email originates, both by overall volume and by which percentage of a country's email is fraudulent.

Top 10 sources of spoofed email (H2 2019)

Country	Suspicious email count	% suspicious
United States	38,278,235	0.2%
Germany	15,549,633	76.8%
Vietnam	11,763,184	99.8%
Russia	11,013,184	93.0%
United Kingdom	10,856,172	66.8%
China	5,807,768	98.8%
France	5,607,213	54.0%
Netherlands	5,207,620	23.4%
India	5,186,443	91.6%
Singapore	4,669,986	73.6%

Source: Valimail

FOR MORE INFORMATION ON VALIMAIL'S SENDER IDENTITY PLATFORM, SEE VALIMAIL.COM.

About the author: Dylan Tweney is the Vice President of Communications at Valimail. The former editor-in-chief of VentureBeat and former editor at Wired, he oversees Valimail's research program.