UDC 004[492.2]

WAYS TO PROTECT A USER'S EMAIL

ANDREI HAIDZEL, DMITRY PIATKIN
Polotsk State University, Belarus

This article describes the process of mail attacks (phishing), because this is how most cyberattacks begin, and technologies that help protect your mailbox.

When creating the Internet, initially there was no way to check the identity of the sender. During the development of the basic e-mail protocols, the costs of processing power, implementation and ease of use were balanced with the risk of fraud. It was hard to imagine that 84% of all e-mail in the future will have a malicious load and be phishing or spam.

The result is that the headers of letters, including the "From:" and "Reply-to:" fields, are very easy to forge. In some cases, it's as easy as typing "john@company.com" in the "From:" field. Combining this with unsuspecting content, convincing graphics and formatting, it is possible to deceive people who thought that the message in their mailbox really came from the bank, the Federal Tax Service, the head or the president of the United States.

Taking into account the widespread distribution of e-mail, you are aware of the basis of our current information security crisis. The weakness in e-mail led to a lot of phishing attacks aimed at getting people to click on malicious links, downloading and opening malicious files, sending a W-2 form (analogous to a 2-NDFL in the US), or transferring money to criminals' accounts.

More recently, Coupa, a Silicon Valley company, has been the focus of attention after sending data on the wages of all 625 employees to the scammer. Russian hackers managed to distribute malware-infected PDF files by sending emails impersonating Harvard's Kennedy School. And last year, one of Europe's biggest companies lost $45M when an employee mistakenly wired the money to a fraudster's account in response to a bogus email. The FBI estimates that one type of phishing attack, the Business Email Compromise (BEC), costs U.S. companies $3 billion per year. [1]

On databreaches.net, a list of facts of phishing form W-2 was compiled. Work on the list this year indicates that the number of cases since 2016 are growing and at the moment it consists of 204 reports. Under the list, you can understand that there are cases of theft of these thousands of employees and this kind of fraud is very common.

HOW AN ATTACKER CAN FORGE AN UNPROTECTED E-MAIL

In fact, the fake address in the "from" field is the basis and the initial stage of most attacks. Why worry about falsifying e-mail with conditional "company.com", when it is possible to simply register a similar fake domain (for example, c0mpany.com) and use it? Or create a Gmail account (randomaddress1347356@gmail.com), assign it a friendly name that looks like the name of the CEO of the company? Because, in fact, to forge sending a letter from a real person's address is even easier than registering a fake domain or creating a Gmail account.

Three simple ways:

On the Internet, you can easily find sites that allow you to send fake emails. There are dozens of them, just a couple of examples: spoofbox.com and anonymailer.net. Many of them are free, some cost money, these services are positioned as legitimate, and the main purpose of use is the drawing of friends.

The algorithm for using is simple. It is only necessary to enter the e-mail address of the recipient in the field "To:", put any desired e-mail address in the "From:" field and after the message is created, confirm the sending. Under the terms of the user agreement, the responsibility for the damage lies entirely with the customers of the service.

The next method is sending using the UNIX command line. If you have a computer with a configured mail service, just type this command: mail -aFrom:whatever@anydomain.com

As a result, you receive a message in which the "From" field will contain "any@anydomain.com". Entering the subject line and the rest of the message, after pressing Ctrl + D, the message is sent to the recipient. The working capacity of this idea depends on how your system is set up. Nevertheless, it works in many cases.

Using PHP, you can create an email with a few lines of very simple code:

```
<?php
$to      = 'nobody@example.com';
$subject = 'the subject';
$message = 'hello';
$headers = 'From: webmaster@example.com' . "\r\n" .
    'Reply-To: webmaster@example.com' . "\r\n" .
    'X-Mailer: PHP/' . phpversion();

mail($to, $subject, $message, $headers);
?>
```

In fact, these are lines of code used as an example in the online guide for the function of sending mail with additional headers / header.

These spoofing tools are greatly simplified. To make messages more realistic, it will take a little more work and, of course, social engineering skills. But the main technical component is very simple. The only thing that really prevents spoofing is the authentication of e-mail by sharing the SPF record, DKIM signature and DMARC. Next, we will describe how these technologies work and how. They are not new, but fortunately for scammers, most domains on the Internet are not yet protected. For example, only about 4% of .gov domains use authentication. What about the other 96%? Attackers can send emails in the guise of outgoing mailboxes of these domains at any time.

According to the source, one of four letters from .gov domains is fraudulent. Domains like justice.gov. House.gov. Senate.gov. Whitehouse.gov., and also domains like democrats.org, dnc.org, gop.com, rnc.org. And DonaldJTrump.com – all of them can be easily used for spoofing by mail scammers.

Methods of protection against spoofing:

The above-described ease of use of non-authenticated e-mail vulnerabilities and the widespread use of these methods as the initial stage for the largest cyberattacks, focuses the attention of the IT community on the need to use e-mail authentication technologies. By implementing email authentication, you can ensure that any user - employee, client or partner receiving an email, will be able to determine whether an email has been sent by a legitimate representative of the company. In addition, you can get transparency and control over who sends e-mail on your behalf.

The importance of this has increased dramatically due to the rapid growth of cloud services (SaaS), more than 10,000 of which send e-mail on behalf of their customers on the topic of sales, marketing, customer support, HR, accounting, legal and other services. Due to forced authentication, you can block anyone who tries to send a message on your behalf - spammers, phishers and even "gray" senders, which may be legitimate, but not listed in the list of allowed.

E-mail authentication standards allow the mail server to verify that an email with your domain in the "From:" field was allowed to be sent on your behalf. Before the message reaches the Inbox of the recipient, the mail server can check:

• Using the SPF record, does the sending server have the right to use the domain name (or names) specified in the message headers?

• If a cryptographic DKIM [2] signature is attached to the message, using an open version of the key in the DNS domain record, you can decrypt the headers of incoming messages and find out whether the message is actually from the claimed sender.

• Due to DMARC [3] configuration, domain owners can create mail processing rules that came from domains that have not been authorized and check whether the headers match with each other (for example, the From: and Reply-to :) fields. The rules include instructions on what the receiving server should do with messages that have not been authenticated, for example, do not skip them, put them in a spam folder, or mark them as potentially dangerous. Authentication by email gives the domain owner global control over what happens to messages sent on their behalf by anyone and anyone. For example, if you represent a mail-sending domain and publish a DMARC record requesting information, you will receive from all recipient domains that also support DMARC statistics about all mail messages that come with a return address from your domain. Statistics comes in XML and contains the IP address of each sender that is subscribed by your domain, the number of messages from each IP address, the result of processing these messages in accordance with the DMARC rules, the results of the SPF and the results of DKIM

WHY DO YOU NEED THE SHARED USE OF THESE TECHNOLOGIES?

In a simplified sense, SPF [4] allows you to create a whitelist for IP addresses. If the mail server with an IP address that is not on your list tries to send an email using your domain, the SPF authentication test will not be passed. However, a big problem with SPF is that the domain specified in the Return-Path field for authentication is used, and not the From field that people are actually reading.

Worse, phishing scammers can set up an SPF record for their own domains. They can then send emails that appear to come from a trusted company or brand, but the domain of that company will be displayed in the From field, and the domain of the fraudster in Return-Path. Such letters will be authenticated by SPF. The additional use of DMARC solves this problem by allowing the domain owner to require an "equalization", which means that the return and outbound addresses must be the same.

SPF records are text, but the syntax is quite complex. It is easy to make typos that are difficult to detect. In doing so, they will make the SPF record useless. An analysis of the SPF [5] records of all 62 sponsors of the RSA 2017 conference showed that only 58 published SPF, while 17 sponsors of the Cybersecurity Conference had errors in the recording. Companies that do not have much experience in the IT field often find SPF even more difficult.

Also, DKIM is not particularly effective against fraud without the use of DMARC. To stop phishing, the most important address is the domain in the From field. However, checking only the DKIM signature does not say anything about the domain in this field. The domain used to sign the message may be completely different from the domain specified in the From field. In other words, hackers can create messages that are signed through DKIM [6] using the domain they control, but the "From" field will contain your bank's email. Most people do not intend to dig into the headers of all incoming messages to make sure that the DKIM signature data is legitimate. It is also worth considering a large number of legitimate e-mail services that can make mailings on behalf of the sender and the problem of secrecy of the private key used to sign messages.

These two early standards, although important, contain important gaps. DMARC [7] is based on them and supplements. DMARC significantly increases the credibility of the email you send, regardless of whether emails from your own mail servers or cloud services that you authorize to send e-mail.

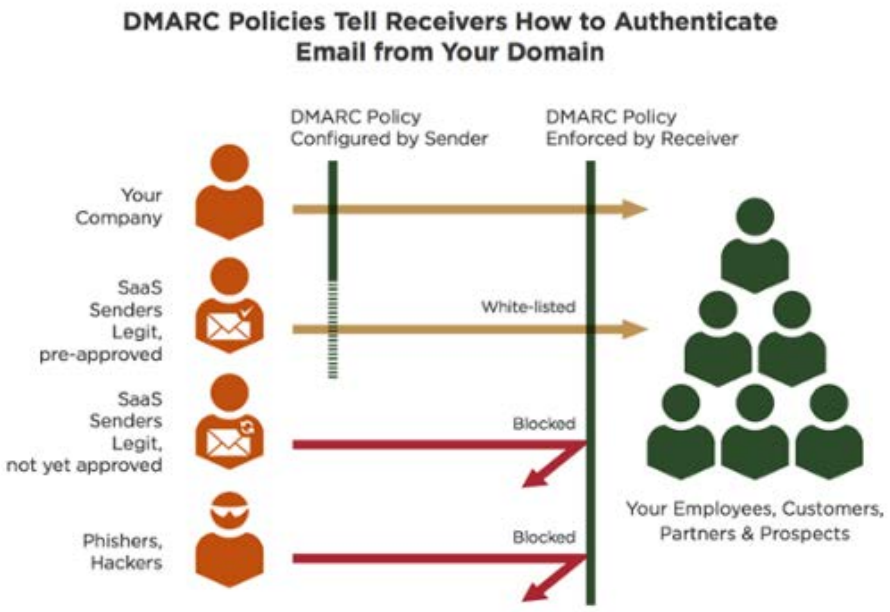

Fig. 1. Diagram of DMARC operation

The main contributions of DMARC are:

1. Configuring a policy that tells receiving e-mail servers what to do with e-mail messages that are not authenticated (nothing, quarantine or failure),

2. providing a reporting mechanism.

Having a policy and a feedback mechanism is what makes it work.

REFERENCES

1. What Is Email Authentication? [Electronic resource] / ValiMail. – Mode of access: https://blog.valimail.com/what-is-email-authentication. – Date of access: 07.01.2018.
2. DomainKeys Identified Mail [Electronic resource] / Wikipedia – The Free Encyclopedia. – Mode of access: https://ru.wikipedia.org/wiki/DomainKeys_Identified_Mail. – Date of access: 10.01.2018.
3. Domain-based Message Authentication [Electronic resource] / Wikipedia – The Free Encyclopedia. – Mode of access: https://ru.wikipedia.org/wiki/DMARC. – Date of access: 13.01.2018.
4. Sender Policy Framework [Electronic resource] / Wikipedia – The Free Encyclopedia. – Mode of access: https://ru.wikipedia.org/wiki/Sender_Policy_Framework. – Date of access: 13.01.2018.
5. What Is SPF? [Electronic resource] / ValiMail. – Mode of access: https://blog.valimail.com/what-is-spf. – Date of access: 15.01.2018.
6. What Is DKIM? [Electronic resource] / ValiMail. – Mode of access: https://blog.valimail.com/what-is-dkim. – Date of access: 16.01.2018.
7. What Is DMARC? [Electronic resource] / ValiMail. – Mode of access: https://blog.valimail.com/what-is-dmarc. – Date of access: 18.01.2018.