VOL. 11, NO. 19, OCTOBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

NEW PHISHING WAVE IN RUSSIA: CORPORATE MAILBOX PASSWORD THEFTS

D. S. Silnov and V. G. Ivanenko
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia
E-Mail: ds@silnov.pro

ABSTRACT

The technologies used to steal passwords are developing day by day. A new technology has become popular in Russia. It gives hackers the opportunity to make money on corporate wars and the intentions of certain people to get access to other persons' information. Today, the password stealing technology has been put in mass production: the pricing has been set, and anyone can place an order for another person's mailbox to be hacked. Current research gives opportunity to develop new protection techniques.

Keywords: mailbox, phishing, hackers, corporate mail.

1. INTRODUCTION

Phishing is a kind of social engineering based on the user ignorance of the basics of online security. The goal of this internet fraud is getting access to the user personal data: login names, passwords, credit card numbers and access codes, and other sorts of confidential information [1]. In most cases, phishing is done by redirecting users with a link or automatic redirection to a fake web page where they enter their confidential data. This is achieved by deceiving the users: the fake web page looks the same way as the original page of the service that the trickster is trying to get your password to [2].

Today, phishing is most used to get access to the free email services. This is because the free services provide the most user-friendly email message handling opportunities. To start working with such a service and receiving emails, you only have to complete a quick and simple registration procedure, and right after that you are able to handle your messages from a web browser window from any corner of the world [3].

In most cases, the internet service providers give their users email boxes when they conclude the contracts for connection. But as a rule, special email applications are required to work with that email boxes. If compared to the free web-based services, making the necessary settings in those applications represent a more difficult task for inexperienced internet users, and besides, such email boxes can only accessed from the computers that the applications are installed and adjusted on. So users prefer the free email services as they provide a more user-friendly alternative.

The low online security level in Russia can be seen through the fact that not only private individuals use the free email services, but also a lot of business people of all categories do so. For example, when buying food, we can see that there are lots of producers who have their email addresses registered with the free email service providers. Those free email service providers now offer the domain binding service, so email boxes can be created with unique domains, without attracting the attention of the swindlers but still enjoying the advantages of the free email services. But the situation gets aggravated as there are a lot of business owners who do not use that opportunity as it requires some special skills in working from a DNS domain. Most often, companies prefer not to resort to the help of competent specialists and to do without any outside assistance for the trivial cost saving purposes [4].

And if the use of the free email services by private individuals looks reasonable, it is a huge gap in the security for companies, as in those mailboxes they keep and update, on a daily basis, great amounts of valuable information concerning their activities, including financial reports, various orders and bank statements. To get access to the corporate information, all you have to know is the password to a specific mailbox, because the email address is what is used as the login name in the system.

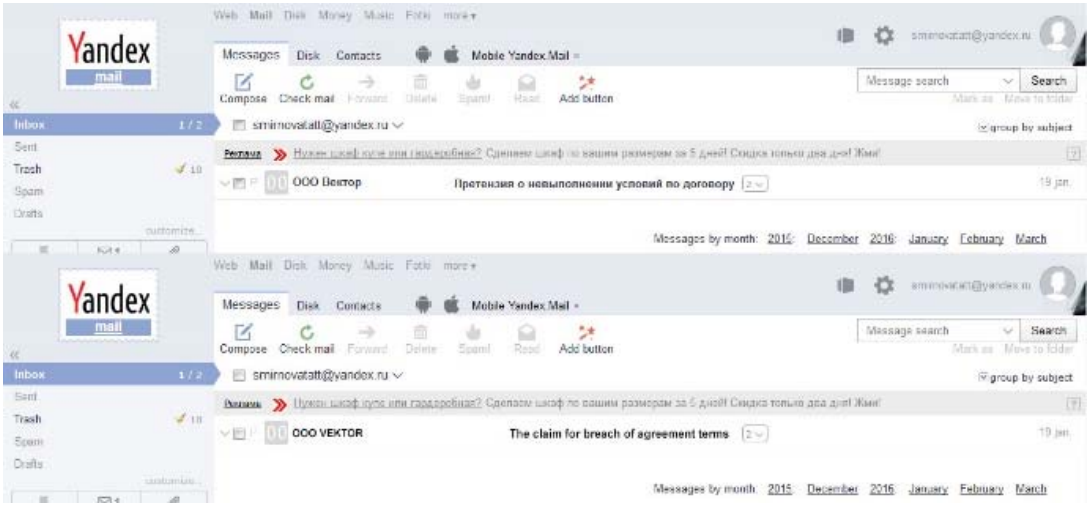

Figure-1. Corporate mail inbox with incoming phishing mail (Russian version on the top, translated - on the bottom).

Having access to the email box actually means having access to all the information kept in the messages that have been sent and received. If when trying to get access to the mailbox, the intruder changes the password, the legal owners of the mailbox lose the ability to access it, for a period of time or forever, until the password is restored with the help of the support department. If this happens, the mailbox owners understand their email has been hacked and take some actions to avoid it in the future. Upon finding the password, the intruders have access to all the messages stored in the mailbox at the moment, so they can get all kinds of information they need from those messages.

But what is even more effective is to get access to the mailbox without changing the current password. Hence, using the unchanged password, both the mailbox owners and the intruders can enter it, but the mailbox owners may not even think that somebody else also has access to their mailbox, so the intruders can read not only the information available in the mailbox at the moment, but also see all the messages that appear there in the future without being noticed. This is exactly the way mailbox phishing is done in most cases.

There is another factor that makes the situation even worse. The password to the mailbox is often used in some other services which belong to the same owner, or the emails kept in the mailbox contain such passwords. So, by getting access to a single mailbox, the intruders also get information and access to other accounts that may also contain some valuable or confidential information, e.g. passwords to social network accounts where some correspondence may be kept as well [5].

In Russia, in the past six months, email account hacking services became quite popular. Before, you had to visit special forums and use email and ICQ to contact those who provide such services. But now there are dedicated websites where you can leave a request to get access to a specific email account [6]. You have to provide the email address and all sorts of information you have about the real mailbox owner. The more information you provide, the better is your chance to get the mailbox hacked. And you pay for the service only after the mailbox has been successfully hacked for you.

The aim of that research is to determine details and mechanisms how hackers steal login details for free mail boxes from its owner. It will give opportunity to find new techniques to protect mailbox owners from new phishing techniques.

2. RESEARCH

To study the email phishing technology from inside, we created two accounts with fictitious names with two popular email service providers, Mail.ru and Yandex, and left four requests on different web resources to get those accounts hacked. The Yandex account was described as the one belonging to wholesales company manager, and the Mail.ru account was supposed to belong to a design studio. So we received three letters: two in the Yandex mailbox and one at Mail.ru.

The first message was titled “Claim on the contract terms default” (Figure-1). According to the intruder’s idea, this kind of title was expected to give rise to the manager’s concern, so it would make him open the message and try to consider the matter carefully.

There was no concrete information in the body of the message. The only thing written there was that the details were represented in the attachment (Figure-2).

Figure-2. Content of phishing mail for corporate mailbox (Russian version on the top, translated - on the bottom).

Actually, there was no attachment there, but it was realistically imitated with a screenshot image. Clicking the picture resulted in a redirection, first to the intermediate page http://losy.netai.net/yad/, then we got redirected from there to http://mail.yandex.ru.id21128839.ru/neo2/. An ordinary user may not notice the double redirection as the URL shown in the browser address line upon the click starts with mail.yandex.ru, which the user trusts without any suspicion. But the address is actually a fake too; it is only an imitation of the original email service page and represents a fifth-level subdomain of the mail domain id21128839.ru owned by the hacker.

For some unknown reasons, probably due to certain lack of attention, the hacker was not fully prepared. Instead of the phishing page located at http://mail.yandex.ru.id21128839.ru/neo2, where the user was most likely expected to enter his or her login name and password to the account, the server returned a page with the catalogue listing. Obviously, the hacker had simply forgotten to put the required page in the catalogue.

The subject of the next message which arrived in that account was “Account blocking”. The message body was saying that the account had been used for spamming, and there was a link there with an anchor stating “User Agreement” (Figure-3). Clicking on the link resulted in the redirection via the intermediate page http://lobbi.comli.com/yad/?login=smirnovatatt@yandex.ru to the page http://mail.yandex.ru.id234wre3.ru/neo2/.

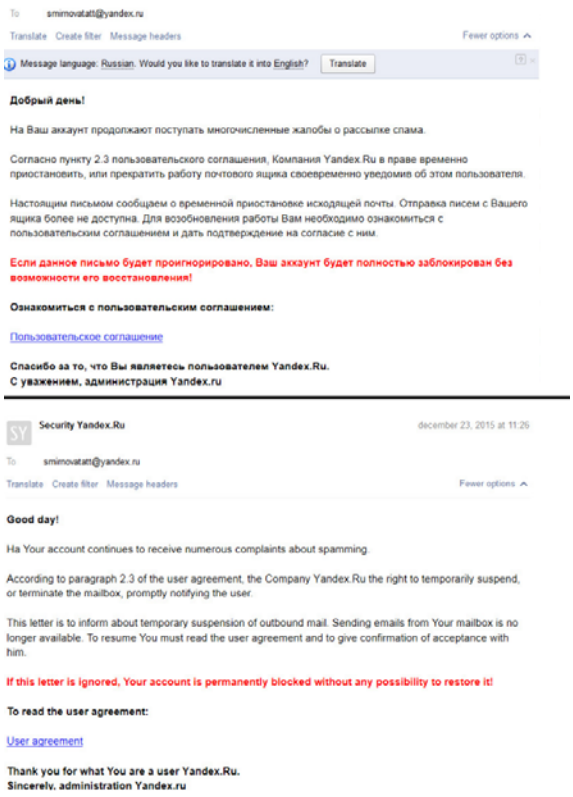

Figure-3. Content of phishing mail for individual mail user (Russian version on the top, translated - on the bottom).

The page asks you to enter your login name and password. It looks identical to the original Yandex.ru page, with the login name already typed there, which imitates an ordinary session timeout when the cookies expire. Users see such pages every day, so it arouses no suspicion (Figure-4). The only thing that may give the phishing page away is its address which only looks similar to the original. But the users do not expect any deception, so they pay no attention to the address. After you enter your password, the data are sent to the hacker, and the page get redirected back to the mailbox. Hence, the intruder has your password while you remain logged in without any idea of the fact that your mailbox has been hacked [7]. To verify whether or not the page is the original one, it is enough to enter any random set of characters in the password field: no matter what you type there, you will be redirected back to the original mailbox page.

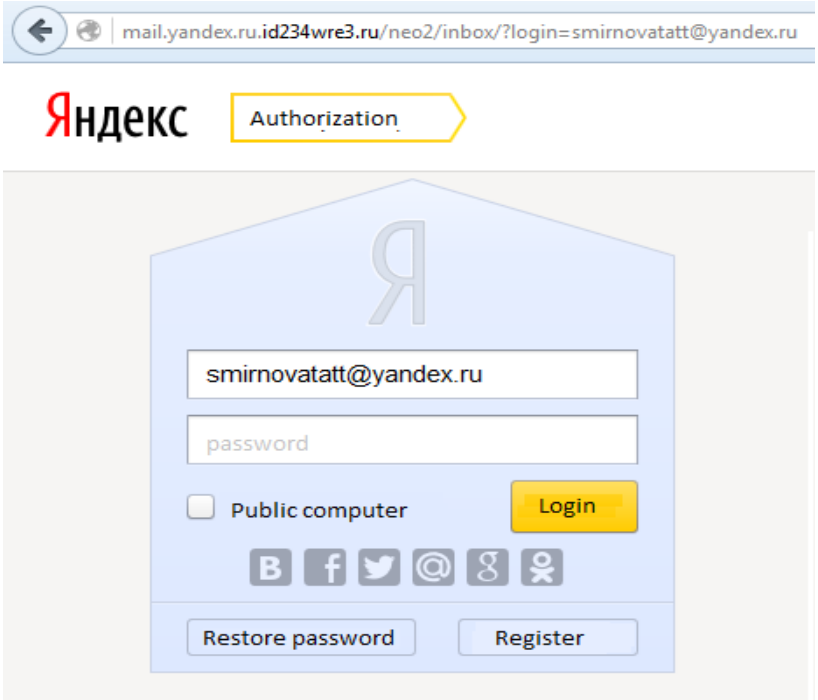

Figure-4. Phishing website with login form imitated to yandex.ru mail service.

As for the Mail.ru account, we received a message with "Numerous complaints against your account" as the subject (Figure-5).

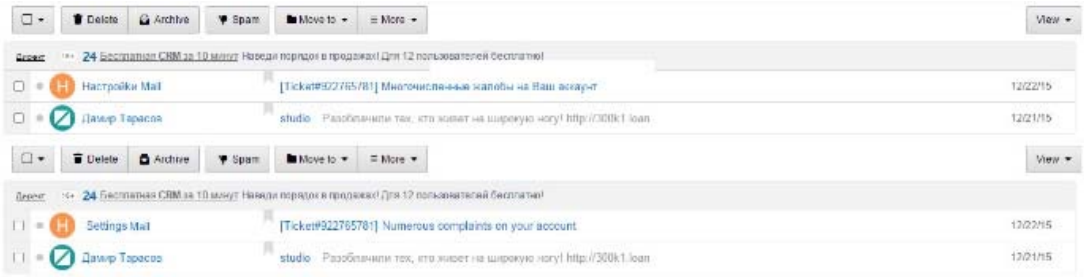

Figure-5. Incoming phishing mail for individual mail.ru account (Russian version on the top, translated - on the bottom).

The body of the message contained a brief description of the issue and said that if we ignored this notice, the account could be blocked. To resolve the issue, we were supposed to read the complaint by following the link. The link points at the e.mail.ru domain, which can well be trusted, but on closer examination we found out that the link actually pointed at a link script redirecting us to an external website. Its address was shown in the parameters, and an ordinary user could hardly notice the trick. Following the link, we got redirected to an intermediate address of the URL shortening service http://vk.cc/4yUxvy and then to a phishing page at http://e.mail.ru.id234wre3.ru/message/inbox/.

The external link script provided by Mail.ru is intended for ensuring the users' security. It warns you that you are leaving the email system and proceed to an external website. But the hackers managed to make sure that http://vk.cc/4yUxvy is recognized by the email system as a trusted URL, so the redirection works without the user being warned. Obviously, there is a gap in the Mail.ru security system, which allows intruders to get round the external link monitor.

The phishing page is an imitation of the original Mail.ru page, but the hackers did not provide the email address placement in the login field as it normally occurs when the session expires. This reduces the hackers' chances as lots of users got accustomed to the fact that the login field is always filled in by default, so they may suspect that something is wrong (Figure-6). This defect can be easily explained through the hacking technology applied there. The redirection is performed vie the trusted URL http://vk.cc/4yUxvy, and it is obvious that making a URL trusted by the system requires a lot of work, which is why there is only one link used for a big number of

hacking attempts for different email account, and they cannot know from which account the redirection will follow. As the link can only be used in that unchangeable form, it remains impossible to build in the parameters pointing at the account login name, so they are unable to place the login name on the phishing page.

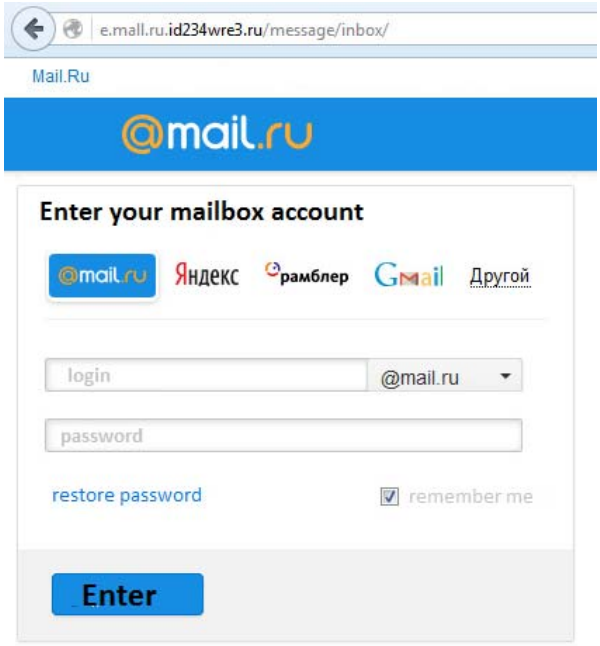

Figure-6. Phishing website for mail.ru user.

3. RESULTS AND DISCUSSIONS

The market for commercial email phishing is developing step by step. It is not large-scale data stealing that this kind of phishing is aimed at. The phishers purposefully try to hack the mailboxes of certain owners, following the requests of third parties. The use of a similar algorithm, as well as the domain names which look very much like one another, prove the assumption that the scheme was originally invented by a single person. And probably, there are those who teach new agents this kind of money-making method. The active development of the Internet and the growing number of users of free social networks will certainly ensure the further evolution of email phishing.

The study revealed a number of different email phishing schemes, contributing to the theft of user accounts. All of the circuits are different from each other and carry information about the logic of functioning that will allow to create effective filters to combat against email phishing. Considering the fact that hackers have begun to create services to gain access to e-mail, we can say that this service is in demand, and the demand for it increases in the course of time. Despite this mail services currently do not have effective means of combating phishing email and allow attackers to carry out the theft of user credentials.

REFRENCES

[1] Chaudhary G. K. 2014. Development Review on Phishing: A Computer Security Threat.

[2] Aaron G. 2010. The state of phishing. Computer Fraud and Security. 2010(6): 5-8.

[3] Gansterer W. N., Pölz D. 2009. E-mail classification for phishing defense. InAdvances in Information Retrieval (pp. 449-460). Springer Berlin Heidelberg.

[4] Gudkova D., Kulikova T., Kalimanova K., Bronnikova D. 2013. Kaspersky Security Bulletin. Spam Evolution.

[5] Shreeram V., Suban M., Shanthi P., Manjula K. 2010. Anti-phishing detection of phishing attacks using genetic algorithm. In Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on (pp. 447-450). IEEE.

[6] Hajgude J., Ragha L. 2012. Phish mail guard: Phishing mail detection technique by using textual and URL analysis. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 297-302). IEEE.