Is targeted phishing really that impossible to resist?

Last month, Gard was notified by several of our correspondents that they had received an unusual e-mail from our CEO asking for details about outstanding payments. Security Advisor, Eili Bjelkåsen, in our Technology and Security department tells the story. Knowing how fraudsters operate is key to understanding how to protect yourself and your company.

Published 15 April 2020

Fraudsters “phish” by creating e-mails that look like they are coming from a trusted source in order to fool the recipient into providing sensitive information or take actions that allow the fraudster to steal information or money. Security experts, cyber security awareness training and the media all warn us: Do not fall for it! And yet, someone always does. Targeting phishing, where the attacker exploits existing relationships is the most effective type of attack whether on the organisational or individual level.

The attack

On 31 March several of our correspondents contacted us to inform us that they had received a strange e-mail from our CEO with the subject line Payments/Invoices.

... can you please confirm to me the status of any outstanding/due payments? ... Kindly advice as soon as possible because there has been a new development in our company so please let me know if there are any outstanding payment. ... the board and our bank has mandated that payments in our favor henceforth to be received using our subsidiary banking details. ... ... reply immediately the status of outstanding payments and due dates and also you wait to hear from us before making any further payments.

This is a well-known and, for trained personnel, relatively easy to spot type of scam sent by unknown attackers to Gard’s business associates. Their goal was to make anyone with outstanding payments due to us first inform the attackers of the amounts due, and later make them pay to the attackers’ bank account. Some of our contacts responded and informed the attackers of outstanding payments. Once we were informed, we notified all correspondents of the scam. Thankfully, we are not aware of anyone paying the attackers.

Why is someone always fooled?

Whenever attackers invest time in researching the company and thus target the attack, the rate of success increases greatly. We are using e-mail as an example to show how fraudsters can target an attack and how you might be able to detect their techniques:

Fraudsters make it look legitimate - known as tailoring

• The e-mail message appeared to be from our CEO because it used the usual format for the e-mail address including what appeared to be the Gard e-mail address. This is a technical trick in which the attackers tell the recipient's mail server that the e-mail message came from Gard. Highly alert readers noticed that the e-mail address a bit 'off'. The e-mail address does not exist. Responses, on the other hand, will be sent to an attacker-owned e-mail address. This is possible to detect by hovering the mouse pointer over the "From:" name displayed in the message to see which e-mail it claims to be from. Then click "Reply" and check if the "To:" address, again, by hovering the mouse pointer over the displayed name, corresponds to the "From:" address in the original message. If these two addresses do not match, alarm bells should ring. In our example, responses would have been sent to a Hotmail-address.
• Fraudsters try to make the language of the message correct in the particular context. The attackers are constantly improving their writing skills, but this is where the reader might experience a slight "gut feeling" that something may be wrong without knowing exactly what. In our example, the "can you please confirm to me" part might trigger this gut reaction. CEOs rarely directly follow up on operational financial activities. Our advice is to listen to such "gut feelings" and make it part of your assessment. Maybe the timing of the message is odd, or maybe you receive it from an unusual sender? Maybe the language is uncharacteristic for the purported sender or words are misspelled?
• The e-mail signature looked correct; it has been shortened but it even included our logo. Most likely it had been copied from a legitimate e-mail message either from our CEO or from another employee and adapted to appear to belong to the CEO. This is a bit trickier to detect, but sometimes the attackers have a slightly older version of the signature, so if you have a recent e-mail from the CEO or someone else in the company, compare it.

Fraudsters make it important and urgent

• The e-mail message appears to be from Gard's CEO. This immediately makes it seem important. But ask yourself: Would the CEO be the sender of such a message?
• Including statements such as "please get back to us at the earliest" and "Kindly advice as soon as possible" triggers urgency for the reader. People are generally service-minded and when stressed, tend to leave critical thinking behind and just get the job done. Attackers know this, and how to exploit it. Take a minute to reflect on the language and you will notice that the word advise is misspelled.

Fraudsters make it interesting

• Statements such as "there has been a development in our company" may spark the reader's curiosity. Maybe, by responding and helping, you may learn more about what is happening? Be aware of such techniques to detect them.

Fraudsters make it current

• At the time of this article, phishing campaigns exploiting the COVID-19 pandemic are all the rage. Many companies have employees working remotely so they may feel less inclined to contact colleagues with questions. Another consequence of the pandemic is that many companies are struggling financially, and messages regarding financial topics may be more likely to arise. Attackers will try to exploit conditions in this time of pandemic so it is even more critical be on the alert to phishing fraud.

Going forward

There are several other characteristics and tricks to phishing and related types of attacks. We have highlighted the most obvious ones in the example above. Most often, theattackers will try to trick the user into submitting their username and password to gain access to any IT systems the user has access to, or open malicious attachments which infect the user's device with different types of malware. This was not the case in this campaign, which might even make it harder to detect. It does not exhibit those most common characteristics we look for in phishing today because there were no attachments or links in the e-mail message.

It all boils down to a simple, sobering fact: E-mail is inherently insecure. Designed in 1982, the SMTP protocol – which we still use today – was made for a time when the 'Internet' was trusted. E-mail messages are just like an old-fashioned letter, the sender can write anything in the From-field in the letter and on the back of the envelope. In later years we have seen amendments to the original protocol trying to increase security and validate the communicating parties, but these amendments must be implemented correctly by all involved parties to work. To achieve this, business and IT must work together and understand the consequences, both on the business side and on the IT side. For organisations with multiple communications partners spread geographically and of different sizes and cultures this can be very challenging.

Gard advises each employee to be a Security **STAR,** steps that are advisable for everyone:

• STOP: Even though the message claims to be urgent, you do have time to stop and catch your breath before you act.
• THINK: What is really happening here?
• ASK: Take the time to ask a colleague, or in this specific example: your regular contact at Gard. Is this really from you? What is my gut feeling trying to tell me? Do not ask by responding to the message itself, the attackers will assure you that everything is in order and that it is safe to do what they want.
• REPORT: If applicable, report to the party the attackers proport to represent so they may follow up. In this case, we were grateful to the correspondents who alerted us to the email. Also, report to your own IT- or IT security department to help alert other users who may be targeted in your organisation.

If you suspect that you may have been tricked, please remember that targeted phishing can be very hard to detect, and even the security experts have been known to fall for it. It is never too late to report and get help to reduce or even fix the damage.