BRANDEFENSE

CYBER THREAT INTELLIGENCE

Compromising Email Accounts with Credential Phishing

Author: Threat Intelligence Team

Release Date: 05.06.2022

Report ID: BD02112102

Brandefense
Digital Risk Protection Platform

info@brandefense.io

+90 850 303 85 35

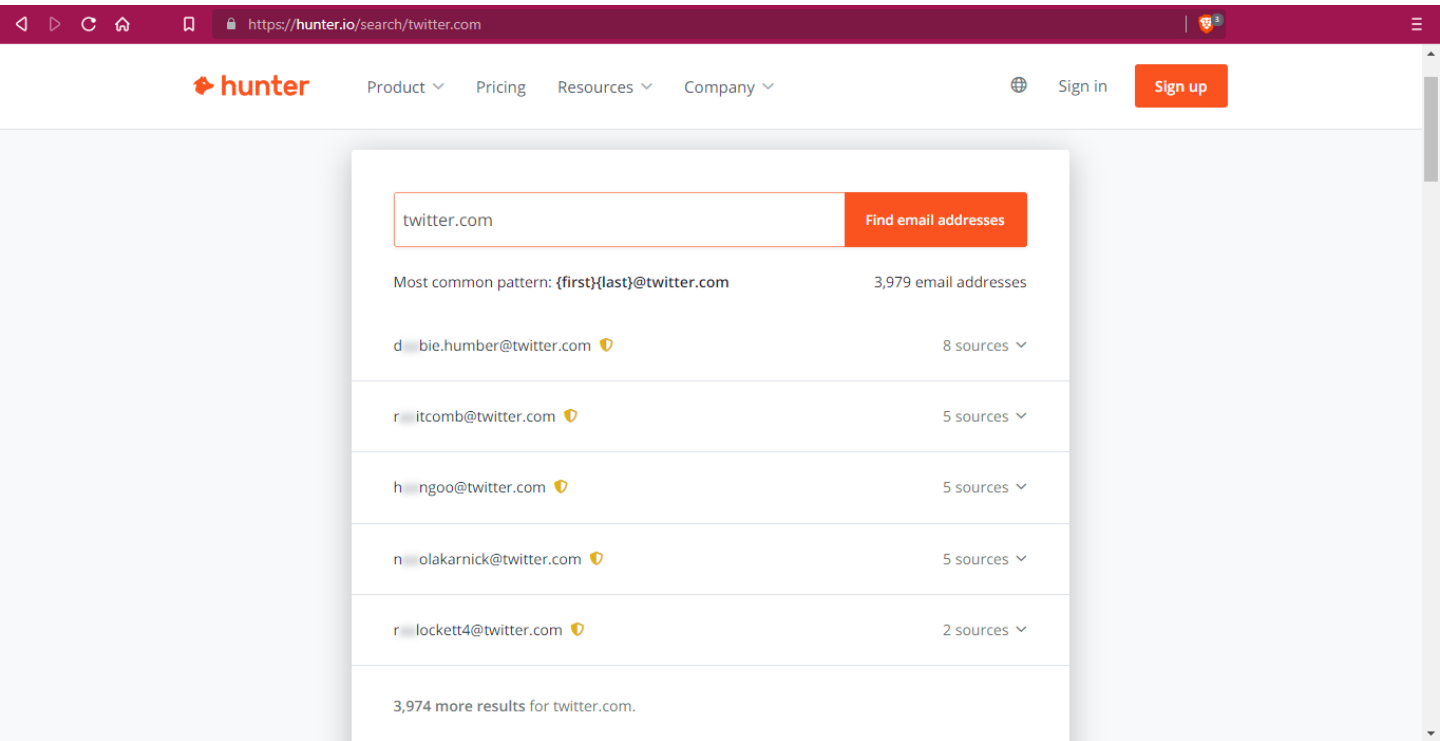
What is Credential Phishing?

Credential phishing is a phishing type which the attackers try to gain the credentials of an account. This is generally done by a fake login interface. But there are other techniques as well (e.g., keylogger). Attackers create a login web page imitating an original web page. The victim assumes that the web page he/she sees is the original one. Therefore, the victim enters the credentials of the account to the web page. However, credentials are taken by the attacker instead of the original server. The attacker steals the credentials and use them to gain access to the victim's account.

Attackers do not only target individuals. They might have bigger goals. Companies are also in the scope of the attackers. These kinds of attacks are called BEC (Business Email Compromise). Email accounts are included in the attack surface. Especially, C-Suite members should be well-protected to the email attacks since they have the most critical data.

Find the Email to Be Phished

You might need to search for an email address for phishing. There are a lot of ways to search for email addresses.
You can search for the email account names of a specific company. https://hunter.io is ready for your use. You can search for the employees' email accounts of a company. Moreover, you can see the template of the email accounts.
For example, we searched for Twitter's employees' email accounts:



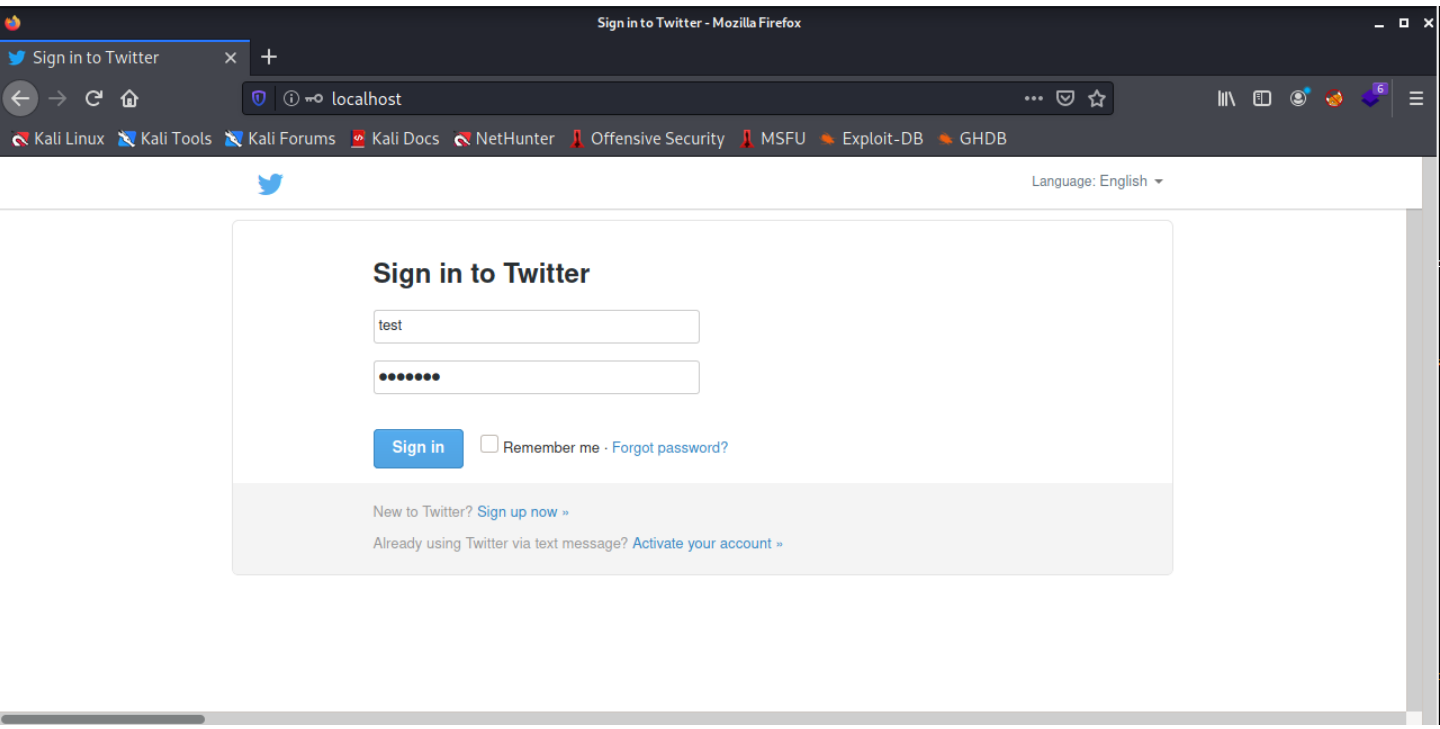
What an attacker can do with these information is that an attacker randomly selects employees of a specific company to compromise company's email accounts (remember BEC) or picks a specific target, but the attacker does not know email address of the target. Here, you can look at the target's company's email address pattern and guess the target's email address.

In case you need to verify the email account, you can use https://email-checker.net/validate to be sure that the email address is correct.

Attack Methods

Attackers can do a bunch of attacks with the information found. Since phishing is the most prevalent attacking technique, companies and employees have to be very careful, while reading emails. Here are what a phishing email may contain to steal your account.

- A link can be embedded into the email and the content of the mail mostly imitate a legitimate corporate or a person. Sometimes content try to scare or hasten you in order to make you decide fast on the legitimacy of the email. You should be calm in those situations. Those links may direct you to a fake login page. Fake login pages seem just like the original ones. It is very difficult to differentiate. An example of a fake website:



You can understand if the site is original or not by looking at the url of the site. In this case, this fake site is created on the localhost for test purposes. But in real cases, those credentials can be read by the attacker as the victim presses the «Sign in».

In the example above, username is entered as «test» and password is entered as «letmein». Here is how a hacker can see the credentials of the victim:

- There could be an attachment inserted into the email. Of course, that document will not be named as «trojan.exe», «keylogger.exe», ... They will imitate a legitimate document. There could be a possibility that the attacker will send an attachment as the attachment that you will be waiting to receive. Attackers can get information about you or listen your communication so that they will know what document you are waiting to receive.

Those attachments may inject malware into your machine. Attackers can steal your credentials with keyloggers, gain the control of your machine and use your machine to spread malware into other machines.

Detection and Mitigation

- Emails contain sender information (email address, name, signature). Those information is crucial to validate the legitimacy of the email. For example, an email could be sent from a personal email address (@gmail.com, @outlook.com, @hotmail.com, ...) but the content seems like a corporate email. That is a suspicious email. Signatures are also a validation method for corporate email addresses.
- Content may reveal the attacker. If the email is coming from a corporate address, then the content should not include any typos. If there are any, then you must be careful. Attackers generally salute you with a general phrase (dear customer, ...), not with your name (dear John).
- If there are any links or attachments suspicious, you should contact with the relevant department of that company to validate if the email is legitimate.

Conclusion

Phishing attacks are a special type of social engineering attacks. Credentials phishing is much more specific. In terms of credential phishing, attackers try to steal your credentials with various techniques. Therefore, you should always be careful, when you logging into a website or an account.