Bangladesh Post
a daily with a difference

Monday, July 20, 2020

5W & 1H of Phishing Campaign

By Sabbir Hossain

Jul.18, 2020

A phishing campaign is a kind of scam ran through email and intended to snip personal information from victims. Phishing basically depend on a vulnerability we can never fully abolish- human mistakes. The theme of the attack or the lure to attract human errors to commit the mistake depends on surroundings. For example, APWG or Anti Phishing Working Group Q1 2020 report states that cybercriminals launched a variety of COVID-19 themed phishing and malware attacks against workers, healthcare facilities, and the recently unemployed keeping in mind the current pandemic.

Who are the targets of phishing campaigns? The target always varies depending on the purpose. In past time attackers usually send large number of scam mails to mass amount of people and wait for the victims take the bait. One very known type is “419 scam”. Yes, you guessed it right! It’s the “Nigerian Prince” scam who left a lot of money and he want to invest or give away to you in return for a “small fee”. This attack became less effective now-a-days as users became aware of such scams at the same time email client algorithms were aligned to identify such scams. Now a days the more popular way is Spear Phishing attack that targets an individual and send him scam emails. Usually attackers work on a single target for weeks even months to gather more information about him and then initiate such attack. Most popular form of such attack is sending out password rest mails or bank portal email and password reset emails. In current pandemic situation one of such attack became very popular which is called “Zoom Attack” when the attackers send fake Zoom Video Conference meeting link to harvest username and password of the victims. Another widely seen attack during COVID-19 is business email compromise attack when the attacker sends fake emails regarding change of bank account or address due to pandemic to lure victims. The scammer imitates an employee or other reliable party, and attempts to trick the employee into transfer cash or confidential information. If we consider sector wise then SaaS and webmail sites are mostly victims of phishing attacks.

What is the purpose of phishing attacks? If we refer to Verizon’s 2019 Data Breach Investigation Report, 88 percent of phishing attacks are financially driven and 10 per cent are intelligence efforts. The main purpose of majority of phishing attack to benefit monetarily. Either the attackers can get the money through taking control of bank account or credit card information or they will get confidential information that they can exchange for money.

Where do Phishing attack origins? It is very difficult to pinpoint origin of a phishing attack. The attackers use several methods to mask their IP, location and other information. Latest available phishing toolkits make it even more difficult to track them as well as increased the possibility to do phishing attacks from around the globe. From various sources the topmost attacks hosting countries list remain similar for several years. China, USA, Russia, North Korea remains top of the list for hosting such attacks. Phishing attacks these days are considerably extra sophisticated, and when we study the mammoth resources behind state-based intelligence, we can understand how difficult it is to track them.

Why is Phishing attack rising? The main reason behind phishing attacks are human errors. Most operators aren't competent to distinguish phishing attempts, and so repeatedly fall victim to attack by clicking on links or opening attachments in emails without bearing in mind the possible consequences. Further thwarting the problem, administrations aren't doing adequate to condense the risks linked with phishing. The criminal organisations committing cybercrime are mostly very well-funded and often backed by states. As a result, they have the technical resources to continually modify attack patterns and use more effective variants of their attacks. The accessibility of phishing kits has given rise to in an explosion of phishing and other exploits coming from an ever-growing grid of substandard cyber criminals.

When we get phished what to do next? Change all your keys (PIN/Passwords) for the accounts that have been compromised as well as the accounts that use the identical or similar keys to those that have been seized by the attacker. If you give away your credit card data in the phishing site, call off your card. Take your device (Phone/Computer) offline or obliterate your email account to circumvent distribution of phishing links to your connection lists. Scan your device for viruses, clicking malevolent links can initiate quiet transfers of malware that go to work corrupting devices deprived of your knowledge. Pay attention for warnings of identity theft and put a fraud alert on your credit account.

How to prevent Phishing Attacks? Awareness & Training is the main tool to prevent phishing attack. He thumbs rule "Think Before You click" and "When in doubt throw it out" should be the two things every user should always remember. There are few other tips to prevent phishing attacks from expert such as: avoid public network, look out and be careful for shortened links, verify website SSL, set 2 factor authentications, use password managers, verify suspicious email with senders through different channel etc. Phishing attack mostly depends on human errors thus it can only be prevented by a lot of trainings, awareness and also deploying right tools in case of companies as well as arranging simulated phishing attacks to educate employees can help. Your caution will pay off to prevent phishing attacks.

References:

- https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
- https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf
- https://www.thesslstore.com/blog/phishing-statistics-latest-phishing-stats-to-know

The writer is a security professional, IT Policy & Risk Analyst at BGD e-GOV CIRT.

Editor-In-Chief : Sharif Shahab Uddin.
Published By **Rick Haque Sikder.**
From 242 Tejgaon Link Road (2nd Floor), Dhaka-1208.
Telephone : 8802-8878428, 8802-8878429 Fax : 8802-8878495.
Email : news@bangladeshpost.net