Global Journal of Computer Science and Technology: H Information & Technology
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Big Phish Little Phish

By Kyle Bynum
Marymount University

Introduction- A cyber-attack is "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."In the cyber realm there are many ways hackers go about getting personal information in an unauthorized way. In this research project I will be focusing totally on Phishing, how it works, some examples and how we can reduce phishing incidents.

Phishing is a cyber security attack that uses email as a weapon. The process of phishing is when the email recipient believes that the message, they are sent is something they want or need. The attackers disguise themselves as a trusted entity of some kind making the recipient feel as if they are conversing with trustworthy person, or a company the victim might do business with. It's one of the oldest types of cyber attacks and it's still one of the most widespread and harmful. In my research I found that the F5 Lab of Artificial Threat Intelligence breaks down phishing into three distinct operations.

GJCST-H Classification: K.6.5

BIGPHISHLITTLEPHISH

Strictly as per the compliance and regulations of:

Big Phish Little Phish

Kyle Bynum

Introduction

A cyber-attack is "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."In the cyber realm there are many ways hackers go about getting personal information in an unauthorized way. In this research project I will be focusing totally on Phishing, how it works, some examples and how we can reduce phishing incidents.

Phishing is a cyber security attack that uses email as a weapon. The process of phishing is when the email recipient believes that the message, they are sent is something they want or need. The attackers disguise themselves as a trusted entity of some kind making the recipient feel as if they are conversing with trustworthy person, or a company the victim might do business with. It's one of the oldest types of cyber attacks and it's still one of the most widespread and harmful. In my research I found that the F5 Lab of Artificial Threat Intelligence breaks down phishing into three distinct operations. These operations are,

1. Target selection - Finding suitable victims, notably, their email addresses and background information to find a psychological hot button that will lure them.
2. Social engineering - Baiting the hook with a suitable lure that would entice a victim to bite into the technical hook set to steal their credentials or plant malware. In the case of spear-phishing, this lure is customized to the targeted victim. At the end of the year, phishers will take advantage of fiscal year-end and holiday events as part of their masquerade.
3. Technical engineering - Devising the method to hack the victim, which can include building fake websites, crafting malware, and hiding the attack from security scanners.

In 2013, a Lithuanian citizen named Evaldas Rimasauskas allegedly hatched an elaborate scheme to defraud U.S. tech companies. The Justice Department shared that Rimasauskas forged email addresses, invoices, and corporate stamps in order to impersonate a large Asian-based manufacturer. The manufacturer was known for doing business with U.S. tech firms, so Rimasauskas used the opportunity to trick the companies into paying for computer supplies. The scheme worked until 2015, the corporate imposter convinced accounting departments at the two tech companies to make transfers worth tens of millions of dollars. By the time the firms figured out what was going on, Rimasauskas had coaxed out over $100 million in payments, which he promptly stashed in bank accounts across Eastern Europe. The companies that Rimasauskas defrauded was Facebook and Google. This incident is the Costliest phishing attack to date. According to the Federal Bureau of Investigation (FBI) this type of phishing is a Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC). This scam targets both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.BEC/EAC statistics were reported to the Internet Crime Complaint Center (IC3). Here is Data from the IC3, international law enforcement complaint data, and filings from financial institutions. The data below shows Domestic and international incidents and the dollar loss between October 2013 and May 2018.

Domestic and International Incidents:	78,617
Domestic and International exposed dollar loss:	$12,536,948,299

This data is the BEC/EAC statistics that were reported in victim complaints where a country was identified to the IC3 from October 2013 to May 2018.

Total U.S. Victims:	41,058
Total U.S. Victims:	$2,935,161,457
Total non-U.S. Victims:	2,565
Total non-U.S. Victims exposed dollar loss	$671,915,009

The FBI shared that the BEC/EAC scam continues to grow. Scammers are targeting small, medium, and large businesses. Between December 2016 and May 2018there was a 136% increase in identified global exposed losses. The scam has been

Author: Marymount University. e-mail: kmsbynum@gmail.com

reported in all 50 states and in 150 countries. Victims of the scam filed their information with the IC3. Financial sources indicate fraudulent transfers have been sent to 115 countries. Observing the statics above I was able to understand why phishing scams so successful. My researched led me to the schemers and the specific people they are targeting. The schemers are counting on employees of the company they are trying to scheme to respond to urgent emails that appear to come from their executives or vendors. As an employee of a corporation if I received an email from my executive or a vendor I always respond in a timely manner and do exactly what they ask me to do. The difference is I make sure that the email is legit and is coming from the actual source.

In the August 2006 Boulder County Business Report, there was a story about how the Boulder Police Department in Colorado was investigating several cases of identity theft and fraud from customers of the Elevations Credit Union which was formally known as the University of Colorado Federal Credit Union. Boulder Police had taken nearly 30 reports from victims who have had more than $39,000 taken from their accounts in early April of that year. The incidents caused the Boulder County Sheriff's Office and the University of Colorado Police Department to investigate eight other cases with loses exceeding $10,500. In this case It seems that the scammers might have got in by using the members passwords and credit card numbers to retrieve the money.

The last incident of phishing I researched was from the New Orleans City of Business Journal in 2004. The journal shared a story about a St. Tammany Parish resident Vicky Magas who received an E-mail in her home account about an offshore worker named Peter Magas. The E-mail stated that Peter and the rest of his family had died and together they left $3 million to his closest heirs. Vicky had never heard of a relative named Peter Magas. The E-mail then told Vicky that if she knew the where his heirs were to click the link provided and follow the instructions and then after she could to claim part of the money. Vicky didn't click the link because she had heard about these kinds of scams, so she sent the E-mail to Cynthia Albert at the New Orleans Better Business Bureau. Albert confirmed her suspicion and stated that this type of phishing is referred to as the "Nigerian Letter Scam."The Nigerian Letter scam focuses on urging consumers or businesses by E-mail or phone to hand over their financial information in return for a promised payoff or shipment of money overseas. The Nigerian scams originate from several countries like Africa, New Zealand, Brazil and Great Britain and are typically signed by someone who allegedly represents the country's ministry of commerce or finance. This type of phishing has been around since the Internet's early ages and is focused on urging consumers or businesses by E-mail or phone to hand over their financial information in return for a promised payoff or shipment of money overseas.

No matter how large or small a company, business, or person is eliminating and minimizing phishing should be a topic of discussion. Conducting my research I was able to find several ways to fight and overcome phishing.

1. *Require Verification Through Other Official Channels*

Reach out to colleagues by using methods like contacting the person directly from company directory, contacting their assistant, or just walk down the hall to speak with the alleged requester face to face

2. *Implement New Processes to Increase Cyber Defenses*

Another way companies can avoid phishing attacks is if they had account verification and safeguard processes in place. This could entail requiring employees to follow set processes like performing account verification with 2 step factor authentications, via phone, or email. Lastly, have signatures from the sender and receiver before any transfers over a set amount is sent.

3. *Implement New Processes to Increase Cyber Defenses Cont*

Have a system like Pass Marks put in to place to increase security. Pass Marks directly addresses the "phishing" e-mail scams. The software protects financial institutions, e-commerce sites and enterprises against Internet phishing attacks.

4. *Implement Employee Cyber Awareness Training*

Offer cyber security awareness training for employees. This will education and train employees to identify and appropriately respond to phishing emails. In addition, these trainings will help strengthen your organization's human firewall. Cyber security awareness training can be offered as a new hire and once each work quarter face to face or online. Periodic phishing testing should be performed to determine the success of the training or to identify areas to focus on in future trainings.

5. *Use Email Signing Certificates*

E-mail signing certificates enable executives and other employees to digitally sign their emails so their recipients can easily verify that they are who they say they are. These certificates are issued by industry-trusted certificate authorities. With E-mail signing certificates mandatory someone in the finance or accounting department can easily verify the identity of the email sender. In addition, these certificates can also be used to send secure emails using asymmetric encryption. This enables you to send an encrypted email to a recipient who has the matching private key, which protects the integrity of your data.

In closing, my research brought me to investigate the large and small incidents of phishing. The investigation led to my discovery of how much of a problem phishing is globally. Personal information and were always at loss during the attacks. Throughout my research with the information provided I was also able to come up with ways to try to overcome phishing and protect company's and individual's integrity.

References Références Referencias

1. Santora, T. (2004). Nigerian letter, phishing scams target businesses, consumers. *New Orleans City Business,* 1. Retrieved from http://proxymu.wrlc.org/login?url=https://search-proquest-com.proxymu.wrlc.org/docview/209570141?accountid=27975
2. Phishing scam hits elevations. (2006). *Boulder County Business Report, 25*(17), 1. Retrieved from http://proxymu.wrlc.org/login?url=https://search-proquest-com.proxymu.wrlc.org/docview/221230502 ?accountid=279
3. Passmarks' fight phishing scams. (2004). *Marketplace, 15*(13), 51. Retrieved from http://proxymu.wrlc.org/login?url=https://search-proquest-com.proxymu.wrlc.org/docview/219623935?accountid=27975
4. Ic3.gov. (2019). *Internet Crime Complaint Center (IC3) | Business E-mail Compromise The 12 Billion Dollar Scam*. [online] Available at: https://www.ic3.gov/media/2018/180712.aspx [Accessed 1 Dec. 2019].
5. F5 Labs. (2019). *2018 Phishing and Fraud Report: Attacks Peak during the Holidays*. [online] Available at: https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays [Accessed 1 Dec. 2019].
6. Hashed Out by The SSL Store™. (2019). *The Dirty Dozen: The 12 Most Costly Phishing Attack Examples - Hashed Out by The SSL Store™*. [online] Available at: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/ [Accessed 1 Dec. 2019].