CRIM2010 Speech

Mel

[Slide 1 - Topic Slide] Hi everyone! My name is Melissa, and here with me I have Tamara, Izzy and Kendall, and we're representatives from CrowdStrike who have been employed by the Democratic National Committee (the DNC) to gather information and investigate the cybersecurity breach in 2016. We aim to inform you, the Federal Bureau of Investigation, on the current findings and offer future recommendations to ensure the safety and security of the American People. We'll be focussing on the implications and interferences of Spear Phishing as a tool of Social-Engineering in the 2016 United States Election.

[Slide 2] The expansion and modernisation technology has allowed cyber capabilities to transform the traditional notions of crime within a digital space. Cybercrime and more specifically social engineering falls under the category of transnational crimes. The development of the internet has allowed for increased anonymity and easier access to a greater number of victims. The concept of anonymity ensures individuals can act as unknown identity in ensuring the protection and identities from being accessed by the victims or third party offenders and as a result, these anonymous individuals collectively share a unique hidden identity. This can lead to the mitigation of the repercussions of crimes committed against others.

Consequently criminal activity also ensures traditional forms of crime prosecution and prevention cannot be adopted to deter acts of crime. The importance of understanding cybercrime lies in the ability to enact detrimental harm to all individuals from corporate institutions, states' governments to independent individuals like yourself. As a result an active defence against attacks are imperative to the health of businesses and individuals worldwide and the evolving nature of cybercrime requires constant development of defensive strategies in order to protect against malicious cyber actors.

Social Engineering / Spear Phishing

[Slide 3] Social engineering is the exploitation of human vulnerabilities instead of targeting the vulnerabilities of a computer system. It's the most type of cyber attack with over 95% of all cyber attacks utilising these tactics (https://purplesec.us/resources/cyber-security-statistics/).

[Slide 4] There are many different types of social engineering but some of the most common types are

- Phishing, where malicious links are sent to targets
- Quid pro quo, where they promise something in exchange for information
- Tailgating, where an authorized person helps an unauthorised person through an electronic barrier
- Baiting, similar to 'Trojan Horse' style attacks
- Pretexting, pretending to be someone else to obtain information
- Blackmail, where they threaten to reveal a secret

- And lastly, dumpster diving, where the attacker will physically search for information about the target

A study was conducted, and the results found that 27% of people will click on a malicious or bogus link when sent under the pretence of a trusted company (Lopez, 2019). While phishing has been found to be the most successful (Lord, 2019), many social engineers will combine different aspects of social engineering and construct a tailored experience for a specific target and situation. It has been found that almost 1 in 5 people will fall victim to a social engineering attack (Ashford, 2018).

So what makes social engineering such an easy attack to pull off? Social engineering relies on common human behaviours, such as trust, curiosity and ignorance. Many people are often also striving to be helpful and like to gain something from nothing (Gulati, 2003). Attackers are aware of the way humans react to certain triggers and use this knowledge to their advantage.

[Slide 5] While there are many types of social engineering, today we'll be focussing on phishing, or more specifically spear phishing and whaling. So we know that phishing is essentially disguising a malicious email as something else in the hopes that someone will fall for it and either unknowingly download malware, share credentials or something else targeting the end user.
[SAlide 6] Spear phishing is a more informed version of this, where the attacker will tailor the disguise to the victim, for example including the name of the target or other identifying information which makes the attack more likely to succeed.

[Slide 7] Whaling is the same as spear phishing with the added specification that the target of the attack is a high profile person, eg person in power or well known person.

[Slide 8] These types of attack are usually in order to break the higher up people who have more power and therefore are more likely to be able to help with the ultimate goal, eg. transfer of funds, credentials etc.

Izzy

The Case:

The case we have chosen is the 2016 US Federal Election. In brief, John Podesta, the Clinton Campaign Chairman, received an email asking him to change his password. He did think that it was a little bit suspicious so he forwarded the email to the IT help desk and they responded with a typo saying the email was legitimate rather than illegitimate. Due to this, he went ahead and clicked the link, changing his password and allowing the hackers access to the DNC networks.

Timeline:

July 2015: Russian intelligence gains access to DNC networks

September 2015: FBI discovered suspicious activity and contacted the DNC IT contractor in charge of the network. He asked him to look into specific activities that they had noticed emanating from the DNC network that could be nefarious.

December 2015: Attacks on elections systems begun

April 2016: Russians stole approximately 300GB worth of documents from DNC network. A significant amount of this data was information pertaining to the Federal Election. These documents included internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of the DNC employees.

April 2016: Crowdstrike was contacted to discuss a suspected breach

April 2016: The GRU began stealing data. They searched one compromised computer for files containing search terms that included Hilary, DNC, Cruz, and Trump.

July 2016: The DCCC public announced it was a victim of Russian hacking

October 2016: DHS and ODNI release joint statement about stolen emails blaming the Russians and suggesting that the theft was intended to interfere with the US election.

January 2017: DHS recognises that the US's election infrastructure is so vital to the American way of life that its destruction would have a devastating effect on the country.

Main Actors:
The main actors in this case study are:

- The GRU (Russian Intelligence Agency)
- FANCY Bear – April 2016
- COZY Bear – July 2015
- The DNC (Democratic National Committee)

What did they do?

- Approximately 70GB data from the Clinton campaign
- 300GB data from the DNC
- Breached into 29 computers on the restricted network and 30 computers of the DNC
- The information was not only used for national intelligence regarding the Clinton campaign but further released and pushed through two forms of exposure. Firstly DCleaks (a front for the cyber-espionage organisation FANCY BEAR). The premise is a website directly focused on exposing emails of prominent political figures. And secondly through an anonymous identity known only as Guccifer 2.0 (used as a media propaganda in funcelling information to organisations such as Wikileaks.

How did they do it?

- They used servers located in the US
- They sent dozens of spear-phishing emails over a period of 5 days
- Gained access to the email account of John Podesta, Clinton's campaign chairman
- In regard to the technical aspect of the attack, FANCY BEAR used two varying hacking tools. The first being Minikatz (this program is only viable once the attacker has breached the network, and allows for the collection of private credentials). Further a secondary software titled X-Agent, grants the hackers access to collect login keystrokes

and screenshots to identify access login information of individuals targeted with the malicious malware. The final programs is a tool to process and exfiltrate mass data from the targeted networks directly to controlled serves hosted by hacking organisations which in this case included

-

Repercussions:

- Mueller Report
    - Verified Russian interference
    -
- Crowdstrike
    - Employed by the DNC and the FBI to assess the situation and find the leak
    - They also found the repercussions on Hilary and the campaign
- How it affected Politics – reduced the chance of Hilary winning – exposed information

Theory:

After we went through the case brief, since we all familiarise ourself with the details of the case, let's all try to examine and explain the criminality in our case by employing some relevant crime theories.

Firstly, According to **Rational Choice Theory (CORNISH & CLARKE, 1987),** people commit crime if the potential reward outweighs the risk. This can be associated with the heightened political risk of Hilary becoming president and the Democratic Party becoming the ruling party, and therefore the act is viewed as an act of heroism to highlight the downfall of the US presidency. Furthermore, despite the benefit of such criminal conduct remains unknown, the potential rewards can be assumed to be financial/monetary gains, psychological pleasure, cyber espionage from Russia to collect the intelligent information about Hillary and the US, causing disruptions to the presidential election and making America great again by collaborating with Trump and electing him as the president eventually.

According to the **Deterrence Theory (Beccaria, marchese, Bellamy, Davies & Cox,1995),** The lack of certainty, severity, swiftness in the sanction leads to delinquency or criminal conduct. There is very low certainty that the hackers would be caught. If they did get caught, the severity of the punishment is likely to be low and it would not be a swift process.

These theories can be linked together because if there was a low chance of being caught, that means that the risk is lowered. Therefore, the reward is more likely to outweigh the risk.

Moving on to the techniques of neutralization (Sykes & Matza, 1957), in our case,the criminality of the hacking group who committed the spearfishing/malware/hacking can be neutralised by justifying the act as a necessary way of exposing the conspiracy and maintaining social justice, when in fact the action is illegitimate and immoral.

Now we are looking at Routine Activity Theory (Cohen & Felson,1979):

Which can be summarised roughly to an equation: Motivations + Opportunity - Guardians = Crime. In the case study, 2016 U.S. Presidential Election which is a perfect timing, Hillary Clinton as a high-profile politician and a competitive presidential candidate, and the Democratic Party as one of the two major parties, which are the best targets. Clinton left herself unguarded by using a personal mail server for formal government communications which exposed a potential threat to her personal privacy and the information security system. The DNC and Hillary campaign aides put their guard down when faced with the phishing attack. The cybercriminals are motivated to commit the crime driven by the incentives stated previously in the rational choice theory.

Legislation:

Now moving on the part which everybody is mostly curious about, did Hillary break the law? And is it a careless behaviour or a criminal conduct?

Let’s look at the federal law related to this case.

Section 1924 Title 18 U.S. Criminal Code and s606, 801 in the National Security Act of 1947, specifically details the definition of the classified information, procedures to access and handle classified information.

Did Clinton know she was putting classified information into an unclassified system?

She and her aides claimed she didn’t. None of her emails including materials was not marked as classified, but some emails later were reclassified, and these were not classified when she sent or received them.

Did she “wilfully communicate” classified information to anyone not authorized to receive it?

She claimed she didn’t. No evidence indicated that she did and most of her exchanges of emails were with other government officials who were granted access to particular materials.

Did she remove classified information “with the intent to retain such documents or materials at an unauthorized location”?

If all she was doing was exchanging emails with her staff, It is difficult to prove that she had the intent to retain anything.

Freedom of Information Act 1967, Federal Records Act 1950 and NARA’s regulations allows officials using personal email accounts who must ensure that official correspondence is turned over to the government. allowed the use of private emails only if federal records were "preserved in the appropriate agency recordkeeping system". Such transgressions, however, do not constitute criminal conduct.

Russian Federation has neither signed nor ratified the Budapest Convention, therefore, such treaty cannot be introduced into force for Russia. Russia has previously refused to sign the Convention, stating that the adoption would go against the Russian Sovereignty. However, Russia currently sits as an observer country but only in its quality of the Member State of the Council of Europe. Despite such international instrument is binding in the U.S., Russia is not bound by it.

Solutions

In conclusion to the current assessment, we further aim to offer recommendations regarding potential actions to ensure the protection and security of future cyber attacks. Now there are 3 main solutions we can provide while offering a cost benefit analysis to understand the potential implications on the notion of cybersecurity on a general basis, and in regard to the effects of spearfishing on political interferences.

1) SETA Education
2) Policy Reform in enforcing sanctions or controls to individuals and organisations
3) Retaliate with cyber military aggression in response to Russian interference

Option 1: SETA

SETA refers to (Security Education Training Awareness). The foundational aspect of SETA aims to develop in-depth cybersecurity knowledge among employees to facilitate, implement and organize security training programs in the prevention of attacks such as spear phishing. Rather than assessing the advancement of technology itself, SETA is a new stance directly focusing on the human behavioural aspect and manners in which individuals can be more technology aware of potential threats against them. SETA acts as an internal human firewall to filter the harmful acts such social engineering in protecting the resources and equity of the organization. Ultimately it aims to provide the organization with human resources who are equipped with the technological security knowledge to improve systems and devices throughout the DNC.

As any program may contend, there are several limitations affecting the overall effectiveness of SETA as a tool of cybersecurity. The greatest criticism is the reliance on human behaviours in utilising educational skills, as this allows for the potential of miscalculation or human error regarding security knowledge. Not to mention the possibility of malicious and negligent behaviours on behalf of individuals themselves. The program currently yields low adoption rates due to the high monetary costs and long transition periods of implementation, decreasing the overall effectiveness.

The second potential solution refers to changes in current policy regarding the enforcement and sanctioning of the illegal use of communication avenues. Despite current protocol regarding elect officials using government email domains concerning election communications, Clinton “illegally” maintained connections through private domains. There are two issues here, firstly the disregard to state legislature including the Freedom of Information Act and secondly leaving information vulnerable to spear phishing and the harvesting of private information. Therefore it is suggested that harsher impositions regarding federal legislature are enforced to maintain greater levels of deterrence in conducting illegal behaviours such as the use of private emails. Or consequently, as the FBI, you maintain the power to hold Hilary accountable for her actions, setting the procedural standard for future individuals through means of sanction deterrence. In regard to the potential cost, changes to legislature are not a simple process but rather require several stages of approval through committee bodies with final agreement required in the House of Senate. Not to mention, as shown in the case of Hilary, you arguably lack the enforcement power or desire to enact convictions regarding individuals in positions of power.

The last recommendation suggested is a direct or indirect attack upon Russian sovregnity. Spear Phishing, espionage or an act of such nature, despite predominantly denied, show clear associations and underpinnings to Russian state involvement. A report by the Pew Center noted 71% of Russian believed they had no involvement in the US election, with 85% holding the belief that the U.S commonly interferes in other nationals' internal affairs, demonstrating clear Russian nationalism. This further contends the negative views of American policy regarding Russia. As discussed, cyber capabilities have modernised the manner in which crime is accessible including the modernisation of state military capabilities. Cyber Warfare is the use of one actors' cyber capabilities to disrupt or cause harm to another states' vital systems for strategic or military purposes. Arguably Russia actively sought to enact harm in disrupting political proceedings, and in turn launched attacks on U.S sovregnity through spear phishing and malicious malware.

Concerning cost benefit analysis, retaliation of cyber means enforces U.S hegemony in securing positionality within the global community. However Russia and the U.S are major powers within the international domain both maintaining nuclear capabilities and WMD. Retaliation on behalf of the U.S could cause the potential to launch international conflict

Based on the evidence provided in assessing the threats regarding cybersecurity and directly spear phishing, the solution offering the greatest benefit is the implementation of SETA programs prior to federal escalation of policy reform and potential conflict. Despite the limited implementation, with the correct cyber infrastructure, SETA offers high reward in adapting behavioural changes rather than simply a technological development. Thankyou for your time today, we hope you take into consideration our recommendations for the future of cybersecurity…. (well at least until the next election)

Reference

Joseph Poushter (2018) “Russians Say Their Government Did Not Try to Influence U.S. Presidential Election” *Pew Research Center,* available at: