COMS30070: Security Behaviours

Tell them that it's human nature

Gabrielle B. Balgobin - qr19324

Prompt: Analyse security failures exposed by Kane Gamble's attacks on US intelligence and security officials

American cryptographer Bruce Shneier once said "Only amateurs attack machines; professionals target people"[3]. Whilst he made this proclamation almost two decades ago, the sentiment still reverberates through today's cybersecurity climate. Since the advent of the Information Age, information has become a key driver of the economy[20]. Fort Knox is secured by impenetrable layers of granite, concrete and steel, so it would be expected that data, "the new gold"[14], would be guarded just as robustly. However, safeguarding information is much more convoluted. Security policies considering both technological and human aspects are required. Despite the complexity of many of these policies, they are still infringed upon. In 2021, Verizon's Data Breach Investigations Report revealed that 85% of breaches involved the human element [1]. This supports Shneier's view of people being a key vulnerability in cybersecurity. Over the years, there have been countless incidents where this weakness has been exploited. One of the most noteworthy occurrences was in 2015 when a British teenager, Kane Gamble, infiltrated various US security officials' accounts by using social engineering. This essay aims to analyse key elements of Kane Gamble's attacks on US intelligence and security officials and propose measures to safeguard against future attacks.

Gamble's initial target was John Brennan, Director of the Central Intelligence Agency. In the first phase of his attack, Gamble learnt Brennan's phone number and used reverse phone look-ups to determine that Brennan's cellular provider was Verizon[2]. Whilst there is not sufficient evidence to pinpoint exactly how Gamble acquired Brennan's number, Kevin Mitnick (a convicted hacker) declares this is a basic task that can be executed via several methods[13]. In his book, "The Art of Deception: Controlling the Human Element of Security", he even gives detailed instructions.

According to "Cubed" (a member of the online group started by Gamble, "Crackas With Attitude - CWA"), Gamble called the telecommunication company impersonating an employee from its very own live chat department, claiming to have an issue with customer lookup tools and acquired Brennan's social security number[7]. The pretext for the communication involved him impersonating an employee hence Gamble needed to appear knowledgeable in company procedures and technical jargon. This con is directly out of the playbook devised by infamous social engineer Kevin Mitnick[13]. This first call allowed Gamble to familiarise himself with the terminology used by the company along with their internal procedures. Whilst directly demanding Brennan's social security number would immediately raise red flags, by stating that he was having problems with customer lookup tools, Gamble boosts his credibility and thus attains the desired information. This con was sustained as employees are generally helpful towards co-workers experiencing difficulties as empathy is part of human nature. This makes the inherent kindness demonstrated by humans a critical vulnerability.

The attack could have be thwarted in this early stage by the Verizon employee simply verifying that the caller (Gamble) was a legitimate employee by asking for an employee identification number which is kept confidential or checking that the telephone number he was calling from was registered to a Verizon office. If it was not registered to a

Verizon office, the employee should have called the phone number listed in the company directory for that person for identity confirmation. Due to the time constraints that exist in work environments and the general helpful nature of call center workers, this action seems unreasonable. However, it is of paramount importance. To protect against future attacks, companies should implement policies requiring identify verification during all telephone calls. It can be argued that information such as an employee identification number is not a sufficient method of authentication. This suggests that more detailed procedures such as organizing data in a hierarchy with different levels of employees only being able to access certain data, implementing verification calls to listed numbers or even establishing in-depth questions that can be used to confirm the identity of a caller should be implemented. As part of employee evaluation, companies should conduct exercises where actors make fake phone calls to their call centres to test if they adhere to these policies and inflict penalties on employees if they break protocol.

The second stage of Gamble's attack was calling the company again but this time impersonating Brennan. On his first endeavour, he was denied access as he could not name Brennan's first pet[5]. Despite tripping over this initial hurdle, Gamble did not give up and instead relied on the unpredictable nature of human behaviour. The reaction of one person is not necessarily the same as another. By constantly calling and interacting with different handlers, Gamble was eventually able to convince a handler to change the pin and security questions thus gaining access to Brennan's Verizon account and obtaining his personal details, router serial number, MAC address, home address and his AOL email address[2][21]. Voice recordings of these calls to Verizon were obtained by the FBI as detailed in their affidavit thus supporting this sequence of events[15]. Making multiple calls until he was matched with a favorable handler is a method outlined by Mitnick where he suggests instead of giving up on the ruse or raising too many red flags, you simply end one call and try targeting another employee[13]. The pretext used in this phase is completely different from the first phase suggesting that Gamble was meticulously tailoring his pretext to his target and his objective. In the latter case, Gamble would have done in-depth research regarding Brennan and used this in his impersonation.

A possible remedy to the security issue above would be to keep a departmental log of all the attempts to access an account. This would allow handlers to flag suspicious activity and exert more caution when conducting transactions regarding that account. For example, if the employee who finally changed the pin allowing Gamble to access the account knew that there were multiple attempts to access the account within a short time-period, he/she would have been more critical and thus less likely to fall for Gamble's social engineering.

Now knowing that Brennan possessed an AOL email account, Gamble once again impersonated Brennan and called AOL customer service requesting a password reset on the account. He was successful in gaining access with the security question being to state Brennan's social security number which Gamble already possessed[7]. By having control of Brennan's personal AOL email account, Gamble was able to access his emails, contacts, cloud storage, and his wife's iPad[5]. This trivial way of initiating a password reset is a security vulnerability that begs to be exploited. To verify a customer's identity, two-factor authentication should be used to provide an extra layer of security[4]. For example, if a malicious actor requests a password reset, in addition to a username, password and/or security question, they should be required to provide an additional code which is sent to a separate device within two minutes.

Evidently, Gamble was not keen on keeping this highly confidential information to

himself as he leaked Brennan's contact list via Pastebin, routed information to Wikileaks and other parties and posted CIA data releases[21]. Kane Gamble could now officially be regarded as an agent of hacktivism[17]. By choosing to forward information to the notorious hacktivist group, Wikileaks, he aligned himself with their interests which are to reduce corruption and create stronger democracies by improving transparency[17]. Another piece of concrete evidence to show that Gamble was ideologically motivated is a statement Gamble made in 2015, "It all started by me getting more and more annoyed about how corrupt and cold blooded the US Government are so I decided to do something about it" [5]. Gamble did not cease at attacking Brennan but on numerous occasions intruded into his family life such as when he accessed his wife's account and changed the answers to security questions to "hacked", "hacker" and "V for Vendetta"[21]. The latter is a movie which follows the life of a man who believes the government has subjugated him[8]. By referencing this movie, Gamble subliminally reaffirms his belief that the government is corrupt. This new understanding of Gamble's motivation can give perspective when analysing his attack.

The success of his attack on Brennan inflated Gamble's ego and motivated him to strike again. After boasting that his newest target was the US Head of Homeland Security, Jeh Johnson, Gamble utilised similar social engineering tactics to hack Johnson's home broadband gaining access to his phone and Comcast account. This is evidenced by the call records showing a series of calls from Gamble to Johnson's telephone number and US Department of Homeland Security (DHS) [21] [5]. Gamble was clearly following in the footsteps of legendary social engineers such Kevin Mitnick, Susan Headley and Lewis de Payne by making impersonation- a vital social engineering tool- a part of his modus operandi. This evident influence of nefarious social engineers on Gamble reflects social cognitive theory which postulates that behaviour is learned from persons whom they observe[9]. Nowadays, the media tends to portray criminals as cool, intelligent and noble. Consequently, individuals are likely to accept and identify with this criminal behavior[18]. To curtail cybercrime, it is reasonable to suggest that the media stops romanticizing cybercriminals and instead educates impressionable youths about responsible cyber behaviour.

Similar to his attack on Brennan, Gamble also targeted Johnson's family by making several calls to their home landline and his wife's mobile phone. His wife received a text message stating "This account in now under the control of FederalSecurity aka FedSec, we will leak everything on this account and everything of Jeh Johnson if the US Army does not stop killing innocent civilians in Iraq, Afghanistan, Egypt, Syria. #FreePalestine"[21]. This text message reiterated that the incentive for the attack was political. However, other voicemails and text messages such as "Hi Spooky, am I scaring you?"[21] seemed to be of a humorous nature and had no political significance. It was almost as if Gamble viewed the entire attack as an elaborate prank. Whilst this notion may seem far-fetched, medical experts declared that Gamble is on the autism spectrum and had the mental development of a 12/13-year-old[5]. Just as a child finds humour in scheming, it is entirely possible that Gamble launched this attack partially for his own personal amusement.

According to the FBI's affidavit, Gamble used the personal information obtained to log into the Law Enforcement Enterprise Portal(LEEP), thus accessing highly sensitive data[15]. In an interview, CWA boasted that they exploited an undisclosed vulnerability in the LEEP portal, giving them access to law enforcement information-sharing portals and investigation tools[16]. The alleged existence of a vulnerability in such a highly confidential portal demonstrates the dire need for organizations to conduct regular penetration testing on their security systems to identify weaknesses and rectify them before a mali-

cious actor capitalises. Gamble also used the portal to access the Justice Department's Joint Automated Booking System in order to gain intelligence on Jeremy Hammond, a U.S. hacker[15]. Gamble seemed to have contingency plans as he made arrangements for a fellow group member to leak Johnson's information if he ever were caught.

When asked to comment on the difficulty of their attacks, Gamble's fellow CWA group member told the media, "It was basically just a walk through"[7]. Whilst this likely is an exaggeration, it is grounded in the truth as Gamble infiltrated Johnson's account not once but twice. After his fellow CWA group member was raided, Gamble deleted the information that he had on Mr Johnson. However, he then decided to re-acquire Johnson's information by "re-jacking" his account. This is evidenced by records of further calls being made to Comcast, Mr Johnson, Mrs DiMarco and the DHS[21]. The fact that Gamble was able to attain unauthorized access to a senior US security official's account twice in a short time spam accentuates the vulnerability of Comcast accounts.

Whilst Gamble was attacking Johnson, he shifted his attention to FBI deputy director, Mark Giuliano. Gamble claimed he first accessed a Comcast email account under Giuliano's wife's name but declined to detail the hack, making it difficult to confirm the validity of these claims[6]. At Gamble's trial, it was disclosed that by once again using social engineering, he impersonated Giuliano and gained access to his Comcast communication and e-mail account and accessed LEEP. Gamble accessed Giuliano's FBI accounts via the Law Enforcement Online (LEO) help-desk by sending emails from Giuliano's account impersonating him[21]. Sending an email from Giuliano's account is a well-known intimidation technique as a low-level help desk employee may have felt compelled to please this high ranking official in fear of the negative repercussions associated with their disobedience. Earlier it was discussed that it is human nature to be helpful and kind. It is suggested that this feeling is intensified when an authoritative figure is involved[13]. In order to reduce occurrences such as this, employees must be aware of how imperative it is to be suspicious of prominent officials and know that once relevant inquiries are made in a cordial manner, it is acceptable.[13] Conversely, superiors must encourage lower ranking employees to be wary and respectfully respond to their overly cautious behaviour. Security protocols which detail the procedure for a high ranking official to acquire information from the lower levels of an organisation should be developed and implemented. These procedures may involve the exchange of emails using keywords and phrases before a request for data is made, having a higher ranking employee sign off on the distribution of data or password resets, or even using telephone calls for verbal confirmation.

During this cyberattack, the FBI realized their system was infiltrated and changed the password. However, Gamble once again put his social engineering skills to good use and called the FBI help-desk pretending to be Giuliano and regained access into the system via a password change. To the help-desk employees this may have been viewed as an everyday request as surveys suggest that 78% of persons have to reset passwords in a 90 days time-frame[11]. Thus, this reasonable request would have given them little reason to become suspicious. In addition, high level security officials may have been defensive against intrusions due to knowledge of previous Gamble's attacks but lower level employees may have operated under the assumption that they were in no danger as they possessed no information of significant importance. To rectify this, companies need to make it explicitly clear that security is enterprise-wide and everyone has a target on their back as they can be the person who causes the entire security system of the organization to collapse. To safeguard against malicious actions such as this, companies must invest in developing comprehensive security policies on a regular basis. All employees must keep

their guard up and be educated on the well-designed, constantly updated security policy. Additionally, there should be a system which detects suspicious activity such as multiple failed account access attempts. Thus, if suspicious activity is detected on certain accounts they would be flagged and before a password reset is initiated, authorisation by someone in a higher position must be given. Alternatively, before a password reset is allowed, the call handler should call the account holder, verify their identity and then ask for verbal verification.

Using this access, Gamble posted volatile information such as personal details of Officer Darren Wilson who shot and killed black teenager Michael Brown and was never convicted[5]. Not only was this information acquired illicitly, but its dissemination endangered someone. Despite this, Gamble may have regarded himself as a hero, as in his eyes, he was helping the family of a boy not much older than him to get the justice they never received. This appeal to higher loyalty is a technique used by criminals to rationalize their actions[19]. Internally, Gamble may have persuaded himself that his actions were for the greater good of the world and thus breaking the law and being a criminal was a small price to pay.

In keeping with his now discernible pattern, he bombarded Giuliano, his family and acquaintances with calls and threats forcing armed guards to secure their home and keep it under surveillance [5]. An explanation as to why Gamble seemed to threaten and harass his targets and their families may be because he simply thought that they deserved it. Neutralisation theory suggests that criminals may perceive their actions as acceptable because they discern their victims in a negative light[19]. In this scenario, Gamble explicitly stated on numerous occasions that he disapproved of the government's policies and deemed them immoral, even suggesting that they were condoning murder. From his perspective, a few prank calls and text messages may have seemed perfectly acceptable when compared to the actions of his victims.

Gamble stated that the purpose of this attack was not to attain information but simply as a retaliation due to the FBI investigation which was launched[6]. This directly contradicts statements made by Giuliano in which he declared that information which Gamble disseminated endangered government personnel and could have been weaponized by terrorist groups and US enemies[21]. Gamble also undermines himself as when conversing with journalist, Wesley Bruer, he disclosed that he targeted Brennan and Johnson because he believed they condoned the killing of innocent Israelis[21]. These contradicting motives suggest that whilst Gamble's cyberattacks may have been incited by his political tenets, he also considered the attack as a game and always wanted to have the upperhand.

Gamble continued his onslaught of cybersecurity attacks by infiltrating myriads of accounts belonging to security officials such as Obama's senior adviser, the Deputy National Security Advisor, the Executive Assistant Director of FBI Science and Technology Branch, the Director of National Intelligence and the Former Director of the National Geo-spatial Intelligence Agency[21]. The incidents involving Avril Haines (Deputy National Security Advisor) and Amy Hess (Executive Assistant Director of FBI Science and Technology Branch) are of particular interest because they showcase how important the gathering of good intelligence on his targets was to Gamble's success.

With respect to Haines, Gamble conducted a substantial amount of reconnaissance using both open source and human intelligence. At this stage, Gamble had already carried out an attack on Comcast and therefore would have interacted with their system and even some employees. This direct interaction would have equipped him with valuable human

intelligence which he utilised in this attack as he pretended to work for Comcast using an alias (Derek) to successfully gain access to Haines' account. In a large company such as Comcast, persons are not expected to know every employee by name as there may be hundreds of offices separated by large geographical distances. However, by just stating that he was an employee, Gamble may have been received more warmly by the Comcast call handler[13]. In his attempt to gain access, he quoted personal details which he had learnt during his preliminary surveying[21]. It would be reasonable to suggest that he attained these personal details via public sources (open-source intelligence) as a basic Google search of public figures tends to yield a vast number of relevant results.

This intrusion could have been avoided if the identity authentication methods outlined previously were employed. Also, Comcast should have had a rigid information security policy which is revised regularly. The company also should have conducted corporate seminars on a regular basis to educate their staff on social engineering techniques and emphasize that just because a person seems familiar with technical jargon and the workings of the company does not mean they are trust-worthy. These seminars which highlight the security policy and the reasoning behind the policy should not just be done once but on a regular basis by different security professionals to re-enforce key principles. In addition to in-person seminars, handbooks which outline the security policy should be distributed to all employees. By delivering the content in both verbal and non-verbal ways, and exposing employees to a variety of perspectives, there is a higher likelihood of employees comprehending, recalling and adhering to the security policy.

In the case of Hess, Gamble once again did extensive background research on his target even familiarising himself with details such as her career history and family life. By simply typing her name and credentials into a search engine, results showing her Linkedin and Facebook profiles appear. This insinuates that the vast majority of research done on Hess may have been open-source intelligence. Gamble developed a convincing story by pretending to be Ms Hess' husband once again demonstrating his expertise in pretexting. He then had a live chat with a Comcast Chat employee. After attempting several times to obtain sensitive information regarding Hess' Comcast account, he finally obtained her MAC ID and modem serial number. This allowed Gamble to access Hess' Comcast device and save her personal data onto his device[21]. The suggested mitigation method of companies keeping a log of how many times an account has been incorrectly accessed in a short period of time is applicable here as the Comcast chat employee who eventually divulged private information would be less likely to break security protocol if they were aware that the account was being repeatedly targeted. Also, if there was a system in place to flag the account for suspicious activity after failed access attempts, this security failure may not have transpired.

It should be noted that in this case along with every other aforementioned attack, Gamble's first move was always to target lower ranking workers in the company's hierarchy who held special privileges. This is a tactic utilised by seasoned social engineers as employees such as these typically do not comprehend the value of the information and power they possess and are consequently more likely to fulfil a malicious actor's request albeit unknowingly[13]. These employees may be seen as weakest link in a company's security. By receiving extensive training in the company's security protocol, they will be armed and capable of defending themselves against such attacks.

Also, almost all of Gamble's victims stored sensitive files and data in their email accounts. This is a cybercriminal such as Gamble's dream as it makes his job exponentially easier. In order to protect files, they should be moved from email accounts to secure file

storage locations[12]. No emails containing keywords such as default password, SSN or account details should live in an inbox[12]. Every individual has a responsibility to protect his or her self and this is one of the small protective measures that can go a long way.

After months of wreaking havoc and attaining classified information such as the details of thousands of FBI employees and case files, Gamble was arrested by the South East Regional Cybercrime unit at his home[21]. Whilst an exact figure of the financial loss due to Gamble's attacks is unknown, hundreds of overtime hours were spent by staff trying to rectify this problem and countless projects had to be aborted[21]. There were also irreparable damages to the reputations of the involved organisations resulting in loss of confidence and trust within their communities. At an individual level, persons whom Gamble targeted experienced deep psychological trauma due to the threatening and invasive nature of Gamble's attacks. Additionally, information leaked may have posed a threat to US national security. After considering the repercussions, the true extent of the devastation caused by Gamble's attacks may never be known.

Kane Gamble has effectively demonstrated that seemingly impenetrable organisations that invest millions of dollars in cutting-edge technology to safeguard their data can be infiltrated. In Bruce Shneier's eyes, he would be a professional as he targeted humans and relied on their inherent weaknesses to allow him to break security. His attacks should serve as a lesson for all organisations and push them towards investing the same amount of resources (if not more) in the human aspect of their security policies. This may entail hiring security professionals to develop and revise robust security policies for the organization on a regular basis, hosting seminars to educate all employees (from the board to the lowest level), creating a security policy handbook or even adapting the way in which employees interact with each other. By implementing measures to protect humans against cybercrime, security assurances can be made. Humans are often regarded as the weakest link in cybersecurity[10]. By strengthening this link little by little, there is a possibility that the chain can eventually become unbreakable. But if this never happens, human nature surely is to blame.

References

[1] *2021 DBIR Master's Guide*. 2021. URL: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.

[2] Arthur Baxter. *The 6 most common social hacking exploit techniques*. Oct. 2016. URL: https://www.intego.com/mac-security-blog/social-hacking/.

[3] Gail Cook. *"only amateurs attack machines; professionals target people"*. Mar. 2018. URL: https://www.lawscot.org.uk/members/journal/issues/vol-63-issue-03/only-amateurs-attack-machines-professionals-target-people/.

[4] Crum and Forster. "Two factor authentication". In: (Sept. 2018).

[5] Hayley Dixon. *British 15-year-old gained access to intelligence operations in Afghanistan and Iran by pretending to be head of CIA, court hears*. Jan. 2018. URL: https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/.

[6] Lorenzo Franceschi-Bicchierai. *Teen hackers who doxed CIA chief are targeting more government officials*. Nov. 2015. URL: https://www.vice.com/en/article/78kzjd/teen-hackers-who-doxed-cia-chief-are-targeting-more-government-officials.

[7] Lorenzo F Franceschi-Bicchierai. *Teen hackers: A '5-year-old' could have hacked into CIA director's emails*. Oct. 2015. URL: https://www.vice.com/en/article/8q84gx/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails.

[8] Kerry Gray. *Symbolism in V for Vendetta*. 2020. URL: https://study.com/academy/lesson/symbolism-in-v-for-vendetta.html.

[9] Colleen J Heffernan. "Social foundations of thought and action: A social cognitive theory, Albert Bandura Englewood Cliffs, New Jersey: Prentice Hall, 1986, xiii+ 617 pp. Hardback. US 39.50.". In: *Behaviour Change* 5.1 (1988), pp. 37–38.

[10] Michael Kassner. *Cybersecurity Pros: Are humans really the weakest link?* Dec. 2020. URL: https://www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link/.

[11] Daniyal Malik. *Study: 78 percent people forget their passwords and then go for reset!* Dec. 2019. URL: https://www.digitalinformationworld.com/2019/12/new-password-study-finds-78-of-people-had-to-reset-a-password-they-forgot-in-past-90-days.html.

[12] Bart McDonough. *Cyber smart: Five habits to protect your family, money, and identity from Cyber Criminals*. Wiley, 2019.

[13] Kevin D. Mitnick. *The art of deception: Controlling the human element of security*. Wiley, 2003.

[14] Robert Peck. *Mark Cuban: "data is the new gold"*. June 2017. URL: https://www.credit-suisse.com/about-us-news/en/articles/news-and-expertise/mark-cuban-data-is-the-new-gold-201706.html.

[15] Mathew J. Schwartz and Ron Ross. *Feds bust alleged 'crackas with attitude' hackers*. Sept. 2016. URL: https://www.bankinfosecurity.com/feds-bust-alleged-crackas-attitude-hackers-a-9389.

[16] Mathew J. Schwartz and Ron Ross. *Hackers claim FBI information-sharing portal breached*. Nov. 2015. URL: https://www.databreachtoday.com/hackers-claim-fbi-information-sharing-portal-breached-a-8667.

[17] Tom Sorell. "Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous". In: *Journal of Human Rights Practice* 7.3 (Sept. 2015), pp. 391–410. ISSN: 1757-9619. DOI: 10.1093/jhuman/huv012. eprint: https://academic.oup.com/jhrp/article-pdf/7/3/391/7194548/huv012.pdf. URL: https://doi.org/10.1093/jhuman/huv012.

[18] Sarah Staggs, Samantha McMichael, and Virginia Kwan. "Wishing to be like the character on screen: Media exposure and perception of hacking behavior". In: *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 14 (Feb. 2020). DOI: 10.5817/CP2020-1-4.

[19] Gresham M. Sykes and David Matza. "Techniques of Neutralization: A Theory of Delinquency". In: *American Sociological Review* 22.6 (1957), pp. 664–670. ISSN: 00031224. URL: http://www.jstor.org/stable/2089195.

[20] *The next stage of the information age: building bridges in a hybrid world*. Nov. 2021. URL: https://www.i-scoop.eu/digital-transformation/information-age/.

[21] *The Queen -v- Kane Gamble*. 2018. URL: https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf.