Cyber attacks: Implications for current and future policy

Introduction

Information networks are now everywhere and no field can escape it, especially not politics. Increasingly often cyber-related scandals are breaking out and the aim of many of them is the destabilizing a country's political life. The Estonian government in 2007 [1], a French political party in 2017 or the German government in early 2019 [3]. These and many other countries have suffered a cyber attack against their governments. Even the United States which is considered the most powerful country in the world, is an recurring victim of these type of cyber attacks. For example, the recent Russian interference in 2016 that targeted the presidential elections had widespread, global publicity. [4]

But how are these attacks carried out? who are the actors behind the scenes. What are the stakes involved and what enables these attacks? To answer these questions, this case study focuses on the group known as Fancy Bear and its attacks on the International Republican Institute and the Hudson Institute Think Tank in 2018. The case was chosen because of its context and the reactions of the actors involved. First section of this case study discusses the Fancy Bear cybercriminal group. Next, the two targets of the attack are introduced and some of the political context will be given before explaining the actual attack in the third section. Finally, the reactions of various parties involved are analysed.

Fancy Bear Group

APT28, Pawn Storm, Sofacy Group, STRONTIUM are some other known names given to Fancy Bear hacker group. The variety of names alone speaks of the scale of the organization. In fact, This group of hackers is linked to Russian military foreign intelligence (GRU) with high probability but no irrefutable evidence of this link has been published.

The group was founded in the mid-2000s and since then this group has been at the origin of numerous cyberattacks. These cyber attacks have had wide variety of targets and motives including for example collecting information on journalists, senior officials of the Orthodox Christian Church, political opponents, governments and companies [5].

Among the most famous attacks by the group include attacks on NATO and the White House in August 2015, using a zero-day exploit of java, spoofing website[6]. An attack on the French TV5Monde television channel, taking control of the 12 television channels as well as Facebook and Twitter accounts [7]. As well as, the Democratic National Committee hack in 2016 during the American elections [8]. All these attacks are complex and can take several months to organize and execute. Indeed, Fancy Bear is known to exploit zero-day vulnerabilities, spread malware and spear phishing. That is why Fancy Bear is classified as an APT, Advanced Persistent Threat, which is a type of stealth and continuous hacking, often orchestrated by humans targeting a specific entity. These kinds of attacks require a lot of resources, resources that only states can afford, which supports suspicions of links with the Russian government as well as the targets being aligned with Russian interests.

The intensification of attacks by this group as well as other hacker groups such as Cozy Bear, also affiliated with the Russian state, suggests that the Russian authorities are no longer concerned with hidden advances and are showing greater audacity.

Targets of the attack

As mentioned in the previous section, Fancy bear is an infamous group of cyber criminals. Their attack targets wary in range from small scale email leaks to serious attacks that are discussed in the news world wide [9]. In this report, the focus is on an attack on two organizations that are key facilities for the future of democracy, namely the international Republican institute and the Hudson institute think tanks [10]. This section describes the attack targets in detail.

International Republican Institute

International Republican institute (IRI) is an organization that was established in April 1983. It is an nonprofit organization and despite its name being similar to an American political party, it is totally nonpartisan organization that does not really take sides in politics. It's true aim is to improve democracy and freedom in the world. To achieve that, they work to create a conversation channel between the governments and the people. They encourage politicians to listen to the citizens and they encourage people to interact in the political decision making process. The greater goal of doing this is to make democracy flourish in countries where there is no democracy, and share best practices between democracies that do flourish to ensure efficient rule of the country and the longevity of current democracies. [11]

As the organization is a nonprofit, the empowering of democracy starts with volunteer experts from all over the world. Example work includes improving electoral processes and querying public opinions as well as increasing women's rights as well as the overall political and democratic systems. These actions are currently being done in 85 countries around the world. [11]

The exact reason why the organization was targeted by Fancy bear remain a mystery. However, knowing that Fancy Bear has russian connections and their repeated attempts to try and shake the state of democracies around the world, It would seem that this was just another attempt to do just that, to shake the trust in the future of democracy by gaining access to something confidential and scandalous and leaking it.

The Hudson Institute

The Hudson institute was established in 1961 by Herman Kahn. It is an organization that attempts to guide decisions makers in their preparation for the future. They try to encourage people to think outside of the box, outside of the conventional way of thinking. New ways of thinking are vitally important when managing step by step transitions to the future as the needs and thoughts will not be what they are now in the future and there needs to be a controlled steps from here to the future. [2]

These steps are required in various fields. For example, Defense will continue to be an important political issue in the future as new ways to wage war are undoubtedly being developed. For example, first and second world wars involved physical machines, while the next one might involve virtual warfare in the cyberspace. With the increased use of cyberspace it is important to understand its effect on people and how to control the change for example when it comes to international relations, economics and culture. In addition, the ever improving technologies for example in health care, will challenge the current way of thinking. The aim of Hudson institute is to create strategies that result in controlled transitions into these new ideas and technologies for example in terms of law making. [12]

Hudson institute is an American institute that operates both in America and globally. They organize publications, conferences, policy briefings and various other recommendations to affect how government and other officials make decisions. [12]

The exact reason for the attack remains a mystery aside from gaining access to the company's credentials. Since Fancy Bear has Russian ties and they have attempted to affect governing of foreign countries in the past, it might be reason enough that it was an important company for American democracy. As American democracy is being pushed to the limits under Donald Trump's presidency.

Description of the attacks

We now know the attackers, Fancy Bear, and the targets, the International Republican Institute and the Hudson Institute. Even if the reasons for this attack are unclear, the goal was to steal usernames and passwords in order to gain access to confidential information.

To steal credentials this, Fancy Bear used social engineering. Social engineering practices exploit the psychological, social and broader organizational weaknesses of individuals or organizations to obtain something fraudulently. For this attack, fancy bear uses a method that the group is familiar with, namely spear phishing. Indeed, Fancy Bear has already carried out this type of attack on at least 4 other targets since 2014.

Phishing consists of making the victim believe that he is speaking to a trusted third party (bank, administration, etc.) to obtain personal information: password, credit card number, number or photocopy of the national identity card or date of birth. It is the most popular attack of the 21st century and is not always easy to detect. Indeed, most often, an exact copy of a website is made in order to make the victim believe that he is on the official website where he thought he or she was connecting to. The victim will then enter his personal codes which will be retrieved by the person who created the fake site, he will then have access to the victim's personal data and will be able to steal and modify everything the victim has on the said website. The attack can also be carried out by e-mail or other electronic means.

Spear phishing [13] is a variant of phishing, the distinction is made on the target. In phishing, victims are more or less random, everyone can be affected, while spear phishing targets particular persons or company's employees. To this end, the attack is more elaborate, cybercriminals will collect information on the victims to make the attack as effective and efficient as possible. Spear phishing is a widely used tool in APT attacks targeting large companies, banks, NGOs or governments.

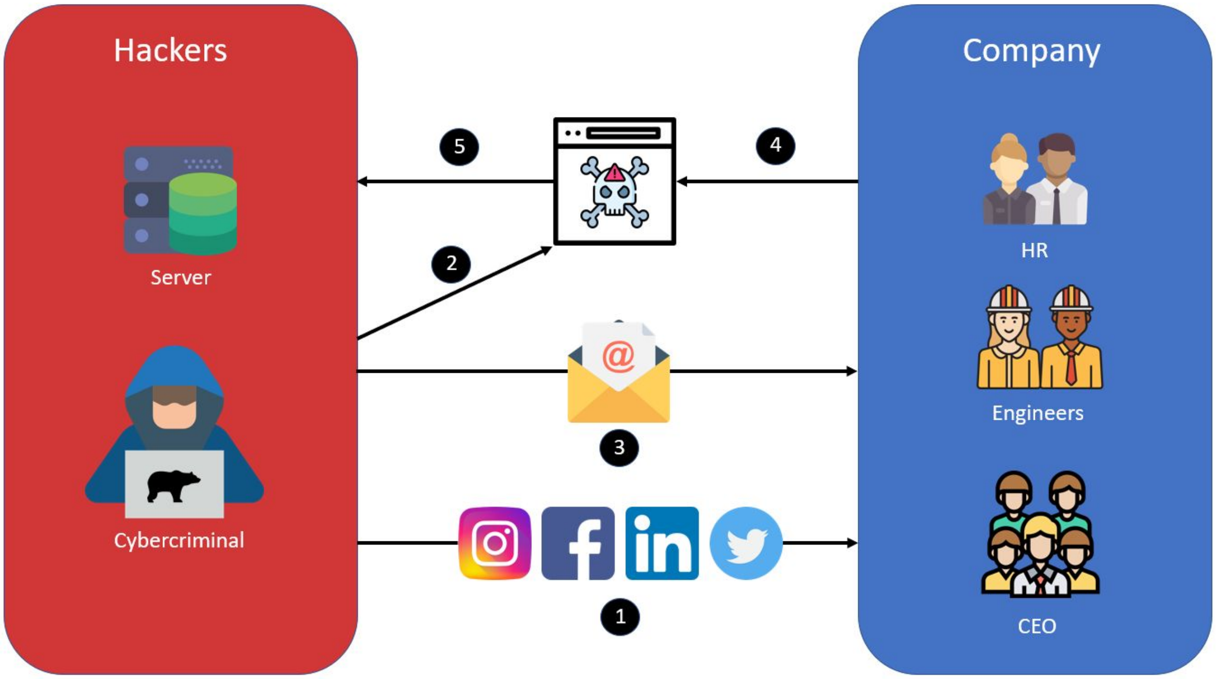

Figure 1 : schema of "spear phishing" attack

The spear phishing attacks are carried out according to the diagram in Figure 1, which will be explained in parallel with how the Fancy Bear's attack took place.

(1) First, hackers seek as much information as possible about the company, how it works, who are the people with high responsibilities in the company, what are their passions etc. For this phase, the Internet and social networks are a gold mine. But it is also possible to go directly to the company's buildings to try to collect information on the company's network, the software used etc. Regarding the Fancy Bear attack, it seems that the group had enough information to know that the institutes are using Microsoft Office 365.

(2) Then, the hacker must create the fake website. To do this, they will use url spoofed, i. e. URLs very close to the URL of the official site, use the same images, typography and graphic charter of the official site in order to deceive the user who will enter his personal information such as username and password.

For the Fancy Bear attack, 6 fake websites [14] were created: "my-iri.org", "hudsonorg-my-sharepoint.com", "senate.group", "adfs-senate.services", "adfs-senate.email" and "office365-onedrive.com". Thus Fancy Bear tried to imitate the websites of the institutions as well as the websites of the American Senate and the Microsoft office services. The goal here was clearly to make the users of these institutions believe that they were on the official sites and that they could connect without any problem.

(3) After creating the fake websites, it is necessary to distribute these fake sites. When phishing attacks on companies are carried out, the main targets are human resources, who are better able to open emails with attachments because of their regular contacts with people unknown to the company. Concerning the spear phishing, the targets will be employees with high access such as engineers, board members or HR for example.Fancy Bear certainly used this method to target people.

(4) Users have now received the email that seems quite legitimate and they go to the fake website thinking it is the real website. This is where social engineering really comes in. The hacker takes advantage of the victim's inattention, naivety or ignorance to deceive him. The victim will connect using his username and password without suspecting anything. The Fancy Bear attack stopped here. Indeed, Microsoft's Digital Crimes Unit (DCU) managed to take control of the 6 websites thanks to an order from the American court. This order [15], obtained in 2017 following further attempts by Fancy Bear to falsify domain names, makes it easier for Microsoft to take control of the domains used by the group in attacks. However, Microsoft has no way of knowing if the attack worked before the sites were seized. To date, there is no way to determine whether or not the attack was successful.

(5) Once the username and password are used by the victims, they are stored on the hackers' servers. Thus, hackers were able to obtain sensitive information without having penetrated the company's network but using social engineering.

Reaction

In August 2018, CEO and President of the Hudson Institute, Kenneth R. Weinstein, publicly announced in the press that they had avoided a spear phishing attack to recover the credentials of their users. He said it was Microsoft that alerted them just in time and revealed the identity of the group behind the attack, Fancy bear, and its alleged link with Russia. In addition, he gave the possible reasons for this kind of attempted attack: ”*We are especially proud of our Kleptocracy Initiative, which has exposed how Mr. Putin and his cronies in the Kremlin and Eastern Europe launder their ill-gotten money through shell companies and offshore accounts in Western jurisdictions”*. Adding that these attempts at intimidation do not work: ”*If Fancy Bear's intention is to embarrass or intimidate us, it won't work.”*[16]

Since the majority of American parties based their IT systems on Microsoft platform Office 365, Microsoft were obliged to react and therefore launched the Defending Democracy Program at the beginning of 2018. It was particularly in anticipation of the upcoming midterm elections in November of the same year and presidential elections in the USA.

It is a programme set up in democratic countries to help stakeholders in their electoral campaigns against cybersecurity issues. These objectives are:

- ***“Protect campaigns from hacking*** *through increased cyber resilience measures, enhanced account monitoring and incident response capabilities;*
- ***Increase political advertising transparency online*** *by supporting relevant legislative proposals such as the Honest Ads Act and adopting additional self-regulatory measures across our platforms;*
- ***Explore technological solutions*** *to preserve and protect electoral processes and engage with federal, state and local officials to identify and remediate cyber threats; and*
- ***Defend against disinformation campaigns*** *in partnership with leading academic institutions and think tanks dedicated to countering state-sponsored computational propaganda and junk news.”* [17]

However, after the attack against the two institutes, Microsoft decided to launch an extend called AccoutGuard. It is a new security service offered free of charge to organizations using Office 365 that participate in political life and the defence of democracy. The service allows these exposed organizations to protect themselves against cyber threats. It includes:

- “*Best practices and security guidance specific to those in the political space.*
- *Access to cybersecurity webinars and workshops.*
- *Notification in the event of a verifiable threat or compromise by a known nation-state actor against the participant’s O365 account.*
- *Notification to both the organization and, where possible, the impacted individual if a registered Hotmail.com or Outlook.com account associated with the organization is verifiably threatened or compromised by a known nation-state actor.*
- *Recommendations to the participating organization for remediation if a compromise is confirmed.*
- *A direct line to Microsoft’s Defending Democracy Program team.”* [18]

Microsoft responds to these attacks by strengthening security systems, raising awareness among campaign teams, being as transparent as possible about future attacks and implementing remediation plans in the event of compromises.

Political consequences

Microsoft therefore confirms that the fake sites are linked to the Russian intelligence unit. These actions could be explained by the fact that one of the objectives of this unit is to disrupt the institutions that are challenging V. Putin's presidency. Among these institutes, we find the Hudson Institute, which is particularly interested in the emergence of kleptocracy in some countries. A kleptocracy is a pejorative term for a political system in which one or more people at the head of a country engage in corruption on a very large scale. Concerning the International Republican Institute, it is undoubtedly to intimidate them in their efforts to promote democracy in the world.

In addition, it should be noted that the IRI Board of Directors is composed of politicians very closed to the Republican Party, who had raised quite a few criticisms about Trump-Putin relations, particularly after their last meeting in Helsinki.

Among them are John McCain and Mitt Romney, two former Republican presidential candidates.

The IRI President reacted by describing this attack attempt as "*consistent with the campaign of meddling that the Kremlin has* *waged against organizations that support democracy and human rights*" Adding that "*It is clearly designed to sow confusion, conflict and fear among those who criticize Mr. Putin's authoritarian regime*"

Microsoft President Brad Smith announced that "*these attempts are the newest security threats to groups connected with both American political parties"* before the midterm elections. And added that the main aim behind these attacks is *"to fracture and splinter groups in our society."* [19]

On the Russian side, government officials formally reject Microsoft's accusations.
Thus the spokesman for the Kremlin states "*We don't know what hackers they are talking about*"
Later, the Russian Foreign Minister added: *"It is regrettable that a large international company, which has been working in the Russian market for a long time, quite actively and successfully has to take part in a witch-hunt that has engulfed Washington (...)"* [23]

These attacks against these institutes are accumulating on the long list of alleged cyber attacks from Russia. Indeed, according to US Director National Intelligence Dan Coats, hacking threats to the United States are on the rise. And they come from Russia in particular. "*The warning signs are there. The system is blinking. It is why I believe we are at a critical point," Coats said "That's why I think we have reached a critical point.* Moreover, according to him, the aim is not simply to disrupt the normal course of American democracy: "*Today, the digital infrastructure that serves this country is literally under attack*," he said.

According to Dan Coats, the "worst" perpetrators of cyber attacks are Russia, China, Iran and North Korea, but Russia is "*the most aggressive foreign actor, without a doubt. And they continue their efforts to undermine our democracy*," he insisted. U.S. authorities charged 12 Russian intelligence agents for hacking into Democratic Party computers during the 2016 presidential campaign, which was won by Republican candidate Donald Trump. [20]

Thus, relations between Russia and the United States have deteriorated and it is as if we were to return again to an atmosphere of cold war. As the last symbol of this deterioration, in October 2018, the US Department of Justice announced that it had charged 7 Russian spies for their role in several cyber attacks. The seven officers in question all belong to the Russian Military Intelligence Unit (GRU). [21]

Conclusion

The general public is familiar with cyber attacks under the prism of money and sometimes blackmail. Indeed, in the general idea, the hacker is a single person who tries to steal sensitive information such as bank details, accounts on certain sites etc..

However, some cyber attacks are on a larger scale. More and more groups of hackers are appearing with links to governments, which therefore have a greater strike force. Attacks are increasingly targeting governments or large organizations more or less close to a country's internal politics.

The first proven attack on a state is Russia's attack on Estonia. A DDoS that has paralyzed several Estonian administration sites as well as banking and media sites. Since 2015, the number of attacks launched by Fancy Bear has increased steadily. The majority of their attacks are against politically linked institutions or institutions openly criticising the Russian government. Since 2016, with suspicions of Russia's interference in the American elections, diplomatic tensions between Russia and the United States are becoming increasingly tense, to the point that a new Cold War is not unthinkable.

Cyberspace has become the new battleground for states and cyber attacks new weapons in the context of hybrid attacks. Even if the attacks are foiled, as the one presented, they will have a diplomatic impact. The attacks on the IRI and Hudson Institute, combined with other attacks by Fancy Bear and other groups, led the USA, the United Kingdom and the Netherlands to publicly denounce Russia on 4 October 2018 over these cyber attacks [22]. Relations between the United States and Russia have never been more tense than since the end of the Cold War.

References

[1] https://www.bbc.com/news/39655415
[2] https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200
[3] https://www.ft.com/content/00954878-0ffa-11e9-a3aa-118c761d2745
[4] https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-trump-election-timeline.html
[5]https://www.nato-pa.int/download-file?filename=sites/default/files/2018-12/166%20CDS%2018%20F%20fin%20-%20PARADES%20AUX%20MENACES%20HYBRIDES%20EMANANT%20DE%20LA%20RUSSIE%20-%20RAPPORT%20JOPLING_0.pdf
[6] https://en.wikipedia.org/wiki/Fancy_Bear#EFF_spoof,_White_House_and_NATO_attack_(August_2015)
[7] https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983
[8] https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/
https://perception-point.io/resources/incident-reports/a-look-inside-fancy-bear/
Fancy Bear
[9] https://en.wikipedia.org/wiki/Fancy_Bear
[10] https://www.bbc.com/news/technology-45257081
[11] https://www.iri.org/who-we-are/faqs
[12] https://www.hudson.org/about
[13] https://www.kaspersky.com/blog/what-is-spearphishing/20412/
[14]
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
[15] http://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network
[16] https://www.hudson.org/research/14515-what-it-s-like-to-be-a-fancy-bear-target
[17] https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program/
[18]
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
[19] https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html
[20]
https://edition-m.cnn.com/2018/07/14/politics/director-of-national-intelligence-dan-coats-cyberattacks-russia/index.html?r=https%3A%2F%2Fwww.google.com%2F
[21] https://www.theguardian.com/us-news/2018/oct/04/us-russia-criminal-charges-olympics-hacking
https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf
[22]
https://www.washingtonpost.com/world/europe/britain-directly-blames-russian-military-intelligence-for-broad-range-of-cyberattacks/2018/10/04/13a3a1f8-c7b6-11e8-9158-09630a6d8725_story.html?noredirect=on&utm_term=.373f1d9501a3
[23]
https://www.reuters.com/article/us-usa-russia-hackers/russian-hackers-targeted-u-s-conservative-think-tanks-says-microsoft-idUSKCN1L60I0