A Romanian at the epicenter of controversy: the Guccifer case and its general impacts and destabilization of the American political scene

Mateo-Daniel DOGARU,
Police Academy "Alexandru Ioan Cuza", Bucharest, Romania
mateodogaru09@gmail.com

Abstract
In the digitalization era, the Guccifer case, involving Romanian hacker Marcel Lehel Lăzăreanu, has become emblematic of information sabotage. Operating under the pseudonym Guccifer, Lăzăreanu executed a series of high-profile cyber-attacks, targeting prominent organizations and political figures. His most infamous act involved hacking the email accounts of influential U.S. political figures and releasing compromising information on online platforms. These actions triggered widespread public confusion and unrest, significantly impacting the political landscape. By exposing confidential and sensitive information, Guccifer fueled speculation and controversy around various political candidates and organizations, thereby destabilizing the democratic process. The Guccifer case is a classic example of information sabotage, not only due to the exposure of secret information but also due to its strategic manipulation to influence public opinion and erode trust in democratic institutions. Guccifer's selective leaking and distribution of information allowed him to craft narratives that damaged the reputations of targeted politicians, fostering an atmosphere of uncertainty and distrust in the electoral system. This case has raised urgent questions about information security and integrity in the digital age. It underscored the fragility of modern political paradigms and demonstrated that threats to democracy can originate from the virtual realm. A single individual, equipped with technology and expertise, can cause significant damage, particularly in the realm of information sabotage. The Guccifer case thus serves as a stark reminder of the vulnerabilities inherent in our digital infrastructure and the critical importance of robust information security measures to protect democratic processes.

Keywords: information, democratic, digital, sabotage.

1. Introduction

Nowadays, everything is based on power, and often power comes from information. So the world is in a constant search for information, whatever the purpose or means. That's why some people try to get hold of sensitive information, which can affect a wide range of people, as in the case of information sabotage.

Information sabotage [1] refers to intentional and malicious activities aimed at disrupting, damaging, or manipulating information systems to achieve specific goals. This can include unauthorized data access, alteration or destruction, and dissemination of false information to undermine the credibility of organizations or individuals. These acts are a subset of cyber sabotage, encompassing any action designed to compromise the integrity and functionality of information and communication technologies.

Anyone can make use of this information sabotage, a relevant example being the Guccifer case that we will study throughout this paper from several perspectives. Marcel Lehel Lazar, known by his pseudonym "Guccifer" is a brilliant Romanian hacker responsible for serious attacks in the form of high-level computer security breaches in Romania and the United States of America.

Marcel Lehel Lazar, born on November 23, 1971, in the village of Sâmbăteni, Arad, became the most famous hacker without equipment and knowledge in the field. Before starting the so-called Guccifer "experiment", a pseudonym that comes from the iconic luxury brand Gucci and the angel kicked out of heaven Lucifer "Gucci's style and Lucifer's light", Marcel was a taxi driver without higher education and without high-performance equipment, but with exceptional intelligence. From behind a computer that at first glance looked like it wouldn't last much longer and a little Samsung smartphone (an old one), he managed to wreak havoc both at home in Romania and abroad, in the United States of America, which showed everyone how easy it is to be a "hacker" and how easy it is to be attacked yourself in our times, the times of digitization.

"He wasn't really a hacker, just a very smart, very patient, and very persistent guy," said Viorel Badea, the prosecutor who handled the case. Guccifer is also known for making public several self-portraits taken by former US President George W. Bush, for revealing to everyone the "flirtations" between Corina Cretu, a member of the European Parliament, and Colin Powel, and for obtaining numerous photos and private messages from national and international celebrities. "This is just a poor Romanian who wanted to be famous," Badea added.

Guccifer's list of attacks is long. In the first phase, in 2011, out of his desire to become famous in Romania, “The Little Smoke” as he was called back in 2011 launched attacks against well-known personalities in Romanian television such as Bianca Drăguşanu, Laura Cosoi, Corina Caragea, but also in the political arena in Romania, in 2013, personalities such as George Maior [2] (the head of the Romanian Intelligence Service between October 2006 - January 2015), Corina Cretu [3], Elena Udrea, Raed Arafat, Emil Boc, and many others.

After the success of his attacks in Romania, Guccifer wanted to expand his horizons to the realm of all possibilities, namely the United States. He launched attacks on major American political figures, managing to get his hands on sensitive information that destabilized elections and democracy in America. Some of the most famous personalities who have fallen into the hands of the hacker are Colin Powell [4], George W. Bush [5], Dorothy Bush Koch, Hillary Clinton [6], and many others. The attacker believes that everyone in power in America is corrupt, and everyone being controlled by Americans is controlled by corrupt people, that’s why Guccifer declared: "I hack the rich and powerful to show the world that they are not above scrutiny. Behind closed doors, they manipulate and deceive, but through my actions, I expose their corruption and bring transparency to the political elite."

2. Methods of attack leading to information sabotage

Guccifer has shown the world that you don't have to be an IT engineer or programmer to cause international damage or become a famous hacker. An old computer, motivation, and a lot of intelligence were behind his frauds that caused a lot of problems both locally in his home country and internationally, as mentioned above, in the United States.

He has managed to use hacking methods considered basic to create more problems than anyone expected. Among the methods used by Guccifer, we can mention: phishing, password guessing, social engineering, or account recovery processes.

Guccifer tried not to use these methods by their default meaning and that's why his hacking methods prominently featured social engineering tactics. While there is no specific documented instance of Guccifer using phishing techniques, his methods did involve elements of social engineering that are closely related to phishing or other methods above mentioned. For example, Guccifer used publicly available information to guess security answers and passwords, which is a common technique in phishing campaigns. He also sent emails that appeared to come from trusted sources to trick victims into revealing their credentials or allowing access to their accounts.

One notable method Guccifer used, which mirrors phishing techniques, involved gaining access to email accounts by exploiting weak security questions and publicly available personal information. For instance, he accessed the email account of Sidney Blumenthal, a close adviser to Hillary Clinton [7], by correctly answering security questions based on publicly available information about Blumenthal.

3. The beginning of Guccifer's highway to fame had its epicenter in Romania

The beginnings of the famous hacker were based in Romania. As we mentioned before, he attacked email accounts or tried to get sensitive data from several political personalities or personalities from Romanian show-biz. Next, we will analyze some important attacks that he initiated on some personalities in Romania.

"In this case there is a reasonable suspicion that, during 2013, on the basis of a single criminal resolution, the defendant L.M.L (Lazăr Marcel Lehel) repeatedly and unlawfully accessed, by violating security measures, e-mail accounts belonging to public persons in Romania, in order to gain possession of confidential data in the e-mail, after which he changed the authentication passwords, thus restricting the access of the right user to the computer data in the e-mail," a DIICOT spokesperson said in a press release about the case.

A big success for Guccifer was when he managed to hack the personal Yahoo account of the former director of the Romanian Intelligence Service (SRI), George Maior. During that time, in 2013, using the most basic forms of attack, Guccifer managed to break into the Yahoo account of the SRI director and reveal sensitive information that could have affected national security, so, the hacker created one of the most dangerous security incidents from Romania.

Guccifer conducted extensive research on George Maior, gathering publicly available information about his personal and professional life. By this, he could correctly answer the security questions that pop up when you try to access your, or in this case another email address or for password recovery. Many email accounts, including those on Yahoo, use security questions to facilitate password recovery. These questions often involve some basic personal information, such as the user's mother's maiden name, the name of a first pet, or the city of birth. Guccifer was able to find answers easily to such questions through

diligent online research. Guccifer could reset Maior's email password by correctly answering the security questions.

While the specific contents of George Maior's emails accessed by Guccifer are not publicly detailed, the hack itself is a significant example of the impact and risks of cyber-attacks on high-ranking officials. Guccifer's hack highlighted the weaknesses in the security measures used by public officials. His ability to breach the email account of a top intelligence official demonstrated the potential risks associated with insufficient security practices. These pieces of information offer a general understanding of Guccifer's methods and the broader implications of his hacks, even though specific revelations from George Maior's emails are not comprehensively detailed.

Guccifer did not only focus on attacking the high political or security pillars of the country. He also revealed sensitive information about personalities in the Romanian show biz, one of the victims being Corina Chiriac herself.

Guccifer's attack on Corina Chiriac was part of his broader hacking activities targeting various public figures. Corina Chiriac, a prominent figure in Romanian showbiz as a singer and actress, had her private emails and documents compromised by Guccifer. Using the same tricks as in George Maior's case, the leaked information about Corina Chiriac included personal communications, possibly revealing details about her personal life, career, and interactions with others, financial details, confidential correspondence, or any other data that was stored in Chiriac's compromised accounts. While the exact contents of the leaked information may vary and could include sensitive or private details, the specifics are not always widely disclosed or discussed publicly out of respect for individuals' privacy. Guccifer's hacking activities were illegal and unethical, and the leaked information could have potentially caused distress or embarrassment to those affected.

4. Guccifer's most impactful actions, ironically, took place in the realm of all possibilities, the United States of America

After the successive attacks against important personalities in Romania, Guccifer extended its horizons to big personalities in the USA, the attacks directed at them being also basic, with the same old equipment that at first glance seems useless but after being used properly it represented a powerful weapon against the American political plan, a weapon that managed to influence the subsequent elections.

The most significant information sabotage was directed at Colin Powell, the Former United States Secretary of State. The hacker on the morning of 11 March 2013 handiworked Colin Powells's Facebook page [8] and posted messages that disparaged, messages with vulgar contents like: 'You will burn in hell, Bush!' or 'Ass hole who would burn in hell for crimes purportedly committed along with Bush and Rockefeller family members'. In another post, Guccifer declared 'Kill the Illuminati! Tomorrow's world will be a world free of Illuminati or will be no more!'. After the former Secretary of State regained control of his Facebook page, he posted a message about the hack and tried to apologize to his followers for 'all the stupid, obscene posts that are popping up.' If that wasn't enough, instead of the messages, Guccifer uploaded to Powell's Facebook page screen grabs showing his prior access to e-

mail accounts of very important personalities like George W. Bush family members [8], including his siblings Neil and Dorothy.

Also, Guccifer's hack into Colin Powell's email uncovered a personal relationship between Powell and Romanian diplomat Corina Crețu. The leaked emails, spanning from 2010 to 2011, contained flirtatious and intimate messages between the two. While Powell denied having an affair, he admitted that their communication was personal. The release of these emails drew significant media attention and fueled speculation about the nature of their relationship.

The information sabotage started by Guccifer was about to get bigger and bigger. In his desire to find out sensitive information and destabilize the American political system he considered corrupt, he also breached the email account of Sidney Blumenthal, a former aide in the Clinton White House, and disseminated stolen memos sent to former Secretary of State Hillary Clinton regarding Benghazi. Guccifer uses basic but effective tactics, targeting the family and friends of his main objectives rather than going after them directly. By compromising their public email accounts, he exploits the relatively simple process of resetting passwords, which often requires answering a few personal questions. This method is not particularly challenging when the target is a celebrity. Guccifer's hack on Sidney Blumenthal, a close associate of Hillary Clinton, led to the exposure of a series of emails that Clinton had sent during her tenure as Secretary of State. While the hack was indirect (Blumenthal's email account was compromised, not Clinton's), it still revealed significant information like leaked emails including private discussions between Blumenthal and Clinton, providing insights into her thoughts and activities during her time as Secretary of State and also a conversation via email that contained sensitive information about the Benghazi attack, from Libya 2012. Also, we can talk about potential conflicts of interest because those emails highlighted some of the Blumenthal’s business interests in Libya.

These leaks contributed to the scrutiny and controversy surrounding Clinton's use of a private email server for official communications, which became a significant issue during her 2016 presidential campaign.

The brilliant hacker broke into the AOL accounts of Bush family pals Willard Heminway and CBS sportscaster Jim Nantz, as well as Dorothy Bush Koch, the sister of George W. Bush and the youngest child of George H.W. Bush. He obtained a wealth of private material about the Bush family, including correspondence between the two former presidents, through the penetration of other accounts. However, the hacker also gained access to private emails, documents, and images from Dorothy Bush Koch's account. For instance, the hacker obtained contact between Scott Pierce, the 82-year-old brother of Barbara Bush, and the 87-year-old former First Lady by breaking into his AOL account. Additionally, Patricia Legere, a friend of the Bush family and a former Miss Maine, and Josephine Bush, the 41st president's sister-in-law, and mother of Access Hollywood host Billy Bush, had their Comcast email accounts compromised by the hacker.

The hacker gained access to private information on the whereabouts, ailments, and travels of the Bush family thanks to the unauthorized incursions. Although the hacker managed to

gain access to AOL and Comcast accounts, it appears that they were not able to breach the personal email accounts of the two former presidents, who use distinct domains for their official post-presidential correspondence.

The hacker withheld information about the purpose of the attacks and the methods used to engineer them across several months of email discussions. However, it appears likely that the hacker's examination of previously hacked email accounts helped identify certain targets. The targeting of individuals of the Bush family's inner circle most likely makes sense given this daisy chain strategy. After falling in sequence, one of the hacker's victims thought their email account was a "domino."

5. Guccifer's payment for all his actions

Ironically said his payment, more concretely we will talk about what punishments Guccifer got for all his attacks so for all the private or classified information he stored or made public.

In Romania, in 2014, Guccifer was arrested, at the proposal of DIICOT Arad, and sent to trial for violating the correspondence of several public figures in Romania, including MEP Corina Cretu and even SRI Director George Maior. In the same year, the Bucharest Court sentenced him to 4 years in prison, plus the 3 years suspended from his previous sentence. The sentence of 7 years remained final and the man from Oradea was then imprisoned in Arad Penitentiary. Initially jailed in 2014 in the country after pleading guilty to charges of unauthorized access to a protected computer system and aggravated identity theft, Guccifer was eventually extradited to the US. The man spent four years in a Pennsylvania prison.

‘Marcel Lehel Lazar, 44, of Arad, Romania, a hacker who used the online moniker “Guccifer,” was sentenced today (September 1, 2016) to 52 months in prison for unauthorized access to a protected computer and aggravated identity theft [8].’ He pleaded guilty before U.S. District Judge James C. Cacheris of the Eastern District of Virginia on May 25, 2016. In exchange for a plea deal, Lazar admitted that from at least October 2012 to January 2014, he willfully obtained unauthorized access to about 100 Americans' [5] personal email and social media accounts to receive their personal information and correspondence. Lazar said that among his victims [9] were members of the immediate families of two previous US presidents, a former presidential advisor, a former member of the US Joint Chiefs of Staff, and a former member of the US Cabinet. According to the statement of facts submitted with his plea deal, Lazar frequently made his victims' private email communication, financial and medical records, and personal photos available to the public. The case was looked into by the Secret Service, DSS, and FBI. The case is being prosecuted by Assistant U.S. Attorneys Maya D. Song and Jay V. Prabhu of the Eastern District of Virginia, as well as Senior Counsel Ryan K. Dickey and Peter V. Roman of the Criminal Division's Computer Crime and Intellectual Property Section. The Office of International Affairs of the Criminal Division rendered noteworthy support. The Romanian government's help in this situation is much appreciated by the Justice Department.

After serving his sentence (August 2021), in an interview with The Intercept, the renowned Romanian hacker said several things about both the people he learned about and his actions.

He made a statement about Bush's unveiled self-portraits: ‘Thanks to Guccifer's infiltration of Dorothy Bush Koch's AOL account, the world now knows that her brother, George W. Bush, likes fine self-portraits in the bathroom,’ writes The Intercept.

Also, he declared: ‘I paid for it. People have to have privacy. But it's not like I want to know what my neighbors are talking about. I wanted to know what these guys in the United States were talking about and that's why (I resorted to this gesture - ed.). I was sure bad things were happening. That's the reason I did it, not for any other dubious reason. What I did is okay,’ Among other things, Guccifer said that he was disappointed that although he helped uncover Hillary Clinton's private email and then cooperated with federal officials, he was the one who ended up in jail, while she was not charged in connection with what he exposed. He also claimed that he came close to breaking into Trump's "inner circle" in October 2013. ‘I was about to break into Trump's boys, Ivanka, and others,’ he claimed. ‘But my computer broke...’

Guccifer declared related to The Intercept article that: ‘The article in The Intercept doesn't contain a lot of detail, it doesn't capture much of the turmoil I experienced. In the book, however, I went into a lot of things, much more deeply. The 300 pages I've written have already drained me of energy,’. ‘There's some incredible stuff in this book, because I'm splitting the difference,’ Guccifer said, predicting an ‘explosive’ return to the public arena.

6. Final conclusions

Guccifer conducted his hacking for a variety of political and personal motives. His primary goal was to reveal wrongdoing, call attention to abuses of authority, and highlight the weaknesses of powerful individuals.

Guccifer has been able to gather and divulge to the public sensitive and compromising information about a number of prominent political and public figures in the United States through his attacks. These include Sidney Blumenthal, Colin Powell, and other members of Hillary Clinton's inner circle's private correspondence. The public perception of the victims has been harmed by these revelations, which have sparked media scandals.

The political climate has been significantly impacted by Guccifer's acts, which have also brought attention to the significance of cyber security. His hacking operations have unintentionally exposed security flaws and breaches, which has led to informatical sabotage. This has highlighted the need for more stringent data protection measures and, consequently, raised awareness of the risks associated with cyberspace in the digital age.

During the 2016 presidential election, several people perceived Guccifer's actions as having the ability to sway public opinion and undermine the Democratic Party's campaign, which was perceived as a side benefit for Donald Trump's campaign. Even though Guccifer didn't have a direct relationship with Trump, the revelations stoked uncertainty and fueled political controversy.

References

[1] "Britannica ‘sabotaje subversive tactic‘," [Online]. Available: https://www.britannica.com/topic/sabotage-subversive-tactic . [Accessed 2024].

[2] "HotNews.ro, Vlad Barza, ‘Hackerul "Guccifer", care i-a spart contul sefului SRI, George Maior, a fost prins la Arad’," [Online]. Available: https://www.hotnews.ro/stiri-esential-16457219-hackerul-guccifer-fost-prins-arad.htm . [Accessed 2024].

[3] Adevărul.ro, "Octavian Palade '„Micul Fum“ şi marele noroc. Cum a reuşit Guccifer să spargă contul Corinei Creţu şi să bage spaima în familia Bush’," [Online]. Available: https://adevarul.ro/stil-de-viata/tehnologie/micul-fum-si-marele-noroc-cum-a-reusit-guccifer-1577962.html. [Accessed 2024].

[4] The Smoking Gun, "Colin Powell Facebook Page Was Hacked By Same Perp Who Broke Into Bush Family E-Mail Accounts," [Online]. Available: https://www.thesmokinggun.com/buster/colin-powell-guccifer-facebook-hack-467842 . [Accessed 2024].

[5] Independent, "Feliks Garcia, ‘Notorious hacker 'Guccifer' pleads guilty to hacking George W Bush and 100 others’," [Online]. Available: https://www.independent.co.uk/news/world/americas/hacker-guccifer-pleads-guilty-george-w-bush-hillary-clinton-emails-a7049001.html . [Accessed 2024].

[6] The Intercept, "Sam Biddle, ‘SORRY, NOT SORRY Guccifer, the Hacker Who Launched Clinton Email Flap, Speaks Out After Nearly a Decade Behind Bars’," [Online]. Available: https://theintercept.com/2023/01/15/guccifer-interview-hacked-clinton-emails/. [Accessed 2024].

[7] Wikipedia, "Guccifer," [Online]. Available: https://en.wikipedia.org/wiki/Guccifer#Arrests_and_convictions_in_Romania. [Accessed 2024].

[8] Office of Public Affairs U.S Department of Justice, "Romanian Hacker “Guccifer” Sentenced to 52 Months in Prison for Computer Hacking Crimes," [Online]. Available: https://www.justice.gov/opa/pr/romanian-hacker-guccifer-sentenced-52-months-prison-computer-hacking crimes.

[9] The Smoking Gun, "Bush Hacker's Victims Include U.S. Senator," [Online]. Available: https://www.thesmokinggun.com/documents/internet/bush-hackers-other-victims-637098. [Accessed 2024].