Exploiting recruitment agencies to steal your personal data

Jovan Radakovic specializes in OSINT and HUMINT collection. Jovan has close to a decade of experience in supporting clients in the global marketplace to navigate the operating environments of interest and mitigate any potential risks associated with their interests. Jovan engagement range from basic due diligence and reputational inquiries to complex financial investigations, asset tracing, litigation support, market entry studies and highly specialized on-the-ground investigations in high-risk jurisdictions.

Shifting the limelight

While the escalating conflict in Ukraine continues to cause international economic havoc, individuals and organizations within and beyond the region are increasingly in danger of experiencing disruptive cyber incidents. Series of economic sanctions against Russia resulted with a response that includes orchestrated cyber-attacks on critical infrastructure, data centers, as well as individuals and commercial entity. Not only has this cyberwarfare opened up questions on the safety of regular citizens, it brought up the question on vulnerabilities within different sectors. While many are correct in arguing that the government databases are the primary target, there are increasing dangers that small and medium enterprises (SMEs) face in the cyber world.

As the matter of cybersecurity policies and standards employed by SMEs is a broad topic, this essay confines its scope on the lifeline of any economy - recruitment agencies. This essay explored the following topics: 1) understanding threat actors and their mechanism within the context of Russia-Ukraine conflict and the nexus between the regional and international cyberwarfare; 2) exploring and bringing attention to how recruitment agencies fall victims to cyberattacks using two recent cybersecurity incidents; 3) looking for solutions on identifying broader cybersecurity concerns and the nexus between seemingly isolated regional conflict and a global cyber-playfield.

Threat Actors and Their Mechanisms

In analyzing the cyber-attacks since the start of the Ukrainian conflict, it is evident that it offered a "bolt hole" for multiple Russian hacking groups that are partnering with the country's intelligence agencies to disrupt Ukrainian and Western national securities. Preliminary desktop research identified over a dozen such groups corroborating the notion that these have publicly sided with the Russian government and are actively engaged in cyber-attacks against Ukrainian and Western governments [1]. Albeit these groups form a "melting pot" of different ideas and expertise, pattern analysis revealed the following common denominators:

1) <u>These hacking groups operate as legitimate companies:</u>

As seen in the example of Conti, a prominent Russian hacking group, its operation was set up as hierarchy with individuals having different responsibilities and roles. The mechanics behind Russian hacking groups are obfuscated given the context and the jurisdiction, but a landmark leak changed how the Western world perceives these threat actors. Conti Leaks – a series of files and chats that were leaked in early 2022, frequently labelled as the Panama Papers of ransomware, offered insight into the group's workings and presented analysis anchors for further investigations and defense strategies. Specifically, the chats contained in the leak contained insight into the group's workings including their offensive strategies, as well as their possible ties and support from the Russian government [2].

Because Conti's ties to the Russian government are tentative, this essay looks into another prominent Russian hacking group Gamaredon Group (Gamaredon), a hacking-cluster targeting multiple Ukrainian and Western datacenters. According to Microsoft and online researchers, the group "has been behind a streak of spear-phishing emails targeting Ukrainian entities and organizations related to Ukrainian affairs since October 2021" [3]. Moreover, according to the same sources, the group is closely linked with Russia's Federal Security Service (FSB), the country's domestic intelligence service, and has been involved in dozens of phishing attacks on Western government, civil, and private organization [3].

2) <u>These hacking groups rely on phishing attacks</u>

Analysis by leading organizations, such as Microsoft, has shown that Russian hacking groups tend to use spear-phishing to infiltrate Ukrainian and Western organizations [4]. Phishing attacks include social engineering techniques where a rouge entity, masquerading as a trusted entity, deceives the victim to open an email/document/text message and injects malicious content to steal the latter's data [5]. Meanwhile, spear-phishing campaigns are targeting a specific individual/organization, which makes them highly effective. It should be emphasized here that circa "90 percent of data breaches occur on account of phishing (according to the US Federal Bureau of Investigation – FBI)" [6]. Moreover, according to a myriad of sources with a strong foothold in the cybersecurity field, phishing attacks will likely continue to increase by over 400 percent on a year-by-year basis [6].

Case study 1 – Ukrainian employment agency

With the above, the first example illustrating the dangers that recruitment agencies face in the light of the ongoing conflict includes the attack orchestrated on January 29 2022. On this date, Gamaredon conducted a "spear-phishing attack pushing a malware downloader" to Ukrainian job search and employment service provider [7]. In layman terms Gamaredon sent a Trojan-infected Word document (job resume to be precise) which when opened connects back to a remote server and begins to install programs that are used to extract/block/delete content.

As the issue above did not gather significant attention, it continues to present a cyber-intelligence gap that many are overlooking. Specifically, recruitment agencies deal with significant amounts of personal data and this begs the question on their General Data Protection Regulation (GDPR) (& other such regulations in other jurisdictions) compliance, as well as their cybersecurity budgets.

Furthermore, desktop research revealed scarce information on the impact of this attack or how these agencies are tackling the aforementioned regulations, and there is a general sense that the impact or such data breaches is undermined in this specific sector. Moreover, when searching for "recruitment agencies and cybersecurity" there seems to be no online chatter on how these are protecting customer/client data and if there are any manuals and standards operating procedures (SOPs) relating to this. The issue is further escalated with a recent data breach in Serbia – where the targeted recruitment agency publicly dismissed any accountability for user data protection.

Case study 2 – Lako do Posla, Serbian employment platform

The idea that the attacks on recruitment agencies are becoming ubiquitous is corroborated with the September 3, 2022, attack on one of the largest Serbian employment agencies – Lako do Posla [8]. Unlike the case with the Ukrainian employment agencies, the precise origin of the attack is unknown. It can only be presumed that it was from Russia given geopolitical context but this speculation could not be validated or qualified due to the scarcity of information about the attack.

Given the lack of any context in the media, a deeper dive was performed to identify if the matter was picked up on general forums such as Reddit, as well as several proprietary hacking forums. What these searches revealed is that over 500 thousand account details were leaked and these included: "email addresses, full names, phone numbers, physical addresses, genders, nationalities and passwords stored as Bcrypt ($2a$08) hashes [9]." While the hashed passwords are not a significant cyber threat, the disclosure of personal details such as addresses and phone numbers presents a significant breach of privacy. Specifically, this information can be used for multiple purposes including corporate espionage (and mapping of one's commercial interests based on the types of roles they were looking for), and blackmail aimed at individuals who are currently employed but were looking for new challenges. However, none of these threats were caught up by the local media or cybersecurity professionals.

Analysis of the chatter picked up from Reddit does not provide any further information about the leak itself but points to a much more disturbing and illegal disclaimer on Lako do Posla's webpage [8]. Specifically, the company, in its disclaimer, claims that: "in using the service, the customer agrees that the provider is not responsible for any data loss, leak, or misuse, and former is responsible for inputting and storing the data on the latter's servers" [10]. This statement presents a potential breach of GDPR (the equivalent regulation in Serbia) and merits further investigation. Again, this was not picked up the media, cybersecurity experts, or the regulatory body - Commissioner for Information of Public Importance and Personal Data.

Conclusion

The underlining observation in the aforementioned case studies is that recruitment agencies are largely oblivious to the dangers that they are exposed to, and, perhaps because of lack of any cybersecurity budgets, are not implemented any security policies and controls. Moreover, as seen in the example of "Lako do Posla", some of these agencies have borderline illegal policies on how they deal with customer data. Hence, the following points are recommended for combating this:

- Raising awareness of risks and threat intelligence for these agencies
- GDPR (relevant local policies) compliance controls and audits

- Training offered to these agencies on different cybersecurity standards and policies – ISO and SOC Certification
- Confidentiality policies:
    a. Principles of least privilege
    b. Integrity policies
    c. Separation of duty
    d. Separation of functions
    e. Data classification
    f. Auditing
- Introducing separated local area networks (LAN) from critical networks and setting up virtual environments to manage external traffic i.e., emails with attachments

References:

[1] "Russia or Ukraine: Hacking Groups Take Sides." *The Record by Recorded Future*, 25 Feb. 2022, therecord.media/russia-or-ukraine-hacking-groups-take-sides/. Accessed 29 Sept. 2022.

[2] "Conti Leaks: Examining the Panama Papers of Ransomware | Trellix." *Www.trellix.com*, www.trellix.com/en-au/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html. Accessed 29 Sept. 2022.

[3] "Microsoft: Russian FSB Hackers Hitting Ukraine since October." *BleepingComputer*, www.bleepingcomputer.com/news/microsoft/microsoft-russian-fsb-hackers-hitting-ukraine-since-october/. Accessed 29 Sept. 2022.

[4] Avivit. "Russian Hackers Infiltrate Ukrainian Organizations via Spear-Phishing￼ | Centraleyes." *Centraleyes*, 10 Feb. 2022, www.centraleyes.com/russian-hackers-infiltrate-ukrainian-organizations-via-spear-phishing%EF%BF%BC/. Accessed 29 Sept. 2022.

[5] Imperva. "What Is Phishing | Attack Techniques & Scam Examples | Imperva." *Imperva*, 2019, www.imperva.com/learn/application-security/phishing-attack-scam/.

[6] L, Shira, and au. "Phishing Attack Statistics 2022." *CyberTalk*, 30 Mar. 2022, www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/.

[7] “Gamaredon (Primitive Bear) Russian APT Group Actively Targeting Ukraine.” *Unit42*, 3 Feb. 2022, unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/.

[8] kosmicki_sin. “! 500.000-1.400.000 Naloga Lakodoposla.com Dumpovano Na Internet (Imena I Prezimena, Mejlovi, Šifre (Ne Znam Da Li Su Plain Ili Hash), Adrese, Matični Brojevi..) > Promenite Šifre Svakako Asap, Sa Privatnošću Se Pozdravite, Jbg.” Reddit, 3 Sept. 2022, www.reddit.com/r/serbia/comments/x4rvhi/5000001400000_naloga_lakodoposlacom_dumpovano_na/. Accessed 29 Sept. 2022.

[9] https://breached.to/Thread-Lako-do-posla-Database-Leaked-Download

[10] “Politika Privatnosti.” *Www.lakodoposla.com*>, www.lakodoposla.com/politika_privatnosti. Accessed 29 Sept. 2022.