Faith-Based ISAO Weekly Cybersecurity Report **20 June 2019**

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

This report is **TLP AMBER**. Recipients may only share **TLP AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

FIND FB-ISAO ON SOCIAL MEDIA!

CYBER THREAT LEVEL

GUARDED

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as **"GUARDED."** As per FB-ISAO's definitions of the Cyber Threat Levels, **"GUARDED"** means FB-ISAO is unaware of any specific threats but a general risk of incidents exists.

This assessment has been developed by FB-ISAO and is our general, nationwide, threat assessment for the US community of faith. As always, for local threat information, members are encouraged to work closely with neighborhood partners, local law enforcement, state and local fusion centers, local FBI field offices, DHS Protective Security Advisors and other local experts and responders.

WHAT'S IN A PICTURE?

IN BRIEF: Social media sites serve many purposes – they can be used to share information with friends and family, to celebrate milestones, to be informed of the latest news, to coordinate activities, and connect with people around the world. The possibilities are endless within this space and growing more every day. However, as has been noted in previous reporting, these possibilities and platforms can also be used for nefarious purposes and by malicious actors. One such purpose was recently revealed in a new report from the Associated Press, in which "foreign intelligence operations routinely use LinkedIn to target, connect with, and eventually gain knowledge about and influence over American political affairs." And while targeting of those in politics or the government could be expected, these nation-states and other malicious actors are also interested in the dealings of organizations and businesses in various sectors. Faith-Based Organizations are just as likely to use social media platforms for outreach as well as making connections and therefore are just as susceptible to these approaches. Using an array of tactics, nation-states and malicious actors are generating fake profiles to engage potential targets from behind a desk as opposed to face to face, in public, and with a greater chance of being exposed. Recognizing the potential threats posed online, and the suspicious indicators of connection requests, can help organizations reduce the risk posed by the swarm of fake profiles that are looking to bypass security enhancements.

KEY TAKEAWAYS & RECOMMENDATIONS:

- Attackers are continuously looking for ways to circumvent organizational defenses;
- Developing fake profiles that can be used by attackers and nation-states to collect information about employees that can then be leveraged to facilitated more sophisticated attacks;
- Using social engineering schemes, attackers will approach targets through LinkedIn, Twitter, Facebook, and other social networks;

Approved for public posting as TLP WHITE by FB-ISAO on 25 June 2019

- Organizations in all industries around the world have seen evidence of these threats in their day-to-day operations and are encouraged to incorporate this threat into training and awareness programs;
- Additionally, reviewing and updating organizational policies and systems can be effective strategies to reduce the risk and minimize impact of such an attack.

DISCUSSION. Last year, there were several reports of "fake" LinkedIn profiles in which these profiles claimed to be an "HR Director". Further analysis revealed that these "profiles" didn't work with or for the reported member and that these profiles appeared to use stock photos. The targets of these "connections" appeared to be senior executives and other Human Resource department members. This is not an isolated incident. The establishment of fake profiles on LinkedIn and across the various social media platforms work in an effort to get a like, a friend, follow, or to open an attachment or click on a link. Over the past several years, **attackers have employed social engineering tactics and techniques against employees in an effort to gain a foothold into the organization to either collect information of value or to facilitate a larger attack**.

For Faith-Based Organizations the threat may not be as obvious, but there are still several reasons nation-states or malicious actors to use social media to target their organizations:

- Enable follow on attacks that may defraud an organization, such as a business email compromise attack;
- Gain access to an organization's sensitive financial information and charitable donations or tithes;
- Track missionary workers who may travel overseas where religious freedoms may not be allowed;
- Collect information about members and their activities in order to attack the member on other platforms or venues.

Last week, the AP reported that "foreign spies routinely use fake social media profiles to hone in on American targets" and the Director of the U.S. National Counterintelligence and Security Center has gone as far as to accuse China in particular of waging "mass scale" spying on LinkedIn. There have been several reports of fake LinkedIn profiles over the past several years and it is a tactic used by hackers and nation-state actors alike. Additionally, as noted in the AP news report, "British, French and German officials have all issued warnings over the past few years detailing how thousands of people had been contacted by foreign spies over LinkedIn." And in October 2017, a hacking group was able to breach Vero, the online music video site, as a direct result of a phishing attack through LinkedIn.

The latest report from the AP follows a **TLP GREEN** FBI Liaison Information Report (LIR 190401001) from April 2019 in which "the FBI's Washington Field Office, in coordination with the FBI's Office of Private Sector (OPS), informed private sector partners regarding foreign intelligence services' (FIS) "exploitation of social media platforms and data to target corporate and US government (USG) clearance holders. FIS and US adversary intelligence officers are using popular US-based social media platforms **to identify, recruit, and conduct operations against USG clearance holders, to include private sector employees or contractors supporting the USG**. FIS officers will use popular US-based platforms and their respective countries' social media platforms for personal and intelligence gathering/operations purposes." While the focus was on corporate and USG clearance holders, the methodology FIS use in these instances are similar across the board:

- A known FIS front company used a publicly available employment website (assessed to be LinkedIn) to target individuals who posted their resume online. The FIS used the website to target, assess, and recruit employees.
- A FIS created a fictitious social media profile on several platforms for the purposes of establishing online relationships/social network with a wide range of connections. The FIS used the social network to develop and assess a targeted pool of profiles.
- A FIS used physical events and online research for social media usage to establish relationships. A FIS who operated a vendor booth at the conference approached a contractor several times and offered sales of

products/services. A week after the conference, the FIS located the contractor on a popular professional linking website. The FIS sent an online request to the contractor via the website.

These threats reveal two primary inherent challenges that make LinkedIn specifically, and other social media sites to a lesser degree, an ideal platform for attackers. The first is in the **implied trust** of the site and that all users online are perceived to be legitimate. It is a common ploy by users of LinkedIn to send out blanket "connection" requests to anyone in their field or within a field they are interested in order to build out their network. This tactic and the legitimacy given to the site makes individuals more likely to accept connection requests from unknown individuals. The second reason these sites are ideal for attackers is because LinkedIn and some other social media sites can **circumvent network filters;** whereas some software programs employed by organizations typically prevent access to some sites, LinkedIn sometimes gets a pass. The thought is that LinkedIn allows "employees to engage in online networking, chat or blog about the company in a professional environment, and for the HR department to use LinkedIn's online job services to find new employees." It is deemed as less threatening and often allowed by most companies. Even so, while most companies do block social media sites on their networks, not all do, thus exposing the organization to the above risks.

These attacks follow a relatively simple formula – some of which was noted above in the FBI LIR:

1. **Create a fictitious profile.** The bio is fabricated, and the photos are typically stolen from other profiles, from various photos online, or as the AP reported, computer generated. Attackers spend additional time cultivating their profiles in order to ensure they have connections that may be similar to their targets. The goal is simply to be enticing enough for the target to want to know more and to lower their suspicion of a potential threat. The attacker **can create thousands of profiles all at a tremendous cost savings** as compared to building out a targeting package, and engaging a target in a physical realm. If a fake profile doesn't take, then it can be thrown away for little cost. If an intelligence officer fails in a meeting with a potential target, that officer may be exposed.
2. Once the profile is created, **the attacker will then send out numerous requests to connect with potential targets**. For LinkedIn requests, this may come in the form of a message requesting to connect, potential job opportunities, questions about a job opening, or similar interests. This request serves as an entry into more detailed discussions through email, or on another social media platform. Similar requests could come across in a message through Facebook, Twitter, or Instagram, amongst others.
3. Once a dialogue has been initiated, the attacker can pursue two main objectives to exploit the relationship:
    a. At any point, s/he can **add a malicious link or attachment** that contains a malicious payload. In the instance of the suspected Iranian-sponsored Mia Ash attacks from 2017, after cultivating a relationship with a target over a period of time, the person behind the keyboard would ultimately send the target a link that leads to an Excel or Word document that will enable a Trojan, which will then infect the target's device. In another popular scheme, attackers may respond to a job request from an organization and include their resume, which is loaded with malicious content. Once the recruiter opens the document, the malware begins to do its damage.
    b. **General Collection.** Once a user approves a connection, the accepted individual (attacker) now has access to the target's full profile, which enables the attacker to collect a wide variety of information: a valid email address, previous experiences, training taken, special interests, and other areas that can help an attacker build a separate spear-phishing attack to be employed at another time. And because the attacker will have a lot of personal information about the target, s/he can tailor the attack to increase the likelihood of success. This is what makes social engineering so successful; an attacker is able to collect information that can then be used to established legitimacy in another attack.

MITIGATION. Employees and organizations at large are not helpless in these instances, but they do have to remain vigilant. Some key areas to review when evaluating a request contain many of the areas that individuals and organizations should review when evaluating potential phishing attacks.

- **What is the Profile Picture?** Some attackers use profiles with good-looking, model-quality photos, a lesser-known actor or actress, or even an image of a well-known public figure. Some attackers won't even put a photo in or will use a blurry image. Attackers may also use the same picture for multiple profiles.
- **Evaluate Work History.** One common signifier of fake LinkedIn accounts is the lack of any real information about the individual; attackers may keep their "profiles" with minimum information and use generic statements and job titles.
- **Limited Connections (often under 100).**
- **Fake Name / Poor Spelling & Grammar.**
- **Evaluate Activity / Lack of Engagement.** Accounts that are not engaging with others or feature very little in the way of updates and content may be phony. Another common sign of a fake account is one that doesn't tend to have anyone following the account.
- **Pitches for Great Business Opportunities or Jobs.** In some instances, these pitches come with a link to apply through, or with a Word document that gives a full job description. These may as well be invitations to download malware. It is recommended that individuals validate the information contained in the message against information on the website of the organization the "recruiter" claims to represent. Also, similar to phishing vigilance, hovering over the link may give an indication if the URL is legitimate or not.
- **Do Not Enable Macros.** You should never download PDF, Word, or Excel files attached to unsolicited emails to begin with. If you do open one of these documents and it says that you need to turn on macros, close the file and delete it immediately.
- **Do Not Chase Connections / Followers.** While it is a challenge, especially when legitimacy is implied by the number of followers an individual has, individuals need to be sure that those they do follow or connect with are real.

From an organizational perspective, there are some additional processes that can help reduce the risk:

- Incorporate this type of threat into regular threat training / updates to all employees;
- Implement security policies and governance that focus on how people interact with data, correspond with email, and use tools like LinkedIn and other platforms;
- Consider establishing written policies that restrict or forbid the use of personal social media accounts for professional work;
- HR personnel or recruiters can be issued organizational LinkedIn accounts to support their recruiting efforts;
- Companies can also onboard temporary or part-time recruiters in the same way they welcome full-time employees, by setting up corporate email and social media accounts for them;
- Put script-blocking and macro-based protections in place. Exploit prevention is also important.

As a general reminder – just because you get a "friend" or "connection" request does not mean that you have to accept it. Do you know the person? Do you know the organization they belong to? Is there value to having the connection? These are some general questions individuals can ask before agreeing to the connection.

How much information is on social media?

In light of recent events with Cambridge Analytica, Panda Security recently evaluated how much information a person can reveal on social media platforms. Panda Security notes that while many users "think they are harmlessly adding information to their profiles, this information can be used for targeted ads, sold to marketers, or worse, sold into the black market. Facebook has even admitted to using 98 different data points to target advertisements." Some of the key points included:

- 51% of users share their family members, which can provide more targets for attackers;
- 25% of users tag their location every month;
- 26% of users share their vacation plans;
- 56% of millennials will share their location to receive a coupon.

The article also contains the amount of general and technical information that attackers could collect through these social media profiles, which could be used by attackers. This information helps attackers develop more sophisticated attacks against those targets or those associated with the target.