Danger of the lazarus group

Business, Company

With technology becoming more integrated into the everyday lives of individuals as well as society as a whole, there is a continued duty to understand the associated dangers of increasing technological use. The Lazarus Group may not be a familiar name to most citizens, but it has caught the attention of corporations, banks and governments. With their increasing operational presence in the cyber world, the average individual should also be informed of the Lazarus Group's capabilities and their reputation as one of the most threatening hacking groups operating in the world. The Lazarus Group's calculated attacks may include any or all of the following elements: a specific type of attack, an explicit target, as well as an identified outcome. The goals associated with these attacks and their growing trends should be known by all members of society in order to stay informed and keep one step ahead of becoming a victim.

Increasingly, the attack methods of the Lazarus Group have changed, becoming more sophisticated over the years. Their initial attacks beginning in 2009, were simpler DDoS style targeting against the South Korean government (" A look…). Since then, they have grown their notoriety by increasing both their number of attacks, as well as the technological skills necessary to successfully complete their intended cyber assaults. For example, the 2014 Sony hack, resulted in the publication of Sony's confidential information including private emails by top executives. This security breach was the result of a Lazarus Group malware attack (" A look…). In 2016, the Lazarus Group focused their sights on the Bangladeshi Central Bank and the bank soon became one of a number of financial institutions infiltrated by the Lazarus Group's hijacking of the bank's SWIFT

network messaging system. This particular attack resulted in the theft of millions of dollars (“ North Korea’s). More recently, the Lazarus Group has diversified their tech assaults to the stealing of crypto currencies and the spreading of WannaCry ransomware as their preferred forms of attack. Typically, Bitcoin theft involves the unlocking of the owner’s virtual wallet to gain access to their Bitcoin. Hackers can then move the seized funds to their own wallet (Mak). Recently in February 2018, McAfee, a computer security company, published research attributing the Lazarus Group to using “ never before seen tactics” in order to steal bitcoin. The latest strategy by the Lazarus Group has been to pose as recruiters for a bank’s administrative position in Hong Kong. The Group then generates “ mass spear phishing” email advertising a fake job with an attached dropbox link containing a false document. The false document contains a “ malicious implant that recipients would be tricked into enabling through a false notification, which states that the file was created in a previous version of Microsoft Word” (Mak). Once the document had been downloaded the document implant could then scan the contents of the computer for any cryptocurrency wallets containing a user’s bitcoins so that they may be easily identifiable for future attacks. This new form of stealing cryptocurrency has been given the operational name HaoBao. These encrypted types of Word documents have been sent to many companies in an attempt to successfully infiltrate a unsuspecting businesses (Mak). Although this type of attack has been used before, McAfee has said the HaoBao operation is a more specific and sophisticated, thus enabling the attacker to leave a smaller digital footprint making it less likely to be noticed. This strategy has focused the tech attack specifically on bitcoin users to gain

access to the contents of their virtual wallets. In reviewing the historical attacks by the Lazarus Group, it is likely we will continue to see a sophisticated progression in how the group continues to attacks its targets.

In addition to the increasing variety and sophistication of the Lazarus Group attacks, the Group has also varied their targets over the years. Since their first attack in 2009, they have expanded their ‘ list’ to include media groups, manufacturing organizations, and financial institutions (“ A Look…). However, not all attacks have the same goal or outcome. The aims of their attacks are as varied as their target list and techniques, and consist of disruption, sabotage, financial theft or espionage. An additional reason for the changing nature of the Group’s attacks is ultimately the attack depends on which group within the Lazarus organization is attacking and whom they are targeting. The Lazarus Group is comprised of subgroups that concentrate on a specific area of interest. For example, Bluenoroff focuses on foreign financial gains, and Andariel focuses on specific South Korean businesses and organizations (“ A Look…). According to TrendMicro, both subgroups’ methods of attack usually included disruption and misdirection, as well as extremely robust anti-forensic techniques used to make the job of law enforcement agencies more challenging (“ A Look…). However, the targeting of cryptocurrency remains the focus of the central Lazarus Group because of the poor regulations and the difficulty in enforcing sanctions on cryptocurrency vs. solid currency (Palmer). The Lazarus Group’s attacks in this area have also allowed for long-term access to their targets. HaoBao, a name given to type of malware used by the Lazarus group, allows the victim to be vulnerable to future attacks by allowing a backdoor for Lazarus group

hackers to periodically exploit, “ Information about the computer name, logged in username, and all the processes running on the system is sent to the attackers” (Palmer). The ongoing beneficial outcomes to the Lazarus group, by using such malware is incalculable if undetected.

Solid arguments have been made linking the Lazarus Group attacks to North Korea. Thus, the Lazarus Group is now regarded as a nation state backed hacking group with legitimate ties to North Korea. The US government publicly blamed North Korea for the WannaCry ransom ware attacks responsible for significant theft in cryptocurrency in 2017 (Cuthbertson). Additionally, the Cyber Warfare Research Center in South Korea has suggested the Lazarus Group could be targeting virtual currency as a result of the economic sanctions imposed on North Korea (Cuthbertson). It is also worth noting that 15 to 25 percent of world bitcoin exchanges come from South Korea, making South Korea a prime target for stealing cryptocurrency as an act of retaliation in response to the tension between the two nations (Cuthbertson). Patrick Wheeler, Director of Threat Intelligence at the security firm Proofpoint explains, “ State Sponsored groups are generally focused on espionage and disruption” (Cuthbertson).

While not all of the Lazarus Group’s have been focused on espionage and disruption, enough of their attacks can be certainly classified as having the characteristics of those types of attacks. The latest tech assaults reported by McAfee on South Korea, describe another change by the Lazarus Group. The Group is now shifting from highly focused attacks to broader attacks using mobile malware. Their strategy is to target Android smartphone and tablet

users in South Korea by appearing to be an app that can translate the bible into Korean. The file is called an APK file and has the ability to install a backdoor on the phone/tablet when it is downloaded. After the malware was analyzed, experts concluded the existence of strong similarities between itself and previous malware used by the Lazarus Group (North Korea's). The similarities of both attacks were too close to have come from a different party. This is new territory for the Lazarus Group, as attempting to hack phones, tablets and other mobile devices has not been in accordance with their previous plans of attack. Though with more South Koreans using smartphones and 79% of them being Android, it is likely that increased attacks will be made on mobile android devices in South Korea (North Korea's). Once the downloaded malware communicates with a command and control servers, locations of which are in the US, India, South Korea, Argentina, and Nigeria, the malware can then collect and transfer data back to their control server where it awaits further instruction from the hackers. This backdoor operation allows hackers to upload, download or browse files within the device it inhabits (North Korea's). The seemingly consistent barrage of attacks on both the South Korean people and government strengthens the connection between North Korea and the Lazarus Group working as a backed nation state hacking organization.

The variety of targets and aims, as well as their continuing sophistication of attack makes the Lazarus Group a strong cyber adversary. At this time the number of individuals involved and the extent of their ' footprint on the digital world' is not known (Cuthbertson). However, with the increasing

number of attacks and additional subgroups within the Lazarus Group, we can assume that many people are needed to run the organization.

Additionally, the Lazarus Group doesn’t seem to claim responsibility for its attacks, which means they prefer anonymity and conform to some of the stereotypes associated in the hacker subculture. Their level of technology surpasses most hacker groups and their knowledge about their targets appears superior to newcomers or others in the hacking industry. While their attacks can include elements of self-gain, such as stealing money, they can also be viewed as striking fear into a society through intimidation and potential threats. In conclusion, the Lazarus Group is a danger to both individual citizens as well as organizations and nations as their attacks can be considered both crimes and acts of terror.