19 March 2021

An Analytic Intelligence Wire Prepared by The Students of Embry-Riddle Aeronautical University

Issue 377
Of Eagle Eye Intelligence

Authors

Patrick Komanowski
Emily Lewis
Savannah Grace Riddles
August Kather
Amalie Hansen
Megan Pfaff

Source: Reuters

Day Month Year

Issue 377
Of Eagle Eye Intelligence

In This Issue

NORTH KOREA: Persistence of Increased Cyberattacks Likely to Fund Nuclear Program

Summary: The Democratic People's Republic of Korea (DPRK) sponsored and conducted a series of unprecedented cyberattacks through the efforts of various Advanced Persistent Threat (APT) groups. The DPRK-sponsored cyberattacks will almost certainly continue and will likely escalate, reinforced by the successes demonstrated in previous attacks. Pyongyang will probably sustain offensive asymmetric attacks to generate revenue to fund its nuclear and ballistic missile programs and to grow hard power, demonstrating national security objectives.

Background: Since 2014, many DPRK cyber actors have operated under the Reconnaissance General Bureau (RGB) in the form of APT groups. These actors, consisting of hackers, cryptologists, and software developers, deploy a wide range of sophisticated malware tools and often operate remotely from North Korea, China, or Russia. Pyongyang actively sponsors cyber-enabled theft which targets financial institutions and digital currency exchanges and politically motivated operations against other foreign entities. North Korean cyberattacks have exhibited significant success in disrupting the integrity and stability of the international financial system. In utilizing APT groups to conduct attacks, North Korea obtains power through asymmetric means of influencing and damaging adversaries. According to the United Nations (UN), North Korean hackers prioritize financial targets to fund the country's flailing economy and subsidize Supreme Leader of North Korea Kim Jong Un's nuclear and ballistic missile program objectives.

Success of Cyberattacks: Pyongyang will almost certainly continue to support cyberattacks through the RGB because of the success garnered by its previous intrusions. In November 2014, DPRK-sponsored cyberattacks compromised the Sony Pictures Entertainment network; they deployed destructive malware and stole proprietary information as well as confidential employee communications. In February 2016, DPRK-sponsored actors allegedly stole $81 million from the Bangladesh Bank via the Federal Reserve Bank of New York. Additional cyber-enabled bank heists occurred through 2019 in Vietnam, Taiwan, Mexico, Malta, and Africa. In May 2017, the DPRK-sponsored ransomware known as WannaCry 2.0 infected hundreds of thousands of computers in over 150 countries, extorting victims for ransom payments in the form of Bitcoin. Since April 2018, DPRK-sponsored actors actively target and hack into digital currency exchanges, stealing approximately $250 million of cryptocurrency to date. North Korea probably finds the consequences of target nations attributing attacks to it inconsequential when compared with the revenue and hard power generated through these successful operations.

Asymmetric Advantage: The DPRK will likely continue to conduct its frequent asymmetric attacks on Western adversaries as its primary means to obtain power. North Korea utilizes asymmetric cyberattacks as a strategic equalizer, empowering Pyongyang to compete against more powerful opponents. DPRK-sponsored APT groups will likely continue to gather global intelligence and conduct offensive cyber operations because more powerful nations struggle to attribute and respond to the asymmetric capabilities of such actors. Examples of such groups include: Kimsuky, Lazarus Group, APT37 (Reaper), the BeagleBoyz, and many more. Since

2012, the Kimsuky APT group has engaged in social engineering, spear phishing, and honeypot tactics to elicit information from victims. The Lazarus Group APT pursue individual and corporate victims, focusing on cryptocurrency exchanges, through the dissemination of cryptocurrency trading applications altered to include malware. APT37, codenamed Reaper, conducts intelligence-gathering operations in support of North Korean strategic objectives and economic interest using zero-day vulnerabilities and wiper malware, according to FireEye. The success of asymmetric attacks may arise as a fundamental tool in the foreign policy and conduct of North Korea within the global scene.

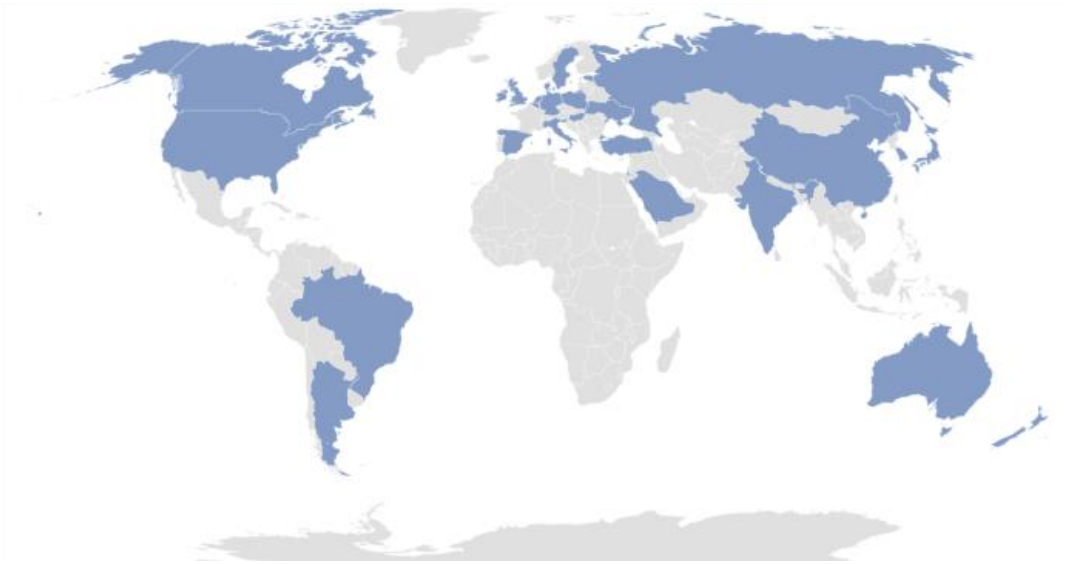

Figure 1: Countries targeted with AppleJesus Malware by North Korean APT actors since 2020.

Lack of Nuclear Funding: Pyongyang will likely continue conducting international criminal cyber operations to boost its battered economy and finance nuclear and missile program objectives. The global recession amid the COVID-19 pandemic damaged North Korea's economy, as demonstrated by its efforts to develop new national economic plans. In the first half of 2020, North Korean trade with China plummeted by 67% due to COVID-19 restrictions and border closures. North Korea's decreasing trade and revenues prohibit it from focusing on key national security objectives like increasing funding for its nuclear program. North Korea, as a result, intends to find alternative means to raise national funds and have found success through cyberattacks. Support for North Korea's nuclear and ballistic missile programs seems to come from the illegally acquired foreign currencies attained through cyber-enabled attacks. The North Korean nuclear program provides Pyongyang a substantial source of hard power as it permits the government to impose its will on other nations in the international community. Therefore, the DPRK will likely prioritize a much larger variety of methods to increase revenue likes conducting more brazen asymmetric attacks to cultivate the hard power it needs to sustain key national objectives.

Outlook and Implications: With the success demonstrated by its effective cyber intrusions, Pyongyang will likely look to the cyber domain as its primary means of generating wealth and harming Western nations. Kim Jong Un's goal to have superior nuclear programs and ballistic missiles seems ambitious, but the DPRK may have a reliable source of revenue to fund such programs through cyberattacks on financial institutions. The DPRK will certainly continue its aggressive policies and operations within the cyber domain despite the potential attribution and responses that result. North Korea will likely grow more enticed to conduct cyberattacks against foreign powers as a means to develop power and prove its staunch national security policies.

The DPRK likely utilizes strategic, asymmetric APT groups to strike its adversaries, as these groups can conduct remote attacks from outside of North Korea in neighboring Russia and China. Kim likely benefits from the use of these asymmetric attacks as they conceal the origin and motive for attacking. The DPRK may look to conduct additional asymmetric attacks through technological social, subversive, or political attacks, using espionage and sedition sponsorship. It appears that North Korea views recouping the power and funding of its economically constricted nuclear and ballistic missile program as its primary objective for conducting aggressive cyberattacks against Western nations. Pyongyang likely believes that acquiring more nuclear power will stave off international intervention. To gain nuclear power and thus cultivate hard power, Pyongyang will likely continue its efforts to raise funding by any means necessary, but with a focus on its profitable and effective asymmetric cyberattacks.

[Patrick Komanowski]

IRAN: Strengthened Military Capabilities Likely Preparing for More Aggressive Stance

Summary: Over the last several months, Tehran continued increasing its conventional military capabilities and unconventional warfare activities. Tehran's growth in military capabilities and increased proxy-initiated attacks likely indicate it intends to respond more aggressively to growing tensions in the region. The rapid advancement in military capabilities almost certainly poses a more significant threat to the region as Tehran becomes a more competitive adversary.

Background: Tehran continues to advance military capability while simultaneously increasing unconventional warfare in the Middle East. Tehran relies primarily on deterrence as its military strategy, however it increased drone use to attack adversaries more frequently. Tehran supplied Houthi forces in Yemen with the Ababil-3 drone, which it used in the September 2019 attacks against Saudi Arabia. Tehran continues to grow its arsenal of ballistic missiles after revealing the IRGC Naval missile facilities in January.

Strengthening Defense Capability: Tehran continues to broaden its conventional military capabilities, probably to increase its retaliatory attack options. For years, Iran relied on asymmetrical warfare, but growth in advanced military equipment and capabilities allows for symmetrical response options. In February 2021 Tehran released the Kaman-22 drone, the latest reconnaissance combat drone with similar capabilities to the MQ-4C drone. Iranian drone capabilities focus on surveillance, intelligence, and reconnaissance. In the last year, Tehran increased its number of long-range missiles and showed its underground missile base on the Gulf. The storage of ballistic missiles off the coast allows for easy access for the Iranian Navy. Tehran will likely focus on producing increasingly capable missiles, drones, and naval weapons to meet operational requirements.

IRGC Missile base. Image obtained from MSN News

Increase in Proxy attacks: Tehran will likely maintain influence in the region and test new equipment through a growing number of Iranian-backed militia attacks in Iraq and Yemen. On 6 March, Iranian-backed Houthi forces fired drones and missiles at the Saudi Aramco facility. Iranian proxies continue targeting Saudi Arabia. Increasing attacks against Saudi Arabia from Yemen and Iraq continue, accompanied by a barrage of rocket attacks on Iraq's allied interests. Tehran likely will continue escalating tensions through its proxies while mobilizing more advanced military equipment.

Outlook and Implications: Tehran will likely continue to strengthen its military to respond forcefully to threats in the region and utilize its defense capabilities to deter direct conflict. Considering the rapid escalation in attacks, Tehran will likely continue using unconventional warfare while strengthening military equipment in preparation for more extensive scaled operations. Acquiring advanced equipment makes Tehran more competitive amongst regional adversaries. Tehran's growth in tactical ability will likely increase the regional threat as it will likely become more willing to retaliate aggressively.

Iran will likely continue to utilize the proxy groups as a strategic advantage, and retaliatory attacks will likely become more frequent as tensions continue to grow. Tehran will likely use the new military resources to equip the militias with more advanced military equipment, advancing its goals of regional influence. Tehran displays a steady increase in frequency and forcefulness of its attacks and will probably try to establish a more aggressive stance in the region.

[Emily Lewis]

CHINA: Olympics Vaccination Plan Likely to Cause Increased Tensions With Japan

Summary: The International Olympics Committee's announcement that China will provide COVID-19 vaccines for athletes will likely increase tensions between China and Japan while alienating nations that have yet to approve Chinese vaccines.

Development: On 12 March, the Chinese Olympic Committee (COC) announced that they allocated COVID-19 vaccine doses for athletes participating in the Beijing 2022 games. The IOC will pay for the athletes' doses and two additional vaccines per athlete for members of the general public in their home country. Japan's Olympic Minister, Tamayo Marukawa, announced that Japan's Olympic athletes will not receive the doses because Japan has yet to approve a Chinese COVID-19 vaccine for public use. No Chinese companies applied for regulatory approval in Japan, which only began vaccination campaigns in February. The IOC announcement came in the wake of controversy surrounding the upcoming Beijing games due to claims of Uighur genocide in China.

Analysis: The COC probably made the decision to provide Chinese COVID-19 vaccines for the Olympics to promote attendance in 2022 and detract from the controversy regarding the Beijing games. Tensions between China and Japan will likely rise since the COC's announcement publicly highlighted Japan's lagging vaccine rollout. Japan may move to enter agreements with Chinese companies and encourage them to apply for authorization in Japan before the games commence, hurrying a typically lengthy process. Additionally, other participating nations will probably prioritize the approval of Chinese vaccines if they have not already.

[Savannah Grace Riddles]

EGYPT: Meeting With Sudanese Officials Likely Indicates Further Cooperation

Summary: A meeting between the Egyptian President and Sudanese officials will likely further cooperation between the two nations over the issue of the Grand Ethiopian Renaissance Dam (GERD).

Development: On 6 March, Egyptian President Abdel Fattah el-Sisi visited Sudan and met with Prime Minister Abdalla Hamdok and General Abdel Fattah al-Burhan, head of the ruling Sovereign Council. El-Sisi discussed with Sudanese officials an array of issues, including developing close economic and military ties and the two nations' dispute with Ethiopia over the GERD, located on the Blue Nile. El-Sisi stated that Cairo and Khartoum agreed on the importance of relaunching "serious and effective" negotiations that aim at achieving a "fair, balanced, and legally binding" agreement on the dam's filling and operation before the next rainy season. Khartoum fears the GERD, which lies close to the border with Sudan, could increase the risk of flooding and affect the safe operation of its own Nile dams, while Cairo fears the water scarcity that will come with a fully operational GERD. In a statement released after the meeting, El-Sisi indicated Cairo's support for Khartoum in its border dispute with Addis Ababa in the Al-Fashqa region.

Analysis: El-Sisi's trip to Sudan almost certainly signifies that Cairo considers Khartoum a valuable ally against Addis Ababa and the GERD. Cairo's support for Khartoum's border dispute with Addis Ababa in the Al-Fashqa region likely indicates that Cairo wants Khartoum to take a more active role in combating Ethiopian regional expansion. The possibility of Cairo increasing its military and economic ties to Khartoum will likely cause Addis Ababa to suspect Egyptian-backed involvement in the border dispute. The agreement of possibly relaunching negotiations with Addis Ababa likely means that Cairo continues considering its options for dealing with the GERD. Without an agreement regarding the GERD, regional conflict will likely escalate.

[August Kather]

RUSSIA: Inside Actor Possibly Behind Hacker Forum Data Breach

Summary: The complexity of the recent hack on a Russian hacker forum indicates that an insider could hold responsibility, possibly allowing law enforcement to uncover the true identities of 3,000 of its members.

Development: On 2 March, an unknown actor hacked the popular hacker forum known as Maza and set the data for sale on the dark web. Maza has become known as a popular forum where the world's most sophisticated cybercriminals and financial fraudsters share tips on how to improve their cyber-crimes. The stolen data includes user IDs, email addresses, hashed passwords, and ICQ numbers, according to Flashpoint vice president Thomas Hofmann. When signing in, the members of the forum found themselves redirected to a breach notification page containing a warning left behind from the hacker reading: "Your data has been leaked. This forum has been hacked," in badly translated Russian.

Analysis: An inside actor seems most likely to have the knowledge of the site's security measures and vulnerabilities. The posted warning message also indicates an inside actor, as law enforcement almost certainly would not have notified members of the breach. The actor likely understood that exposing the breach would scare members into going underground. The data gathered in the breach would certainly help law enforcement uncover the identifies of thousands of members within the group.

[Amalie Hansen]

SAUDI ARABIA: Agreement with Germany Likely to Garner Investment for Vision 2030

Summary: Riyadh's emergence as a potential producer for green hydrogen energy will probably create a flow of investment into the Vision 2030 plan.

Development: On 11 March, Saudi Minister of Energy Prince Abdul-Aziz Bin Salman and German Minister for Economic Affairs and Energy Peter Altmaier signed a memorandum of understanding establishing Berlin's willingness to purchase Saudi-produced hydrogen. This deal establishes a market in Europe for Riyadh to sell green hydrogen, making the massive upfront cost of building the facilities to produce green hydrogen economically viable. Green hydrogen, or hydrogen produced using renewable energy sources, has become especially attractive as a fuel, according to the Wall Street Journal. Abdul-Aziz stated that the innovation of green hydrogen constitutes the next step in diversifying the Saudi economy and committing to the Paris Climate Agreement as well as the Saudi Vision 2030 plan for renewable energy.

Analysis: Riyadh's emergence as a green hydrogen producer and Berlin's willingness to purchase Saudi hydrogen fuel will likely increase investment into green hydrogen as an alternative fuel source. With a market for green hydrogen tentatively secured, Riyadh will most likely move forward with production, fulfilling the Vision 2030 plan for sustainable energy and economic diversification.

[Megan Pfaff]

About GSIS

Embry-Riddle Aeronautical University's (ERAU) Bachelor of Science in Global Security & Intelligence Studies (GSIS) degree program at our Prescott Campus blends both academic and professional studies to equip students with the knowledge and skills necessary to become future leaders in intelligence, security, and law enforcement. The program provides students with a sound foundation in the liberal arts, including international relations, foreign languages and cultures, international law, foreign policy, political and military history, and other essential topics.

About EE

Eagle Eye Intelligence (EE) is an intelligence and research organization led by the students of the GSIS program at ERAU in Prescott, Arizona.

Dr. Philip E. Jones founded EE and Embry-Riddle's GSIS program in 2002, following a career with the Central Intelligence Agency and consulting work in international development and global security. Currently, Professor Dale R. Avery, a former career intelligence analyst at the Central Intelligence Agency and Office of the Director of National Intelligence, serves as EE's faculty advisor.

EE strives to provide actionable intelligence and analysis to its customers during the academic year. We are driven by a number of goals – continuous development, nonpartisanship, interdisciplinary studies, global awareness, and professionalism.

EE does not cite sources in the final publication; however, we log every source we use in our research and are happy to share them upon request. The official EE Source Database is available on our website's resources page for a general overview of our sourcing methods.

The views expressed in this publication are those of the authors, and do not represent the position Embry-Riddle Aeronautical University or the College of Security and Intelligence.

Alli McIntyre, a junior in the GSIS program, currently serves as EE's Editor in Chief. For questions or comments, contact the team at editorsee@gmail.com or Professor Avery at 928.777.4708.

© 2020 by Eagle Eye Intelligence. All rights reserved.

Eagle Eye Intelligence
3700 Willow Creek Rd.
Prescott, AZ 86301
eagleeyeintel.com