Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

State-Sanctioned Hacking Groups: An Overview

April 2022

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

State-Sanctioned Hacking Groups: An Overview

Introduction

While many foreign nation-states militaries and intelligence services engage in malicious cyber activities, state-sanctioned hacking groups also pose a significant threat. While official state entities (often known as advanced persistent threat groups, or APTs) are capable of engaging in complex cyberattacks, state-sanctioned hacking groups often engage in lower-level activities such as cybercrime and cyber harassment. Still, these groups are capable of causing financial harm, disruption of systems and networks, and other negative effects.

For the purposes of this paper "state-sanctioned hacking groups" will refer to groups engaged in malicious cyber activity, who are not officially part of a foreign nation-state government, yet are given "safe haven" to engage in activities that are likely tacitly approved by their host government. This includes groups who may receive covert funding/guidance. For example, this may include a group based in Russia which targets the U.S. and other Western nations, without explicit direction from the Russian government. Still, the Russian government may allow this group to operate within Russia's borders, since its targets are in line with Russia's geopolitical objectives.

Background

There are numerous types of groups that may engage in hacking. These groups include hacktivists, individuals seeking to leverage cyberattacks into political change. Cybercriminals commit cyberattacks for personal profit. Terrorists aiming to destroy, incapacitate, or exploit critical infrastructures may also use hacking. Insider threats may exploit their access in executing cyberattacks. It should be noted these group differ from Advanced Persistent Threat (APT) Groups. These groups utilize sophisticated techniques targeting high-value organizations.[1]

All of these groups may utilize a variety of attack methods in attempts to hack others - ransomware, phishing, and malware to name a few. Per the DNI, "business-e-mail compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes" in 2020.[2] Potential targets include private business, public utilities, critical infrastructure, journalists, public figures, government, and defense institutions.

While state-sanctioned hacking groups themselves may not be an official part of foreign nation-state governments, such groups can easily serve the political objectives of U.S. adversaries. The "big 4" adversaries of China, Russia, Iran, and North Korea have used and will continue to use state-sanctioned hacking groups for political benefits. Use of these groups has numerous benefits. Like cyberattacks coming from the state itself, benefits of the attack, to include information gathering, disruption of infrastructure, monetary benefits, etc., will be seen. Unlike cyberattacks coming from the state itself, state-sanctioned hacking groups can achieve similar types of geopolitical benefits for the state, while providing a certain amount of deniability to the state in their involvement in the cyberattack. The level of cooperation between state and state-sanctioned hacking groups is inherently unclear. While they may have similar geopolitical aims, the level of

support and direction given by the state can vary significantly and be difficult to quantify without direct insight and intelligence into the relationship.[3,4,5]

Case Study: DarkSide

The transnational cybercriminal hacking group known as "DarkSide" is a "ransomware-as-service" (RaaS) group, meaning that the developers of DarkSide receive a share of the proceeds from cybercriminal affiliates that deploy cyberattacks. This hacking group is a ransomware variant which implements a dynamic-link library program. This program is used to delete Volume Shadow copies available on the system. DarkSide further requires the victim to de-crypt their data in their systems and incentivize a payment to keep their data from being released on the dark web. Reports have indicated that individual RaaS operators such as DarkSide take approximately 25 percent for ransom fees less than $500,000. However, this number decreases to ten (10) percent for ransom fees that exceed $5 million. In 2021, DarkSide terminated its operations after the servers used for its operations were seized, and an unknown individual washed out the cryptocurrency from the account Darkside utilized in order to pay its affiliates. Cybercriminal organizations such as DarkSide have the potential to draw a strong response from the United States with their RaaS attempts. Reports indicate this potential for a strong response from the United States likely contributed to the conclusion of DarkSide operations. According to the U.S. Department of State, "the DarkSide ransomware variant appeared initially in August 2020 and was used to rapidly launch a global ransomware campaign in more than 15 countries that targeted multiple industry sectors, including financial services, legal services, manufacturing, professional services, retail, and technology". Since the DarkSide account was opened in March 2021, the group is reported to have received $17.5 million from 21 Bitcoin wallets.[6,7,8,9,10]

On 07 May 2021, the Colonial Pipeline Company became a victim of DarkSide's RaaS operations. In turn, this led to the company's decision to temporarily shut down the 5,500-mile pipeline which carries 45 percent of the fuel used on the East Coast of the United States. With the Colonial Pipeline Company supplying almost 50 percent of the East Coast's jet fuel and gasoline, both air and land travel vehicles along with their consumers that depend on the Colonial Pipeline, were negatively impacted as consumers of the company's gas supply sought to immediately purchase as a potential price surge in oil due to gas shortages became imminent because of Darkside's RaaS attack. The pipeline shut down for five (5) days until the ransom was paid, and some states experienced surges in gas prices due to a shortage in oil supply. The Colonial Pipeline Company acknowledged on 19 May 2021 that it wound up paying $4.4 million worth of bitcoin to DarkSide after the group's successful RaaS attack on the company's pipeline.[11]

According to open source reports, Moscow's intelligence services have influence over Russian criminal ransomware groups and possess a broad insight into their activities; however, they do not control the organization's targets. U.S. government officials have assessed that the Russian government allows for cybercriminals and their distinct groups to operate as long as they do not interfere with the Kremlin's own operations. Cybercriminal groups may potentially be given protection by the Russian government in return for cyber expertise that may potentially benefit Russia's ability to effectively utilize cyber technology on a more global scale. Cyber experts have noted that the RaaS network is based in Russia as federal security in the federation may permit and employ cybercriminals and groups such as DarkSide. However, U.S. officials have reported that

there is currently no evidence that the ransomware software used by DarkSide to temporarily shut down the Colonial Pipeline (an important critical infrastructure asset that supports the U.S. economy in addition to transportation and energy services) was used by the Russian government.[11,12]

Case Study: REvil

REvil, also known as Sodinokibi, was a ransomware group that also used a RaaS model that would share profits with affiliates for distributing its code. Affiliates were reportedly promised 70% for carrying out attacks. The group operated out of Russia or elsewhere in Eastern Europe. Like many groups in the region, it conspicuously avoided Russian targets. Many affiliates would later assert that REvil used a backdoor to hijack chats with victims to intercept their payments.[13] REvil or its affiliates would extradite sensitive, proprietary, or compromising data and threaten to publish it if the target declined to pay. The group targeted multiple sectors, including information technology, healthcare, finance, and even celebrity entertainers.[14] REvil's code first appeared in April 2019. The group's last major attack was against the U.S. software company Kaseya in July 2021, which affected between 800 and 1,500 businesses that used the company as a managed service provider (MSP). Kaseya was able to obtain an encryption key to unlock the affected data in the same month.[15] The group initially disappeared in July 2021 amid speculation that its websites had been targeted by law enforcement. The websites were restored from backups by September. In October 2021, the group's websites were taken offline permanently by a multiagency international coalition, including the U.S. Cyber Command, the FBI, the Secret Service, and their counterparts abroad.[16] In November 2021, the U.S. Department of Justice charged two suspects, Yevgeniy Polyanin and Yaroslav Vasinskyi for crimes in connection with the REvil attacks.[17] Vasinsky, a Ukrainian national, was also arrested, but he was not extradited from Poland for trial until March 2022.[18] Polyanin is still wanted by the FBI and believed to be in Russia, which is his country of origin.[19] In January 2022, under pressure from the U.S., Russia's Federal Security Service (FSB) claimed to have arrested several members of REvil, seized its assets, and otherwise dismantled the remains of the group. An image of the arrests was published in open source.[20]

One of REvil's high-profile ransomware attacks occurred in June 2021 against JBS, a Brazilian company that processes and provides one-fifth of the world's meat. It has operations in not only its home country, but the U.S., Australia, New Zealand, Canada, Mexico, France, the Netherlands, and the U.K.[21] On 01 June 2021, hackers from REvil encrypted a large segment of the company's data and demanded $11 million in BitCoin. The campaign began with reconnaissance in February 2021. After initial penetration efforts failed, the group's hackers accessed JBS systems using leaked credentials from an Australian employee. REvil hackers began exfiltrating data from March through May. After that, additional data was exfiltrated from JBS Brazil to Mega, a cloud-based filesharing and storage service. The total amount of stolen data reached five terabytes taken over three months and stored in Mega and with other malicious IPs in Hong Kong not associated with JBS.[22]

The attack had international ramifications. Food processing companies rely heavily on automation and interdependent systems. JBS closed facilities in Utah, Texas, Wisconsin, Minnesota, Nebraska. All of the company's beef processing facilities in the U.S. were closed, and chicken and pork processors were also forced to either close or downsize their operations in the short term.[23]

Operations were also affected in other countries. The shutdowns affected market prices, but U.S. retailers saw limited short-term impact due to the availability of other suppliers. The nature of the data exfiltrated by REvil was not available in open source. However, on June 9, 2021, JBS announced that it had paid the ransom in order to decrypt its data.[24] This move proved controversial, as many in law enforcement believe that paying ransoms encourages future attacks.

While Russia's FSB eventually took credit for dismantling the group, voices in the U.S. cybersecurity community suggested that REvil may have been protected by the Russian intelligence community and/or the Kremlin.[25] The Russian government has long turned a blind eye towards such groups. In some cases, the FSB has used cybercriminals as proxies against targets in the U.S. and elsewhere to maintain plausible deniability. Corrupt officials may also take a payout from cybercriminals in exchange for allowing them to operate. The relationships between hackers and the Kremlin, officials, and/or the FSB are best described as "ad hoc." The arrangements develop on a case-by-case basis. However, targeting Russian citizens or companies has usually resulted in a swift response by law enforcement.[26,27] In the case of REvil, the group's relationship to the Russian government remains a "known unknown." In June 2021, a Russian researcher conducted an anonymous interview with a representative from REvil. The spokesperson asserted that the JBS attack was purely for monetary gain and that REvil usually avoided targets in the U.S. after the law enforcement response to the Colonial Pipeline attack. According to the interview, REvil was surprised that U.S. officials had suggested involvement by the Kremlin. However, as a result, REvil would begin targeting companies in the U.S.[28] The interview was conducted well before the group's websites were permanently removed, but the ransomware attack on Kaseya occurred less than a month later. The authenticity of the interview is impossible to verify, as is the spokesperson's claims about REvil's relationship with the Russian government, or lack thereof.

Case Study: Iran-Linked Groups

In January 2020, a U.S. drone strike in Iraq killed Qassem Soleimani, the head of the Iranian Revolutionary Guard Corps.[29] In response, Iran-linked hacking groups launched a retaliatory cyberattack against the Federal Depository Library Program in which the group vowed revenge and posted an altered photo of then-President Donald Trump being punched in the jaw. The attack was believed to have been carried out by low-skilled Iranian nationalist hackers, and did not result in data compromise. This "cyber vandalism" did not have major impacts, as the website is primarily utilized by U.S. libraries to access official U.S. government documents, such as legislation and regulations.[30]

Still, the attack shows the willingness of non-state groups to engage in hacking activities in support of a nation-state. In the 48 hours following the killing of Soleimani, hacking attempts emanating from Iran reportedly almost tripled.[31] While some of this activity may have been the result of state-affiliated military/intelligence organizations, it is likely that a significant portion of the activity resulted from non-state actors similar to those who apparently breached the website of the Federal Depository Library Program. This uptick in activity is also likely associated with a retaliatory motive to avenge Soleimani's killing by the U.S.

Iran-linked groups have been accused of similar activities in recent years, to include the targeting of private U.S. companies' stolen data (which could be used for the planning of future attacks), as well as activity related to U.S. elections. In many of these cases, it remains difficult to discern the level of Iranian government involvement.[32]

Outlook

State-sanctioned hacking groups such as those detailed in this paper are likely to continue engaging in low-level malicious cyber activity, such as ransomware attacks and "cyber vandalism." Nation-state adversaries of the U.S. (such as Russia, China, Iran, and North Korea) will also likely continue to tolerate these groups as long as they continue to target the U.S. and other Western nations, thus serving the geopolitical objectives of their host nations. Moreover, despite these groups' relatively "low-skilled" nature, the current global interconnectedness of cyber systems and operational technology can result in outsized impacts from relatively modest attacks, as seen in the 2021 attack on Colonial Pipeline. Stakeholders must remain aware of the current cyber threat environment in order to successfully mitigate the threats posed by malicious cyber actors such as state-sanctioned hacking groups.

---

[1] SBS Cybersecurity Top 25 Threat Actors - 2019 Edition. (2019, December 12). Retrieved 1 April, 2022, from https://sbscyber.com/resources/top-25-threat-actors-2019-edition.

[2] Annual Threat Assessment of the US Intelligence Community. (2022, February). Office of the Director of National Intelligence. Retrieved April 1, 2022, from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

[3] Khurshudyan, I., & Morris, L. (2021, June 12). Ransomware's suspected Russian roots point to a long detente between the Kremlin and hackers. Washington Post. Retrieved April 1, 2022, from https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html

[4] Lopez, C. T. (2021, May 14). In Cyber, Differentiating Between State Actors, Criminals Is a Blur. US Department of Defense. Retrieved April 1, 2022, from https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/

[5] How states could respond to Policy Brief non-state cyber-attackers. (2020, June). Netherlands Institute of International Relations. Retrieved April 1, 2022, from https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf

[6] U.S. Department of Homeland Security CISA Cyber + Infrastructure. (2021, July 8). Malware Analysis Report. Retrieved March 30, 2022, from https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a.

[7] Tetra Defense. (n.d.). DarkSide Ransomware: A Brief History. Retrieved March 30, 2022, from https://www.tetradefense.com/cyber-risk-management/darkside-ransomware-a-brief-history/.

[8] Krebson Security. (2021, May 14). DarkSide Ransome Gang Quits After Servers, Bitcoin Stash Seized. Retrieved March 30, 2022, from https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/.

[9] U.S. Department of State. (2021, November 4). DarkSide Ransomware as a Service (RaaS). Retrieved March 31, 2022, from https://www.state.gov/darkside-ransomware-as-a-service-raas/.

[10] Morrison, S. (2021, June 8). How a Major Oil Pipeline Got Held for Ransom. Retrieved March 31, 2022, from https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

[11] Perlroth, N. (2021, May 13). Colonial Pipeline Paid 75 Bitcoin, or Roughly $5 Million, to Hackers. Retrieved March 31, 2022, from https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html.

[12] RFE/RL. (2021, May 10). Biden Says Russia Has 'Some Responsibility' in Pipeline Ransomware Attack. Retrieved April 1, 2022, from https://www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html.

[13] Vaas, L. (2021, September 21). How REvil May Have Ripped Off Its Own Affiliates. Retrieved April 1, 2022, from https://threatpost.com/how-revil-may-have-ripped-off-its-own-affiliates/174887/.

[14] O'Donnell, L. (2020, May 12). REvil Ransomware Attack Hits A-List Celeb Law Firm. Retrieved April 1, 2022, from https://threatpost.com/revil-ransomware-attack-celeb-law-firm/155676/.

[15] Panettieri, J. (2022, March 11). Alleged Kaseya REvil Ransomware Hacker Extradited, Arraigned. Retrieved April 1, 2022, from https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/.

[16] Bing, C. & Menn, J. (2021, October 21). EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline. Retrieved April 1, 2022, from https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

[17] U.S. Dept. of Justice. (2021, November 8). Ukrainian Arrested and Charged with Ransomware Attack on Kaseya. Retrieved April 1, 2022, from https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[18] U.S. Dept. of Justice. (2022, March 9). Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas. Retrieved April 1, 2022, from https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas.

[19] U.S. Dept. of Justice. (n.d.). FBI Most Wanted – Yevgyeniy Igoryevich Polyanin. Retrieved April 1, 2022, from https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin/.

[20] BBC. (2022, January 14). REvil Ransomware Gang Arrested in Russia. Retrieved April 1, 2022, from https://www.bbc.com/news/technology-59998925.

[21] JBS Foods. (n.d.). Our Locations. Retrieved April 1, 2022, from https://jbsfoodsgroup.com/our-locations.

[22] Sherstobitoff, Ry. (2021, June 8). JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified. Retrieved April 1, 2022, from https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march.

[23] Batista, F., Dorning, M., & Hirtzer, M. (2021, June 1). All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack. Retrieved April 1, 2022, from https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs.

[24] JBS Foods. (2021, June 9). JBS USA Cyberattack Media Statement - June 9. Retrieved April 1, 2022, from https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.

[25] Sigalos, M. (2021, June 2). Russia-Linked Cybercriminal Group REvil Behind Meatpacker JBS Attack. Retrieved April 4, 2022, from https://www.cnbc.com/2021/06/02/russian-linked-cybercriminal-group-revil-behind-meatpacker-jbs-attack.html.

[26] Maurer, T. (2018, February 2). Why the Russian Government Turns a Blind Eye to Cybercriminals. Retrieved April 4, 2022, from https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499.

[27] Burgess, M. (2022, March 10). Leaked Ransomware Docs Show Conti Helping Putin From the Shadows. Retrieved April 4, 2022, from https://www.wired.com/story/conti-ransomware-russia/.

[28] Health Information Sharing and Analysis Center. (2021, June 7). H-ISAC TLP White Threat: Alleged REvil Ransomware Operator Says All U.S. Entities Can Now Be Targeted. Retrieved April 4, 2022, from https://www.aha.org/h-isac-reports/2021-06-07-h-isac-tlp-white-threat-bulletin-alleged-revil-ransomware-operator-says.

[29] BBC News. (2020, January 3). Qasem Soleimani: US kills top Iranian general in Baghdad air strike. Retrieved April 6, 2022, from https://www.bbc.com/news/world-middle-east-50979463.

[30] Zaveri, M. (2020, January 7). Government Website Is Hacked With Pro-Iran Messages. The New York Times. Retrieved April 6, 2022, from https://www.nytimes.com/2020/01/06/us/iran-hack-federal-depository-library.html

[31] Fung, B. (2020, January 9). Hacking attempts originating in Iran nearly triple following Soleimani strike, researchers say. CNN. Retrieved April 6, 2022, from https://edition.cnn.com/2020/01/08/tech/iran-hackers-soleimani/index.html

[32] Lyngaas, S. C. (2021, November 12). FBI warns US companies about Iranian hackers - CNNPolitics. CNN. Retrieved April 6, 2022, from https://edition.cnn.com/2021/11/11/politics/fbi-iran-hacking-warning/index.html