Pegasus Spyware and the NSO Group

1st Tristan Woodard
Cybersecurity Program
Old Dominion University
Norfolk, Virginia
twood016@odu.edu

***Abstract*— The Pegasus Spyware has been employed in recent years and the capabilities of the software are continually concerning. Various sources will be used to understand the technology, how it is used, and where it comes from in order to understand the scope and implications for modern society.**

Keywords—Cybersecurity, Spyware, Cyberwarfare, Surveillance, Hacking

I. Pegasus Spyware

In 2021 the Guardian described Pegasus Spyware as "perhaps the most powerful piece of spyware ever" [1]. There is seemingly a large amount of evidence to back up this claim. There is no accepted definition for what exactly constitutes spyware, however, In Aycock's Spyware and Adware it is recommended we instead diagnose each software individually for certain "spyware characteristics" to determine if a piece of software is spyware or not [2]. In the 10 characteristics Aycock lays out, Pegasus not only checks every box, but makes the outlined characteristics seem inadequate in scope . As an example, one such characteristic is that the software avoids attempts to uninstall said software. As will be detailed later on, Pegasus can be remotely uninstalled at any point at the first sign of danger, will automatically uninstall if it loses connection to the hacker's control center, and leaves almost no trace that it was installed in the first place [3]. Pegasus has the capability to retrieve any photo on a device, copy every message, record every phone call., have detailed access to the entirety of your GPS data, contacts, app data, and theoretically any piece of data available on the device. Pegasus will even harvest your usernames and passwords of your accounts and use that to worm deeper into your device. This is not the full extent, however. Not only does Pegasus copy and relay the data currently on your device, it also remotely controls the device to direct it towards controlling new data itself. Pegasus can seemingly direct your camera or microphone to turn on, even when you are not using your device, and harvest the data it collects from that process. This is why Pegasus is such a massive breach of security and useful tool for malicious agents. It will not only harvest any past data stored on a device, but it will also transform your own device into a surveillance super weapon and use it against you. Pegasus was created by the Israeli company NSO that was founded in 2010 [4]. Pegasus itself has at least been sold and in use since 2016. Pegasus has been sold to at least 40 different countries, and while the full scope of its usage is not fully known, it seems that at least 1,000 individuals across numerous countries over the globe have been selected for potential surveillance [5]. In terms of targets, the entire gamut is run, from heads of state being compromised such as Imran Khan, currently the former Prime Minister of Pakistan, Emmanuel Macron, current Prime Minister of France, and Boris Johnson the Prime Minister of the United Kingdom, to small-time activists and journalists[5][6]. Yes, it seems that at least 50 business executives were targeted, and at least 60 human rights activists. Another target was Jamal Khashoggi, the Saudi dissident and journalist who was brutally butchered at the order of the Saudi Crown [7]. It was found, sometime after the killing, that Pegasus Spyware was installed by agents of the United Arab Emirates onto the phone of Jamal Khashoggi's wife. With what we know about Pegasus Spyware, it is entirely possible that the data collected could have seriously aided in his killing.

II. How Pegasus Works

Pegasus Spyware seems to overwhelmingly use zero-day exploits to infect machines and start its work [1]. It's important to know however that spearphishing is also commonly used to attack targets. spearphishing is a targeted form of phishing that is a social engineering attack [8]. With Pegasus Spyware, the intention is primarily that a target will click on a link allowing for Pegasus to install itself, most often by exploiting the default browser of the device to allow it to install. These spearphishing attacks can be incredibly easy to engineer, and known kits are available that can automatically create them en masse. They most often appear as messages from reputable entities like embassies, falsified invoices, messages from coworkers or family, or other urgent alerts[9]. Zero-day vulnerabilities are much more varied and potentially more difficult to employ, however, they usually allow a greater reward. Zero-day vulnerabilities are vulnerabilities only known by the attacker and importantly are unknown by the defender [10]. A Zero-day vulnerability has no patch, no alert from a defensive system, and no remedy at the time. These vulnerabilities vary in reach and scope, however, each year there are numerous zero-day vulnerabilities discovered even in

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

important and supposedly sec systems. Maddie Stone of Google's Project Zero detected 24 Zero-Day vulnerabilities, for instance[11]. She also would go on to analyze these vulnerabilities and conclude that often patches for these vulnerabilities are in part incomplete, or are not full enough to eliminate future zero-day vulnerabilities of a similar type. Again, the nature of these vulnerabilities make their usage potentially more difficult, but it also allows for unparalleled strength for attacks against specific targets. For instance, Pegasus hackers have utilized certain Zero-Day vulnerabilities to succeed at attacking in a method possibly considered the "Holy Grail" of attack methods, the zero-click attack.. Unlike in a spearphishing attack that requires input by the user to click a link or perform an action to compromise themselves, a zero-click attack requires no input on that of the user . Simply by the attacker performing a manner of steps, the defender's system becomes infected. Zero-day vulnerabilities are often used to perform zero-click attacks, and without the zero-day vulnerabilities in place it would likely never be possible to perform zero-click attacks. One such example of such an attack is CVE-2021-30860, or the designation given by the Common Vulnerabilities and Exposures project to an attack commonly known as FORCEDENTRY [10]. There are numerous question marks surrounding FORCEDENTRY, but it seems as if the main cause for the exploit is a programming error called an integer overflow. An integer overflow is a type of buffer overflow, which means that there is an error where the space allocated in memory is not properly allocated, and a certain type of input is causing the data to "overflow" past the limits allocated, which allows for attacker controlled inputs to be directly injected into the memory space. Out of all that is known about FORCEDENTRY we do know that an integer overflow was exploited to perform the measures that allowed Pegasus to be installed onto a device. This is all the more notable as Apple had specifically implemented a defensive measure called BlastDoor which was designed to protect from a previous zero click attack called Kismet, and better protect users [12]. We also know that FORCEDENTRY would likely also need a way to execute code freely from restrictions and escape the "sandboxing" in place in mobile devices. "Sandboxing" refers to internally segmenting a system so that if one part of a system is ever compromised, it is disconnected from other parts in a way that ensures the entire system is not completely compromised as well [10]. With the "how" it gets onto the device in mind, it's equally important to cover what it does when it gets there. Once Pegasus is installed onto the kernel level of a device, it is effectively able to see any data in memory or inputs on the device [3]. Pegasus will use this information to collect available usernames and passwords and unlock the device further for the purpose of deeper exploitation. Pegasus will relay every piece of this information back to a control center by encrypting the data and passing it along "anonymizing nodes", which it can do over mobile data or Wi-Fi. This shows how the devices are able to be completely and utterly compromised and how seemingly all the data a device can offer end up in the hands of the control center on the other side. Pegasus can also seemingly self-destruct whenever necessary, by direct order, or automatically after certain prerequisites are met, allowing for little to no chance of catching the program. It's important to note that this process is not entirely secret, however. While it is designed with intention to be nearly undetectable, artifacts are supposedly left behind by the process, and Amnesty International has released a tool to help attempt to detect Pegasus on machines.

III. Who Made and Uses Pegasus

The NSO group has supposedly sold Pegasus software to over 40 countries [5]. Many countries use it more than others however, with the Sunni Despotates of Bahrain, Saudi Arabia, the United Arab Emirates, and Morocco using it often, as well as heavy usage from other authoritarian regimes like Hungary, India, and Azerbaijan, and has also seen use in stifling the Catalonian independence movement, and use in Mexico [6]. Many other agencies have also purchased Pegasus and either have not harnessed it as much, or have just not been caught using it. For instance, the CIA purchased Pegasus back in 2018 with the FBI purchasing the technology in 2019 [13]. There are concerns that the U.S. may have lent its use to U.S. ally Djibouti, who is often criticized for human rights abuses, torture, and other atrocities. The spyware has seemingly been used to compromise journalists, human rights advocates, and for political schemes. With these facts uncovered and accusations levied, NSO has continually claimed that Pegasus software is only to be used for "anti-terrorist" and "anti-crime" actions [5]. They claim to have only leased it to intelligence agencies and claim it will suspend usage when it is not used correctly. This information is hard to verify. Among the numerous overreaches, atrocities, and disturbing actions associated with its use, it has been only reported so far that Saudi Arabia, The United Arab Emirates, and some agencies within Mexico have received suspensions from the program [14]. NSO has declined to name any suspensions, however, as it claims it is prohibited from detailing information about clients, leaving everyone to make their own assumptions on whether it is true. The company further responds that, stating that it will only sell to intelligence agencies approved by the Israeli Defense Ministry. NSO claims that after an internal investigation into itself it found no evidence that its software was present on the wife of Jamal Khashoggi, or that French Prime Minister Emmanuel Macron was a target by Moroccan wielders of the Software. It may not need to be said, but one can only imagine that an internal investigation clearing itself of wrongdoing is not exactly an unexpected result. To further understand NSO however, and its background, a deeper analysis of past and near history should be looked into. The NSO Group, who created the Pegasus spyware, was founded in 2010 by Israeli Citizens Shalev Hulio, and Omri Lavie who are both believed to be alumni of Israel's Intelligence Unit 8200 [15]. According to Hulio, the two were approached by Israeli Intelligence and thus Hulio, Lavie, and Niv Carmi, a former Mossad operative, combined to start the business [16]. Mexico was seemingly the first big buyer, using the technology to hunt El Chapo, but also to spy on journalists, activists, and seemingly everyone close to then candidate, and

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

current President of Mexico, Andrés Manuel López Obrador, among which three of the sons, his wife, brothers, staff, driver, and cardiologist were all attacked with the software. From there, the company rapidly expanded into supplying the technology to seemingly any bidder. It was later revealed, however, that the software is not only an international affair. In 2020, when the protests against then Israeli Prime Minister Benjamin Netanyahu were gaining steam, the Israeli government seemingly planted the software on its own citizens [17]. This spyware attack had seemingly no warrants, no court approval, and no limits. Among those spied on are mayors, protest leaders, political opposition, and former government employees. With this information in hand, one may be inclined to think that those in the Israeli government who are in league with NSO may be ousted by now, as Benjamin Netanyahu was replaced after these protests. This is very likely not the case. Shiri Dolev is the current president of NSO [18]. Shiri Dolev is close friends with Ayelet Shaked, who is the current Minister of the Interior under Naftali Bennett, the Prime Minister who replaced Netanyahu. She was also close allies with him even before his tenure. In 2020 Bennett and Shaked campaigned hard for more cooperation between NSO and the Israeli government, citing COVID-19 as a factor for the partnership. Shalev Hulio, a founder of NSO mentioned previously, was spotted partying with Bennett's military secretary Avi Gil at a new year's party [19]. They caused controversy as they supposedly were not following proper Covid related guidelines at the event. Current Secretary of Defense under Bennett, Benny Gantz, formerly was president of the intelligence company Fifth Dimension [20]. The company supposedly specialized in tracking systems and sold intelligence to law enforcement and intelligence agencies. If that sounds familiar, it was rumored that in 2018 before Fifth Dimension shut down, the company was in the early stages of being bought out by NSO. Ram Ben Barak was also an advisory board member of Fifth Dimension, and was also a deputy director of Mossad and is currently in the Israeli Parliament as the director of the Foreign Affairs and Defense Committee [21][22]. In 2021 Barak announced to the media that "The defense establishment appointed a review commission made up of a number of groups", addressing the fact that the government appointed a group to investigate NSO after the controversy [23].

IV. Conclusion

The information surrounding Pegasus Spyware can help citizens, governments, and other organizations better understand the current conditions surrounding cyber threats, spyware, and the modern reality of cyber terror and state-sponsored cyber warfare. In regard to how attacks are conducted, it seems important to still emphasize training and learning related to phishing attacks. In cases where phishing is not even required, it is important for professionals and businesses to identify exploits, and patch them accordingly. Properly patching exploits seems to still be a pivotal issue. In regard to the modern reality and what all this information means, it paints a dark reality for the state of surveillance, cyber terror, and state sponsored cyber warfare. In the case of Israel, the country represents a nation that has seemingly embraced its ability to conduct state sponsored cyber warfare and cyberterrorism. Both the past and current Israeli governments have connections to NSO specifically, and the cyber-surveillance industry at large. Not only have they used the technology on their own citizens, but they have sold the technology to seemingly almost any bidder. It's reasonable to believe that the powerful Pegasus technology has likely been a boon for business and political deals with neighbors. This paints a harsh reality where countries could develop all sorts of cyber weapons meant to empower regimes and control citizenry, and use it to further their geopolitical goals. Israel and NSO seemingly has not and possibly can not be subject to any outside regulation or control. NSO and Pegasus have only seemingly been investigated by internal investigations, and by the teams appointed by the very same Israeli government that it has close ties to. The conclusion of this report is that the claims that the Pegasus spyware could be the "most powerful piece of spyware ever" is very possible. It can be injected into a device via phishing or by numerous zero-day exploits. This gives it the ability to potentially enter a device through a zero-click attack that requires no input from the defender. From there, it can harvest any data on the device, and use the device to gather even more data. The spyware has been used by numerous regimes in order to surveil citizens, monitor human rights activists and political opponents from heads of state to local rivals, and has even seemingly been connected to brutal killings. It seems as if there are no checks or balances for the NSO group, or the faction of the Israeli government that it has ties to. Pegasus and its frightening capabilities, seems to line up perfectly with the geopolitical and strategic goals of Israel as well, offering little to no mechanisms in the way to challenge its global deployment as a harmful and invasive tool of surveillance and violence. All this information signals the need for a stronger and more robust central authority (or group of authorities) with to either be created, or stem from another pre-existing group in order to control, monitor, and prevent state sponsored cyber-warfare and criminal levels of overreach in surveillance, tracking, and breaches of human rights in the cyber realm. With seemingly no checks in place to curtail the effects of software like Pegasus, companies like NSO, and countries like Israel, it stands to reason that such a central authority is necessary to protect the cyber-world in much the same way similar entities, treaties, and conventions have been made in order to protect the physical world. It would be to the hopes and benefits of many that in the future there can be some sort of international coalition and consensus that convenes and seeks to control or limit the capability of state sponsored cyber-warfare, rogue cyber-states, spyware super weapons, and hopefully empowers

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

the defenders of cyberspace to perform a more successful job in patching, finding, and eliminating exploits.

[1] D. Pegg and S. Cutler, “What is Pegasus spyware and how does it hack phones?”, The Guardian para July 18 2021. [Online], Available: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [Accessed April 24, 2022].

[2] J. Aycock, Spyware and Adware. New York City: Springer US 2011.

[3] K. Zetter, “Pegasus Spyware: How It Works and What It Collects”, August 4 2021. [Online]. Available: https://zetter.substack.com/p/pegasus-spyware-how-it-works-and?s=r [Accessed April 24, 2022].

[4] G Woodruff, “What We Know About the Secretive Company Behind the Pegasus Spy Software”, Slate para July 20 2021. [Online], Available: https://slate.com/technology/2021/07/nso-group-pegasus-spyware.html [Accessed April 24, 2022].

[5] AL JAZEERA AND NEWS AGENCIES, “Pegasus: What you need to know about Israeli spyware”, AlJazeera para February 8 2022. [Online], Available: https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus [Accessed April 24, 2022].

[6] R. Farrow, “How Democracies Spy on Their Citizens”, The New Yorker para April 18 2022. [Online], Available: https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens [Accessed April 24, 2022].

[7] C. Faife, “New analysis further links Pegasus spyware to Jamal Khashoggi murder”, The Verge para Dec. 21 2021. [Online], Available: https://www.theverge.com/2021/12/21/22848485/pegasus-spyware-jamal-khashoggi-murder-nso-hanan-elatr-new-analysis [Accessed April 24, 2022].

[8] B. Sterling, “Spearphishing journalist smartphones with Pegasus”, Wired para Oct 6, 2018. [Online], Available: https://www.wired.com/beyond-the-beyond/2018/10/spearphishing-journalist-smartphones-pegasus/ [Accessed April 24, 2022].

[9] M. Price. Conference Lecture, Topic: “Patching Your Biggest Vulnerability: Your Employees” Webroot , Broomfield, CO, Jan. 9, 2019.

[10] C. Crowley, “What you Need to Know about CVE-2021-30860 aka FORCEDENTRY w/ Chris Crowley”, Sep 16, 2021. [Online]. Available: https://www.youtube.com/watch?v=LcDVXagFdBM [Accessed April 24, 2022].

[11] M. Stone. USENIX Enigma 2021. Conference Lecture, Topic: “The State of 0-Day in-the-Wild Exploitation.”USENIX, Mar 1, 2021.

[12] B. Marczak, A. Abdulemam1, N. Al-Jizawi, S. Anstis, K. Berdan, J. Scott-Railton, and R. Deibert, “Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits” Aug. 21 2021. [Online].Available: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/.
[Accessed April 24, 2022].

[13] M Levenson, “F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones”, The New York Times para Jan. 28, 2022. [Online], Available: https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html.

[14] D Estrin, “A Tech Firm Has Blocked Some Governments From Using Its Spyware Over Misuse Claims”, NPR para July 29, 2021. [Online], Available: https://www.npr.org/2021/07/29/1022409865/nso-suspended-govvernment-contracts-spyware-pegasus-project

[15] T Brewster, “Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text”, Forbes para Aug. 25, 2016. [Online], Available: https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=58728c073997

[16] A. Travère and P. Rueckert, “THE RISE AND FALL OF NSO GROUP,” forbiddenstories.com, para. July, 19 2021. [Online]. Available: https://forbiddenstories.org/the-rise-and-fall-of-nso-group/. [Accessed April 24, 2022].

[17] T. Ganon, “Israel police uses NSO’s Pegasus to spy on citizens” calcalistech.com, para. Jan. 1 2022. [Online]. Available: https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html [Accessed April 24, 2022].

[18] N. Landau and N. Gontarz, “‘No Tenders in War’: Defense Minister Insists on Team-up With NSO to Battle Coronavirus”, Haaretz para Apr. 1, 2020. [Online], Available: https://www.haaretz.com/israel-news/.premium-israel-s-defense-minister-insists-on-teaming-up-with-nso-to-battle-coronavirus-1.8732531 [Accessed April 24, 2022].

[19] T. Schneider, “‘Government military secretary spotted partying with NSO executives”, The Times of Israel para Jan. 5 2022. [Online], Available: https://www.timesofisrael.com/government-military-secretary-spotted-partying-with-nso-executives/ [Accessed April 24, 2022].

[20] T. Shahaf, “NSO in talks to buy Israeli intelligence co Fifth Dimension”,Globes para Nov 11 2018. [Online], Available: https://en.globes.co.il/en/article-nso-in-talks-to-buy-israeli-intelligence-co-fifth-dimension-1001260088 [Accessed April 24, 2022].

[21] Crunchbase “PERSON: Ram Ben Barak” crunchbase.com. [Online]. Available: https://www.crunchbase.com/person/ram-ben-barak. [Accessed April 24, 2022].

[22] Knesset.gov, “MK Ram Ben Barak appointed as chair of provisional Foreign Affairs and Defense Committee”.
June 16, 2021 [Online]. Available: https://m.knesset.gov.il/en/news/pressreleases/pages/press16621s.aspx. [Accessed April 24, 2022].

[23] AFP, “Israel appoints commission to review Pegasus-maker NSO
”, The Times of Israel para July 22 2021. [Online], Available: https://www.timesofisrael.com/liveblog_entry/israel-appoints-commission-to-review-pegasus-maker-nso/ [Accessed April 24, 2022].