Marcus Sowers

Old Dominion University

CS462 – Cybersecurity Fundamentals

4/18/22

The Recent Controversies around Pegasus Spyware

As society is continuously advancing and growing with technology, the future holds a lot of unexpected outcomes that we may not be ready for. Technology is beginning to be the base for everything that happens in the world today, whether it is used for communication, information/data, entertainment, etc. With the advanced technology we have today, there are a lot of pros that come from it. Even though there is positive results and opportunity from such advancements, society must understand that there is possible negative threats and vulnerability that can come with it also. According to Pew Research Center, 97% of Americans now own a cellphone of some kind (Mobile Fact Sheet). It was stated that 15% of those American adults are "smartphone-only" internet users, which basically means they use their cellphone strictly for communication and not take advantage of the internet accessibility. With almost everyone in America using a cellphone, the risk of cellphone threats is potentially high because the usage of these devices is extremely high. This research paper will go into detail and discuss the recent controversies with the confirmation of spyware being used against technology around the world.

This research paper will discuss one specific spyware that can easily gain access to a smartphone and obtain everything on it. This spyware is called Pegasus and it was developed by Israeli cybersecurity organization NSO Group, which sells its software to various clients, including governments, to track criminal and terrorist activity (Billy Perrigo and Patrick Lucas

Austin). Pegasus spyware can be used to attack and infiltrate smartphones through various apps downloaded to the device. Once Pegasus has infiltrated a device, it can access any information and data from the device. The data stolen can be in the range from communications like text messages and call logs, passwords, recordings, photos, videos, social media accounts, etc. If the specific device has a camera, Pegasus could also give the attacker the ability to use them for live surveillance without the victim knowing. The scariest part about this spyware is it can access a device without interaction from the user, nor be easily detected. Many devices are vulnerable if they are attacked by the Pegasus spyware including smartphones, laptops, tablets, and computers. Any device that has the ability to download and store applications and calls are usually the devices at high risks. Pegasus spyware has already been applied and put into motion multiples times within recent history.

In July of 2021, a list provided by Amnesty International and Forbidden Stories contained around 50,000 phone numbers that included various executives, government officials, pro-democracy activists, news reporters, and certain journalist (Billy Perrigo and Patrick Lucas Austin). This Pegasus Spyware controversy may not have occurred in a specific country, but it should be notified that it was used against a specific company and device. Even though the Pegasus spyware tool was never completely confirmed to be used to hack the iPhones for sensitive information, a good amount of phone numbers infiltrated were devices owned by "significant" people like government officials, journalist and other personnel stated above. In November 2021, Apple announced that they were filing a legal complaint in US courts against NSO Group, referring to the defendants as "amoral 21st century mercenaries." Apple further noted that the "Citizen Lab's disclosure of the spyware was critical in enabling the company to track down and neutralize NSO Group's exploitation of Apple's infrastructure and customers"

(Ron Deibert). With this type of ability to undetectably attack a device, it should be a huge understanding to why there is such controversy about this topic.

In my opinion, I have a few concerns about the weak privacy security of smartphones with respect to the Pegasus spyware. My major concern when examining this spyware is who can have access to it, and how much power they possible hold with this access. The NSO Group stated that it built Pegasus so that governments can utilize this spyware for mostly law enforcement use and counterterrorism. One incident law enforcement utilized this spyware is when it was used by the Mexican government. In 2011, Pegasus was used to track the notorious drug baron Joaquín "El Chapo" Guzmán (Bhanukiran Gurijala). If this government was able to track this stealthy drug baron, I believe almost any government or private contractor can utilize it to track or hack almost anybody on this Earth. With this type of technological access, there is a possible case that this type of software can violate multiple human rights.

My last concern I have about the weak privacy security of smartphones with respect to the Pegasus spyware is the possible violation of human rights and if this type of software is legal. According to Ari Azra Waldman and Matthew Tokson, courts are now "confronting new technologies often adopt the nonintervention principle, or the idea that courts should refrain from addressing the Fourth Amendment implications of new surveillance practices until the relevant social norms become clear" (Ari Azra Waldman and Matthew Tokson). This is a huge concern is my opinion because where exactly do we draw the line for "social norms"? Technology is advancing and improving at such an intense rate its hard to regulate what is exactly normal or not. The Fourth Amendment of the U.S. Constitution states that the people have a right to be protected from unreasonable searches and seizures by the government. These rights shall not be violated unless warrant is issued upon probable cause. How are we able to uphold are guarantee

to this right if created software like Pegasus is used and is possibly violating it? This should be a huge concern to anyone who owns a smartphone because we are not fully guarantee this right, we were once promised before the rising of this technological era. In this term paper I discussed a recent Pegasus spyware controversy that occurred, how it can infect a device, what may be compromised, which devices are vulnerable, my concerns about the privacy shortcomings of smartphones with respect to the Pegasus spyware, and the use of Pegasus spyware used by states/governments.

Work Cited

Austin, Patrick Lucas, and Billy Perrigo. "Pegasus Spyware Reportedly Hacked Thousands of IPhones Worldwide. Here's What to Know." *Time.Com*, July 2021, p. N.PAG. *EBSCOhost*, https://search-ebscohost-com.proxy.lib.odu.edu/login.aspx?direct=true&db=a9h&AN=151505532&scope=site.

DEIBERT, RON. "Protecting Society from Surveillance Spyware." *Issues in Science & Technology*, vol. 38, no. 2, Winter 2022, pp. 15–17. *EBSCOhost*, https://search-ebscohost-com.proxy.lib.odu.edu/login.aspx?direct=true&db=a9h&AN=156382827&scope=site.

Gurijala, Bhanukiran. "What Is Pegasus? A Cybersecurity Expert Explains How the Spyware Invades Phones and What It Does When It Gets In." *The Conversation*, West Virginia University, 26 Jan. 2022, https://theconversation.com/what-is-pegasus-a-cybersecurity-expert-explains-how-the-spyware-invades-phones-and-what-it-does-when-it-gets-in-165382.

"Mobile Fact Sheet." *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 23 Nov. 2021, https://www.pewresearch.org/internet/fact-sheet/mobile/#:~:text=Who%20owns%20cellphones%20and%20smartphones%20%20%20,%20%204%25%20%2016%20more%20rows%20.

Tokson, Matthew, and Ari Ezra Waldman. "Social Norms in Fourth Amendment Law." *Michigan Law Review*, vol. 120, no. 2, Nov. 2021, pp. 265–313. *EBSCOhost*, https://doi-org.proxy.lib.odu.edu/10.36644/mlr.120.2.social.