Evan Harmony

ISM 4323

January 17, 2017

Trident: A Tool for Cyber-Warfare

Every century it is possible to look back and see the most influential inventions that have changed the way that we, as a people, operate. The advent of the Internet completely changed everything but as the technology was evolving there were major growing pains. Security often seems to be one aspect that is overlooked until it is too late; the ILUVYOU worm and the Morris Worm are perfect examples of that. Both led to sweeping changes in the management and regulation of the internet, they also revealed the poor practices and lack of awareness of the end user. We are now entering an era where the users are so far removed from the knowledge of how their devices work that implementing and teaching these practices will be critical for information security going forward.

Not even a decade has passed since Apple first released the iPhone, the first smartphone on the market, but it is clear that it has fundamentally changed the IT landscape. The report that follows will outline one of the most advanced attacks against a mobile device ever found. The story revolves around the Ahmed Mansoor, the target of the attack, as well as the NSO Group, the creators of the spyware. There will then be a brief technical explanation of how the exploits are carried out. Followed by a discussion of device security and why this is important going forward.

Ahmed Mansoor is a civil rights activist from the United Arab Emirates (UAE). In April of 2011 he was imprisoned after signing a petition advocating for democracy in the UAE. Mansoor was arrested with a group of four other men who became known as the “UAE Five”. In

November of 2011 the four other members of the group were sentenced to two years in prison while Mansoor was sentenced to three. Throughout the trial many civil rights watch groups condemned not only the imprisonment of the men, but also the due process of the trial. After the men were sentenced they all unexpectedly received pardons which the president's office would not comment on. Since his pardon Mansoor has continued his work as a civil rights activist but has been subjected to multiple attacks. Both attacks have been through email; however, the first attack, in 2011, utilized FinFisher IT Intrusion while the second, in 2012, used Hacking Team. Fortunately both of these email attack were caught but Mansoor has had to remain constantly vigilant. In 2016 Mansoor received a text message from an unknown number claiming to have information on state sanctioned torture of Emerati prisoners with a link to a webpage. Mansoor, wary from his previous attacks, did not open the link but instead forwarded it to Citizen Lab. Citizen Lab is headquartered at the Munk School of Global Affairs, University of Toronto in Canada. Their mission is to "… undertake research that monitors, analyzes, and impacts the exercise of political power in cyberspace." Citizen Lab then opened the link on a factory reset iPhone running iOS 9.3.3, the same version the Mansoor was currently running. After analyzing the attack it was traced back to an IP address known to belong to the organization known as NSO Group.

The NSO Group is an Israeli based IT company that creates unique surveillance and cyber-warfare products to sell to governments. There is not much information about them as they sell their product and services only to governments. But they are far from unique, there are many companies that specialize in cyber-intelligence and they are becoming big business. NSO Group was acquired in 2014 by the US private equity firm Francisco Partners for $130 million. NSO has developed their own spyware known as Pegasus which is what was behind the attempt to break into Mansoor’s device. Pegasus is the product that is sold to governments and it allows them to interface with the command and control (C2) server that links to the infiltrated clients. The second part of the attack on the mobile device are the three iOS exploits that are used to gain access to the kernel. The exploits work together to remotely jailbreak the phone and are collectively known as Trident.

The three Trident exploits are identified in the Common Vulnerabilities and Exposures (CVE) database as CVE-2016-4655, CVE-2016-4656, and CVE-2016-4657. CVE 4657 is the first in the series and exploits a memory corruption vulnerability in the Safari WebKit. This exploit grants code execution rights to a webpage. This leads to the next exploit CVE 4655 which maps the kernel memory of the device. The code that is executed from the Safari exploit returns the location of the kernel memory. This is vital because to jailbreak the phone the kernel address is required. This exploit circumvents the defenses of Kernel Address Space Layout Randomization (KASLR) which is a defense mechanism that randomly maps out the kernel memory address locations. Once Pegasus knows the kernel memory location it can carry out the main objective which is to jailbreak the device, CVE 4656. Once the device is jailbroken all of the information on it is compromised. The attack utilizes the Cydia Mobile Substrate to hook into the applications currently on the phone without installing any new ones. These hooks bypass the iOS security mechanisms and allow information to be passed outside of the application and sent back to the C2 server. It appears that not only are all default iOS apps such as Phone and Message vulnerable but there are APIs for almost every popular app available such as WhatsApp or Viber. This means that the device is under complete control from whomever is on the other end of the Pegasus dashboard.

The Trident exploits and the Pegasus spyware together bring to life a rather frightening reality, although they were patched by Apple within ten days of being found. This is the only documented instance in which a remote jailbreak has been seen in a real life scenario. The advanced nature and obfuscation techniques of this attack are something that has rarely been seen as well. The executed code is very well documented and commented, it shows a high level of sophistication and appears that these zero-day exploits have been available at least as far back as iOS 7. The malware is also very thought out as certain processes are prohibited from running during operation of the device to ensure that the target remains unaware of the agent on their phone. For example the malware will not allow remote access to the camera while the screen is unlocked. Also the link that is sent to the target is a one-time use link, which prevents any analysis after the link has been used.

In a business environment an attack of this nature is obviously highly unlikely, as these vulnerabilities are very costly to find, but equally important to study. The expertise and understanding of the underlying hardware and software is much more advanced than that of your typical APT. It is apparent that having been trained on what to look for and educating the end user can ensure breaches do not occur, and that is even true in this case. After all this very advanced threat originated from a phishing attack, a problem which still plague's large enterprises. Fortunately Ahmed Mansoor not only had the wherewithal to not click on a link from an unrecognized number but also had the connections to forward the link to the correct authorities. Policy implementation and training are vital in today's business environment. There has been such a rise in the security of the hardware and software that the end-users are now the weakest link. Social engineering has become extremely popular over the last few years as a result. Specialized variants of older attacks, like spear phishing and whaling, are being seen now deceive targets of the more familiar phishing attack that has been around for many years. With the increase of personal data that is freely available online via social media sites, it is now easier to build unique attack to target a small group or even a single person, and is much more likely to be effective.

Another takeaway from this case is in what manner the victim was targeted, in this instance his mobile device. Going forward mobile devices will become some of the biggest threats to secured networks. Already there has been a huge increase in demand for Mobile Device Management (MDM). With 64% of American adults owning smartphones in 2015 this will be a focus for many organization going forward. According to Gartner 40% of US employees of large enterprises use personally owned devices for work. Going forward securing devices that connect to a private network will be a challenge since there is no way to control how the device is being used outside of the workplace, but with improved teaching practices and adherence to good security practices there is hope.

Works Cited

"About the Citizen Lab - The Citizen Lab." *Citizen Lab*. University of Toronto, n.d. Web. 23 Oct. 2016.

Bazaliy, Max, Andrew Blaich, Kristy Edwards, Michael Flossman, and Seth Hardy. "Sophisticated, Persistent Mobile Attack against High-value ..." *Lookout Blog*. Lookout Inc., 25 Aug. 2016. Web. 23 Oct. 2016.

Britton, John. "Mobile Security Alert: Pegasus & Trident within Your Business." *Air-Watch*. N.p., 6 Sept. 2016. Web. 23 Oct. 2016.

Marczak, Bill, and John Scott-Railton. "The Million Dollar Dissident: NSO Group's IPhone Zero-Days ..." University of Toronto, 24 Aug. 2016. Web. 23 Oct. 2016.

Rivera, Janessa. "Gartner Says 40 Percent of U.S. Employees of Large ..." Gartner, 21 Oct. 2014. Web. 23 Oct. 2016.

Rivera, Janessa. "Gartner Says By 2018, More Than 50 Percent of Users Will ..." Gartner, 8 Dec. 2014. Web. 23 Oct. 2016.

Smith, Aaron. "U.S. Smartphone Use in 2015 | Pew Research Center." Pew Research Center, 1 Apr. 2015. Web. 23 Oct. 2016.