Applying Diamond Model: Lawful Intercept Abuse

Sneha Talwalkar
School of Cybersecurity & Privacy
Georgia Institute of Technology

CONTENTS

Applying Diamond Model: Lawful Intercept Abuse

***Abstract*—UAE government, a nation-state adversary targeted their own human rights defender, Ahmed Mansoor, with the 'Trident', a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware on Aug 10th, 2016. This incident of Lawful Intercept (LI) abuse is analyzed using the Diamond Model of Intrusion Analysis in the following report. Detailed investigation and evidence gathering was possible because Ahmed Mansoor chose to report suspicious messages on his iPhone to Citizen Lab (an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto) and Citizen Lab along with the Lookout Security researchers initiated a responsible disclosure process and contacted Apple on Aug 15th, 2016.[1] Only after Apple released the patch for the exploits, these researchers published a report, titled, 'THE MILLION DOLLAR DISSIDENT' on Aug 24th, 2016[1]. Majority of this incident analysis relies on this report and continues to further investigate, how the incident links with US mercenaries based on a Reuter's article titled, 'Special Report: Inside the UAE's secret hacking team of U.S. mercenaries' drawing the need for transnational laws governing LI[2]**

I. Applying the Diamond model

A. Adversary

The UAE government launched Project Raven, a clandestine team that included more than a dozen former U.S. intelligence operatives recruited to help the United Arab Emirates engage in surveillance of other governments, militants and human rights activists critical of the monarchy in 2009. The original idea was for Americans' to develop and run the program for five to 10 years until Emirati intelligence officers were skilled enough to take over. Before 2012, the nascent UAE intelligence-gathering operation largely relied on Emirati agents breaking into the homes of targets while they were away and physically placing spyware on computers. In 2015, the power dynamic shifted, UAE grew more uncomfortable with a core national security program being controlled by foreigners and forced the Project Raven to be run through a domestic company, DarkMatter. The Americans identified vulnerabilities in selected targets, developed or procured software to carry out the intrusions and assisted in monitoring them. But an Emirati operative would usually press the button on an attack. This arrangement was intended to give the Americans "plausible deniability" about the nature of the work. Thus, the UAE government became a well-resourced adversary customer who started carrying out uncontrolled surveillance against prominent journalists, activists, and also the target citizens of different countries through computer security firms such as DarkMatter and Israel's NSO group.

B. Victim

1) Victim personae: Prominent Emirati activist Ahmed Mansoor, who publicly criticized the country's war in Yemen, treatment of migrant workers and detention of political opponents, was given the code name Egret, and was a target of the UAE government since 2011. There were other targets such as Rori Donaghy, a British journalist who had also been under attack from the UAE government. Another source from Reuters reveals that a lead analyst working for UAE's Raven project used to probe the accounts of potential Raven targets and learn what vulnerabilities could be used to penetrate their email or messaging systems. She saw American citizens and Yemeni targets listed on the Raven's target files[2]

2) Victim asset: Ahmed Mansoor's iPhone was targeted, previously his emails and computers were also targeted. On the morning of August 10, 2016, Mansoor received an SMS text message that appeared suspicious. The next day he received a second, similar text. The messages promised "new secrets" about detainees tortured in UAE prisons, and contained a hyperlink to an unfamiliar website. The messages arrived on Mansoor's stock iPhone 6 running iOS 9.3.3.

3) Vulnerabilities and Exposures: The main motive of this adversary was to jailbreak into the victim's device and install spyware that would stealthily monitor every activity of the victim. The vulnerabilities exploited in this incident were zero-day vulnerabilities in iPhone and they were documented after the responsible disclosure by the Citizen Lab team as follows:

- **CVE-2016-4657** An exploit for WebKit, which allows execution of the initial shellcode
- **CVE-2016-4655** A Kernel Address Space Layout Randomization (KASLR) bypass exploit to find the base address of the kernel
- **CVE-2016-4656** 32 and 64-bit iOS kernel exploits that allow execution of code in the kernel, used to jailbreak the phone and allow software installation

4) Victim Susceptibilities: Interestingly, the victim was suspicious of the malicious links because the message was unsolicited and instead of clicking the links, he sent the message to the Lab for investigation. However, if the attack had involved social engineering, the adversary could have induced Mansoor into clicking the links by sending a pre-agreed message. Due to the lack of mitigation efforts around lawful intercept abuse, ineffective human rights policies, and the failure of spyware companies to perform the necessary due diligence, the victim stays susceptible. Similarly, due to the lack of transnational laws around foreign surveillance, American and

[1]Although the victim did not fall prey to the adversary's malicious links, the said example is an 'Incident' per NIST definition: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or **attempts to gain**, access to a system or system resource without having authorization to do so.

Yemeni citizens are susceptible to unlawful surveillance from the UAE government.

C. Capability

The spyware was hypothesized to be NSO's Pegasus spyware solution in the beginning of the investigation, it was capable of employing victim's iPhone's camera and microphone to eavesdrop on activity in the vicinity of the device, recording his WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking his movements. However, through the Hacking team's leaked emails (that included NSO's sales pitches and product documentations) after the 2015 breach, two things were clear- in the operation targeting Mansoor, the one-click vector was used, with anonymizer sms.webadv.co. and that the C2 servers were: aalaan.tv and manoraonline.net.

D. Infrastructure

1) Type 1 Infrastructure: An infected device could transmit the collected information back to a Pegasus Data Server at the operator's premises via the PATN (Pegasus Anonymizing Transmission Network). Once the collected information arrived on the Pegasus Data Server, an operator could visualize the information on a Pegasus Working Station.

2) Type 2 Infrastructure: Israel's NSO Group used to sell Pegasus, a government-exclusive "lawful intercept" spyware product. NSO Group was owned by an American venture capital firm, Francisco Partners Management. As of this writing, the NSO group is known to be blacklisted by the US government[3] The investigators identified what appeared to be a mobile attack infrastructure while dealing with another UAE based threat group Stealth Falcon. In spyware attack case of the victim Mansoor, 237 live IP addresses were found, and after their domain names were extracted, *.webadv.co, manoraonline.net, and aalaan.tv were found which interestingly, connect to 'News Media' perhaps indicating the use of fake news articles to trick activist and journalist targets into clicking on spyware links. Other infrastructure used - online accounts, document sharing, shipment tracking, corporate account portals.

3) Service Providers: Two domain names that appear intended to masquerade as an official site of the International Committee of the Red Cross (ICRC): icrcworld.com and redcrossworld.com. Perhaps because a target may trust an SMS appearing to come from an ISP or Telco they subscribe to, ISP/Telco were on the list of domains found. Additionally, topcontactco.com a look- alike of tpcontact.co.uk, a website belonging to Teleperformance, a company that has managed UK visa application processing in many countries was also found. A complete list of domains and service providers was not published because they may have been used for legitimate law enforcement operations at the time of investigation.

Social-Political Meta Features

Clearly, the **intention** of the UAE government was to learn the cyber operations from the American mercenaries to conduct Cyber espionage under the pretext of lawful interception and counterterrorism. With every successful attack against activists like Mansoor, the confidence of the adversary grew stronger. This is also the reason why they kept trying to intercept Mansoor's devices waiting for him to fall prey to their attacks. When the documented attacks did not work, the adversary adopted zero-day exploits.

Type of relationship: Persistent The fact that the UAE government's Raven Project strategically selected high value targets like Mansoor Ahmed, key Yemeni and American citizens, it was obvious that these were **Victims of interest** and the adversary was taking all the efforts to establish continued access with the victim through multiple attacks. This was also confirmed by the fact that Trident, the chain of exploits, was re-run locally on the phone at each boot, using the JavaScriptCore binary. To facilitate persistence, the spyware disabled Apple's automatic updates, and detected and removed other jailbreaks.

Cyber-Victimology: possibility of shared threat space One of the Raven project's key targets in 2012 was Rori Donaghy[2] He was a British journalist and also an activist (like Mansoor) who authored articles critical of the country's human rights record. The surveillance against Donaghy was given the codename 'Gyro' just like Mansoor was named 'Egret'. The attack method in both cases is also similar in that the adversary entices the victim to bring hope to those who are suffering and attempts to monitor user activity, emails, apps and browsing history through establishing persistent access with the adversary by exploiting vulnerabilities. Three U.S. journalists were found on the target list of the UAE government's project Raven[2] The striking similarities in the choice of the victims and attack methods suggests that there is a possibility of a Shared Threat Space. If transnational laws are not developed against lawful intercept, countries like UAE, will continue their surveillance operations against activists and journalists all over the world significantly affecting foreign relations.

Technology Meta Features

Based on the number of attacks carried out by the UAE government-led threat groups, it is very clear that there exists a shared threat space, as of this writing, based on the analysis carried out thus far and it may be subject to change in the future. Based on this shared threat space, it can be speculated that the contextual indicators of the adversary's attack tactics are 'Spyware'. Therefore, any associations of 'activists or journalists' with 'spyware' should raise flags about the UAE government's involvement during subsequent investigations. Below is a detailed technological summary of the attack chain. The result for every event after 'Message sent' is 'Fail' because the adversary reported the incident before falling prey. The timeline of each event after 'Navigate to the URL' is greater than 10 seconds but less than 10 minutes. The attack chain is designed fast enough and stealthy so that it goes unnoticed to the victim.

Event1 UAE government's Raven project used NSO groups

mobile attack infrastructure to send Mansoor Ahmed messages with spyware links on Aug 10-11, 2016 (Hypothetical)

Event2 Instead of clicking the suspicious links on the unsolicited messages, Mansoor reported them to the Citizen Lab for investigation. The Lab researchers accessed the links on a stock factory-reset iPhone 5 running iOS 9.3.3. Mansoor's device was an iPhone 6, running iOS 9.3.3 and this version was not available for testing.(Actual)

Event3 Researchers opened the links through Safari browser and after 10 seconds of 'Navigating to URL' the Safari window closed and there was no further noticeable activity on the iPhone screen.(Actual)

Event4 In the background, the phone was served Safari exploit, followed by intermediate files (final111), and a final payload (test111.tar). The first two payloads form the Trident exploit chain, and test111.tar was the payload. (Actual)

Event5 Stage 1 of the exploit: Obfuscated JavaScript was downloaded. The JavaScript downloaded (via XMLHttpRequest) stage2 binaries for 64-bit (iPhone 5s and later), depending on the type of device. It employed a previously undocumented memory corruption vulnerability in WebKit to execute this code within the context of the Safari browser (CVE-2016-4657). Stage 2: Exploited a function that returned a kernel memory address, from which the base address of the kernel could be mapped (CVE-2016-4655), then it employed a memory corruption vulnerability in the kernel (CVE-2016-4656). Downloaded and installed stage3, which was the spyware payload. Stage 3: Payload could spy on apps including: iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype, Line, KakaoTalk, WeChat, Surespot, Imo.im, Mail.Ru, Tango, VK, and Odnoklassniki.(Actual)

Event6 The attack payload beaconed back to command and control (C2) servers delivered in stage2 of the Trident, via HTTPS. These are the C2 servers for the spyware sent to Mansoor: aalaan.tv and manoraonline.net.(Actual)

Horizontal correlation Internal databases of the Raven project led by UAE, contained passports of Americans identified as their surveillance targets. On the target lists were U.S. journalists and Yemenis. UAE security forces sought surveillance against 2 Americans.[2]

II. Policy assessment

A. Frequency of Incidents

The global Lawful Interception Market size is expected to grow USD 3.5 billion in 2021 to USD 12.9 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 29.3 percent during the forecast period.[6]

B. Associated Risks

LI risks the Privacy of citizens, affects foreign relations when lawful intercept transcends country borders. The spyware tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order.

C. Mitigation

There are country specific laws for LI and only one international attempt towards harmonizing national laws on Computer and Cybercrime. The principal global treaty-based legal instrument relating to LI (including retained data) is the Convention on Cybercrime (Budapest, 23 Nov 2001)[5]. The threat model for every country adopting LI is very different today from what it was 20 years ago. Besides, the treaty-based draft should be revised in collaboration with all the participating countries instead of expecting the countries to sign the draft.

In today's era of cloud computing and globalization, lawful intercept can easily transcend national frontiers. Hence, it is important for countries to draw clear boundaries to avoid foreign conflict. There was no Transnational law that could deter the UAE government from carrying out spy operations against American citizens. Better ways need to be developed to share technology and services among different countries to promote internet security and privacy for the citizens of the countries engaged in the trade of intelligent services. Foreign offensive cyber operations should be strictly audited. As of this writing, the Biden administration has signed a law that prohibits U.S. intelligence officials with knowledge of spy craft and national security secrets from selling their services to other countries for 30 months after retiring and The Commerce Department's Bureau of Industry and Security (BIS) has added NSO Group et al. to Entity list to mitigate unlawful surveillance[4][3]. These efforts, however, will not deter the UAE cybersecurity firms such as Dark Matter from abusing intelligence services because mercenaries continue to operate and there are no transnational laws or trade agreements that draw the line between lawful interception and unlawful foreign surveillance.

References

[1] Bill Marczak and John Scott-Railton. , *"The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender"*. Citizen Lab Research Report No. 78, University of Toronto, August 2016., https://www.semanticscholar.org/paper/The-Million-Dollar-Dissident%3A-NSO-Group%E2%80%99s-iPhone-a-Marczak-Scott-Railton/041f49d72510e333fc99d12dcbb76424ce5ad911.

[2] Reuter, "Special Report: Inside the UAE's secret hacking team of U.S. mercenaries", shorturl.at/cyCU3.

[3] commerce.gov, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities,", https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

[4] Joel Schectman, Christopher Bing., "U.S. bars ex-spies from becoming 'mercenaries," shorturl.at/pvFX0

[5] Bill Convention on Cybercrime - Wikipedia , https://en.wikipedia.org/wiki/Convention_on_Cybercrime#cite_note-auto-6.

[6] researchandmarkets.com. , *"Research and Markets ltd. Global Lawful Interception Market by Component (Solution and Services), Network (Fixed Network and Mobile Network), Mediation Device, Type of Interception (Active, Passive, and Hybrid), End User (Government and LEA), and Region - Forecast to 2026.,* shorturl.at/yBGQZ.