Research < Targeted Threats The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE **Human Rights Defender** This report was written with the assistance of the research team at Lookout Security. Update (Sept 1, 2016): Today Apple released security updates for Desktop Safari and Mac OS X. These updates patch the Trident vulnerabilities that identified in this report for desktop users. The Trident vulnerabilities used by NSO could have been weaponized against users of non iOS devices, including OSX. We encourage all Apple users to install the update as soon as possible. Citizen Lab is not releasing samples of the attack at this time to protect the integrity of still-ongoing investigations. This report describes how a government targeted an internationally recognized human rights defender, Ahmed Mansoor, with the Trident, a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware. 1. Executive Summary Ahmed Mansoor is an internationally recognized human rights defender, based in the United Arab Emirates (UAE), and recipient of the Martin Ennals Award (sometimes referred to as a "Nobel Prize for human rights"). On August 10 and 11, 2016, Mansoor received SMS text messages on his iPhone promising "new secrets" about detainees tortured in UAE jails if he clicked on an included link. Instead of clicking, Mansoor sent the messages to Citizen Lab researchers. We recognized the links as belonging to an exploit infrastructure connected to NSO Group, an Israel-based "cyber war" company that sells *Pegasus*, a government-exclusive "lawful intercept" spyware product. NSO Group is reportedly owned by an American venture capital firm, Francisco Partners Management. The ensuing investigation, a collaboration between researchers from Citizen Lab and from Lookout Security, determined that the links led to a chain of zero-day exploits ("zero-days") that would have remotely jailbroken Mansoor's stock iPhone 6 and installed sophisticated spyware. We are calling this exploit chain Trident. Once infected, Mansoor's phone would have become a digital spy in his pocket, capable of employing his iPhone's camera and microphone to snoop 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. We are not aware of any previous instance of an iPhone remote jailbreak used in the wild as part of a targeted attack campaign, making this a rare find. CVE-2016-4657: Visiting a maliciously crafted website may lead to arbitrary code execution CVE-2016-4655: An application may be able to disclose kernel memory. <u>CVE-2016-4656</u>: An application may be able to execute arbitrary code with ke Once we confirmed the presence of what appeared to be iOS zero-days, Citizen Lab and Lookout quickly initiated a responsible disclosure process by notifying Apple and sharing our findings. Apple responded promptly, and notified us that they would be addressing the vulnerabilities. We are releasing this report to coincide with the availability of the iOS 9.3.5 patch, which blocks the Trident exploit chain by closing the vulnerabilities that NSO Group appears to have exploited and sold to remotely compromise iPhones Recent Citizen Lab research has shown that many state-sponsored spyware campaigns against civil society groups and human rights defenders use "just enough" technical sophistication, coupled with carefully planned deception. This case demonstrates that not all threats follow this pattern. The iPhone has a well-deserved reputation for security. As the iPhone platform is tightly controlled by Apple, technically sophisticated exploits are often required to enable the remote installation and operation of iPhone monitoring tools These exploits are rare and expensive. Firms that specialize in acquiring zero-days often pay handsomely for iPhone exploits. One such firm, Zerodium, acquired an exploit chain similar to the Trident for one million dollars in November 2015. The high cost of iPhone zero-days, the apparent use of NSO Group's government-exclusive Pegasus product, and prior known targeting of Mansoor by the UAE government provide indicators that point to the UAE government as the likely operator behind the targeting. Remarkably, this case marks the *third* commercial "lawful intercept" spyware suite employed in attempts to compromise Mansoor. In 2011, he was targeted with FinFisher's FinSpy spyware, and in 2012 he was targeted with Hacking Team's Remote Control System. Both Hacking Team and FinFisher have been the object of several years of revelations highlighting the misuse of spyware to compromise civil society groups, journalists, and THREE "LAWFUL INTERCEPT" PRODUCTS USED AGAINST MANSOOR lackina**Team**l FINFISHER CITIZEN LAB 2016 Figure 1: Ahmed Mansoor, the "Million Dollar Dissident." The attack on Mansoor is further evidence that "lawful intercept" spyware has significant abuse potential, and that some governments cannot resist the temptation to use such tools highlight the continuing lack of effective human rights policies and due diligence at spyware companies, and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuses of "lawful intercept" and the continuing lack of incentives to address abuse and the continuing lack of incentives to address abuse and the continuing lack of the conspyware. Our report proceeds as follows: • Section 2 provides an overview of the attack against Ahmed Mansoon. • Section 3 details NSO Group's tradecraft, gleaned from what appears to be a copy of NSO Group documentation leaked in the Hacking Team emails. • Section 4 summarizes our technical analysis of the attack against Mansoor (in collaboration with Lookout). Section 5 describes how we found what appears to be the NSO Group's mobile attack infrastructure while working on our previous <u>Stealth Falcon</u> report. Section 6 links the spyware used in the attack on Mansoor to NSO Group Section 7 outlines evidence of other individuals targeted with the infrastructure that we linked to NSO Group, including Mexican journalist Rafael Cabrera. Section 8 explains how the attack on Mansoor fits into the context of ongoing attacks on UAF dissidents • Section 9 concludes the report. 2. Ahmed Mansoor Targeted With iPhone Zero-Day Ahmed Mansoor is an internationally recognized human rights defender, blogger, and member of Human Rights Watch's advisory committee. Mansoor, who is based in the UAE, was jailed for eight months in 2011 along with four other activists for supporting a prodemocracy petition. After he was released, Mansoor's passport was confiscated, his car was stolen, and \$140,000 disappeared from his bank account. Mansoor is banned from traveling overseas, and his work continues to attract significant harassment and punishment 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. Figure 2: Ahmed Mansoor received suspicious text messages in August 2016. Credit: Martin Ennals Mansoor quickly forwarded the messages to Citizen Lab researchers for investigation. He has good reason to be concerned about unsolicited messages: every year since 2011, Mansoor has been targeted with spyware attacks, including with FinFisher spyware in 2011 and Hacking Team spyware in 2012 (see Section 8: Ahmed Mansoor and Previous UAE Attacks). Messages (6) InfoSMS Back (6) +45 609910233 Text Message Today 1:44 PM أسرار جديدة عن تعنيب إماراتيين في سجون الدولة : //.https:// /sms.webadv.co أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : <u>//:https</u> /<u>sms.webadv.co</u> 3589003s/ 9573305s/ Figure 3: SMS text messages received by Mansoor (English: "New secrets about torture of Emiratis in state When Mansoor's messages reached us, we recognized the links: the domain name webadv.co belongs to a network of domains that we believe to be part of an exploit infrastructure provided by the spyware company NSO Group (see **Section 6: Linking NSO Group Products to the Attack on Mansoor**). We had first come across the NSO Group infrastructure during the course of our earlier research into Stealth Falcon, a UAE-based threat actor (see Section 5: Tracking a Mobile Attack Infrastructure) When we first found the infrastructure and connected it to NSO Group, we hypothesized that operators of the NSO Group spyware would target a user by sending them an infection link containing one of the exploit infrastructure domain names. Though we had previously found several public occurrences of links involving these domains on Twitter (see Section 7: Evidence of Other Targets), none of the links we found seemed to be active (i.e., none produced an infection when we tested them). In other exploit infrastructures with which we are familiar (e.g., Hacking Team's exploit infrastructure), we had noted that operators prefer to deactivate such links after a single click, or after a short period of time, perhaps in order to prevent the disclosure of the exploit to security researchers We accessed the link Mansoor provided us on our own stock factory-reset iPhone ${\bf 5}$ (Mansoor had an iPhone 6) with iOS 9 3 3 (the same version as Mansoor). When we clicked the link, we saw that it was indeed active, and watched as unknown software was remotely implanted on our phone. This suggested that the link contained a zero-day iPhone remote jailbreak: a chain of heretofore unknown exploits used to remotely circumvent iPhone security measures. To verify our observations, we shared our findings with Lookout Security. Both research teams determined that Mansoor was targeted with a zero-day iPhone remote jailbreak. The chain of exploits, which we are calling the Trident, included the following (see Section 4: The Trident iOS Exploit Chain and Payload for more details): • <u>CVE-2016-4657</u>: 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 The implant installed by the Trident exploit chain would have turned Mansoor's iPhone into a digital spy in his pocket. The spyware, which appears to be NSO's Pegasus spyware solution, was capable of employing his 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. 3. NSO Group and the Pegasus Solution The attack on Mansoor appears to have used Pegasus, a remote monitoring solution sold by NSO Group Technologies Ltd (see Section 6: Linking NSO Group Products to the Attack on Mansoor). NSO Group, based in Herzelia, Israel (CR# 514395409), develops and sells mobile phone surveillance software to governments around the world. The company describes itself as a "leader" in "mobile and cellular Cyber Warfare," and has been operating for more than six years since its founding in 2010. NSO Group appears to be owned by a private equity firm with headquarters in San Francisco: Francisco Partners Management LLC, which reportedly acquired it in 2014 after approval from the Israeli Defense Ministry. However, as of November 2015, Francisco Partners was <u>reportedly exploring</u> selling NSO Group, with a stated valuation of up to \$1 billion. Interestingly, Francisco Partners previously <u>invested in Blue Coat</u>, a company selling network filtering and monitoring solutions, whose technology has been used by repressive regimes according to previous Citizen Lab research. **NSO GROUP** Figure 4: Image from an NSO Group brochure posted on SIBAT (The International Defense ration Directorate of the Israel Ministry of Defense). NSO Group has largely avoided the kind of high profile media attention that companies like Hacking Team and FinFisher have sometimes courted. The company maintains no website, there is little concrete information about NSO Group's Pegasus product available online and we know of no prior technical analysis of NSO Group's products or infrastructure Some previous media reports have linked <u>NSO Group and Pegasus</u> to a scandal involving potential illegal eavesdropping in Panama, and possible <u>sales to Mexico</u>. Other reports have suggested that NSO Group's activities have <u>aroused concern within the United States</u> Two of NSO Group's three co-founders, Shaley Hulio and Omri Lavie, are also co-founders of mobile security company Kaymera, which promises a "Multi Layered Cyber Defense Approach" to clients. On Kaymera's website, the company reprints a Bloomberg article pointing out that they "play both sides of the cyber wars." The article also quotes NSO Group's CEO, who suggests that they entered the defense business when potential clients saw the capabilities of NSO Group's tools. COMPREHENSIVE MULTI-PURPOSED MOBILE SECURITY Figure 5: Kaymera's website promises comprehensive mobile security 3.1. Pegasus Documents in Hacking Team Leak Much of the publicly available information about Pegasus seems to be rumor, conjecture, or unverifiable claims made to media about capabilities. However, when we examined the Hacking Team emails leaked online after a 2015 breach, we found several instances of Hacking Team clients or resellers sharing what appeared to be NSO Group's product documentation and sales pitches For instance, in December 2014, a reseller of surveillance technologies to the Mexican government forwarded a PDF document containing detailed technical specifications of NSO Group's Pegasus system to Hacking Team. According to the document's metadata, it appears to have been created in December 2013 by Guy Molho, who is <u>listed on LinkedIn</u> as the Director of Product Management at NSO Group. 3.2. Device Infection According to the purported 2013 NSO Group Pegasus documentation found in the Hacking Team materials, NSO Group offers two remote installation vectors for spyware onto a target's device: a zero-click vector, and a one-click vector. The one-click vector involves sending the target a normal SMS text message with a link to a malicious website. The malicious website contains an exploit for the web browser on the target's device, and any other required exploits to implant the spyware. In the attack against Mansoor, the Trident exploit chain was used. To use NSO Group's zero-click vector, an operator instead sends the same link via a special type of SMS message, like a WAP Push Service Loading (SL) message. A WAP Push SL message causes a phone to automatically open a link in a web browser instance, eliminating the need for a user to click on the link to become infected. Many newer models of phones have started ignoring or restricting WAP Push messages. Mobile network providers may also decide to block these messages Figure 6: Diagram from purported NSO Group Pegasus documentation showing the sequence through which the spyware ("Agent") is installed on a target's mobile device. Source: Hacking Team The documentation refers to a malicious website employed in installation of the spyware ("Agent") as an Anonymizer, which communicates with a Pegasus Installation Server located on the operator's premises. When a target visits a malicious link from their device, the Anonymizer forwards the request to the Pegasus Installation Server, which examines the $target \, device's \, \underline{User-Agent} \, \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, header \, to \, determine \, if \, Pegasus \, has \, an \, exploit \, chain, \, such \, as \, the \, device's \, \underline{User-Agent} \, header \, to \, determine \, device's \, \underline{User-Agent} \, header \, to \, determine \, device's \, \underline{User-Agent} \, header \, to \, determine \, device's \, \underline{User-Agent} \, header \, to \, determine \, device's \, \underline{User-Agent} \, header \, to \, device's \, \underline{User-Agent} \, header \, \underline$ Trident, that supports the device. If the device is supported, the Pegasus Installation Server returns the appropriate exploit to the target device through the Anonymizer and attempts an infection. If infection fails for any reason, the target's web browser will redirect to a legitimate website specified by the Pegasus operator, in order to avoid arousing the target's suspicion. In the operation targeting Mansoor, the one-click vector was used, with anonymizer sms.webadv.co (see Section 4: The Trident iOS Exploit Chain and Payload for more 3.3. Data Collection According to the purported NSO Group documentation, once successfully implanted on a phone using an exploit chain like the Trident. Pegasus can actively record or passively gather a variety of different data about the device. By giving full access to the phone's files, messages, microphone and video camera, the operator is able to turn the device into a silent digital spy in the target's pocket. Figure 7: Diagram from purported NSO Group Pegasus documentation showing the range of information gathered from a device infected with Pegasus. Source: Hacking Team Emails. In the spyware used in targeting Mansoor, we confirmed many elements of this functionality. and observed indications that the collection of the following types of data was supported, among others (see Section 4.2: The Payload for more details): • Calls made by phone, WhatsApp and Viber, • SMS messages, as well as messages and other data from popular apps like Gmail, WhatsApp, Skype, Facebook, KakaoTalk, Telegram, and others, • A wide range of personal data, such as calendar data and contact lists, as well as passwords, including Wi-Fi passwords. 3.4. Exfiltration According to the purported NSO Group documentation, an infected device transmits collected information back to a Pegasus Data Server at the operator's premises, via the PATN (Pegasus Anonymizing Transmission Network). The PATN appears to be a proxy chain system similar to Hacking Team's anonymizers and FinFisher's relays. The chain is intended to obfuscate the identity of the government client associated with a particular operation. Once the collected information arrives on the Pegasus Data Server, an operator may visualize the information on a Pegasus Working Station. ire 8: A purported screenshot of NSO Group's Pegasus Working Station software, which visualizes m infected devices (as of March 2012). Source: Hacking Team Emails. The implant in the attack targeting Mansoor communicated with two PATN nodes: aalaan.tv and manoraonline.net. The first of these, aalaan.tv, appears to be a lookalike domain for the legitimate <u>alaan.tv</u>, a Gulf-based satellite television channel (see **Section 5.2** for more details on lookalike domains observed in apparent NSO Group infrastructure). 3.5. Prioritizing Stealth One interesting design decision of NSO Group's Pegasus system, according to the purported NSO Group documentation, is that it emphasizes stealth above almost all else. As the documentation states: ve understand that it is more important that the source will not be exposed and the target will suspect nothing than keeping the agent alive and $Certain\ Pegasus\ features\ are\ only\ enabled\ when\ the\ device\ is\ idle\ and\ the\ screen\ is\ off,\ such$ as "environmental sound recording" (hot mic) and "photo taking." The documentation also states that the spyware implements a "self-destruct mechanism," which may be activated automatically "in cases where a great probability of exposing the agent exists." However, the documentation claims that sometimes Pegasus removal can result in an infected device rebooting immediately after removal. 4. The Trident iOS Exploit Chain and Payload In this section, we describe our technical analysis of the attack on Mansoor, including the Trident iOS Exploit chain and payload. Given the accelerated timeframe of this case, we are publishing the results of a preliminary analysis. Recall that the investigation that led to the discovery of the Trident exploit chain began when UAE human rights activist Ahmed Mansoor forwarded to Citizen Lab two suspicious links that he received via SMS on his iPhone (Section 2). Suspecting the links to be iPhone spyware associated with NSO Group (Section 6), we accessed them from our own stock factory-reset iPhone 5 running iOS 9.3.3. Mansoor's device is an iPhone 6, running iOS 9.3.3; we did not have an iPhone 6 available for testing. Although the latest iOS version when Mansoor received the links was 9.3.4, this version had been released only <u>one week</u> We accessed the links by opening Safari on our iPhone, and manually transcribing the links from the screenshots that Mansoor sent. After about ten seconds of navigating to the URL, which displayed a blank page, the Safari window closed, and we observed no further visual activity on the iPhone's screen. Meanwhile, we saw that the phone was served what appeared to be a Safari exploit, followed by intermediate files (final111), and a final $payload \ (\textbf{test111.tar}). \ The \ first \ two \ payloads \ form \ the \ Trident \ exploit \ chain, \ and \ test111.tar)$ is the payload. f_gog.html?a=568_320_2_5GX543&b=______&nocach (application/octet-stream) f_gog.html?a=568_320_2_5GX543&b=3&nocache= tf_brc.html?m=0 HTTP/1.1 ktf_bed.html?s====&&d=Tring%20to%20download%20bundle%28try%3A0%29 HTTP/1.1 /test111.tar HTTP/1.1 conducted by a stage2 binary (in final111). All previous requests are conducted by Safari. Suspecting what we had observed to be the work of a zero-day iPhone remote jailbreak, we shared the exploit and payloads with colleagues at Lookout Security, initiated a responsible disclosure process with Apple, and sent Apple the exploit and payloads 4.1. The Trident Exploit Chain This section provides a high-level overview of the Trident exploit chain used in the attack against Mansoor. For further details, see Lookout's report. When a user opens the links sent to Mansoor on an iPhone, a stage1 containing obfuscated JavaScript is downloaded. The JavaScript downloads (via XMLHttpRequest) stage2 binaries for either 32-bit (iPhone 5 and earlier) or 64-bit (iPhone 5s and later), depending on the type of device. The stage 1 employs a previously undocumented memory corruption vulnerability in WebKit to execute this code within the context of the Safari browser (CVF-2016-4657). The stage2 exploits a function that returns a kernel memory address, from which the base address of the kernel can be mapped (CVE-2016-4655). The stage2 then employs a memory corruption vulnerability in the kernel (CVE-2016-4656). This last vulnerability is employed to disable code signing enforcement, allowing the running of unsigned binaries. The stage2 downloads and installs the stage3, which is the spyware payload. 4.2. The Payload This section provides a high-level overview of the functionality of the spyware payload. For more details, see Lookout's report. 4.2.1. Persistence The Trident is re-run locally on the phone at each boot, using the JavaScriptCore binary. To facilitate persistence, the spyware disables Apple's automatic updates, and detects and removes other jailbreaks The attack payload includes a renamed copy of Cydia Substrate, a third-party app developed $framework, which it uses to help facilitate \, recording \, of \, messages \, and \, phone \, calls \, from \, calls$ $targeted\ apps.\ \ To\ record\ Whats App\ and\ Viber\ calls,\ the\ spyware\ injects\ Whats App\ and\ Viber\ calls,$ using the Cydia Substrate, hooks various call status methods, and sends system-wide notifications when call events occur; the spyware listens for these notifications and starts or stops recording as appropriate. It appears that the payload can spy on apps including: iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype, Line, KakaoTalk, WeChat, Surespot, Imo.im, Mail.Ru, Tango, VK, and Odnoklassniki. The spyware also exfiltrates calendar and contact data, as well as passwords saved in the phone's keychain, including Wi-Fi passwords and networks. 4.2.3. Exfiltration The attack payload beacons back to command and control (C2) servers delivered in stage2 of the Trident, via HTTPS. One of the binaries in the stage2 of the link sent to Mansoor contained the following string: The Base64 string decodes to: ==&i=MTphYWxhYW4udHY6NDQzLDE6bWFub3Jhb25saW51Lm51dDo0NDM=&s=zpvzPSYS674= This appears designed to look like a text message from Google containing a two-factor authentication code, though legitimate Google messages of this type do not contain a link. and contain one fewer digit in the verification code. Base64-decoding the "i" parameter of 1:aalaan.tv:443,1:manoraonline.net:443 These are the C2 servers for the spyware sent to Mansoor: ${\bf aalaan.tv}$ and A similar obfuscation appears to be used for exchange of information over SMS between an infected phone and the C2 Server. In case the spyware's C2 servers are disabled or unreachable, an operator may deliver updated C2 servers to an infection using this type of SMS, similar to FinFisher's "emergency configuration update" functionality 5. Tracking a Mobile Attack Infrastructure This section explains how we first identified what appeared to be a mobile attack infrastructure while tracking Stealth Falcon. We then outline some basic observations about the infrastructure, including themes in the domain names used by the attackers. We link the infrastructure we found to NSO Group in **Section 6**. 5.1. Stealth Falcon Leads Us to a Mobile Attack Infrastructure A year or so before Ahmed Mansoor received his suspicious SMS messages, we were tracking <u>Stealth Falcon</u>, a threat actor targeting individuals critical of the UAE government at home and abroad, several of whom were later arrested. For full details on Stealth Falcon, read our May 2016 report. In the course of our investigation, we traced Stealth Falcon's spyware to dozens of different command and control (C2) domains. One server that matched our C2 fingerprint for Stealth Falcon's custom spyware, **icloudcacher.com**, was connected to the email address pn1g3p@sigaint.org, according to data in its DNS SOA record. The same email address appeared in WHOIS records for the following three domains: These domains did not match our Stealth Falcon fingerprint. As we examined the domains, however, we found that the index page on these domains contained an iframe pointing to the website as rarabiya.com (Asrar Arabiya, or "Arabian Secrets" in English), which appears to be a benign website that takes a critical view of the Arab World's "dictatorships." The index page also contained a nearly invisible iframe pointing to an odd looking site, smser.net. <iframe src="https://smser.net/9918216t/" width="1" height="1" border="0"></iframe>
<iframe src="http://saraarabiya.com/" style="width:100%; height:1200px; position:absolute; top:-5px; left:-5px; "border="0"></iframe> Figure 10 : HTML content of the index page on the three fake "Asrar Arabiya" domains We suspect that the three domains we identified were attempting to mislead users into believing they were visiting the legitimate as rararabiya. com website. Since we had linked the operation to Stealth Falcon, we suspected that the additional domain, **smser.net**, might be an attack domain. We visited the URL in the iframe, https://smser.net/9918216t/, and were redirected to https://smser.net/redirect.aspx. Figure 11: HTML content of https://smser.net/redirect.aspx. The page tells the web browser to redirect the We devised a number of fingerprints for various behaviors of smser.net, checked Shodan and Censys, and conducted our own scanning with zmap to identify related servers. We found 237 live IP addresses, and extracted their domain names from the SSL certificates returned by the each server. The SSL certificates we found included *.webadv.co, manoraonline.net, and aalaan.tv, the three domains in the spyware attack sent to We linked these IPs and domain names to what appears to be NSO Group exploit infrastructure. 5.2. Coding the Domain Names We coded the domain names we found, and identified several common themes, perhaps indicating the type of bait content that targets would receive. Interestingly, the most common theme among the domains we identified was "News Media," perhaps indicating the use of fake news articles to trick targets into clicking on spyware links. An example of one such attack in action is the targeting of Mexican journalist Rafael Cabrera (Section 7.1). We also noted the prevalence of themes we had seen in other spearphishing attacks, e.g., online accounts, document sharing, shipment tracking, corporate account portals. Another common theme was ISPs, perhaps because a target may trust an SMS appearing to come $\,$ from an ISP or Telco they subscribe to. **LOOKALIKES & THEMES IN EXPLOIT INFRA. NAMES** ■ ECOMMERCE ■ UNSUBSCRIBE ■ ACCOUNT INFORMATION SOCIAL NETWORKING **CITIZEN LAB 2016** Figure 12: Most commonly recurring domain name themes Alarmingly, some of the names suggested a willingness on the part of the operators to impersonate governments and international organizations. For example, we found 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. We also identified the domain **topcontactco.com** which may be a lookalike for tpcontact.co.uk, a website belonging to Teleperformance, a company that has managed UK visa application processing in many countries. 10) Once you have completed your visa application and made your appointment you must create an account on the Teleperformance website www.tpcontact.co.uk @.Failing to create an account on the Teleperformance website may delay your appointment at the visa application centre. Pick your resident country and click submit then Create an account. You can find your GWF xxxxxxxxx (reference) in the emails you have received from UKVI. Figure 13: Screenshot from an article published by the UK Government on how to apply for a visa. https://www.gov.uk/government/world-loca n-news/how-to-apply-for-a-uk Visa applicants are required to visit the legitimate tocontact.co.uk website as part of the online visa application process. We found similar evidence of government-themed sites The following table provides further examples of themes found in the domain names. cnn-africa.co CNN unonoticias.net univision.click Las Ultimas Noticias Shipment Tracking FedEx track-your-fedex-package.org Vodacom (Mozambique) iusacell-movil. com.mx Iusacell (Mexico) Sabafon (Yemen) newtarrifs.net Generic Popular Online fb-accounts.com Facebook googleplay-store.com whatsapp-app.com Google WhatsApp adjust-local-settings.com Teleperformance Visa Application Processing topcontactco.com Portal for the UK (tpcontact.co.uk.) International Committee of the Red Cross organizations redcrossworld.com checkinonlinehere.com, Generic Airlines turkishairines.info Turkish Airlines Pokemon The Pokemon Company pickuchu.com Table 1: Examples of domain names and themes We also examined the domain names for evidence of links to any specific country and found a range of countries. Our criteria was whether the domain name contained the name of a $telecom\ provider, ISP, local\ website, government\ service, geographic\ location, a\ country's$ TLD, or the name of a country The UAE and Mexico dominate this list, although other countries are also worth noting, including: Turkey, Israel, Thailand, Qatar, Kenya, Uzbekistan, Mozambique, Morocco, Yemen, Hungary, Saudi Arabia, Nigeria, and Bahrain. **COUNTRY THEMES IN EXPLOIT INFRASTRUCTURE NAMES** - UAE UZBEKISTAN ■ MOZAMBIQUE ■ KENYA ■ THAILAND ■ QATAR ■ ISRAEL ■ YEMEN MOROCCO SAUDI ARABIA **CITIZEN LAB 2016** Figure 14: Country theme based on domain name Citizen Lab is refraining from publishing a full list of domain names at this time given the possibility that some domains may have been used in legitimate law enforcement operations. 6. Linking NSO Group Products to the Attack on Mansoor use of NSO Group's Pegasus product. We explain how we connected the domain name in the link that Ahmed Mansoor received, sms.webadv.co. to a network of domain names that we had mapped out while working on the May 2016 Stealth Falcon report (Section 5). We also highlight links to the UAE. 6.1. Spyware Points to NSO Group's Pegasus Solution The final payload that we identified, test 111 tar, contained several files, including libaudio.dylib, which appeared to be the base library for call recording, libimo.dylib, which appeared to be the library for recording chat messages from apps, and two libraries for WhatsApp and Viber call recording: libvbcalls.dylib, and libwacalls.dylib. In each file, we found several hundred strings containing the text "_kPegasusProtocol," the name of NSO Group's solution. kPegasusProtocolAgentControlElement_iv kPegasusProtocolAgentControlElement_key kPegasusProtocolAgentControlElement_cip kPegasusProtocolProtocolElement_iv kPegasusProtocolProtocolElement_key Figure 15: "Pegasus" strings in the payload. 6.2. Historical Scanning Data Connects Mansoor Attack to NSO Group-linked Infrastructure The links sent to Mansoor used the domain **sms.webadv.co**. The network of 237 live IP addresses we mapped (Section 5) included 52.8.153.44, to which sms.webadv.co resolves and which returns an SSI certificate for *.webadv.co. The 237 IPs also included 52.8.52.166 (aalaan.tv) and 162.209.103.68 (manoraonline.net), which were the two C2 servers in the spyware used in targeting Mansoor. However, the 237 IPs and related domain names that we mapped did not provide insight $% \left(1\right) =\left(1\right) \left(1\right) \left($ into the identity of the threat actor. The IP addresses all appeared to be associated with cloud VPS providers, which gave no clue as to the identities of the operators, and the WHOIS information was mostly private. We did note that several domain names had WHOIS registrants based in Israel (e.g., thainews.asia, kenvasms.org). We examined historical scanning data to see whether we could attribute the 237 IPs to a threat actor. We noted that at least 19 of these IPs had previously returned a different distinctive Google redirect in response to a "GET /". Figure 16: Response to an HTTP GET exhibited by 19 IPs in historical scanning data (note that the first three bytes represent the unicode byte order mark — BOM). These 19 IPs included an IP address that (later) resolved to **manoraonline.net**, one of the C2 servers for the spyware sent to Mansoor We then searched the same historical data for other IP addresses that matched this same fingerprint. Overall, between October 2013 and September 2014, we identified 83 IPs that matched the fingerprint. We found several IPs of particular interest. The IP address 82.80.202.200 matched our fingerprint from October 2013 until April 2014 HTTP/1.1 200 OK

Content-Type: text/html
Last-Modified: Tue, 04 Jun 2013 15:28:04 GMT
Accept-Ranges: bytes
ETag: "09a91b3861cel:0"
Server: Microsoft-1187.5
Date: Mon, 28 Oct 2013 21:23:12 GMT
Connection: close
Content-Length: 127
Vacf\xbb\xbf-KTML>SHEAD>CMETA HTTP-EQUIV="refresh" CONTENT="0;URL=http://www.google.com/">
</RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></RODY></ri></ri> The domain name qaintqa.com pointed to this IP address at the same time (from April 2013 to April 2016), according to DomainTools. The registrant information for this domain is: We also found two other IP addresses of interest that matched the fingerprint: $\textbf{82.80.202.204} \text{ and } \textbf{54.251.49.214} \text{ matched the fingerprint in March 2014}. \text{ The former was } \textbf{10.202.204} \text{ and } \textbf{10.202.204} \text{ and } \textbf{10.202.204} \text{ matched the fingerprint in March 2014}. \text{ The former was } \textbf{10.202.204} \text{ matched the fingerprint in March 2014}. \textbf{10.202.204} \text{ matched 2014}. \textbf{10.202.204} \text{ m$ $pointed \ to \ by \ \textbf{mail1.nsogroup.com} \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ and \ an alternative \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2014-09-24 \ to \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2015-05-06 \ (Passive Total), \ the \ latter \ from \ 2015-05$ was pointed to by nsoqa.com from 2015-09-01 until present (DomainTools). Both domains are registered to NSO Group. Given these findings, we strongly suspected the network of domain names we uncovered was part of an exploit infrastructure for NSO Group's mobile spyware. 6.3. Additional UAE Infrastructure Recall that our first window into this infrastructure came from our Stealth Falcon research, when we identified the smser.net domain, fingerprinted it, and traced it to 237 live IP addresses that shared the same characteristics (Section 5.1). Using PassiveTotal, we were able to further trace smser.net to seven other domains, indicating Stealth Falcon targeting that appeared to use NSO Group's Pegasus solution in Qatar (ooredoodeals.com), UAE (alawaeltech.com, which may be a fake mobile phone company based in the Emirate of Ajman), and Bahrain (bahrainsms.co). Based on our $\underline{\text{previously published research}},$ we believe there is strong circumstantial evidence to support the conclusion that the operator of Stealth Falcon is connected to an entity within the LIAF Government We also identified five .ae TLDs that all shared the same registrant name ("Gerald Binord"), which may have been used to target people in the UAE. We further identified another group of domains including **damanhealth.online** ("Daman Health" is a <u>UAE-based health insurer</u>) and uaenews.online, which also included a domain turkeynewsupdates.com, suggesting an operator that is targeting both UAE and Turkey targets. 7. Evidence of Other Targets In two cases, Mexico and Kenya, we found evidence of other targets who may have been $targeted\ with\ NSO\ Group's\ Pegasus,\ based\ on\ messages\ they\ sent\ or\ received\ containing$ links that involve domain names we traced to what appears to be a mobile attack infrastructure associated with NSO Group's Pegasus (see **Section 5: Tracking a Mobile** Attack Infrastructure 7.1. Mexico: Politically Motivated Targeting? In the case of Mexico, one target appears to be the journalist Rafael Cabrera, who recently reported on the Casa Blanca controversy, a reported conflict of interest involving the President and First Lady of Mexico. On August 30, 2015 the journalist Cabrera $\underline{\text{tweeted}}$ that he had received suspicious messages purporting to come from Mexican television station **UNO TV**. His tweet included screencaptures of the messages, which said that Mexico's Presidency was considering defamation claims and imprisonment of reporters related to the Casa Blanca report that Cabrera had worked on. Rafael Cabrera Me han llegado estos dos supuestos mensajes de UnoTV desde este número: (55) 6106 7277. No es gracioso UNOTV.COM/ POR TEMA DE CASA PRESIDENCIA BLANCA PRESIDENCIA PODRIA ENCARCELAR DEMANDARA POR **REPORTEROS** DUIENES MIENTRAS INVESTIGA VER NOMBRES: http:// PUBLICARON REPORTAJE DE LA bit.ly/1LLY8oK CASA BLANCA. NOTA: Mensaje de texto 155 38 8:35 AM - 30 Aug 2015 Figure 17: Messages purporting to come from UNO TV suggesting that a story he was linked to might result in defamation charges or incarceration. Image via Mexican journalist Rafael Cabrera's tw The English translations of the messages are as follows: UNOTV.COM/ THE PRESIDENT'S OFFICE WILL SUE FOR DEFAMATION THOSE WHO PUBLISH REPORTING ON CASA BLANCA. NOTE: [MALICIOUS LINK] UNOTV.COM/ ON THE TOPIC OF THE CASA BLANCA, THE PRESIDENCY COULD INCARCERATE REPORTERS WHILE THEY LOOK INTO THE NAMES: [MALICIOUS LINK] The links in the screenshots expand to http://fb-accounts.com/1074139s/ and http://unonoticias.net/3423768s/. These match two domain names we linked to the apparent NSO Group infrastructure. A director at UNO TV responded to Cabrera's Tweet. saying that these were "...not our messages 100%." Luis Vázquez Fabris

©ELSABRIS @Tomoo_Terada @CeciFonsecaM @raflescabrera @UnoNoticias @ELSABRIS @AntonioUNOTV no son nuestros los mensajes 100% View trans 10:39 AM - 30 Aug 2015 Figure 18: A director from UNO TV states that the suspicious SMS messages sent to Cabrera were not from his company. Image via Twitter We were unable to achieve a successful infection from either link sent to Cabrera. presumably because the links were several months old when we found them, and had been clicked on either by Cabrera himself, or by other interested parties who saw Cabrera's tweet. Continuing our investigation, we made contact with Cabrera and learned that he had been recently targeted with an additional series of messages containing suspicious links. Mensajes (81) 2075 4118 Detalles Mensajes (55) 6108 9094 Detalles LINOTY COM/ PODRIA Facebook reporta IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN intentos de acceso a la cuenta: Rafa Cabrera. Evite bloqueo de cuenta, verifique en: 2018. DETALLES: https://fb-2408931s/ Mensajes (81) 2095 3203 Detalles TELCEL.COM/ ESTIMADO USUARIO tienes los huevos de ver como fajo a tu pareja. Mira nada mas no cojemos bn rico y en tu na: http://bit.ly/246dkRy LE RECORDAMOS QUE PRESENTA UN ADEUDO DE \$8,854.90 M/N VERIFICLIE DETALLES: https s-telcel.com.mx/ 3975827s/ Figure 19: Additional SMS messages sent to Rafael Cabrera containing links to the exploit infrastructure The English translations of the messages are as follows (clockwise from top-left): ok reports efforts to access the account of: Rafael Cabrara. Avoid account blockage, Verify at: UNOTV.COM/ CARMEN ARISTEGUI MAY RUN AS AN INDEPENDENT CANDIDATE IN 2018. DETAILS: [MALICIOUS TELCEL.COM/. DEAR CLIENT WE REMIND YOU THAT YOU HAVE AN OUTSTANDING DEBT OF \$8,854.90 IN NATIONAL CURRENCY. TO VERIFY DETAILS [MALICIOUS LINK] [CL Note: this message contains highly profane sexual taunts, followed by a malicious link] The fourth message is most noteworthy, as it contained profane and personal sexual taunts, unlike the other messages. Each of these messages contained a link that would have led, we believe, to the infection of his iPhone with NSO Group's Pegasus spyware via the Trident Similar SMS messages have also been reported in other online posts from Mexico. 7.2. Kenya: A Tweet Discussing the Opposition In the case of Kenya, we found a past tweet containing a link to the NSO Group exploit infrastructure from June 3, 2015. The tweet, sent by a "Senior Research Officer" in the Office of the Senate Minority Leader, references $\underline{\mathsf{Moses}\,\mathsf{Wetangula}}$, who is the current Minority Leader of Kenya's Senate Kachu wa Sisungo Senate Minority leader Moses Wetangula nominated by Inter-Parliamentary Union for top achiever award nation-news.com/4077017s/ @BikoObimbo 5:48 AM - 3 Jun 2015 Figure 20: A Kenya-related link to apparent NSO Group infrastructure. 8. Ahmed Mansoor and Previous UAE Attacks In this section, we provide an overview of previous attacks we have documented against Ahmed Mansoor, and other UAE dissidents. The technical sophistication of previous attacks we observed pales in comparison to the present attack. Ahmed Mansoor has been a frequent target of past electronic attacks. In March 2011, he was targeted with FinFisher spyware disguised as a PDF of a pro-democracy petition he had previously signed. The spyware arrived in the form of an executable file inside a .rar file attached to an email. Mansoor noticed that the file was an EXE file rather than a PDF, and did not open it. Mansoor and four other activists (the "UAE Five") were imprisoned in April 2011, and charged with insulting the leaders of the UAE. Mansoor and the others were pardoned in November of the same year. In July of 2012, Ahmed Mansoor's laptop was infected with Hacking Team spyware delivered via a booby-trapped Microsoft Word document exploiting an old Microsoft Office vulnerability, CVE 2010-3333. The spyware sent information from his computer to a UAE intelligence agency, apparently operating under the auspices of the office of Sheikh Tahnoon bin Zayed al-Nahyan, a son of the founder of the UAE, and now the UAE Deputy National Security Advisor. Attackers broke into Mansoor's email account shortly after the infection. We assisted Mansoor in recovering from the attack. Another UAE-based human rights activist, and a UAE-based journalist were also targeted in the same operation. In early 2013, Mansoor was sent a link to a website that attempted to install spyware on his computer by exploiting a public Java vulnerability for which no patch had yet been issued. He realized the link was suspicious and did not click on it. Throughout 2013 and 2014, Mansoor was unsuccessfully targeted several times with spyware, mostly XTremeRAT, SpyNet RAT, and niRAT delivered as executable files in attachments or through Google Drive links. In 2014, Mansoor's Twitter account was hacked In a campaign stretching from 2012 until 2016, UAE dissidents at home and abroad were targeted by Stealth Falcon, an attacker likely linked to a UAE government agency. Stealth $Falcon \ sent \ out \ links \ involving \ a \ fake \ URL \ shortener \ that \ employed \ Javascript \ to \ profile$ targets' computers, checked which antivirus programs they had installed, and attempted to deanonymize them if they were using Tor. Stealth Falcon also sent out Microsoft Word documents containing custom spyware that was installed if a user enabled macros. Targets included five dissidents who were later arrested or convicted in absentia, as well as Rori Donaghy, a UK-based journalist who had been publishing articles about leaked emails involving members of the UAE government. 9. Conclusion In this report, we identify a highly technically sophisticated attack involving a zero-day $iPhone\ remote\ jailbreak-Trident-which\ installs\ spyware\ on\ a\ phone\ whose\ user\ clicks$ just once on a malicious link. We connected the attack to NSO Group's Pegasus spyware suite, sold exclusively to government agencies by Israel-based NSO Group. We made the $\ensuremath{\mathsf{NSO}}$ connection based on our previous work tracing a group of servers that appeared to be part of an infrastructure for attacking mobile phones. Long before Ahmed Mansoor had forwarded us any suspicious links he received, we had mapped out a set of 237 servers (Section 5), and linked this set to NSO Group (Section 6). When Mansoor sent us screencaptures of the SMS messages containing the links, we immediately matched the links' domain name to our list of suspected servers associated with NSO Group's Pegasus We visited the links Mansoor sent us from a colleague's factory-reset stock iPhone, and managed to capture the exploits and payload, as the phone was infected. We shared these artifacts with Lookout to gain more insight into the technical capabilities of the exploits and spyware, and with Apple as part of a responsible disclosure process. Apple has been highly responsive, and has worked very quickly to develop and issue a patch in the form of iOS 9.3.5, approximately 10 days after our initial report to them. Once an iPhone is updated to this most recent version, it will be immediately protected against the Trident exploit chain used in this attack. While we assume that NSO Group and others will continue to develop replacements for the Trident, we hope that our experience encourages other researchers to promptly and responsibly disclose such vulnerabilities to Apple and to other vendors. All iPhone owners should update to the latest version of iOS (9.3.5) immediately. If you're unsure what version you're running, you can <u>check it yourself</u> by tapping **Settings** > **General** > **About** > **Ve** Citizen Lab agrees with Apple that users should avoid opening or downloading items from messages and cluzen Lau <u>agrees with appar</u> that user's should avoid opening of uovinoading terms from messages and websites unless they are certain that they come from a legitimate, trusted source. If you uncertain about the source, you <u>should not click the link or open the file</u>. If you believe you have been the victim of a targeted attack, should consider sharing it with a trusted expert. If you suspect you have been the target of this attack, please contact the Citizen Lab at info@citizenlab.org. Zero-day exploits are expensive and rare, especially one-click remote jailbreak exploits for iPhones, like the Trident. Such exploits can fetch <u>hundreds of thousands</u> or even a <u>million</u> dollars. While Citizen Lab research has shown that many state-sponsored spyware campaigns against civil society groups and human rights defenders use "just enough" technical sophistication, coupled with carefully planned deception, the attack on Mansoor demonstrates that not all threats follow this pattern. This is the third time Mansoor has been targeted with "lawful intercept" spyware; Mansoor was targeted in 2011 with spyware from FinFisher (based in Germany and the UK), in 2012 with spyware from Hacking Team (based in Italy), and now in 2016 with what appears to be spyware from NSO Group (based in Israel and reportedly owned by a US firm). That the companies whose spyware was used to target Mansoor are all owned and operated from democracies speaks volumes about the lack of accountability and effective regulation in the cross-border commercial spyware trade. While these spyware tools are developed in democracies, they continue to be sold to $countries\ with\ notorious\ records\ of\ abusive\ targeting\ of\ human\ rights\ defenders.\ Such\ sales$ occur despite the existence of applicable export controls. For example, Israel's export regime incorporates the dual-use technology controls of the Wassenaar Arrangement, including those related to "intrusion software." As such, NSO Group would presumably be required to obtain a license to export its products to the UAE. If NSO Group did submit a license application, the human rights abuses perpetrated by the UAE, including the misuse $\frac{1}{2}$ of "lawful intercept" capabilities, must not have outweighed authorities' other motivations Clearly, additional legal and regulatory scrutiny of the the "lawful intercept" market, and of NSO Group's activities in relation to the attacks we have described, is essential. Citizen Lab and others have repeatedly demonstrated that advanced "lawful intercept" spyware and others have repeatedly demonstrated that advanced "lawful intercept" spyware and others have repeatedly demonstrated that advanced "lawful intercept" spyware and others have repeatedly demonstrated that advanced "lawful intercept" spyware and others have repeatedly demonstrated that advanced "lawful intercept" spyware and others have repeatedly demonstrated that advanced "lawful intercept" spyware and other spyware and spyware and other spyware enables some governments and agencies, especially those operating without strong $\,$ over sight, to target and harass journalists, activists and human rights workers. If spywards and human rights workers are significant to the significant properties of the significant $companies \ are \ unwilling \ to \ recognize \ the \ role \ that \ their \ products \ play \ in \ undermining \ the \ role \ that \ their \ products \ play \ in \ undermining \ the \ role \ that \ their \ products \ play \ in \ undermining \ the \ role \ that \ their \ products \ play \ in \ undermining \ the \ role \ that \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ undermining \ the \ their \ products \ play \ in \ products \ play \ in \ play \ pl$ human rights, or address these urgent concerns, they will continue to strengthen the case for further intervention by governments and other stakeholders. Note: We are not releasing the malicious files at this time to protect the integrity of ongoing **Acknowledgements** Special thanks to the team at Lookout that we collaborated with in our investigation, especially: Max Bazaliy, Andrew Blaich, Kristy Edwards, Michael Flossman, Seth Hardy, and Very special thanks to our talented Citizen Lab colleagues, especially: Ron Deibert, Sarah McKune, Claudio Guarnieri, Adam Senft, Irene Poetranto, and Masashi Nishihata Special thanks to the teams at Apple Inc. with whom we have been in contact for their prompt and forthright engagement during the disclosure and patching process Special thanks to Nicholas Weaver for supplying the iPhone that we infected in Section 4.Special thanks to Zakir Durumeric Special thanks to TNG and others who provided invaluable assistance, including with translation, but requested to remain anonymous. Citizen Lab's research into targeted threats against civil society is supported by the $\underline{\mathsf{John}\,\mathsf{D}}$ and Catherine T MacArthur Foundation. This material is also based upon work supported by the Center for Long Term Cybersecurity (CLTC) at UC Berkeley. **Disclosure Timeline** Citizen Lab researchers received the initial suspicious link on August 10th 2016, and, shortly thereafter, contacted Lookout Security. After both teams confirmed the presence of a remote jailbreak we initiated a responsible disclosure process and contacted Apple on Teams from Citizen Lab and Lookout continued our analysis until the public release of iOS 9.3.5 by Apple, which closes the vulnerabilities that we disclosed. **Media Mentions** <u>The New York Times, Motherboard, Motherboard</u> (2), <u>Motherboard</u> (3), <u>Motherboard</u> (4), <u>Gizmodo</u>, <u>Wired</u>, <u>Washington Post</u>, <u>The Guardian</u>, <u>ZDNet</u>, <u>CBC Metro Morning</u> (audio), Associated Press (video), Mashable, Foreign Policy, Reuters, CPJ, National Post, Quartz, Ars Technica, Wall Street Journal, Wall Street Journal (2), BBC News, BBC News (2), The Independent, TechCrunch, CBC News, CBC News (2), Telegraph, Business Insider, Business Insider (2), Al Jazeera, South China Morning Post, SC Magazine, ABC Australia, The Next Web, Russia Today, Xinhua, The Journal Ireland, The Australian, International Business Times, Buzz Feed News, Computerworld, Threatpost, USA Today, CNET, Financial Times PCMag, Newsweek, Huffington Post, Huffington Post (2) Techdirt, Engadget, Forbes, The <u>Daily Dot, IT World Canada, Global News, BNN, ITnews, Techmoran, YourMiddleEast,</u> TechRepublic, Macworld, Bloomberg, YourMiddle East, The Hill, An Ninh The Gioi, Baon Israel Valley, Radio FM4, Ctoutiao, Albawaba, Press TV, Verdict, Voltaire Net, Voltaire Net (2) Tags: Related: Patching Apple Zero Days Commercialization of Digital Spying, Malware, NSO Group, reckless, Surveillance, UAE ်ခ မေရ မိရာရ ABOUT CONNECT

munk school TORONTO

NEWSLETTER