Ryan Heavican
CS6725 Fall 2021

The Rise of Private Cyber Surveillance & The Fall of Human Rights: Applying the Diamond Model to the 2021 Cyberattack on a Bahraini Activist

Introduction

In February 2021, a zero-day exploit was used by the Bahraini government to install sophisticated spyware on an iPhone 12 Pro that belonged to a member of the Bahrain Center for Human Rights (BCHR). The BCHR is an award-winning non-governmental organization that continues to promote human rights in Bahrain despite being banned since 2004 by the increasingly repressive Bahraini government, a Constitutional Monarchy that has been controlled by the Al-Khalifa family for centuries (Abdulemam, et al., 2021). The Bahraini government created neither the exploit nor the spyware used against the activist. Rather, these shockingly effective technologies were developed by NSO Group (NSO), a private Israeli company that sells cyber surveillance products to governments around the world.

The attack was discovered by the Citizen Lab, an Internet watchdog at the University of Toronto, and prompted Apple to issue emergency updates for its iOS operating system. Apple is suing NSO for damages and an injunction in Federal court (Perlroth, Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones, 2021). Intentionally or not, the Citizen Lab utilized many aspects of an analytic methodology for intrusion analysis called the Diamond Model to identify the attack. The primary features of the Diamond Model--its four social-political and technological meta features--proved especially useful in strengthening the analysis of the attack. Further analysis utilizing the Cybersecurity Pedagogic Framework shows that changes have already resulted from the attack at the organizational and national layers of cybersecurity, known as Layers 8 and 9. However, further policy repercussions must result. Change is particularly needed at the transnational level, known as Layer 10, to prevent similar attacks in the future and to increase protections for billions of people across the planet, including dissidents and human rights defenders.

The Attack

That the Bahraini activist had been hacked by the Bahraini government was unsurprising, but the technological capabilities used in the attack were. Previous technological analysis by the Citizen Lab showed that Bahrain had been using the Pegasus spyware against members of Bahraini civil society since its purchase from NSO in 2017 (Abdul Razzak, Deibert, Marczak, McKune, & Scott-Railton, 2018). This spyware gives comprehensive access to an iPhone, including messages, photos, contacts, call history, browser history, and can even activate the microphone and camera (Middle East Eye, 2021). The Citizen Lab utilized forensic processes to analyze the activist's phone after noticing an uptick in Pegasus activity (Abdulemam, et al., 2021).

This analysis showed that NSO developed a zero-click exploit that required an attacker to simply send an iMessage without any victim interaction to install Pegasus (Whittaker, This tool tells you if NSO's Pegasus spyware targeted your phone, 2021). The exploit utilizes an integer overflow to crash the IMTranscoderAgent image service, circumventing an iOS security feature called BlastDoor. Because the exploit thwarted BlastDoor of iOS 14.4 and 14.6, it was dubbed FORCEDENTRY and given CVE-2021-30860 (Whittaker, A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen

Lab, 2021). The Citizen Lab attributed the attack to a Bahraini government operator dubbed LULU (Abdulemam, et al., 2021).

The Diamond Model

The Diamond Model is a framework for intrusion analysis that utilizes a scientific approach to ultimately bolster cybersecurity defenses by classifying events into campaigns, correlating them across events, and forecasting adversary operations. The framework employs a structure of four connected nodes representing Adversary, Victim, Capabilities, and Infrastructure. In its simplest form, the framework describes how an Adversary deploys a Capability over Infrastructure against a Victim (Betz, Caltagirone, & Pendergast, 2016, p. 7). Capabilities include technical elements such as malware, exploits, stolen certificates and credentials, and attacker tools. Infrastructure includes IP addresses, domain names, and email addresses. Adversaries include personas, email addresses, handles, and phone numbers of the attacker. Similarly, Victims include personas, email addresses, and attacked network assets (Betz, Caltagirone, & Pendergast, 2016, p. 17).

The framework includes meta-features to facilitate analysis of the four nodes. These meta-features include those used to characterize events, such as Timestamp, Phase, Result, Direction, Methodology, and Confidence, as well as event groups known as Activity Threads and Activity Groups to correlate different events and adversaries (Betz, Caltagirone, & Pendergast, 2016, p. 7). The framework can be extended to include two additional fundamental meta-features. These are the Social-Political meta-feature that informs the Adversary-Victim relationship, and the Technology meta-feature that informs the Capabilities-Infrastructure relationship.

Adversary and Victim

Applying the Extended Diamond Model to the BCHR incident gives insight into the attack and helps mitigate further attacks. Specifically, examination of the Social-Political relationship between the Adversary and Victim allows the application of analysis in non-traditional domains such as psychology, criminology, victimology, marketing, consumer behavior, and economics to expand mitigation options (Betz, Caltagirone, & Pendergast, 2016, p. 22).

The Bahraini government, the Adversary in this case, has a history of brutally repressing dissent to retain political power (Abdulemam, et al., 2021). Although officially a Constitutional Monarchy, Bahrain has been controlled by the Al-Khalifa family for centuries who continue to expand control over the country. The Bahraini government has a pattern of arrests, torture, and aggressive silencing of political opposition, which includes Internet censorship of content related to human rights, opposition parties (which are banned), Shiite websites, and local and regional news sources (Abdulemam, et al., 2021). Bahrain ranks 168 of 180 countries on the 2021 World Press Freedom Index and is among the Middle East's most repressive states (Freedom House, 2021). Bahrain's repression has accelerated with the 2011 Arab Spring uprising, in which hundreds were tortured by security forces, and has continued through COVID-19, which is being used as a pretext to impose further restrictions (Abdulemam, et al., 2021).

Bahrain's Internet governance adheres to a national model where Internet censorship and surveillance of individuals flourishes. The Victim in this incident is the unnamed BCHR member (Abdulemam, et al., 2021). Cyberattacks targeting BCHR member's devices have occurred since at least

2017 (Abdulemam, et al., 2021). Throughout this time, Bahrain has proven to be an extremely persistent and well-resourced Adversary. The Victim, on the other hand, represents a non-expendable commodity that Bahrain would devote considerable resources to target, which is a powerful example of what the Diamond Model terms an enduring Victim of Interest (Betz, Caltagirone, & Pendergast, 2016, p. 23). Bahrain has the goal of acquiring the personal information of Victims they perceive as political threats to eliminate those threats and increase the stranglehold over Bahraini civil society. Fortunately, although motivations and capabilities of Bahrain over its Victims are significant, transnational civil society defenders have supported these Victims, including the Citizen Lab and Amnesty International.

Capability and Infrastructure

An Extended Diamond Model analysis of the Capabilities and Infrastructure used in the attack reveals a growing trend pattern of leveraging the private surveillance industry. Bahrain developed neither the FORCEDENTRY exploit, nor the Pegasus spyware used in the attack. These Capabilities were developed by NSO and sold to Bahrain starting in 2017 (Abdulemam, et al., 2021). Thus, Bahrain was the Adversary Actor leveraging NSO's Capabilities. In fact, in its intensely nationalistic pursuit of surveillance technologies, Bahrain previously purchased malware from the companies FinFisher and Hacking Team (Abdulemam, et al., 2021).

Human rights groups, like the Citizen Lab and Amnesty International in conjunction with over a dozen other organizations, have monitored NSO spyware since 2020 in an effort called the Pegasus Project, by utilizing leaked lists of targeted individuals and tracking NSO's Infrastructure (Mekhennet, Priest, & Timberg, 2021). This Infrastructure was crucial in analyzing the attack. Bahrain leveraged NSO's Command and Control (C2) Capabilities, but these Capabilities and related Infrastructure were instrumental in identifying the attack (Abdulemam, et al., 2021). Furthermore, the attack Infrastructure consisted of both NSO and Bahrain's assets, including IP addresses and domain names. However, Bahrain also used its own Infrastructure to deliver exploits to Victims.

Bahrain has a unique relationship with the technical Infrastructure within its borders. The government has de-facto control of this Infrastructure and requires Bahraini Internet Service Providers to pursue its goals (Abdulemam, et al., 2021). For instance, government operators have taken control of Bahraini citizen's phone numbers to facilitate surveillance. Similarly, operators have spoofed and redirected websites by utilizing Internet Infrastructure (Amnesty International, 2021). Although operators might have been leveraging Type 2 Bahraini Infrastructure in the attack, which is controlled by a third party, Bahrain had full control over the assets as in Type 1 Infrastructure, which is fully owned by the Adversary. Bahraini operators, dubbed LULU, also utilized this Infrastructure to control IP addresses that ran their own Pegasus C2 servers (Abdulemam, et al., 2021). Analysis of this Infrastructure significantly aided the investigation by the Citizen Lab that attributed the attack to Bahrain.

Policy Assessment

Analyzing the policy implications of the attack is made easier by using the Cybersecurity Pedagogic Framework, which supplements the layers of the Open Systems Interconnection (OSI) Model with three additional layers: Layer 8 is Organizational, Layer 9 is Governmental, and Layer 10 is International/Transnational. Although further change is needed, consequences at these three layers have resulted from the attack.

An initial consequence of NSO facilitated attacks predates the BCHR incident. In 2019, Facebook sued NSO for damages and an injunction because NSO utilized Facebook's WhatsApp messaging platform to install spyware in prior attacks (Perlroth, WhatsApp Says Israeli Firm Used Its App in Spy Program, 2021). This represents Layer 8 reaction in which a private organization seeks redress from another organization. A second major reaction to the NSO's attacks came at Layer 9 in November 2021, when the US Commerce Department blacklisted NSO for maliciously targeting dissidents, activists, journalists, and others (Bergman, Perlroth, Sanger, & Swanson, 2021). This ban prohibits US companies from selling technology to NSO or its subsidiaries, and represents a significant Layer 9 reaction to attacks perpetrated by NSO. Interestingly, Israel is lobbying against this ban on behalf of NSO (Kirchgaessner, 2021).

Subsequently, in late November 2021, Apple also filed a lawsuit seeking damages and a permanent injunction banning NSO from using any Apple software, services, or devices (Apple, 2021). Apple dubs companies like NSO "mercenary spyware firms" that have committed flagrant violations against users. Apple argues that its team has devoted substantial financial resources, like those required of the emergency patch of FORCEDENTRY, to NSO and other state-sponsored actors. Apple further argues that NSO created more than 100 fake Apple IDs to carry out attacks, which breaks Apple's iCloud Terms and Conditions (Perlroth, Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones, 2021). Like with Facebook's actions, Apple's legal response to NSO represents a strong Layer 8 reaction at the organizational level. NSO now faces major market reaction, also at Layer 8, resulting from the lawsuits and blacklisting. The company had considered an Initial Public Offering on the Israeli stock market but now risks defaulting on $500 million debts (Scigliuzzo, 2021).

There must be a stronger Layer 10 transnational policy response to combat the threat of private cyber surveillance in addition to the current reactions at Layers 8 and 9. International human rights organizations like Amnesty International and the Citizen lab have taken the lead on combatting NSO, but this is not enough. Individual governments must band together to combat the threat of private cyber intelligence. Blacklists by individual governments do not prevent the threat due to the anarchic nature of the Internet. Similarly, relying on market forces and legal remedies sought by individual companies is too precarious when combatting threats like NSO. The United States needs to take the lead in pressuring transnational bodies, like the European Union and NATO, to blacklist companies like NSO.

Conclusion

An analysis of the February 2021 attack of a Bahraini human rights activist illuminates the grave threat posed by the mercenary cyber surveillance industry. Applying the Diamond Framework to the attack shows an exceptionally persistent Adversary, Bahrain, leveraging its own controlled Infrastructure while utilizing a third party's immensely effective Capabilities and Infrastructure to attack Victims, who are members of Bahraini civil society. A policy analysis drawing on the Cybersecurity Pedagogic Framework shows that actions against NSO have taken place at Layers 8 and 9, but more action is needed at the Layer 10 transnational level. Transnational NGOs have taken the lead on combatting the private surveillance industry, but transnational governmental alliances must do the same. Until then, the threats posed by NSO will grow. In fact, the US State Department reported an attack on dozens of employees that was facilitated by NSO Capabilities and Infrastructure just a few days ago (Atwood & Lyngaas, 2021).

References

Abdul Razzak, B., Deibert, R., Marczak, B., McKune, S., & Scott-Railton, J. (2018, September 18). *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Retrieved from The Citizen Lab: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Abdulemam, A., Anstis, S., Deibert, R., Scott-Railton, J., Berdan, K., Al-Jizawi, N., & Marczak, B. (2021, November 27). *From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits. The Citizen Lab*. Retrieved from The Citizen Lab: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

Amnesty International. (2021, July 18). *Forensic Methodology Report: How to catch NSO Group's Pegasus*. Retrieved from Amnesty International: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Apple. (2021, November 23). *Apple sues NSO Group to curb the abuse of state-sponsored spyware*. Retrieved from Apple Newsroom: https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

Atwood, K., & Lyngaas, S. (2021, December 3). *US State Department phones were hacked with NSO Group spyware*. Retrieved from CNN: https://www.cnn.com/2021/12/03/politics/state-department-nso-spyware/index.html

Bergman, R., Perlroth, N., Sanger, D. E., & Swanson, A. (2021, November 2021). *U.S. Blacklists Israeli Firm NSO Group Over Spyware*. Retrieved from The New York Times: https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html

Betz, C., Caltagirone, S., & Pendergast, A. (2016). The Diamond Model of Intrusion Analysis. *Center for Cyber Intelligence Analysis and Threat Research*.

Culliford, E., & Stempel, J. (2021, November 9). *Facebook can pursue malware lawsuit against Israel's NSO Group - US appeals court*. Retrieved from Reuters: https://www.reuters.com/technology/facebook-can-pursue-malware-lawsuit-against-israels-nso-group-us-appeals-court-2021-11-08/

Freedom House. (2021). *Bahrain*. Retrieved from Freedom House: https://freedomhouse.org/country/bahrain

Kirchgaessner, S. (2021, August 24). *Phones of nine Bahraini activists found to have been hacked with NSO spyware*. Retrieved from The Guardian: https://www.theguardian.com/world/2021/aug/24/phones-of-nine-bahraini-activists-found-to-have-been-hacked-with-nso-spyware

Mekhennet, S., Priest, D., & Timberg, C. (2021, July 18). *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*. Retrieved from The Washington Post:

https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Middle East Eye. (2021, August 24). *Pegasus: Bahrain hacked phones of nine activists with NSO spyware*. Retrieved from Middle East Eye: https://www.middleeasteye.net/news/bahrain-pegasus-spyware-targets-dissident-activists-home-abroad

MITRE. (2021, March 13). *CVE-2021-30860*. Retrieved from Mitre CVE Program: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860

Perlroth, N. (2021, November 23). *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*. Retrieved from The New York Times: https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html

Perlroth, N. (2021, January 15). *WhatsApp Says Israeli Firm Used Its App in Spy Program*. Retrieved from The New York Times: https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html

Scigliuzzo, D. (2021, November 22). *Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-11-22/israeli-spyware-firm-nso-seen-at-risk-of-default-as-sales-drop

Whittaker, Z. (2021, August 24). *A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen Lab*. Retrieved from TechCrunch: https://techcrunch.com/2021/08/24/nso-pegasus-bahrain-iphone-security/

Whittaker, Z. (2021, July 19). *This tool tells you if NSO's Pegasus spyware targeted your phone*. Retrieved from TechCrunch: https://techcrunch.com/2021/07/19/toolkit-nso-pegasus-iphone-android/