Pegasus

Surveillance Spyware

Austin Eversole

Introduction

- My name is Austin Eversole
- I am studying Computer Science and plan to graduate with a graduate degree in Dec. 2022

- One fun fact is that I spent a lot of my free time trying to fight a Win32/Malas-M virus outbreak on my high school's computer network.
- The reason I cared so much (besides helping the school of course) was that it prevented me from playing the video game Halo at school (couldn't play it at home) because it would actively delete *.exe’s and replace them with shortcuts to malware.

The story of Pegasus

- Pegasus spyware was developed before 2016 (potentially 2011[5]) by the Israel-based cyber-arms company NSO Group.
- It is a Trojan horse virus
  - Installs on Apple (iOS) and Adroid Devices
- It can discreetly activate the microphone and camera
- It also intercepts and steals information from texts, emails, contacts, FaceTime calls, and most communication apps
- It was named after Pegasus, the winged horse of Greek mythology.
  - Pegasus can be sent "flying through the air" to infect cell phones[1]

The story of Pegasus (cont.)

- Ahmed Mansoor a human rights activist from the UAE received a strange text message from a number he did not recognize. He has been victim to government hackers in the past, so he was suspicious and sent the message to a security researcher.[2]
- It turns out this link led to malware that exploited three zero-day iOS exploits to allow attackers to “jailbreak” the Apple security features and have full access to his phone.
- The security researcher let Apple know, who subsequently patched the exploits.
- This led to a full investigation called the “Pegasus Project” [3], including a later investigation by Amnesty International

The story of Pegasus (cont.)

- It was called the "most sophisticated" smartphone attack ever, and the first time a malicious remote exploit used jailbreaking to gain unrestricted access to an iPhone [2]
  - Jailbreaking exploits can be worth as much as $1 million
- The NSO Group claims Pegasus is used to “investigate terrorism and crime”.
  - NSO sold the Pegasus spyware to numerous countries including authoritarian governments. This is why Amnesty International got involved.
  - It has been used for surveillance of anti-regime activists, journalists, and political leaders and has been potentially associated with at least 2 deaths

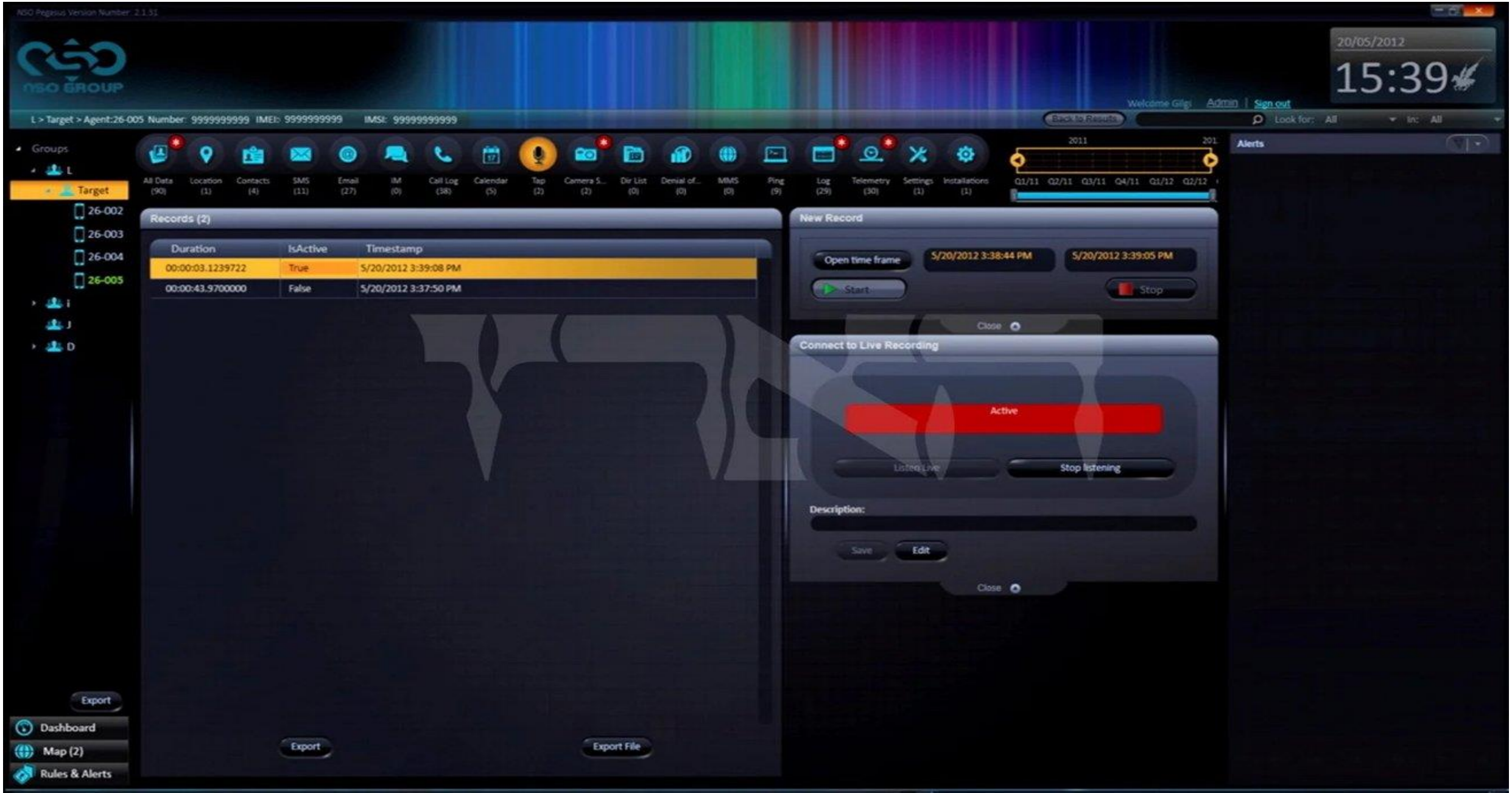
The story of Pegasus (cont.)

- The true extent of Pegasus is hard to track down because NSO group is extremely quiet about it and Pegasus was developed to run stealthily
- It was found that Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, the United Arab Emirates, and likely Jordan were clients of NSO and used Pegasus
- Pegasus is still being widely used against high-profile targets as of 2022[4]

Screenshots of the Pegasus Spyware[5]

The client-facing side of the tool is user friendly, and all that may be required (depending upon the case) of the client to begin deployment of Pegasus is to enter the target's phone number into the tool[9]

Screenshots of the Pegasus Spyware[5]



Technical Details & Indicators of Compromise

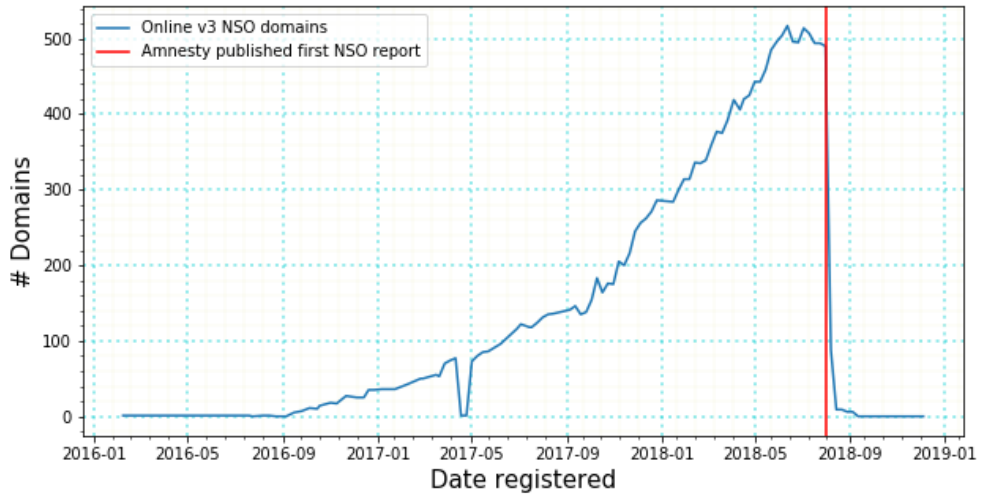
- Attack Vectors (to our best knowledge)
  - Used Phishing / Whaling when first discovered (2016)
  - Used Zero-click attacks at least since 2019
    - WhatsApp revealed Pegasus would be installed onto a target's phone by calling the target phone; the spyware would be installed even if the call was not answered
    - Pegasus has also used iPhone iMessage vulnerabilities and network-based attacks
  - If neither Phishing or Zero-click attacks succeed[6]
    - Pegasus can also be installed over a wireless transceiver located near a target
    - Or with physical access to the phone

Technical Details & IOC's (cont.)

- NSO Group claims that Pegasus leaves no traces whatsoever.
- This isn't quite true.
  - Amnesty International's Forensics Report found suspicious redirects in safari browsing history and resource logs
    - These redirects are the result of network injection through rogue cell towers, or through dedicated equipment placed at the mobile operator
    - These redirects didn't just happen when using Safari, but also in other apps like Twitter
- Domain names include but not limited to:
  - https://bun54l2b67.get1tn0w.*free247downloads[.]com*:30495/szev4hz
  - https://gnyjv1xltx.info8fvhgl3.*urlpush[.]net*:30875/zrnv5revj
  - tahmilmilafate[.]com, documentpro[.]org, baramije[.]net
  - opposedarrangement[.]net (part of Pegasus network infrastructure)
  - Forensics show Pegasus may have switched to using Amazon Web Services for its network infrastructure

Technical Details & IOC's (cont.)

- Command and Control Server
  - Pegasus's C2 server is hosted on a web server on port 443 with a unique domain and TLS certificate.
  - These edge servers would then proxy connections through a chain of servers, referred to by NSO Group as the "Pegasus Anonymizing Transmission Network" (PATN). Most of them are hosted in Europe and North America.
    - PATN uses randomized url paths and subdomains unique per exploit (as seen in the previous slide)
    - There are 4 known iterations of PATN, each with around 500 domain names.
    - PATN v3 was rapidly shut down by NSO Group once Amnesty International published their report (see below graph from Amnesty's Forensics report)
    - Pegasus has recently shifted from using registered domains to using Amazon Web Services for their C2 server to protect Pegasus from internet scanning techniques



Technical Details & IOC’s (cont.)

- Malware Dropper
  - “bh”process, which may stand for BridgeHead – probably an internal NSO toolkit
    - iOS Sample code contains bh.c, which loads API functions that relate to the next stage payloads and their proper placement on the victim’s iPhone
    - Soon after this process runs, root permissions are obtained, and Apple crash reporting is disabled.
- File Names and Executables
  - Processes that run after *bh* are likely later stages of Pegasus spyware. These include but are not limited to:
    - “roleaboutd”, “msgacntd”, “pcsd”, “fmld” (Network injection attack vector)
    - "mptbd", "ckebld", "fservernetd", "ckkeyrollfd“ (Apple Photos attack vector)
    - "roleaccountd“, "stagingd“, (iMessage and Apple Music attack vector)
    - “gatekeeprd”, “rolexd” (iMessage attack vector)
  - Pegasus also disguises itself as legitimate Apple iOS process names

Technical Details & IOC’s (cont.)

- Hashes
  - There are many different hashes of Pegasus spyware, as they are many updates that have been made to it over the years.
  - One hash from the Android version of Pegasus from Virus Total is shown below:

4bdf706507c48d2f0886825f651417f4b2281d3b73aa056b3c4e40d88c7beb81

  - Was unable to find any hashes from the Apple version of Pegasus

Technical Details & IOC's (cont.)

- Anti-Forensic Techniques
  - Pegasus has been shown to self-destruct after 60 days or if it is installed on an unintended device. [11]
  - Disables Apple Crash reporting, hides its processes as legitimate Apple iOS processes
  - It has recently started hiding leftover traces better (seemingly specifically targeting the forensics path taken by Amnesty International)
  - Pegasus does not maintain persistence anymore, so exploit code is not recoverable from non-volatile memory.
  - NSO Group shut down its PATNv3 servers as soon as they were compromised by Amnesty International's first Forensics Report
  - On the newest version of PATN that has been investigated (PATNv4)
    - Before connecting with PATN, a connection must pass validation at a validation server. Passer-by's or internet crawlers would only see a decoy PHP CMS
    - Uses a unique subdomain for every exploit attempt. Each subdomain was generated and only active for a short period of time. Researchers can't find the location of the exploit server based on historic device logs anymore.
    - Pegasus takes steps to avoid internet scanning by running the web server on a random high port number.
    - Pegasus directly connects to the Pegasus C2 servers without first performing a DNS lookup or sending the domain name in the TLS SNI field.
    - Uses Amazon Web Service to protect NSO Group from some Internet scanning techniques.

Technical Details & IOC’s (cont.)

- Privilege Escalation
  - The BirdgeHead (*bh* process) payload is believed to contain the privilege escalation attack.
- Persistence
  - Earlier versions of Pegasus (2016) maintained persistence on the device after reboot.
  - As of 2021, Pegasus seems to no longer maintaining persistence on iOS devices.

MITRE ATT&CK® Techniques [12]

Audio Capture – T1429	
Compromise Client Software Binary – T1645	(apple) modifies the system partition to maintain persistence (android) attempts to modify the device's system partition
Event Triggered Execution: Broadcast Receivers – T1524.001	(Android specific) listens for the BOOT_COMPLETED broadcast intent in order to maintain persistence and activate its functionality at device boot time
Exploitation for Privilege Escalation – T1404	
Out of Band Data – T1644	uses SMS for command and control.
Protected User Data: Call Log, Contact List – T1636.002 .003	
Protected User Data: Calendar Entries – T1636.003	(Android specific)
Protected User Data: SMS Messages, – T1636.0034	(Apple specific)
Software Discovery – T1418	(Android specific) accesses the list of installed applications

NOTE: Some information from MITRE in this list are not accurate and does not reflect the current state of Pegasus

MITRE ATT&CK® Techniques [12]

Stored Application Data – T1409	(apple) Accesses sensitive data in files, such as saving Skype calls by reading them out of the Skype database files (android) accesses sensitive data in files, such as messages stored by the WhatsApp, Facebook, and Twitter applications. It also has the ability to access arbitrary filenames and retrieve directory listings
System Network Configuration Discovery – T1422	(Android specific) checks if the device is on Wi-Fi, a cellular network, and is roaming
System Information Discovery – T1426	(Apple specific) monitors the victim for status and disables other access to the phone by other jailbreaking software
Video Capture – T1512	(Android specific)
Drive-By Compromise – T1456	(Apple specific) distributed through a web site by exploiting vulnerabilities in the Safari web browser on iOS devices
Location Tracking	(Apple Specific)

NOTE: Some information from MITRE in this list are not accurate and does not reflect the current state of Pegasus

Affected Products & Services

- Apple (iOS) and Android OS devices are the targets of Pegasus
- There are significantly more forensic traces accessible to investigators on iOS devices than stock Android devices
  - As a result, most cases of confirmed Pegasus infections are on iPhones, so we cannot draw an accurate iPhone vs. Android infection rate comparison
- A fully patched iPhone 12 running iOS 14.6 was compromised
  - The most recent iPhone model and iOS version at the time of Amnesty International's Forensics Report in 2021
- Pegasus's rate of successful compromises over the years suggest that there is no reason all iPhone models and iOS versions right now in 2022 couldn't be remotely comprised

Affected Products & Services

- Rather than being a specific exploit, Pegasus is a suite of exploits that uses many vulnerabilities in the system
- Vulnerabilities
  - The 2016 discovery of Pegasus yielded three new zero-day exploits:
  - CVE-2016-4655: Information leak in kernel
    - A kernel base mapping vulnerability that leaks information to the attacker allowing them to calculate the kernel's location in memory.
  - CVE-2016-4656: Kernel memory corruption leads to jailbreak
    - 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to secretly jailbreak the device and install surveillance software – details in reference.[37]
  - CVE-2016-4657: Memory corruption in the webkit
    - A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.
  - Google found another exploit dubbed FORCEDENTRY in 2021
  - It is likely that Pegasus uses many still undocumented zero-day exploits

Mitigations

- If you think you may be infected,
  - All Indicators Of Compromise (IOCs) are available on Amnesty International's GitHub[7]
  - Use the Mobile Verification Toolkit (MVT) to identify potential traces of compromise on your device[8]
    - Acquire and analyze data from Android devices
    - Read analysis of records from iOS backups and filesystem dumps
  - Get a new phone?

- For best effort to prevent being infected,
  - Ensure that the OS and apps in the device are updated[11]
  - Avoid clicking links in email, text or message that does not look reputable.
  - Only install apps from Google Play Store or Apple's App Store.

Hacker Identification

- Israel-based cyber-arms company NSO Group.
- Founded in 2010, has around 500 employees[9]
- Pegasus is its biggest and most infamous acknowledged product
- Sued by Apple and Whatsapp for their involvement with Pegasus

Repercussions of Malware

- Pegasus is still very alive and kept up-to-date for paying NSO Group clients
- NSO Group was blacklisted by U.S. in November 2021[9] for “maliciously target government officials, journalists, business people, activists, academics and embassy workers” including U.S. Citizens when in Uganda
- L3Harris backed out of acquiring NSO technologies after talks were revealed to public in June 2022
- Once a ghost and a legendary name among government-level surveillance software, NSO Group is now facing financial troubles.
- August 2022
  - CEO of NSO Group stepped down
  - 100 employees being let go

Key Takeaways & Lessons Learned

- Perspective of Device Manufactures:
  - Pegasus still to this day uses many zero-day vulnerabilities
  - There is discussion that the Apple should raise the bounty in its bug bounty program to convince bug finders to report it instead of making much more money off the zero-day black market
- Perspective of Government-level surveillance software companies:
  - NSO Group's financial troubles after Pegasus was made public is likely to be a lesson:
  - Ensure their products are not discovered
  - Be careful in selecting clients to not sell to authoritarian or unstable governments that may use their surveillance software in ways that the public would disagree with
- Pegasus was implicated in human rights violations. The public is now more aware of the seriousness of the impact of surveillance software

Works Cited

1. Jonathan Bouquet, The Gaurdian, 2019, “May I have a word about… Pegasus spyware”
2. Lorenzo Franceschi-Bicchierai, 2016, VICE “Government Hackers Caught Using Unprecedented iPhone Spy Tool”
3. Pegasus Project (investigation) – Wikipedia
4. Front Line Defenders, 2022, “Report: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware”
5. Mike Peterson, 2022, AppleInsider “Rare Pegasus screenshots depict NSO Group's spyware capabilities”
6. David Pegg, Sam Cutler, The Guardian, 2021 “What is Pegasus spyware and how does it hack phones?”
7. investigations/2021-07-18_nso at master · AmnestyTech/investigations · GitHub
8. Forensic Methodology Report: How to catch NSO Group’s Pegasus - Amnesty International
9. NSO Group – Wikipedia
10. Herb Keinon, The Jerusalem Post, 2021, “Lessons need to be learned from the NSO affair”
11. Aditya Saroha, The Hindu, 2021, “Pegasus Issue | What are zero-click attacks and how do they infect smartphones”?
12. Pegasus for Android, Software S0316 | MITRE ATT&CK®, Pegasus for iOS, Software S0289 | MITRE ATT&CK®

Cover page image from https://twitter.com/vxunderground/status/1418207502974525441 and from AppleInsider[4]