Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools

amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools

Summary

- In October 2019 Amnesty International published a first report on the use of spyware produced by Israeli company NSO Group against Moroccan human rights defenders Maati Monjib and Abdessadak El Bouchattaoui. Through our continued investigation, Amnesty International's Security Lab identified similar evidence of the targeting of **Omar Radi**, a prominent activist and journalist from Morocco from January 2019 until the end of January 2020.
- Evidence gathered through our technical analysis of Omar Radi's iPhone revealed traces of the same "network injection" attacks we described in our earlier report that were used against Maati Monjib. This provides strong evidence linking these attacks to NSO Group's tools.
- These findings are especially significant because Omar Radi was targeted just three days after NSO Group released its human rights policy. These attacks continued after the company became aware of Amnesty International's first report that provided evidence of the targeted attacks in Morocco. This investigation thus, demonstrates NSO Group's continued failure to conduct adequate human rights due diligence and the inefficacy of its own human rights policy.

Introduction

In October 2019 Amnesty International published the report "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware", where we detailed the targeting of Moroccan human rights defenders Maati Monjib and Abdessadak El Bouchattaoui using surveillance technology produced by the company NSO Group. In this current report, Amnesty International now reveals that **Omar Radi**, another prominent human rights defender and journalist from Morocco was also targeted using NSO Group's tools.

Photo Credits: Fanny Hedenmo

The Moroccan authorities have lately intensified their crackdown on peaceful dissent , with arbitrary arrests and prosecutions of individuals, including journalist Omar Radi, rappers and Youtubers, many of whom have been targeted simply for criticizing the King or other officials. Since November 2019, Amnesty International documented ten cases of activists who have been unlawfully arrested and prosecuted. All ten individuals have been charged with "offending" public officials or institutions, the King or the Monarchy, which are all crimes under Morocco's Penal Code. Between November 2019 and March 2020, all ten individuals and activists-were handed prison sentences ranging from a four months suspended sentence and a four year prison sentence. Amnesty International has called on the Moroccan authorities to drop charges and free those sentenced for exercising their right to free expression, and to reform the criminal code to decriminalize these forms of protected expression.

On 26 December 2019, Moroccan authorities arrested Radi for a tweet he posted earlier that year, in April, criticizing the judicial system for upholding the verdict against protesters from the 2017 protest movement in Morocco's northern region known as the Hirak el-Rif. A few days after his arrest, a Casablanca court granted him provisional release. But on March 17, a court in Casablanca convicted him to a four-month suspended sentence and a 500 dirhams (52 dollars) fine.

Omar Radi is a Moroccan award-winning investigative journalist and activist who worked for several national and international media outlets, including Atlantic Radio, TelQuel. His work investigated the links between corporate and political interests in Morocco and touched upon questions of corruption and other human rights abuses in Morocco and often tackled the persistence of impunity and lack of justice in the country.

Amnesty International's Security Lab performed a forensic analysis of Omar Radi's phone and found traces suggesting he was subjected to the same network injection attacks we first observed against Maati Monjib and described in our earlier report. Through our investigation we were able to confirm that his phone was targeted and put under surveillance during the same period he was prosecuted. This illustrates how human rights defenders (HRDs) may often have to deal with the twin challenges of digital surveillance alongside other tactics of criminalisation at the hands of Moroccan authorities leading to a shrinking space for dissent.

Network Injection, rogue cell towers and NSO

The lack of transparency around the surveillance industry makes it difficult to know what tools are being used, sold, purchased and abused, and therefore for victims and watchdogs to seek accountability. Despite this, our research so far has shed light on how NSO's technologies have evolved. Until early 2018, NSO Group's customers were found primarily using SMS and WhatsApp messages in order to trick targets into opening a malicious link, which would result in exploitation and infection of their mobile devices. As we documented in our October 2019 report, Amnesty International first observed attackers adopting new techniques to more stealthily and effectively deliver the malware. Using what we describe as "network injections", attackers are now capable of installing the spyware without requiring any interaction by the target.

Whereas previous techniques relied to some extent on tricking the user into taking an action, network injections allow for the automatic and invisible redirection of targets' browsers and apps to malicious sites under the attackers' control, most likely unknown to the victim. These will rapidly leverage software vulnerabilities in order to compromise and infect the device.

This is only possible where attackers are able to monitor and manipulate the Internet traffic of the target. In both Omar and Maati's cases all injections happened while using their LTE/4G mobile connection.

This type of attack is possible using two techniques: deploying a device commonly referred to as a "rogue cell tower", "IMSI Catcher" or "stingray", or by leveraging access to the mobile operator's internal infrastructure. It is currently unclear which of these two options have been used against Omar and Maati.

However, NSO Group's network injection capabilities were briefly described in a document named "Pegasus – Product Description" – apparently written by NSO Group – that was found in the 2015 leak of the competing Italian spyware vendor, Hacking Team. Specifically, in January 2020, Business Insider reported about mobile interception technology NSO Group exhibited during Milipol, an event and trade show on homeland security held in Paris in November 2019.

Photo Credit: Becky Peterson/Business Insider

The picture displays what appears to be a model of rogue cell tower sold by NSO Group – a tool which could be used in one of the two above-identified techniques to bring about a network injection attack.

These devices act as portable base stations and impersonate legitimate cellular towers in order to trick phones in the vicinity to connect to them and enable the attacker to manipulate the intercepted mobile traffic. The rogue cell tower in the picture seems to be composed of different cards stacked horizontally, likely to allow the operators to intercept over multiple frequency bands for GSM, 3G, 4G networks etc. Just as NSO Group simulated for their exhibition booth at Milipol, this electronic equipment can be quite small in size and easily transported and hidden on small vehicles.

Alternatively, attackers can similarly intercept and hijack mobile Internet traffic of targeted smartphones if they can leverage access to the victim's mobile operator. In this case, instead of placing a rogue cell tower in the vicinities of the target, attackers would rely on the existing network infrastructure of the mobile operator in use by the target.

In sum, previous attacks against HRDs documented by Amnesty in Morocco have raised the possibility of NSO tools being used in network injection attacks. It is also clear from publicly available information that NSO Group sells network injection capabilities. Taken together with the technical evidence that we detail in the next section, showing overlaps in timing, recovered forensic artifacts and attack infrastructure linked to previous surveillance attacks in Morocco using NSO tools, this strengthens the evidence linking NSO's network injection tools to this attack.

Omar Radi targeted with network injections between January 2019 and January 2020

Our previous analysis of Maati Monjib's phone indicated the execution of malicious software on it from early 2018 until at least June 2019. While between 2017 and 2018 he was targeted through SMS messages carrying malicious links tied to NSO Group, in our report from October 2019 we described how Maati Monjib's phone appeared to have been subjected to malicious redirects while he was navigating the Internet using the Safari browser. We argued that those redirects were symptomatic of network injection attacks which manipulated unencrypted web traffic in order to force Maati Monjib's browser to visit an exploitation site, located at the domain **free247downloads[.]com**, without his knowledge.

While analysing Omar Radi's iPhone, we found traces of the same domain. Forensic artefacts that Amnesty International extracted from the device suggests network injection attacks occurred on 27th January, 11th February, and 13th of September 2019.

In addition to the same exploitation site, we identified the same evidence of execution of malicious software we recovered from Maati Monjib's phone in Radi's too. This provides us additional evidence that the same spyware was used in both cases, which we believe – based on infrastructure overlaps and characteristics of the links used - to be NSO Group's Pegasus.

The following timeline records the key dates linked to NSO Group's spyware in Morocco. Forensics evidence recovered from both phones shows the links between the different stages of the attacks.

And below, a graphic depicting the network injection attack on Omar's phone observed while he was visiting a website in clear text (HTTP and not HTTPS):

On 2nd October 2019, as part of our publication process, we provided NSO Group with an advanced copy of our findings from our report "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware" and gave them an opportunity to respond to the revelations in the report. According to data collected by the Internet survey service Censys.io, the attackers-controlled infrastructure associated with subdomains of **free247downloads[.]com** were shut down by 6th October 2019, after nearly uninterrupted operation since its first appearance a year earlier, just days after we notified NSO of our findings but before our publication on 10th October 2019.

Additionally, our analysis of Omar's phone revealed traces of similar network injections as recently as 29th January 2020. These most recent attempts involved the new, previously undisclosed, domain name **urlpush[.]net**.

The domain name *urlpush[.]net* was only registered on 6th November 2019, several weeks after our previous publication, suggesting that our publication may have pushed the attackers to change infrastructure.

In sum, while the timing is suggestive of a link to NSO, technical details of the attacks, including that both sites redirect to the same website, and operate attacks with several matching execution and forensic artefacts, is strong evidence to link NSO Group's tools to the targeted attack on Omar Radi.

Who is behind these attacks?

NSO Group claims that they only sell their products to government agencies. According to their website, "*NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror*".

In their September 2018 report "Hide and Seek: Tracking NSO Group's Spyware Operations in 45 Countries" Citizen Lab identifies an operator they dubbed "ATLAS" focused on Morocco. Our own research indicates the continued use of the same malicious network infrastructure across attacks to be characteristic of a single and same entity behind the use of NSO Group's product in Morocco. In addition, as described earlier, the network injection attacks we have documented in Morocco require either physical proximity to the targets or leverage over mobile operators in the country which only a government could authorize. Because of this, and the continued targeting of Moroccan human rights defenders, we believe Moroccan authorities to be responsible.

Therefore, despite the unlawful surveillance of Maati Monjib and Abdessadak El Bouchattaoui that Amnesty International uncovered and documented in October 2019, we conclude that the Moroccan government actively remained a customer of NSO Group until at least January 2020 and continues to unlawfully target HRDs, such as in the case of Omar Radi.

All this is happening in a context where HRDs in Morocco are increasingly being put under surveillance. The continued abuse of NSO Group's tools in the country indicates Moroccan authorities are failing to respect and protect the rights to freedom of expression, association, and peaceful assembly.

Additionally, despite numerous instances of human rights abuse, exporting jurisdictions that grant NSO Group licences have failed in their responsibility to protect human rights by not adequately scrutinising and failing to deny export authorization where there is a substantial risk that the export in question could be used to violate human rights.

We asked NSO Group to respond to the revelations detailed in their report. Their response is included in its entirety in the Appendix. NSO Group did not confirm or deny whether the Moroccan authorities use their technologies and stated that they will review the information submitted. Amnesty International will follow up on their response. We also wrote to the Moroccan government, however did not receive a response.

Additional details of these attacks are discussed in the *Technical Appendix* annexed to this report.

NSO Group's repeated failure to check the abuse of its tools

In October 2019, in response to our report that NSO Group's tools were used to unlawfully target HRDs in Morocco, NSO Group told Amnesty International in a letter: *"Our products are developed to help the intelligence and law enforcement community save lives. They are not tools to surveil dissidents or human rights activists. That's why contracts with all of our customers enable the use of our products solely for the legitimate purposes of preventing and investigating crime and terrorism. If we ever discover that our products were misused in breach of such a contract, we will take appropriate action."*

We asked NSO Group whether they took any action in response to our previous report including details about investigations, why they did not terminate its contract with Moroccan authorities, and details of any mitigation measures they may have taken. NSO Group did not specifically respond to these questions in their response, stating confidentiality reasons.

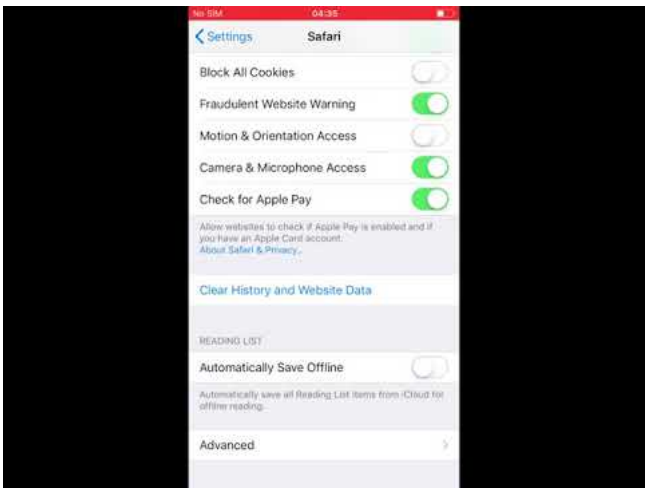
Despite these assertions, this report provides strong evidence that Omar Radi was unlawfully targeted using NSO Group's tools in January 2020. This is after NSO Group became aware of Amnesty International's first investigation. The company's tools are being used in support of Moroccan government's efforts to persecute people for free expression and clamp down on dissent.

This suggests that contrary to its claims, NSO Group has not taken adequate action to stop the use of its tools for unlawful targeted surveillance of HRDs in Morocco, despite being aware that this was taking place. This indicates that NSO Group has failed to conduct adequate human rights due diligence in order to prevent or mitigate harm, and as a result has not met its responsibility under international standards not to contribute to human rights violations.

In February 2019, UK-based private equity firm Novalpina Capital supported a management buyout of NSO Group. Novalpina Capital owns a controlling stake of the company. On 10th September 2019, Novalpina Capital/NSO Group said that it would implement a human rights policy and the company would be governed by a 'Governance, Risk, and Compliance Committee'. As detailed in this report, merely three days after this announcement, on 13th September 2019, Omar Radi was targeted. This is further evidence that there is a significant gap between the company's stated policy and actual practice.

How to check for similar attacks on your iPhone

If you are a Moroccan human rights defender and an iPhone user, you can follow the steps described in the following video to check for evidence of attacks similar to those described in this report:



Watch Video At: https://youtu.be/VaCL7kTaRyE

How to protect against network injection attacks

Because they rely on hijacking your own mobile Internet traffic, in order to be successful the attackers need to inspect the content of the websites you visit. To do so it waits for unencrypted HTTP visits. While many websites by now support transport encryption (indicated by links starting with *https://* instead of *http://*), many still don't.

Network injection attacks are difficult to identify because they provide very little visual clues. With other tactics for the delivery of the spyware, such as with malicious links sent via alluring SMS messages, someone targeted might be alerted and avoid clicking. A network injection attack instead happens invisibly while regularly navigating the Web.

Equipping your phone with a VPN could help, as it would obfuscate all incoming and outgoing traffic, preventing it from being manipulated. However, picking a good one is important. Many malicious or dubious VPN apps are available on iOS and Android app stores. Avoid the ones that are free of cost, because they are more likely to monetize the data you generate and be less respectful of your right to privacy.

Make sure to always keep your device and installed applications up-to-date. Security patches are regularly shipped by the device and software manufacturers. Lagging behind might unnecessarily expose your device even to casual attackers.

Recent reports from security researchers suggest that even advanced attackers increasingly struggle to maintain persistent access to a compromised mobile device. If so, a reboot of the device would disable the infection. Therefore, as a precaution, you might want to occasionally turn your smartphone off and on again.

Conclusion

In October 2019, we first documented evidence of NSO Group's tools being used to target two Moroccan HRDs. One of the two HRDs, Maati Monjib, was also targeted using network injection attacks. We suspected that these were also linked to NSO Group's tools. In this report, we detail the unlawful targeted surveillance of another Moroccan HRD, Omar Radi, including the strong technical evidence that links NSO Group's tools to this attack.

These attacks on HRDs are part of an intensifying clampdown of peaceful dissent in Morocco. The continued abuse of NSO Group's tools in the country indicates Moroccan authorities are failing to respect and protect the rights to freedom of expression, association, and peaceful assembly.

In addition, NSO Group's repeated failure to act on the misuse of its tools by Moroccan authorities, indicates that it has failed in its human rights responsibilities to not contribute to human rights violations and failed to conduct adequate human rights due diligence in order to mitigate harm.

Recommendations

Moroccan authorities and exporting countries should implement a proper human rights regulatory framework that governs surveillance. Until such a framework is implemented, a moratorium on the sale, transfer, and use of surveillance equipment should be enforced, as recommended by the UN Special Rapporteur for Freedom of Expression issues, David Kaye. This human rights framework, at a minimum, should include:

For Moroccan Authorities:

- Disclose information about all previous, current, or future contracts with private surveillance companies, including those with NSO Group.
- Halt the unlawful surveillance of journalists and human rights defenders in violation of their rights to privacy and freedom of expression.
- Ensure the effective implementing and enforcement of article 24 of the Moroccan constitution and the Code of Criminal Procedure, Chapter 5 to ensure that any digital surveillance is authorised by competent judicial authorities in advance.
- Ensure that public prosecutors and the National Control Commission for the protection of Personal Data (CNDP) conduct an independent and effective investigation in cases of unlawful targeted digital surveillance.

For Exporting States:

- Deny export authorization where there is a substantial risk that the export in question could be used to violate human rights.
- Ensure that all relevant technologies are scrutinized prior to transfer.

In addition to this, **NSO Group and Novalpina Capital** should, at a minimum:

- Urgently take pro-active steps to ensure that they do not cause or contribute to human rights abuses, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs in Morocco do not continue to become targets of unlawful surveillance.
- Terminate or suspend its contract with the Moroccan authorities.
- Ensure transparency regarding the volume, nature, value, destination, and end user of surveillance transfers.

Appendix I: NSO Group's Response

"We have received your letter of 9 June 2020, regarding the alleged targeting of a human rights defender by authorities in Morocco using our technology. Due to the confidentiality constraints detailed below, we cannot confirm or deny that such authorities use our technology. We appreciate your bringing this issue to our attention. Consistent with our Human Rights Policy, NSO Group takes seriously its responsibility to respect human rights, and is strongly committed to avoiding causing, contributing to, or being directly linked to negative human rights impacts.

We are deeply troubled by the allegations in your letter, and will immediately review the information therein and initiate an investigation if warranted. While you have provided certain information regarding the alleged misuse, to investigate the issue thoroughly, we need certain details, such as a phone number, the name of the individual, or a MSISDN (Mobile Station International Subscriber Directory Number) as set out in our public Whistleblowing Policy. Absent that information, our inquiries will be substantially constrained. If you would provide some or all of that information, it would greatly facilitate our ability to determine whether our products have been used in a manner inconsistent with our policies, any commercial agreements that may exist, international norms, or applicable domestic laws. In accordance with our policies we shall maintain this information in strict confidence and not divulge it other than as required to conduct a thorough investigation.

Your letter also poses several questions regarding any relationship NSO Group might have with Moroccan authorities, and the actions we undertook following a report by Amnesty International into alleged misuse of NSO's products by those authorities. While we seek to be as transparent as feasible in response to allegations that our products have been misused, because we develop and license to States and State

agencies technologies to assist in combatting terrorism, serious crimes, and threats to national security, we are obligated to respect state confidentiality concerns and cannot disclose the identities of customers. However, the attached correspondence with UN Special Rapporteur David Kaye contains a fulsome description of how we address human rights due diligence, measures that we may require in individual customer relationships to mitigate or prevent the risk of human rights impacts, our investigatory steps when we receive allegations of potential misuse, and a range of responses when a misuse is identified. We can assure you that we followed this approach with respect to your previous report, though due to the aforementioned confidentiality constraints we are unable to provide further details.

We do hope you will provide us with further details, as noted above, to allow us to investigate the disconcerting allegations described in your letter.
Best Regards,
Chaim Gelfand, Adv. Head of Compliance NSO Group"

Technical Appendix

Omar's Safari browsing history was purged in early October 2019, eliminating records of earlier Safari redirects using free247downloads[.]com. However, additional traces left on the device indicated us the timings of network injection attacks against him.

Forensic evidence of network injection attacks

On 27th January 2019 a folder was created associated with the domain:

private/var/mobile/Containers/Data/Application/4FC7C4F8-602A-4EA0-AF28-3264694AB07B/SystemData/com.apple.SafariViewService/Library/WebKit/WebsiteData/**https_skapth05c.get1tn0w.free247downloads.co**

Interestingly, this folder acts as storage for Twitter's mobile app for iOS. The folder name "**com.apple.SafariViewService**" refers to a service of the same name provided by the operating system which allows other apps to leverage Safari's browser engine to easily preview websites from within the app. We believe the presence of a "WebsiteData" folder for the malicious *free247downloads[.]com* domain indicates that a network injection attack occurred while Omar Radi was using the Twitter app and, after clicking on a link that lead to an unencrypted HTTP website, an exploitation was attempted on his phone.

On 11th February 2019 the following folder was created:

private/var/mobile/Containers/Data/Application/AE2D9AEB-8935-408D-9499-023635ACA6E7/Library/WebKit/WebsiteData/IndexedDB/**https_d9z3sz93x5ueidq3.get1tn0w.free247downloads.com_30897**/

This folder, located inside Safari's application data storage, contains several empty IndexedDB databases created subsequently to a visit to the malicious domain. While this detail was not included in our previous report, our forensics investigation of Maati Monjib's phone also revealed similar IndexedDB files. While we have not managed to recover any exploit payload, we suspect the creation of these files might be symptomatic of the vulnerabilities used against Omar Radi's and Maati Monjib's phones in 2019.

This network injection attack and exploitation appear to have been successful, and few seconds later the following file was modified:

/private/var/root/Library/Preferences/com.apple.CrashReporter.plist

On 13th September 2019 an additional network injection attack succeeded, suspicious processes were executed on the phone, and the following file was modified:

/private/var/mobile/Library/Preferences/com.apple.softwareupdateservicesd.plist

The contained value **SUAutomaticUpdateV2Enabled** was set to *false*, disabling the auto-update functionality of the phone and locking it at a vulnerable version.

Nameserver is shut down after communicating with NSO Group

The nameserver associated with the network injection subdomains was located at **ns-get1tnow.free247downloads[.]com** and resolved to the IP address 35.180.42.148. This IP addresses was assigned to an Amazon Web Service data center located in France. According to Censys data, this host remained operational from October 2018 until it was shut down on October 4th or 5th 2019:

[{"table":"20190929","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]

[{"table":"20190930","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]

[{"table":"20191001","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]

[{"table":"20191002","ports":["53"],"tags":["dns"],"updated_at":"2019-09-29 13:22:40"}]

[{"table":"20191003","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]

[{"table":"20191004","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]

[{"table":"20191005","ports":["53"],"tags":["dns"],"updated_at":"2019-10-03 06:47:28"}]

[{"table":"20191006"}]

The shutdown occurred shortly after we provided advanced notice of our findings from our previous report "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware" to NSO Group on 2nd October 2019. The report was published only on October 10th.

New Infrastructure is set up after our disclosures

Less than a month after our publication new infrastructure was set up on the domain **urlpush[.]net**, which we later discovered involved in more recent network injection attacks against Omar Radi.

On 27th January 2020, while visiting a link to a news site he clicked from the Facebook app, Omar's browser was hijacked and finally redirected in under 3 milliseconds to the new exploitation server with the same URL structure as the one we previously observed in 2019:

https://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#074196419827987919274001548622738919835556748325946#2

Suspicious of this unusual behavior, Omar Radi promptly took a screenshot of his Safari browser attempting to open the malicious site while being connected to the 4G network:

A second network injection and exploitation was attempted on 29th January 2020. This apparently failed, and instead redirected the browser to the website of a legitimate business based in France. We observed this same website used as a decoy in failed attacks against Maati Monjib in 2019.

The nameserver for the urlpush.net subdomains resolved to the IP address 72.105.81.177. This IP address is assigned to the hosting provider Linode and is located in Germany.


Maroc Telecom 4G 11:06 AM
gnyjv1xltx.info8fvhgl3.urlpush.net