by Lorenzo Franceschi-Bicchierai and Riccardo Coluccini

Researchers Find Google Play Store Apps Were Actually Government Malware

Security researchers have found a new kind of government malware that was hiding in plain sight within apps on Android's Play Store. And they appear to have uncovered a case of lawful intercept gone wrong.

- SHARE
- TWEET

Leggi in italiano.

Hackers working for a surveillance company infected hundreds of people with several malicious Android apps that were hosted on the official Google Play Store for months, Motherboard has learned.

In the past, both government hackers and those working for criminal organizations have uploaded malicious apps to the Play Store. This new case once again highlights the limits of Google's filters that are intended to prevent malware from slipping onto the Play Store. In this case, more than 20 malicious apps went unnoticed by Google over the course of roughly two years.

Motherboard has also learned of a new kind of Android malware on the Google Play store that was sold to the Italian government by a company that sells surveillance cameras but was not known to produce malware until now. Experts told Motherboard the operation may have ensnared innocent victims as the spyware appears to have been faulty and poorly targeted. Legal and law enforcement experts told Motherboard the spyware could be illegal.

"These apps would remain available on the Play Store for months and would eventually be re-uploaded."

The spyware apps were discovered and studied in a joint investigation by researchers from Security Without Borders, a non-profit that often investigates threats against dissidents and human rights defenders, and Motherboard. The researchers published a detailed, technical report of their findings on Friday.

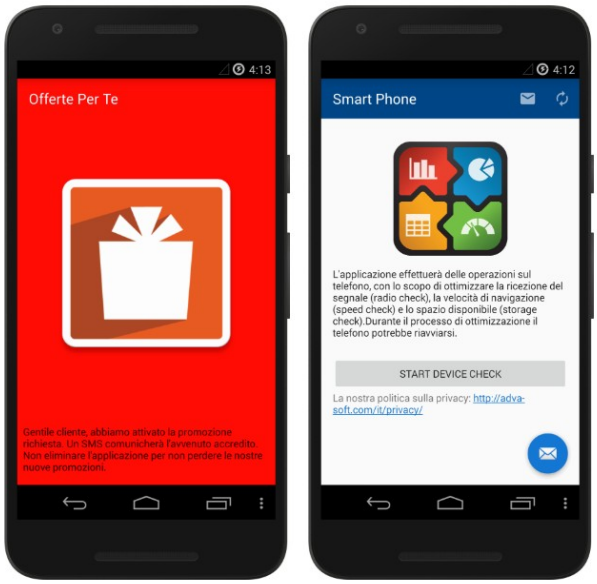
"We identified previously unknown spyware apps being successfully uploaded on Google Play Store multiple times over the course of over two years. These apps would remain available on the Play Store for months and would eventually be re-uploaded," the researchers wrote.

Lukas Stefanko, a researcher at security firm ESET, who specializes in Android malware but was not involved in the Security Without Borders research, told Motherboard that it's alarming, but not surprising, that malware continues to make its way past the Google Play Store's filters.

"Malware in 2018 and even in 2019 has successfully penetrated Google Play's security mechanisms. Some improvements are necessary," Stefanko said in an online chat. "Google is not a security company, maybe they should focus more on that."

MEET EXODUS

In an apparent attempt to trick targets to install them, the spyware apps were designed to look like harmless apps to receive promotions and marketing offers from local Italian cellphone providers, or to improve the device's performance.



A screenshot of one of the malicious apps. (Image: Security Without Borders)

The researchers alerted Google earlier this year to the existence of the apps, which were then taken down. Google told the researchers and Motherboard, that it found a total of 25 different versions of the spyware over the last two years, dating back to 2016. Google declined to share the exact numbers of victims, but said it was below 1,000, and that all of them were in Italy. The company would not provide more information about the targets.

The researchers are calling the malware Exodus, after the name of the command and control servers the apps connected to. A person who's familiar with the malware development confirmed to Motherboard that was the internal name of the malware.

Exodus was programmed to act in two stages. In the first stage, the spyware installs itself and only checks the phone number and its IMEI—the device's unique identifying number—presumably to check whether the phone was intended to be targeted. For that apparent purpose, the malware has a function called "CheckValidTarget."

But, in fact, the spyware does not appear to properly check, according to the researchers. This is important because there are currently some legally permissible uses of narrowly targeted malware—for example, with a court order, law enforcement can legally hack devices in many countries.

In a test done on a burner phone, the researchers saw that after running the check, the malware downloaded a ZIP file to install the actual malware, which hacks the

phone and steals data from it.

“This suggests that the operators of the Command & Control are not enforcing a proper validation of the targets,” Security Without Borders concluded in the report. “Additionally, during a period of several days, our infected test devices were never remotely disinfected by the operators.”

Got a tip? You can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv. And you can reach Riccardo Coluccini securely on OTR chat at rcoluc@jabber.ccc.de, and riccardo.coluccini@vice.com.

At that point, the malware has access to most of the sensitive data on the infected phone, such as audio recordings of the phone’s surroundings, phone calls, browsing history, calendar information, geolocation, Facebook Messenger logs, WhatsApp chats, and text messages, among other data, according to the researchers.

The spyware also opens up a port and a shell on the device, meaning it allows the operators to send commands to the infected phone. According to the researchers, this shell is not programmed to use encryption, and the port is open to anyone on the same Wi-Fi network as the target. This means that anyone in the vicinity could hack the infected device, according to the researchers.

“This inevitably leaves the device open not only for further compromise but for data tampering as well,” the researchers wrote.

A second, independent analysis by Trail of Bits, a New York-based cybersecurity company that looked into the malware for Motherboard, confirmed that the malware samples all connect to the servers of one company, that the IP addresses identified by Security Without Borders are all connected, and that the malware leaves the target device more vulnerable to hacking.

WHO IS BEHIND THE SPYWARE?

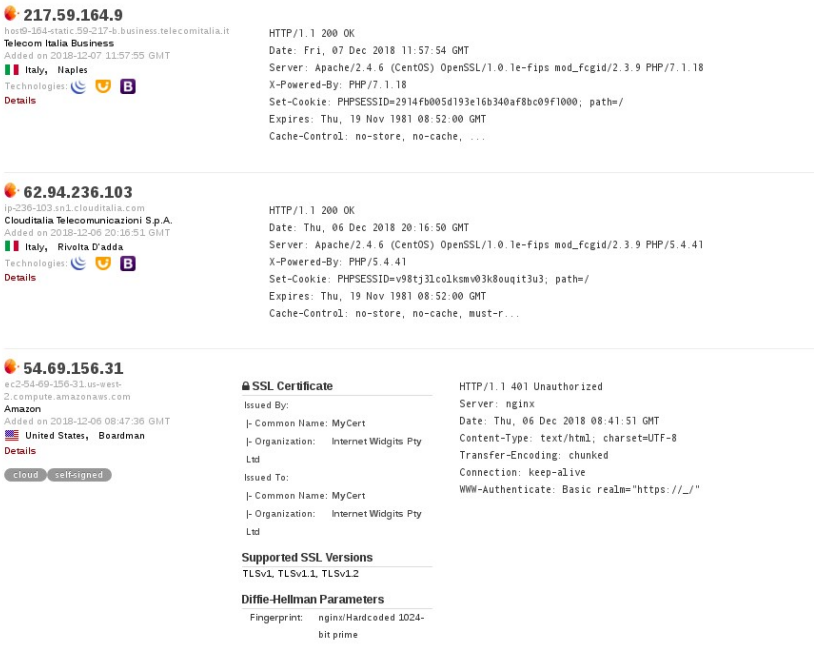
All the evidence collected by Security Without Borders in its investigation indicates the malware was developed by eSurv, an Italian company based in the southern city of Catanzaro, in the Calabria region.

The first hint that the authors of the malware were italian came from two strings inside the malware code: “mundizza,” and “RINO GATTUSO.” Mundizza is a dialectal word from the southern region of calabria that loosely translates to garbage. Rino Gattuso is a famous retired Italian footballer from Calabria.

The real smoking gun, however, is the command and control server used in several of the apps found on the Play Store to send the data back to the malware operators.

The server, according to the researchers, shares a TLS web encryption certificate with other servers that belong to eSurv’s surveillance camera service, which is the company’s main public business. Also, some of these servers identified by the researchers display eSurv’s logo as the icon associated with the server’s address, the icon you can see in your browser’s tab, also known as favicon.

Other spyware samples communicate with a server belonging to eSurv, according to the researchers. Google confirmed the servers belong to eSurv. The Trail of Bits researcher who reviewed the technical report and the spyware confirmed that it’s linked to eSurv.



A sample of eSurv's command and control servers. (Image: Security Without Borders)

Finally, an eSurv employee explained in a resume publicly available through his LinkedIn page that as part of his job at the company, he developed “an ‘agent’ application to gather data from Android devices and send it to a C&C server”—a technical, albeit clear, reference to Android spyware.

Motherboard reached out to the developer, who declined to comment, arguing that the answer would be “confidential information. I don’t think I can say anything about this ;)”

We reached out to eSurv multiple times via email and LinkedIn. Initially, an employee of the company claimed to be surprised and shocked by our findings, given that eSurv only sells video surveillance, she said. A few hours after our phone call, the company took down its site for a couple of weeks.

After we followed up and asked for clarification, the company declined to comment.

eSurv appears to have an ongoing relationship with Italian law enforcement, though Security Without Borders was unable to confirm whether the malicious apps were developed for government customers.

eSurv won an Italian government State Police tender for the development of a “passive and active interception system,” according to a document published online in compliance with the Italian government spending transparency law. The document reveals that eSurv received a payment of € 307,439.90 on November 6, 2017.

We filed a freedom of information request to obtain information on the tender, the list of companies that participated, the technical offer sent by the company, and the invoices issued by eSurv. Our request, however, was rejected. The Anti-Drug Police Directorate, an agency within the State Police which responded to the request, said it could not respond with the documents because the surveillance system was obtained with “special security measures.”

Over the last few months, several sources with knowledge of Italy’s spyware market told Motherboard that a new company from Calabria was getting several contracts to

develop surveillance software with law enforcement and government agencies. Some of those sources specifically named eSurv as that new company that was taking the local market by storm.

Finally, a source close to eSurv, who asked to remain anonymous because he was not authorized to speak to the press, said that the company sells malware to the Italian police.

“They publish [the spyware] on the Play Store and then induce the person to download it and open it,” the source said in an online chat.

IS THIS ALL LEGAL?

Using spyware with warrants or a judge’s authorization is, generally speaking, legal in most countries in Europe, as well as the United States. In this case, however, eSurv’s spyware may not be operating according to the law, experts told Motherboard.

“I don’t think there are reasons to believe this spyware is legal,” Giuseppe Vaciago, an Italian lawyer who specializes in criminal law and surveillance, told Motherboard after reviewing the report by Security Without Borders.

Vaciago explained that a spyware acting according to Italian law should not install itself on any target without first validating that the target is legitimate, something Exodus does not properly do, according to the researchers.

Moreover, Vaciago explained that Italian law effectively equates spyware with physical surveillance devices, such as old school hidden microphones and cameras, limiting its uses to capturing audio and video.

“This software, on the other hand, is able to do, and effectively appears to have done, much more invasive activities than those prescribed by the law,” Vaciago told Motherboard in an email.

“Opening up security holes and leaving them available to anyone is crazy and senseless, even before being illegal.”

The fact that the malware leaves the device vulnerable to other hackers is perhaps the worst element of Exodus, according to a police agent who has experience using spyware during investigations, and who asked to remain anonymous because he’s not allowed to speak to the press.

“This, from the point of view of legal surveillance, is insane,” the agent told Motherboard. “Opening up security holes and leaving them available to anyone is crazy and senseless, even before being illegal.”

At the end of 2017, Italy introduced a law regulating the use of spyware for law enforcement activities and investigations—the law only regulates the use of spyware to record audio remotely, leaving out all the other features that surveillance software can have, such as intercepting text messages, or taking screenshots of the screen. In May 2018, the Ministry of Justice published technical requirements that must be respected in the development and use of spyware by law enforcement agencies.

In an opinion issued by the Italian Data Protection Authority in April of last year, the authority criticized the requirements for being too vague when it came to describing the interception system’s components, and it emphasized that authorities need to ensure that installing the spyware on a target does not reduce the overall security of the infected device.

“This is in order to prevent the device from being compromised by third parties, avoiding negative consequences on the protection of personal data contained therein as well as on investigative activities,” the authority wrote.

Apps that offer promotions and marketing offers from local telecommunication providers is a front that has been used by Italian government malware before. In fact, Italian telecommunication companies can be forced by the government to send text messages to facilitate malware injection on suspects’ devices, as previously reported by Motherboard Italy.

Details of this activity were found in a hearing of the Company Security Governance of the Italian cellphone provider Wind Tre Spa, held in March of 2017 by the Parliamentary Committee for the Security of the Republic (COPASIR)—a committee that supervises the activity of the intelligence services.

According to the document, which summarizes the hearings, when it comes to the use of spyware for investigations, the telecommunication operators are consulted to facilitate the infection of third party devices with the malware. These operations “consist mainly in expanding the bandwidth and sending messages to request certain maintenance activities,” the document reads. These activities may be included in what are called “mandatory justice services” for telecommunication operators, services that are detailed in a specific price list by the Ministry of Justice: ranging from 15 Euros for wiretaps and internet communication flow, to 110 Euros for “assistance and feasibility studies.”

At the time of publication, the Italian State Police did not respond to multiple requests for comment on the technology subject to their tender, nor they had replied to questions on the use of this spyware. Questions to two Italian Public Prosecutor's Offices went unanswered as well.

The police agent agreed that eSurv’s spyware lacked the right scope and safeguards to ensure it wouldn’t hit people who were not being under investigation.

“You can’t do something indiscriminate,” the police agent told Motherboard. “Putting something on the Play Store thinking you’re going to infect an undetermined number of people, and do trawling is something absolutely illegal.”

The source close to eSurv confirmed that, at times, the apps ended up on the wrong phones, as “oblivious people,” the source said, “unknowingly downloaded the app and infected themselves.”

Instead of doing anything to stop that, however, the company used the victims as “guinea pigs.”

Listen to CYBER, Motherboard’s new weekly podcast about hacking and cybersecurity.

- Tagged:
- SURVEILLANCE
- News
- privacy
- Google
- cybersecurity
- malware
- spyware
- google play
- Infosec
- Tech news
- information security
- government hacking
- eSurv

Watch This Next

Image: Cathryn Virginia/Motherboard
State of Surveillance
|
by Lorenzo Franceschi-Bicchierai
|
Oct 24 2018, 8:04am

Government Spyware Vendor Left Customer, Victim Data Online for Everyone to See

The Germany-based spyware startup Wolf Intelligence exposed its own data, including surveillance target's information, passports scans of its founder and family, and recordings of meetings.

- SHARE
- TWEET

A startup that claims to sell surveillance and hacking technologies to governments around the world left nearly all its data—including information taken from infected targets and victims—exposed online, according to a security firm who found the data.

Wolf Intelligence, a Germany-based spyware company that made headlines for sending a bodyguard to Mauritania and prompting an international incident after the local government detained the bodyguard as collateral for a deal went wrong, left a trove of its own data exposed online. The leak exposed 20 gigabytes of data, including recordings of meetings with customers, a scan of a passport belonging to the company's founder, scans of the founder's credit cards, and surveillance targets' data, according to researchers.

Security researchers from CSIS Security discovered the data on an unprotected command and control server and a public Google Drive folder. The researchers showed screenshots of the leaked data during a talk at the Virus Bulletin conference in Montreal, which Motherboard attended.

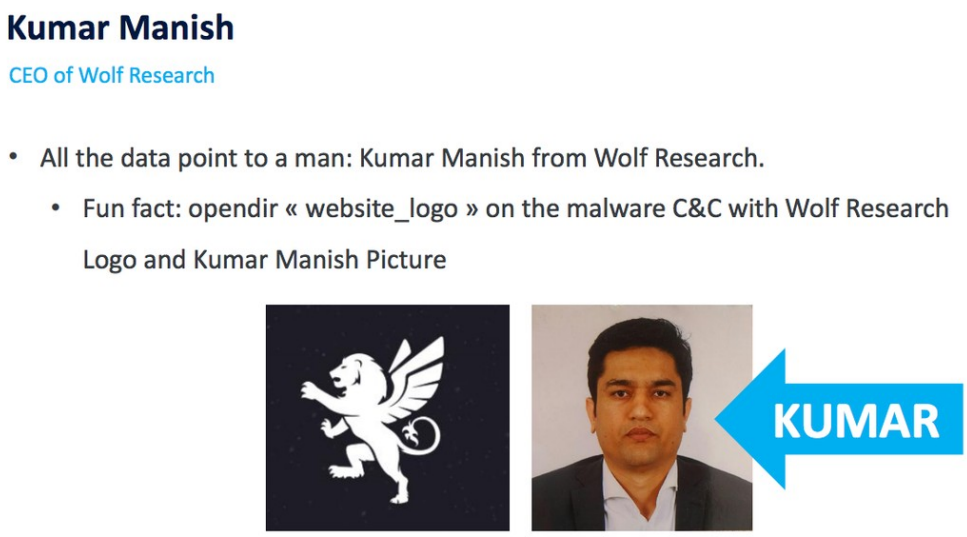
"This is a very stupid story in the sense that you would think that a company actually selling surveillance tools like this would know more about operational security," CSIS co-founder Peter Kruse told Motherboard in an interview. "They exposed themselves—literally everything was available publicly on the internet."

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv

In an online chat, Wolf Intelligence founder Manish Kumar told me that it wasn't his company that left the data online, but a reseller he refused to identify. He also said that he plans to sue CSIS for hacking his reseller; CSIS is adamant that it did not hack anything, as everything was exposed and open to anyone

"They claim wrong that it's for hacking innocent people, and damage our image." Kumar said, but refused to answer additional questions about who was the reseller, and who his customers are.

CSIS researcher Benoît Ancel told Motherboard the researchers "have many indications that it was not a reseller," and was instead a mistake by Wolf Intelligence. To support this, he shared pictures from the servers such as a screenshot of an exposed database that shows one of Kumar's cellphone numbers and a series of intercepted text messages, and a screenshot of a Slack conversation between Kumar and one of his employees.



A slide from CSIS talk, showing Kumar's headshot, which was stored in the exposed server.

Wolf Intelligence is part of the so-called "lawful intercept" industry. This is a relatively unregulated—but legal—part of the surveillance market that provides hacking and spy software to law enforcement and intelligence agencies around the world. Hacking Team, FinFisher, and NSO Group are the more well-known companies in this sector. According to a recent estimate, this market is expected to be worth $3.3 billion in 2022.

These companies generally sell spyware that infects computers and cell phones with the goal of extracting evidence for police or intelligence operations, which can be particularly useful when authorities need to get around encryption and have a warrant to access the content of a target's communications. But in the past, companies like Hacking Team, FinFisher, and NSO Group have all sold their malware to authoritarian regimes who have used it against human rights defenders, activists, and journalists.

As demand for these technologies has grown, many smaller players have entered the market. Some of them have made embarrassing mistakes that have helped cybersecurity researchers expose them.

A screenshot of the Wolf Intelligence malware panel, included in a leaked marketing brochure.

This mistake, however, may be the worst we've ever seen.

"Maybe they were thinking that the server was secure, I don't know, but it was definitely stupid," Kruse said. "Everything was just floating around on the internet. That's why I thought this story was too good to be true."

Kruse's colleagues Benoît Ancel and Aleksejs Kuprins found the data as they were investigating a banking malware sold on the internet underground and used by several cybercriminals, the two said during a talk at the Virus Bulletin conference in Montreal in early October. They said that banking malware had shared infrastructure with a malicious Remote Access Trojan or RAT.

The researchers said they were able to find a Windows, an Android, and an iOS variant of that RAT, and figured out that it was produced by Wolf Intelligence. They also found data belonging to several victims in countries such as Egypt, Saudi Arabia, and Turkey. One of the victims, they said, is a human rights defender.

The malware itself, according to the researchers, is pretty rudimentary.

"It's very shitty and it's just copy paste from open source projects," Ancel told Motherboard in a phone interview, referring specifically to Wolf Intelligence's iOS malware. Motherboard did not independently analyze the malware, and Kumar stopped responding to Motherboard soon after I began talking to him.

Read more: Hacker 'Phineas Fisher' Speaks on Camera for the First Time—Through a Puppet

During the public presentation in Montreal, Ancel said that Kumar "seems to be the kind of criminal who try to scam people with a shitty product."

Ancel and Kuprins are not the first to publicly question the quality of the Wolf Intelligence's products and to slam its founder.

"Manish is a walking scam," security researcher Agostino Specchiarello told me, who once met with Kumar to consider a business deal with him. "He used to claim that stuff made by others was his."

A map showing the location of targets of Wolf Intelligence customers. Image: CSIS Security

In early 2017, Hacking Team's CEO David Vincenzetti told Motherboard that Kumar is a "criminal of the worst kind."

Yet, Hacking Team worked with Kumar once, according to a former company employee who asked to remain anonymous to discuss details of his previous job.

Kumar did not respond to questions regarding his deals with Hacking Team.

The CSIS researchers said that after their talk at Virus Bulletin, Wolf Intelligence shut down the exposed servers.

"They are here and still in the business," Ancel told me.

Get six of our favorite Motherboard stories every day by signing up for our newsletter.

- Tagged:
- SURVEILLANCE
- News
- privacy
- cybersecurity
- spyware
- Leak
- Infosec
- Tech news
- information security
- Manish Kumar
- Wolf Intelligence
- Government Spyware

State of Surveillance
|
by Lorenzo Franceschi-Bicchierai
|
Dec 5 2017, 9:00pm

Ethiopia Allegedly Spied on Security Researcher With Israel-Made Spyware

The digital rights watchdog Citizen Lab has exposed a new spyware company that sells surveillance technology to governments.

Image: John Wollwerth/Shutterstock

On March 30 of this year, Bill Marczak woke up and checked his email. His eyes immediately spotted something suspicious in his inbox: a message about Ethiopia containing only a one line link written in comic sans font.

The phishing email that the hackers sent to Bill Marczak. Image: Bill Marczak

Marczak is a researcher at Citizen Lab, a group that studies how governments around the world use new technologies such as spyware against dissidents and activists. For years, Marczak and his colleagues have exposed several hacking attacks against people all over the world. This time, however, Marczak himself became the target.

"It was pretty shocking," Marczak told me in a phone call.

Marczak received the email while he and his colleagues were investigating a series of phishing emails sent to Ethiopian journalists and activists with a history of criticizing the current government. Those emails, including the one sent to Marczak, were designed to infect targets with spyware made by the Israeli company Cyberbit, a subsidiary of the defense contractor Elbit Systems, according to a new report published on Wednesday by Citizen Lab.

In the last few years, governments all over the world have purchased spyware designed to monitor targets' computer and cellphone communications, siphoning off emails, text messages, chats, calls, and more from the victims' devices. There is now a flourishing, albeit lightly regulated, market for these kind of products. Countries like Ethiopia and Mexico have already been caught using several different spyware products made by surveillance tech vendors such as FinFisher, Hacking Team, or NSO Group.

Citizen Lab already showed that Ethiopia bought spyware from FinFisher and Hacking Team, showing that despite some companies getting exposed for helping governments spy on their citizens, the spyware market is now crowded enough that customers can just switch to a different provider. This new research also shows that despite Citizen Lab's previous investigations showing abuse of these technologies, Ethiopia keeps using them to target dissidents.

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzo@jabber.ccc.de, or email lorenzo@motherboard.tv

This latest investigation began when Jawar Mohammed, the executive director of Oromia Media Network, received a suspicious email in October of 2016 and forwarded it to Citizen Lab, which is part of the University of Toronto's Munk School of Global Affairs. Oromia Media Network broadcasts from the United States, and covers news from the Ethiopian state of Oromia. Mohammed and his colleagues have often come in the crosshairs of the Ethiopian government. Earlier this year, Ethiopia charged Mohammed with terrorism and treason for the alleged role of his company in fueling protests.

"The government doesn't like what I do. The fact that I do a lot of reporting and expose their corruption and killings," Mohammed told Motherboard in a phone call. "Both

the charges and hacking are to meant to take me out of the market, disable me and prevent me from reporting."

Mohammed said he wasn't surprised to be targeted with spyware, as he and his colleagues are aware of being a "top target for government because of our reporting."

The Ethiopian embassy in Washington DC did not respond to a request for comment.

Read More: The Tragedy of Ethiopia's Internet

Once Mohammed sent Marczak the phishing emails, the researcher started to analyze them and found that the malicious links pointed to websites designed to look like real news and media sites such as EastAFRO.com. The sites showed targets a pop up prompting them to download a malicious new version of Adobe Flash player, which contained the malware.

Code referencing something called PC Surveillance System PSS was "all over the spyware code," Marczak said. PSS is a spyware product for Windows sold by Cyberbit, according to Citizen Lab.

The malware connected to a command and control server, and when Citizen Lab scanned the internet for similar servers it found several others. Shockingly, the servers displayed a public directory of files, and among them were logs listing all the hacking victims with their IP addresses and geolocation, which helped Citizen Lab to identify and warn logical targets with the help of Ethiopian activists.

"That was the really surprising thing," Marczak told me. "The extent to which this stuff was easily discoverable."

Thanks to these files, Citizen Lab was able to find several other victims and alert them. All of them received phishing emails resembling the ones Mohammed and Marczak received, according to Citizen Lab.

A spokesperson for Cyberbit replied to an email containing a series of specific questions with a statement. The spokesperson said that each Cyberbit sale is regulated and approved by the Israeli Ministry of Defense, and the company "does not operate the products" and "is not exposed to the manner in which its products are operated by intelligence and defense agencies, which operate covertly by nature."

"Cyberbit Solutions is fully committed to confidentiality towards its customers and is not permitted to relate to any specific transaction or specific customer." the statement continued. "The company's products contribute greatly to national security in the countries where they are sold and the law enforcement and defense authorities in these countries are committed to operating them in accordance with the law."

This likely won't be the last time a government gets caught using spyware against dissidents, but this might be one of the sloppiest attempts we've seen yet.

This story has been updated to include Cyberbit's statement.

- Tagged:
- SURVEILLANCE
- Hacking
- privacy
- cybersecurity
- malware
- phishing
- spyware
- ethiopia
- Infosec
- citizen lab
- Cyberbit

Hacking
|
by Lorenzo Franceschi-Bicchierai
|
Nov 27 2018, 8:38am

Malware Companies Are Finding New Ways to Spy on iPhones

Kaspersky Lab's found evidence that a small spyware government contractor sells iOS malware, showing it may not be as rare as some people think.

Image: Motherboard

Thanks to a combination of tight controls and innovative security features, Apple has made the iPhone perhaps the most secure consumer device in the world. But nothing is unhackable, and iOS malware isn't as rare as many may think.

Earlier this year, Russian cybersecurity firm Kaspersky Lab found evidence that a small government spyware maker called Negg developed a "custom iOS malware that allows GPS tracking and performs audio surveillance activity," according to a private report the company sent to subscribers. The discovery of Negg's iOS malware has never been reported outside of Kaspersky.

"We have uncovered an iOS implant," Kaspersky Lab researcher Alexey Firsh told Motherboard in an email. "We assume that at the moment of discovery it was in a development stage and was not fully adapted to infect potential victims."

"We have uncovered an iOS implant."

Malware on iOS has always been rare, thanks to the increasing difficulty of jailbreaking iPhones and Apple's continuous focus on locking down its devices. This has driven prices for iOS bugs and exploits through the roof. Nowadays, companies are willing to pay around $3 million for software that jailbreaks and hacks iPhones—and researchers are reluctant to report bugs to Apple simply because others pay better.

Governments around the world have been willing to spend a fortune on iOS malware. Saudi Arabia paid $55 million to purchase iPhone malware made by NSO Group, according to a recent report by Israeli newspaper *Haaretz*. There's several companies specializing in iOS malware, such as Azimuth, NSO Group, and some more. But despite the appearances, iOS malware isn't only in the hands of big companies and their government customers.

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv

Security researcher Zuk Avraham recently wrote on Twitter that iOS jailbreaks, the basis of any kind of malware for iOS, aren't as rare as people think, and estimated that there are more than 50 groups who have iOS exploits. While most people believe that only powerful government adversaries have access to iPhone exploits, more discoveries are being made that suggest that lesser-known groups have exploits as well.

Now, even relatively smaller companies have iOS malware.

Earlier this year, Kaspersky Lab reported having found a sophisticated spyware for Android dubbed Skygofree. Sources told Forbes at the time that the spyware was made by Italian government surveillance contractor Negg, a small upstart that isn't as well known as NSO or Azimuth. While investigating Negg's Android malware, Kaspersky Lab found that one of its command and control servers pointed to a "rogue Apple [Mobile Device Management] server," according to the company's private report.

A source who received the report shared details contained in it with Motherboard on condition of staying anonymous since they were not authorized to share the information.

Mobile Device Management or MDM is a feature in iOS that allows companies to manage and monitor devices given to their employees. By installing an MDM profile or certificate on an iPhone, a user gives the MDM owner some control over the device. This mechanism can be used by malware creators. In July, security firm Talos found that a hacking group used MDM to target a few iPhones in India (Mobile Device Management can be turned on for every iPhone.)

Costin Raiu, the head of Kaspersky Lab's research team, said that Negg's MDM server is still active. In its private report, Kaspersky Lab researchers wrote that "the code contains many mentions that let us presume that the developer is a small Italian company named Negg."

Negg did not respond to a message sent to its official information email address. When Motherboard called its office, an employee said she'd refer questions to the company owner, who was not available at the time. Apple did not respond to a request for comment.

It's unclear how government hackers get the malware on target's iPhones. Kaspersky Lab researchers speculated it may be via social engineering "using fake mobile operators sites." In other words, this malware does not leverage any bugs or exploits in iOS, but instead takes advantage of MDM, which is a specific design feature in the operating system. In this way, it relies on a tried-and-tested social hacking technique—tricking users into installing something. For many years, the average user could essentially click on any link, download any app, and otherwise use their iPhone without worrying about targeted surveillance. That may soon no longer be the case.

"You're basically turning over administrative control of your phone to the attacker."

In May, Motherboard revealed that Italian cell phone providers were helping cops install malware on suspected criminals' phones.

According to former Cyber Command hacker and now director of cyber solutions at Point3 Ryan Duff, this discovery should not be seen as too much of a worrisome sign.

“As far as MDM as an injection method for malware, it's pretty lame,” Duff told Motherboard in an online chat. “As far as risk goes, it's pretty low. You can't just force an iPhone to connect to an MDM server. You would have to get them to install a device profile onto their phone. You'd need to social engineer them in some way to installing the profile.”

Raiu said that Kaspersky is not sure how Negg—or its customers—get the malware on the target iPhones. It could either be social engineering, Raiu said, or “even physical access.” Kaspersky is unsure if Negg has any zero days or specific iOS exploits.

Even if MDM-based malware is not as sophisticated as malware that gets injected with expensive and unknown vulnerabilities—or zero-days—once it’s on the phone the result is the same: the hackers—be them criminals or government-sponsored—have access to everything on the phone.

“You're basically turning over administrative control of your phone to the attacker,” Duff told me. “So of course they can install malware from there.”

Listen to CYBER, Motherboard’s new weekly podcast about hacking and cybersecurity.

Hacking
|
by Lorenzo Franceschi-Bicchierai
|
Mar 25 2019, 10:53am

Israeli Hacking Company NSO Group Is Trying to Clean Up Its Image

The notorious and controversial Israeli hacking and surveillance tools vendor NSO Group has launched a big marketing campaign with a new website and Google ads.

Image: Courtesy of CBS 60 Minutes

In the summer of 2016, a Dubai-based human rights activist was targeted with a sophisticated iPhone hacking tool. That piece of malware had been developed by NSO Group, an Israeli company that sells surveillance and hacking tools to governments around the world.

It was the first time its malware—called Pegasus—was discovered in the wild, but NSO Group had been selling it since 2011, according to Israeli newspaper Yedioth Ahronoth. In 2016, NSO was so reluctant to get any public attention that it didn’t even have a website, and the little press coverage it got was vague and made it look like the company was secretive.

Three years later, NSO is stepping into the light with a marketing and public relations push unprecedented for a company that operates in the shady world of government hacking contractors. Whereas only two years ago only people who follow the government spyware industry knew what NSO was, it is now giving more interviews to the press (including a segment on *60 Minutes* this weekend), buying Google search ads, and just launched a sleek new website.

“Nothing has been proven.”

Many people probably heard of NSO for the first time in December 2018, when a *New York Times* story that claimed the company helped Saudi Arabia spy on the *Washington Post* journalist Jamal Khashoggi before he was killed in the Saudi consulate in Istanbul, Turkey in October of last year.

A reader who wanted to learn more about NSO would understandably turn to Google search, where, in some cases the first result would be a Google Ad campaign paid for by NSO. The ads are not visible at the time of publication but Motherboard has seen them multiple times over the last few days. Ads for NSO’s new site came up when searching for the company’s name, but also when searching for the name and words such as “abuse,” and “human rights.”

A screenshot of a Google ad for NSO Group. (Image: Motherboard)

An NSO Group spokesperson told Motherboard that “like many companies, NSO purchased Google Search ads as part of our new website launch.”

“The ads are displayed to users who might want to learn more about NSO and our work helping intelligence and law enforcement agencies prevent and investigate crime and terror to save lives,” the spokesperson said in a statement sent via email.

Google did not respond to multiple requests for comment.

The only other time a spyware company like NSO Group did anything like this was when Hacking Team, an Italian company that also sells spyware to governments, made an infamous commercial featuring a hooded actor. In 2012 FinFisher, a British-German competitor, gave Bloomberg access to its managing director.

Got a tip? You can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email

lorenzo@motherboard.tv.

NSO's new website features buzzwordy statements on how the company operates ("We take a pioneering approach to applying rigorous, ethical standards to everything we do") and tries to lure new hires by showcasing employees enjoying the company's game room and doing pilates. The site also claims NSO's tech helps "save thousands of lives around the globe."

NSO Group's marketing campaign has been accompanied by what appears to be a carefully orchestrated public relations tour. In the last few weeks, NSO's founders gave an extensive on the record interview to Yedioth Ahronoth, and sat down with CBS News's *60 Minutes*, allowing cameras inside the company's office for the first time.

In interviews for the Yedioth Ahronoth story and the *60 Minutes* feature, NSO executives didn't share a lot of new information about the company, but took the opportunity to deny any abuses of its technology, and strongly deny Pegasus had any role in the killing of Saudi Arabian journalist Jamal Khashoggi.

"You can dress up Frankenstein all you want, but deep down he's still a monster."

In Yedioth Ahronoth, NSO Group claimed to have helped stop "several very big terror attacks in Europe," and have a crucial role in bringing down Mexican drug lord Joaquín "El Chapo" Guzmán. Talking to *60 Minutes*, NSO Group's co-founder Shalev Hulio said Pegaus spyware has helped save "tens of thousands of people."

This sudden openness comes at a crucial time for the company.

In the last three years, researchers at Citizen Lab, an academic group at the University of Toronto's Munk School that studies how new technologies impact human rights, has uncovered around 30 cases where NSO spyware was used to target human rights activists and journalists in countries like Mexico, United Arab Emirates, but also Canada. In the summer of last year, Amnesty International accused the company of providing malware to someone who targeted one of its researchers. Then in November, *Forbes* found that someone had attempted to hack a Saudi dissident in London with NSO's malware.

Read more: It's Amateur Hour in the World of Spyware and Victims Will Pay the Price

NSO Group's founders also just recently regained control of the company with the help of a European private equity firm. The deal valued the company at around 1 billion, according to reports. As a result of the deal, some financial firms have taken a look at the company, revealing interesting new details about it, such as the fact that the company has more than 60 customers in 35 countries, and around 600 employees.

Despite the multiple public cases of abuse detailed by researchers and journalists, NSO Group's co-president Tami Shachar told *60 Minutes* that "nothing has been proven."

Hulio doubled down, saying "we only had real three cases of misuse, three cases. Out of thousands of cases of saving lives, three was a misuse, and those people or those organizations that misuse the system, they are no longer a customer and they will never be a customer again."

Ronald Deibert, Citizen Lab's founder and director, said NSO Group should acknowledge and prevent abuse, instead of "putting window-dressing on their increasingly smeared public profile."

"Our (and others) data-driven, peer-reviewed and evidence-based research into NSO spyware shows indisputably that their technology has been used to target journalists, human rights defenders, staff at Amnesty International, research scientists, health advocates, and investigators into mass disappearances," Deibert told Motherboard in an email. "That's not something you can PR out of peoples' minds. You can dress up Frankenstein all you want, but deep down he's still a monster."

Listen to CYBER, Motherboard's new weekly podcast about hacking and cybersecurity.

- Tagged:
- mexico
- israel
- cybersecurity
- HUMAN RIGHTS
- hackers
- spyware
- Saudi Arabia
- marketing
- Infosec
- citizen lab
- information security
- NSO Group
- NSO

State of Surveillance
|
by Lorenzo Franceschi-Bicchierai
|
Sep 18 2018, 3:00am

Cyber Sleuths Find Traces of Infamous iPhone and Android Spyware 'Pegasus' in 45 Countries

A new report by digital human rights researchers reveals that the infamous spyware Pegasus, made by NSO Group, has traces in 45 countries around the world, including the United States.

Security researchers say they have found traces of an infamous iPhone and Android government spyware program in 45 countries around the world over the last two years.

Citizen Lab, a digital rights watchdog at the University of Toronto's Munk School of Global Affairs, published a report on Tuesday detailing a new scanning technique to identify systems used by governments who have purchased the so-called "Pegasus" spyware, made by the Israel-based NSO Group. Thanks to this technique, Citizen Lab's researchers said they were able to identify 1,091 IP addresses that matched their fingerprint for NSO's spyware. Then, the researchers clustered the IP addresses into 36

separate operators with traces in 45 countries where these government agencies "may be conducting surveillance operations" between August 2016 and August 2018.

Some of the countries where the researchers spotted Pegasus in democratic countries, such as the United States, France, and the UK, but there's also countries with questionable human rights records such as the United Arab Emirates, Bahrain, Mexico, Turkey, and Yemen. There's a caveat though. In some cases, the researchers aren't sure if the traces they found indicate an infection—thus a target that may have been hacked from a foreign country—or an operator.

"Sometimes it feels like we're shouting in the dark. Cases of spyware abuse keep piling up, and evidence keeps mounting that spyware is sold to governments that shouldn't have it," Bill Marczak, one of the authors of the report, told Motherboard in an online chat. "I can only hope that our research is causing these companies to think twice about sales where there is the potential for spyware abuse, causing potential customers to think twice about being associated with a company dealing with repressive governments, and causing potential investors to think twice about the inherently risky business of selling spyware to dictators."

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv

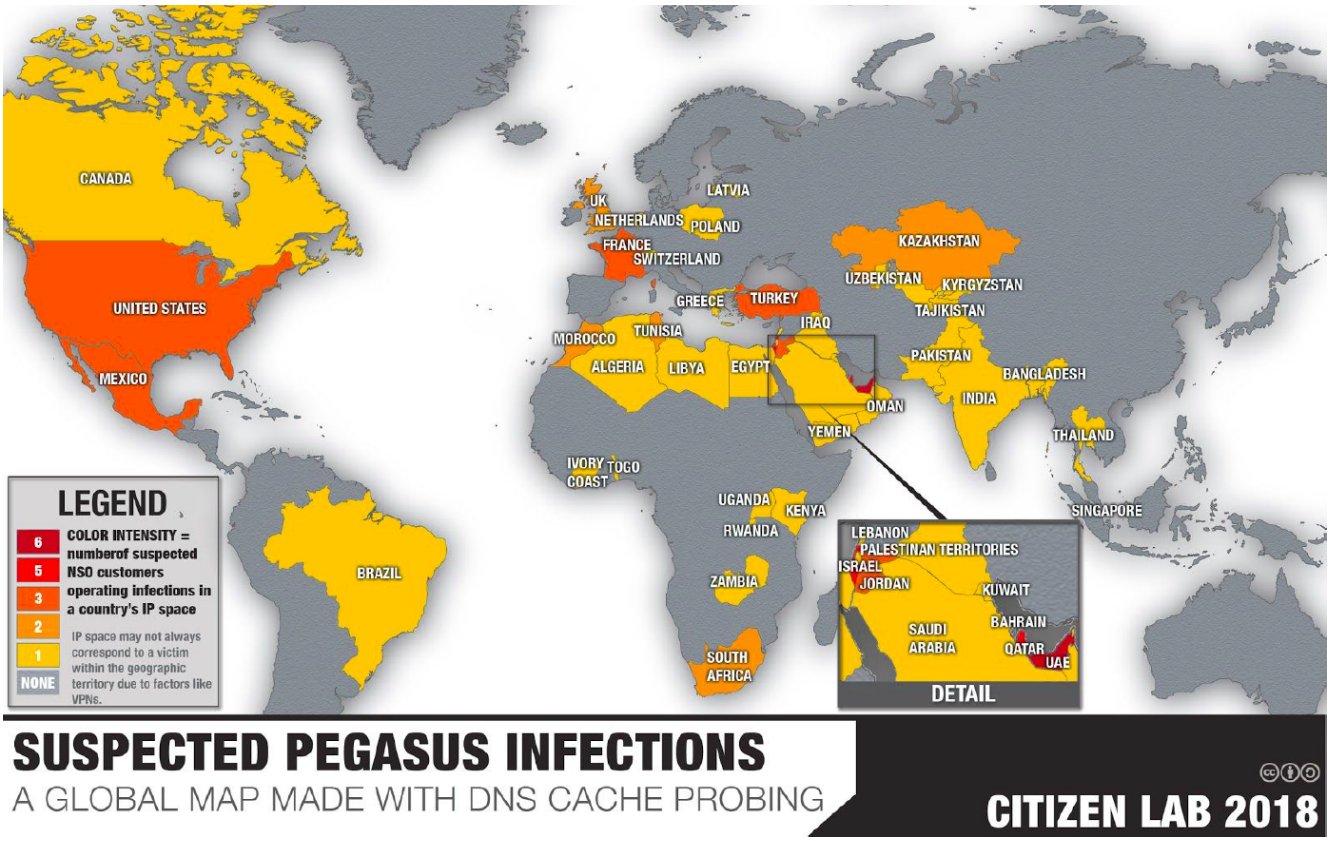
Mobile security firm Lookout could not confirm all the countries Citizen Lab identified but said that it is also tracking NSO and that it have detected "three digits" Pegasus infections around the world, meaning more than 100.

"We know NSO is continuing to expand their operations, they're getting lots of customers," Lookout's vice president of security intelligence Mike Murray said in a telephone interview.

In a statement, an NSO spokesperson said that "the list of countries in which NSO is alleged to operate is simply inaccurate."

"NSO does not operate in many of the countries listed [in the report]," the spokesperson said.

Digital human rights researchers have been studying companies in the government spyware business—so-called "lawful intercept" in industry parlance—for years. These are companies such as the Italian Hacking Team, the Anglo-German FinFisher, and NSO itself, which produce surveillance software and market it exclusively to government agencies around the world. Over the years, Citizen Lab and other organizations have documented several cases of countries abusing these tools to target journalists, dissidents, and human rights workers.



Citizen Lab in particular has also been able to trace and map the proliferation of tools like Hacking Team's Remote Control System spyware and FinFisher's product. In 2014, Citizen Lab found Hacking Team in 21 countries. And the organization found FinFisher in 25 and 32 countries during scans conducted in 2013 and 2015, respectively.

In 2016, Citizen Lab and Lookout found that the government of the United Arab Emirates had attempted to hack the iPhone of well-known human rights activist Ahmed Mansoor with NSO's spyware. (Mansoor is now imprisoned.) Israel and the UAE have officially no diplomatic relations, but according to an Israeli tech entrepreneur who has visited Dubai multiple times, this doesn't stop Israeli companies from doing business there.

Read More: Ron Deibert's Lab Is The 'Robin Hood' of Cybersecurity

"Don't scream on the street that you're Israeli and it's OK," the entrepreneur told Motherboard. He spoke under condition of anonymity not to strain his relationship with the Israeli government.

"Three times I was there, I was there with Israeli phone, I used my Israeli phone," he told me "And I know that they have all kinds of technology that once I landed they know that there is an Israeli in the country. No way that they don't know. They don't care."

Neither does Israel, he said, adding that companies like NSO, which sell sensitive tech like spyware, need to apply for an export license before each sale.

Representatives of the Israeli government in the US did not respond to a request for comment.

"The company works in full compliance with all applicable laws, including export control laws," NSO's statement read. "Our products have saved the lives of thousands of people."

Solve Motherboard's weekly, internet-themed crossword puzzle: Solve the Internet.

- Tagged:
- SURVEILLANCE
- News
- israel
- Hacking
- cybersecurity
- iPhone
- malware
- Hacking Team
- spyware
- Infosec
- UAE
- citizen lab
- Tech news
- NSO Group
- Government Spyware
- lawful intercept

State of Surveillance
|
by Lorenzo Franceschi-Bicchierai
|

Cyber Sleuths Find Traces of Infamous iPhone and Android Spyware 'Pegasus' in 45 Countries

A new report by digital human rights researchers reveals that the infamous spyware Pegasus, made by NSO Group, has traces in 45 countries around the world, including the United States.

Security researchers say they have found traces of an infamous iPhone and Android government spyware program in 45 countries around the world over the last two years.

Citizen Lab, a digital rights watchdog at the University of Toronto's Munk School of Global Affairs, published a report on Tuesday detailing a new scanning technique to identify systems used by governments who have purchased the so-called "Pegasus" spyware, made by the Israel-based NSO Group. Thanks to this technique, Citizen Lab's researchers said they were able to identify 1,091 IP addresses that matched their fingerprint for NSO's spyware. Then, the researchers clustered the IP addresses into 36 separate operators with traces in 45 countries where these government agencies "may be conducting surveillance operations" between August 2016 and August 2018.

Some of the countries where the researchers spotted Pegasus in democratic countries, such as the United States, France, and the UK, but there's also countries with questionable human rights records such as the United Arab Emirates, Bahrain, Mexico, Turkey, and Yemen. There's a caveat though. In some cases, the researchers aren't sure if the traces they found indicate an infection—thus a target that may have been hacked from a foreign country—or an operator.

"Sometimes it feels like we're shouting in the dark. Cases of spyware abuse keep piling up, and evidence keeps mounting that spyware is sold to governments that shouldn't have it," Bill Marczak, one of the authors of the report, told Motherboard in an online chat. "I can only hope that our research is causing these companies to think twice about sales where there is the potential for spyware abuse, causing potential customers to think twice about being associated with a company dealing with repressive governments, and causing potential investors to think twice about the inherently risky business of selling spyware to dictators."

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv

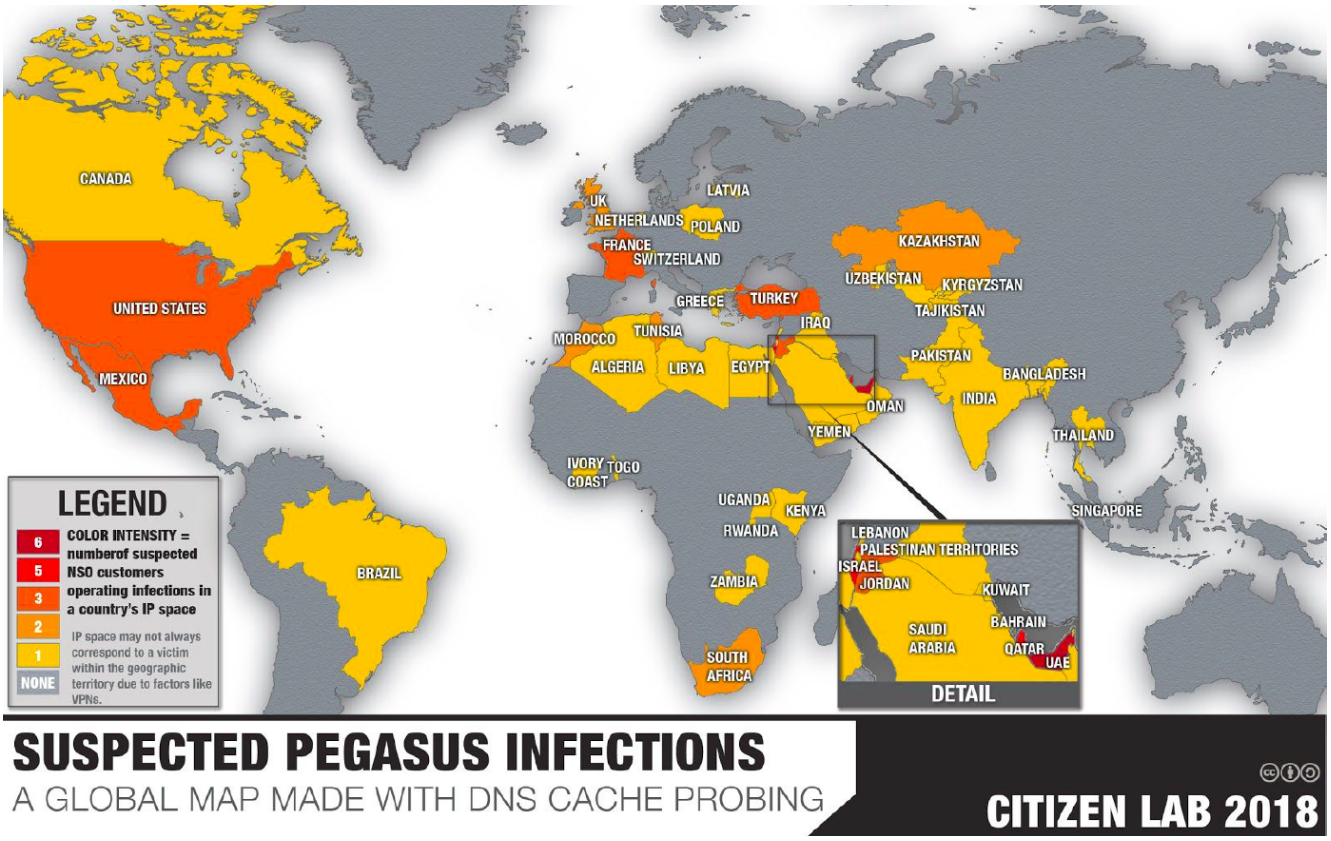
Mobile security firm Lookout could not confirm all the countries Citizen Lab identified but said that it is also tracking NSO and that it have detected "three digits" Pegasus infections around the world, meaning more than 100.

"We know NSO is continuing to expand their operations, they're getting lots of customers," Lookout's vice president of security intelligence Mike Murray said in a telephone interview.

In a statement, an NSO spokesperson said that "the list of countries in which NSO is alleged to operate is simply inaccurate."

"NSO does not operate in many of the countries listed [in the report]," the spokesperson said.

Digital human rights researchers have been studying companies in the government spyware business—so-called "lawful intercept" in industry parlance—for years. These are companies such as the Italian Hacking Team, the Anglo-German FinFisher, and NSO itself, which produce surveillance software and market it exclusively to government agencies around the world. Over the years, Citizen Lab and other organizations have documented several cases of countries abusing these tools to target journalists, dissidents, and human rights workers.



Citizen Lab in particular has also been able to trace and map the proliferation of tools like Hacking Team's Remote Control System spyware and FinFisher's product. In 2014, Citizen Lab found Hacking Team in 21 countries. And the organization found FinFisher in 25 and 32 countries during scans conducted in 2013 and 2015, respectively.

In 2016, Citizen Lab and Lookout found that the government of the United Arab Emirates had attempted to hack the iPhone of well-known human rights activist Ahmed Mansoor with NSO's spyware. (Mansoor is now imprisoned.) Israel and the UAE have officially no diplomatic relations, but according to an Israeli tech entrepreneur who has visited Dubai multiple times, this doesn't stop Israeli companies from doing business there.

Read More: Ron Deibert's Lab Is The 'Robin Hood' of Cybersecurity

"Don't scream on the street that you're Israeli and it's OK," the entrepreneur told Motherboard. He spoke under condition of anonymity not to strain his relationship with the Israeli government.

"Three times I was there, I was there with Israeli phone, I used my Israeli phone," he told me "And I know that they have all kinds of technology that once I landed they know that there is an Israeli in the country. No way that they don't know. They don't care."

Neither does Israel, he said, adding that companies like NSO, which sell sensitive tech like spyware, need to apply for an export license before each sale.

Representatives of the Israeli government in the US did not respond to a request for comment.

"The company works in full compliance with all applicable laws, including export control laws," NSO's statement read. "Our products have saved the lives of thousands of people."

Solve Motherboard's weekly, internet-themed crossword puzzle: Solve the Internet.

- Tagged:
- SURVEILLANCE
- News
- israel
- Hacking
- cybersecurity
- iPhone
- malware
- Hacking Team
- spyware
- Infosec
- UAE
- citizen lab
- Tech news
- NSO Group
- Government Spyware
- lawful intercept

Watch This Next

State of Surveillance
|
by Lorenzo Franceschi-Bicchierai and Joseph Cox
|
Sep 20 2018, 8:05am

They Got 'Everything': Inside a Demo of NSO Group's Powerful iPhone Malware

A source managed to see Israeli surveillance vendor NSO Group's powerful iPhone malware up close. Despite a wave of highly controversial customers, the company appears to be popular worldwide.

Image:

When an Israeli entrepreneur went into a meeting with the infamous spyware vendor NSO, company representatives asked him if it would be OK for them to demo their powerful and expensive spying software, known as Pegasus, on his own phone.

The entrepreneur, who spoke to Motherboard on condition of anonymity because he was not authorized to talk about the meeting, agreed, but said that NSO would have to target his other iPhone, which he brought with him and had a foreign phone number. He gave NSO that phone number and put the phone on the desk.

After "five or seven minutes," the contents of his phone's screen appeared on a large display that was set up in the meeting room, all without him even clicking on a malicious link, he said.

"I see clicking on all kinds of icons: email icon, SMS icon, and other icons," he told Motherboard. "And suddenly I saw all my messages in there and I saw all the email in there and they were capable to open any information that was on my [iPhone]."

The entrepreneur added that the NSO representatives accessed the microphone and the camera on his iPhone.

That demonstration highlighted the power of an increasingly popular product among governments: software for remotely hacking phones in order to access communications and other data from targets. NSO is one of the main companies providing such a product to agencies around the world, including a number of customers that have used it to target human rights activists, nonprofit workers, and journalists in the United Arab Emirates and Mexico.

Got a tip? You can contact Lorenzo Franceschi-Bicchierai securely on Signal on +1 917 257 1382, or OTR on lorenzofb@jabber.ccc.de; and Joseph Cox on Signal on +44 20 8133 5190, or OTR on jfcox@jabber.ccc.de. Details on our SecureDrop, a system to anonymously submit documents or information, can be found here.

Pegasus can infect fully up-to-date Android and iPhone devices, and siphon a target's emails, Facebook chats, and photos; pick up their GPS location and phone calls, and much more. NSO provides this toolkit, and then customers—law enforcement or intelligence agencies—deploy it themselves on their targets. As the *New York Times* recently reported, NSO demos its products to potential clients. The company is currently facing a number of lawsuits, including allegations it participated in illegal hacking operations itself.

The company operated in relative secrecy until researchers at Citizen Lab published a report on NSO in 2016 linking the company's product to the hack of Ahmed Mansoor, a human rights activist in the United Arab Emirates.

A source familiar with NSO told Motherboard that the company has around 600 employees, with approximately 250 working in research and development—which includes creating exploits in-house to break into phones. (Motherboard confirmed that the source has direct and current knowledge of the company.)

The company has a group of engineers dedicated to making sure the company's tools keep working because cell phone companies are in a constant "war" against government hacking providers "to block all those open windows that allow companies like NSO to go in," according to the entrepreneur who attended the meeting, who was told that as part of the company's sales pitch. NSO typically tries to keep a low profile. It has a minimal web presence and only attends select trade shows, though copies of its product brochures have leaked over the years.

The source familiar with NSO added the company has around 100 employees in customer support.

Human rights organizations have repeatedly and for years criticized NSO for selling its products to customers that targeted not just political dissidents like Mansoor, but journalists in Mexico, and an Amnesty International researcher. In the statement previously sent to Motherboard, NSO said its products are used to combat terrorism, child abduction, and other serious crimes.

Read more: Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia

On Tuesday, researchers from Citizen Lab published a report saying it had found NSO's Pegasus product being used in 45 countries, including in the United States.

In a statement sent to Motherboard, NSO pushed back and said many of the countries listed by Citizen Lab were not customers, and said that its product cannot work in the United States. Earlier research has noted that Pegasus has a so-called "suicide" feature, which can disable the customer's deployment of the malware. The source familiar with NSO elaborated, and said this can trigger if the customer is authorized to use the product against targets in one country but the target moves into another.

Worldwide, NSO's customers have purchased the capability to target between roughly 350 to 500 devices (15 to 30 per customer), according to the source. More potential customers approached NSO after the first Citizen Lab report on NSO's tools being used to target Mansoor, the source said.

For every potential sale, NSO has to get explicit permission—an export license—from Israel's Ministry of Defense. With that green light, the company then asks a so-called business ethics committee to approve the sale.

"NSO's Business Ethics Committee, which includes outside experts from various disciplines, including law and foreign relations, reviews and approves each transaction and is authorized to reject agreements or cancel existing agreements where there is a case of improper use," NSO said in the statement. The source familiar with NSO said the committee includes two lawyers who are experts in human rights, and three former US officials.

It's up to them to approve the sale, and they have shut down deals that had already been closed and approved by the Israeli government, according to the source.

NSO employees visit their customers audit how the tools are being used, the source added. These visits involve interviews with operators and visits to the facilities. If the NSO employees see something they don't like, they can escalate the issue, which can lead to the customer's systems being shut down remotely, the source said.

NSO's competitor Hacking Team in the past also claimed to have a similar committee. But after the devastating breach the company suffered in 2015, leaked documents and emails revealed that the alleged external independent committee was simply a law firm hired by Hacking Team to make sure its deals did not go against local export laws. Hacking Team continued to sell to a slew of highly controversial customers, including Sudan.

That's why NSO will have to do better to convince its critics.

"NSO Group's claims about 'strict due diligence' and a supposed 'Business Ethics Committee' are implausible in the face of the facts," Citizen Lab's director Ron Deibert told Motherboard. "Our research on the UAE, Mexico, and, more recently, targets of espionage at Amnesty International—in sum, dozens of targets that are neither criminals nor terrorists— demonstrate their ineffectiveness."

Amit Serper, an Israeli security researcher at Cybereason who was invited for a job inteview at NSO, is skeptical about the company's ability to avoid customers that will abuse its tools. (Serper said he has no direct knowledge of abuses.)

"It's like Hacking Team," Serper told Motherboard in an online chat. "Those companies always end up doing business with the wrong people—because money."

Regardless, NSO's business is booming, and that's because its products are capable of impressing those who see them in action.

"I didn't see it coming and everything was on the wall in five minutes," the entrepreneur said.