Security Newsletter

26 Jul 2021

Subscribe to this newsletter

NSO Says 'Enough Is Enough,' Will No Longer Talk to the Press About Damning Reports

The Israeli surveillance technology maker denied that the list, which underpins a series of bombshell stories in several media outlets, has anything to do with the company.

The spyware giant NSO Group claimed that a list of 50,000 phone numbers, which is the basis of a series of explosive stories about alleged abuses by its customers, has nothing to do with the company or its customers.

In the last few days, a group of news outlets from all over the world, including The Washington Post and the Guardian have published several stories detailing new alleged abuses of NSO's spyware in several countries, including India, Hungary, Rwanda, and others. These stories are based on a leaked list of more than 50,000 phone numbers, which are alleged to be people of interest to NSO's customers.

Amnesty's security lab analyzed 37 smartphones included in the list, and found evidence that they were either hacked or targeted with NSO's spyware.

Read More on Vice

More #News

- New Leak Reveals Abuse of Pegasus Spyware to Target Journalists Globally
- Hooking Candiru - Another Mercenary Spyware Vendor Comes into Focus
- EU takes aim at ransomware with plans to make Bitcoin traceable, prohibit anonymity
- TSA issues second cybersecurity directive for pipeline companies

- Home and office routers come under attack by China state hackers, France warns
- Researchers Hid Malware Inside an AI's 'Neurons' And It Worked Scarily Well
- Twitter reveals surprisingly low two-factor auth (2FA) adoption rate
- Akamai DNS global outage takes down major websites, online services
- CISA warns of stealthy malware found on hacked Pulse Secure devices
- Dutch Police Arrest Two Hackers Tied to "Fraud Family" Cybercrime Ring
- Kaseya Gets Universal Decryptor to Help REvil Ransomware Victims
- APT Hackers Distributed Android Trojan via Syrian e-Government Portal
- US court gets UK Twitter hack suspect arrested in Spain

#Breach Log

- Attackers deploy cryptominers on Kubernetes clusters via Argo Workflows
- Ransomware gang breached CNA's network via fake browser update
- MacOS malware steals Telegram accounts, Google Chrome data
- Saudi Aramco data breach sees 1 TB stolen data for sale
- 1,000 GB of local government data exposed by Massachusetts software company

#Patch Time!

- Turns Out That Low-Risk iOS Wi-Fi Naming Bug Can Hack iPhones Remotely
- Microsoft shares mitigations for new PetitPotam NTLM relay attack
- Apple fixes bug that breaks iPhone WiFi when joining rogue hotspots
- Atlassian asks customers to patch critical Jira vulnerability
- New Linux kernel bug lets you get root on most modern distros
- 16-year-old bug in printer software gives hackers admin rights
- Fortinet fixes bug letting unauthenticated hackers run code as root
- Oracle Warns of Critical Remotely Exploitable Weblogic Server Flaws
- Windows "HiveNightmare" bug could leak passwords

#Tech and #Tools

- Meet WiFiDemon – iOS WiFi RCE 0-Day Vulnerability, and a Zero-Click Vulnerability That Was Silently Patched
- Sequoia: A Local Privilege Escalation Vulnerability in Linux's Filesystem Layer
- GitHub brings supply chain security features to the Go community
- When coin miners evolve, Part 1: Exposing LemonDuck and LemonCat, modern mining malware infrastructure
- Forgot password? Taking over user accounts Kaminsky style
- Summer of SAM - incorrect permissions on Windows 10/11 hives
- Cloudflare's Handling of an RCE Vulnerability in cdnjs

Summer break!

It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks but don't worry, we'll be back. See you soon for some awesome infosec news!

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us