OPINI PUBLIK

Pratama Persadha: Hindari Pegasus, Sebaiknya Presiden dan Pejabat Negara Tak Pakai Whatsapp

Updates - OPINIPUBLIK.ID
Jul 25, 2021 - 17:25

Dr. Pratama Persadha, Chairman CISSReC

JAKARTA - Pegasus kembali ramai diperbincangkan setelah laporan Amnesty Internasional bahwa ada sejumlah Presiden, Perdana Menteri dan Raja yang menjadi target dari malware buatan NSO, perusahaan asal Israel. Salah satu

yang menjadi perhatian internasional adalah info bahwa salah satu yang menjadi korban Pegasus adalah Presiden Prancis, Emmanuel Macron.

Laporan dari Amnesty International dan Citizen Lab, menyusul dugaan kebocoran data pada 50.000 target potensial alat mata-mata Pegasus NSO,termasuk didalamnya adalah 10 Perdana Menteri, 3 Presiden dan 1 Raja menjadi target Pegasus. Sebelumnya juga ramai diberitakan bahwa Jamal Kashogi, jurnalis Saudi yang tewas juga menjadi target Pegasus.

Pegasus merupakan malware berbahaya yang bisa masuk ke gawai seseorang dan melakukan kegiatan surveillance atau mata-mata. Pegasus sebenarnya merupakan sebuah "trojan" yang begitu masuk ke dalam sistem target, dapat membuka "pintu" bagi penyerang untuk dapat mengambil informasi yang berada di target. Lebih spesifik boleh dikatakan bahwa pegasus merupakan sebuah spyware.

Dalam keterangannya pada Sabtu (24/7), pakar keamanan siber Pratama Persadha menjelaskan bahwa malware seperti ini banyak juga di jual bebas di pasaran, bahkan ada beberapa yang bisa didapatkan dengan gratis. Yang membedakan adalah teknik atau metode yang digunakan agar malware tersebut untuk dapat menginfeksi korban, serta teknik untuk menyembunyikan diri agar tidak dapat terdeteksi oleh anti virus maupun peralatan security dan juga teknik agar tidak dapat di tracking.

"Saat ini sangat sulit untuk menghindari kemungkinan serangan malware. Pegasus sendiri hanya membutuhkan nomor telepon target. Ponsel bisa jadi terhindar dari Pegasus jika nomor yang digunakan tak diketahui oleh orang lain," terang chairman lembaga riset siber CISSReC (communication & information system security research center) ini.

Menurut Pratama, teknik yang digunakan oleh pegasus ini biasa disebut dengan "remote exploit" dengan menggunnakan "zero day attack." Zero day attack merupakan suatu metode serangan yang memanfaatkan lubang keamanan yang tidak diketahui bahkan oleh si pembuat sistem sendiri belum diketahui. Juga serangan ini biasanya sangat sulit terdeteksi oleh perangkat keamanan, walaupun terupdate. Hal ini yang membuat pegasus ini sangat berbahaya.

"Bila menilik malware Pegasus, cukup dengan panggilan WhatsApp, ponsel penerima sudah terinfeksi, bahkan tanpa harus menerima panggilannya. Dengan metode yang sama dan mengirimkan file lewat WhatsApp juga bisa menyebabkan peretasan " kata pria asal Cepu, Kabupaten Blora, Jawa Tengah ini.

Pratama menjelaskan, bahwa tidak hanya aplikasi Whatsapp saja yang bisa dimonitor namun semua aplikasi yang terinstal didalam smartphone tersebut.

Lebih jauh, Pegasus dapat mengumpulkan semua data ponsel jika malware berhasil ditanamkan, maka data dari ponsel bisa disedot dan dikirim ke server. Bahkan yang lebih mengerikan, Pegasus bisa menyalakan kamera atau mikrofon pada ponsel untuk membuat rekaman secara rahasia.

"Prinsipnya adalah, Pegasus bisa melakukan segala hal di Smartphone kita

dengan kontrol dari dashboard. Bahkan bisa melakukan pengiriman pesan, panggilan dan perekamanan yang tidak kita lakukan." terang pria asal Cepu jateng ini.

“Bagi Indonesia ini seharusnya menjadi pegingat pentingnya kita mengembangkan perangkat keras sendiri serta aplikasi chat serta email yang aman digunakan oleh negara, sehingga mengurangi resiko eksploitasi keamanan oleh pihak asing,” terang Pratama.

Ditambahkan Pratama, presiden dan para pejabat penting negara harus waspada disarankan tidak lagi memakai Whatsapp karena menjadi pintu masuk Pegasus. Founder Telegram Paul Durov bahkan menegaskan bila Whatsapp sejak awal memang tak serius membangun keamanan pada aplikasinya.

“Kasus yang paling ramai adalah peretasan ponsel iPhone milik Jeff Bezos. Ponselnya diretas sesaat setelah komunikasi dengan Pangeran Saudi Muhammad bin Salman. Akhirnya foto-foto dan chat pribadi dengan selingkuhannya seorang pembawa berita nasional di AS terkuak ke publik dan Bezos cerai dari istrinya. Dari tim forensik yang memeriksa ponsel Bezos ditemukan bukti yang mengarah pada ponsel telah diretas oleh Pegasus”, jelasnya.

Pratama lantas menghimbau karena saat ini ancaman serupa juga bisa terjadi ke presiden maupun para pejabat di tanah air. Yang paling bisa dilakukan sekarang adalah melakukan forensik pada perangkat gawai yang dibawa. Selanjutnya melakukan protokol keamanan untuk nomor yang dipakai komunikasi antar petinggi negara harus dirahasiakan tidak boleh bocor ke siapapun. Karena nomor ini adalah pintu masuk dari pegasus lewat Whatsapp.

“Ponsel apapun termasuk iPhone masih bisa ditembus oleh Pegasus. Langkah preventif yang paling bisa dilakukan adalah menggunakan software enkripsi, sehingga data yang ditransmisikan atau dicuri oleh pegasus tidak serta merta langsung bisa dibuka atau diolah,” jelasnya.

Dr. Pratama Persadha
Chairman CISSReC