INDONESIA SATU

Dr. Pratama Persadha: Thanos Serang Sejumlah Kementerian dan Lembaga Negara

Tony Rosyid - INDONESIASATU.CO.ID

Sep 14, 2021 - 15:04

Dr. Pratama Persadha, Chairman CISSReC

JAKARTA - Pada Jumat (10/9) Insikt Group mengabarkan adanya peretasan di 10 Kementerian Lembaga pemerintah Indonesia, disebutkan dilakukan oleh Mustang Panda Group, peretas asal Tiongkok menggunakan private ransomware bernama Thanos. Bahkan peretasan ini langsung dikaitkan dengan upaya spionase Tingkok dalam upaya menghadapi situasi yang menghangat di Laut China Selatan.

Dalam keterangannya Minggu (12/9), pakar keamanan siber Pratama Persadha menjelaskan bahwa kita belum mengetahui persis kebenaran dari informasi ini, jadi bisa saja ini baru klaim sepihak. Menurutnya kita perlu menunggu buktinya seperti pada kasus eHAC Kemenkes beberapa waktu lalu.

“Kalau mereka sudah share bukti peretasannya seperti data dan biasanya upaya deface, baru kita bisa simpulkan memang benar terjadi peretasan. 10 kementeriannya yang mana juga masih belum jelas. Namun bila ini spionase antar negara, memang bukti akan lebih sulit untuk didapatkan, karena motifnya bukan ekonomi maupun popularitas,” jelas chairman lembaga riset keamanan siber CISSReC (Communication & Information System Security Research Center) ini.

Dijelaskan Pratama, ini tetap bagus sebagai trigger, untuk semua Kementerian dan Lembaga pemerintah di Indonesia untuk mulai cek-cek sistem informasi dan jaringannya. Lakukan security assesment di sistemnya masing-masing. Perkuat pertahanannya, upgrade SDM nya, dan buat tata kelola pengamanan siber yang baik di institusinya masing-masing.

“Pada pertengahan 2020 juga terjadi isu serupa di lingkungan Kemenlu dan beberapa BUMN. Saat itu ada warning dari Australia bahwa email salah satu diplomat kita mengirimkan malware aria body ke email salah satu pejabat di Australia Barat,” terangnya.

Menurutnya email dari diplomat kita sudah berhasil diambil alih oleh peretas, yang diperkirakan kelompok Naikon asal Tiongkok. Namun juga belum diketahui persis hanya email saja atau sampai perangkat yang diretas, karena banyak malware yang dibuat dengan tujuan menyamai kemampuan malware pegasus yang bisa melakukan take over smartphone.

“Perlu dilakukan deep vulnerable assessment terhadap sistem yang dimiliki. Serta melakukan penetration test secara berkala untuk mengecek kerentanan sistem informasi dan jaringan. Lalu gunakan teknologi Honeypot dimana ketika terjadi serangan maka hacker akan terperangkap pada sistem honeypot ini, sehingga tidak bisa melakukan serangan ke
server yang sebenarnya,” terang Pratama.

Ditambahkan olehnya, perlu juga memasang sensor Cyber Threads Intelligent untuk mendeteksi malware atau paket berbahaya yang akan menyerang ke sistem. Lalu terakhir dan paling penting membuat tata kelola pengamanan siber yang baik dan mengimplementasikan
standar-standar keamanan informasi yang sudah ada.

“Kami telah mencoba melakukan profiling threat actor. Mustang Panda adalah hacker group yang sebagian besar anggota dari Tiongkok dimana grup ini membuat private ransomware yang dinamakan Thanos.”

“Ransomeware ini dapat mengakses data dan credential login pada device PC yang kemudian mengirimkannya ke CNC (command and control) bahkan hacker bisa mengontrol sistem operasi target. Private ransome Thanos mempunyai 43 konfigurasi yang berbeda utk mengelabui firewall dan anti virus, sehingga sangat berbahaya,” terangnya.

Ditambahkan Pratama, segala langkah yang diperlukan harus segera dilakukan pemerintah. Untuk mengetahui apakah tindak spionase ini terkait dengan konflik Laut China Selatan atau tidak. Karena dalam beberapa tahun terakhir tensi terkait isu ini memang meningkat di kawasan Asia Tenggara. Semoga ini menjadi momentum perbaikan keamanan siber di lembaga negara.

Narasumber Dr. Pratama Persadha
Chairman CISSReC