Data tentera Malaysia disyaki dicuri penggodam sama tahun lalu

Januari 11, 2023 @ 9:10pm

SINGAPURA: Kempen penggodaman yang disyaki dikaitkan dengan kerajaan Asia menggodam tujuh sasaran berprofil tinggi di Asia Tenggara dan Eropah, termasuk agensi kerajaan dan tentera, menurut firma keselamatan siber Group-IB.

Bloomberg melaporkan, kumpulan penggodam baharu yang dikenal pasti dan digelar Dark Pink, menggunakan e-mel pancingan data dan perisian lanjutan untuk menjejaskan pertahanan cawangan tentera di Filipina dan Malaysia, serta organisasi kerajaan di Kemboja, Indonesia dan Bosnia-Herzegovina, yang bermula sejak September hingga Disember tahun lalu.

Menurut Group-IB yang berpangkalan di Singapura, penggodam itu juga menyasarkan beberapa organisasi lain membabitkan sebuah pertubuhan bukan berasaskan keuntungan, pertubuhan agama dan agensi pembangunan negara Eropah yang berpangkalan di Vietnam, kata laporan yang diterbitkan hari ini.

Bagaimanapun, sehingga kini agensi kerajaan dan ketenteraan di negara yang dinyatakan itu belum mengeluarkan sebarang ulasan berhubung permintaan e-mel untuk mendapatkan maklum balas.

"Aktiviti Dark Pink adalah signifikan, kerana jelas sekali mereka cuba mencuri dokumentasi daripada rangkaian yang terjejas untuk mencari maklumat sensitif.

"Melihat kepada modus operandi kumpulan itu, mereka menyasarkan sasaran yang merangkumi badan kerajaan dan tentera, serta set alatan canggih mereka, Dark Pink yang berkemungkinan besar adalah kempen pengintipan negara bangsa yang tidak didokumenkan sebelum ini," kata Penganalisis Perisian di Group-IB, Andrey Polovinkin.

Serangan siber yang mungkin berpunca daripada rantau Asia-Pasifik bertujuan untuk pengintipan korporat, termasuk untuk mencuri dokumen dan merakam audio daripada peranti yang disasarkan, menurut Group-IB.

Penggodam menghantar e-mel sasaran mereka yang mengandungi pautan web yang boleh digunakan untuk memuat turun fail berniat jahat, yang kemudiannya akan mencuri maklumat peribadi daripada peranti yang dijangkiti termasuk kata laluan, sejarah penyemak imbas dan data daripada aplikasi sosial seperti Viber dan Telegram.

Sementara itu, penyelidik China dari firma DAS-Security yang berpangkalan di Zhejiang juga menerbitkan laporan di WeChat Jumaat lalu mengenai penggodam, yang dinamakan Saaiwc Group.

Katanya, kumpulan itu menyasarkan inisiatif kepimpinan Vietnam yang dikendalikan oleh jabatan negara Amerika Syarikat, tentera Filipina dan kementerian ekonomi dan kewangan Kemboja masing-masing pada Mei, Oktober dan November.

Organisasi kerajaan dan ketenteraan sering menjadi sasaran utama penggodam, memandangkan data sulit dan sensitif pada rangkaian mereka dan e-mel terus menjadi salah satu kaedah pelanggaran biasa.

Asia menjadi rantau yang paling disasarkan oleh serangan siber, menurut indeks perisikan ancaman IBM Security tahun lalu, yang menerima satu daripada empat serangan yang direkodkan. - AGENSI