Serangan tanpa fail

Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

BAGAIMANA serangan tanpa fail (*fileless atttack*) beroperasi tanpa menggunakan perisian jahat atau *malware*?
- Muhammad, JB.

Kaedah ini membolehkan penjenayah siber tidak perlu meletakkan *malware* pada sistem komputer untuk masuk ke dalamnya. Serangan tanpa fail atau tanpa jejak kaki ini menggunakan aplikasi yang sah atau bahkan sistem pengoperasian dalam serangan dibuat.

Seterusnya dibincangkan secara umum langkah demi langkah bagaimana serangan tanpa fail ini beroperasi.

1 Pengguna akan menerima mesej *spam* menerusi laman sosial, e-mel dan sebagainya yang mengandungi sambungan ke alamat URL laman web jahat.

2 Pengguna yang menerima mesej *spam* mengklik alamat URL laman web jahat tersebut.

3 Laman web jahat atau *malicious web* ini akan memuat masuk fail tertentu seperti fail *Flash* yang merupakan satu rentanan atau *vulnerability* kepada komputer pengguna.

4 Fail tadi akan membuka aplikasi *Windows PowerShell* untuk membolehkan arahan dibuat menerusi baris arahan dan dijalankan menerusi memori komputer.

5 Aplikasi *PowerShell* ini akan muat turun dan menjalankan skrip kod yang ditanam daripada pelayan komputer kawalan dan arahan.

6 Skrip kod *PowerShell* ini akan menempati lokasi pengguna dan menghantar data pengguna kepada penjenayah siber.

Keadaan ini menyebabkan perisian antivirus atau aplikasi keselamatan terlepas pandang dalam membuat imbasan berkaitan dengan serangan tanpa fail ini seperti serangan *Ransomware* dan lain-lain.

Serangan tanpa fail ini mengambil kesempatan ke atas mana-mana aplikasi komputer yang dibenarkan dipasangkan ke dalam komputer sasaran.

Perisian antivirus boleh mengesani serangan ini dengan gabungan pelbagai teknik pengesanan termasuk analisis berasaskan pada corak tingkah laku bagi sesuatu proses atau aplikasi.