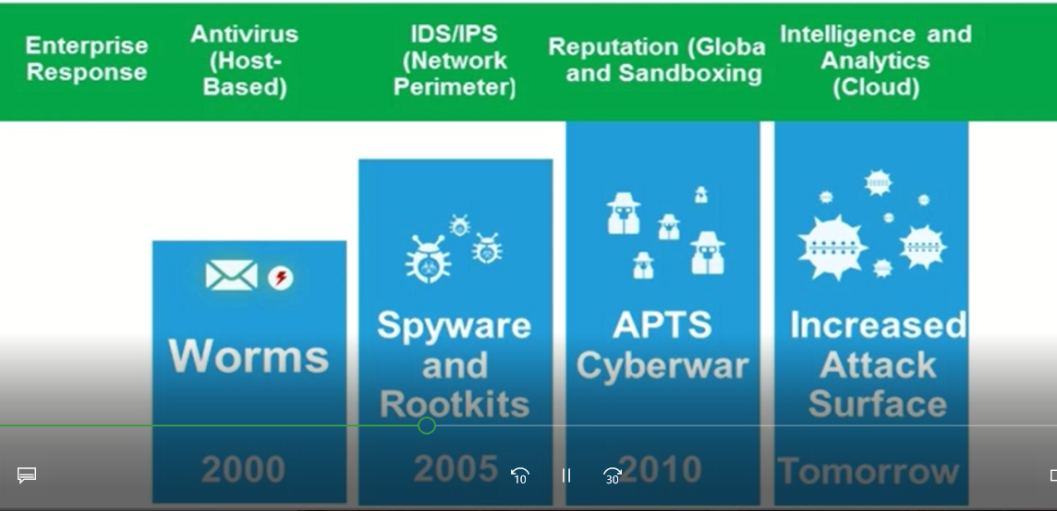
**Threatscape Introduction and Overview**

1. **Pengertian Threatscape**

Merupakan beberapa cara yang dikembangkan menjadi perindustrian untuk mengatasi penyerangan-penyerangan yang ada pada jaringan. Penyerangan-penyerangan bisa menjadi : Perorangan, Kelompok kecil dari hacker, Kejahatan yang terorganisir, Pemerintahan nasional, Ataupun gabungan-gabungannya.

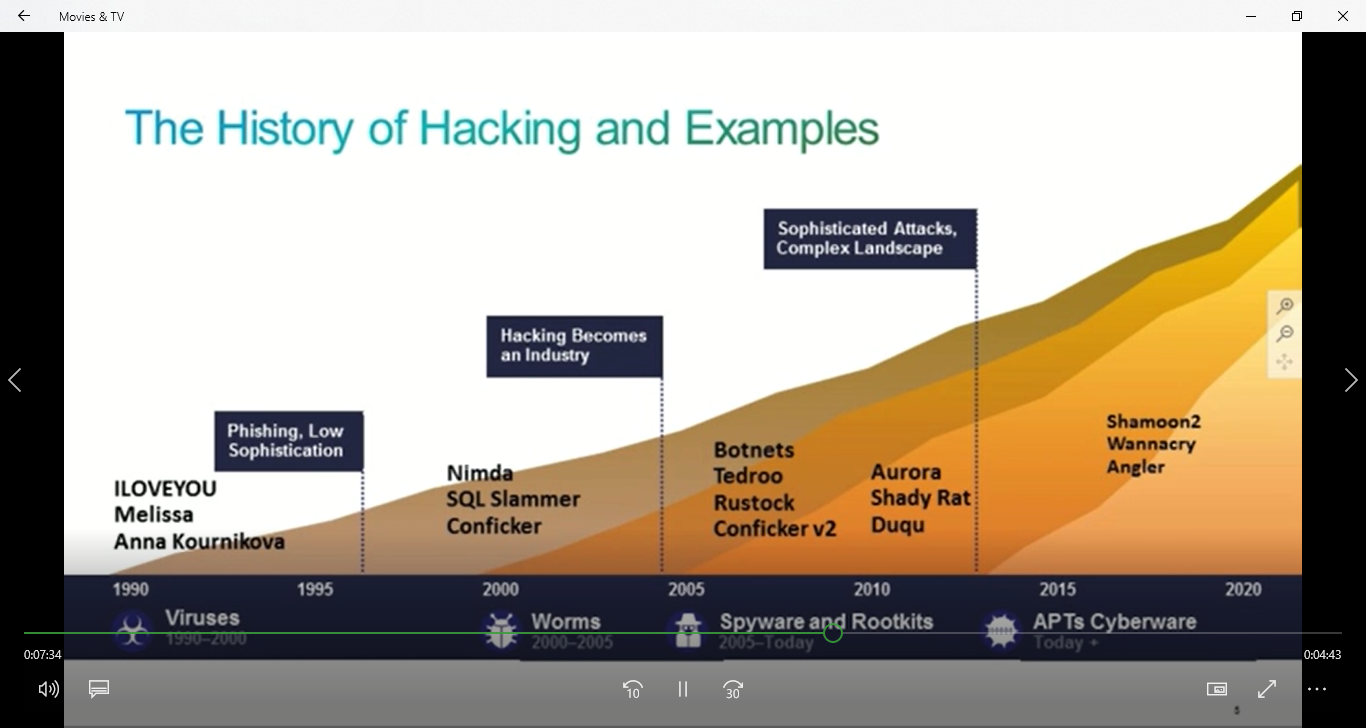
Yang dimaksud dengan penyerangan (attacker) adalah sebuah penggabungan konsep ancaman pengamanan jaringan dari kosep lama maupun konsep yang baru ataupun (yang sedang dikembangkan).

1. **Tanggapan perusahaan mengenai Attacker yang ada**



* Pada tahun 2000 Penyerangan (Atteacker) berupa Worms Threatscapenya adalah Antivirus.
* Pada tahun 2005 Penyerangan (Atteacker) berupa spyware dan rootkits Threatscapenya adalah jaringan parameter IDS/IPS.
* Pada tahun 2010 Penyerangan(Atteacker) berupa APTS Cyberwar Threatscapenya reputation (global dan sandboxing)
* Pada 2011-2020 Penyerangan (Atteacker) berupa increased attack surface Threatscapenya adalah cloud(intelligence and analytics)

1. **Sejarah dari hacking dan contohnya**



Dari gambar diatas dapat kita lihat dimana penyerangan semakin kompleks dan beragam dari tahun ketahun.

1. **Bagaimana perindustrian hacking berkesempatan mendapatkan uang**



Dari data-data diatas dapat kita lihat bagaimana hacking mampu mendapatkan penghasilan dengan berbagai bentuk sajian seperti(spam, account, keamanan jaringan, info dan data penting) dari berbagai aplikasi ataupun media yang banyak digunakan oleh pengguna internet.

1. **Perbedaan Malwer dan attacker tools**

Malwer adalah merupakan software yang membuat dokumen pada computer tampa diketahui oleh pengguna(nama umum dari virus komputer) sedangkan attacker tools adalah hardware yang mampu membuat penyerangan-penyerangan pada computer.

1. **Istilah-istilah pada Threatscape**

* Vulnerability : salah satu kelemahan yang membahayakan keamanan atau fungsi sebuah system.
* Exploit : pengguna mesin untuk mempengaruhi sebuah vulnerability yang bertujuan untuk membahayakan sebuah system.
* Threat : persoalan atau kejadian yang berpotensi untuk pembuat kerusakan ataupun untuk sebuah asset.
* Risk : threat khusus yang berkemungkinan sebagai penyerangan spesifik yang akan mengexploit sebuah vulnerability yang khusus dari sebuah asset.

Daftar Pustaka :

<http://learningnetwork.cisco.com/community/learning_center/ccna-security-training-videos>

Diakses pada tanggal 30 November 2017