Video yang akan di review ini adalah video dari situs resmi Cisco yang berjudul Network Security Threatscape – Review of Attack Types bagian pertama yaitu bagian **Evolusi Serangan Dunia Maya**. Video ini rilis pada 17 November 2017 dan terkahir di modifikasi pada 20 November 2017 oleh kboswort.

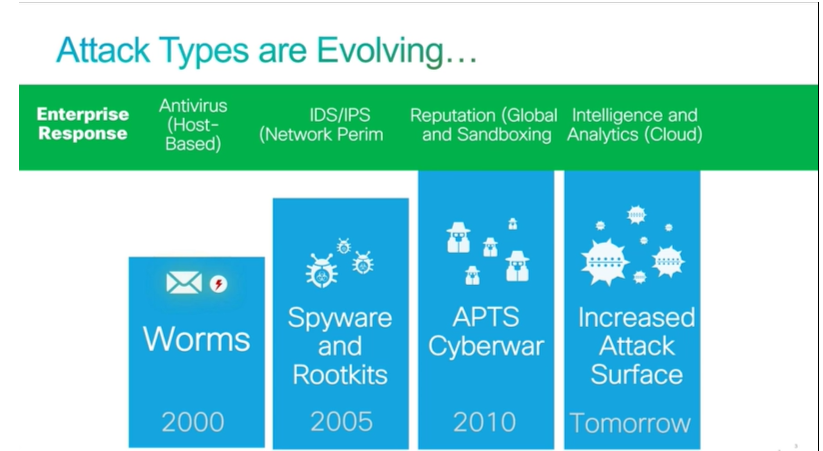




1. **Perkenalan**

Bagian perkenalan ini menjelaskan tentang cara untuk mendapatkan sertifikasi CCNA.

1. **Attacks Type are Evolving**



Bagian kedua menjelaskan tentang perkembangan tipe-tipe serangan. Pada bagian ini disebutkan bahwa secara garis besar terdapat 4 jenis serangan dalam kurun waktu antara tahun 2000 sampai beberapa tahun setelah ini, yaitu:

1. **Worms**

Worms berkembang dari tahun 2000. Worms adalah sebuah serangan semacam cacing yang bisa memakan komputer. Memakan disini dalam artian worm dapat menyerang langsung ke memori komputer. Worm dapat aktif sendiri tanpa bantuan manusia dan dapat mengkopi dirinya sendiri lalu menyebar secara bebas ke dalam jaringan.

1. **Spyware dan Rootkits**

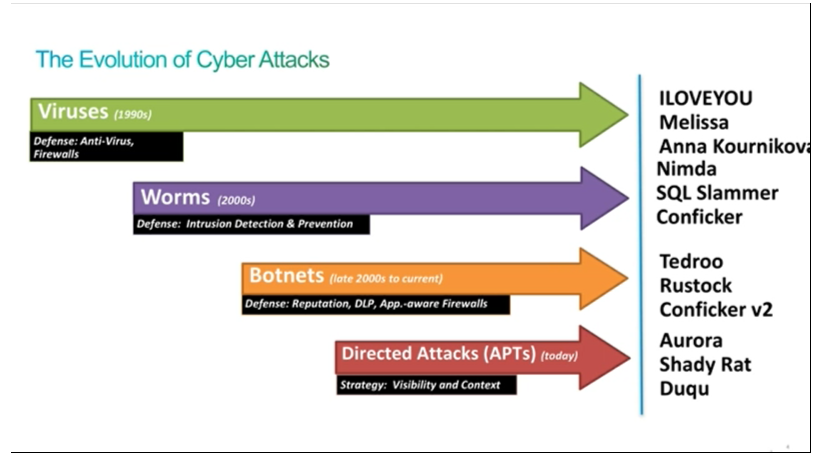
Serangan jenis ini mulai dari tahun 2005. Spyware atau perangkat pengintai melakukan serangan berupa pengumpulan dan pengiriman informasi tentang pengguna komputer tanpa diketahui oleh si pengguna tersebut. Informasi tersebut biasanya adalah pola pencarian dalam internet yang digunakan untuk menampilkan iklan berupa pop-up.

Rootkit adalah salah satu jenis spyware yang “menyusup” ke dalam komputer dengan cara menempel pada file keygen, crack, patch, dan game. Jenis serangan ini sulit di deteksi karena sudah tertanam pada sistem operasi komputer.

1. **APTS Cyberwar**

APTS atau Advanced Persistents Threat adalah salah satu jenis perang didunia maya yang berkembang di tahun 2010. Serangan ini di ibaratkan seperti kanker karena terus menerus berdiam di dalam komputer dalam waktu yang lama. Dan selama itulah ia akan melakukan serangan. Serangan ini sangat sulit di deteksi dan bertujuan untuk melemahkan sistem sehingga menjadi sebuah celah keamanan.

1. **Increased Attack Surface** adalah serangan yang diperkirakan akan berkembang besok atau di masa depan.
2. **The Evolution of Cyber Attack**



Pada bagian ketiga ini dijelaskan evolusi serangan yaitu dimulai dari:

1. **Virus** yang mulai berkembang ditahun 1990’an. Virus yang saat itu lumayan terkenal adalah : ILOVEYOU, Melissa, Anna Kournikova dan Nimda. Defense atau pencegahan yang dilakukan adalah menggunakan *Anti-Virus* dan pertahanan sistem windows yaitu *Firewall*.
2. **Worms** yang berkembang di tahun 2000’an. Worm yang saat itu lumayan terkenal adalah SQL Slammer dan Conficker. Pencegahan yang dilakukan adalah dengan menggunakan metode *Intrusion Detection and Prevention.*
3. **Botnets** yang berkembang dari akhir 2000’an. Botnets yang paling terkenal saat itu adalah Tedroo, Rustock, dan Conficker v2. Pencegahan yang dilakukan adalah dengan *Reputation, DLP, App, aware Firewalls.*
4. **Directed Attack (APTs)** yang sedang berkembang saat ini. Serangan yang paling terkenal adalah Aurora, Shady Rat, dan Duqu. Strategi pencegahannya adalah dengan *Visibility and Context.*
5. **Common Attack Methods**



Bagian keempat ini menjelaskan tentang metode serangan yang saat ini digunakan, yaitu:

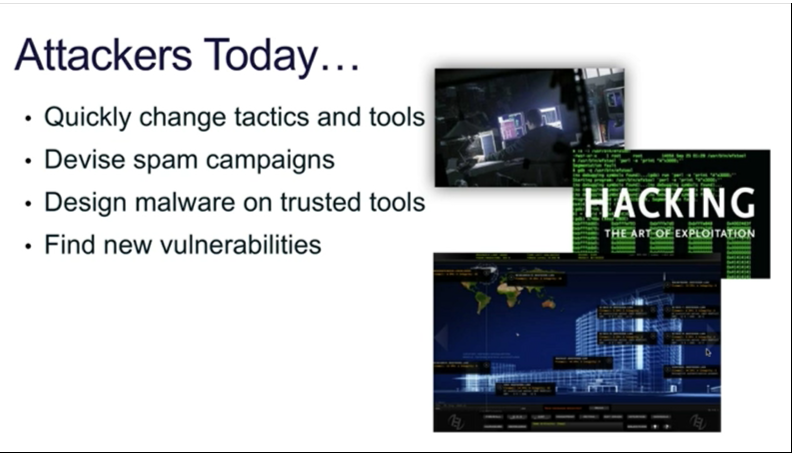
1. **Social Engineering**

Social engineering merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi targetnya melalui hal-hal yang bersifat pribadi. Misalnya melalui penyusupan malware ke dalam file e-mail, pemalsuan notifikasi, pembajakan media sosial, penyamaran sebagai perusahaan tertentu dan lain lain.

1. **Technical Exploit**
2. **Zero-day Attack**

Ini adalah metode serangan untuk mencari celah keamanan yang berada dalam software dan bertujuan untuk menyusupkan spyware, malware, atau guna mendapatkan akses ke informasi pengguna. Istilah zero-day merujuk pada sifat celah keamanan yang tidak diketahui keberadaannya oleh orang lain, termasuk oleh pihak pengembang software itu sendiri.

1. **Attackers Today**



Bagian kelima ini menjelaskan tentang kebiasaan atau sifat penyerang saat ini, yaitu:

1. Cepat mengubah taktik dan tools
2. Merencanakan penyebaran spam
3. Mendesain malware kedalam tool yang terpercaya
4. Menemukan celah baru

REFERENSI

<https://learningnetwork.cisco.com/docs/DOC-33768> Diakses pada 1 Desember 2017.