TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

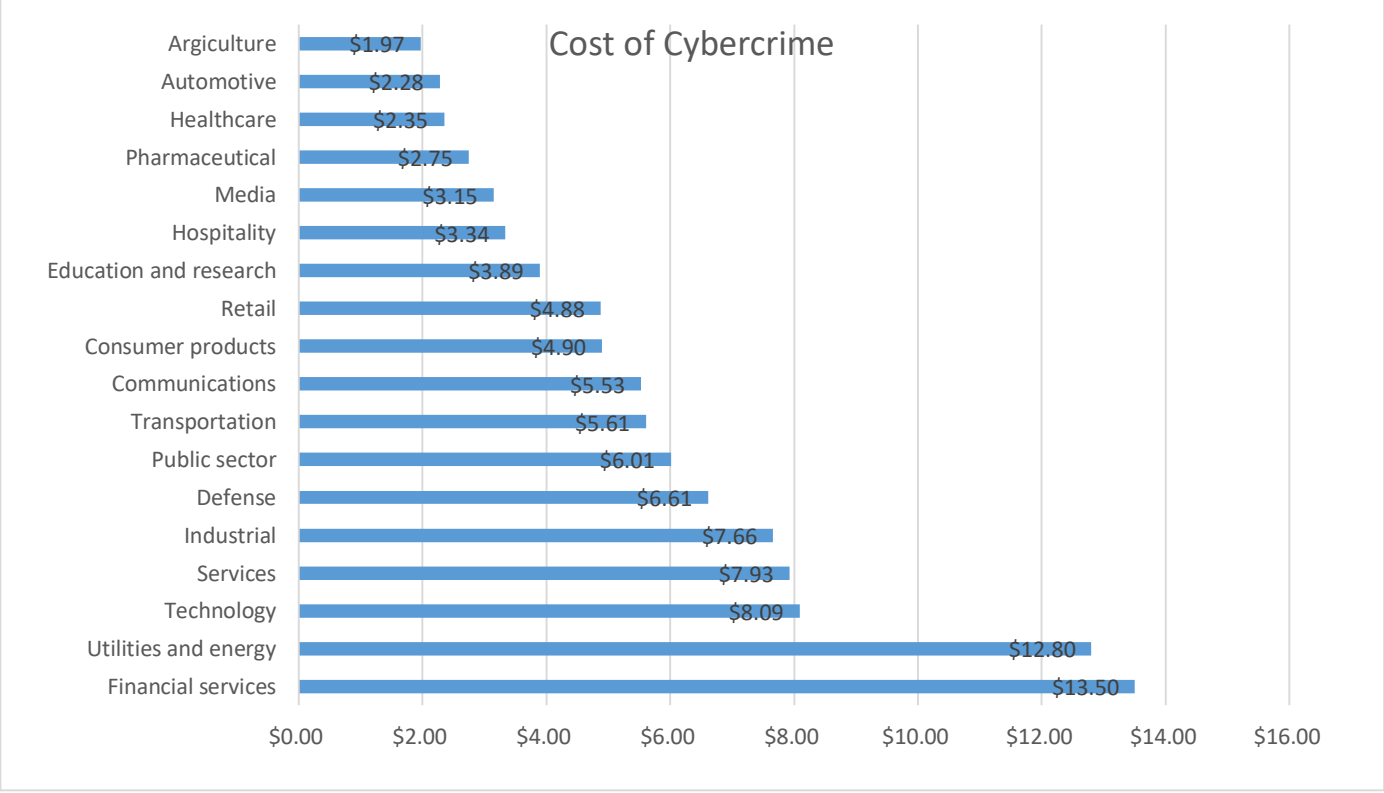
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Forensic Investigations: Tools and Hacks Observed - Ondrej Krehel

Biaya dari Cybercrime

Rata-rata biaya pertahun dari cybercrime dalam jutaan USD per sektor ganda perusahaan.

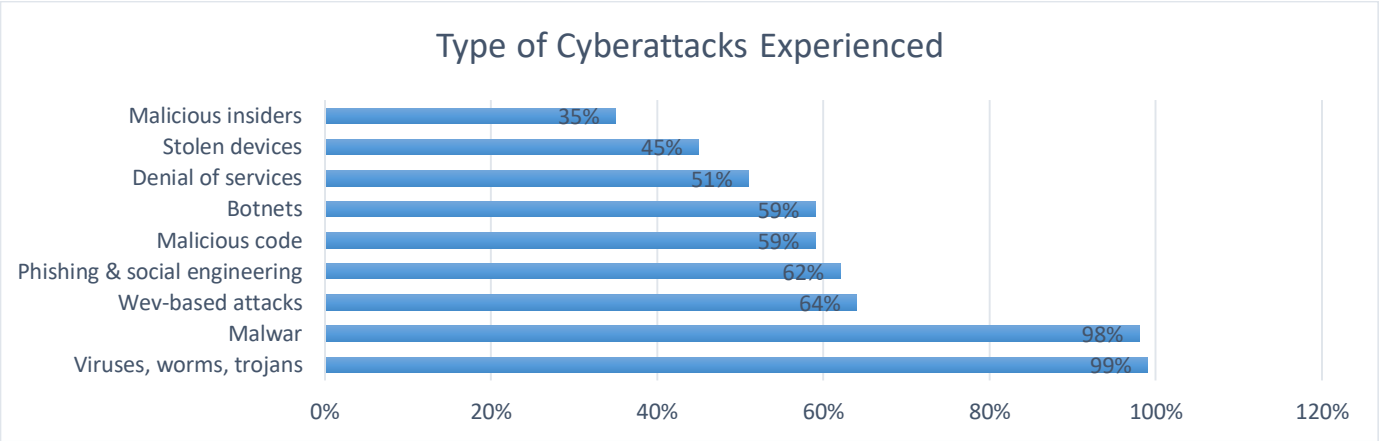
Sector	Cost
Financial services	$13.50
Utilities and energy	$12.80
Technology	$8.09
Services	$7.93
Industrial	$7.66
Defense	$6.61
Public sector	$6.01
Transportation	$5.61
Communications	$5.53
Consumer products	$4.90
Retail	$4.88
Education and research	$3.89
Hospitality	$3.34
Media	$3.15
Pharmaceutical	$2.75
Healthcare	$2.35
Automotive	$2.28
Argiculture	$1.97



Jenis serangan cyber yang dialami

Type	Percentage
Viruses, worms, trojans	99%
Malwar	98%
Wev-based attacks	64%
Phishing & social engineering	62%
Malicious code	59%

Botnets	59%
Denial of services	51%
Stolen devices	45%
Malicious insiders	35%



Tools

Havij

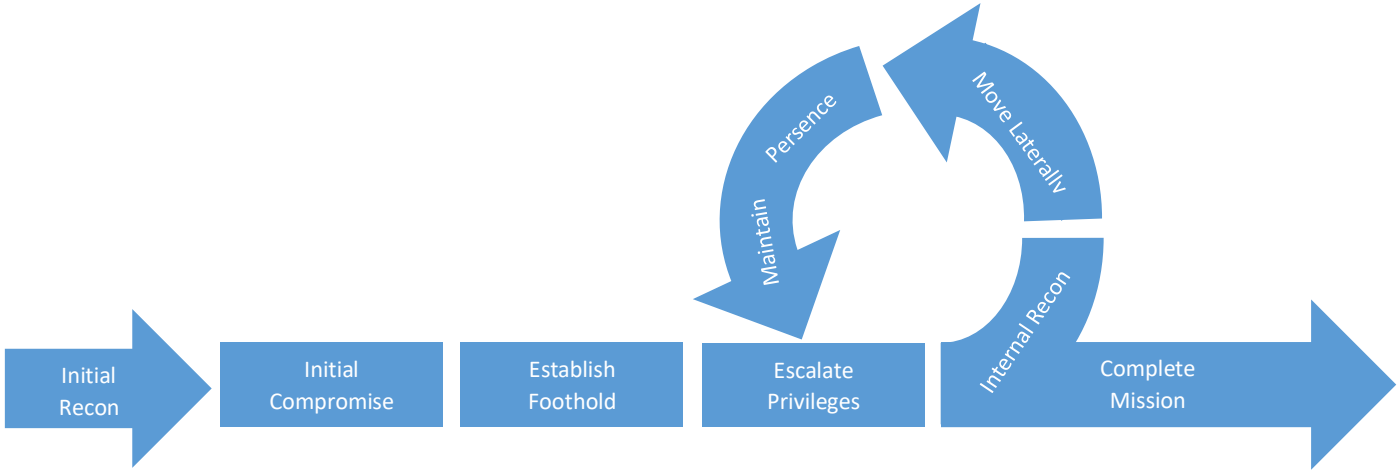
- Tools yang bisa:
  - back-end database fingerprinting
  - pengambilan DBMS login names and password hashes
  - dump tabales and columns
  - mengambil data dari database
  - mengeksekusi SQL statements terhadap server
  - mengakses file system and mengeksekusi operating system shell commands

Mimikatz

- Tools yang bisa mengekstrak dari RAM:
  - Plaintext passwords
  - Hashes
  - PIN codes
  - Kerberos tickets
- Bisa juga melakukan pass-the-hash, pass-the-ticket, atau membuat Golden ticket
- Digunakan dalam APT campaigns

Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) adalah jenis malware yang dapat tidak terdeteksi selama jangka waktu yang lama, menunggu kesempatan untuk menyerang, dan membocorkan data anda secara diam-diam.



APT Lifecycle

- Acquiring Volatile Evidence
  - Network Conncections
    - NMAP
    - Netstat
  - Running Processes
    - Procmon
    - Process Monitor
  - RAM Capture and Analysis
    - Volatility
- Network Traffi Analysis
  - tshark, tcpdump.
- Initial Malware Processing
  - Remux - Mastiff, Viper, Maltrieve

- Tools Gather the following:
  - Network Connections
  - Running Processes
  - RAM Capture and Analysis
- Network Traffic Analysis
- Initial Malware Processing
- Digital Forensic Collection and Analysis of stored Information

Network Forensics

Case Study: AlienSpy at Wall Street

AlienSpy merupakan backdoor yang digunakan untuk melakukan kontrol remote desktop, mengumpulkan data, spionase dll. Malware ini memiliki berbagai nama alias diantaranya Adwind RAT (Remote Access Tool), AlienSpy, Frutas, jFrutas, Unrecom, Sockrat, JSocket, dan jRat.

Korban biasanya mendapatkan email dengan attachment, ketika user mengklik membuka file ini maka malware terinstall.

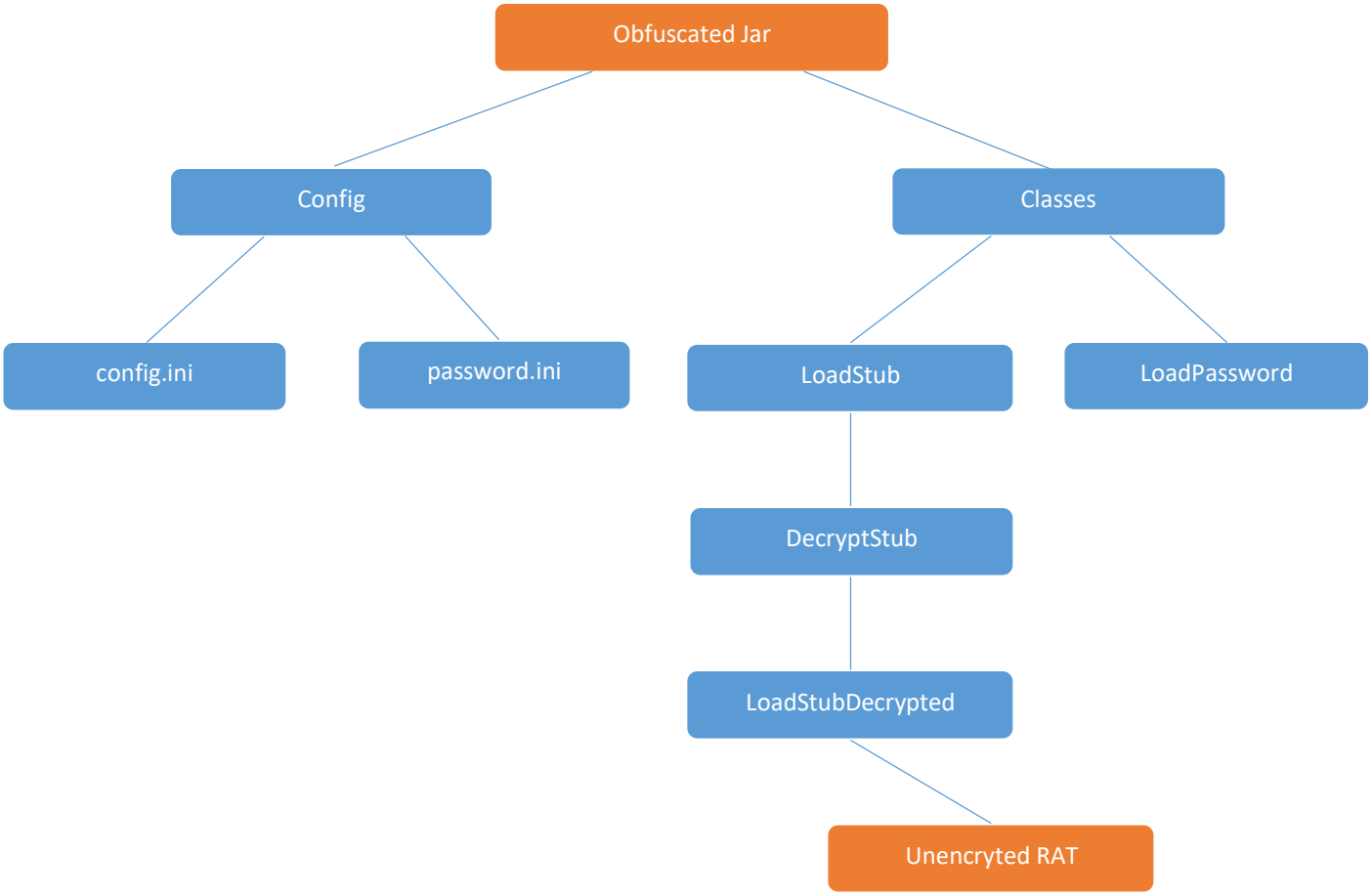
AlienSpy: Haking-as-a-Service Evolved

- Haking-as-a-Service platform
- Plans mulai dari $19.99
- Sangat berorientasi pada pelanggan, tool mudah digunakan
- Mengizinkan siapapun untuk melakukan sophisticated attacks
- Berevolusi dari waktu ke waktu dari Frutas > Adwind > Unrecom dan lainnya
- AlienSpy malware diadopsi oleh cybercrime gangs yang terorganisir

AlienSpy merupakan versi perbaikan dari RAT Frutas, Adwind dan Unrecom, yang selama beberapa tahun terakhir telah digunakan dalam berbagai kampanye penjahat cyber. Trojan menyebar melalui email phishing dengan lampiran berbahaya. RAT generasi baru ini bahkan mampu menonaktifkan beberapa antivirus.

Untuk menganalisis AlienSpy bisa menggunakan Allatori Java Obfuscator.

Conteiner dari payload (malicious jar) yang dikemas didalam package ini memiliki struktur sederhana yang berisi dua resource files (config.ini & password.ini) dan empat class files.



Setelah dieksekusi, conteiner mengikuti simple patch untuk mendekripsi dan mengeksekusi payload.

- Init LoadStub Thread
- Load config.ini contents
- Spawn DecryptStub Thread
- Pembuatan key -- Load password.ini contents dan menambahkan static_key (diatur di LoadPassword.class)
- Decrypt config.ini key menggunakan key yang sebelumnya telah dibuat
- Spawn LoadStubDecrypted
- Initialize JarInputStream object dari decoded config data
- Spawn thread dengan decoded Jar

Source: Forensic Investigations – Tools and Hacks Observed - Ondrej Krehel
(https://www.youtube.com/watch?v=68f-VAV89QQ)