

MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park"



Malware

PERTEMUAN 3

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park"



Tujuan Pembelajaran

- Mahasiswa dapat menganalisa jenis dan bahaya malicious software
- Mahasiswa dapat menganalisa potensi bahaya dari aplikasi di internet
- Mahasiswa dapat melakukan analisa serangan malware

Malicious Software / Malware

- Software yang **dirancang untuk merusak** atau mengambil akses komputer tanpa sepengetahuan pengguna
- Menjadi istilah umum untuk menyebut aplikasi jahat: Virus, worms, trojan, ransomware, spyware, botnet, dll
- Beberapa mudah dideteksi, tetapi ada yang menyamar, hingga sulit terdeteksi

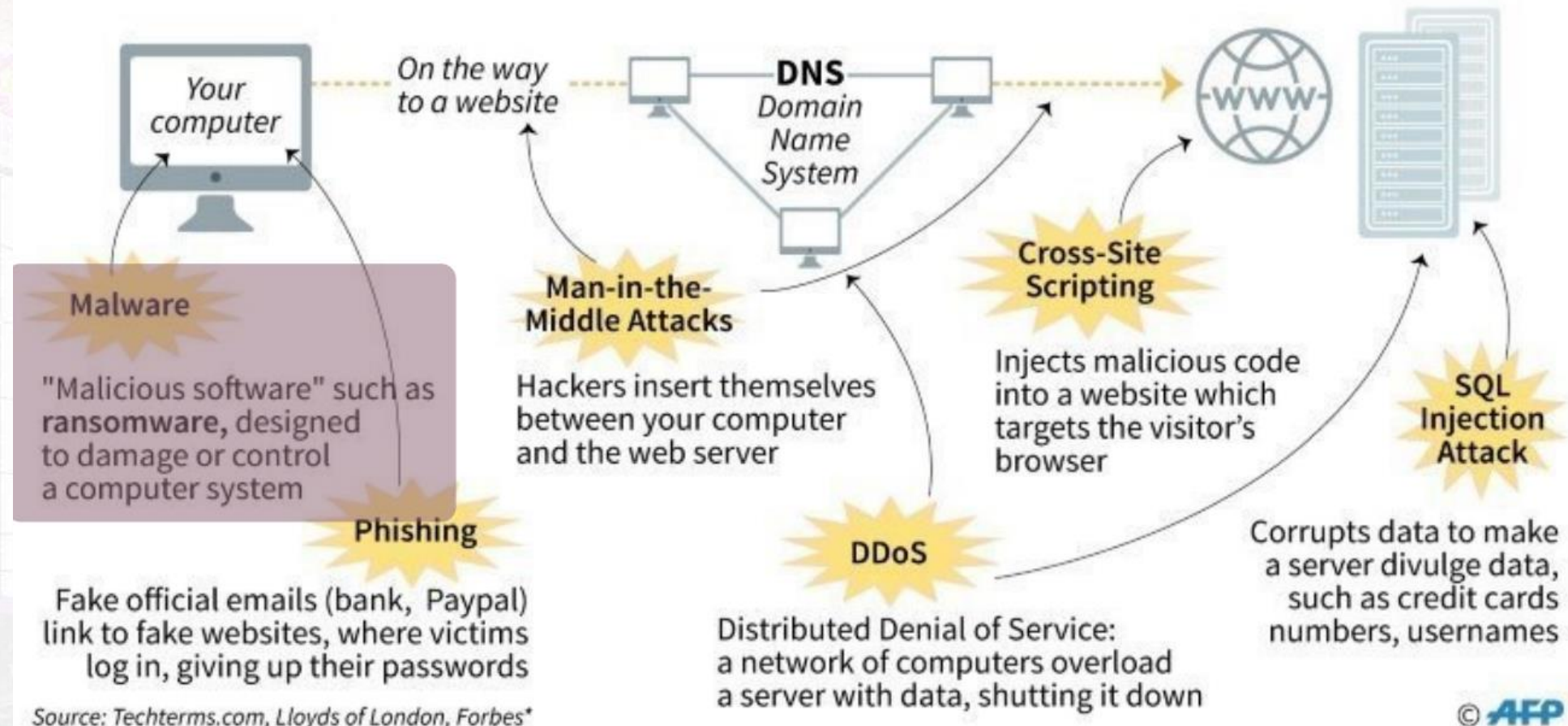
Malware (malicious software)

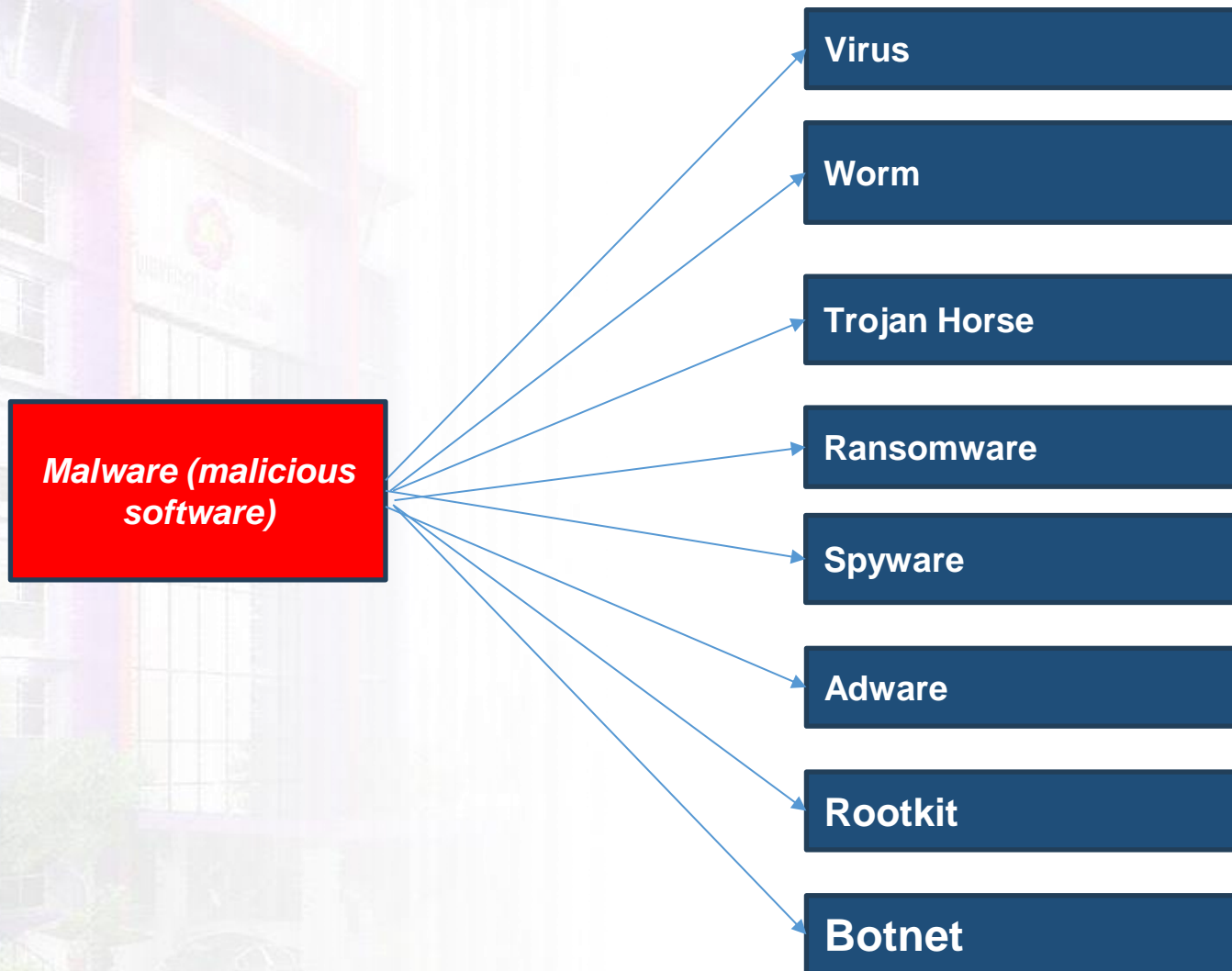
- **Malware (malicious software)** adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, mencuri, atau menyebabkan tindakan berbahaya pada sistem komputer, jaringan, atau perangkat pengguna. Malware merupakan salah satu ancaman utama dalam keamanan siber.
- **Malware** sendiri digolongkan kedalam jenis perangkat lunak berbahaya untuk keamanan dan kesehatan perangkat komputer serta jaringan. Oleh karena itu, penting untuk kita tetap berhati-hati dan semaksimal mungkin menjaga keamanan data pribadi kita ketika mengakses berbagai situs, aplikasi, dan layanan media streaming.

Cyber Attacks

The different types of cyber attacks

Cyber crime worldwide cost \$400 billion in 2015 and is forecast to reach \$2 trillion in 2019*





WORMS



VIRUS



TROJAN



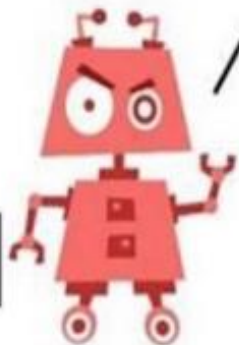
RANSOMWARE

MALWARE TYPES Explained



ADWARE

BOTS

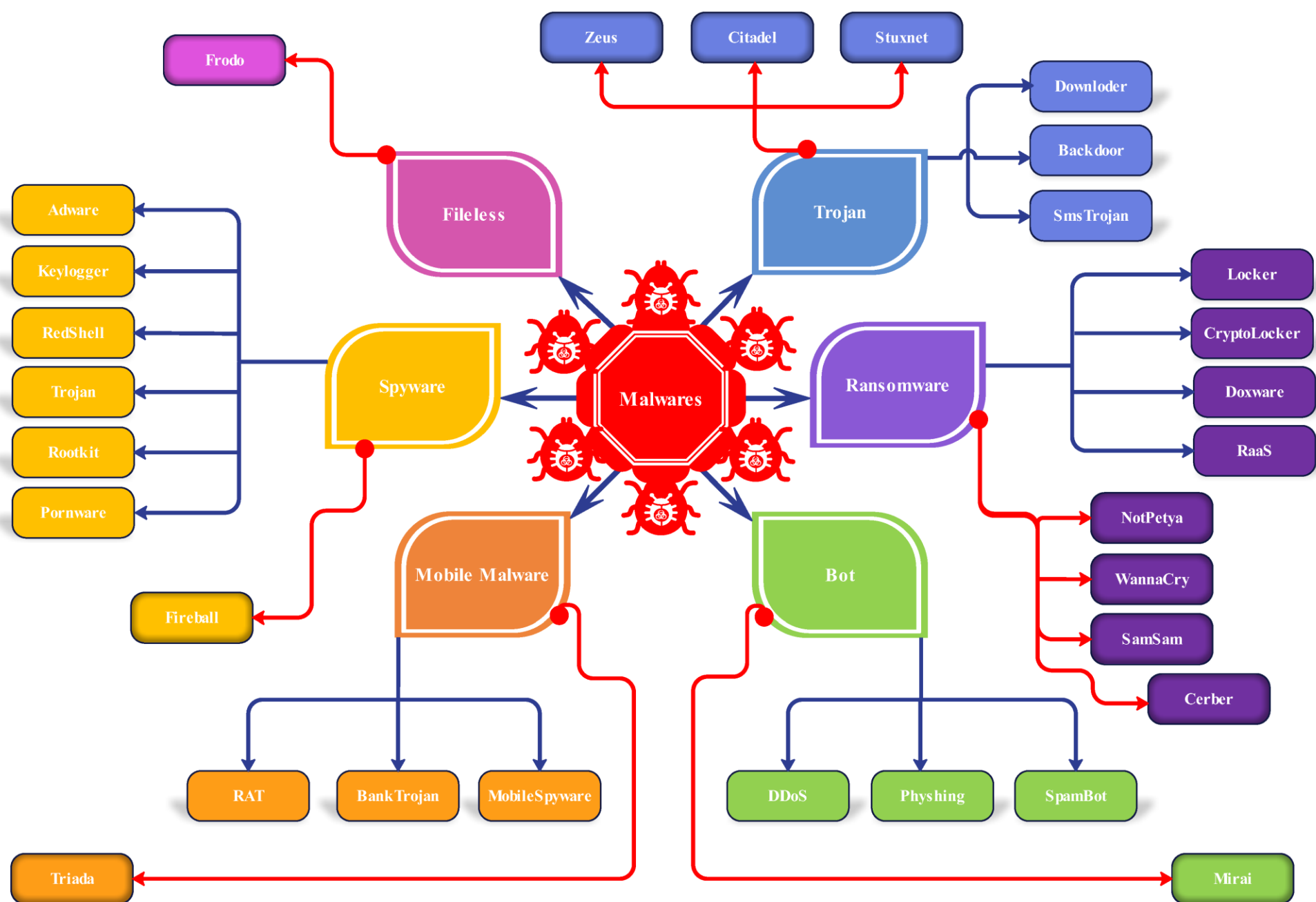


SPAM



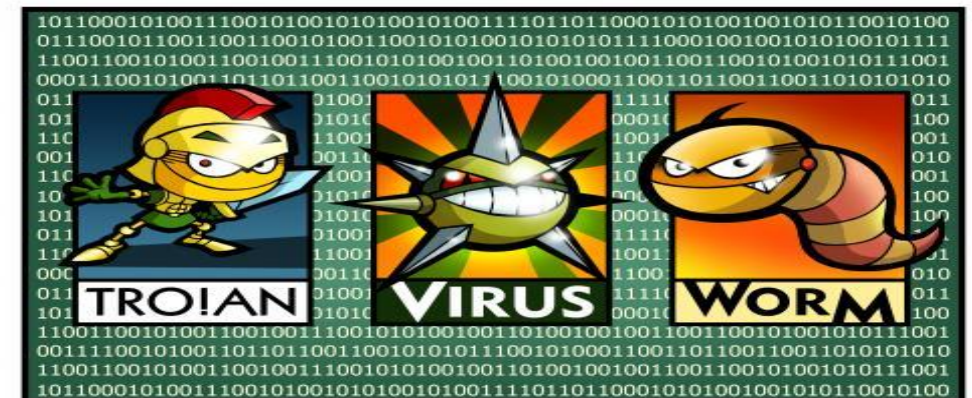
SPYWARE





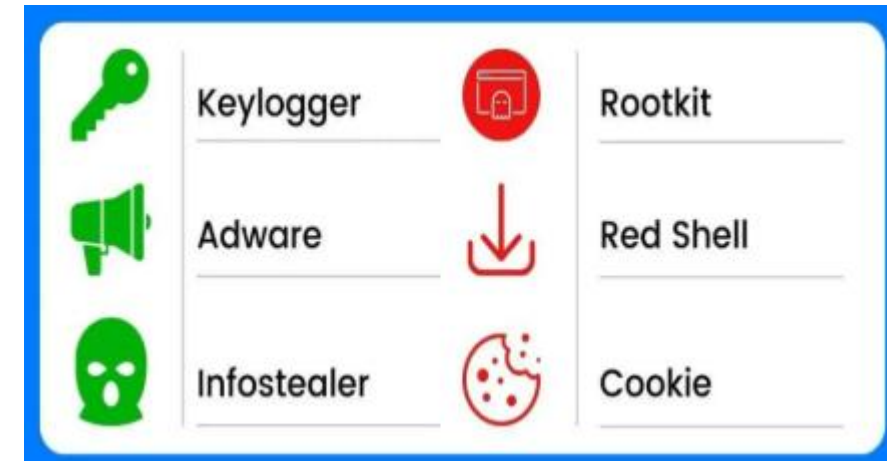
Penjelasan

- **Virus** adalah malware yang menempel pada file atau program dan menyebar ketika file atau program tersebut dijalankan.
- **Worm** adalah malware yang dapat mereplikasi diri dan menyebar melalui jaringan tanpa memerlukan bantuan pengguna.
- **Trojan Horse (Trojan)** menyamar sebagai perangkat lunak yang sah, tetapi memiliki fungsi berbahaya seperti membuka akses bagi penyerang.



Penjelasan

- **Ransomware** Ransomware mengenkripsi data korban dan meminta tebusan untuk mengembalikan aksesnya.
- **Spyware** memata-matai aktivitas pengguna dan mengumpulkan informasi tanpa sepengetahuan mereka.
- **Adware** menampilkan iklan yang tidak diinginkan, sering kali mengumpulkan data pengguna untuk menargetkan iklan lebih lanjut.

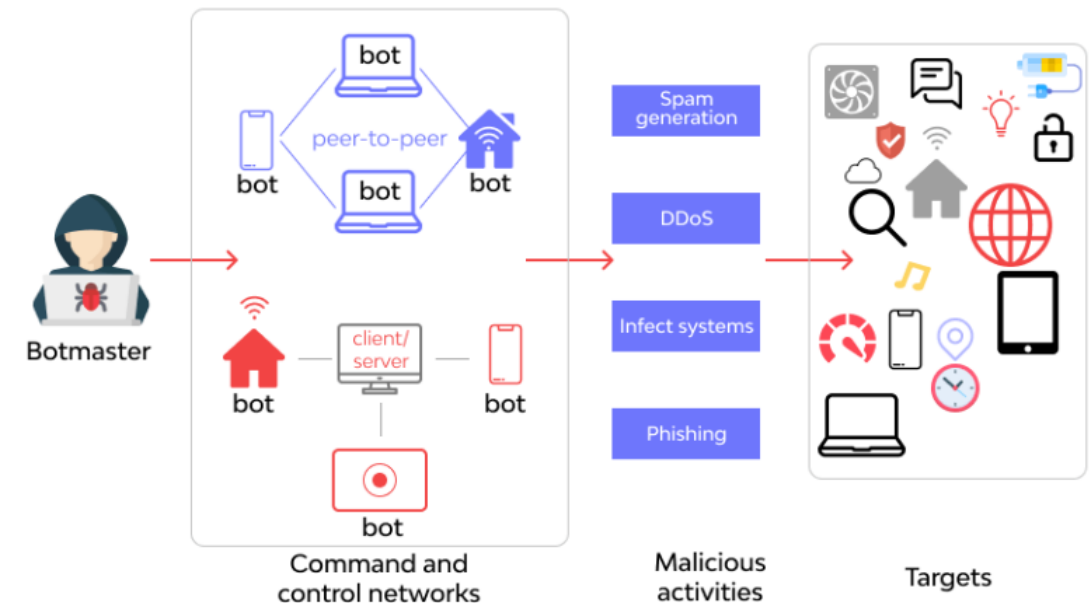


Penjelasan

- **Rootkit** dirancang untuk mendapatkan akses administratif ke sistem dan menyembunyikan keberadaannya dari deteksi sistem keamanan.
- **Botnet** adalah kumpulan perangkat yang telah terinfeksi malware dan dikendalikan oleh penyerang untuk melakukan serangan siber, seperti DDoS.



Botnet command and control architecture



Cara Penyebaran Malware

- **Lampiran Email File** berbahaya yang dikirim melalui email.
- **Download Tidak Aman** Mengunduh perangkat lunak dari sumber yang tidak terpercaya.



SARUMA SEJAHTERA
PT. Bank Pembiayaan Rakyat Syariah

WASPADA!

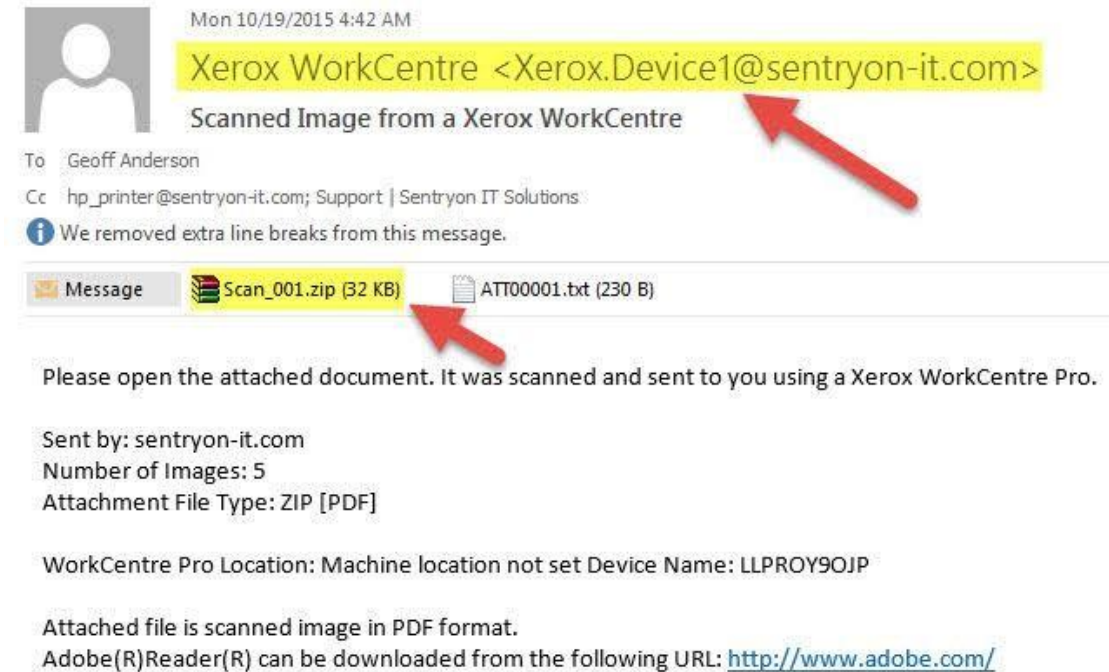
Modus Penipuan Berkedok Kiriman File Apk Melalui WA

Marak beredar di media sosial modus penipuan baru berkedok kiriman file mirip file apk undangan.

Pelaku mengirimkan file APK palsu yang sebenarnya berisi aplikasi (APK) berbahaya yang jika diunduh kemudian diinstall bisa mengambil data pribadi dan menguras rekening korban

Ingat! Jangan pernah membuka file atau link yang dikirimkan dari orang tidak dikenal.

www.sarumasejahtera.com/websar



Mon 10/19/2015 4:42 AM

Xerox WorkCentre <Xerox.Device1@sentryon-it.com>
Scanned Image from a Xerox WorkCentre

To Geoff Anderson
Cc hp_printer@sentryon-it.com; Support | Sentryon IT Solutions
We removed extra line breaks from this message.

Message Scan_001.zip (32 KB) ATT00001.txt (230 B)

Please open the attached document. It was scanned and sent to you using a Xerox WorkCentre Pro.

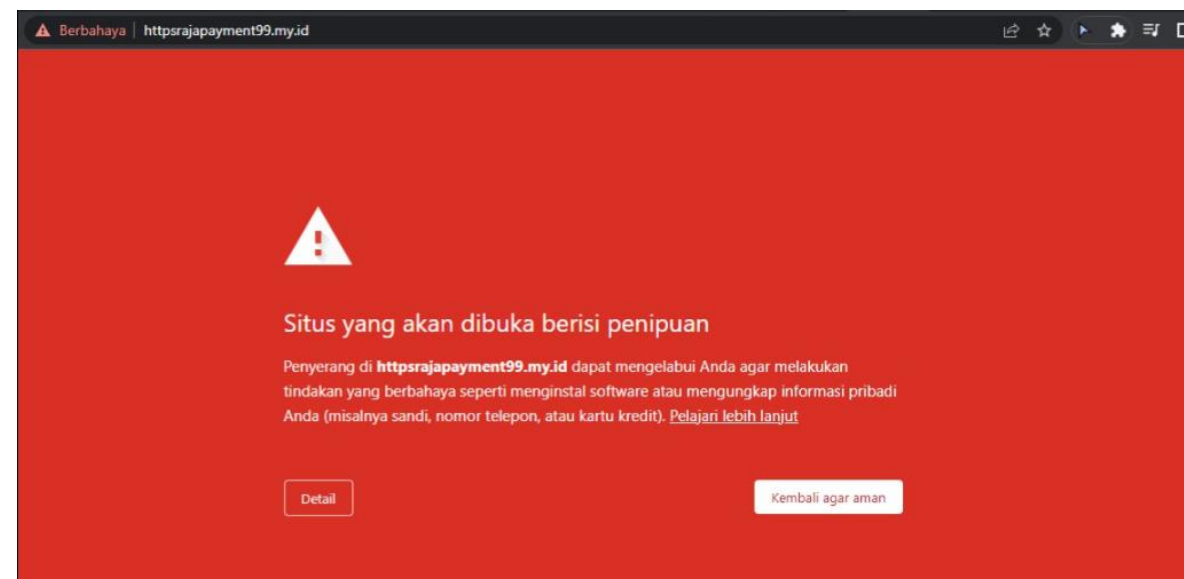
Sent by: sentryon-it.com
Number of Images: 5
Attachment File Type: ZIP [PDF]

WorkCentre Pro Location: Machine location not set Device Name: LLPROY90JP

Attached file is scanned image in PDF format.
Adobe(R)Reader(R) can be downloaded from the following URL: <http://www.adobe.com/>

Cara Penyebaran Malware

- **Exploit Kit** Memanfaatkan kerentanan dalam perangkat lunak untuk menginfeksi sistem.
- **Media yang Terinfeksi USB** atau perangkat eksternal yang mengandung malware.
- **Situs Web Berbahaya** Situs web yang mengandung skrip berbahaya yang mengeksploitasi kerentanan browser



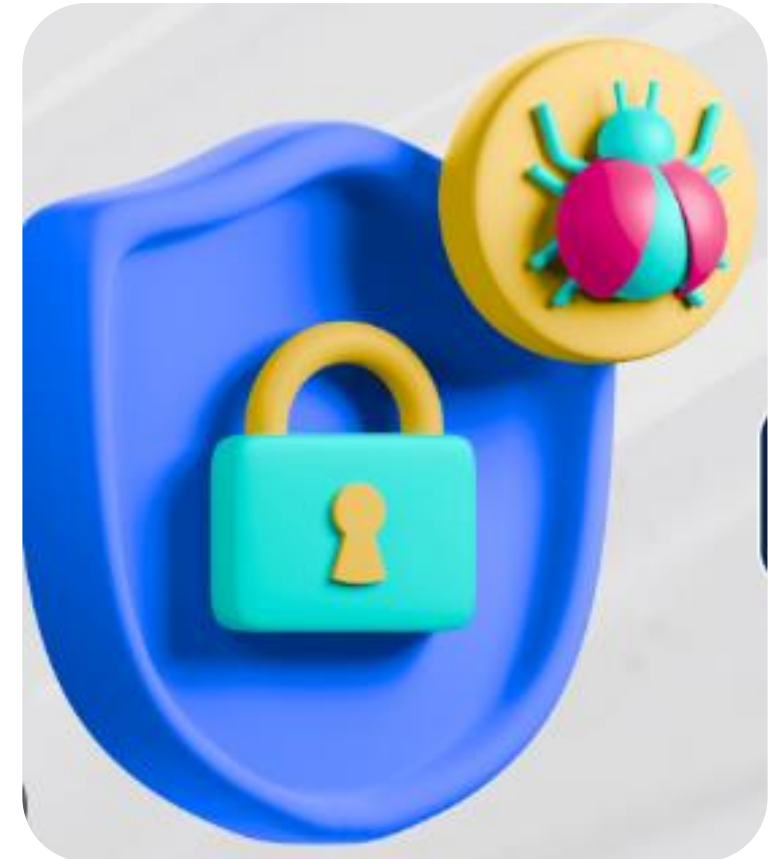
Dampak Malware

- Malware seperti ransomware dapat mengunci atau menghapus data pengguna.
- Spyware dan keylogger dapat mencuri informasi pribadi dan kredensial login.
- Malware dapat menghabiskan sumber daya sistem, membuat perangkat berjalan lebih lambat.
- Serangan malware dapat menyebabkan kerugian finansial, baik secara langsung maupun tidak langsung.
- Perusahaan atau organisasi dapat mengalami kebocoran data yang merugikan.



Teknik Deteksi

- Menggunakan perangkat lunak keamanan untuk mendeteksi dan menghapus malware. **Antivirus dan Antimalware**
- Mengamati aktivitas mencurigakan yang dapat menunjukkan keberadaan malware. **Analisis Perilaku**
- Menjalankan program dalam lingkungan terisolasi untuk mengidentifikasi aktivitas berbahaya. **Sandboxing**
- Menggunakan data intelijen ancaman untuk mengenali pola serangan. **Threat Intelligence**



Pencegahan Malware

- Selalu memperbarui sistem operasi dan perangkat lunak untuk menutup celah keamanan.
- Menggunakan filter web dan firewall untuk mencegah akses ke situs berbahaya.
- Tidak membuka lampiran atau mengklik tautan dari email yang mencurigakan.
- Memasang dan memperbarui antivirus serta firewall.
- Melatih pengguna untuk mengenali ancaman keamanan dan menerapkan praktik terbaik keamanan.



**ANTISIPASI
SERANGAN
MALWARE
RANSOMWARE
WANNACRYPT**

JANGAN PANIK DAN IKUTI TIPS SEDERHANA INI

1. Sebelum hidupkan komputer/server, terlebih dahulu matikan Hotspot/Wifi dan cabut koneksi kabel LAN/Internet.
2. Setelahnya, segera pindahkan data ke sistem operasi non windows (linux, mac) dan/atau lakukan BACK UP/COPY Semua Data ke MEDIA STORAGE TERPISAH.

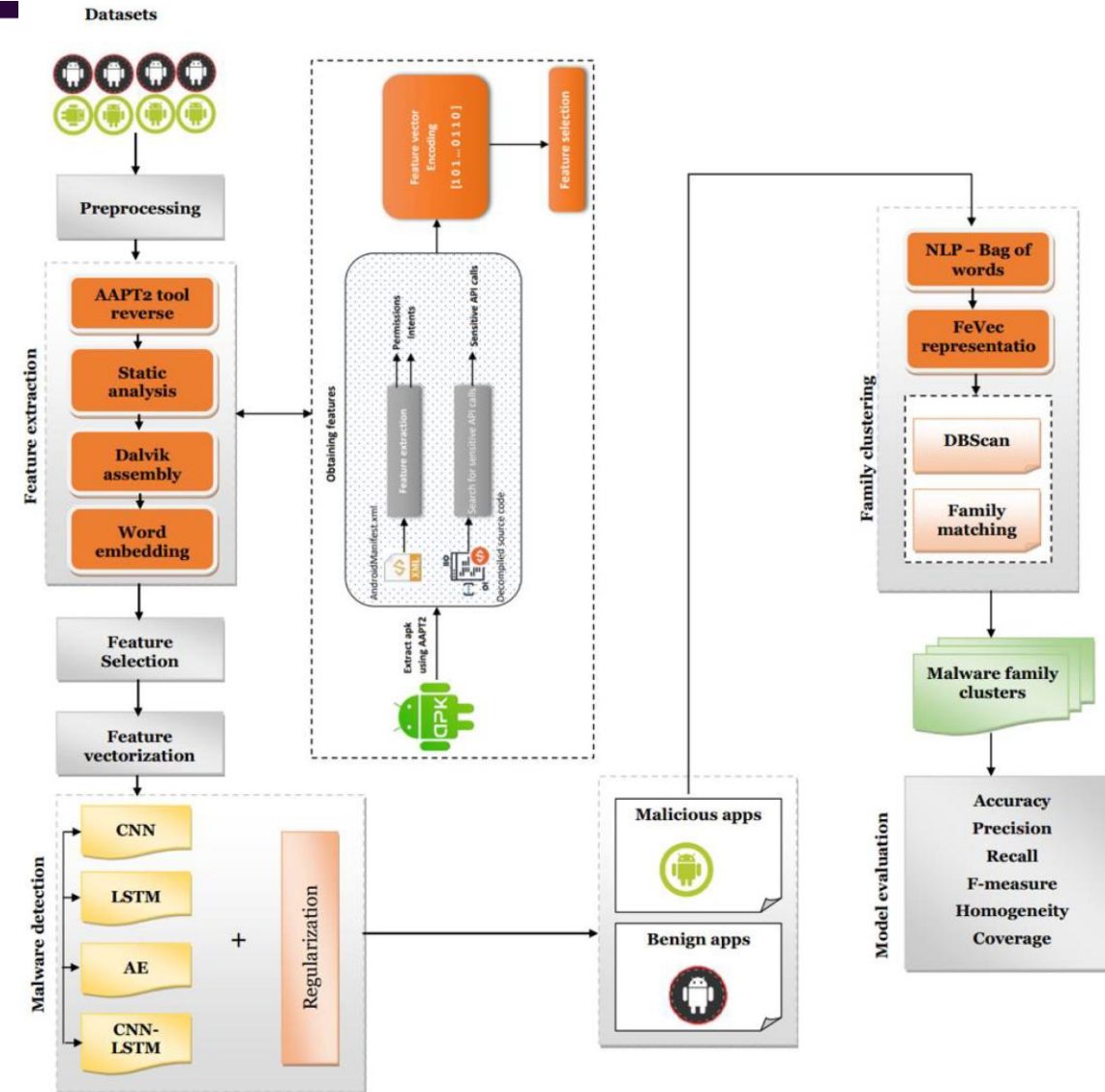
**KEMUDIAN DARI PENGELOLA TEKNOLOGI INFORMASI
DAPAT MELAKUKAN TINDAK LANJUT TEKNIS LAINNYA :**

1. Lakukan Update security pada windows anda dengan install Patch MS17-010 yang dikeluarkan oleh microsoct. Lihat : <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>. Updating sebaiknya dilakukan dengan cara mengambil file patch secara download menggunakan komputer biasa, bukan komputer yang berperan penting.
2. Lakukan update AntiVirus. Contoh AV: Kaspersky Total Security, Eset, Panda, Symantec yang bisa download versi trial untuk 30 hari gratis dengan fungsi atau fitur penuh dan update. Pastikan AV meliputi ANTI RANSOMWARE.
3. Non aktifkan fungsi SMB (Server Message Block) dan jangan mengaktifkan fungsi macros.
4. Block Ports : 139/445 & 3389

⚠ Untuk menjadi kehati-hatian :
Penularan dapat melalui penyebaran file attachment email dan link ke situs Malware - bukan hanya lewat penyebaran melalui jaringan.

Tren dan Tantangan Masa Depan dalam Keamanan Malware

- Malware Berbasis AI Malware semakin canggih dengan pemanfaatan kecerdasan buatan.
- Serangan terhadap IoT Perangkat IoT menjadi target utama karena sering kali memiliki keamanan yang lemah.
- Serangan Zero-Day Eksploitasi celah keamanan yang belum ditemukan sebelumnya.
- Peningkatan Phishing dan Social Engineering Teknik manipulasi psikologis untuk menyebarkan malware semakin berkembang.



Mencegah dan Mengatasi Ancaman Malware

- Gunakan *Software Antivirus/Antimalware*
- Hindari Klik Link Sembarangan
- Berhati-hati saat *Menginstal Software*
- Pastikan Sistem *Operasi Up-to-Date*
- Lakukan Backup Secara Rutin
- Gunakan *Password* yang Kuat
- Nonaktifkan *Pop-Up* dan *Instal Anti-Malware* yang Berkualitas



Malware Analysis

- What is Malware Analysis ?

Proses **menganalisis** sampel malware dan mengekstrak sebanyak mungkin informasi di dalamnya

Tujuan:

- Memahami **jenis dan fungsi-fungsi** yang dimiliki malware
- Memahami cara malware menyerang, apakah ada target tertentu atau tidak
- Memahami bagaimana malware berkomunikasi dengan penyerang
- Menandai malware (**signature**) sehingga dapat digunakan untuk mendeteksi malware sejenis di kemudian hari

Jenis



HARDER

PRACTICAL

Static Analysis

Mengamati source code malware lgsg, tanpa dieksekusi

- Reverse engineering: **pattern, flow, library, signature** .

Dynamic Analysis

Jalankan malware di sandbox/isolated lab dan amati perilaku sistem setelah malware dijalankan

- **Behaviour analysis**
- **Properties analysis**
- **Fully-automated analysis**

Safety Guideline

- Don't use main computer
- Isolate your network
- Disable network sharing
- Don't plug any USB
- Take snapshots

Demo

- Isolated lab Physical machines:

Deep Freeze, FOG/Freeghost Virtual machines: VirtualBox, VMWare, Xen, KVM •

- OS Windows 7 VM (64bit-prefered)

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

- FLARE VM – Distribusi windows untuk malware analysis

<https://github.com/fireeye/flare-vm>

- Cuckoo Sandbox

<https://cuckoosandbox.org>

Sample Malware

- <https://contagiodump.blogspot.com/>
- <https://virusshare.com/>
- <https://domcomp.com/tld-list>
- <https://malware.lu/>
- www.malshare.com

Cloud Sandbox

- <https://app.any.run/>
- <https://www.joesandbox.com/#windows>
- <https://valkyrie.comodo.com/>
- <https://intezer.com/>
- <https://www.secondwrite.com/>
- <https://www.hybrid-analysis.com/>

Kesimpulan

- Malware merupakan ancaman utama dalam keamanan siber yang terus berkembang dengan berbagai teknik serangan baru. Untuk mengurangi risiko serangan, organisasi dan individu harus menerapkan strategi keamanan yang kuat, termasuk deteksi dini, pencegahan, dan respons cepat terhadap ancaman siber.

Referensi

- Schneier, B. (2018). "Click Here to Kill Everybody: Security and Survival in a Hyper-connected World".
- Symantec Threat Report 2023.
- NIST Cybersecurity Framework.
- OWASP Malware Threats Database.



UNIVERSITAS
AMIKOM
YOGYAKARTA

