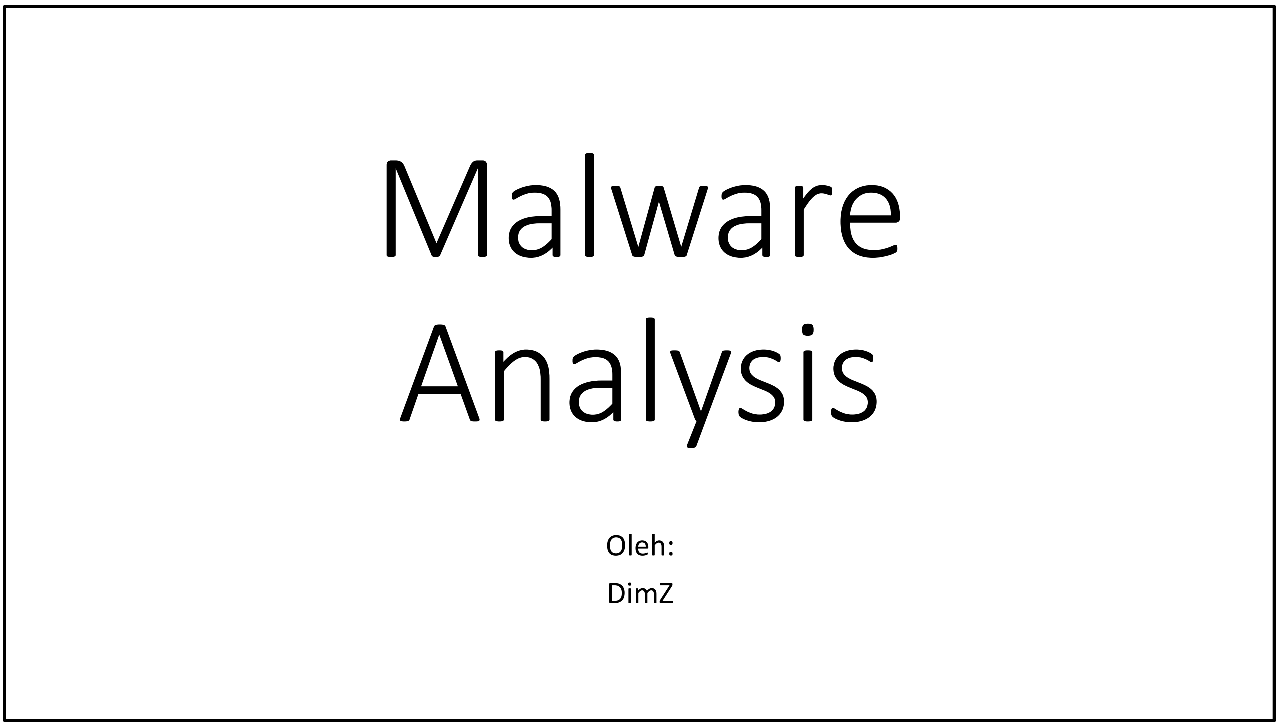
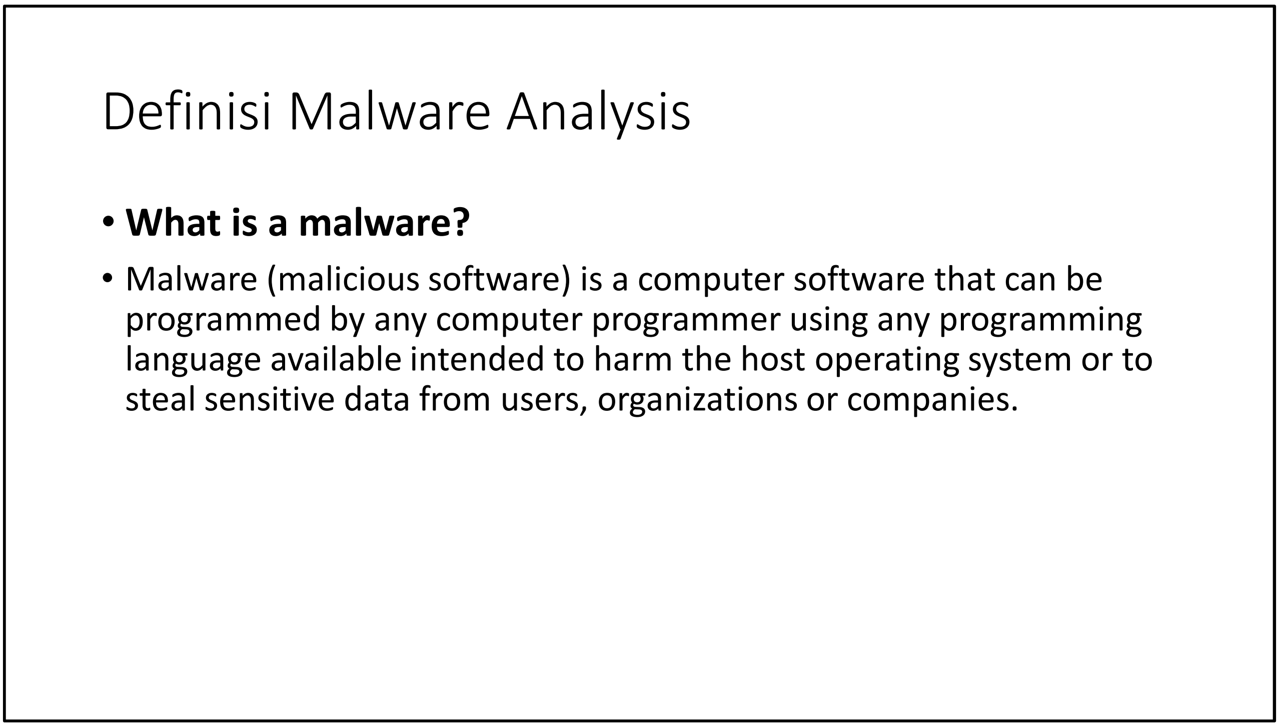


Malware Analysis

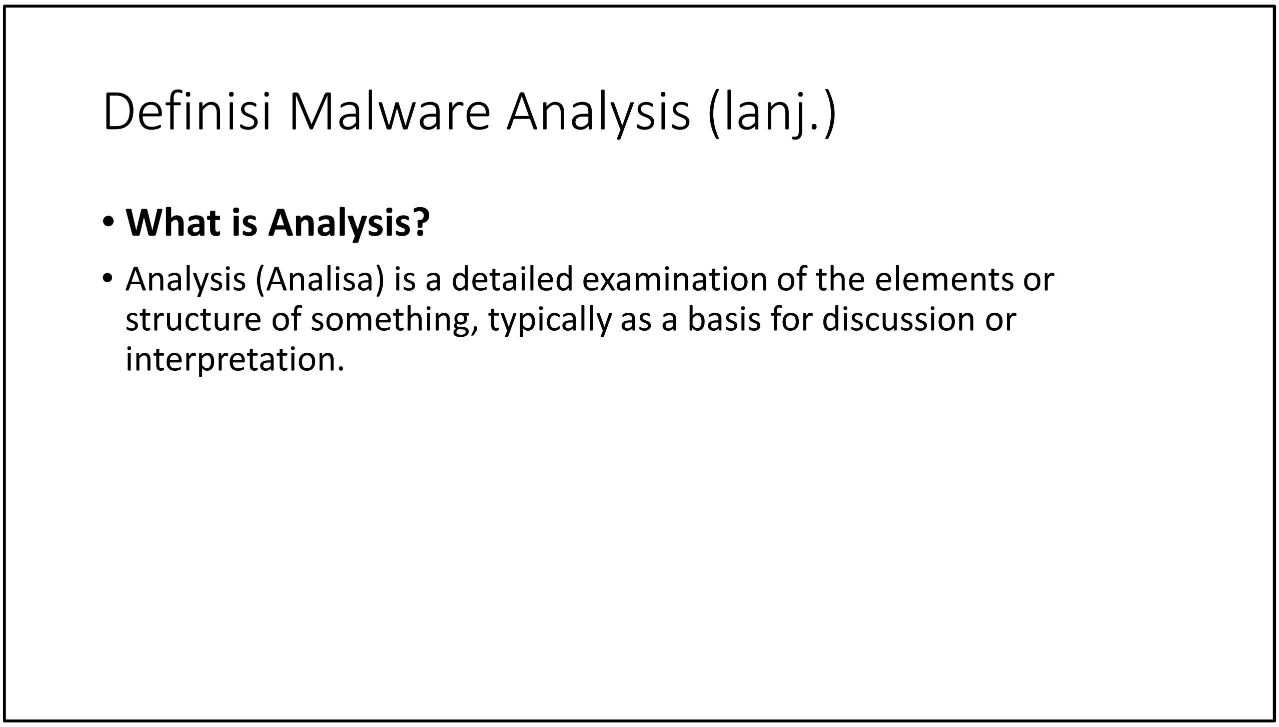
Oleh:

DimZ



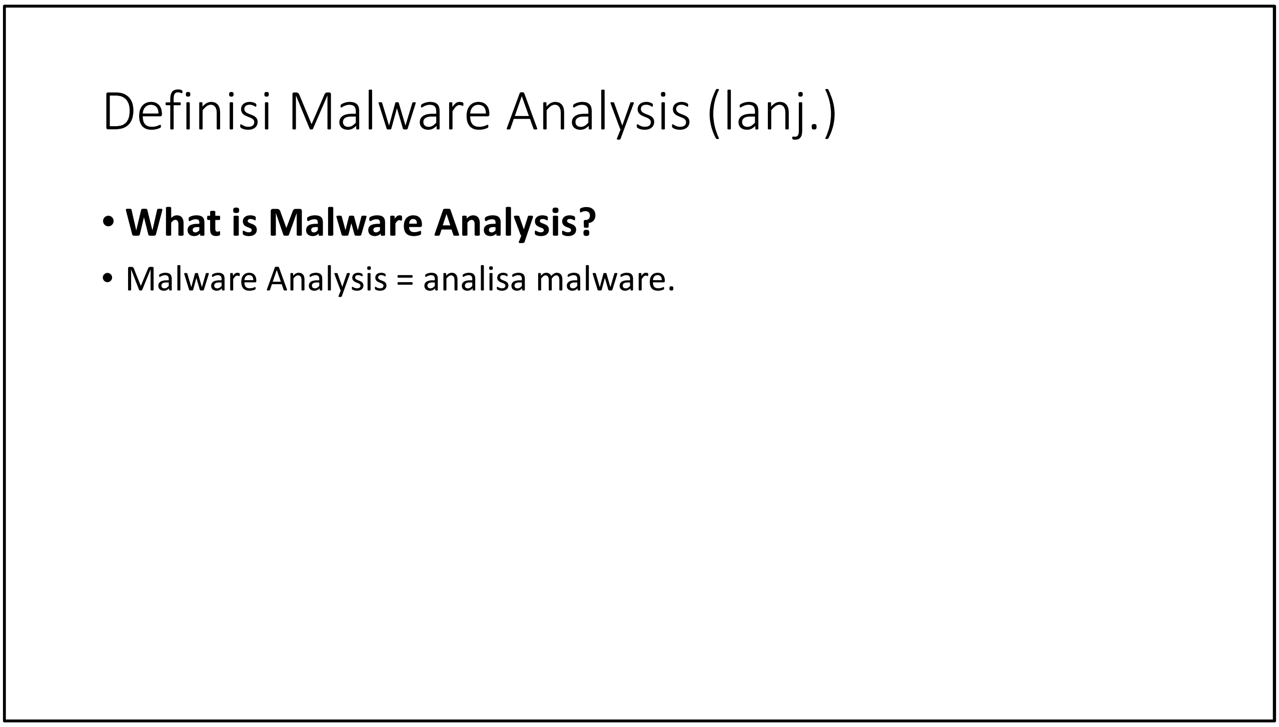
Definisi Malware Analysis

- **What is a malware?**
- Malware (malicious software) is a computer software that can be programmed by any computer programmer using any programming language available intended to harm the host operating system or to steal sensitive data from users, organizations or companies.



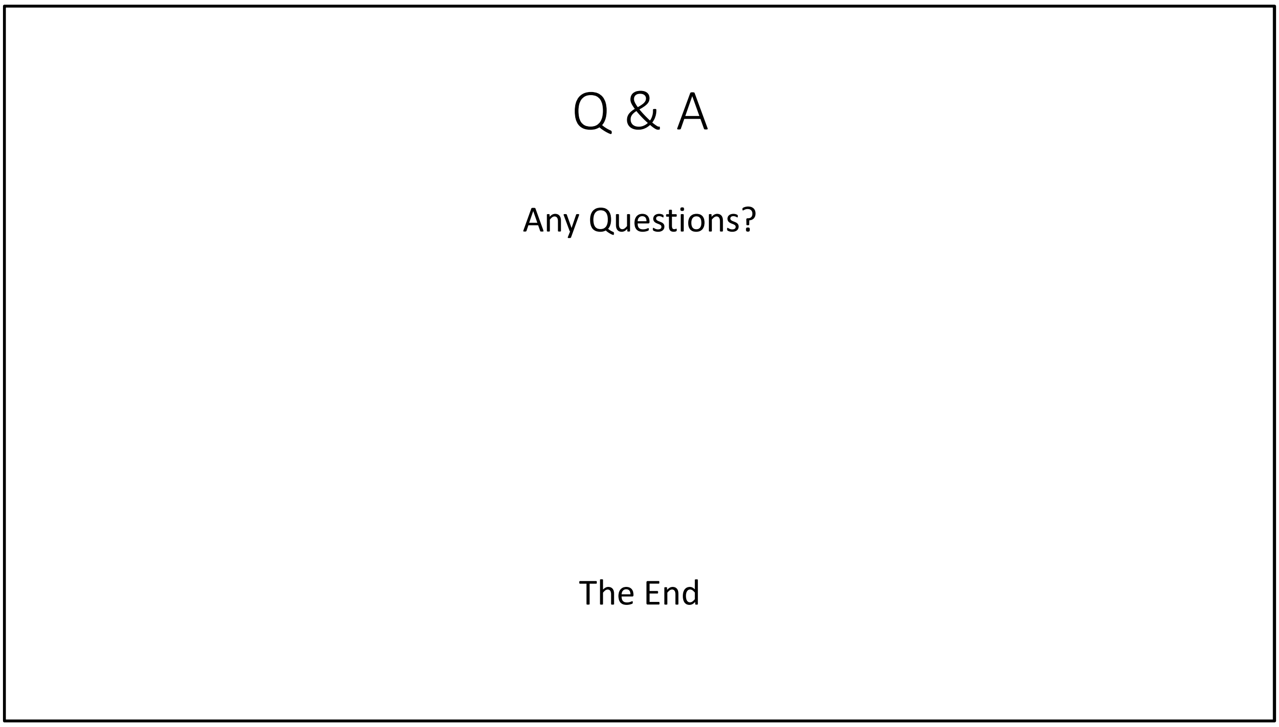
Definisi Malware Analysis (lanj.)

- **What is Analysis?**
- Analysis (Analisa) is a detailed examination of the elements or structure of something, typically as a basis for discussion or interpretation.



Definisi Malware Analysis (lanj.)

- **What is Malware Analysis?**
- Malware Analysis = analisa malware.



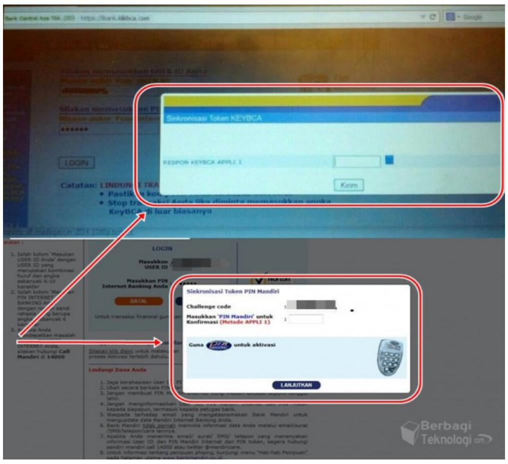
Q & A

Any Questions?

The End

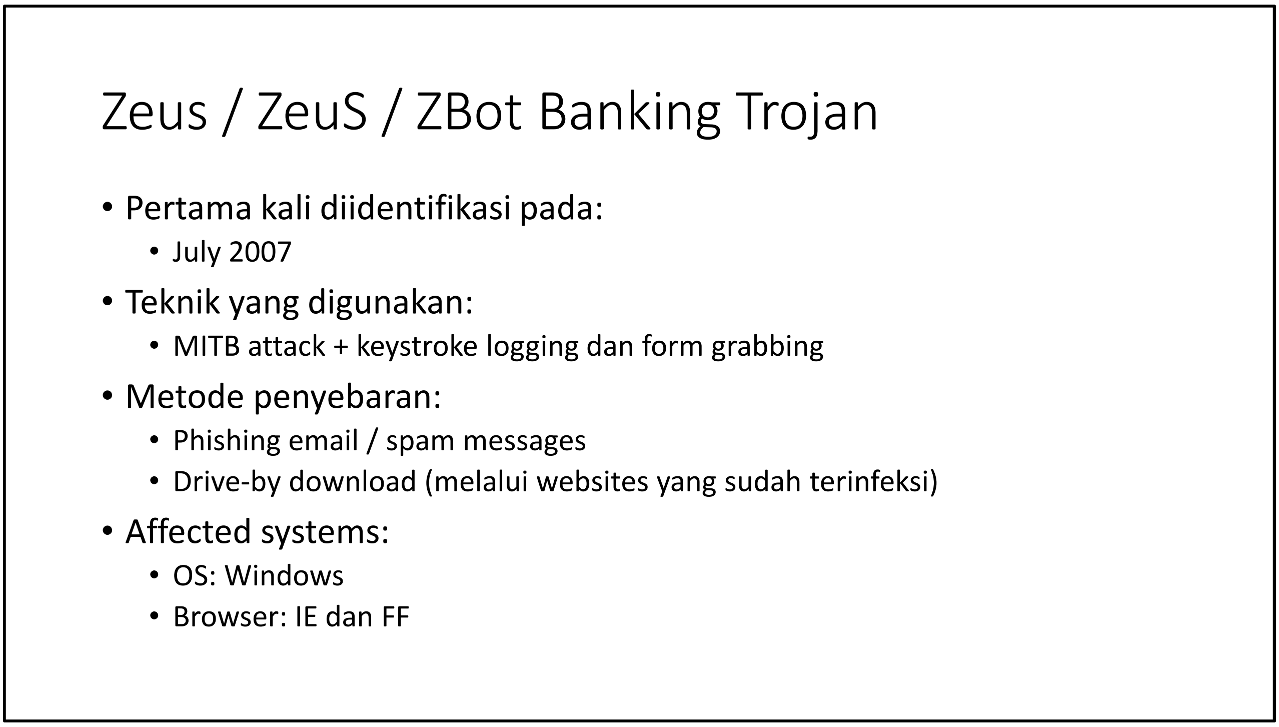
Malware Sinkronisasi Token

- Pelaku: Zeus Banking Trojan
- Screenshot:



Definisi dari Banking Trojan

- Banking Trojan is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.
- Contoh Banking Trojan:
    - Carberp
    - Citadel
    - SpyEye
    - Zeus



Zeus / ZeuS / ZBot Banking Trojan

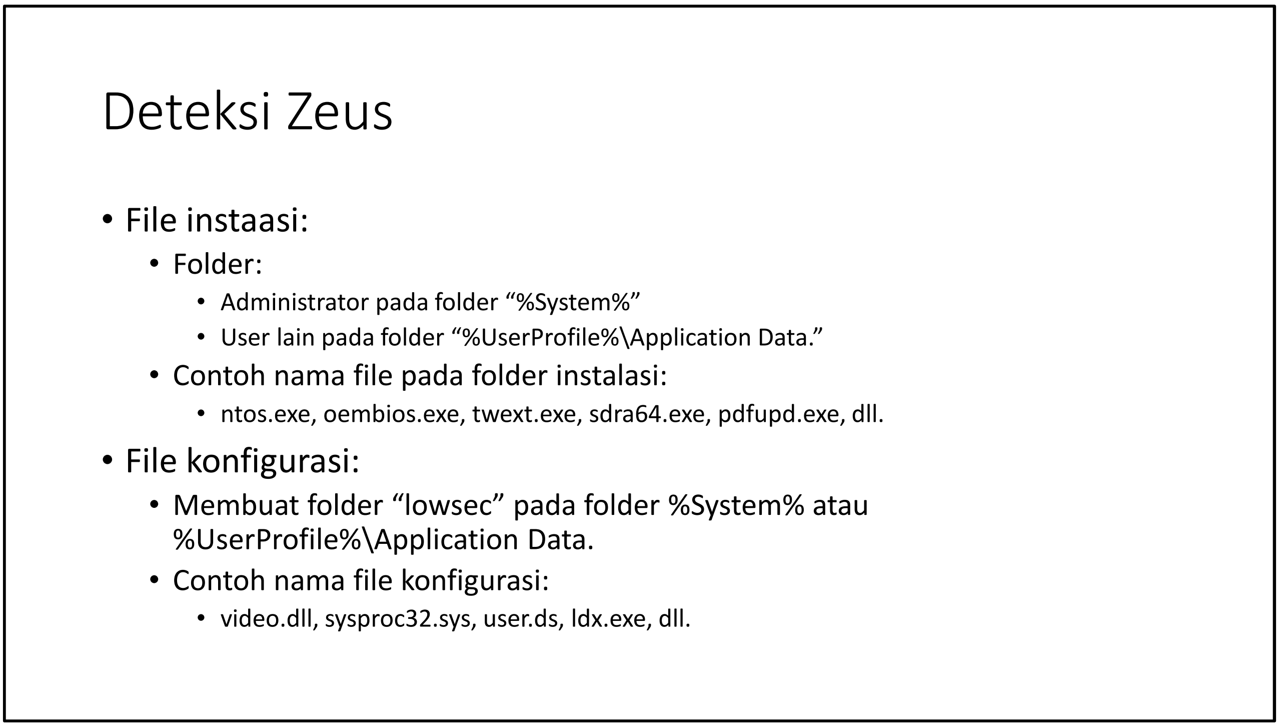
- Pertama kali diidentifikasi pada:
  - July 2007
- Teknik yang digunakan:
  - MITB attack + keystroke logging dan form grabbing
- Metode penyebaran:
  - Phishing email / spam messages
  - Drive-by download (melalui websites yang sudah terinfeksi)
- Affected systems:
  - OS: Windows
  - Browser: IE dan FF

MITB Attack

- What is MITB Attack?
  - Man in the Black ???

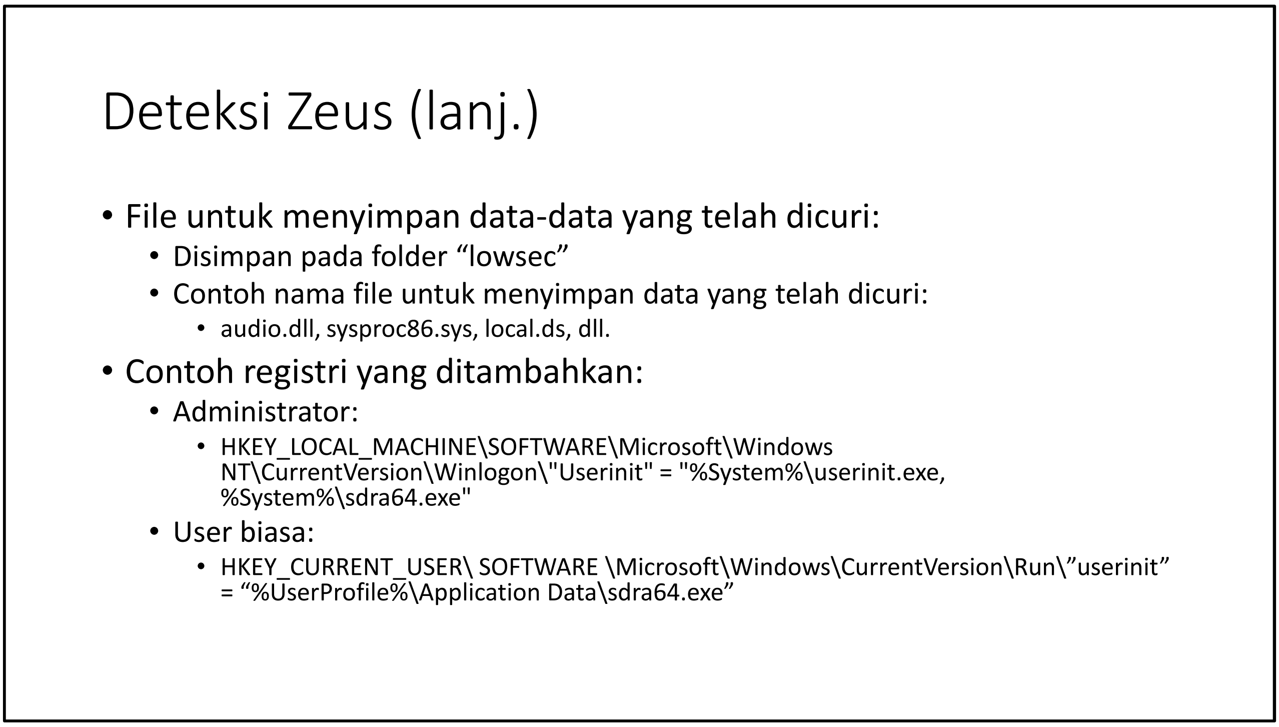
MITB Attack (lanj.)

- MITB (Man-in-the-browser) Attack is a proxy Trojan horse that infects a web browser by taking advantage of vulnerabilities in browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host web application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or two or three-factor Authentication solutions are in place.
- The majority of financial service professionals in a survey considered MitB to be the greatest threat to online banking.



Deteksi Zeus

- File instaasi:
  - Folder:
    - Administrator pada folder “%System%”
    - User lain pada folder “%UserProfile%\Application Data.”
  - Contoh nama file pada folder instalasi:
    - ntos.exe, oembios.exe, twext.exe, sdra64.exe, pdfupd.exe, dll.
- File konfigurasi:
  - Membuat folder “lowsec” pada folder %System% atau %UserProfile%\Application Data.
  - Contoh nama file konfigurasi:
    - video.dll, sysproc32.sys, user.ds, ldx.exe, dll.



Deteksi Zeus (lanj.)

- File untuk menyimpan data-data yang telah dicuri:
  - Disimpan pada folder “lowsec”
  - Contoh nama file untuk menyimpan data yang telah dicuri:
    - audio.dll, sysproc86.sys, local.ds, dll.
- Contoh registri yang ditambahkan:
  - Administrator:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Userinit" = "%System%\userinit.exe, %System%\sdra64.exe"
  - User biasa:
    - HKEY_CURRENT_USER\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\”userinit” = “%UserProfile%\Application Data\sdra64.exe”

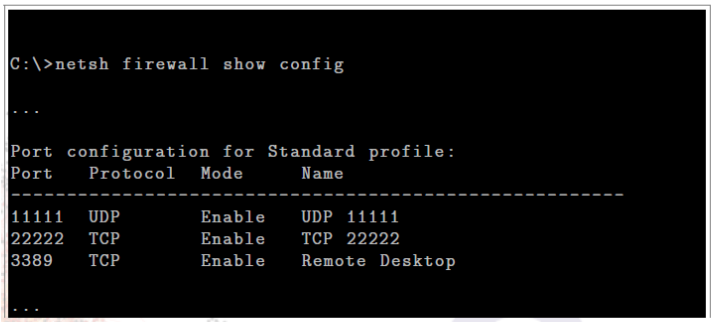
Deteksi Zeus (lanj.)

- Contoh penambahan service:
  - Administrator
    - winlogon.exe
  - User lain:
    - explorer.exe
  - Dan svchost.exe

- Source: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=2

Deteksi Zeus (lanj.)

1. Tutup semua browser, ketik di cmd: netstat
2. Lakukan whois ke IP-IP yang muncul
3. Buka situs IT Security, seperti: www.Symantec.com
4. Netsh:

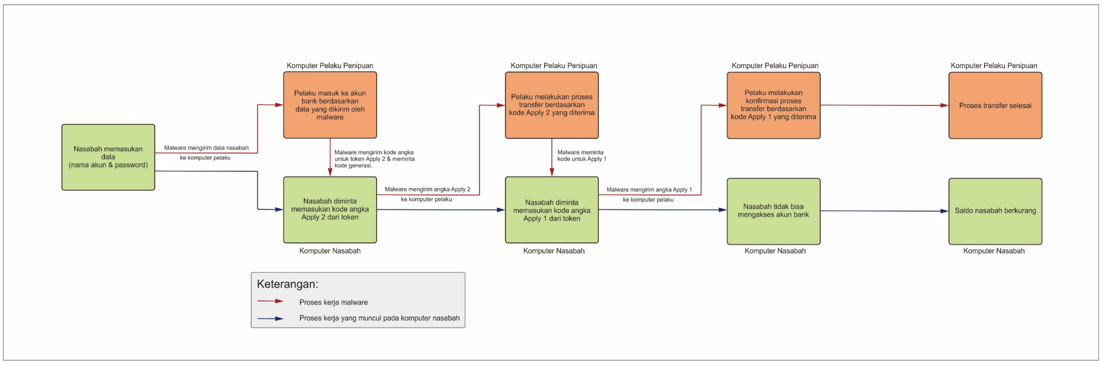


```
C:\>netsh firewall show config

...

Port configuration for Standard profile:
Port   Protocol  Mode     Name
-------------------------------------------------------
11111  UDP       Enable   UDP 11111
22222  TCP       Enable   TCP 22222
3389   TCP       Enable   Remote Desktop

...
```

Code Snippet

- Pemblokiran terhadap situs-situs keamanan seperti: www.Symantec.com
- Daftar situs bank-bank asing
- Daftar situs bank local:
  - BCA
  - Mandiri
  - BNI

Cara Kerja Zeus Pada Sinkronisasi Token



Nasabah memasukan data (nama akun & password)

Malware mengirim data nasabah ke komputer pelaku

Komputer Pelaku Penipuan

Pelaku masuk ke akun bank berdasarkan data yang dikirim oleh malware

Malware mengirim kode angka untuk token Apply 2 & meminta kode generasi.

Nasabah diminta memasukan kode angka Apply 2 dari token

Komputer Nasabah

Malware mengirim angka Apply 2 ke komputer pelaku

Komputer Pelaku Penipuan

Pelaku melakukan proses transfer berdasarkan kode Apply 2 yang diterima

Malware meminta kode untuk Apply 1

Nasabah diminta memasukan kode angka Apply 1 dari token

Komputer Nasabah

Malware mengirim angka Apply 1 ke komputer pelaku

Komputer Pelaku Penipuan

Pelaku melakukan konfirmasi proses transfer berdasarkan kode Apply 1 yang diterima

Nasabah tidak bisa mengakses akun bank

Komputer Nasabah

Komputer Pelaku Penipuan

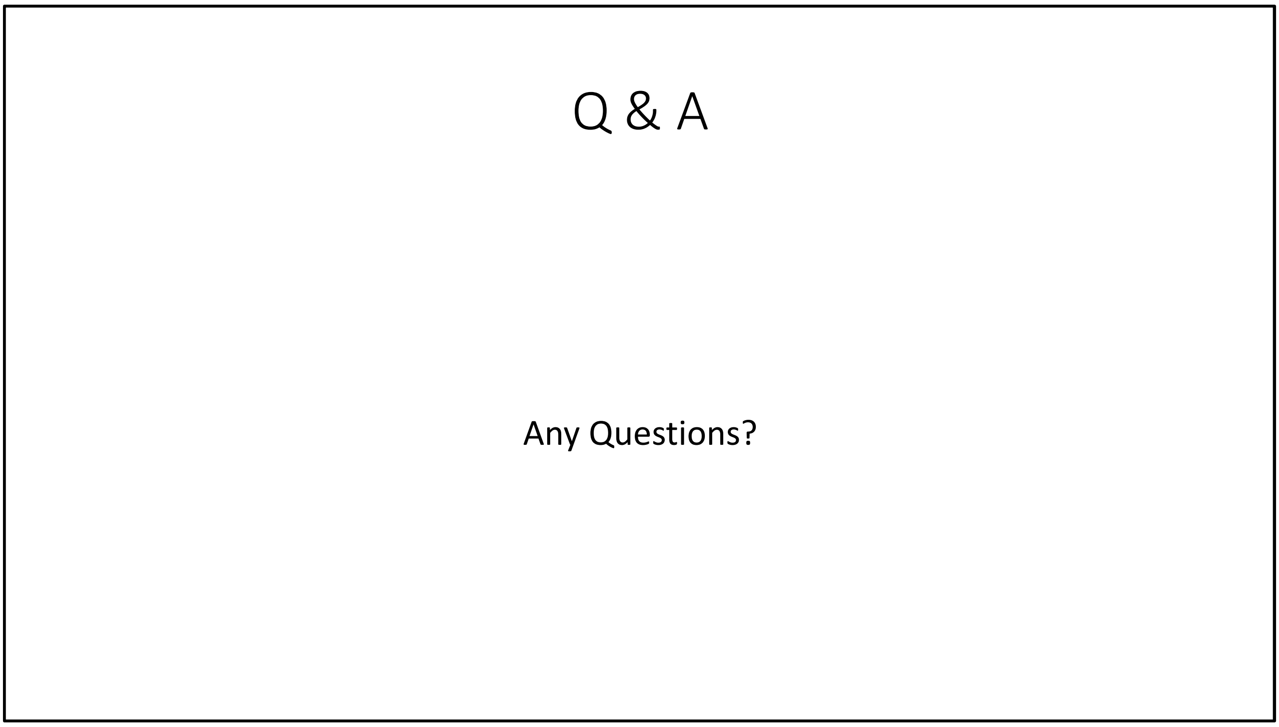
Proses transfer selesai

Saldo nasabah berkurang

Komputer Nasabah

Keterangan:

- Proses kerja malware
- Proses kerja yang muncul pada komputer nasabah



Q & A

Any Questions?

THE END

- Tirimikisi -