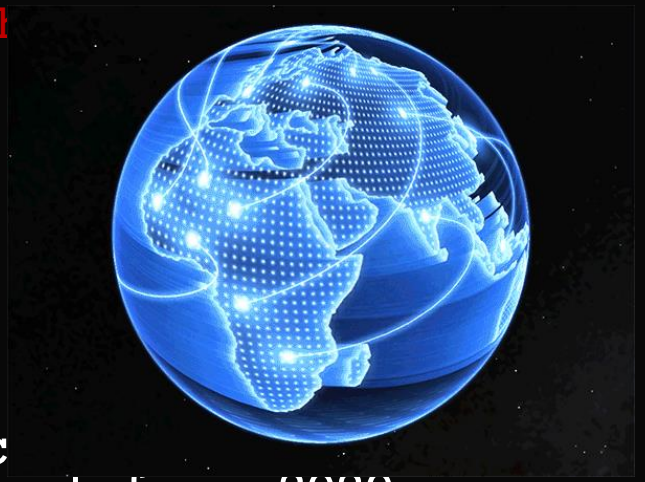
OVERVIEW OF THREATS AND THEIR DETECTION

Dr. Ashu Sharma

INTERNET

- The development of computer security has a military origin, and since 1950 it is a major concern.
- US government was a major force behind security research and technology.
- Internet came in the late 1960s with the creation of ARPANET
- first message was sent over the ARPANET in 1969
- The smart devices/phone technology continued to advance throug



- In 2007 Android based smart device was unveiled by Google.
- Today Android is the most dominant OS in the smart devices.
- An estimate shows that more than 15 billion smart devic
  wise and are expected to be reaching 200 billion by the end of year 2020.

- **According to official data released this month, more than 700 websites of government departments have reportedly been hacked in the past four years.**

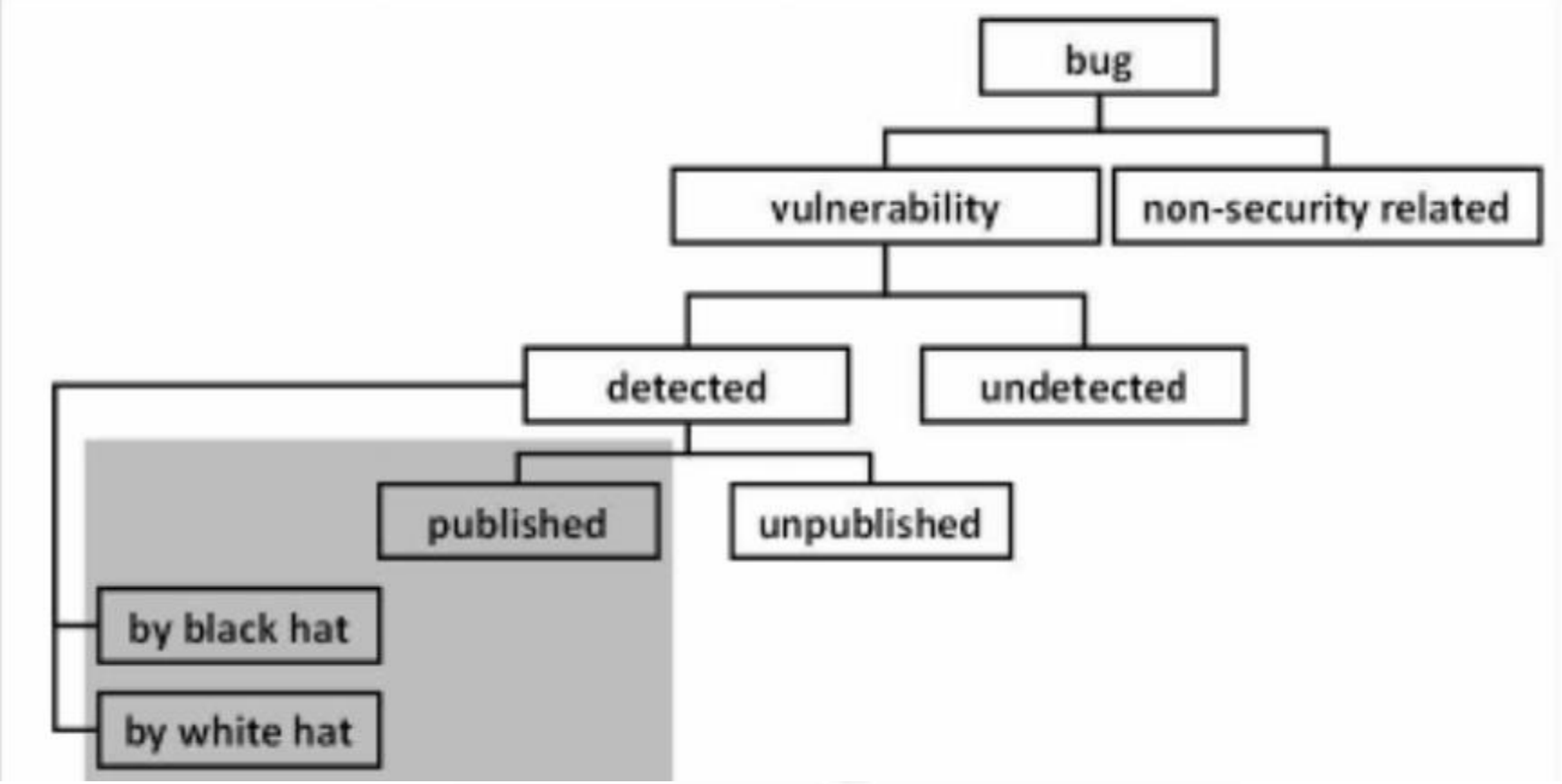
HOME MINISTRY WEBSITE BLOCKED AFTER ATTEMPTED HACK: REPORT 12 FEB 2017

IRCTC website hacked, information of around 1 crore people feared stolen

Maze Ransomware attack to hit Cognizant revenue

San Francisco: Google on Friday said it saw 18 million daily malware and phishing emails related to COVID-19 last week, revealing how the bad actors are working overtime to target people working from home and facing other restrictions due the pandemic.

INTRODUCTION TO MALWARE: BASIC TERMS



- Malicious software which enters the computer system without users authorization and takes undesirable actions.

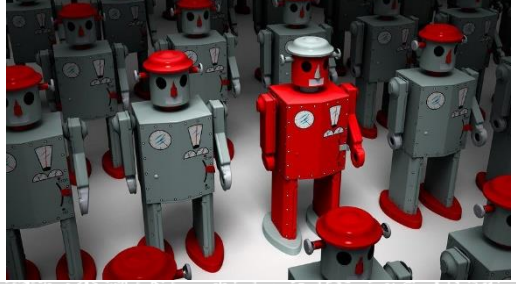
Malware Structure

Three Parts

– Attack Vector: The means by which a malware spreads, enabling it to replicate, also referred as Infection Vector.

– Trigger: The event or condition that determines when the payload is activated or delivered.

– Malicious Activities: The payload may involve damage or may involve benign but NOTICEABLE activity.



VIRUSES, BACKDOOR, WORMS,

Bots, Trojan Horses

Malware Structure

Three Parts

– Attack Vector: The means by which a malware spreads, enabling it to replicate, also referred as Infection Vector.

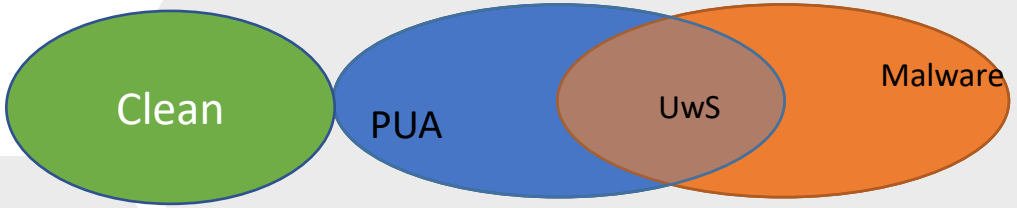
– Trigger (optional): The event or condition that determines when the payload is activated or delivered.

– Malicious Activities: The payload may involve damage or may involve benign but NOTICEABLE activity.

1ST GENERATION MALWARE (CLASSIFICATION OF MALWARE)

Definitions

- PUA (Potentially Unwanted Application) - Programs that are not wanted in an Enterprise environment and their behaviours can lead to a loss of productivity. These are defined by behaviour and/or reputation.
- UwS (Unwanted Software) - Programs that exhibit behaviours that lead to a loss of control by the user.
- Greyware - The combination of PUA and UwS and both erode a delightful Windows experience.



Unwanted Software Worksheet

Adware: A program that runs on a user's computer and displays promotions for products and/or services in programs other than itself in a way that does not provide the user choice and control.

High

- Promotions do not have a clear close button that immediately closes it.
  - *The intent of closing the ad opens another ad.*
- Promotions do not have clear attribution of their source in each promotion.
- The program opening the promotion does not have a working uninstaller that uses a standard and discoverable uninstall method.
  - *The entry's name in the standard uninstall method must match the name shown in the attribution.*

BrowserModifier: A program that makes browser modifications without user choice and control.

High

- Adds a browser toolbar, extension, plugin, default search or add-on without user choice and control.
- Redirects browser traffic (such as search queries and website visits) without user choice and control.
- Bypasses user consent dialogues from the browser or operating system.
- Removes or limits the user's ability to view or modify browser features or settings.
- Deletes or modifies search providers or add-ons from other publishers without user consent via a user interface.
- Re-enables an add-on that the user disabled without user consent via a user interface.
- Changes browsing experience without using the supported extensibility models.

Misleading: The program makes misleading and/or fraudulent claims about files, registry entries and/or other items on the system.

High

- Reports errors in an exaggerated or alarming manner about the user's system and requires the user to pay for fixing the errors or issues monetarily or by performing other actions.
- Indicates nonexistence of the memory.dmp file as an error/problem/etc.
- Indicates prefetcher files for installed programs are junk/error/etc.
- Does not provide individual correct details for errors/issues.
- System scanner/optimizer that purports to be from Microsoft

MonitoringTool: A program that monitors activity, such as keystrokes or captures screen images.

Severe

- Stores or transmits any of the following either without user choice and control or in a stealth manner:
  - Keystrokes
  - Screenshots
  - Email and instant messages
  - Voice and video/webcam
  - Banking details
  - Passwords

SoftwareBundler: A program that installs out of context software without user choice and control or that may be potentially unwanted.

High

- There is no ability to decline installing the offered, bundled program and/or exit the installer (the only option is to click next)
- Bundles other potentially unwanted software that we currently detect.

MisleadingAd

Special (enforced by SmartScreen)

- Advertisements must not deceptively lead users to believe they need something that is missing from their computer.
- Advertisements must not deceptively lead users to believe they have a problem with their system.
- Advertisements must not impersonate a system message or component.
- Advertisements must not impersonate a web component.
- A program download may not be invoked directly from an advertisement.
- Advertisements must have a defined border.
- Advertisements must not contain malicious code.

PUA worksheet

PUA: Programs adding extra advertising outside of themselves.

Moderate	• The program displays advertisements, promotions, or prompts the user to complete surveys for other products or services in programs other than itself. • The program adds extra advertisements into webpages.

PUA: Programs with little value and high risk.

Moderate	• The program is a system optimizer (e.g. registry optimizer, driver optimizer, performance optimizer) that solicits payment, and is persistent on reboot. • The program monitors and transmits user activities in programs other than itself for the purpose of marketing research.

PUA: Programs offering 3rd party bundled software.

Moderate	• The program includes offers and the carrier app is not by the same entity as the program. • The program offers other programs that qualify by the PUA OC criteria.

PUA: Programs installing in non-standard ways or changing identity for the purpose of evasion.

Moderate	• The program installs into non-standard install locations and adds itself to start automatically. • The program or variations of it change the program install location, program name, browser extension name, or digital signing certificate multiple times per month. • The program acts differently in the presence of a security product.

PUA: Programs unduly affecting performance negatively.

Moderate	• The program uses your computer resources to mine cryptocurrencies.

PUA: Programs with poor industry reputation.

For Automation Use Only. Not for use by researchers or for disputes.	• A program is considered detectable by reputable vendors.

https://www.microsoft.com/en-us/wdsi/antimalware-support/malware-and-unwanted-software-evaluation-criteria

Adding Signatures - PUA

Only Blocking signatures are allowed, not detection or clean.

Signatures must be limited to those users with the PUA feature turned on.

Only add attributes like “PUA:Block:<threatname>” for example “PUA:Block:CoinMiner“

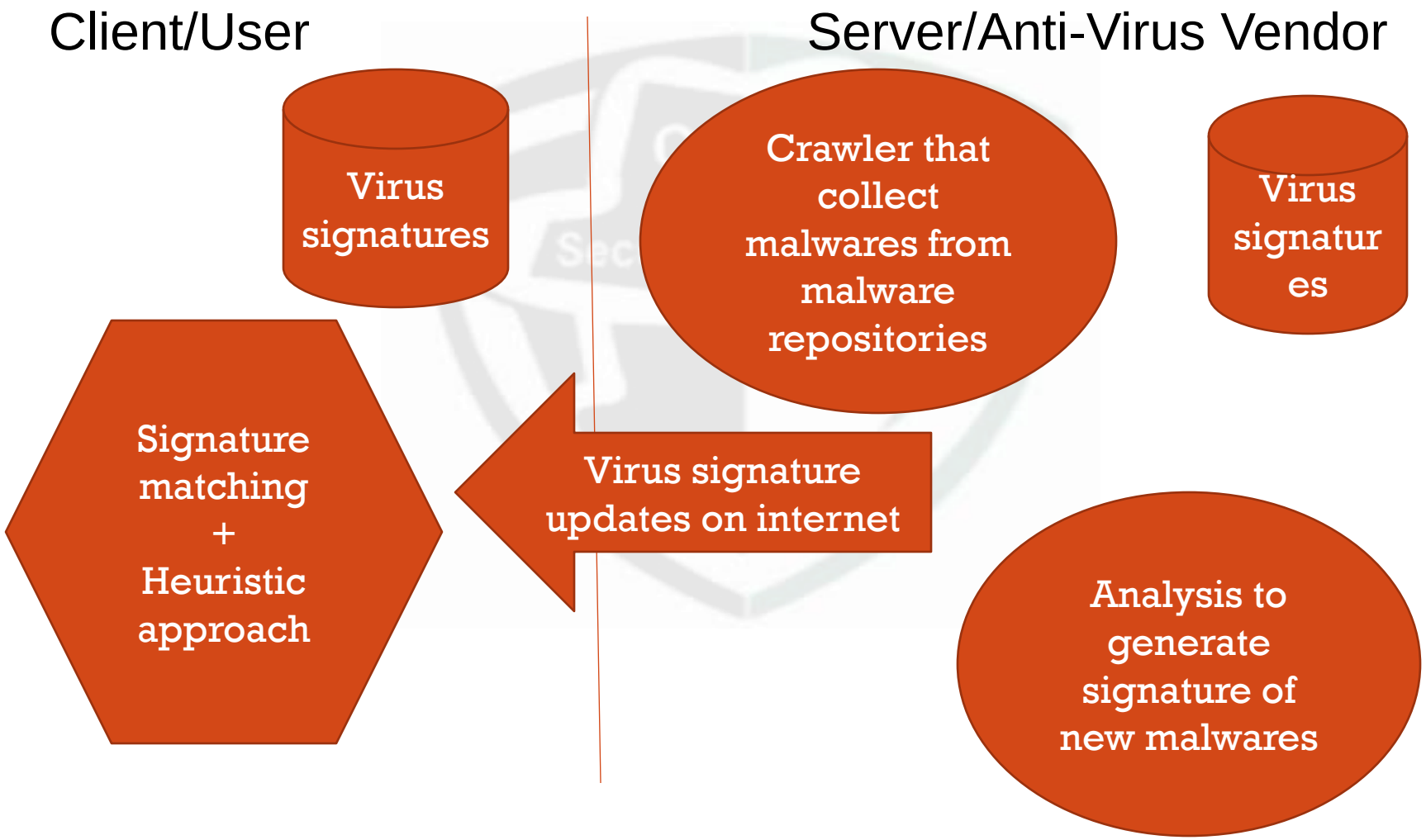
Customer Response

- FP (False Positive)

  - Vendor Inquiry

  Analysis Sample again
  Recommend changes in the Software
  Recommend to take certificate

Antivirus Defense System



Signatures.

- Types of Malware signatures
  - Strict Signatures
    Identification of malware
    <Sha, CRC1, CRC2,.. CRCN Malware Name>
  - Loose/Heuristic Signatures
    - Identification + Classification of malware/ Identify its family

Signatures.

- Types of Malware signatures
  - Strict Signatures
    Identification of malware
    <Sha, CRC1, CRC2,.. CRCN Malware Name>
  - Loose/Heuristic Signatures
    - Identification + Classification of malware/ Identify its family

```
#include <sys/types.h>                  /* standard POSIX headers */
#include <sys/stat.h>
#include <dirent.h>
#include <fcntl.h>
#include <unistd.h>
struct stat sbuf;                       /* for lstat call to see if file is sym link */

search(char *dir_name)
{                                       /* recursively search for executables */
    DIR *dirp;                          /* pointer to an open directory stream */
    struct dirent *dp;                  /* pointer to a directory entry */

    dirp = opendir(dir_name);           /* open this directory */
    if (dirp == NULL) return;           /* dir could not be opened; forget it */
    while (TRUE) {
        dp = readdir(dirp);             /* read next directory entry */
        if (dp == NULL) {               /* NULL means we are done */
        chdir ("..");                   /* go back to parent directory */
        break;                          /* exit loop */
    }
    if (dp->d_name[0] == '.') continue; /* skip the . and .. directories */
    lstat(dp->d_name, &sbuf);           /* is entry a symbolic link? */
    if (S_ISLNK(sbuf.st_mode)) continue; /* skip symbolic links */
    if (chdir(dp->d_name) == 0) {       /* if chdir succeeds, it must be a dir */
        search(".");                    /* yes, enter and search it */
    } else {                                /* no (file), infect it */
        if (access(dp->d_name,X_OK) == 0) /* if executable, infect it */
            infect(dp->d_name);
    }
    closedir(dirp);                     /* dir processed; close and return */
}
```


```
rule RuleName : Tag1 Tag2 Tag3
{
    meta:
        description = "Simple description of this rule"

    strings:
        $a = "some string to search in file"
        $b = "another string to search in file"

    condition:
        $a or $b
}
```

1

2

3

4

MALWARE SAMPLES

Where to Get Malware Samples for Analysis?

https://zeltser.com/malware-sample-sources/
http://www.tekdefense.com/downloads/malware-samples/
http://thezoo.morirt.com/
http://openmalware.org/
https://github.com/InQuest/malware-samples
https://github.com/ashubits/samples

Contagio Malware Dump: Password required
FreeTrojanBotnet: Registration required
Hybrid Analysis: Registration required
KernelMode.info: Registration required
MalShare: Registration required
Malware.lu's AVCaesar: Registration required
PacketTotal: Malware inside downloadable PCAP files
SNDBOX: Registration required
theZoo aka Malware DB
URLhaus: Links to live sites hosting malware
VirusBay: Registration required
VirusSign: Registration required

Malware Analysis

- Basic Analysis
  - File Structure and file Identification.
  - Automation Analysis: VT, Hybrid-Analysis.com, herdProtect, etc.
- Static Analysis
  - Malicious Indicators.
  - Tools.
  - Challenges: Packers and Obfuscations.
- Dynamic Analysis
  - Virtual Environment.
  - Custom Packers or Cryptors.
  - Debuggers X64 DBG.
  - Challenges: Anti Debugging And Anti VMS.

Basic Analysis: File Structure and file Identification.

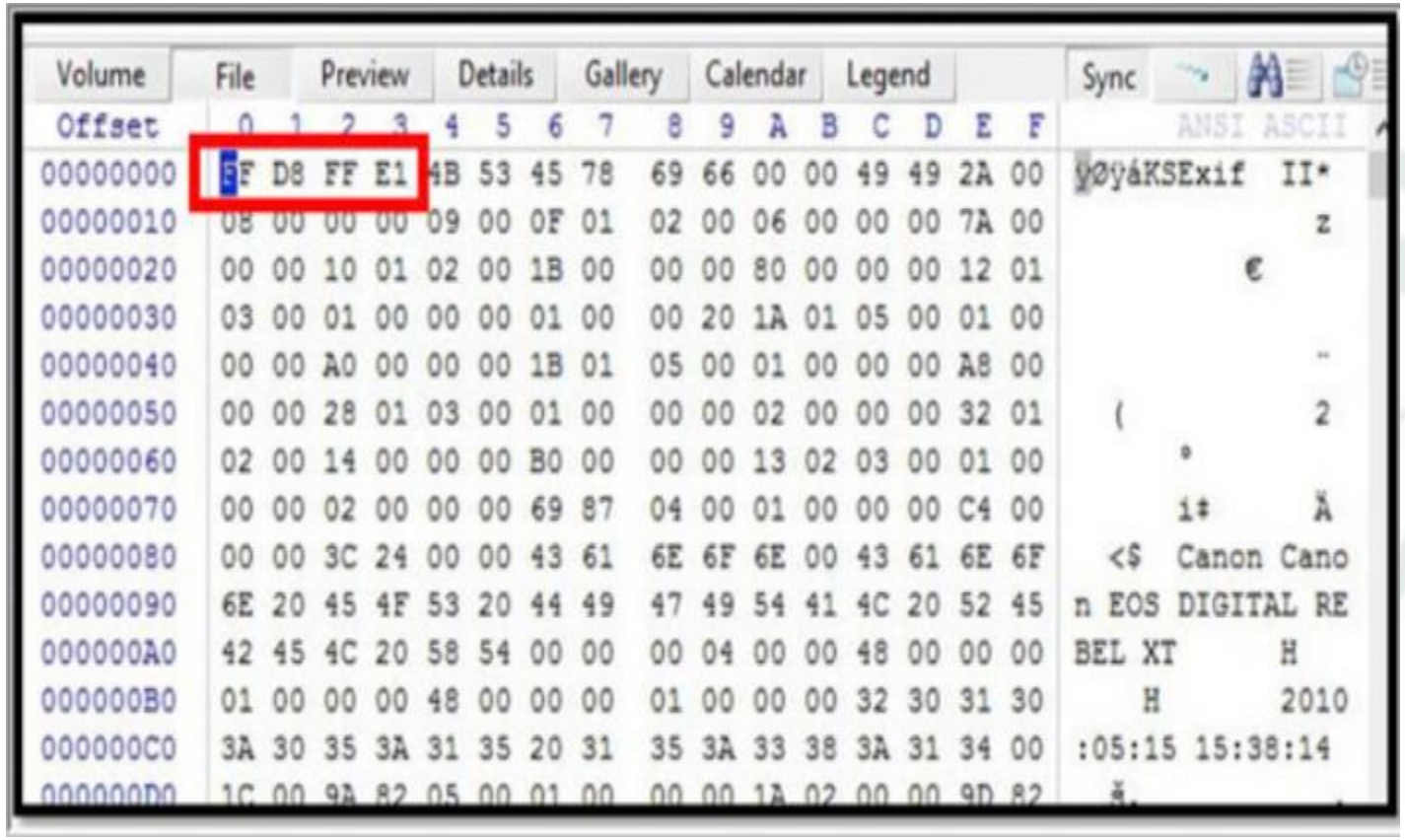
- Recognize the file
  - .doc
  - .exe, .dll, .com, .sh, etc.
  - .txt
  - .pdf, etc.
- File Structure
  - Header
  - Payload

https://en.wikipedia.org/wiki/List_of_file_signatures

Basic Analysis: Virustotal

- File Details
- Relation ships
  - Network connections
  - Similar files
- Memory strings (private Account)
- Behaviour of File

Basic Analysis: File Type

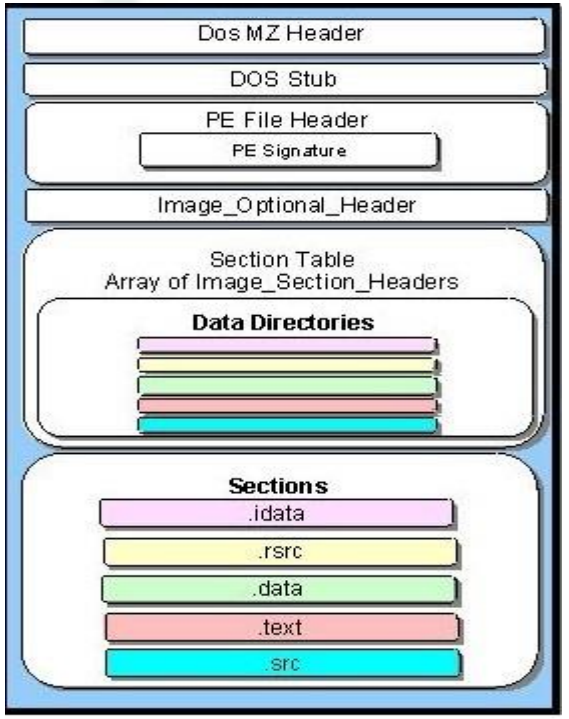


https://en.wikipedia.org/wiki/List_of_file_signatures

Basic Analysis: PE file Structure

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	DOS header
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	DOS stub
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	
00000080	50	45	00	00	4C	01	03	00	8D	FA	81	4D	00	00	00	00	PE signature, PE file header
00000090	00	00	00	00	E0	00	02	01	0B	01	08	00	00	0A	00	00	
000000A0	00	08	00	00	00	00	00	00	9E	28	00	00	00	20	00	00	PE standard fields
000000B0	00	40	00	00	00	00	40	00	00	20	00	00	00	02	00	00	
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	PE NT fields
000000D0	00	80	00	00	00	02	00	00	01	82	00	00	03	00	40	85	
000000E0	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	
00000100	4C	28	00	00	4F	00	00	00	00	40	00	00	A8	05	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Data directories
00000120	00	60	00	00	0C	00	00	00	A4	27	00	00	1C	00	00	00	
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000150	00	00	00	00	00	00	00	00	00	20	00	00	08	00	00	00	
00000160	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	00	
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	
00000180	A4	08	00	00	00	20	00	00	00	0A	00	00	00	02	00	00	.text section header
00000190	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	
000001A0	2E	72	73	72	63	00	00	00	A8	05	00	00	00	40	00	00	.rsrc section header
000001B0	00	06	00	00	00	0C	00	00	00	00	00	00	00	00	00	00	
000001C0	00	00	00	00	40	00	00	40	2E	72	65	6C	6F	63	00	00	
000001D0	0C	00	00	00	00	60	00	00	00	02	00	00	00	12	00	00	.reloc section header
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	42	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000200	80	28	00	00	00	00	00	00	48	00	00	00	02	00	05	00	.text section
00000210	E4	20	00	00	C0	06	00	00	09	00	00	00	01	00	00	06	
00000220	00	00	00	00	00	00	00	00	50	20	00	00	80	00	00	00	
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

File.exe
Pebear
Cffexplorer
PEexplorer



Static Analysis

- Indicators
  - Digital Signature
  - Resources information
    - Embedded files
    - Malicious Scripts
  - Strings
    - Imports
    - Exports
    - Embedded URLS/IPS example: http://magnaki.com/

Tools: SigCheck, BinTex/Strings, PeStudio

Example: some interested strings

- Digital Signature: not verified
- Imports:
- Strings found

ShellExecuteExA - Can be used to run applications

Socket APIs - Make network connections

File API - read/modify files

60.248.52.95:443 - Potential network signature

http://www.ueopen.com/test.html - Potential network signature

cmd.exe - The malware could be trying to run shell commands

*(SY)# - Potential network signature, possible used for a remote shell prompt

Example: Inferences

- What happens when you run this malware?

  Connects to 60.248.52.95, offers up a remote shell, then deletes itself

- Are there any network based signatures?

  Connects to port 443 on 60.248.52.95

- What do you think is the purpose of this malware?
  - To act as a backdoor by offering a remote shell to the attacker

EVOLUTION OF MALWARE

1st Generation/Static Malware:

- Virus, Backdoor, Trojan horse, Rootkit, Scareware, Adware, Worm, etc.

2nd Generation/Dynamic Malware:

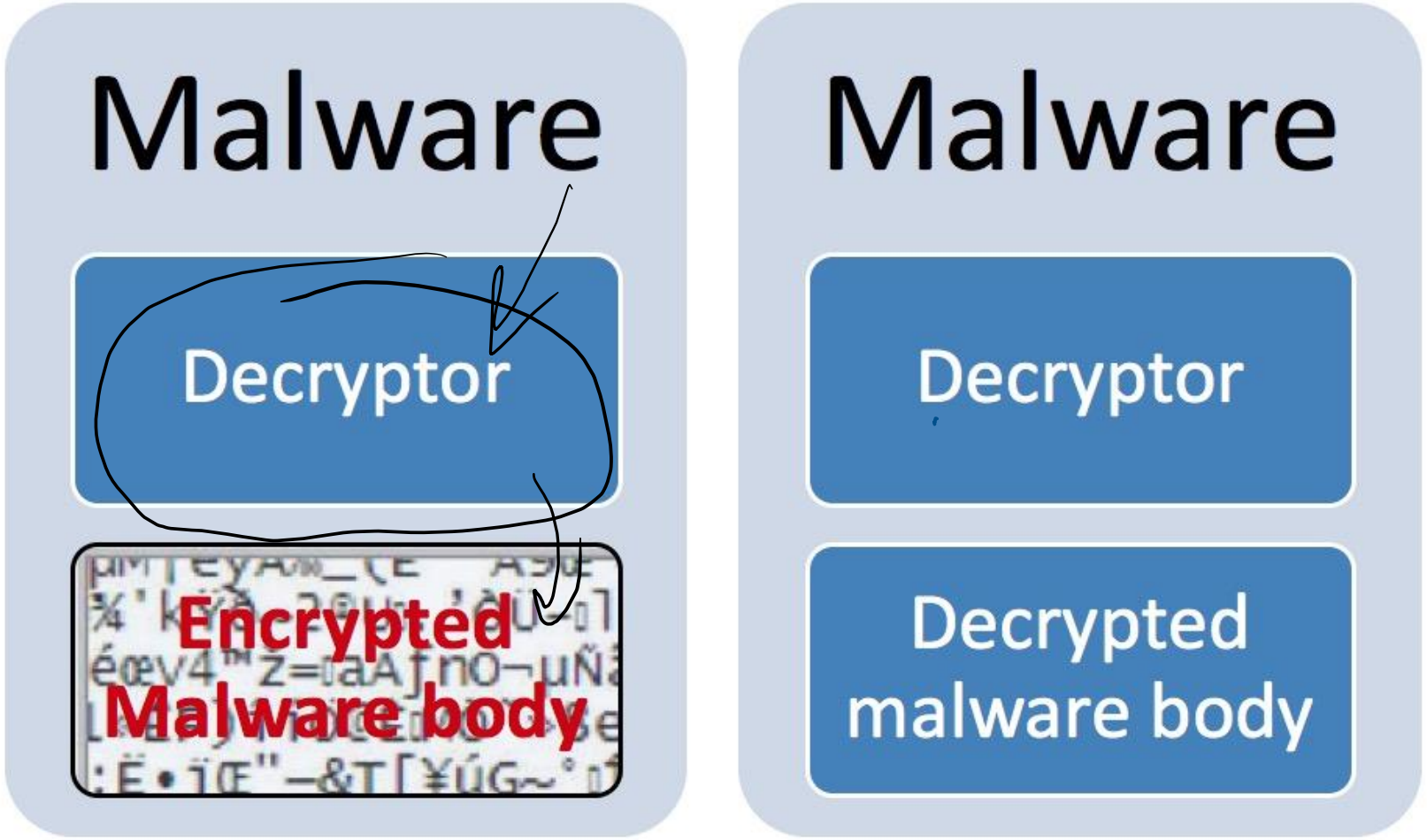
- Encryption
  - •Encrypted Malware
  - •Packed Malware
  - •Oligormorphic Malware
- Obfuscation
  - •Polymorphic Malware
  - •Metamorphic Malware.

Challenges

"Being able to go undetected by any security vendor

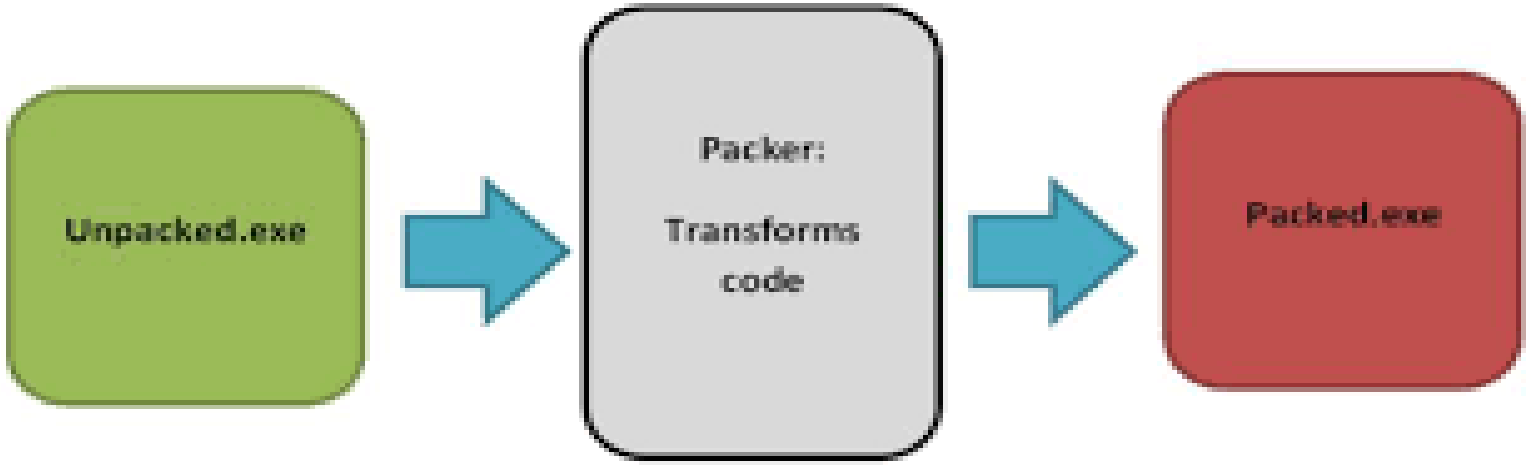
is the holy grail for malware authors"

- **Packers:** This usually is short for "runtime packers" which are also known as "self-extracting archives".
- **Crypters:** Encrypt the Malware with some logics (mostly custom logics)

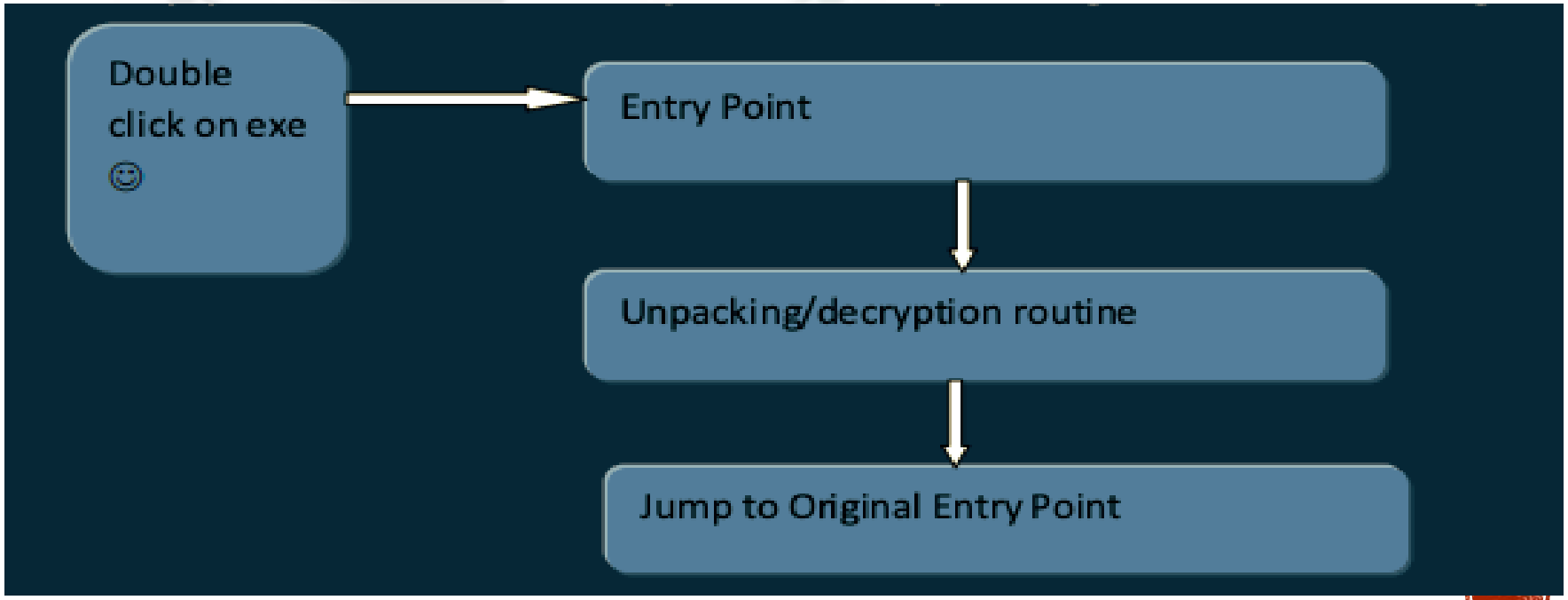


Packer/Crypters

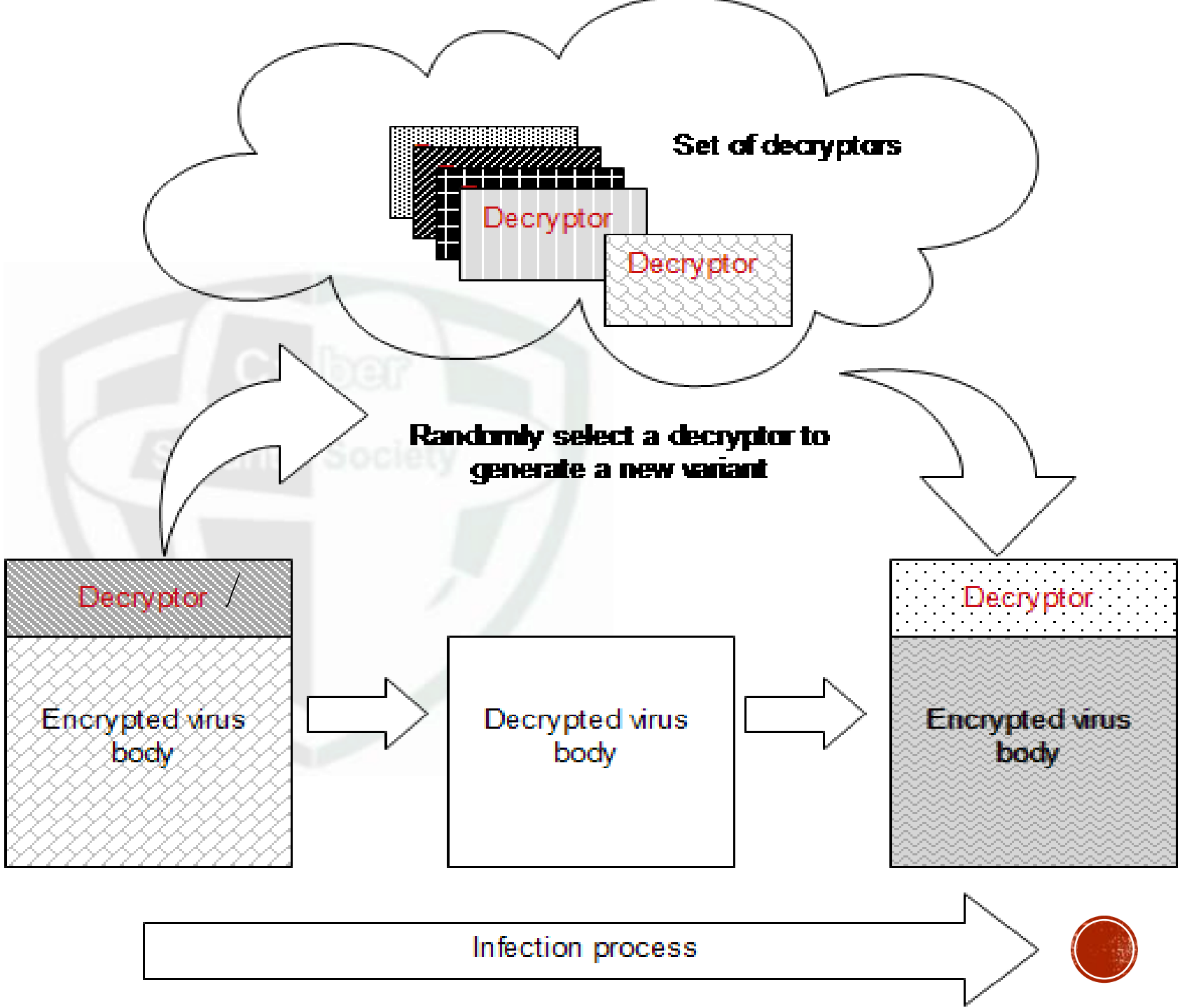
- packer



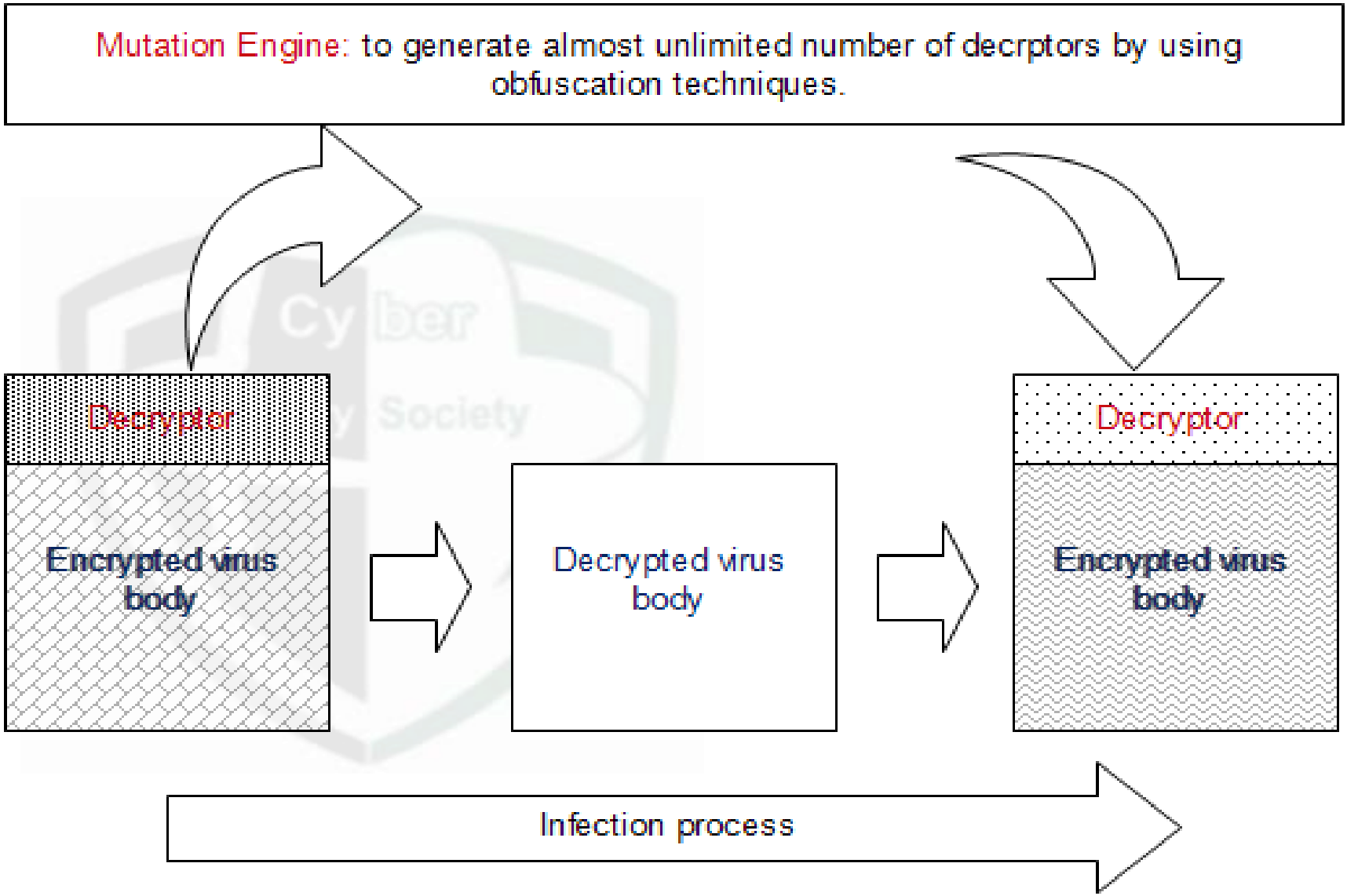
- **Cryptor**



OLIGORMORPHIC MALWARE



POLYMORPHIC MALWARE



OBFUSCATION TECHNIQUES

- Register usage exchange
- This method was used by the Win95/RegSwap virus, which was created by the virus writer Vecna and released in 1998.
- **Different generations of the virus will use the same code but with different registers**

a)

```
5A                  pop edx
BF04000000          mov edi,0004h
8BF5                mov esi,ebp
B80C000000          mov eax,000Ch
81C288000000        add edx,0088h
8B1A                mov ebx,[edx]
899C8618110000      mov [esi+eax*4+00001118],ebx
```

b)

```
58                  pop eax
BB04000000          mov ebx,0004h
8BD5                mov edx,ebp
BF0C000000          mov edi,000Ch
81C088000000        add eax,0088h
8B30                mov esi,[eax]
89B4BA18110000      mov [edx+edi*4+00001118],esi
```

OBFUSCATION TECHNIQUES

- Register usage exchange
- This method was used by the Win95/RegSwap virus, which was created by the virus writer Vecna and released in 1998.
- **Different generations of the virus will use the same code but with different registers**

a)

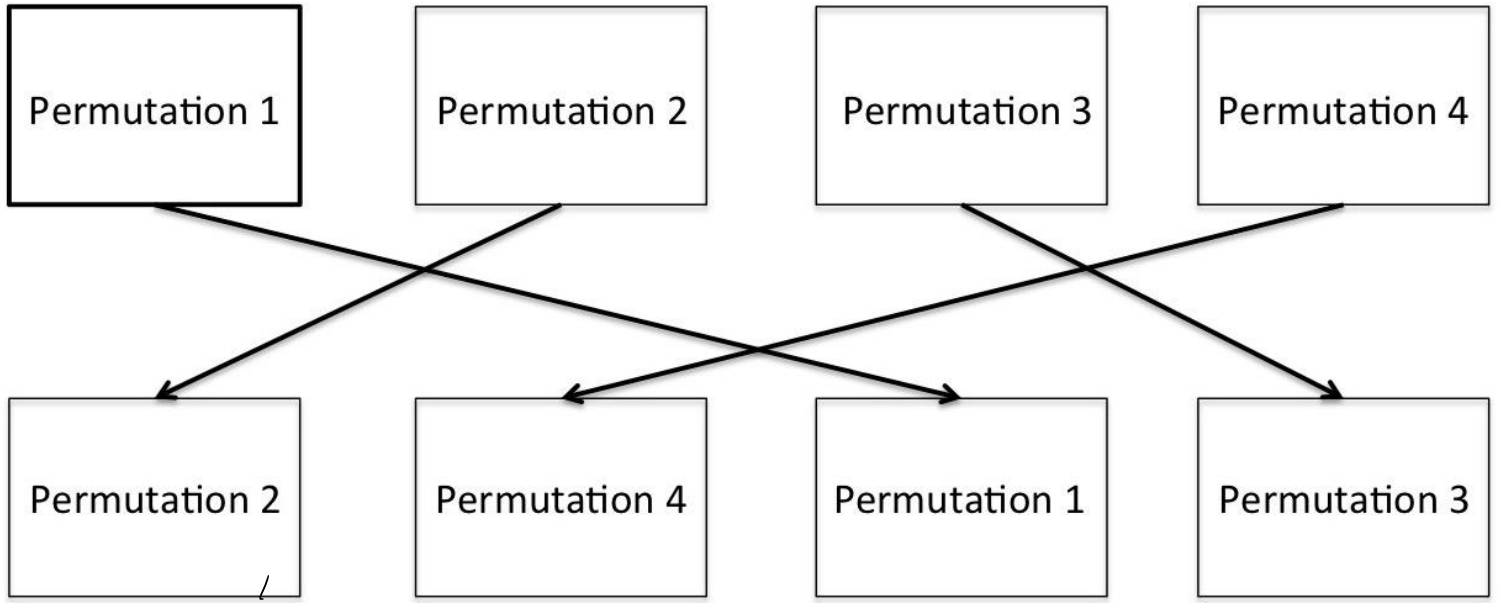
```
5A              pop edx
BF04000000      mov edi,0004h
8BF5            mov esi,ebp
B80C000000      mov eax,000Ch
81C288000000    add edx,0088h
8B1A            mov ebx,[edx]
899C8618110000  mov [esi+eax*4+00001118],ebx
```

b)

```
58              pop eax
BB04000000      mov ebx,0004h
8BD5            mov edx,ebp
BF0C000000      mov edi,000Ch
81C088000000    add eax,0088h
8B30            mov esi,[eax]
89B4BA18110000  mov [edx+edi*4+00001118],esi
```

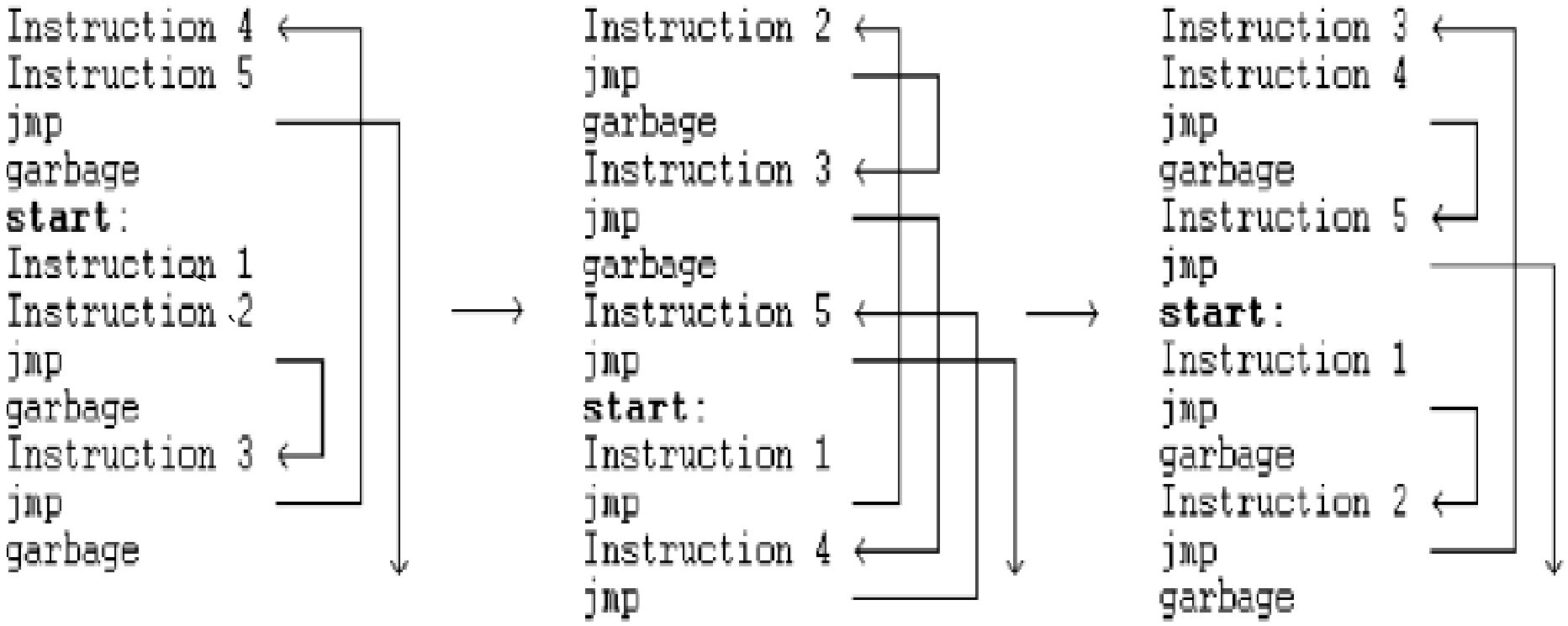
OBFUSCATION TECHNIQUES

- Permutation Techniques

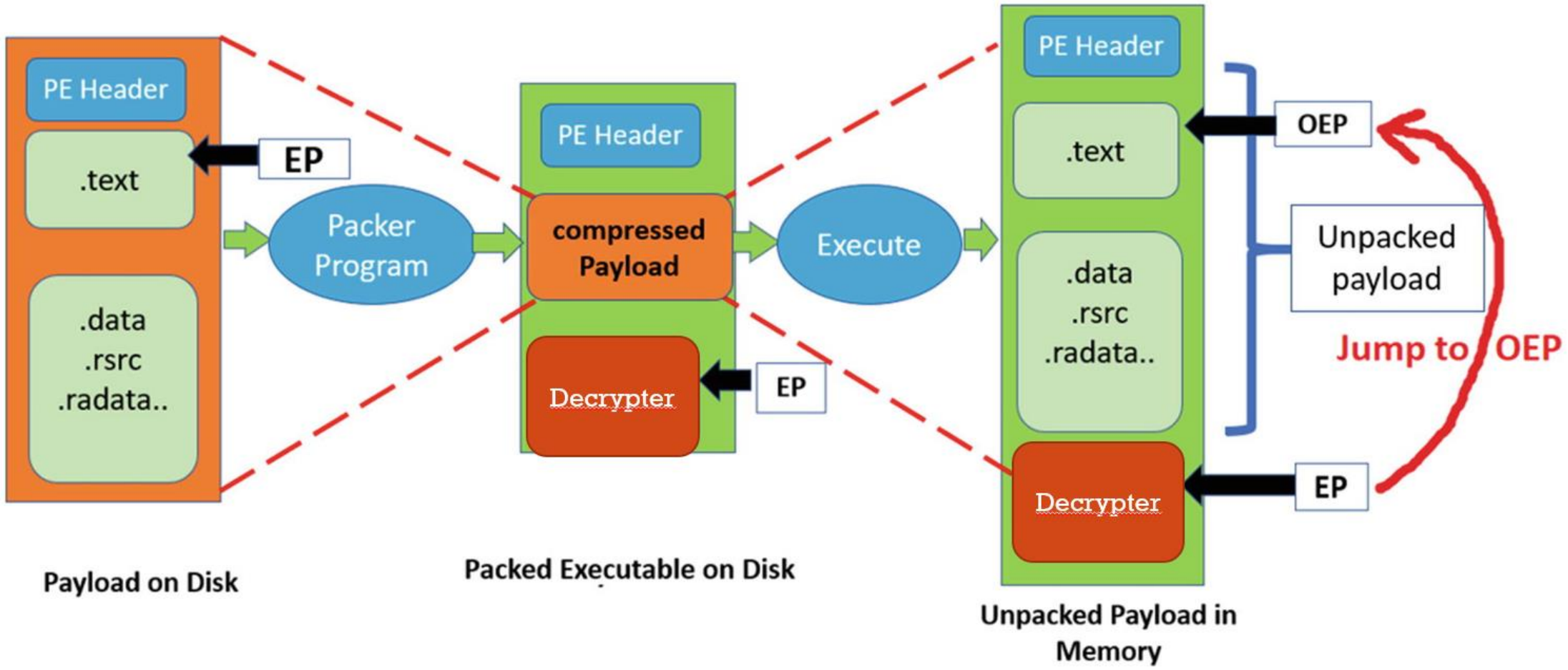


OBFUSCATION TECHNIQUES

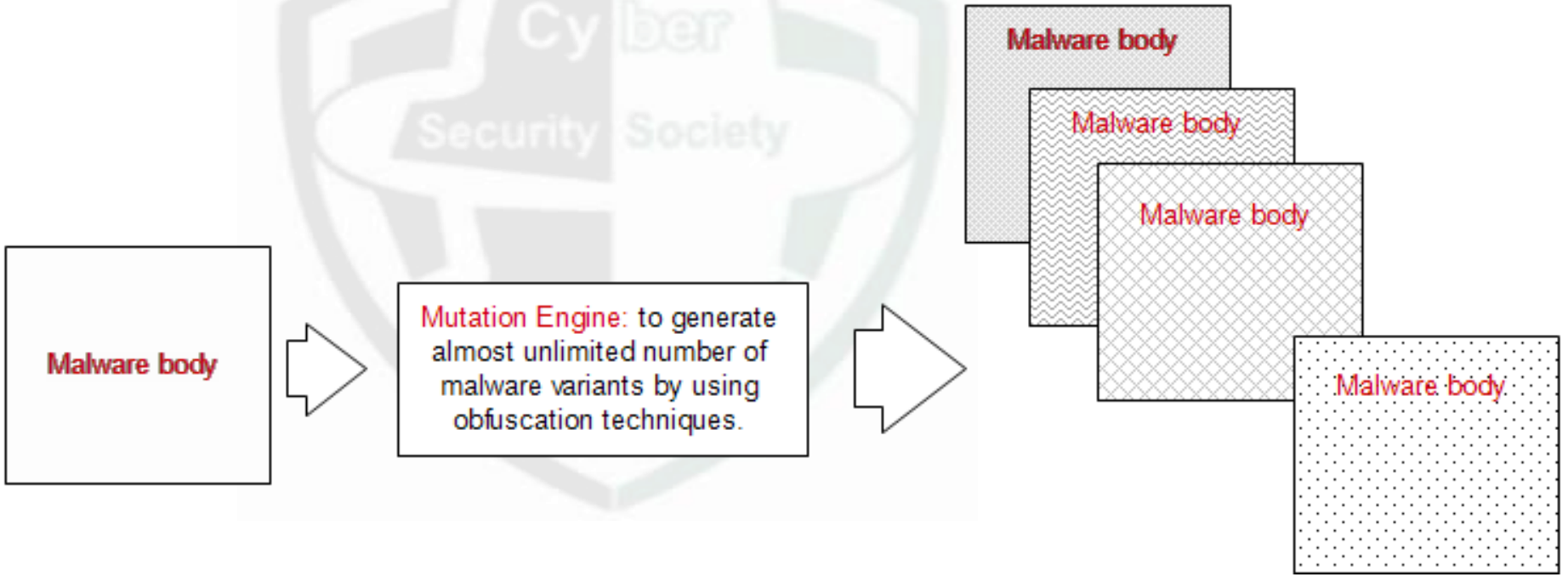
- Insertion of Jump Instructions



DYNAMIC SIGNATURES



METAMORPHIC MALWARE



DYNAMIC ANALYSIS- Basic Indicators

- Change in Registries entries
- File operations
- Network connections
- Memory strings
- Files dropped in Startup folders

Tools: **ProcessHacker, ProcessMonitor, NetworkMonitor, APTdate, etc**

OBFUSCATION IN SCRIPT FILES

(A)

```
function setText(data) {
document.getElementById("myDiv").innerHTML = data;
}
```

(B)

```
function ghds3x(n) {
h = "\x69\u006En\u0065r\x48T\u004DL";
a="s c v o v d h e , n i";x=a.split(" ");b="gztxleWentBsyf";
r=b.replace("z",x[7]).replace("x","E").replace("s","").replace("f","I")
["repl" + "ace"]("W","m")+"d";
c="my"+String.fromCharCode(68)+x[10]+"v";
s=x[5]+x[3]+x[1]+"um"+x[7]+x[9]+"t";d=this[s][r](c);if(+!![])
{ d[h]=n; } else { d[h]=c; } }
```

SOCIAL ENGINEERING

- Social engineering uses various methods of contact and trust building in order to elicit an action or divulging of information that can be used for malicious purposes such as entry to a building or performing cyber-attacks.

  - **Phishing emails** that are crafted in such a way to entice you into clicking on malicious links or providing more information

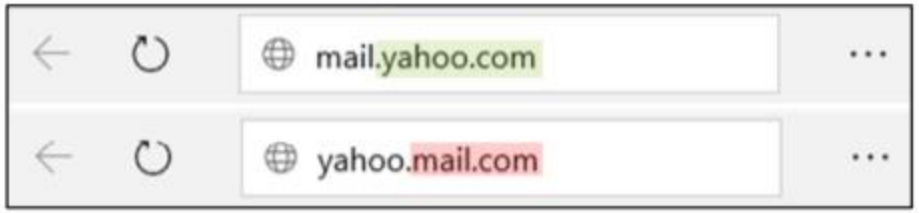
  .

Link manipulation is done by directing a user fraudulently to click a link to a fake website. This can be done through many different channels, including emails, text messages and social media.

1. Use of sub-domains

The URL hierarchy always goes from right to left. If you are accessing **Yahoo Mail**, the correct link should be mail.yahoo.com – where Yahoo is the main domain, and Mail is the sub-domain.

A phisher may try to trick you with the fraudulent link yahoo.mail.com which will lead you to a page with a main domain of Mail and a sub-domain of Yahoo.



2. Hidden URLs

This is when a phisher hides the actual URL of a phishing website under plain text, such as "Click Here" or "Subscribe".

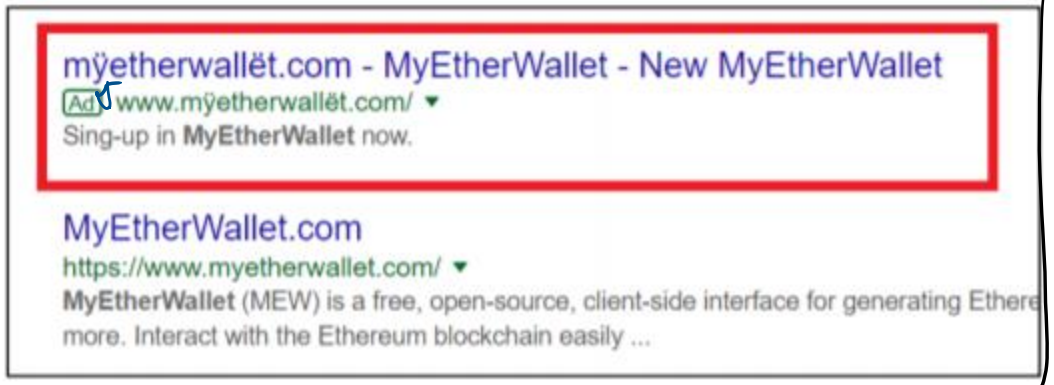
A more convincing scam could even display a legitimate URL that actually leads to an unexpected website.

3. Misspelled URLs

When a hacker buys domains with a variation in spellings of a popular domain, such as facebok.com, googlle.com, yahooo.com. This technique is also known as URL hijacking or typosquatting.

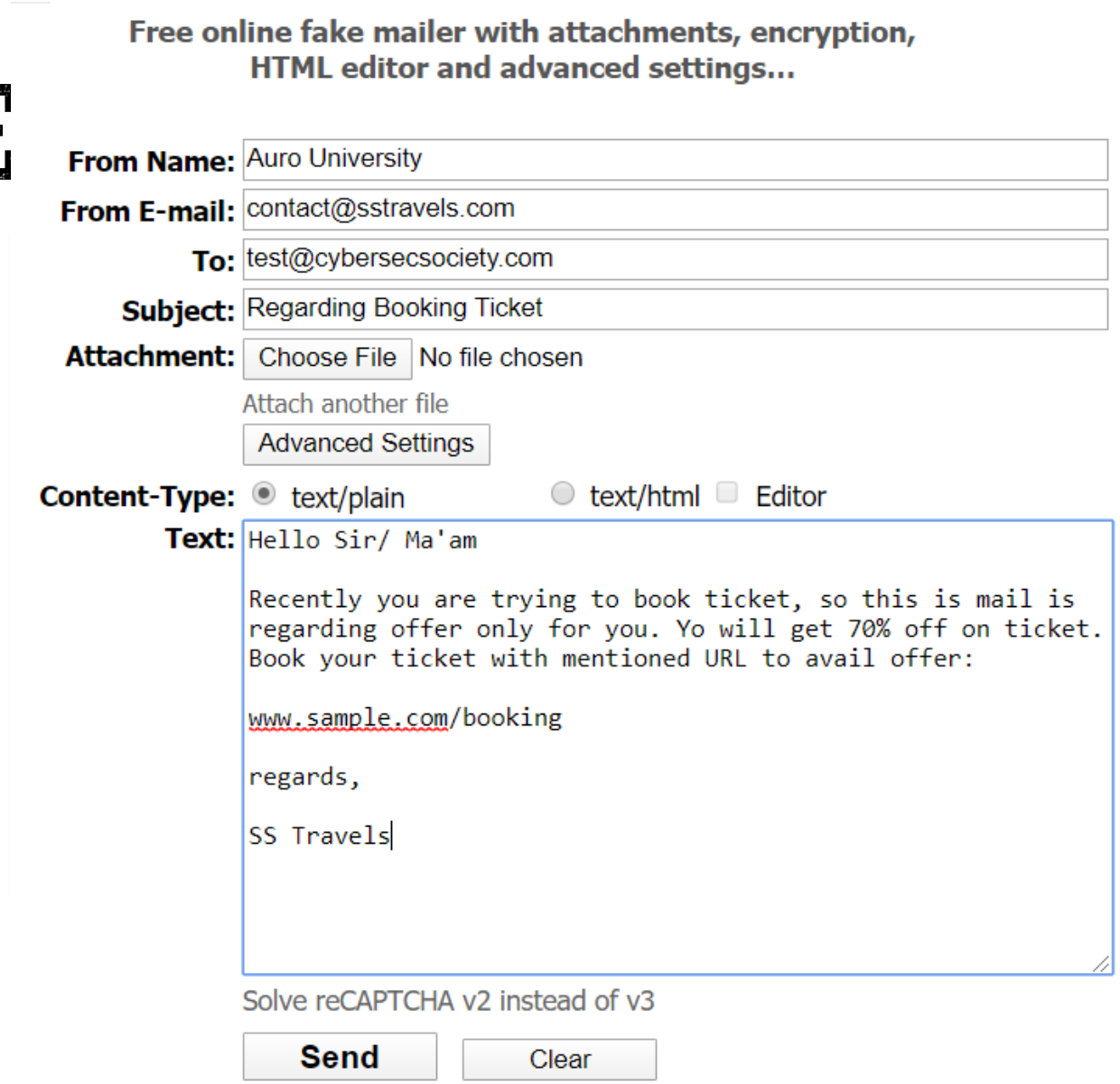
4. IDN homograph attacks

In this technique, a malicious individual misguides a user towards a link by taking advantage of similar looking characters.

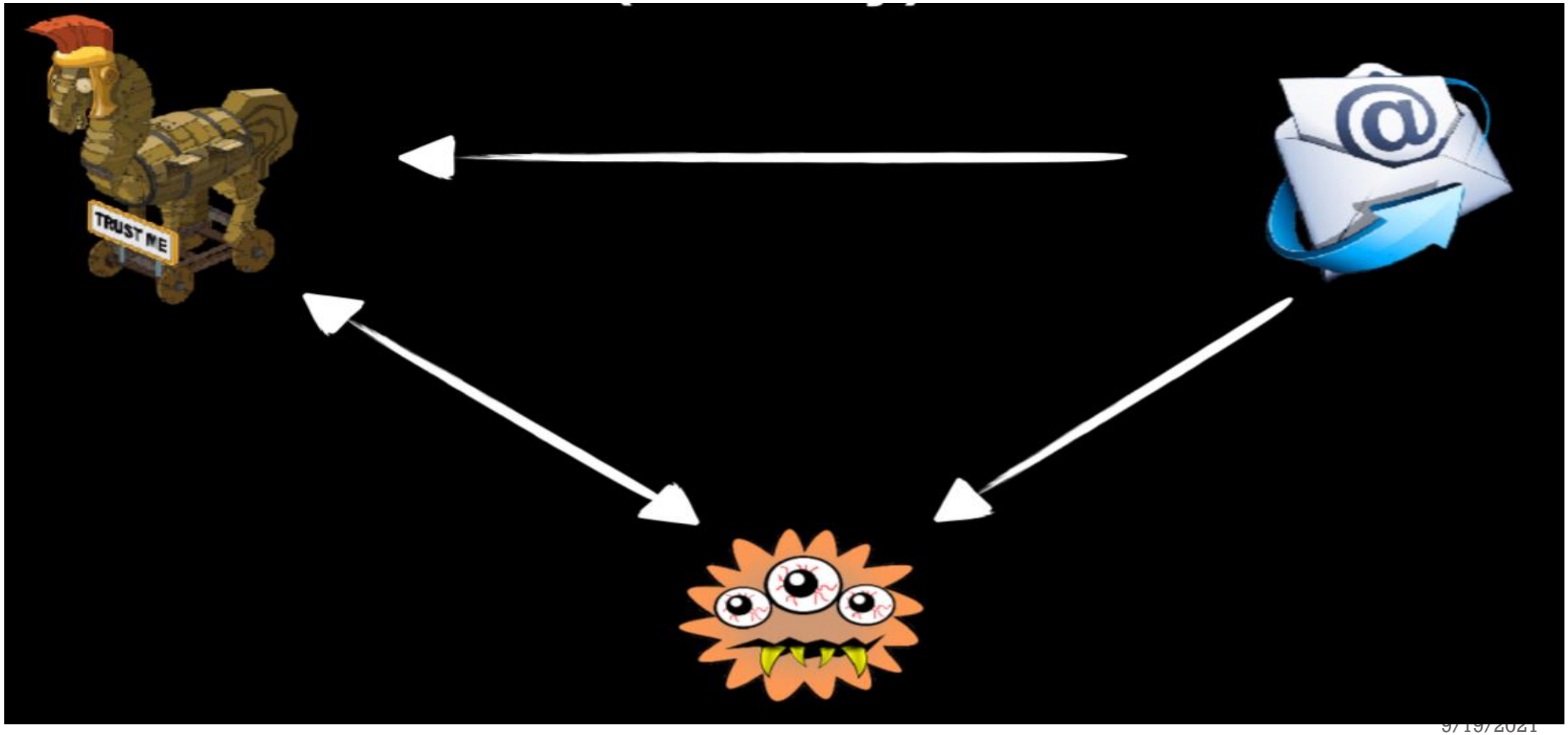


RELAY SERVE

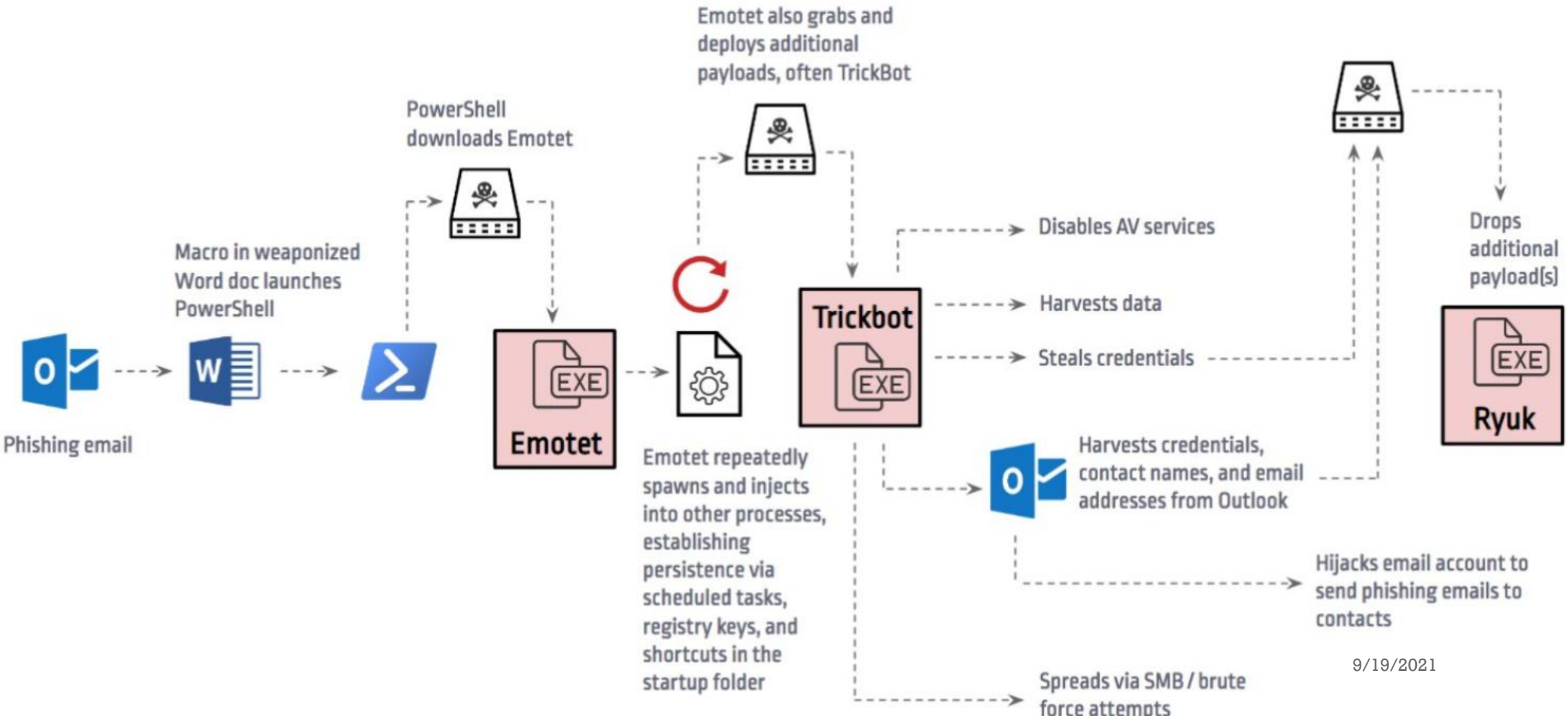
- https://emkei.cz/



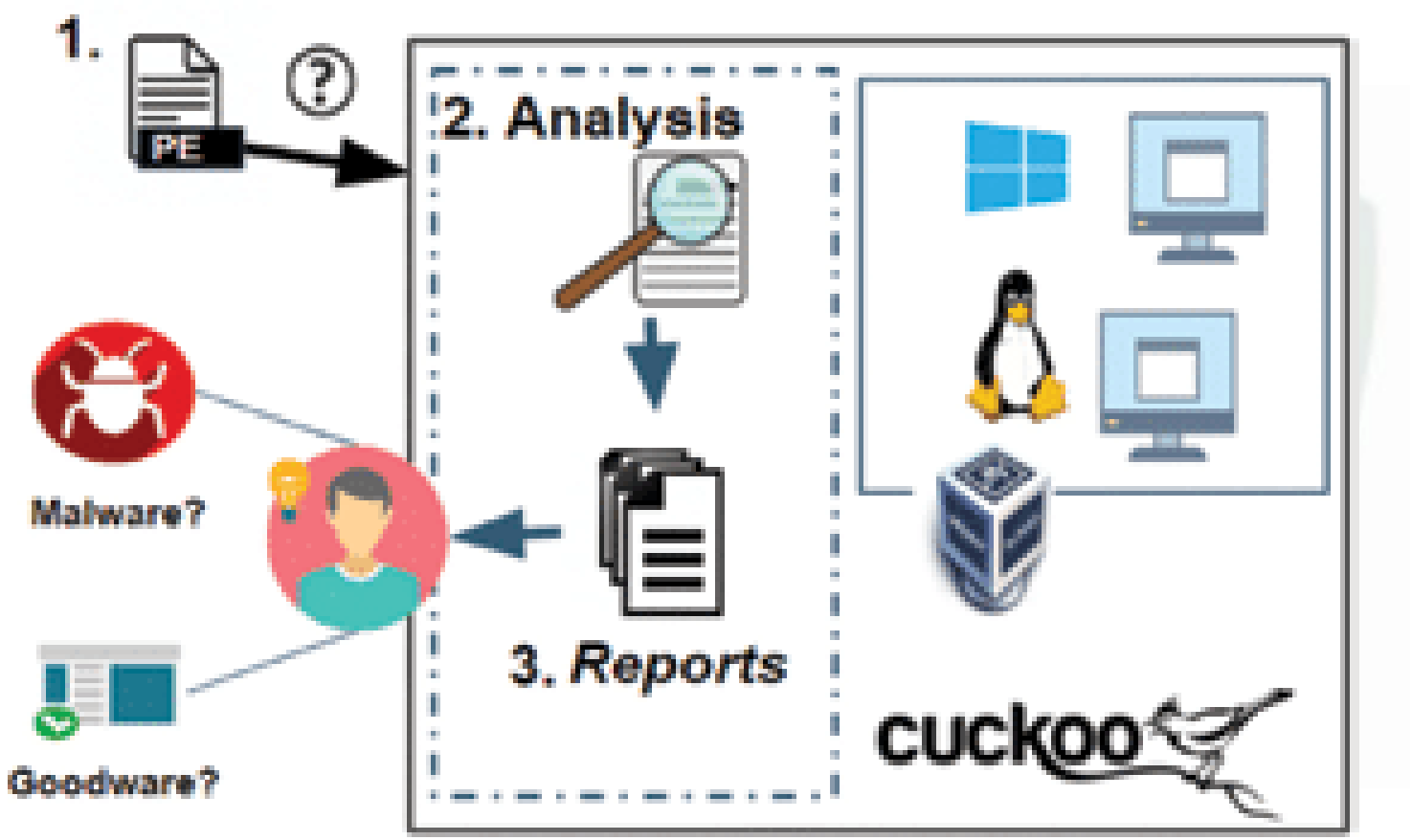
ADVANCED PHISHING



PHISHING WITH EMOTET MALWARE



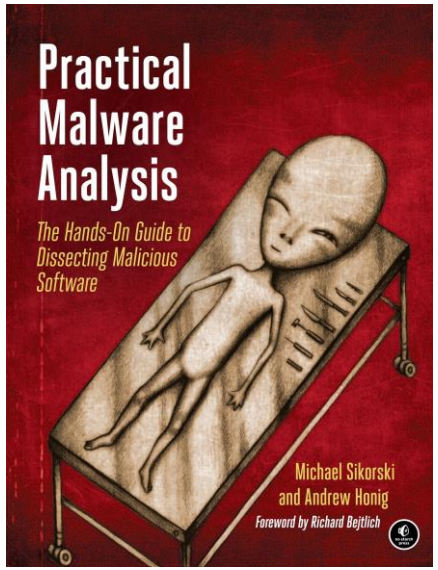
Malware detection System



WORK PROCESS

THANK YOU ☺

Where to Get Malware Samples for Analysis?



https://zeltser.com/malware-sample-sources/
http://www.tekdefense.com/downloads/malware-samples/
http://thezoo.morirt.com/
http://openmalware.org/
https://github.com/InQuest/malware-samples
https://github.com/ashubits/samples

Contagio Malware Dump: Password required
FreeTrojanBotnet: Registration required
Hybrid Analysis: Registration required
KernelMode.info: Registration required
MalShare: Registration required
Malware.lu's AVCaesar: Registration required
PacketTotal: Malware inside downloadable PCAP files
SNDBOX: Registration required
theZoo aka Malware DB
URLhaus: Links to live sites hosting malware
VirusBay: Registration required
VirusSign: Registration required

Dr. Ashu Sharma
@ashu.abviiitm@gmail.com