



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Mar. 25, 2008

A decorative graphic consisting of a vertical red bar on the left and a horizontal blue bar crossing it, both with a slight gradient.

Analysis of targeted attack and recent malware

Yuji Ukai

Researcher

Information-Technology Promotion Agency, Japan

Security Engineering Laboratory

IT Security Center (ISEC)

Introduction



The targeted attacks which target the specific companies/organizations are growing into a serious problem.

It is hard to know what is happening

- Recent malware attacks
- Different than traditional malware attacks

(sequential attack, downloader, using vulnerability, anti-reversing, anti-detection, target is restricted)

It is hard to get enough information and technical countermeasure.

- Details are not clear enough
- Making accurate threat analysis is difficult

The technical measures (Anti-Virus approach, etc) for traditional malware attacks are good enough ?

We do static analysis for entire code of recent malware for targeted attack.

We try to find the technical measures for targeted attack.

Targeted attack and recent malware 1

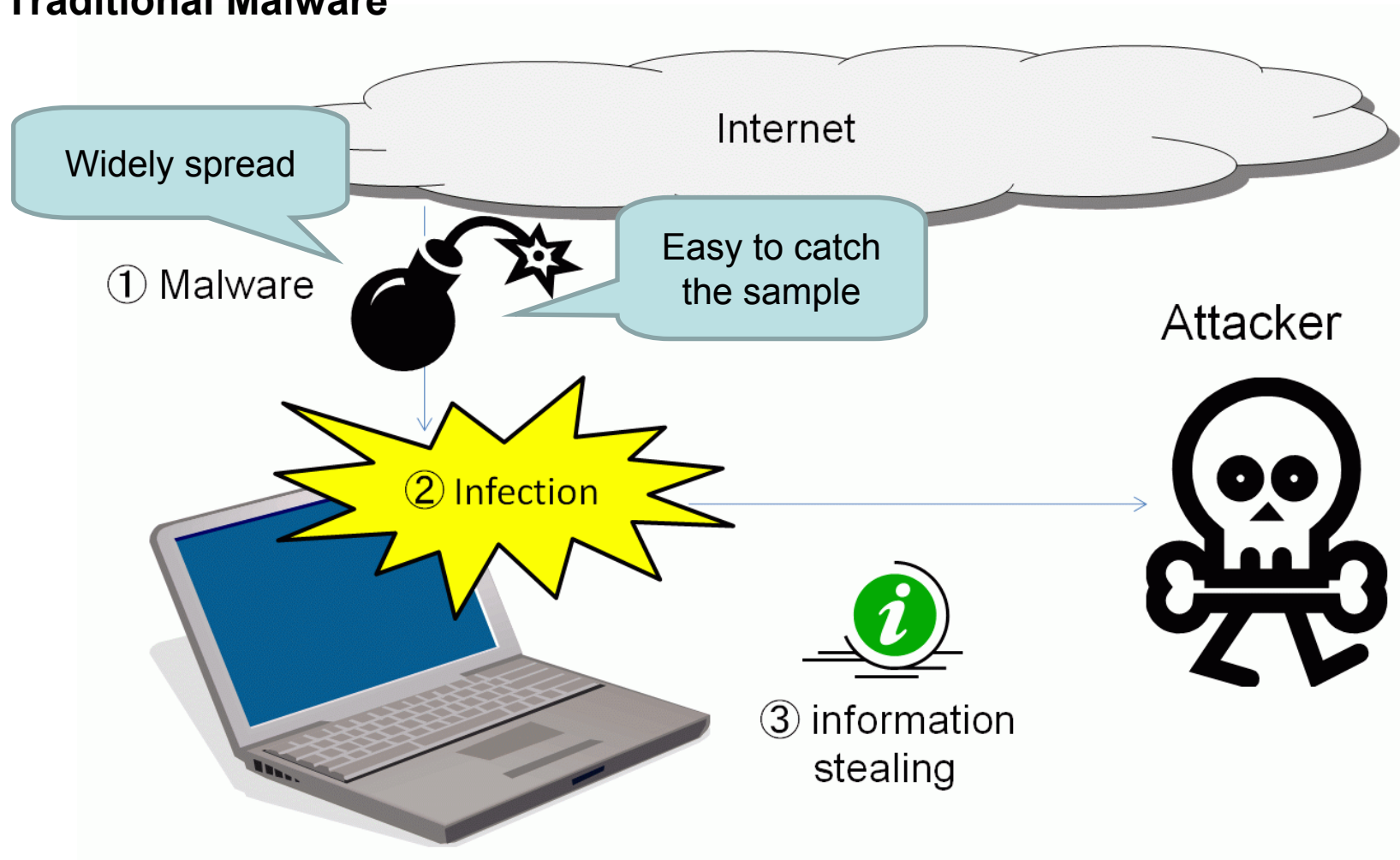


Recent malware is :

- One of the recent malware attack.
- Target (organization/people) is restricted.
- Targeted attack is happened with social engineering.
--- Hard to realize.
- Using 0-day/passive vulnerability.
--- Hard to detect/prevent
- Advanced anti-analysis/anti-detection technique.

Targeted attack and recent malware 2

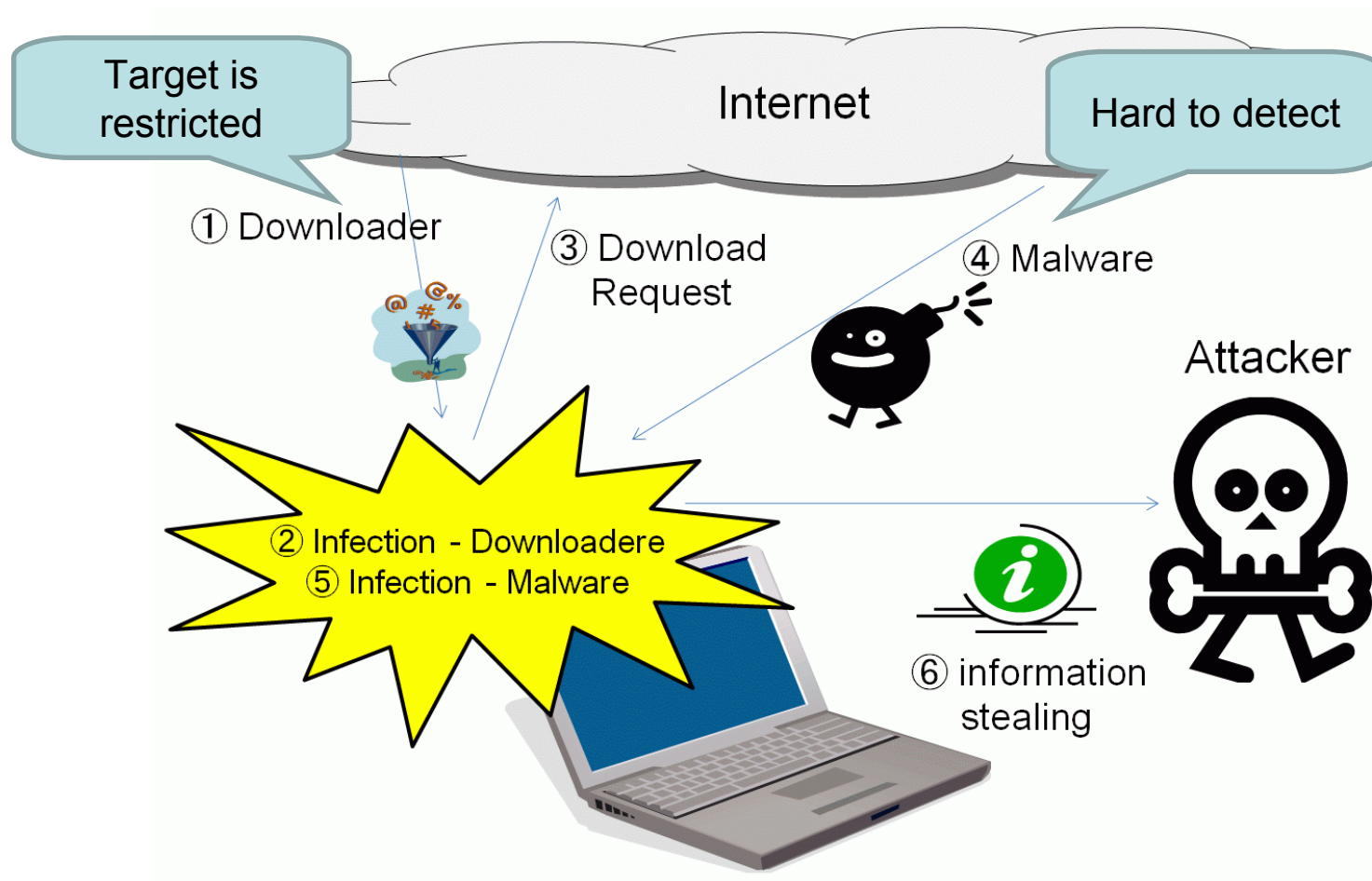
Traditional Malware



Targeted attack and recent malware 3

Sequential malware for targeted attack.

Traditional solutions (Anti-virus, Intrusion detection, etc) are not good enough.



Malware analysis and threat analysis



Recent malware:

- Attacking process is getting complicated.
- Code size is getting bigger.

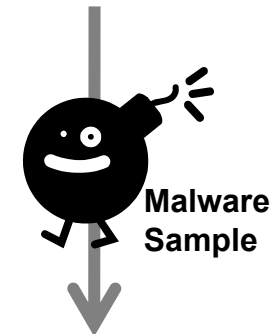
Malware definition pattern should be developed efficiency and quickly.

API (Application Program Interface) tracing, monitoring resources (file system, registry, etc.), network traffic analysis, etc...

Automated analysis is good enough to develop malware definition pattern.

However, anti-virus product is intended to prevent malware, not for threat analysis.

Automated analysis is not good enough for threat analysis.



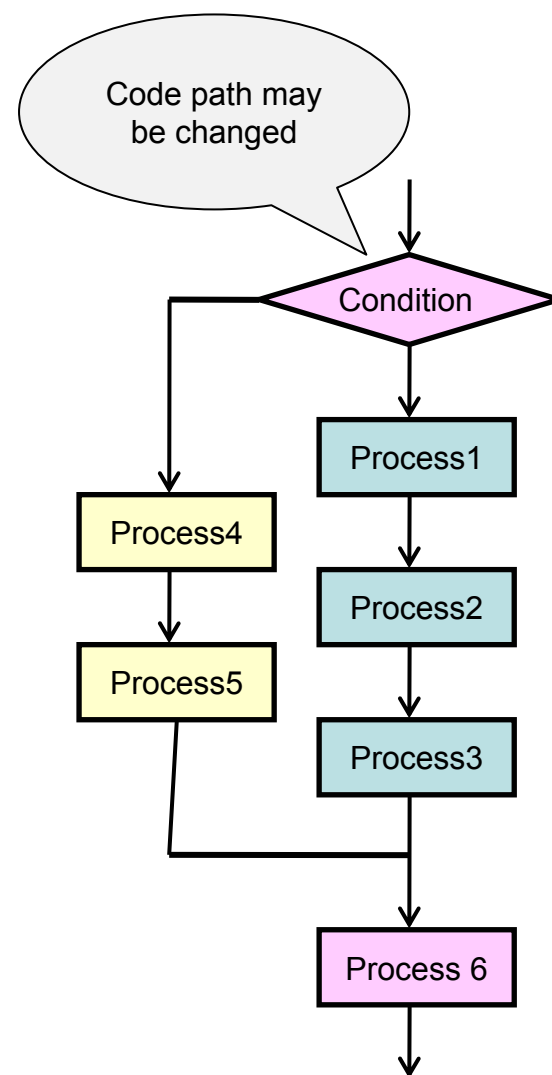
Can be used for threat analysis ??

Problems of threat analysis by automated malware analysis

Automated malware analysis :

Accurate analysis is difficult because details can not be analyzed.

- Code path may be changed.
- Hard to know what happens in different condition.
- Hard to create accurate code flow from trace log.
- Network traffic is encrypted.
- Next attacker's action can not be expected.



Overview



a. Vulnerabilities for targeted attacks - investigation of actual conditions

b. Vulnerability analysis

- Attack vector, Vulnerability type, Reliability analysis, Environment dependency analysis.
- Characteristics of software used by targeted attack

c. Malware for targeted attacks - investigation of actual conditions

d. Malware analysis

- Static and dynamic analysis.
- Analysis of attacker's server to deliver the sequential malware.
- Comparison of generic malware (ex. Storm worm)
- Attacking model analysis of targeted attacks.
- Detection and prevention of targeted attacks.
- Advanced analysis technique of the malware for targeted attacks

Vulnerabilities for targeted attacks 1

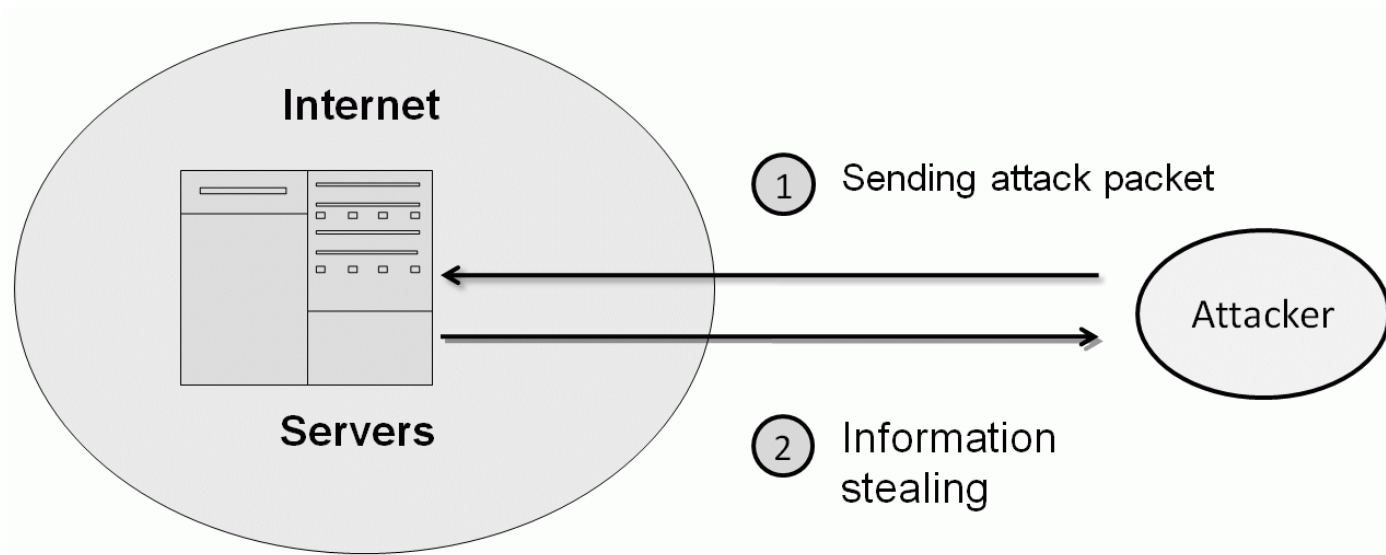
Target is a desktop PC located in the intranet (not the internet).

Target can not be accessed from outside of the intranet.

- Passive attack is used to attack.

Active attack :

- Attack the network service directly.
- It is hard to attack the intranet PC directly (Firewall, NAT, etc.)

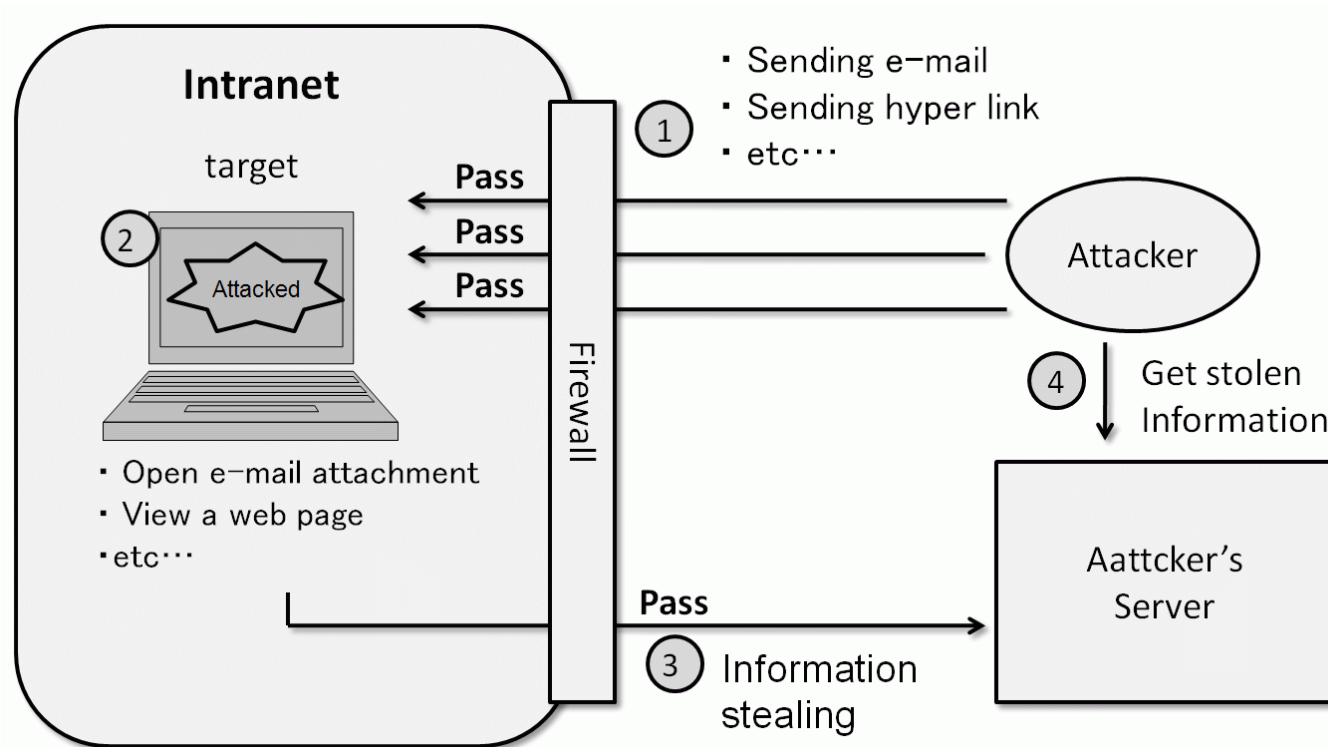


Vulnerabilities for targeted attacks 2

Passive attack:

Some kind of action (clicking of hyper link, opening e-mail, etc.) by targeted user is necessary.

Attack can be reached to the target into the intranet easily compared with active attack.



Examples of vulnerabilities used by actual targeted attacks 1

MDropper	
Name	Vulnerabilities
Trojan.Mdropper.A Trojan.Mdropper.B Trojan.Mdropper.D	Microsoft Word (MS03-050)
Trojan.Mdropper.C Trojan.Mdropper.F Trojan.Mdropper.G	Microsoft Office (MS03-037)
Trojan.Mdropper.J	Microsoft Office(MS06-037)
Trojan.Mdropper.H Trojan.Mdropper.I Trojan.Mdropper.K Trojan.Mdropper.Q Trojan.Mdropper.T Trojan.Mdropper.U Trojan.Mdropper.W Trojan.Mdropper.X	Microsoft Office (0-day, or unknown)
Trojan.Mdropper.L Trojan.Mdropper.P Trojan.Mdropper.S	Microsoft Word (MS06-027)
Trojan.Mdropper.N Trojan.Mdropper.R	Microsoft Office (MS06-047)
Trojan.Mdropper.Z	Microsoft Word (MS07-015)

Examples of vulnerabilities used by actual targeted attacks 2

PPDropper	
Name	Vulnerabilities
Trojan.PPDropper Trojan.PPDropper.D Trojan.PPDropper.E	Microsoft Office (MS06-012)
Trojan.PPDropper.B Trojan.PPDropper.C	Microsoft Power Point (0-day, or unknown)
Trojan.PPDropper.F	Microsoft Office (MS06-058)
Trojan.PPDropper.G	Microsoft Office (MS07-015)

Examples of vulnerabilities used by actual targeted attacks 3

Tarodrop, Acdropper, etc.	
Name	Vulnerabilities
Troj_Tarodrop	Ichitaro (0-day)
Exploit-LHAZ.a	Lhaz LHA vulnerability
Trojan.Radropper	WinRAR vulnerability
Trojan.Acdropper	Microsoft Jet Database Engine
Trojan.Acdropper.B	(0-day, or unknown)

Microsoft vulnerabilities used by targeted attacks



Vulnerability	Overview
MS03-037	Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution
MS03-050	Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run
MS06-012	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
MS06-027	Vulnerability in Microsoft Word Could Allow Remote Code Execution
MS06-047	Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution
MS06-058	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution
MS07-015	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
Lhaz vulnerability	ZIP file handling vulnerability could allow remote code execution
WinRAR vulnerability	LZH file handling vulnerability could allow remote code execution

Software and vulnerability for targeted attacks **IPA**[®]

1. “Safe” to open

Attachment of e-mail, hyperlink to external web server.

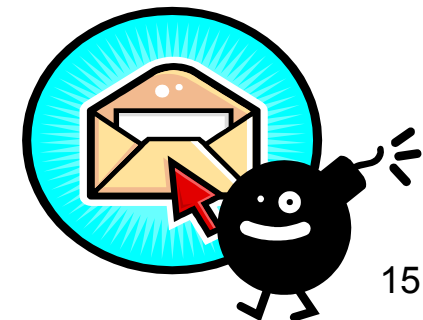
- Not an executable file. Data file which includes exploit.

Web browsers and e-mail clients are currently well audited.

- Number of "true exploitable vulnerabilities" is decreasing.

Vulnerabilities in applications (not in OS) being used.

- Word processing software, archive software, etc.



Software and vulnerability for targeted attacks IPA[®]

2. Vulnerabilities in popular applications are used in many cases.

- Guessing of applications installed in the target PC is difficult.
Popular application is targeted.
- Popularity of application is different between countries.
Vulnerabilities in domestic applications are also targeted.



Vulnerability used by targeted attacks

TROJ_MDROPPER Series and PPDROP Series

(1) Attack Vector

- Microsoft Office file
- e-mail attachment
- Malware infects by exploiting the vulnerability

(2) Type of vulnerability

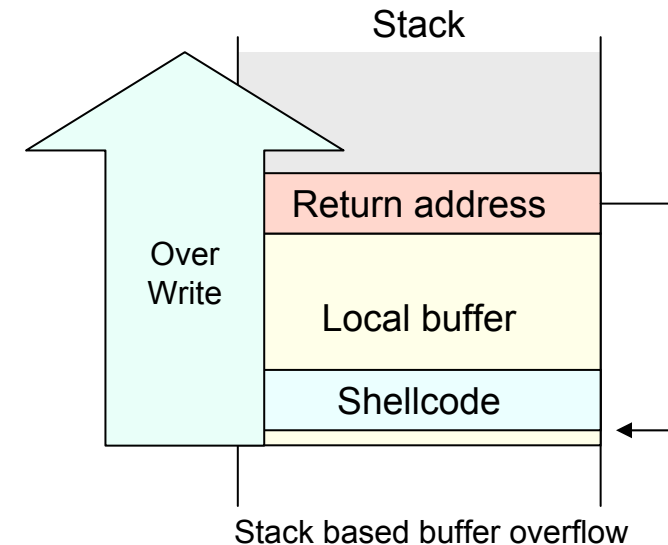
- Buffer overflow vulnerability (stack based)

(3) Reliability

- Highly reliable vulnerabilities are only used.

(4) Environment dependency

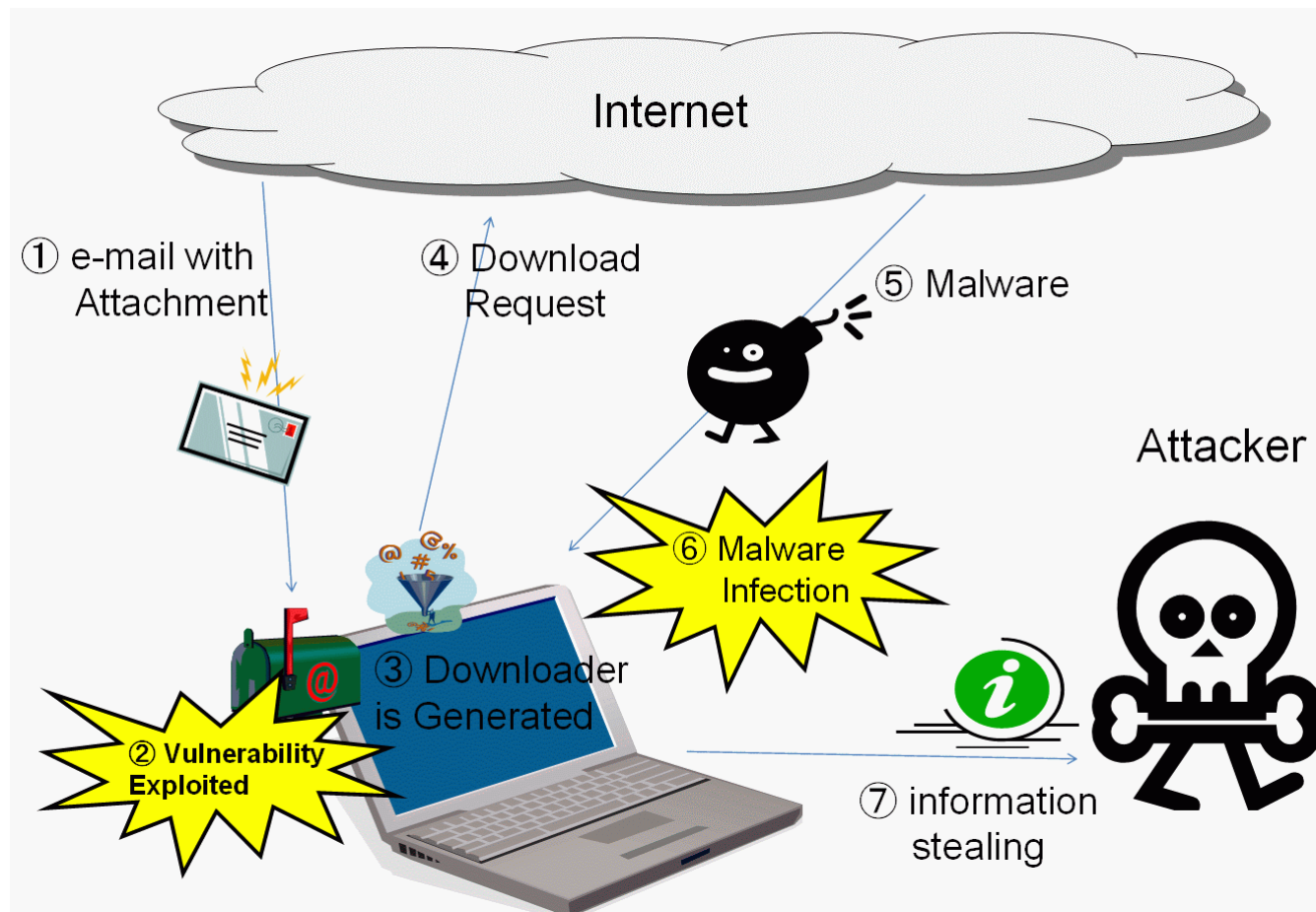
- Exploit for TROJ_MDROPPER doesn't work in our environment due to high environment dependency
- Most part of attacking is advanced, but the exploiting method is poor.



Recent malware for targeted attacks

“Sequential malware” → “Downloader” + “Malware”

TROJ_MDROPPER Series and PPDROP Series



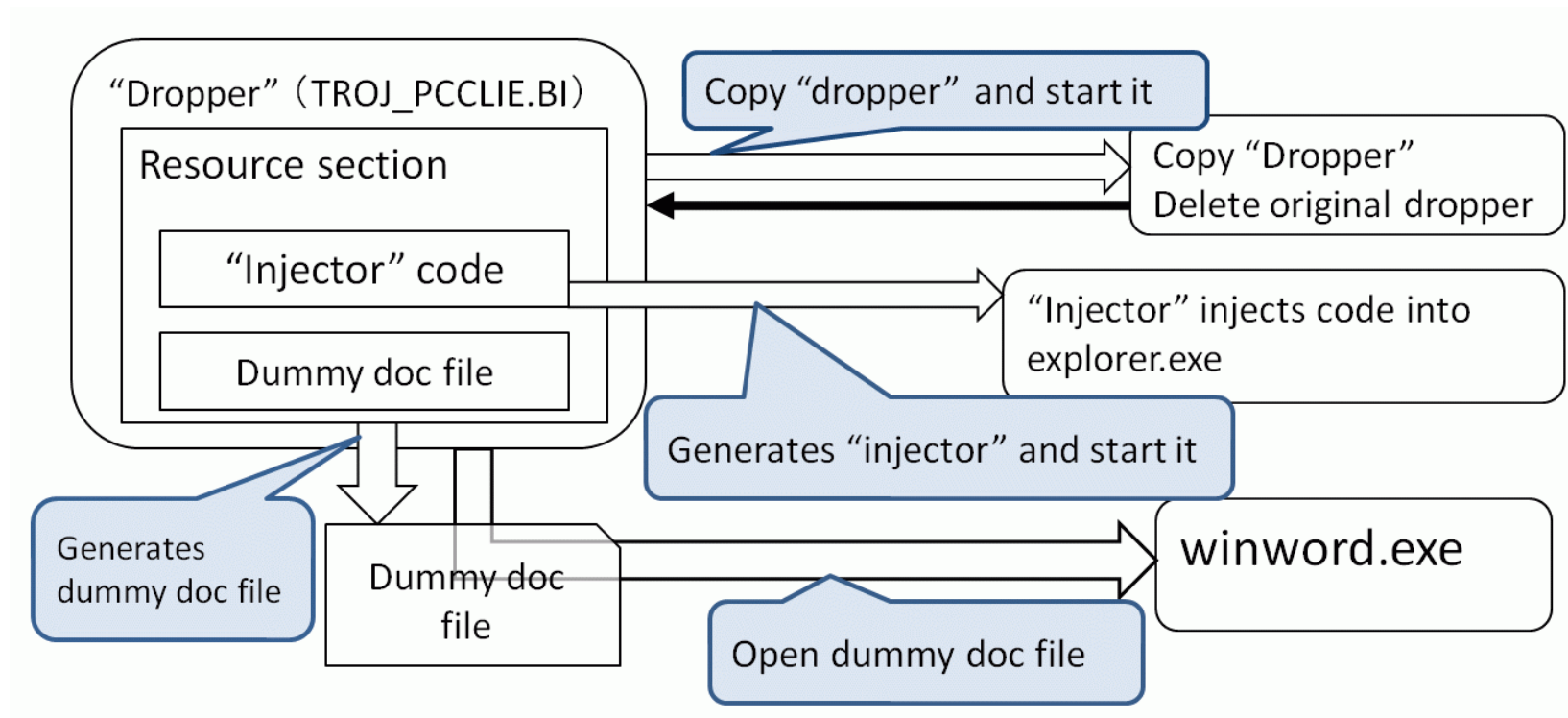
Attacking process of TROJ_PCCLIE



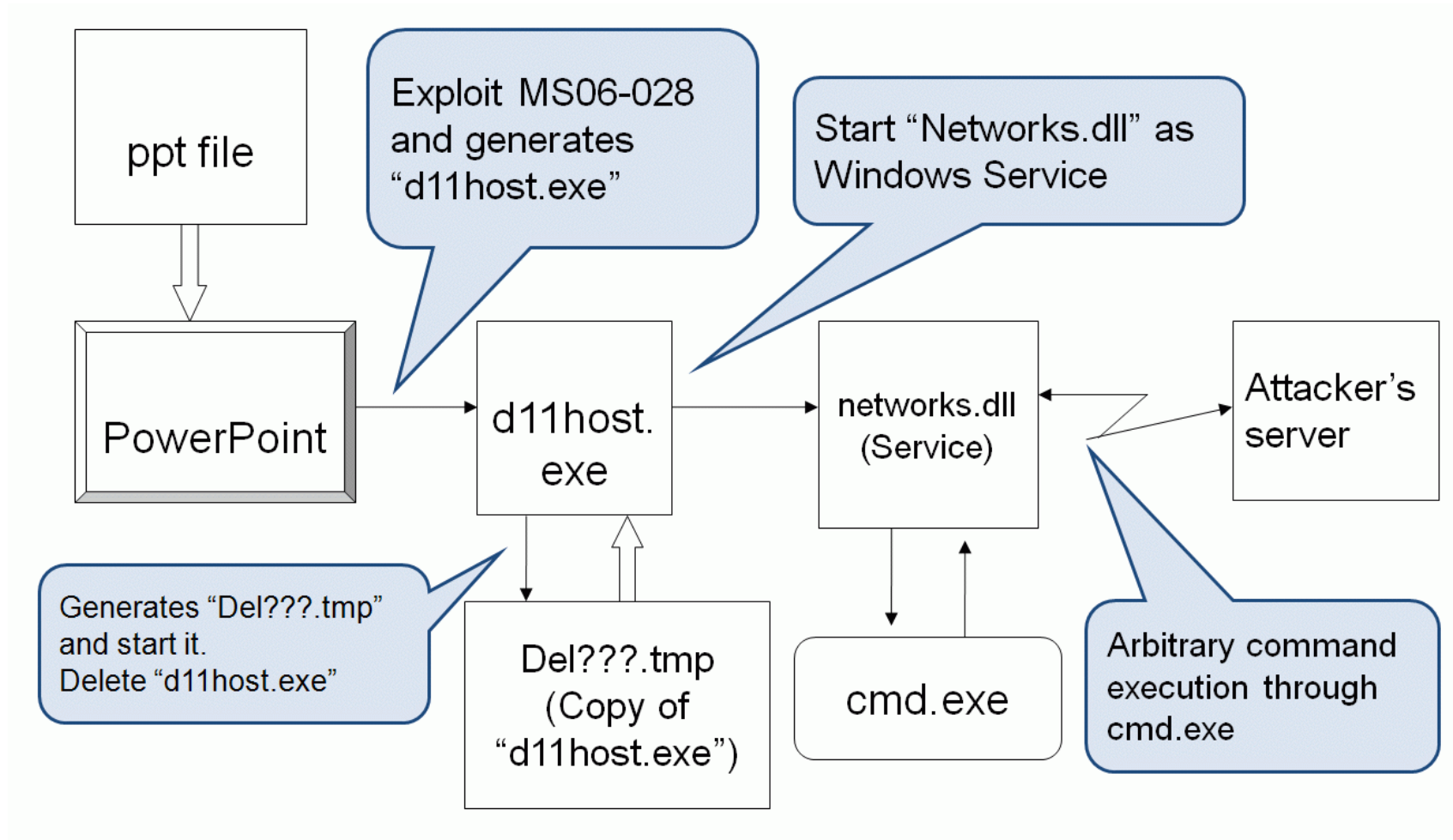
Almost same as TROJ_MDROPPER

Differences :

- Executable file (Icon image is same as MS Word document)
- Generates two executables and a document file.



Attacking process of TROJ_PPDR0P



Servers for TROJ_MDROPPER series



Port 80/TCP(Trasmission Control Protocol) and 443/TCP are used for communication between the malware and attacker's server.

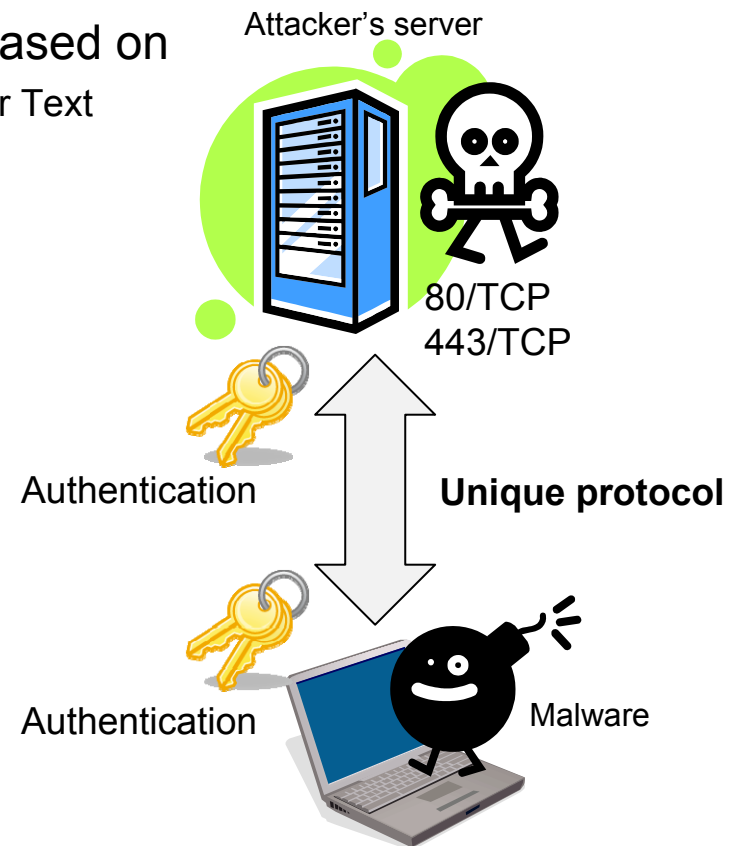
However, the communication protocols are not based on HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol over SSL)

An unique protocol for malware communication



The server is not a web server.

The authentication is implemented in both of malware side and server side.



Problems in automated threat analysis



TROJ_MDROPPER Series

Described as follows in the web page of an Anti-Virus vendor

- (a) Write to the process memory of “explorer.exe”
- (b) Start “iexplorer.exe” and open the backdoor
- (c) Receive the command and send the stolen information



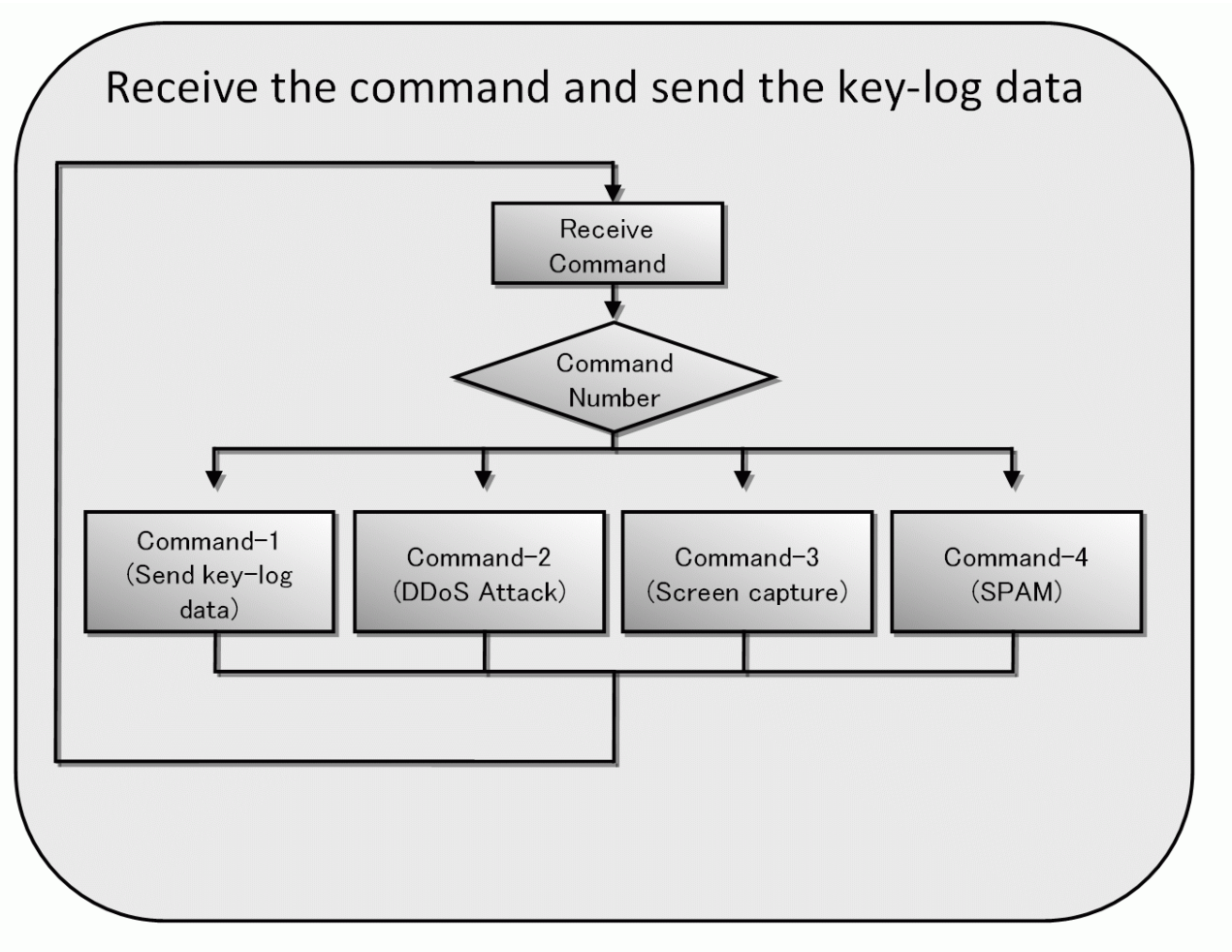
**This analysis said “receive the command”...
but actually, **the backdoor doesn't receive the command.****

The backdoor receives “code”

The downloaded code **may be changed.
Attacker can replace the code on his/her server easily.**

Command and code - 1

Command

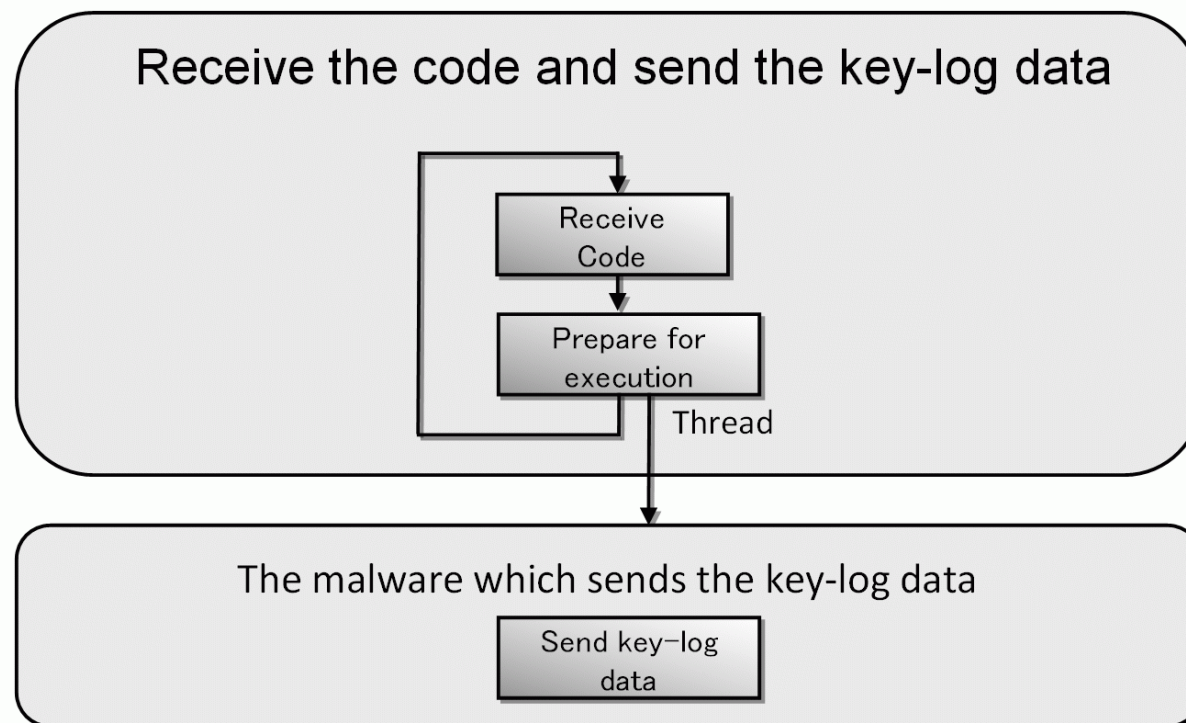


All threats can be listed

Command and code - 2



Code



The code which acts as “malware” is downloaded from internet.

The action of "malware" is **depend on the implementation of "2nd malware" placed on the attacker's server.**

The automated threat analysis method can only show the threat at run time. 25

Code reception is “2nd malware attack” - 1



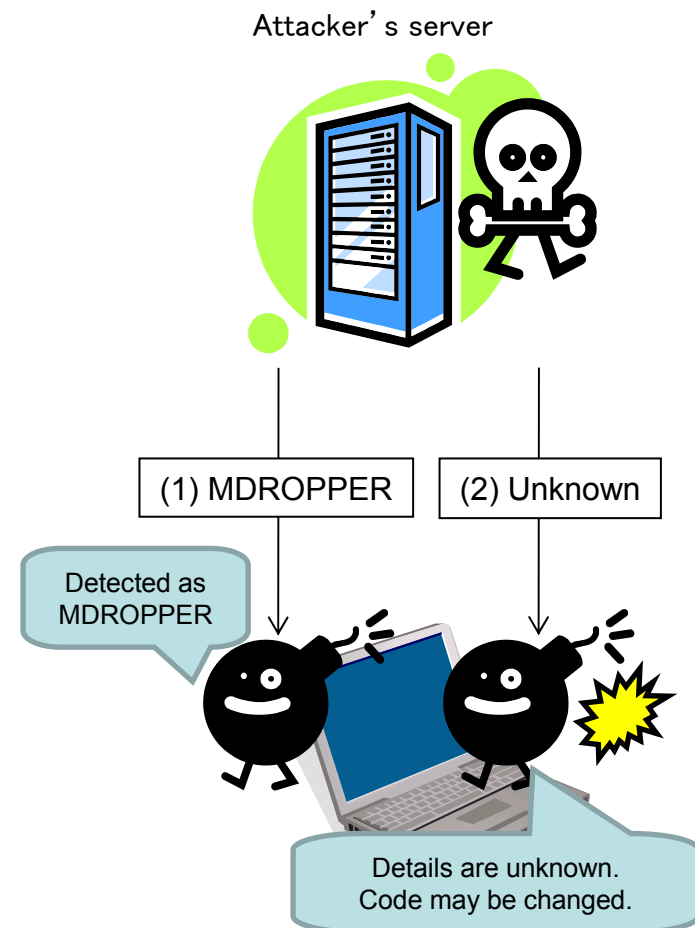
When we analyzed MDropeer, we recognized two blocks of code have been downloaded.

- 1st code - It just downloads 2nd code.
- 2nd code - Send key-log data, host information and user information.



Packet is encrypted.

Automated analysis method can not decrypt the packets and see what kind of information is included.



Code reception is “2nd malware attack” - 2



The downloaded code – “2nd malware” - send information.

Is this one of the action of MDropper ?

"This is the action of 2nd malware, not MDropper"

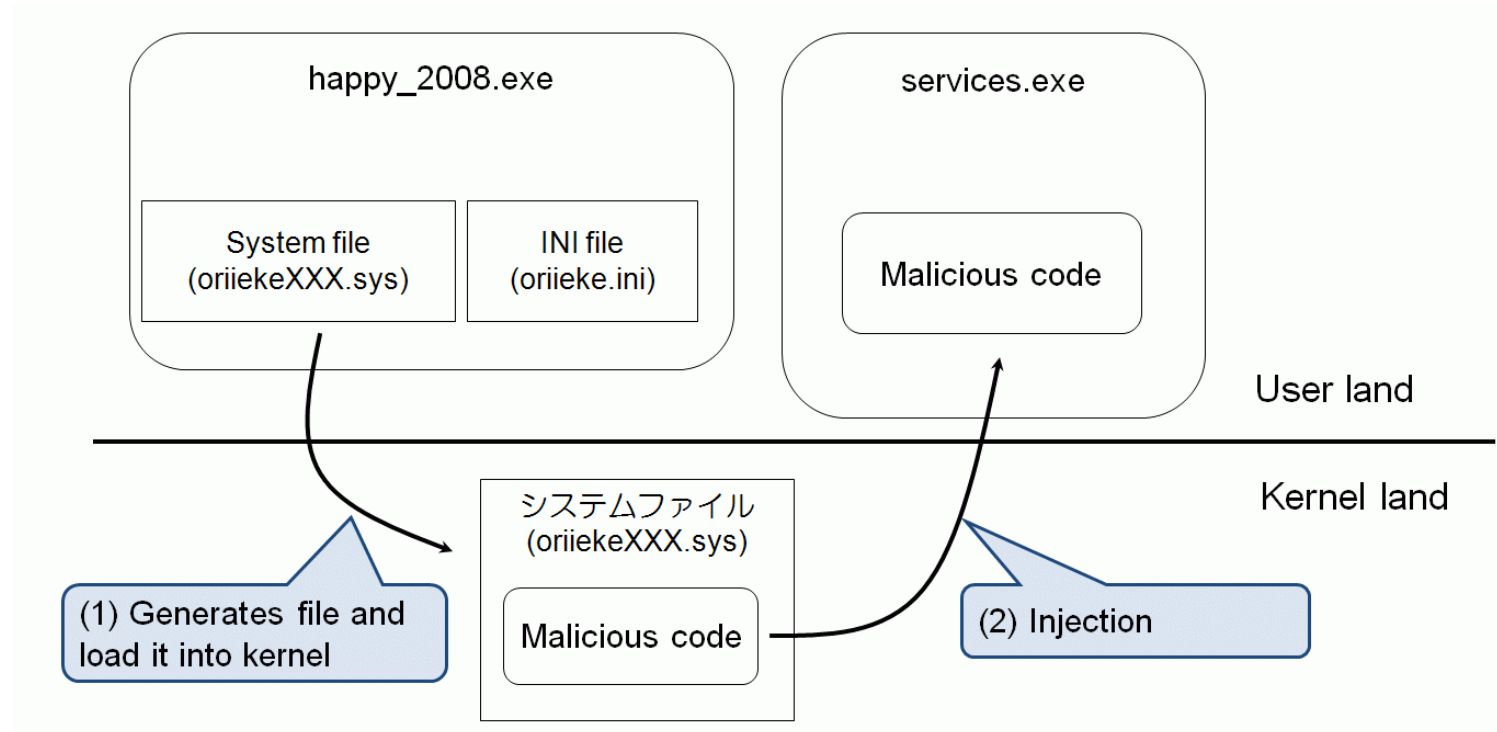
The action of "malware" is depend on the implementation of "2nd malware" placed on the attacker's server.

We can not know what happens even if we analyze the entire code of MDropper.

The incident-response based on the automated threat analysis from Anti-Virus vendor may not be suitable.

Comparison of generic malware

Storm Worm (Peacomm)



Same basic techniques –

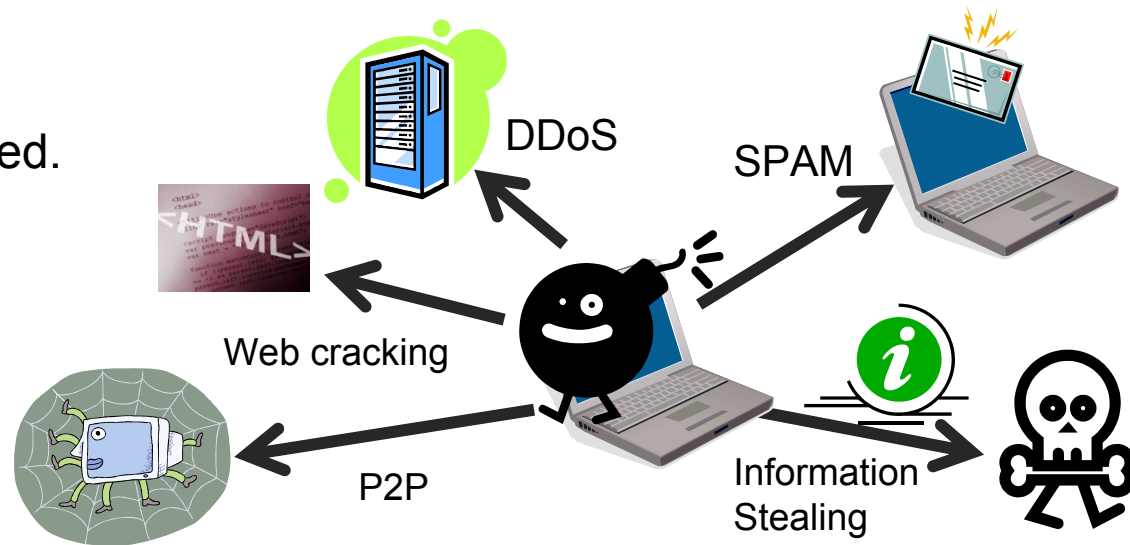
Coed injection, Obsfucation, Anti-forensics, Anti-Debugging, Anti-Disassembling, etc...

Purpose of generic malware and targeted attack malware

Generic malware

Many features are implemented.

- “Fat and multiple functions”



Targeted attack malware

The main purpose is information stealing

- “Slim and specific function”



Efficient threat analysis method



Automated threat analysis method is efficient to know the overview.

Most steps of attacking are just garbages. We don't need detailed information of them.

(Code decoding, Code injection, etc...)

We apply the automated analysis method and find the "point" to start the manual analysis.

Example...

Find the packet reception (calling recv() API)

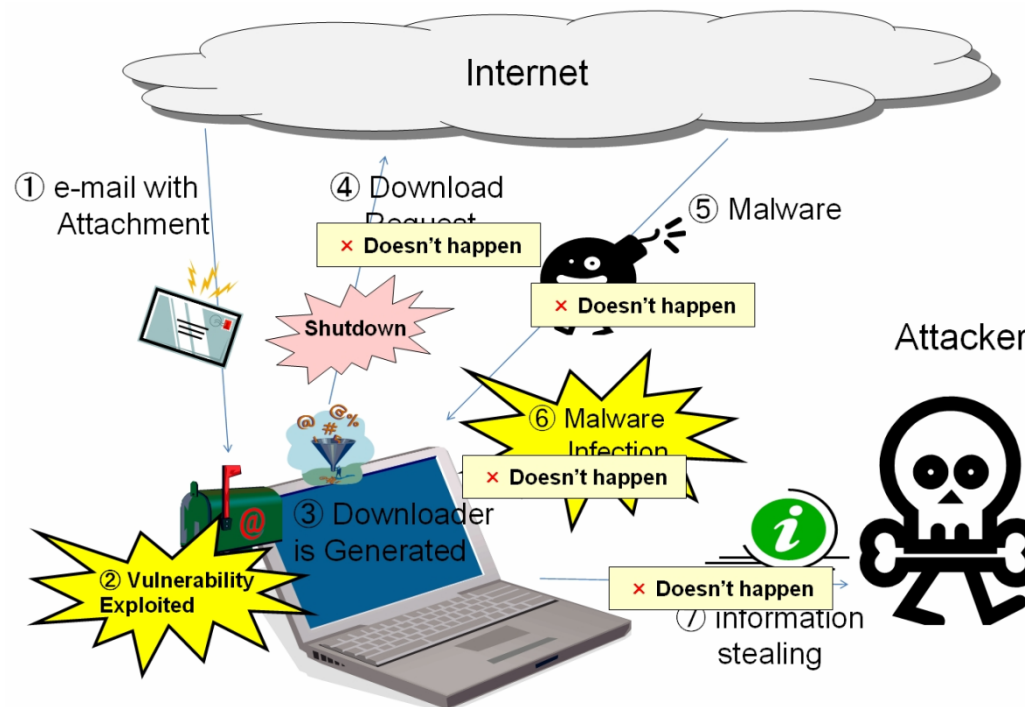
Before packet reception - Automated analysis

After packet reception - Manual analysis

Prevention of targeted attack malware

TROJ_MDROPPER, PCCLIE, TROJ_PPDROP

If we shut down the download request, the actual threat doesn't happen.



1. Close **all outbound unnecessary ports**
2. If the packet which is **not based on HTTP/HTTPS** is detected, we **close the connection**.
3. We use the **web-proxy** to access to the external web server.

Conclusion



Followings make analysis hard

- Multiple code obfuscation
- Own API tables
- Dummy code injection
- Anti-Debugging
- Anti-Reverse engineering
- Multi-thread
- Compressed code
- Code injection to the other processes
- Partial code reception from remote host

Future work

- We could not use IDA on most of entire process (This is painful...)
- We need more "black belt" analyst. The education is necessary.
- We need some "tools" to help quick analysis.
- We must continue to watch the targeted attacks to find better measures.