



**Let your CSIRT do malware analysis,
Recruit-CSIRT has done it!**



Tatsuya Ichida

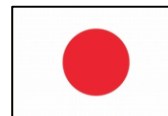
Recruit Technologies, Co. Ltd.



FIRST TC Amsterdam 2017, 25th April

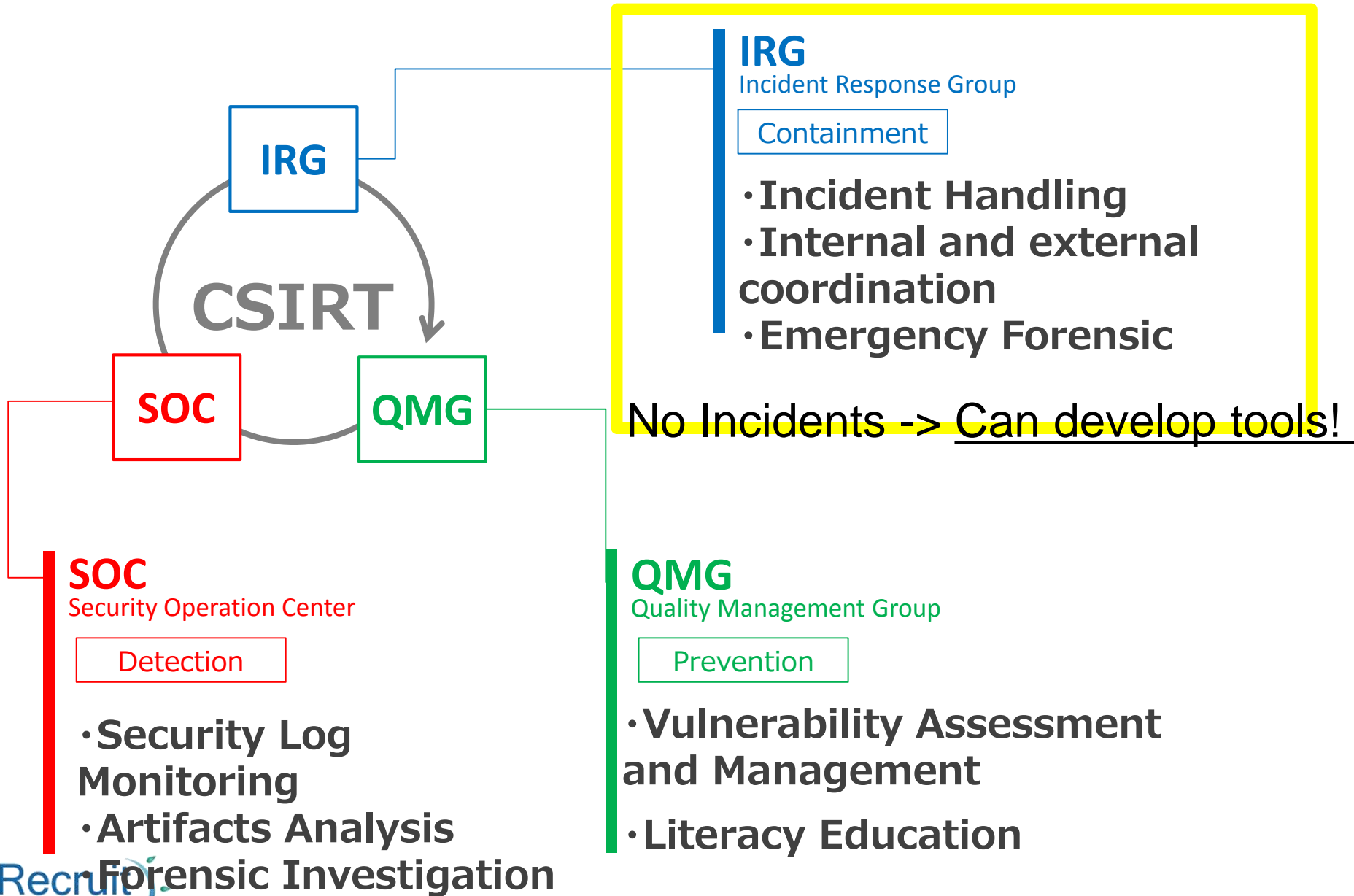
- Self-introduction
- Background and Motivation
- Malware Analysis System for Recruit-CSIRT
- Advantages and Disadvantages
- Conclusion

Tatsuya Ichida (age 29)



Recruit-CSIRT since 2015

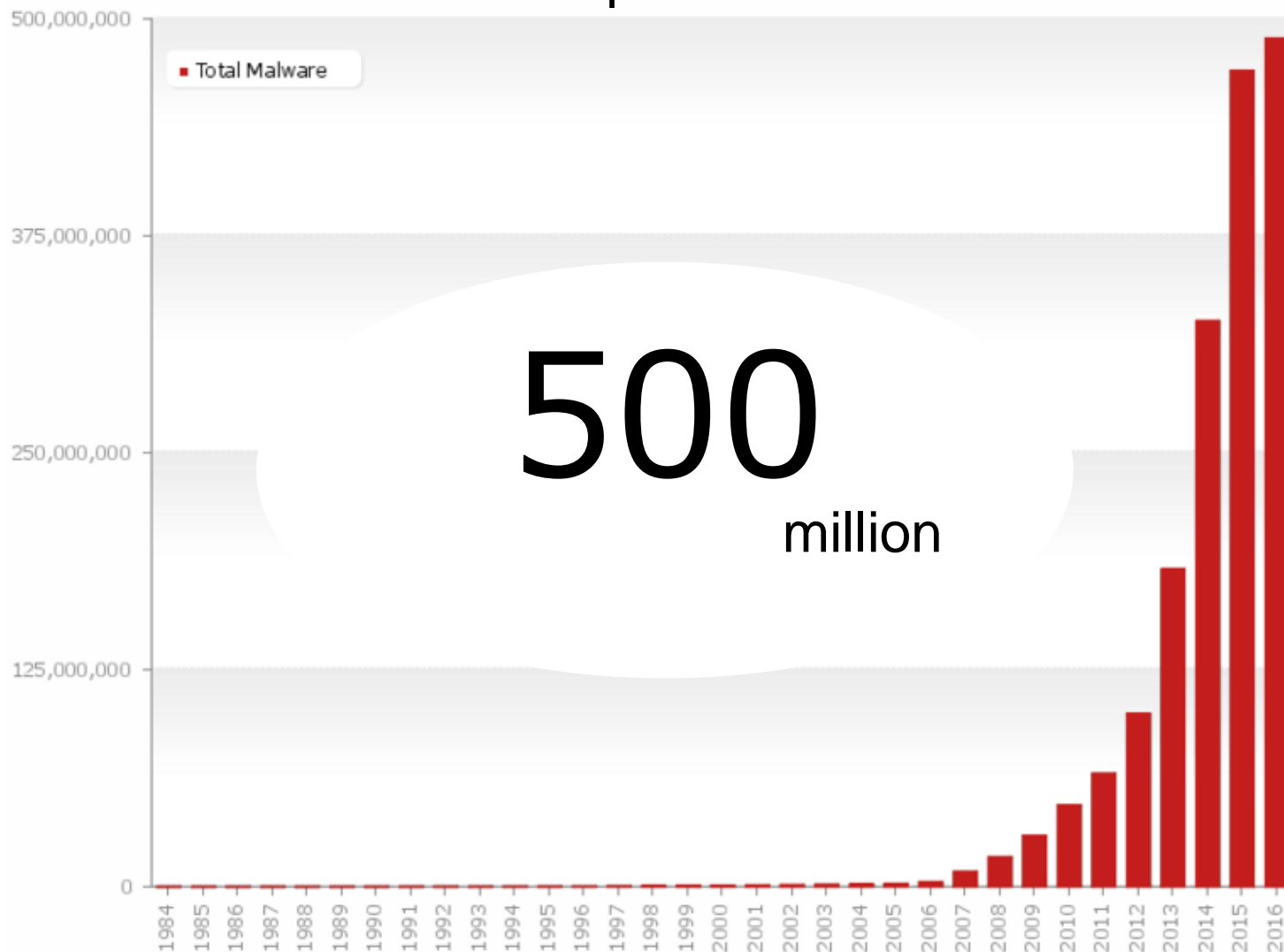
- Security Engineer
 - for developing useful tools
- Incident handler
 - at Recruit-CSIRT
- Loves Malware Analysis
- Splunk Log Analyst
- Tokyo Denki University CySec speaker
- In the past,
 - Security Operation Center, Malware Analysis Leader
- CISSP, GCIH, GPEN





Background and Motivation

Malware explosion in the wild

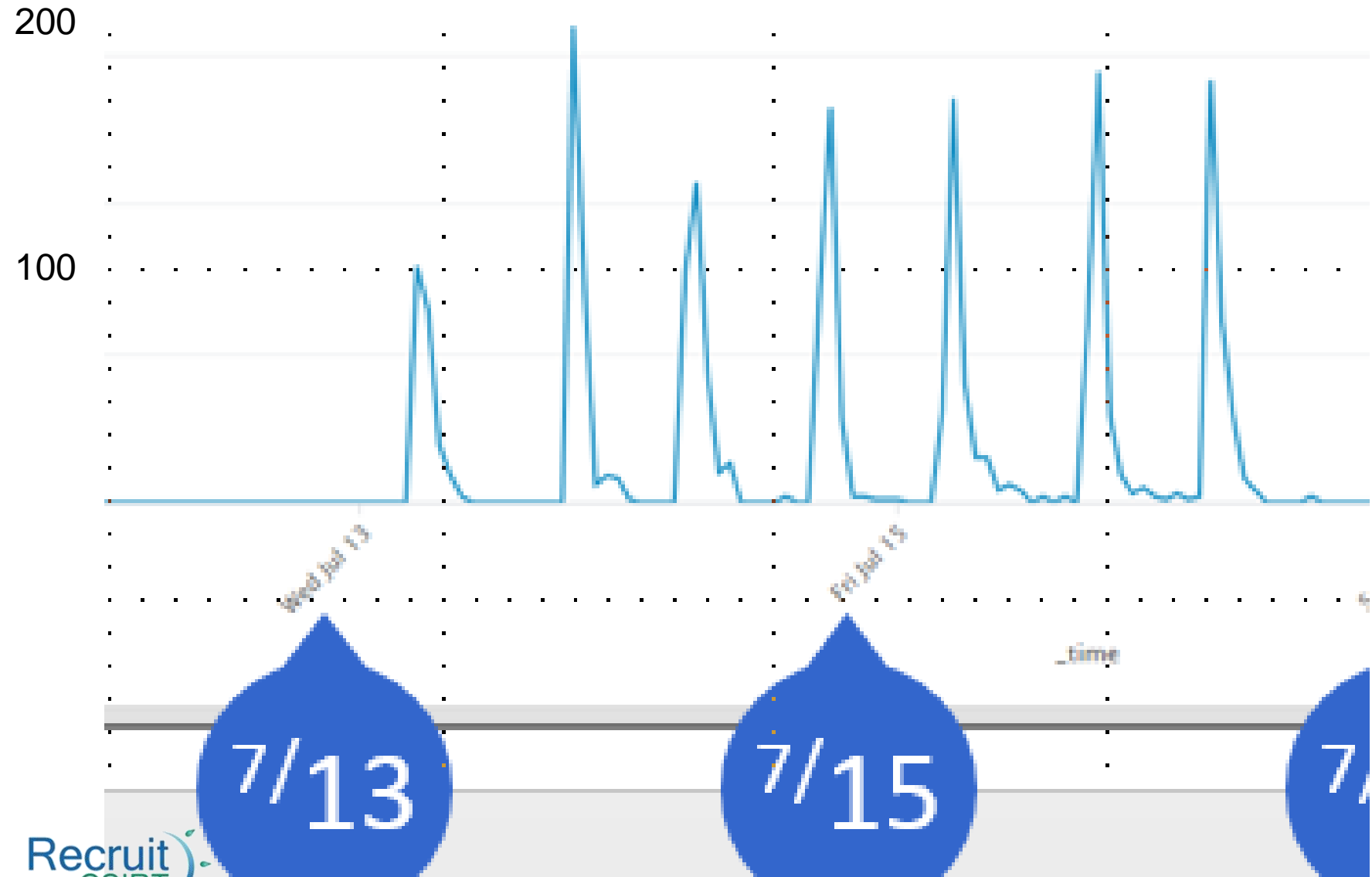


Last update: 02-12-2016 12:39

Copyright © AV-TEST GmbH, www.av-test.org

Ref : <https://www.av-test.org/en/statistics/malware/>

Ransomware explosion in our env



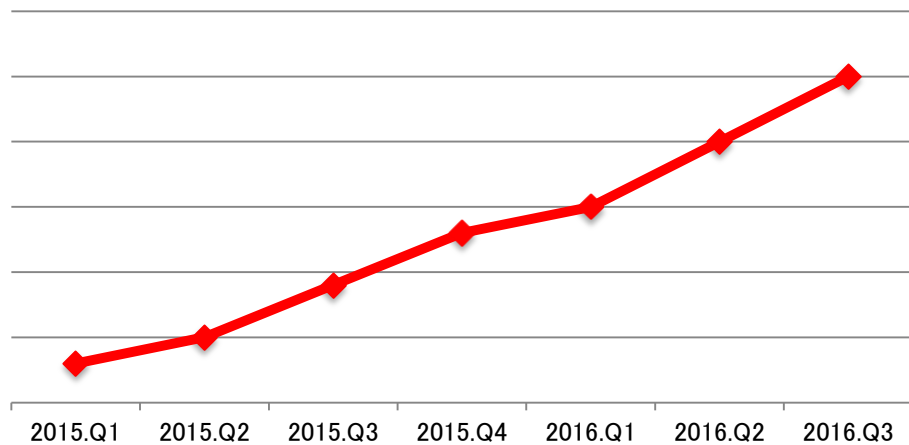
We discovered a malware file over 100MB in size!



100MB

Can it be done Reverse Engineering rapidly? No way!

Work time



FIRST Step

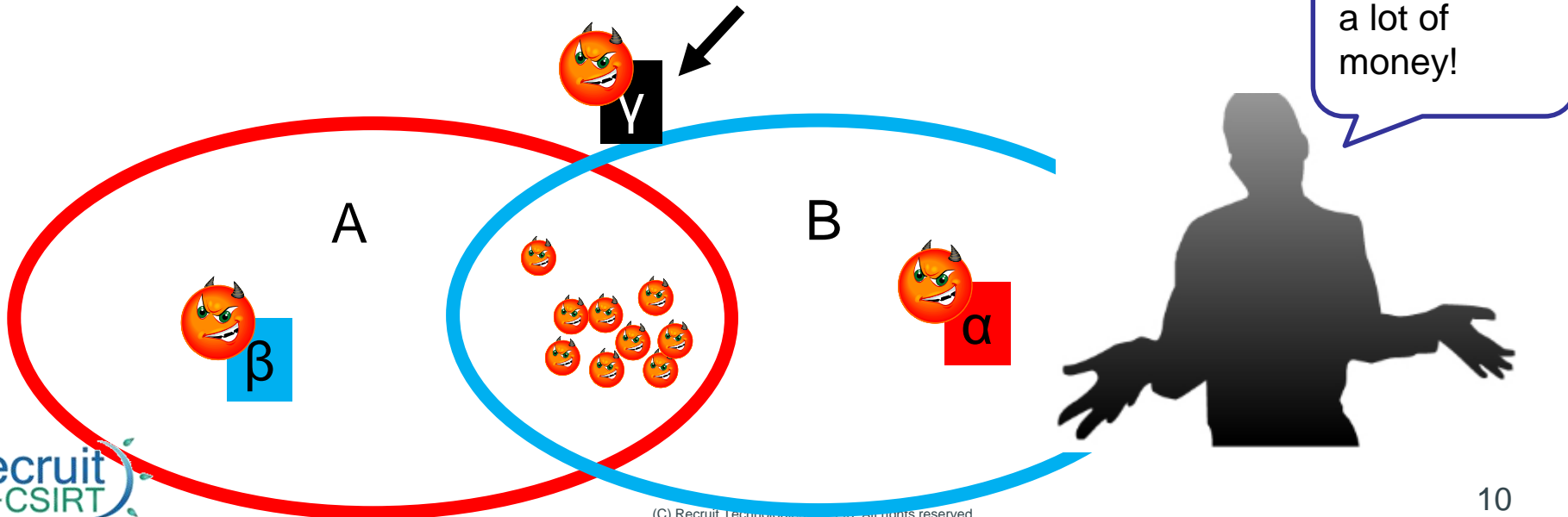
- ✓ Using Commercial Malware Analysis Products.
 - ✓ Sandbox Product A -> Advantage of **Anti-Sandbox**.
 - ✓ Sandbox Product B -> Advantage of **Mal-Signature**.

But .. When We got malware

malware 「 α 」 was not analyzed by A because of the Browser Version.

malware 「 β 」 was not analyzed by B because of Anti-sandbox technique

malware 「 γ 」 was not analyzed by both because of the size !





Let's create our own malware analysis system

Purpose

- Reducing cost
- Reducing user work time
- Stored knowledge internally

It's impossible to create a malware analysis system that can handle all samples perfectly.

government of the people, by the people, for the people
by Lincoln

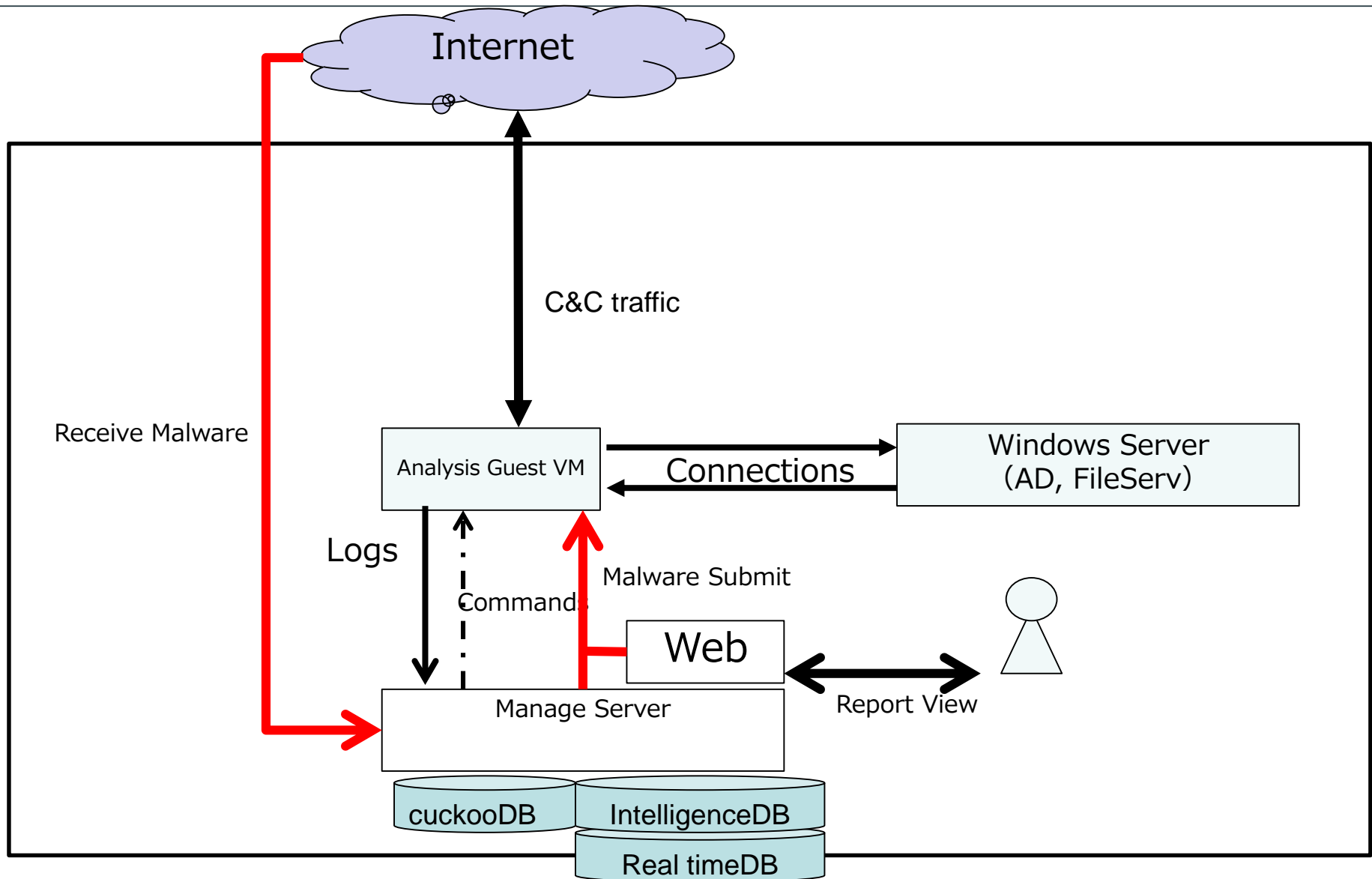


Analysis of our CSIRT, by our CSIRT, for our CSIRT
by Recruit

Our system's target is "our malware"



Malware Analysis System for Recruit-CSIRT



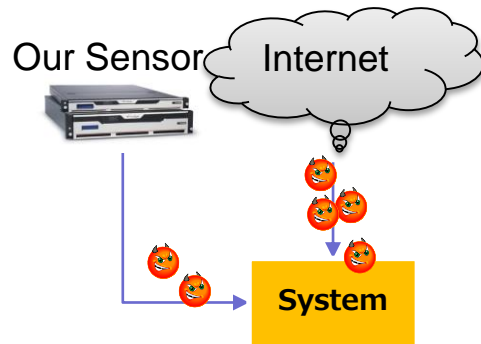
Analysis Scheme

Auto-Collect Malware

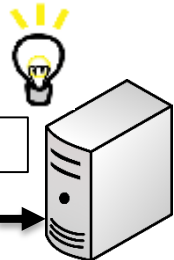
Auto-Optimize Analysis env

Real-time View of Behavior Changes

Post Intelligence



*Image Confidential
In speaking only
you can see*



- From Introduced Malware Detection Sensor
 - Targeted Malware
- From Internet Malware DB
 - Newest Malware before being targeted

- Auto-time Sync
- Over 100MB huge malware analysis
- Auto-Defense against external attacks
- Anti-Virus management

- Auto-log collector
 - Pcap excluding normal
- Real-time Visualization
 - mark behavior changes
 - Intelligence Table
 - Process Behavior Table
 - Packet Traffic Table
- Auto-C&C Server Analysis

- Block The C&C traffic
 - C&C's IP
 - C&C's FQDN



based



based





Advantages and Disadvantages

Advantages

Optimized guest image env

Capable of analyzing huge malware samples

Anti-Virus detection control

Auto-C&C analysis

Real-time visualization

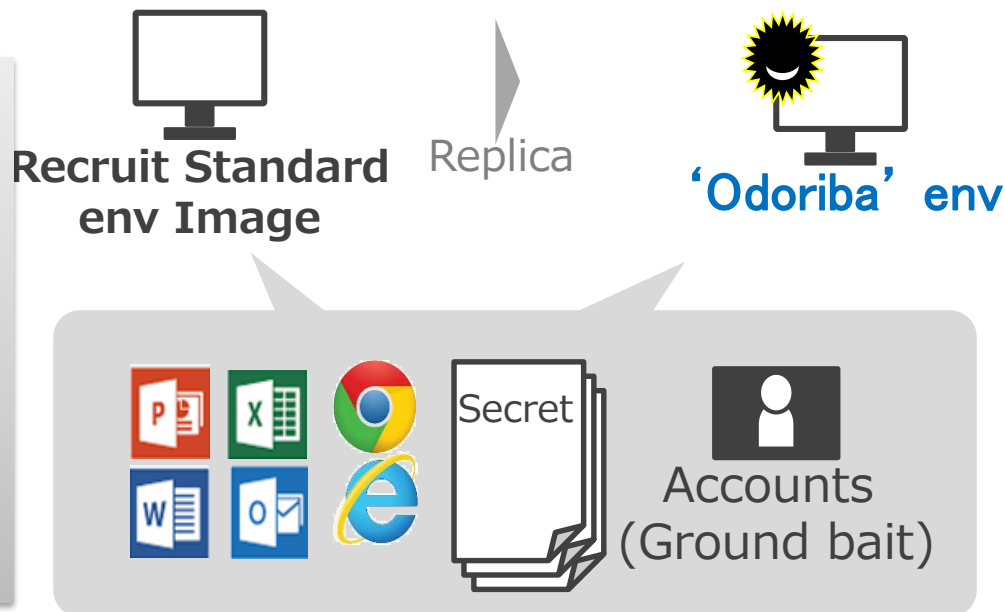
Disadvantages

Cannot handle a lot of malware

No accelerated sleep bypass

Weak to virtual env evasion

*Image Confidential
In speaking only
you can see*



- the Same Image
 - Same Middleware, Same Applications, Same Versions
- Some Ground bait, Mouse Control and Real Date

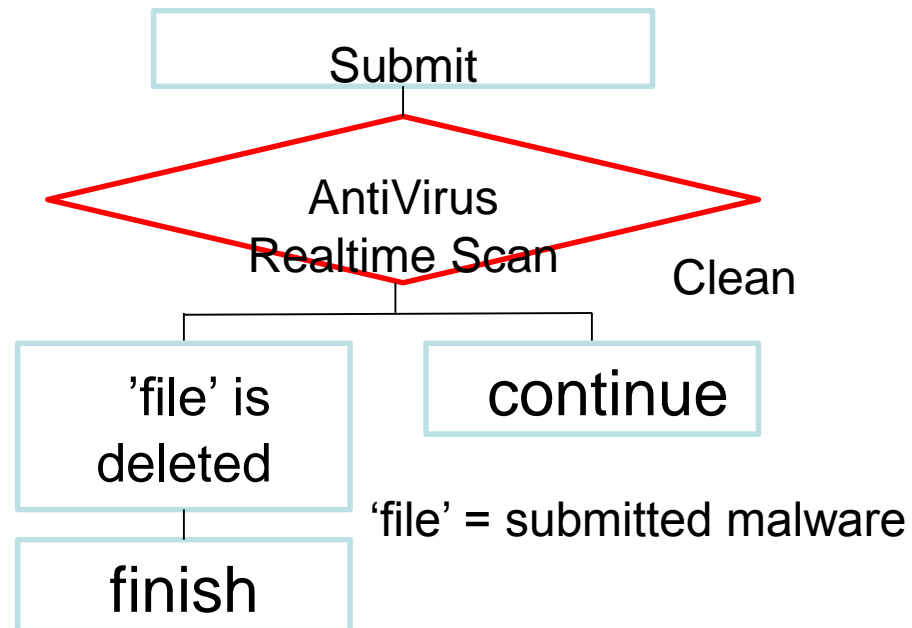
It help us to focus only on **malware infecting our env**



- ***Cuckoo Sandbox 2.0 rc1***
 - Agent Default
 - `/cuckoo/agent/agent.py`
 - XMLRPC based connection to host
 - » Huge malware samples cause memory exceptions
 - » Because of oversize XMLRPC's memory...
 - Manager Default
 - `/cuckoo/lib/cuckoo/core/guest.py`
 - Has two managers
 - OldGuestManager Class(default) and GuestManager Class(for new agent)

- ***We enhanced Cuckoo Sandbox 2.0 rc1***
 - New Agent We added functions to the agent: time-sync, etc.
 - <https://github.com/jbremer/agent/blob/master/agent.py>
 - HTTP based Connection: Agent launches SimpleHTTPServer
 - No limit on Chunk Data to submit
 - Manager uses “GuestManager Class” in guest.py

*Image Confidential
In speaking only
you can see*



Almost Sandbox system -> Antivirus disabled

Usually prevents analysis

Our system permits Antivirus to delete the sample.
We observe while the malware and its child processes exist in our env.

Monitor Traffic

Process behavior (Based on Win API calls)

Certainly malware emits traffic

But it may not include C&C traffic

Rootkit traffic cannot be caught

Pcap (Catch on host)

Include all traffic even from rootkits

Include much normal traffic

Huge volume

Except
Windows and Normal
App traffic

Monthly Update to
“tcpdump exception rule”

Store IntelligenceDB
(IPv4 or FQDN)

Analysis target

Result Update DB

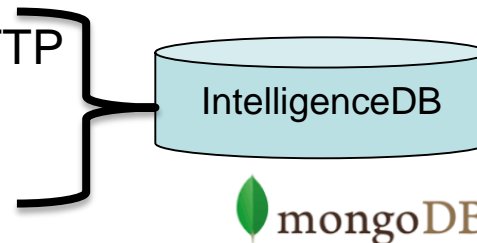
Multi
Thread

— Check whether is on hosting server via HTTP

— Check its whois info from cymru

— Check virustotal reputation

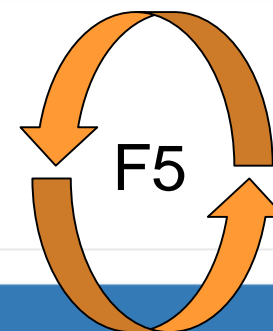
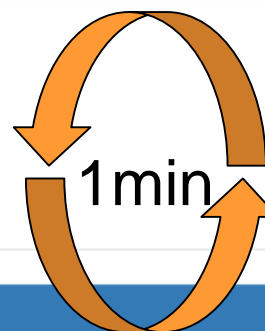
(downloaded malware from)



Default cuckoo report cannot be watched until analysis finished.

Created 'running page' to see the real-time behavior

直近のリロード時刻： 10時40分52秒
リアルタイム解析結果 View (60秒でリロード)
解析終了ボタン
Analysis Finish Button
Files URLs



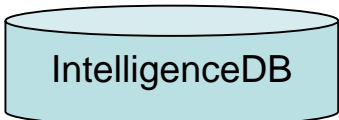
update

| Running Files | | | | | | |
|-----------------|----|--------------------------------------|--------------------|--|----------------------------------|-----------------------------------|
| Intelligence IP | | | | | | |
| C2 IP | CC | Whois | WebAccess Response | WebAccess Title | Virustotal Download malware urls | Virustotal Download malware files |
| 15.11.5 | US | C...ADENET - Cl... .., US | 403 | <title>Direct IP access not allowed Clk...</title> | Not yet | Not yet |
| 2...26 | US | GAN... | 400 | <title>Invalid URL</title> | 0/NULL | None |
| 3...J | US | AK... ..il Tech... ..S | 400 | <title>Invalid URL</title> | None | None |
| 1...71 | AU | EC... ..ings, Inc. d/... .. US | 404 | <title>404 - Not Found</title> | 0/NULL | None |

FILE: 20963.doc

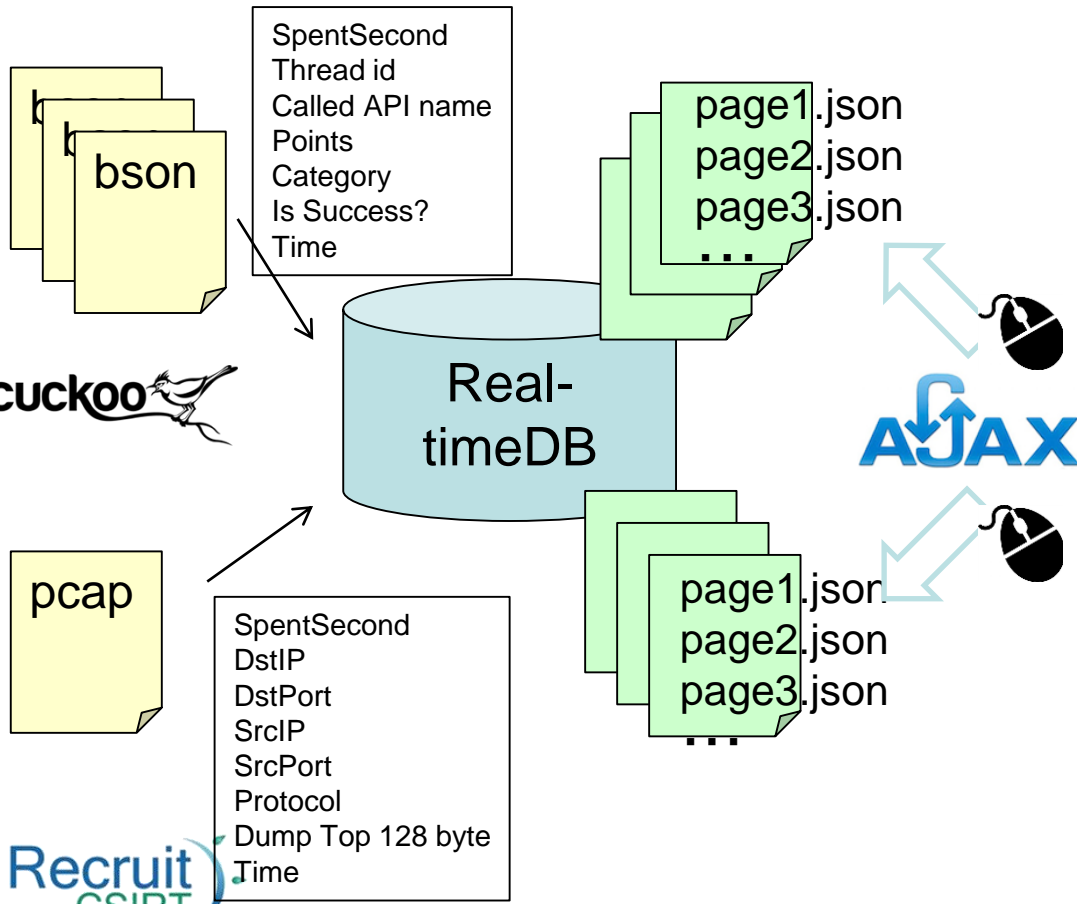
Real-time view tells us the behavior changes ASAP
-> Rapid Block Action & Rapid Re-Analysis

Advantages – 「Real-Time Visualization」 2



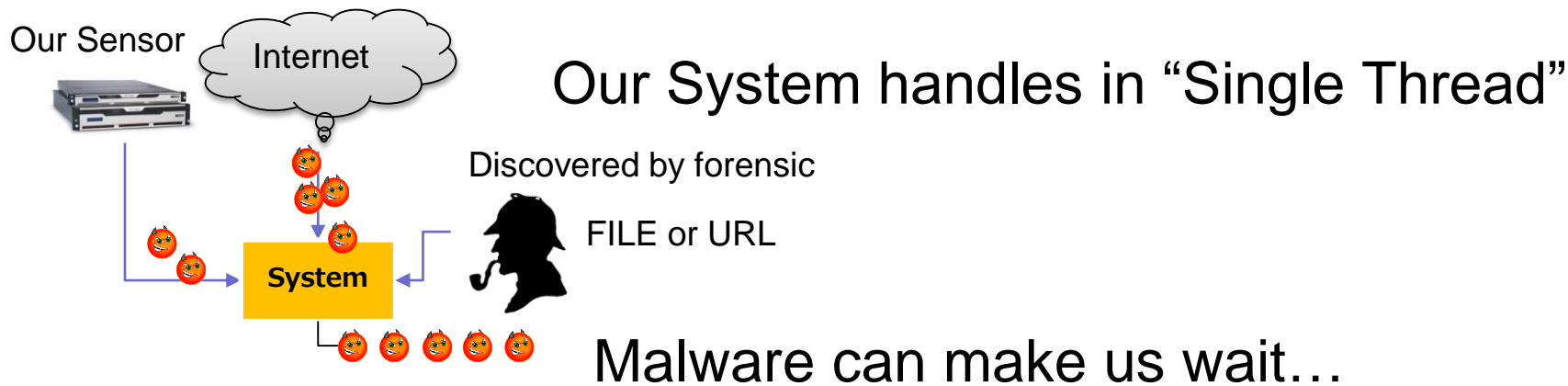
FQDN,IP,WhoisOwner,CC,
WebResponse,WebTitle
VT MalDownloadUrls,
VT MalDownloadFile

| OS IP | CC | Whois | WebResponse | WebAccess Title | WebTotal Download malware url | WebTotal Download malware file |
|--------------|----|--|-------------|--|-------------------------------|--------------------------------|
| 184.43.12.12 | US | QUARK, INCORPORATED - CloudFlare Inc. US | 400 | -the-ghost-of-sleep-at-ahmed-1/Qualification | None | None |
| 203.21.120 | US | AMAZON-031 - US | 100 | -amazon-031/Qualification | CVURL | None |
| 80.7.18.50 | US | AMAZON-49 - Amazon Technologies Inc. US | 400 | -amazon-49/Qualification | None | None |
| 10.16.21.121 | US | 2000CART - MED (Amazon.com Services, Inc.) US - Amazon.com Services, Inc. US - Amazon.com Services, Inc. | 100 | -amazon-2000c-1/Qualification | CVURL | None |



| Spent seconds | Thread id | Called API name | Points | Category | Is Success ? | Time |
|---------------|-----------|---------------------|---------------------------|-----------------|--------------|--------------------|
| 0.3 | 528 | ...proc... | 7715.5861 (challenge1.us) | ...folder... | yes | 2017-04-11 20:1940 |
| 0.30 | 528 | api/type | NA | NA | yes | 2017-04-11 20:1942 |
| 0.30 | 528 | getSystemMalware... | ... | synchronization | yes | 2017-04-11 20:1943 |
| 0.30 | 528 | uploadFile/... | ... | upload | yes | 2017-04-11 20:1943 |
| 0.30 | 528 | uploadFile/... | ... | upload | no | 2017-04-11 20:1943 |

| Spent seconds | DstIP | DstPort | SrcIP | SrcPort | Protocol | Dump Top 128 byte | Time |
|---------------|---------------|---------|---------------|---------|--------------|--|--------------------|
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | HTTP Request | Host: Vmactmpload1... Host: Vmactmpload1... Host: Vmactmpload1... Host: Vmactmpload1... | 2017-04-11 20:2000 |
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | tcp | -body 0 bytes | 2017-04-11 20:2000 |
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | tcp | -body 0 bytes | 2017-04-11 20:2000 |
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | tcp | -body 0 bytes | 2017-04-11 20:2000 |
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | tcp | -body 0 bytes | 2017-04-11 20:2000 |
| 0.0 | 172.16.17.101 | 80 | 172.16.17.101 | 49186 | tcp | -body 0 bytes | 2017-04-11 20:2000 |



Generally, preprocessing seems to be important for this system.

- reducing the input sample
 - (auto) duplicate hash
 - (auto) untargeted extension and file-type
 - (manual) ‘targeted’ or ‘common’ by analyst
- reducing during analysis
 - Handle Anti-Virus detection

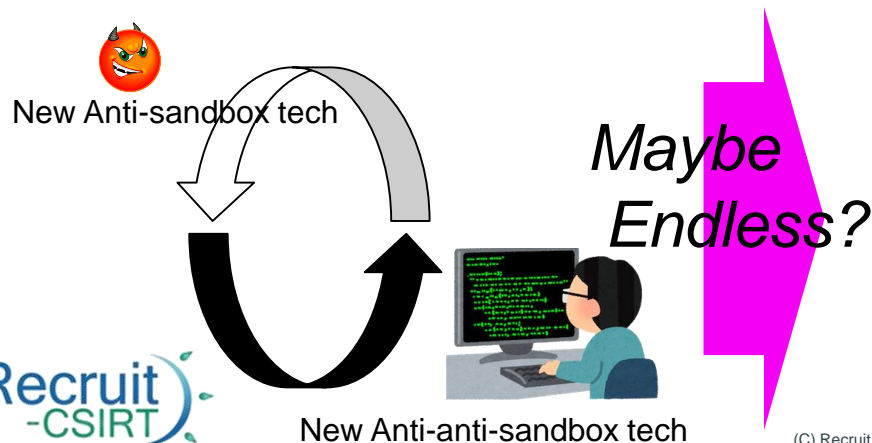
But we

Focus Deeper Analysis
than shallow and efficient

When we catch APT malware through forensic,
We analyze long-term to observe the changes

C&C’s domain, IP
spawn files,
Attacker’s visit etc...

- ❖ Malware often calls ‘Sleep’ to wait for some time
- ❖ Some Sandbox products have functions...
 - ❖ **Accelerated sleep bypass**
 - ❖ In order to analyze the sample efficiently
- ❖ However malware is evolving...
 - ❖ Have Anti-sandbox techniques for this
 - ❖ Ex. CPU Clock difference using GetTickCount etc..



Our human resource is limited.
We don't take this into account.

i.e. **Raw Analysis**

- ✧ Malware often checks **whether** it runs on a virtual machine **or not**, halts its execution in analysis envs.
- ✧ There may be also endless Anti-Sandbox techniques employed.

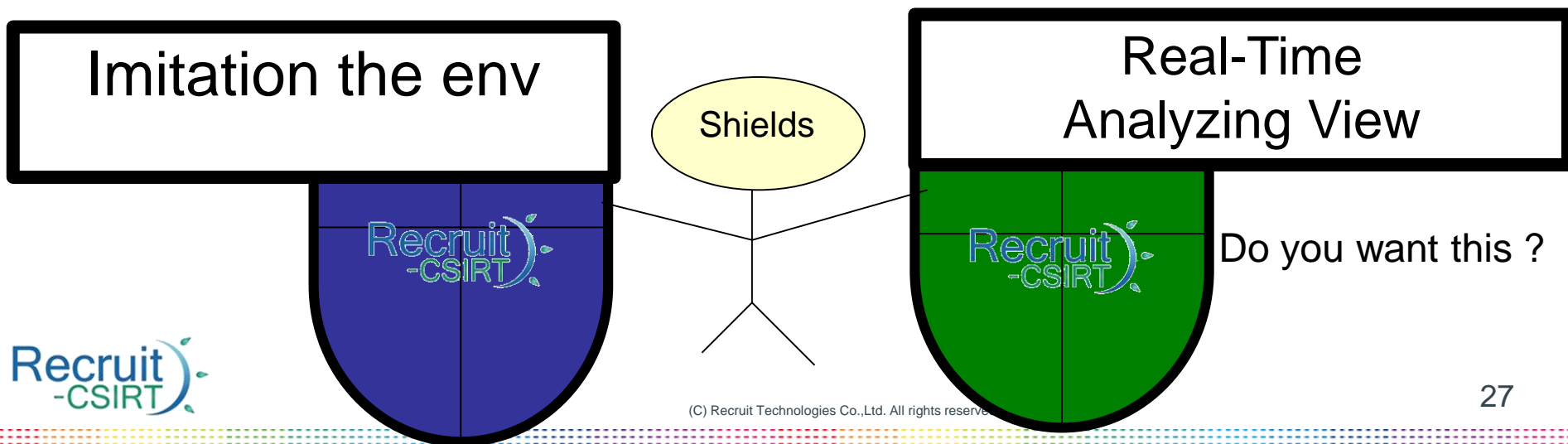
Recruit changed Office PCs to **VDI Thin Client**.
Virtual env = Our env

Some Signature should be removed, **but not all**.
It is important to imitate VDI's Virtual env.



Conclusion

- ✓ Effective for our malware which is affected
- ✓ **Can** be used **flexibly**
 - ✓ Theoretically no limit, since it is developed by ourselves
- ✓ Our System is **not perfect** to analyze all malware.



Thanks to FIRST and OSSs.

