



28 th ANNUAL
FIRST CONFERENCE **SEOUL**
JUNE 12 - 17, 2016



**GETTING TO THE
SOUL OF INCIDENT
RESPONSE**

A blurred night street scene with lights and buildings, creating a sense of motion and depth. The lights are out of focus, creating a bokeh effect. The buildings are also blurred, suggesting a fast-paced environment.

Chasing the operation after the infection of the continuing cyber attacks - Emdivi -

Takahiro Kakumaru, CISSP, NEC Corporation

Hiroki Iwai, Deloitte Touche Tohmatsu LLC

Kenzo Masamoto, Macnica Networks Corp.



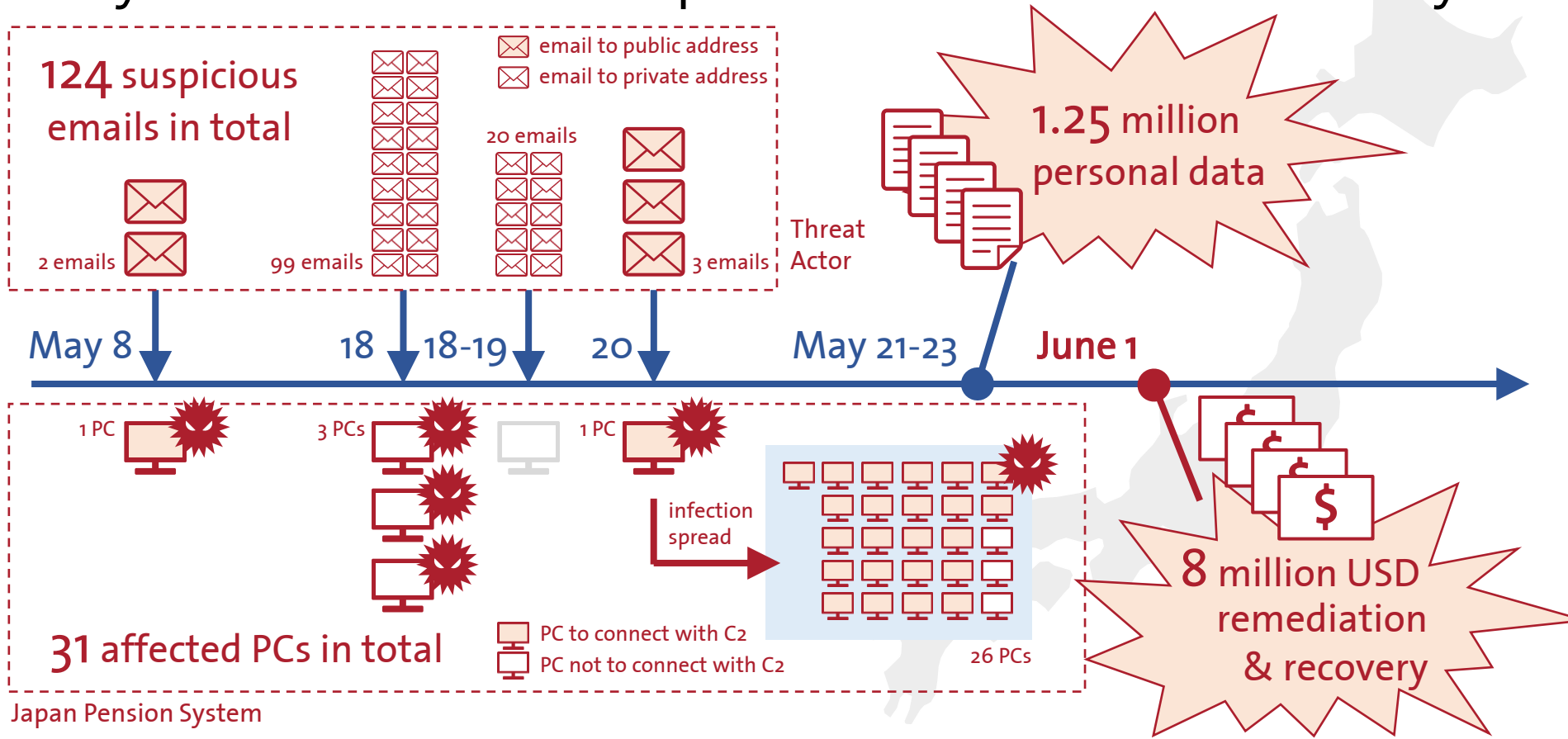
Disclaimer

“The opinions expressed in this presentation and on the following slides are solely those of the presenters and not necessarily those of their employers.”

Hackers Hit Japan Pension System (May, 2015)

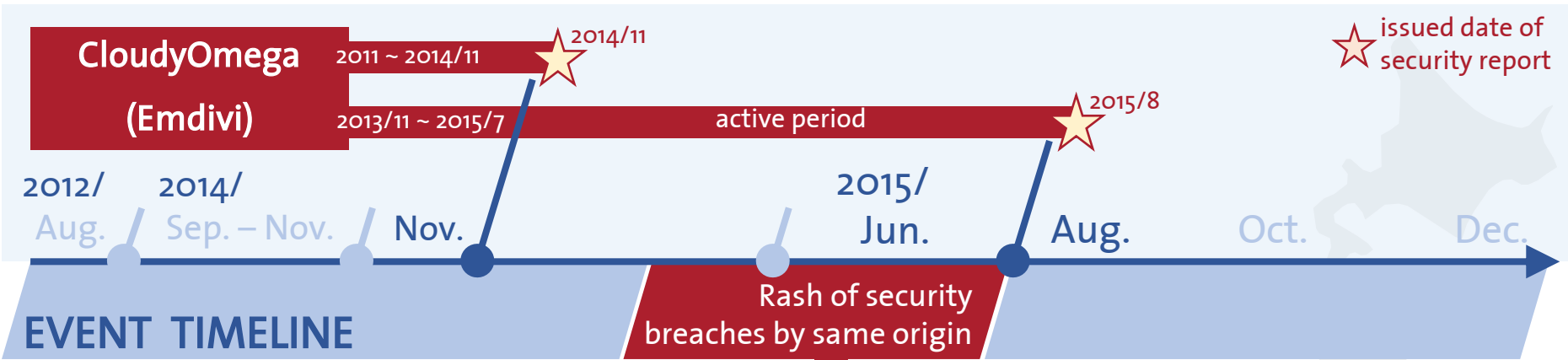
[1] Investigation Report (<https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf>)
 [2] Incident Report (http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf)

- Cyberattacks allowed the personal data to be hacked in May



- “Emdivi” malwares used in targeted attacks against Japan

Incidents reporting lead to suspicion of Emdivi




A series of incident reporting by victim organizations (June, 2015)

(release date)	Incident
2015/6/1	▲ nenkin.go.jp (JPS)
2015/6/9	▲ paj.gr.jp (PAJ)
2015/6/10	▲ tokyo-cci.or.jp (TCCI)
2015/6/13	▲ nihs.go.jp (NIHS), ncnp.go.jp (NCNP), kenporen.com (NFHIS)
2015/6/16	▲ jica.go.jp (JICA), hirosshima-ic.or.jp (HIC), city.ueda.nagano.jp
2015/6/17	▲ jesconet.co.jp (JESCO), kyoukaikenpo.or.jp, hidajapan.or.jp (HIDA)
2015/6/19	▲ med.kagawa-u.ac.jp, ghi.gr.jp
2015/6/22	▲ waseda.jp
2015/6/23	▲ kyu-dent.ac.jp
2015/6/25	▲ moj.go.jp (MOJ)

*All security breaches are supposed to be done by same threat actors

- After major incident was found out, a lot of security breaches had been revealed soon after.

Chasing the Emdivi Operation

1. Introduction
 2. Analysis of the Emdivi Operation
 3. Considerations of the Emdivi Operation
 4. Summary of the Emdivi Operation
- 

What's Our Challenge (and Who Are We?)

- Our goal is not only sharing CTI, but also analyzing collectively.

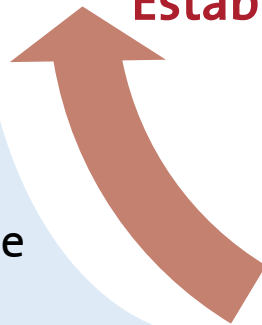
*Cyber Threat Intelligence

Takahiro Kakumaru
Security Researcher
(NEC Corporation)



Hiroki Iwai
Security Researcher
(Deloitte Japan)

**Linking bits of information
Establishing a connection
each other**

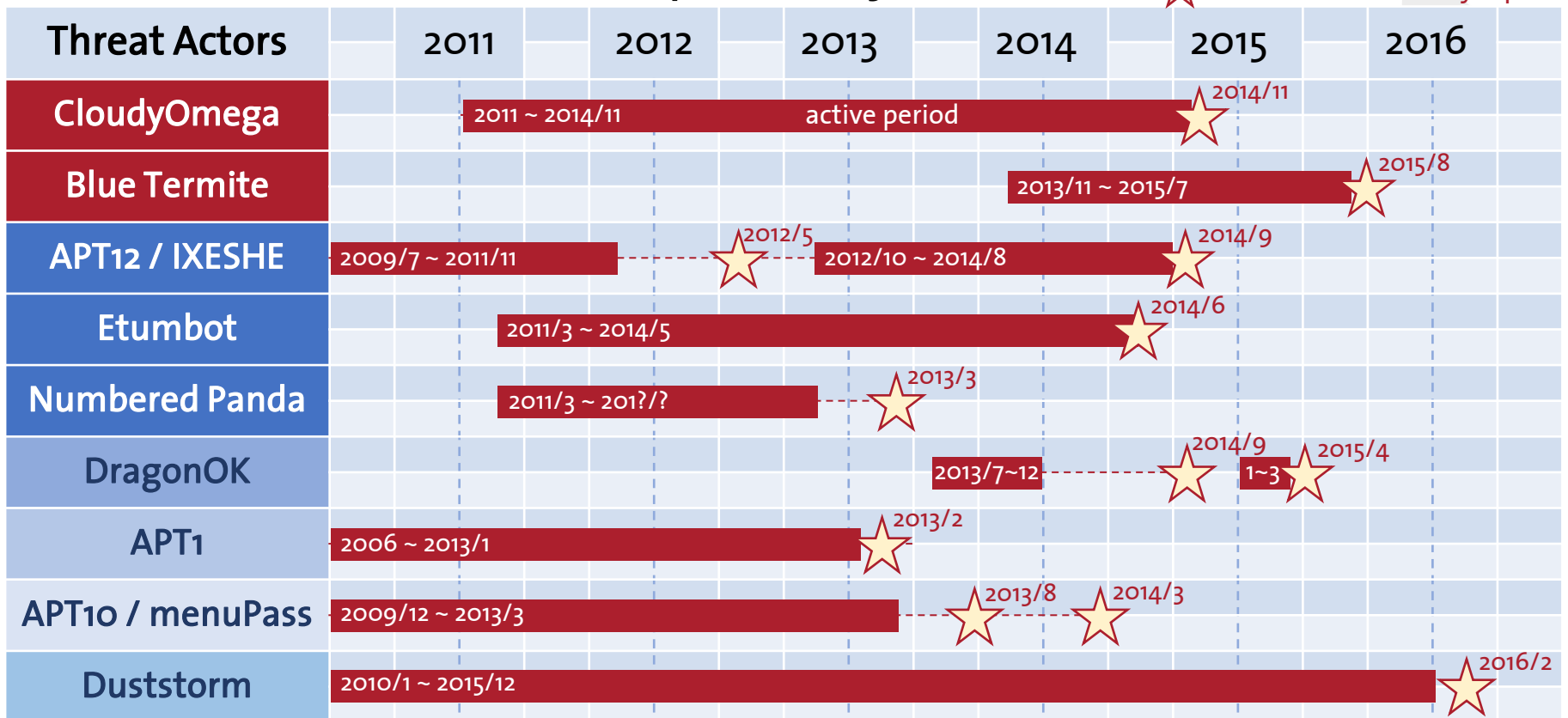


Kenzo Masamoto
Security Researcher
(Macnica Networks Corp.)

- **It's necessary to analyze the things we have with each other, and to understand what is currently going on!**

Cyber Attack Landscape in Japan (2011~present)

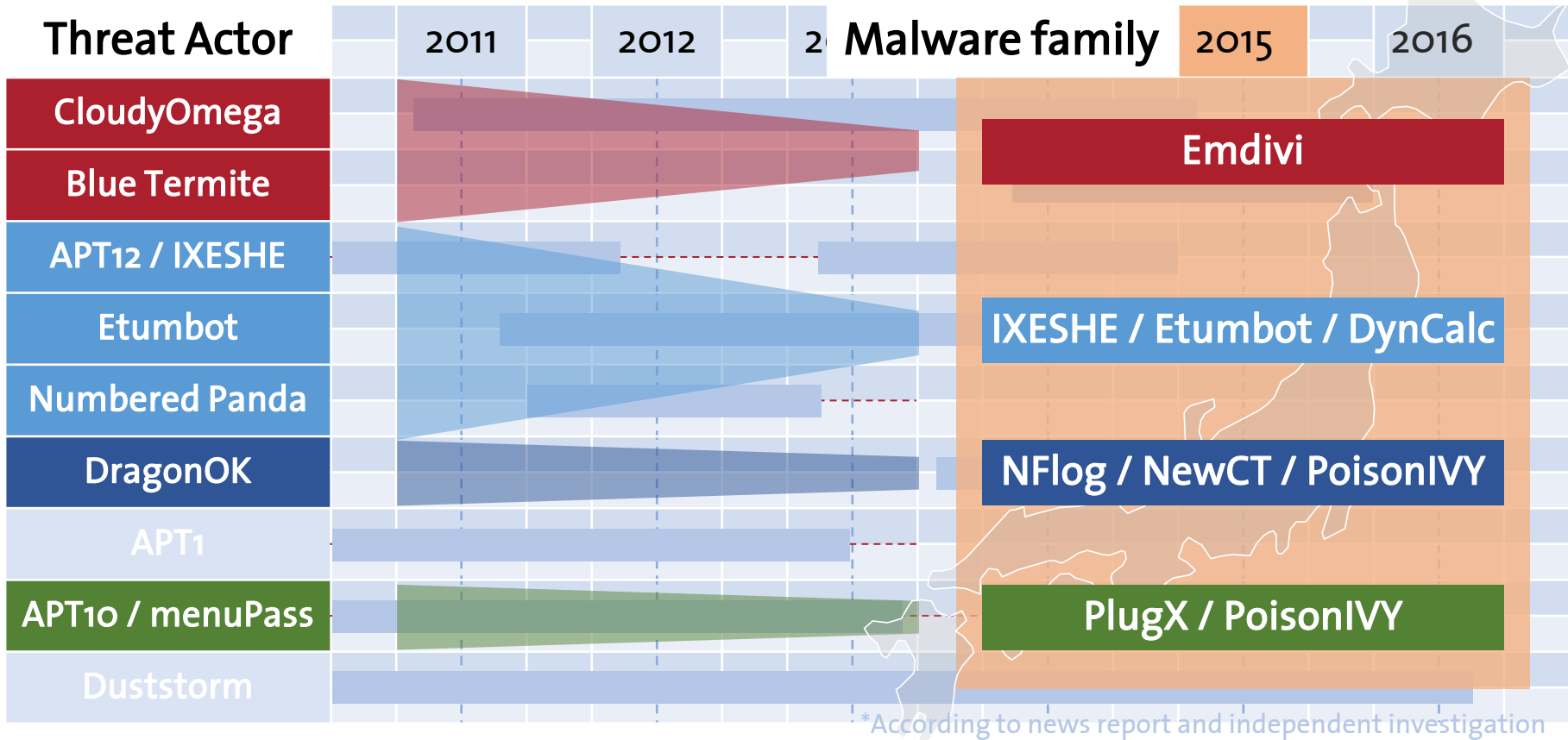
Timeline of threat actors reported by vendors



- It was not until recently that targeted attacks against Japan revealed by the security reports.

Major Cyber Attacks in Japan (2015)

- Relationship between threat actors and malware family



- Let's chase how the threat actors used Emdivi with our findings.

Emdivi is Not Over Yet!?

- Threat actor's behaviors recently

1. Emdivi malware compiled on October, 2015
2. Updated domains used for previous campaign as C2

• globaljihad.org	2016-03-22
• sakuranorei.com	2016-05-10
• tokyo-sakura.com	2016-05-10
• ninjia.org	2016-05-16
• pokemonn.net	2016-04-25

CloudyOmega Group

3. Emdivi C2 connections from Asia (Vietnam, Philippines)

- **We believe the CloudyOmega group has been moving for next phase!!!**

**KEEP
CALM
IT'S
NOT OVER
YET!**

Domain Auction Market

- One of the just updated domain has been lined up!?

tokyo-sakura.com 2016-05-10 updated

Domain auction at GoDaddy

Almost 1 month later...

+ tokyo-sakura.com

(confirmed on 2016-06-12)

新加坡 GoDaddy™ 所有产品 域名 建站 主机 Web 安全 线上营销 优惠券 GoDaddy Pro

域名拍卖 域名拍卖 上架拍卖域名 工具 定价

域名拍卖 tokyo-sakura 搜索 高级搜索

绝对不要错过另一个拍卖
轻松地使您的过期域名脱手而出。
从免费的 GoDaddy 投资者“应用程序”了解和竞价。

立即参加 您已经是拍卖会员了吗? 登录

热门搜索项 要返回的搜索结果
最热门 25

搜索结果

关注	名称	竞价/出价	流量	评估	价格	输入竞价/出价	剩余时间
<input checked="" type="checkbox"/>	tokyo-sakura.com	1	7	-	\$12 *	USD\$ 竞价 \$17 或以上	1D 9H

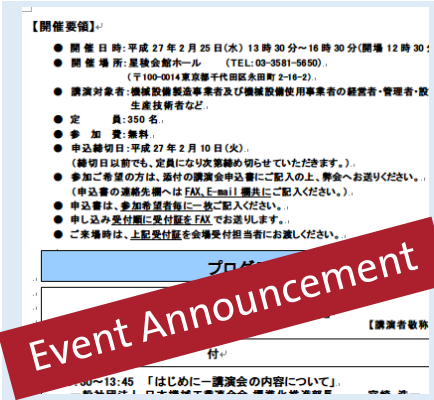
* 若需要，需另加为期一年的域名注册续费及ICANN 费用。

未选中任何拍卖 继续查看

官方时间 — 网页上次更新时间：
2016/06/12 04:35 AM (PDT)

Just the tip of the iceberg

• Targeting sectors have been spread by a number of decoys



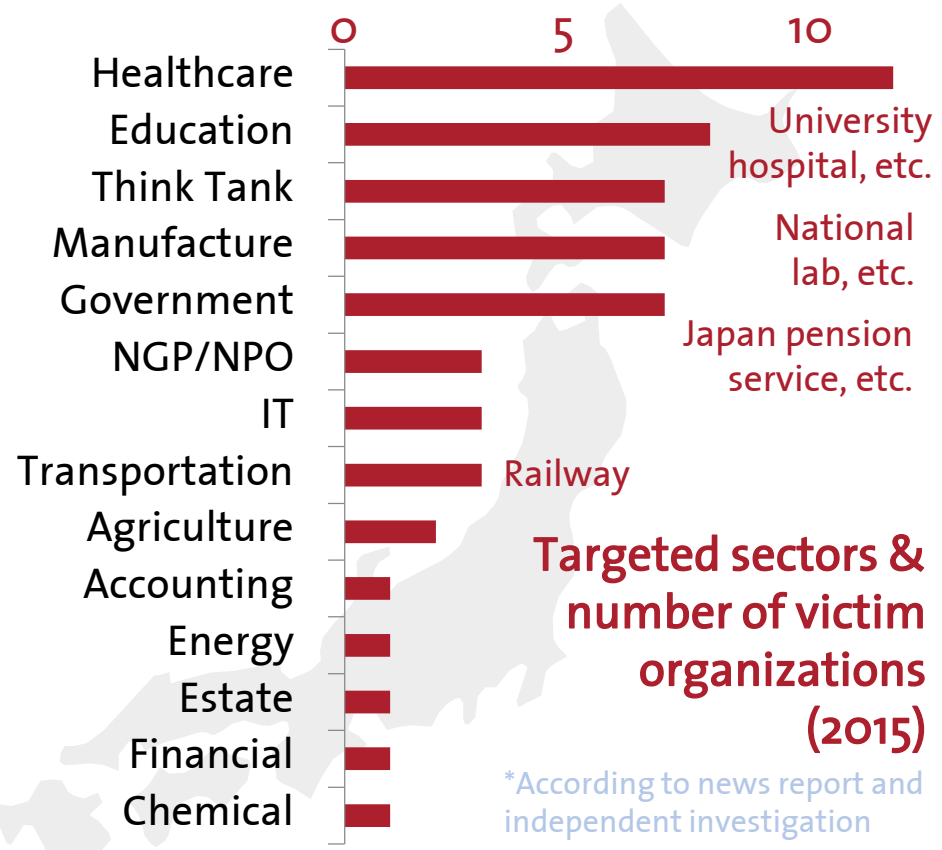
- Highly targeted decoy sample:
particular industry, or organization

- Decoy document:
“event announcement for specific association”



- Less targeted decoy: sample
unspecified industry, or organization, but highly relevant to recipients

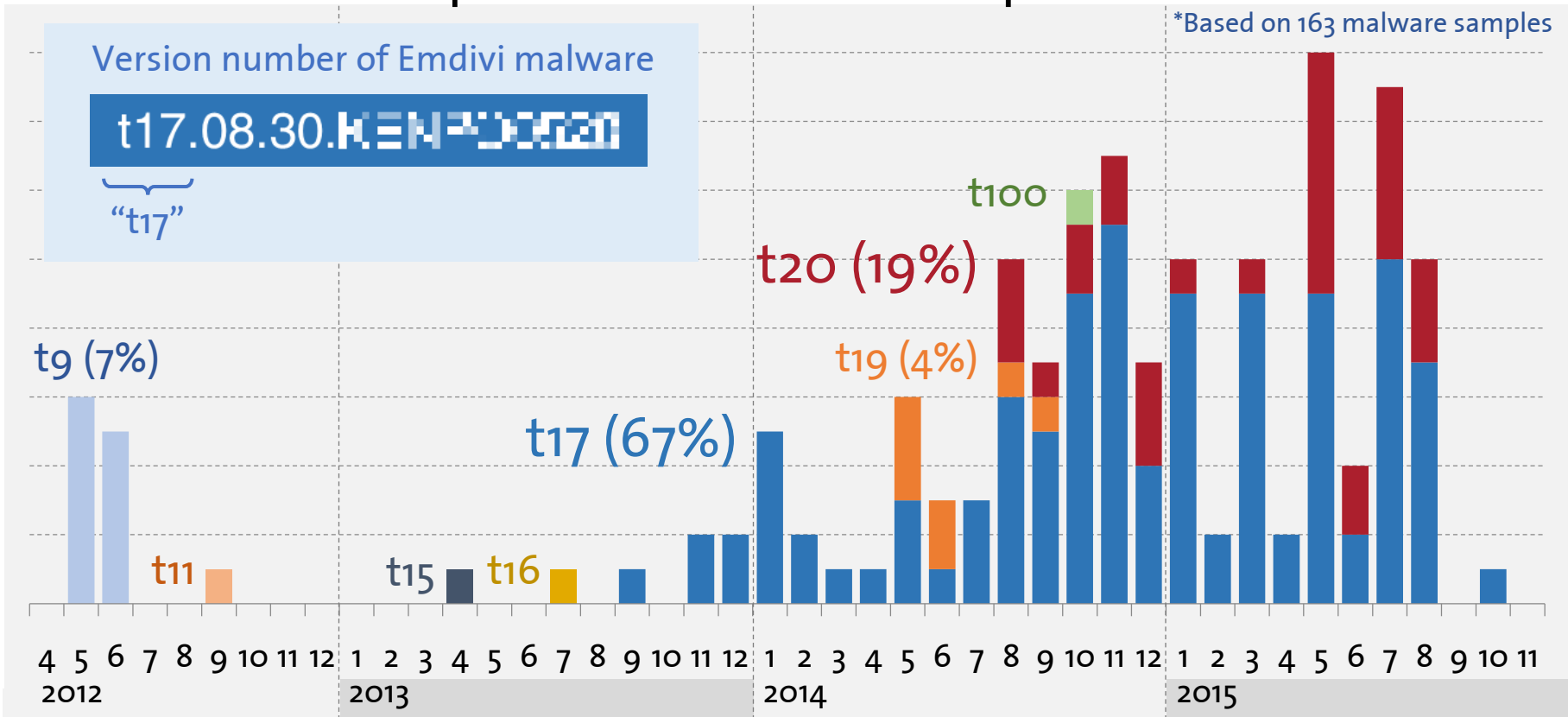
- Decoy document:
“notification of medical expense”



• Massive targeted attack with custom decoy template used for various industries.

Variants of Emdivi Malware

- Timeline of compile time and numbers per malware versions



- t17 and t19/t20 have been used in actual attacks since 2013 for initial compromise and maintain persistence, respectively.

Evolving TTP during attack period

Change history of dropper types

Flash zero-day vulnerability (CVE-2012-5054)

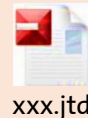
medical payment



Execution program (.exe) with decoy documents

Japanese Word Processor Vulnerability (CVE-2014-7247)

"Ichitaro" document



(.exe) with decoy again...



Watering hole attack with a zero-day vulnerability in its Flash Player (CVE-2015-5119) leaked from Hacking Team

2012/
Aug.

2014/
Sep. – Nov.

Nov.

2015/
Jun.

Aug.

Oct.

Dec.

EVENT TIMELINE

Rash of security breaches by same origin

Updated malware had not been detected by improved evasive techniques

Security breaches

A series of Incident Reporting (JPS, MOJ, etc.)

Security vendors started to update their detection rules

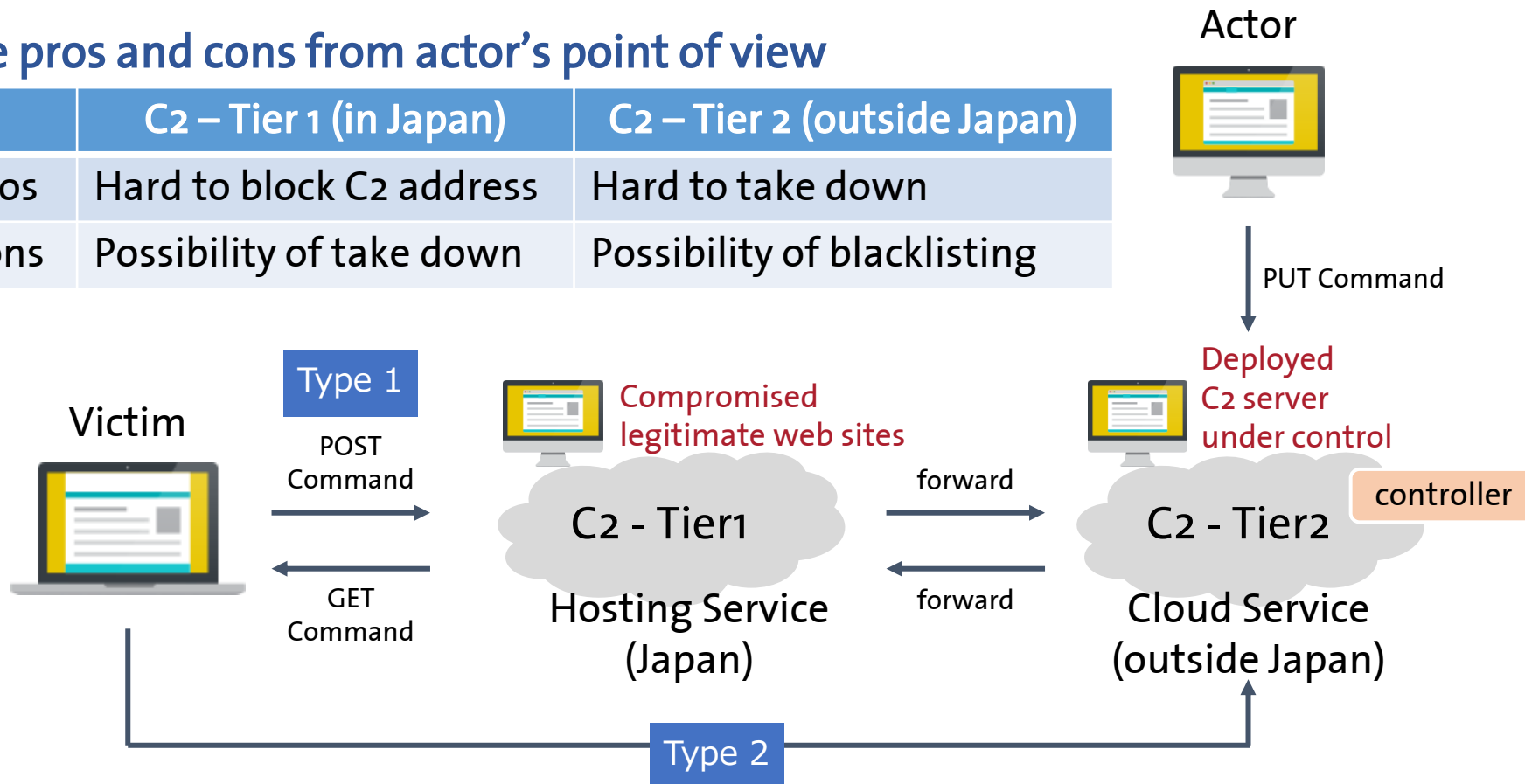
Security breaches has been newly detected at several organizations.

- Threat actors look for new way at all times and adopt it for evasion of detection.

Hybrid architecture of Emdivi C2 infrastructure

The pros and cons from actor's point of view

	C2 – Tier 1 (in Japan)	C2 – Tier 2 (outside Japan)
Pros	Hard to block C2 address	Hard to take down
Cons	Possibility of take down	Possibility of blacklisting

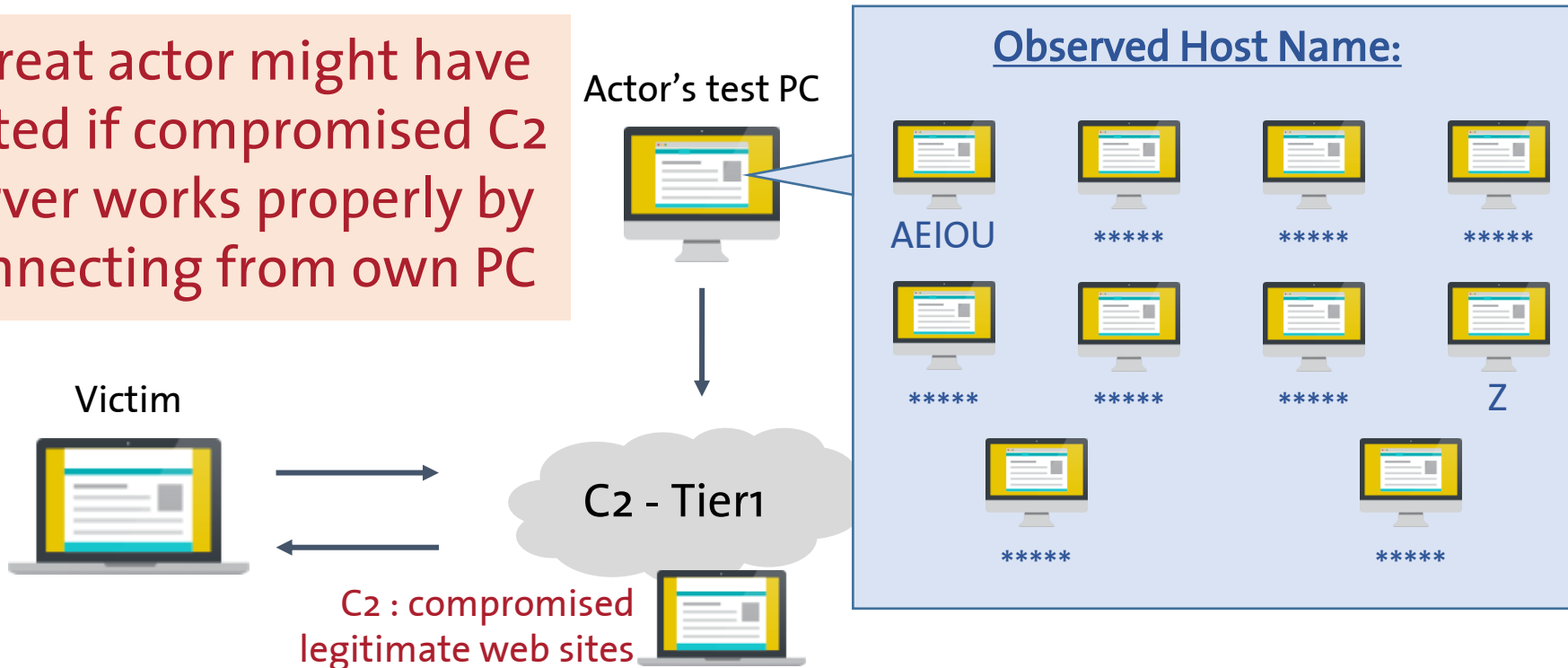


- Hybrid architecture brings certain advantages to keep C2 infrastructure over long periods of time

Threat Actor Attribution (Location)

- Where most of threat actors are involved in operation?

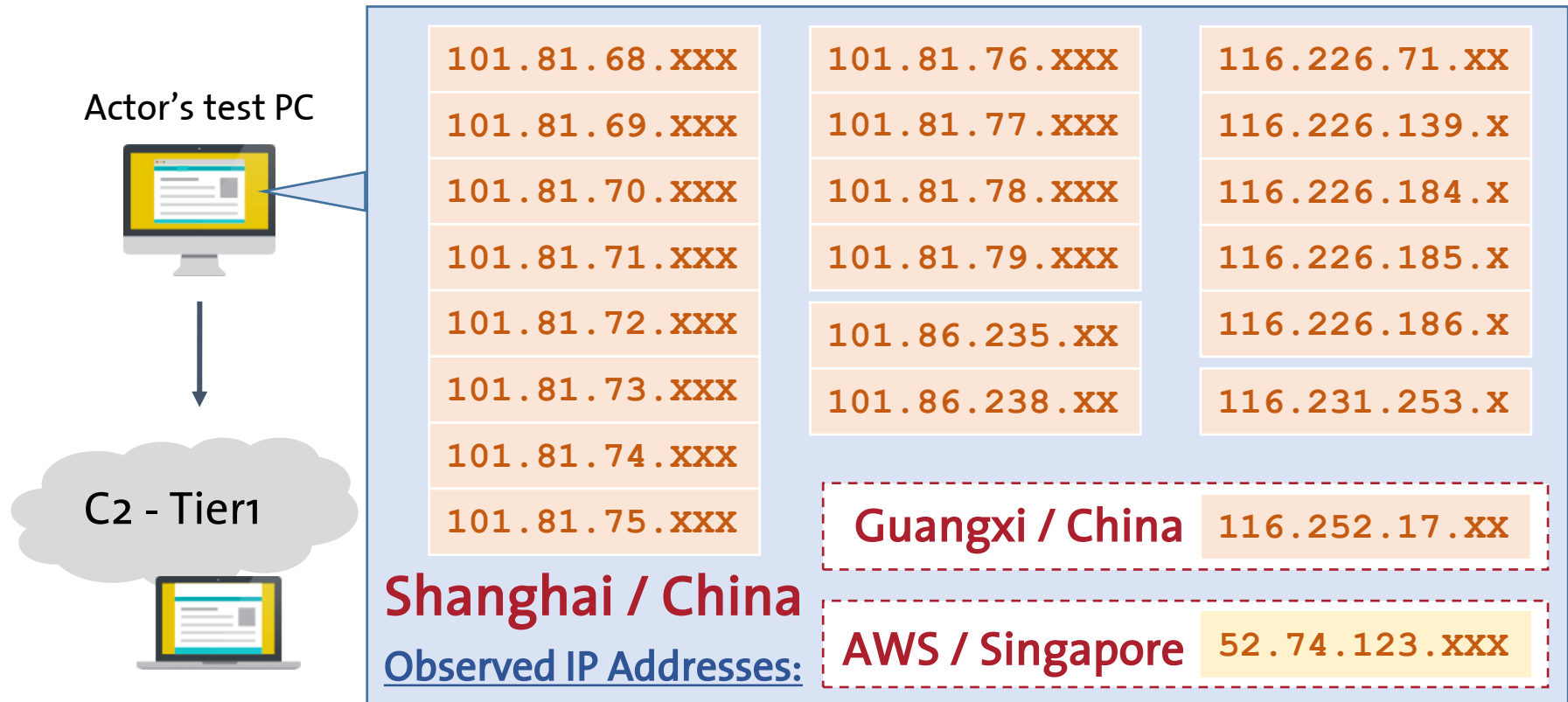
Threat actor might have tested if compromised C2 server works properly by connecting from own PC



- Attack campaign had been achieved by at least 10 computers.

Threat Actor Attribution (Location)

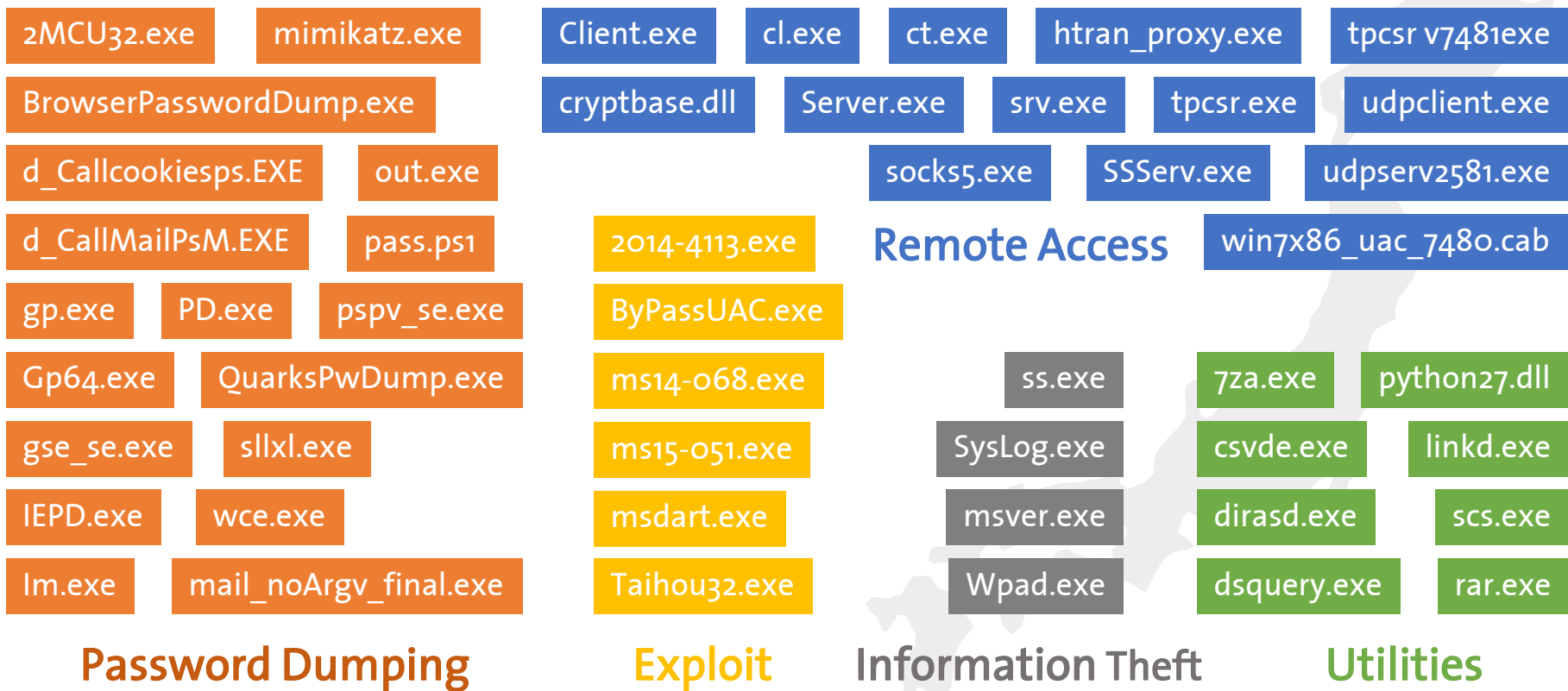
- Where most of threat actors are involved in operation?



- Almost all of IP addresses are assigned by ISP in Shanghai

Tools used by threat actors after the infection

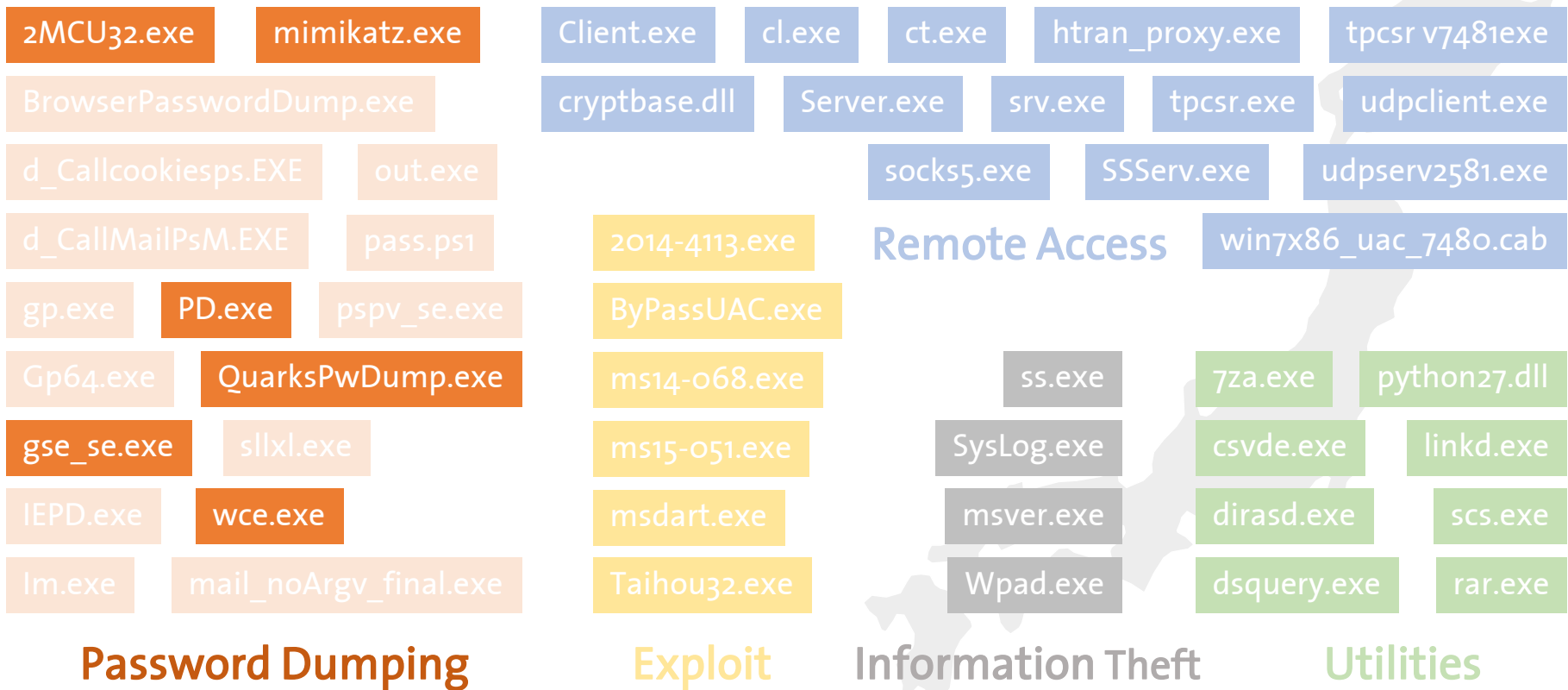
- Category classification of tools used for further invasion



- A set of tools are different by targeted organizations **18**

Why functionally overwrapped for same sake?

- OS password dumping tools for different preferences



- If so, a number of person actually execute in parallel **19**

Making a mistake during attack (1)

- What if an actor forgets to use proxy for execution?

1. Unmasked IP address – Direct access to webmail



Actor's IP address

```
D=LT3T114DCA7HIF3HTWCIIMXR09/2RYA7JCADDZED4TCHKSTYg7g2057PE0ZP
/gU1S+vjcfQgtaFGryGec1S8h32CeQMkV00tM6fFfaJ/ar0BJ6HRrLJAz7VT
/4XROe80xpcnD8AD01MaXVBSkY=;
Message-ID: <244596.37080.qm@web101312.mail.kks.yahoo.co.jp>
X-YMail-OSG:
I dv7pIEVM1nbu1uHi2yMPdeSzw5oIGhYCGHPdEYxn5bqQLTJQZHLfqB4g4I5
zgQIXoNdazjgUMaJdi9at_3zCGWE0GNqnSbtYI3ZijcIxVCNjVBCZmwr2GCv
R9Qx03Fbfn7NI_suyIEGnR_vihU1.cwAaqy7W4AUwJZbcNgD.YKmOLDnH4TX
uH70gxwyL6lpySpCnNYxVFS_YpcPIEuMPKyPQqiI09bqxIuf.Z86u0dpxGwy
dXXbvLZsWPFo51RcrjuCv7Bi6iszoadaDQyJKkh00WwWazSeYi8M25ZBdC
yqwr+YvgsuMvR_vfL_WvJIS54oIfYtkT1VITUAhD3diEA_Y0YYeYic_INQfPvT
Received: from [116.180.180.180] by web101312.mail.kks.yahoo.
Jan 2015 11:28:00 JST
X-Mailer: YahooMailWebService/0.8.111_57
X-YMail-JAS:
XTT5fGEVM1lpnBQUc4U7nc.CWrXgVVwsZZxvFOvGQqEnw7uk9nBt6QdWCwJ5
Xg.IGkftfZ.dPefzXgUzDxoZIEMNkJiLEna042bKwdiV4v
References:
```

- Source IP address was revealed at mail header.

Making a mistake during attack (2)

- What if an actor puts time by mistake for execution?

2. Time Difference – AT command

GotTime	cmd
2015年██月██日 16:28:53	at ¥¥██████████.co.jp
2015年██月██日 16:30:05	copy mimikatz.exe ¥¥██████████.co.jp¥c\$¥windows¥temp
2015年██月██日 <u>16:30:30</u>	at ¥¥██████████.co.jp <u>15:31</u> cmd /c "c:¥windows¥temp¥mimikatz.e
2015年██月██日 <u>16:30:57</u>	at ¥¥██████████.co.jp <u>16:31</u> cmd /c "c:¥windows¥temp¥mimikatz.e
2015年██月██日 16:31:12	at ¥¥██████████.co.jp

JST

local time

1 hour time difference from Japan

- What does this mean?

How to make decoy documents?

- 3 types of decoy file have been observed

a) Documents manually described

- natural language writing skill
- slightly different fonts from original expectation

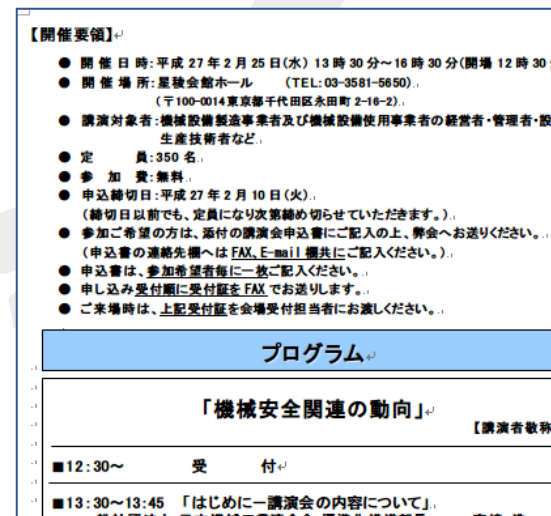
b) Word or PDF output of web contents

- Document file may include meta information, EXIF

c) Documents taken from victim's system

- sensitive documents not to be disclosed such minutes, and timely manner

- It's not easy task how to prepare decoy files for any purpose. 22



Summary of Threat Actor Attribution

Location of IP addresses used by possible actor's computers

AWS / Singapore



1.5 %



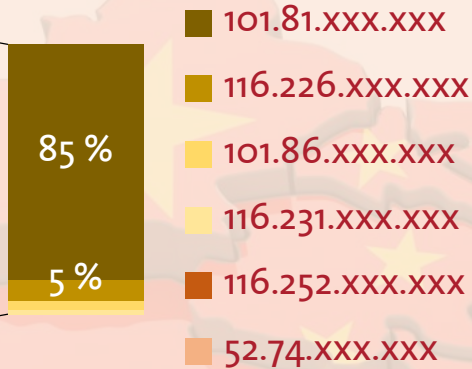
Shanghai

97 %

1.5 %



Guangxi



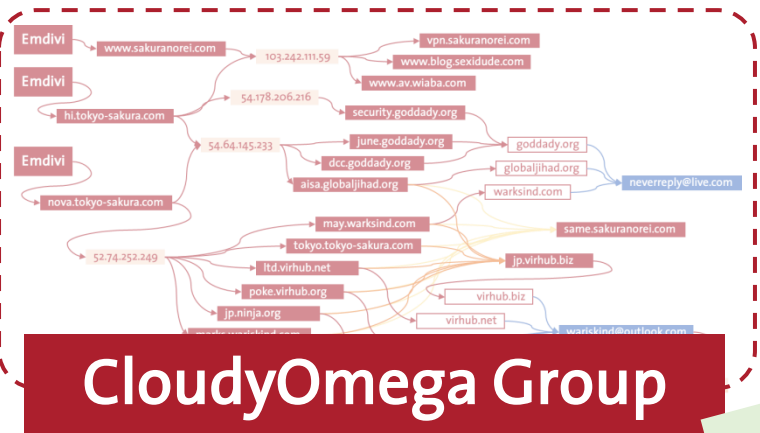
slightly different character font

1 hour time difference

compose skill of decoy

Attack campaign by at least 6 people and 10 PCs

Threat Actor Attribution (Campaign)



1. Victim organization



ongoing analysis

1. Name of victim organization



- Domain: "virhub.net"
- created on 2015-04-11
- 50.63.202.35 (GoDaddy.com)

- Domain: "virhub.info"
- created on 2015-04-11
- 50.63.202.53 (GoDaddy.com)

2. Similar activity, but weak proof yet

- Domain: "feerlook.org"
- created on 2015-03-26
- 50.63.202.32 (GoDaddy.com)



• Future attack campaign will look like mixed characteristics from several attack campaign.

Summary of Collectively Analysis based on CTI

1. In Emdivi operation, both highly and less targeted phishing mails with various decoys had caused a series of incidents.
2. Hybrid architecture of C2 infrastructure brings certain advantages to threat actors.
3. Threat actor is human and therefore prone to making mistakes.

Thoughts about the Future

1. Social Engineering worked effectively so far and is still valid option.
2. Hybrid architecture of C2 is expected to continue for the meantime.
3. Actor's mistake is key to identify threat actors.
4. **Threat Actor is human, it's better to exchange not only Threat information, but also things that humanness could be appeared.**

Q & A

- **Thank you for your attention**



References

- CloudyOmega (Symantec)
 - <http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan>
- Blue Termite (Kaspersky)
 - <https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/>
- APT12 (FireEye)
 - <https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html>
- IXESHE (Trendmicro)
 - http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf
- Etumbot (Arbor Networks)
 - <https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf>
- Numbered Panda (CrowdStrike)
 - <http://www.crowdstrike.com/blog/whois-numbered-panda/>
- DragonOK
 - <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>
 - <http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/>
- APT1
 - http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- menuPass
 - <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf>
- APT1o
 - http://www.rsaconference.com/writable/presentations/file_upload/tta-ro2-nation-state-hacktivist-attacks-targeted-hits-on-asian-organizations_copy1.pdf
- Duststorm
 - https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf