RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: TTA-F03

Are Enterprises in a Losing Battle Against Targeted Attacks?

Masayoshi Someya

Senior Security Evangelist
Trend Micro Incorporated.

Many High Profile Data Breaches

2014 – A year of data breach

Month	Industry	Country	Employees	Details
Feb	University	US	9,000	290,000 staff and student details breached
Feb	E-Commerce	JP	270	1,160 customer details breached
May	Auction	US	18,000	145 million customer details breached
Jul	Manufacturing	JP	430	62,000 customer details breached
Aug	Retail	JP	170	900 customer details breached
Aug	Healthcare	US	90,000	4.5 million patient details breached
Sep	University	US	3,000	4,000 student details breached
Sep	Airline	JP	10,000	190,000 customer details breached
Oct	Financial	US	260,000	83 million customer details breached
Nov	Postal	US	800,000	Staff and customer details breached
Dec	Press	JP	1,600	17,000 customer details breached
Dec	Trade	JP	5,600	600 personal details breached

2015 – A year of data breach

Month	Industry	Country	Employees	Details
Jan	Fast food	US	500?	Potentially breached credit card details
Jan	Insurance	US	37,000	Up to 37.5 million personal data breached
Jan	Food	JP	Unknown	About 2,000 personal data breached
Jan	Newspaper	JP	4,600	17 PCs infected with backdoor
Feb	Service	US	2,000	Over 50,000 driver details breached
Feb	Retail	JP	20	Up to 6,600 credit card details breached
Feb	Trade	JP	1,600	800 personal data breached
Mar	Credit card	JP	30	84,000 credit card details breached
Apr	Hotel	US	5,000?	Credit card details breached
May	Government	US	100,000	100,000 taxpayer details breached
Jun	Public sector	JP	26,000	1.25 million pensioner details breached

US entertainment：
A Prime Example of Business Impact

Network forced shut down

Docs inc. exec's wages uploaded

employees received threat email

Unreleased films uploaded

Employees' data inc. SSN breached

FBI alleges North Korea

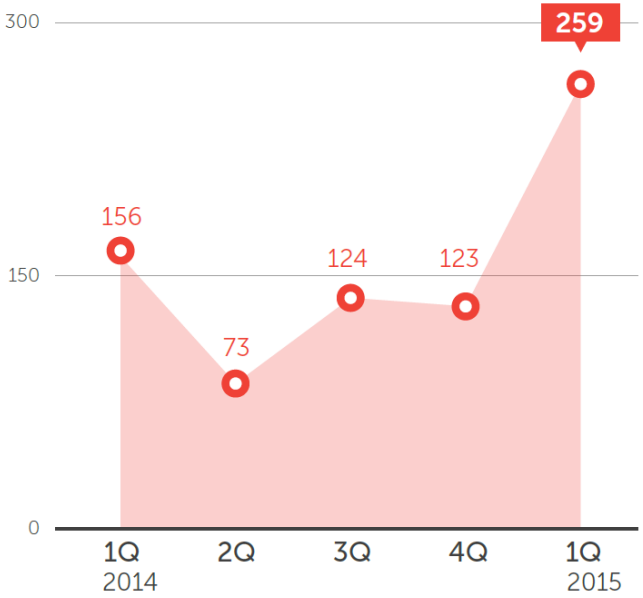
2014 – A year of credit card breach

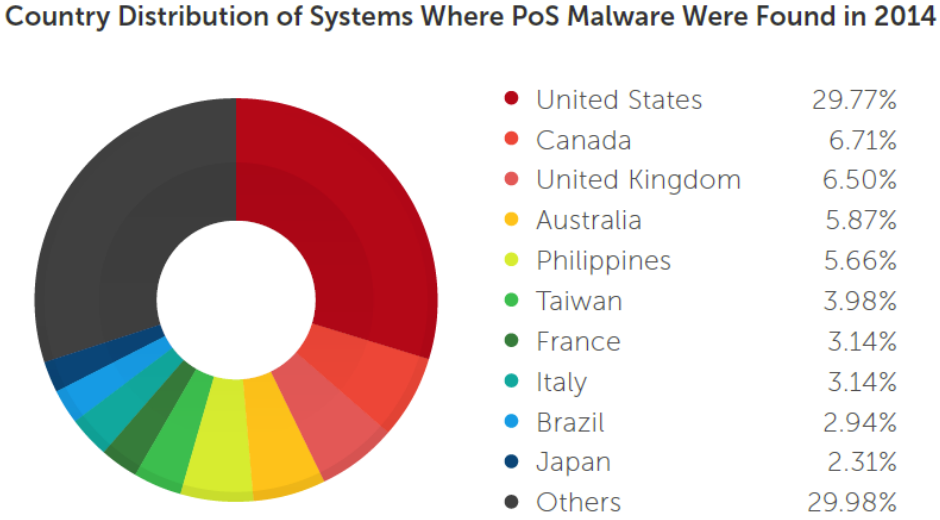
Month	Industry	Details
Jan	Department store	3 million card details breached
Jan	Art	350,000 customer details breached
Feb	Hotel	Breached at 14 hotel chains
Mar	Beauty products	25,000 custome
Jun	Restaurant	Credit card detai
Aug	Supermarket	Credit card detai
Aug	Shipping	Credit card detai
Aug	Grocery	Credit card detai
Aug	Restaurant	Credit card detai

Month	Industry	Details
Sep	DIY	Credit card details breached
Oct	Ice cream shop	Credit card details breached at 395 shops
Oct	Supermarket	Point-of-Sales terminals infected
Oct	Office equipment	Credit card details breached at 11 shops
Nov	Casino	1,600 credit card details breached
Nov	Parking	Credit card details breached
Nov	Airport	Credit card details breached at parking facility
Nov	Parking	Credit card details breached at 17 locations

2014 – A year of credit card breach

- Culprit – The rise of ‘Point-of-Sales malware’

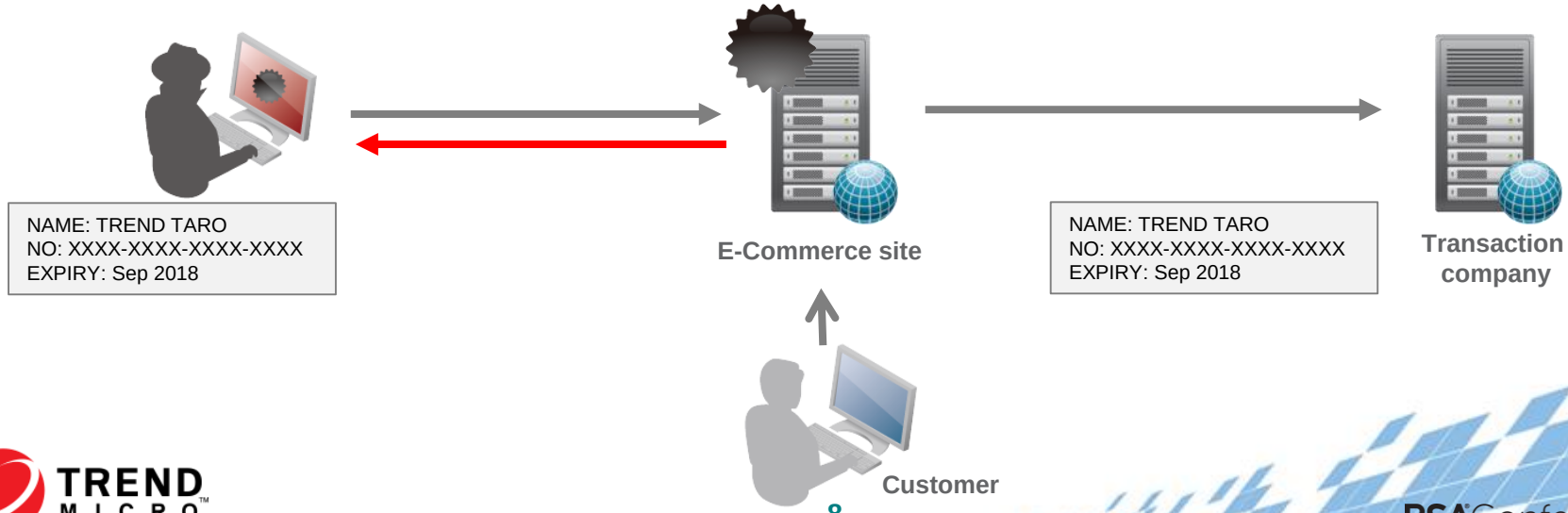




Trend Micro 2015 Q1 Security Roundup: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/rpt-trendlabs-2015-1q-security-roundup-bad-ads-and-zero-days-reemerging-threats-challenge-tr.pdf

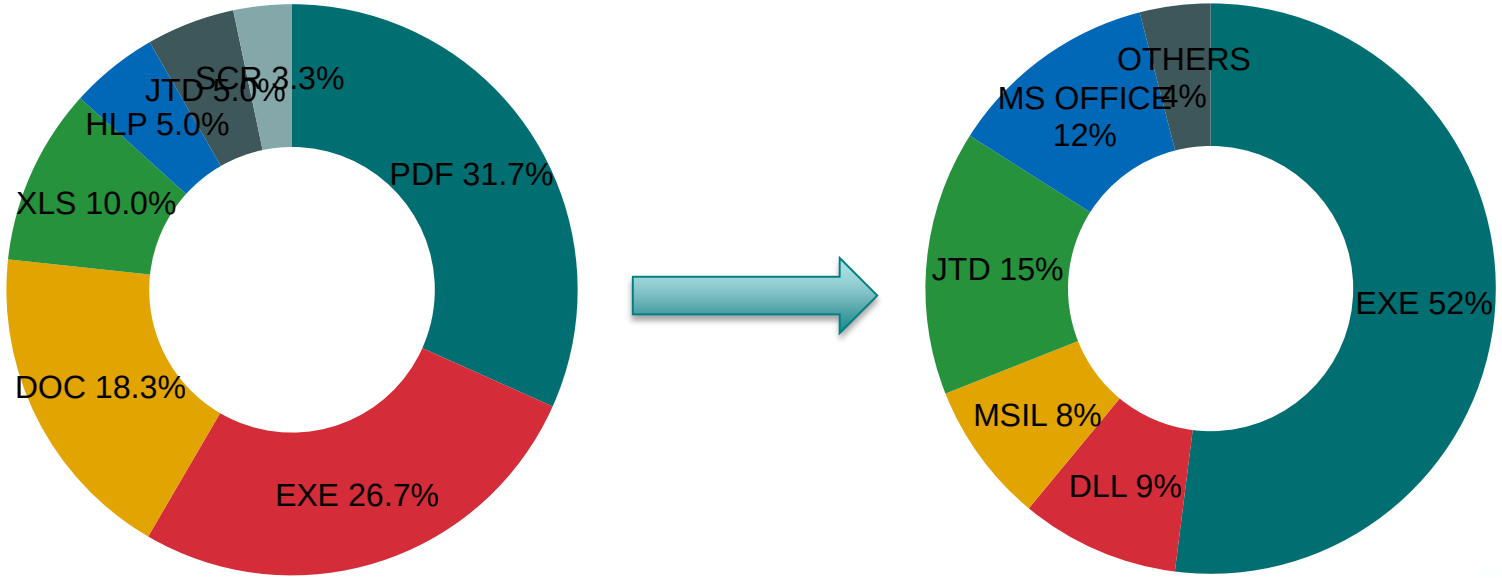
JP E-Commerce：
Data stolen from servers without data?

Month	Industry	Size	Details	Cause
Jul, 2014	Manufacturing	400	60,000 PII and 600 credit card details breached	Middleware vulnerability
Aug, 2014	Retail	170	900 credit card details breached	Middleware vulnerability



Attachment in spear-phishing email

- Are Attackers infiltrating without relying on vulnerabilities?

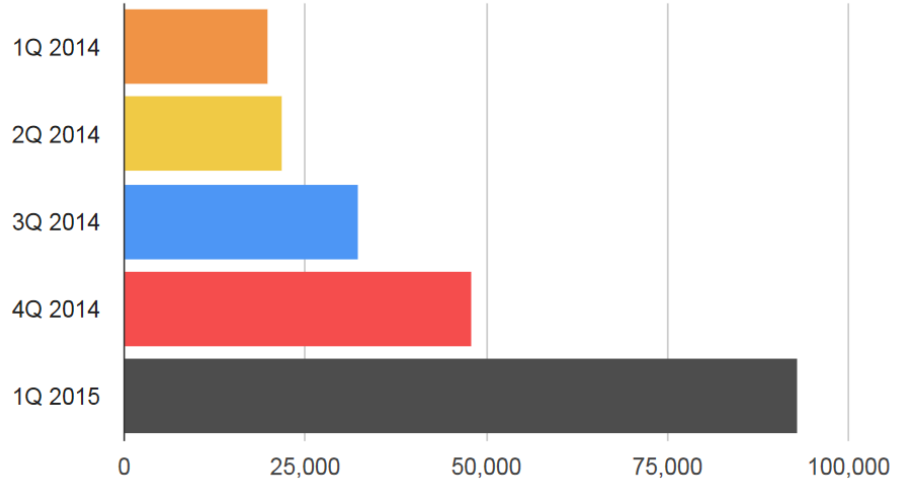


Annual Targeted Attack Roundup 2015:
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161

Re-emergence of old school macro malware

Countries That Posted the Highest Number of Macro Malware Infections in 1Q 2015

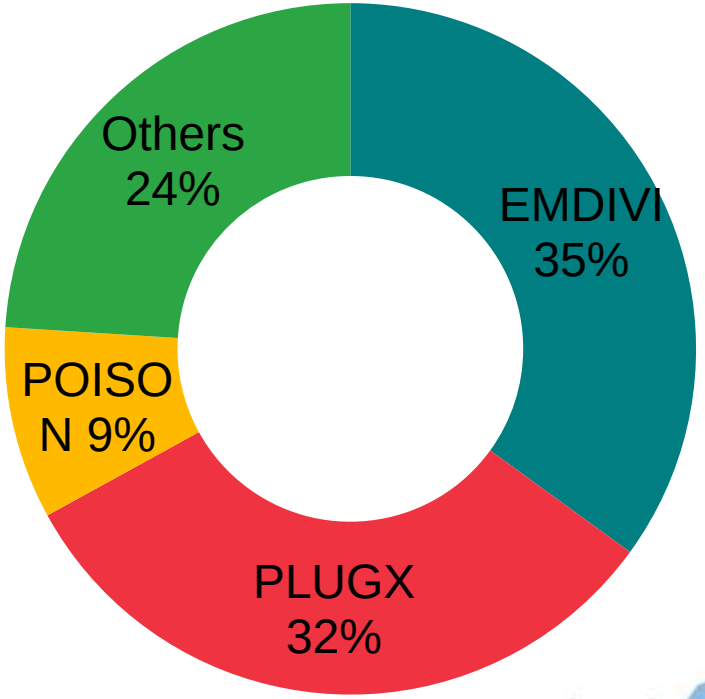
China	22%
United States	14%
United Kingdom	12%
Japan	7%
Australia	5%
France	5%
Italy	4%
Taiwan	3%
Germany	3%
India	2%
Others	23%



Trend Micro 2015 Q1 Security Roundup: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/rpt-trendlabs-2015-1q-security-roundup-bad-ads-and-zero-days-reemerging-threats-challenge-tr.pdf

Backdoor adopted in targeted attacks

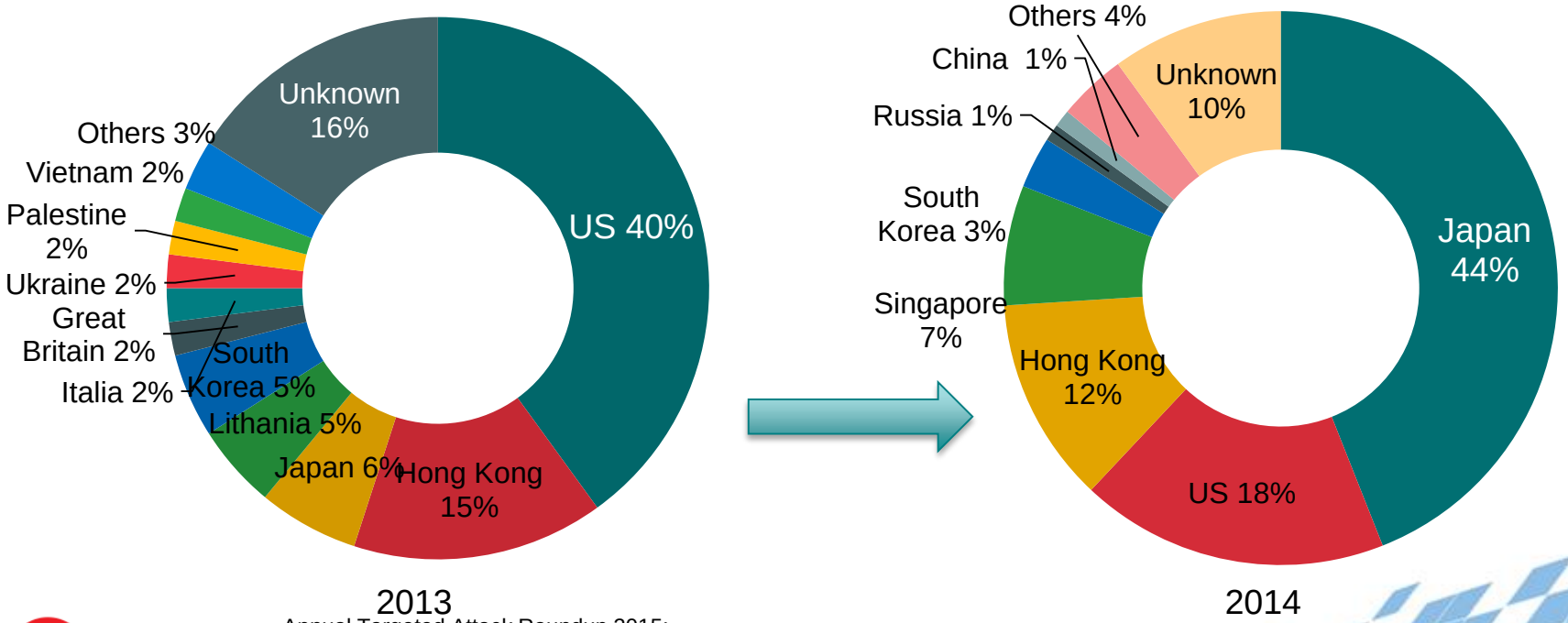
- POISON most commonly used until 2012
- Shifted to PLUGX in 2013
- Newly emerged EMDIVI the most widely-used backdoor in 2014



Annual Targeted Attack Roundup 2015:
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161

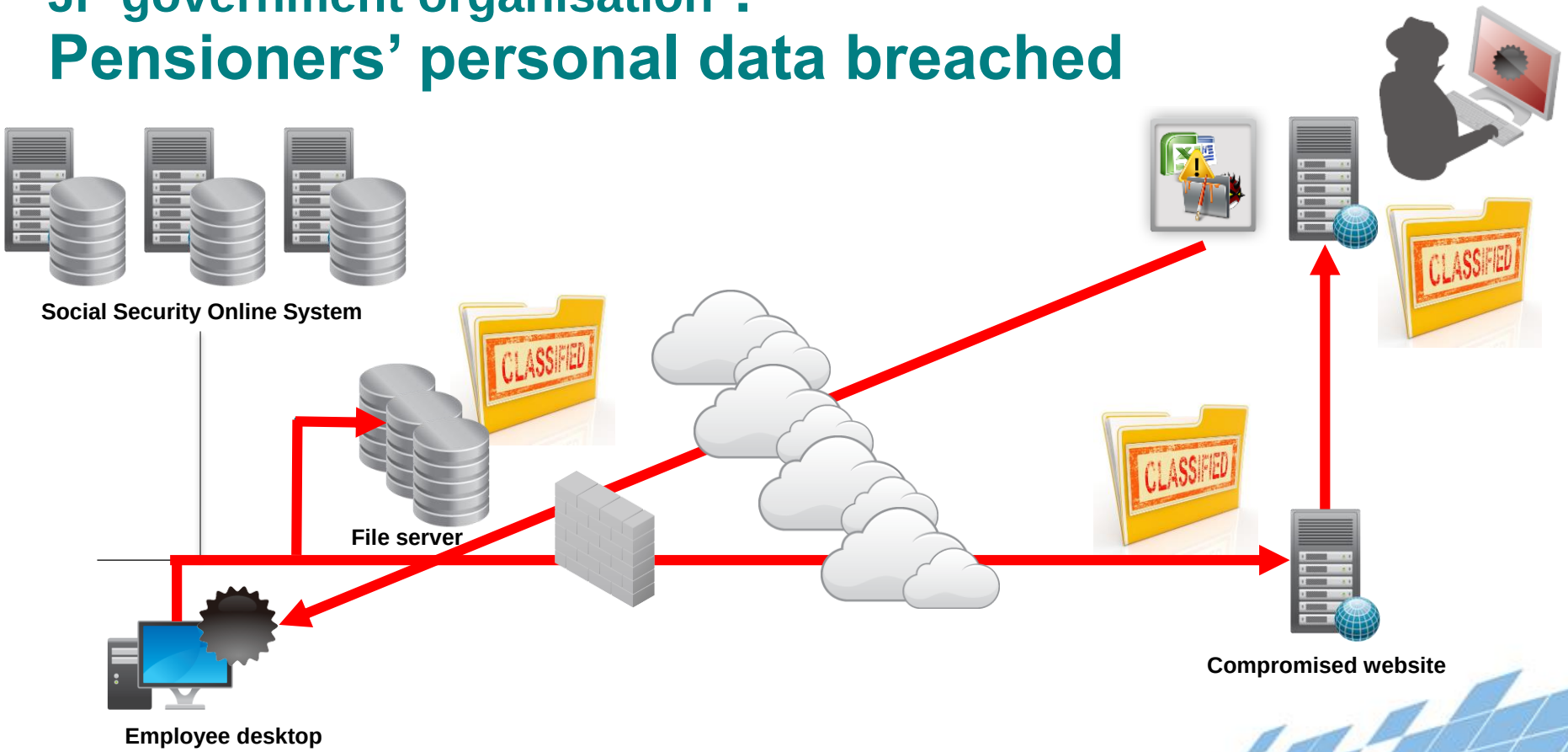
Backdoor C&C communication

- Why are attackers moving C&C into the same country?



Annual Targeted Attack Roundup 2015:
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161

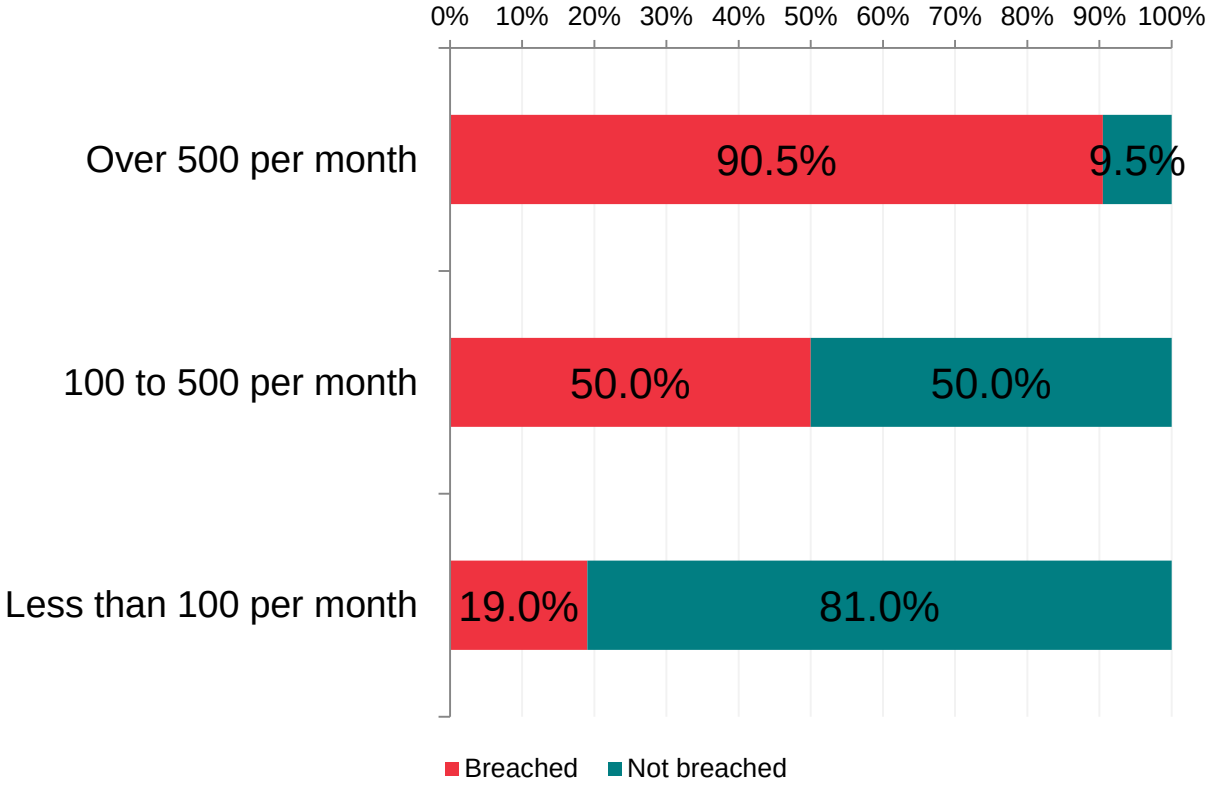
JP government organisation：
Pensioners' personal data breached



Visibility check points through experience

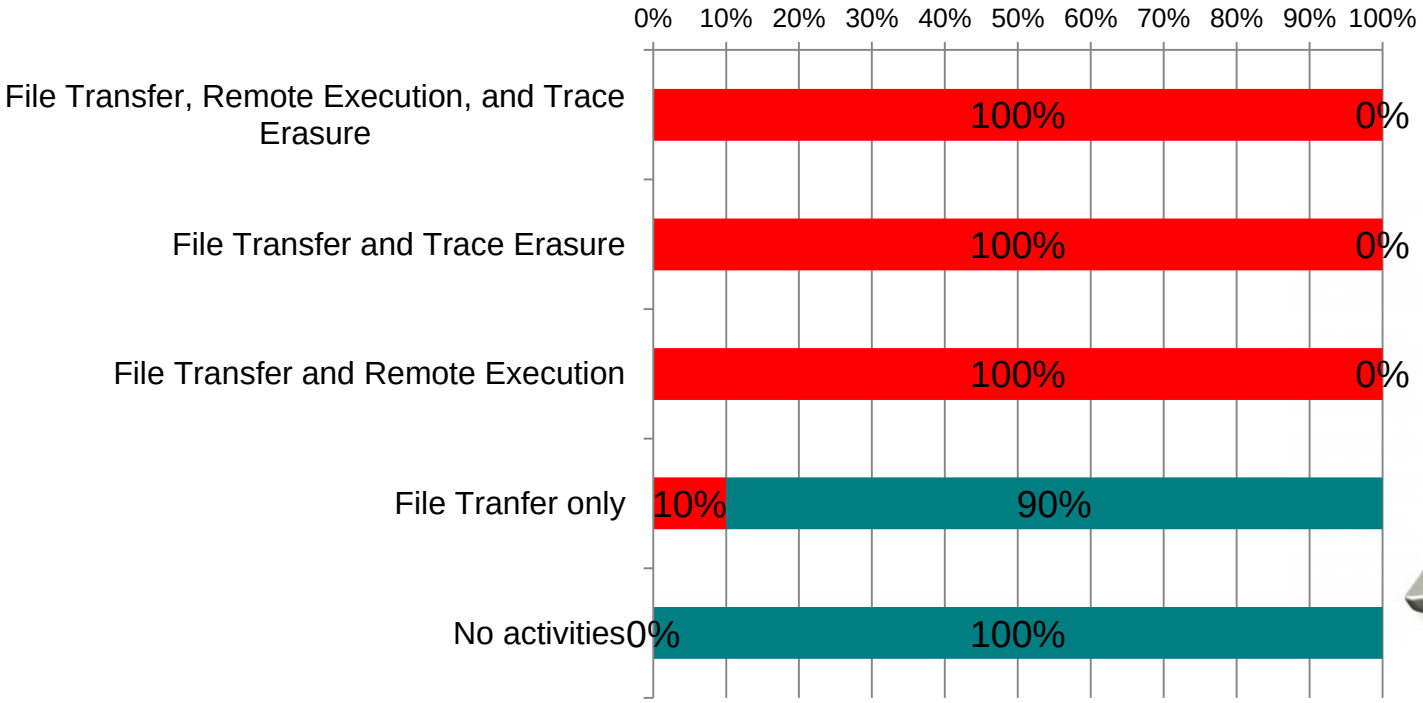
Step Zero	Gaining admin privilege	Spear-phishing email
		Remote login via bruteforce / dictionary attack
Step One	File transfer	Copy executables to Windows admin share
		Transfer executables via FTP
		Execute echo command remotely
Step Two	Remote execution	Execute PsExec
		Create remote tasks
		Create remote services
Step Three	Trace erasure	Delete tasks remotely
		Delete services remotely
		Delete event log remotely

Login failures… so what?



Annual Targeted Attack Roundup 2015:
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161

Attackers will always erase the ‘trace’

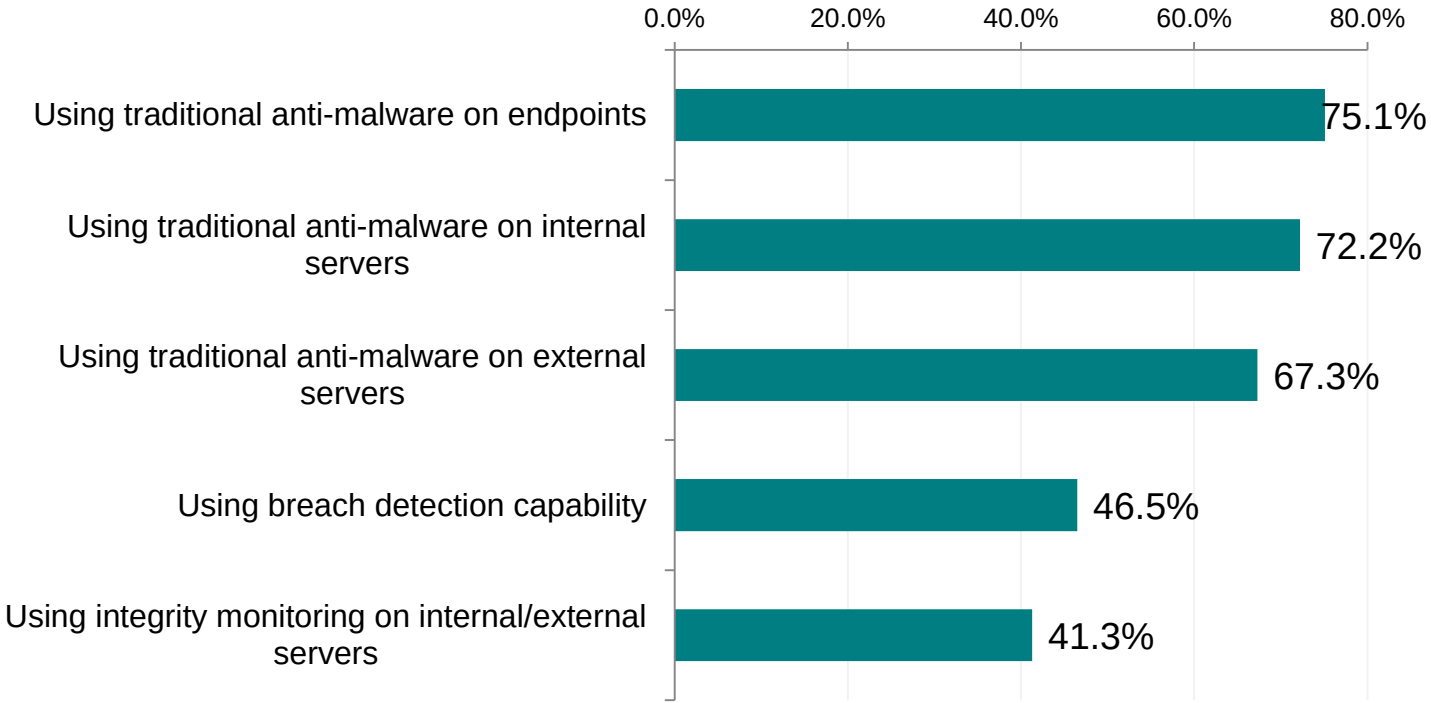


Annual Targeted Attack Roundup 2015:
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161

Breach period can be lengthy

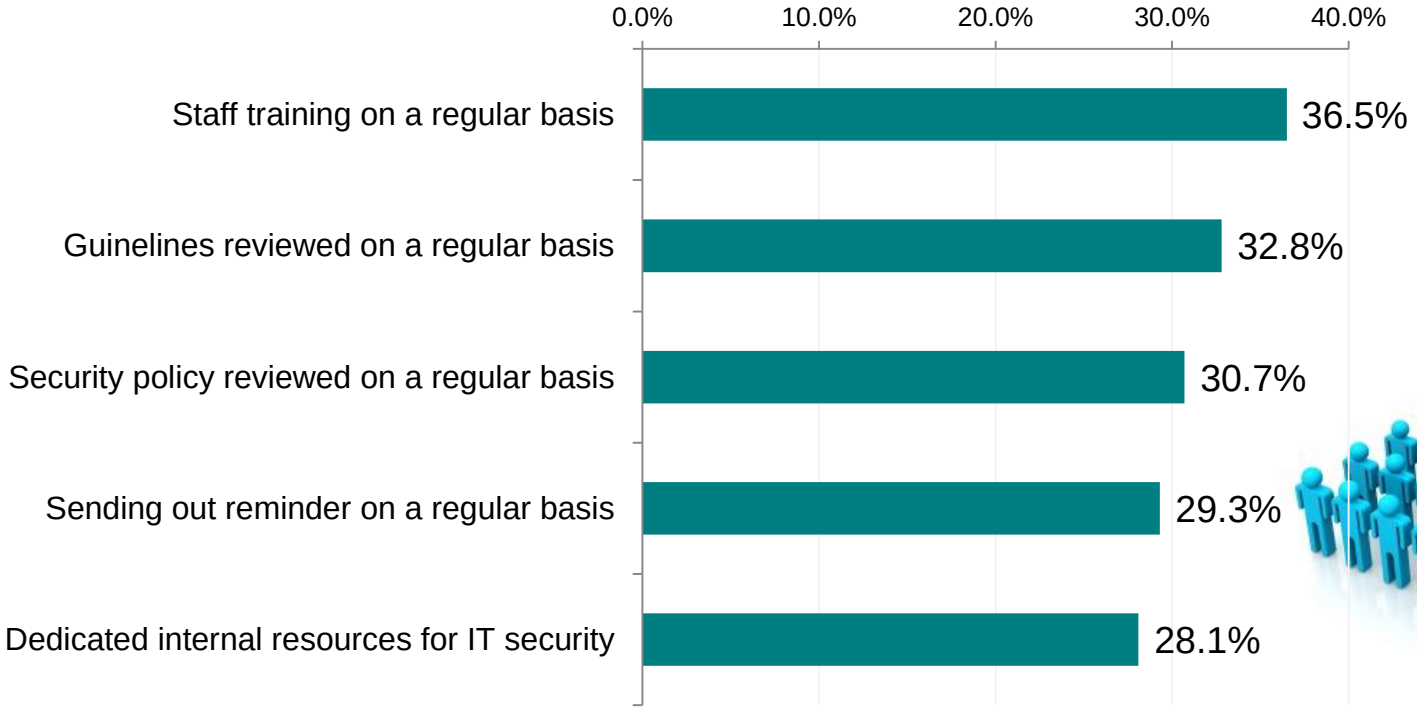
Month	Industry	Country	Employees	Breach period
Jan	Fast food	US	500?	Two months
Jan	Insurance	US	37,000	Two months
Jan	Food	JP	Unknown	Three months
Jan	Newspaper	JP	4,600	One and a half months
Feb	Service	US	2,000	Four months
Feb	Retail	JP	20	Ten months
Feb	Trade	JP	1,600	Four months
Mar	Credit card	JP	30	Four months
Apr	Hotel	US	5,000?	Seven months
May	Government	US	100,000	Three months
Jun	Public	JP	26,000	One months

Next-generation… what?!



Source: Trend Micro 'Enterprise Security – State of Reality Survey 2015'
URL：Http://www.go-tm.jp/sor2015

Our employees aren't that stupid, really…



Source: Trend Micro 'Enterprise Security – State of Reality Survey 2015'
URL：Http://www.go-tm.jp/sor2015

Enterprises don't understand targeted attacks

- Common 'wrong' questions asked about targeted attack incident
  - What's the detection name?
  - When did you release a pattern file?
  - Are we safe from the same sample used against <victim>?
  - How could they open an attachment in a 'suspicious email'?
  - What's the 'silver bullet'?

Do we have data to protect? Really?

- Do they have the importance of data defined, and carry out regular audit?

25%

Source: Trend Micro 'Enterprise Security – State of Reality Survey 2015'
URL：Http://www.go-tm.jp/sor2015

Easy peasy! We are not gonna be targeted!

- ‘We don’t have risks because…’
  - ‘We are not a government or defence agency’
  - ‘We are not a recognised brand’
  - ‘We are not a large enterprise’
  - ‘We don’t have data that are valuable’
  - ‘We have never been targeted before!’

Observations on the current threat landscape

- Attackers are changing tools and tactics to achieve their goal
- They are also relying on traditional attack vectors and tactics
- Businesses are doing far from enough to protect their data, with both technologies and people
- They have old mind set and misconceptions without grounds
- However, attacks are happening against enterprises of all sizes, all industries

Apply what you have learned today

- Next week you should:
  - Think about what if attacks happened to ‘your organisation’
- In the first three months following this presentation you should:
  - Assess your current security measures and risks
  - Define the importance of your data
  - Raise awareness within your enterprise
- Within six months you should:
  - Build incident response capability
  - Strengthen endpoints and servers with latest security suites
  - Adopt breach detection capability in-house or outsourced

One thing to remember

- Breach will happen, to any size business… including you.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Thank you!