Innovative R&D by NTT

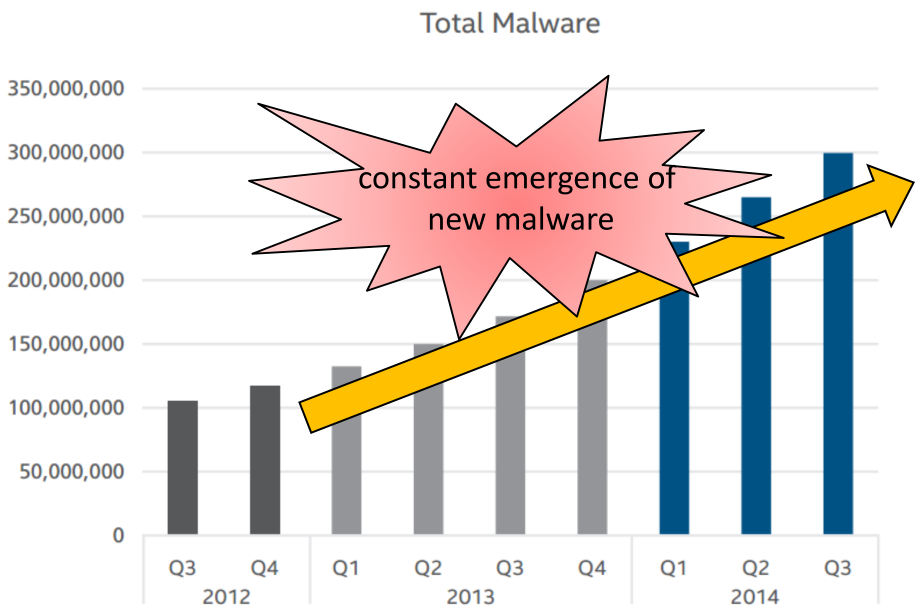
NTT R&D's anti-malware technologies

Jan. 21, 2015

NTT Secure Platform Laboratories
Takeo HARIU

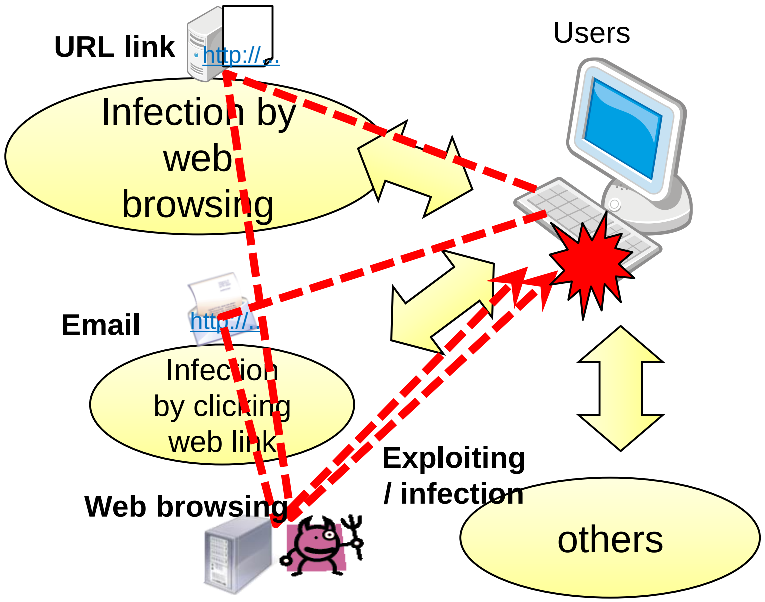
Malware Threats

- ◆ Malware causes most of cyber attacks
- ◆ Major infection routes are web browsing, URL links in email messages, attachment files, etc.



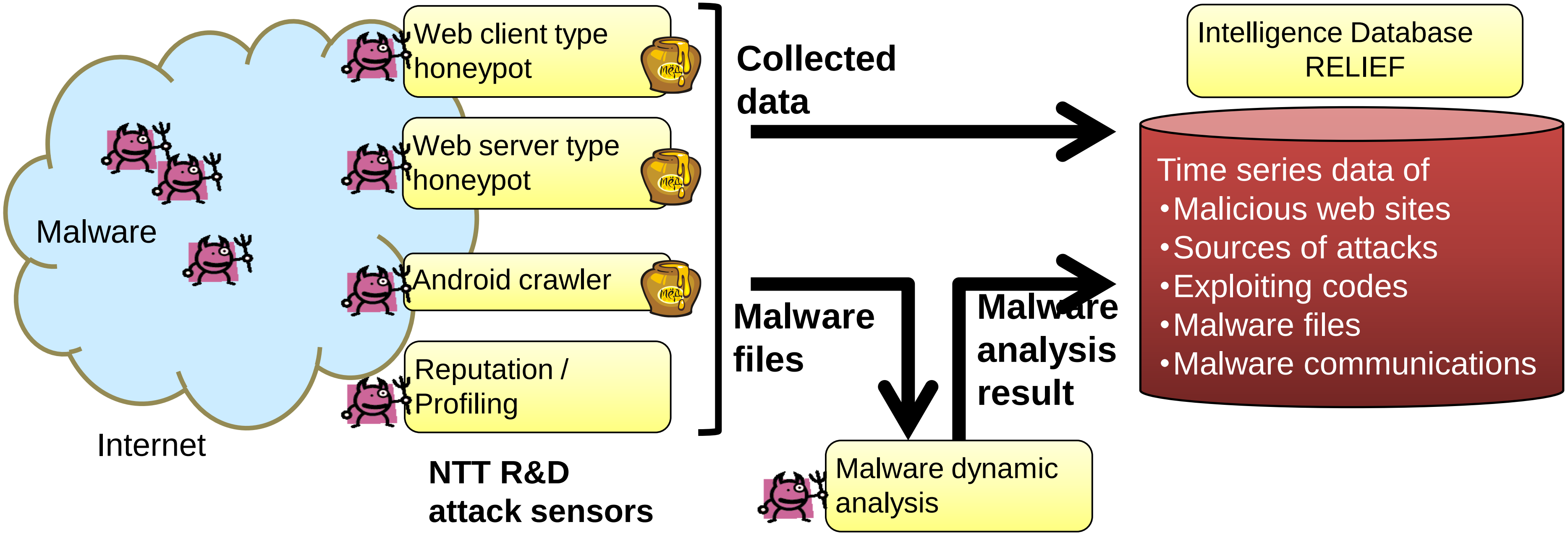
McAfee Labs Threats Report Nov. 2014

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf?cid=BHP032



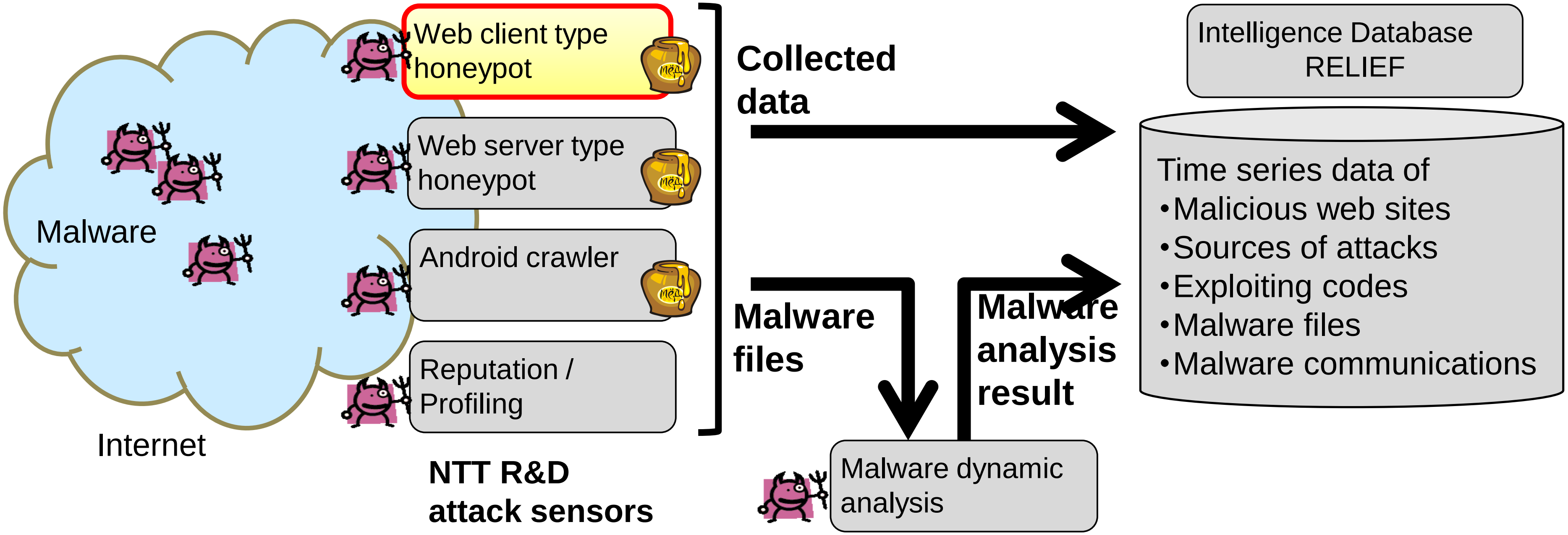
NTT R&D’s Anti-malware Technologies

- ◆ Detect/gather the latest attacks using “honeypot” sensors
- ◆ Analyze gathered data such as malware samples
- ◆ Construct an intelligence database of threat information
- ◆ Implement countermeasures such as access filtering



NTT R&D's Anti-malware Technologies

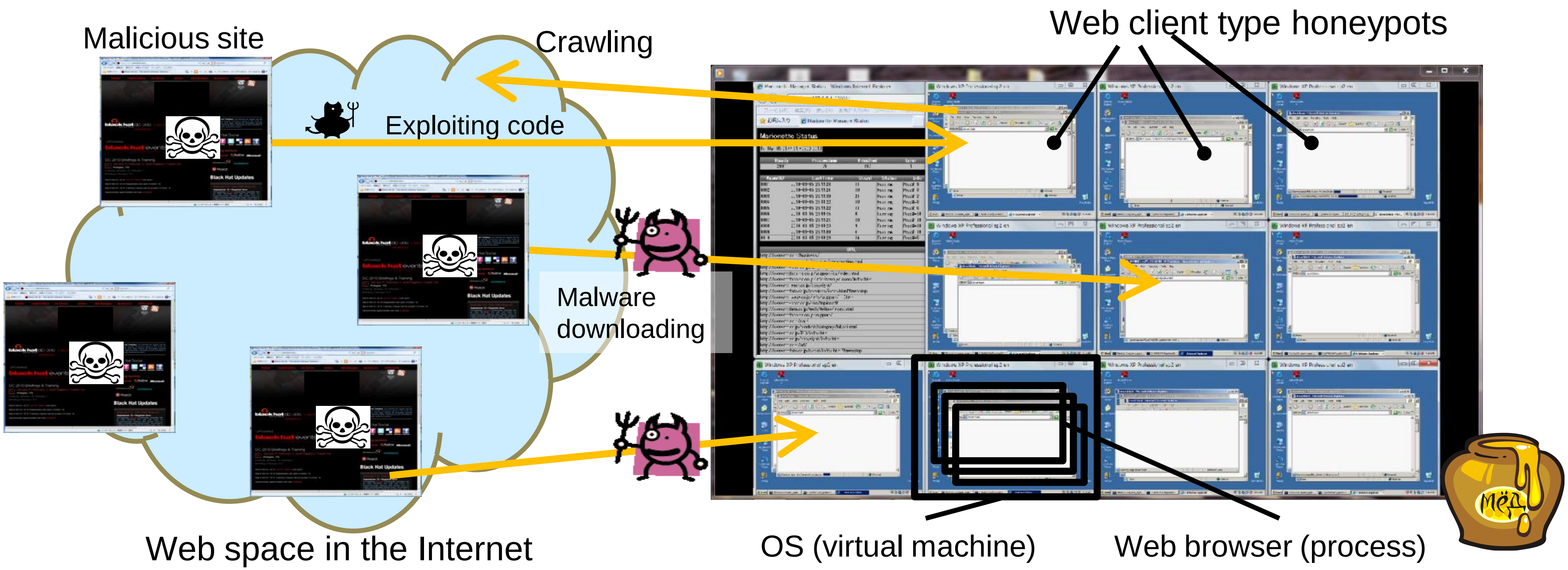
- ◆ Detect/gather the latest attacks using "honeypot" sensors
- ◆ Analyze gathered data such as malware samples
- ◆ Construct an intelligence database of threat information
- ◆ Implement countermeasures such as access filtering



Time series data of
- Malicious web sites
- Sources of attacks
- Exploiting codes
- Malware files
- Malware communications

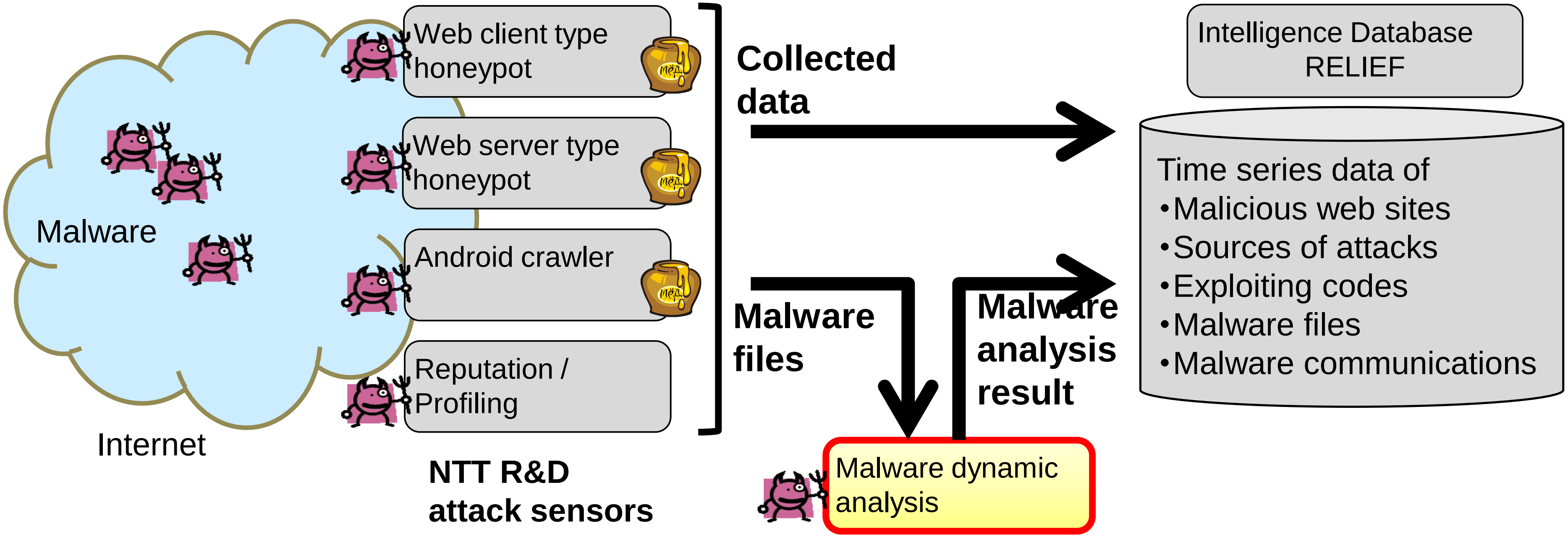
Web Client Type Honeypot

- ◆ A decoy web crawler which detects attacks to web browser vulnerabilities
- ◆ Crawls web sites, finds malicious web sites with exploiting codes or malware files, specifies attacks, and collects malware files
- ◆ Highly parallelized OSes and browsers make it possible to crawl many web sites



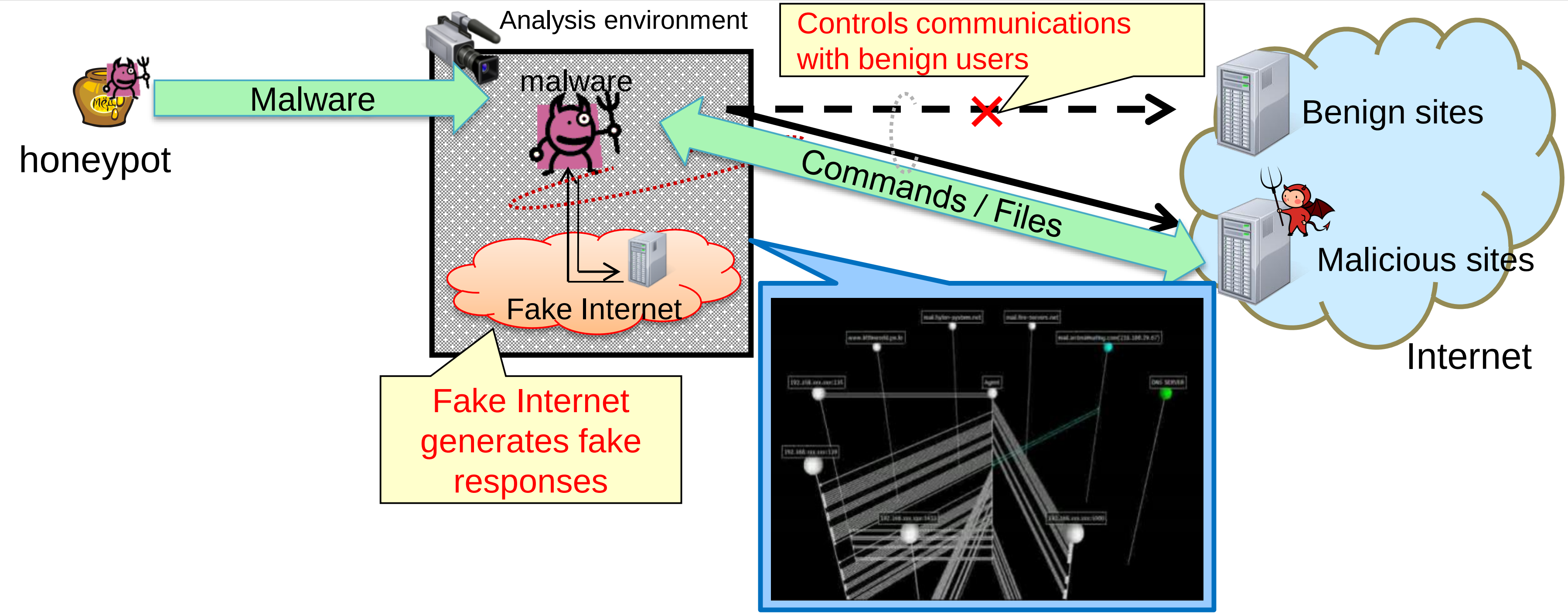
NTT R&D’s Anti-malware Technologies

- ◆ Detect/gather the latest attacks using “honeypot” sensors
- ◆ Analyze gathered data such as malware samples
- ◆ Construct an intelligence database of threat information
- ◆ Implement countermeasures such as access filtering



Malware Dynamic Analysis

- ◆ Some malware acts communicating with attacker's C&C servers, so malware dynamic analysis in Internet environment is important
- ◆ Analyze malware behavior safely by using Fake Internet
- ◆ Extract malware-related hosts information such as attacker's C&C servers, malware distribution sites

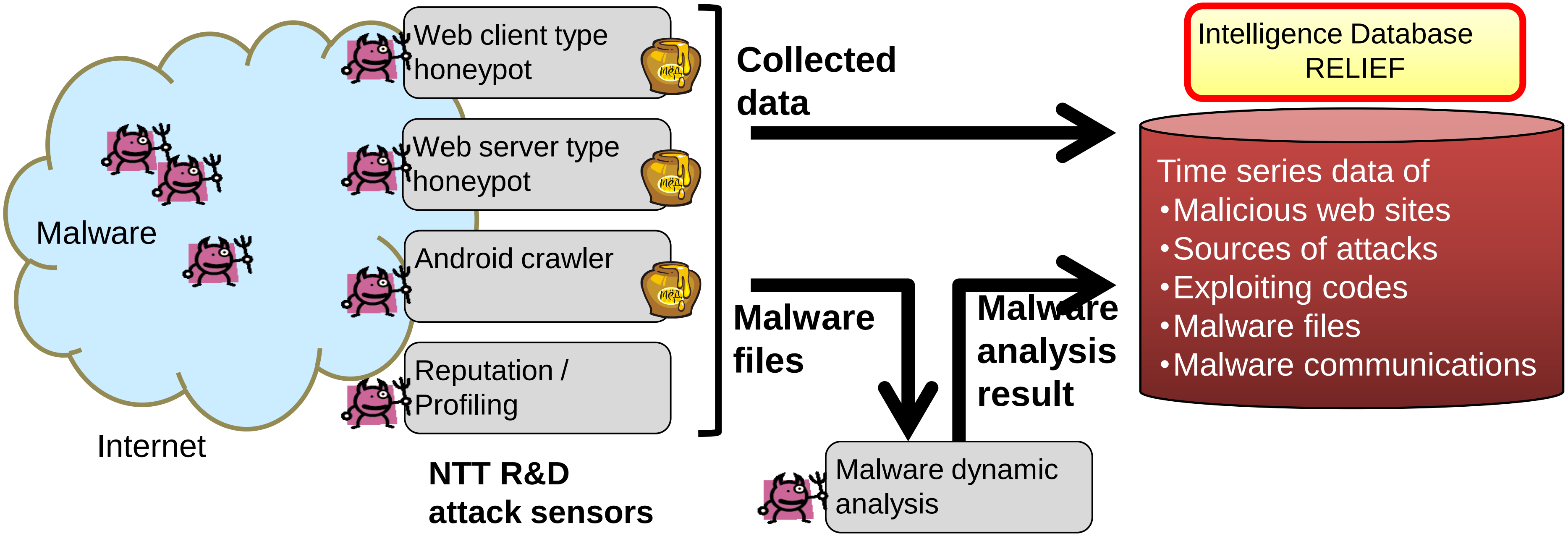


Controls communications with benign users

Fake Internet generates fake responses

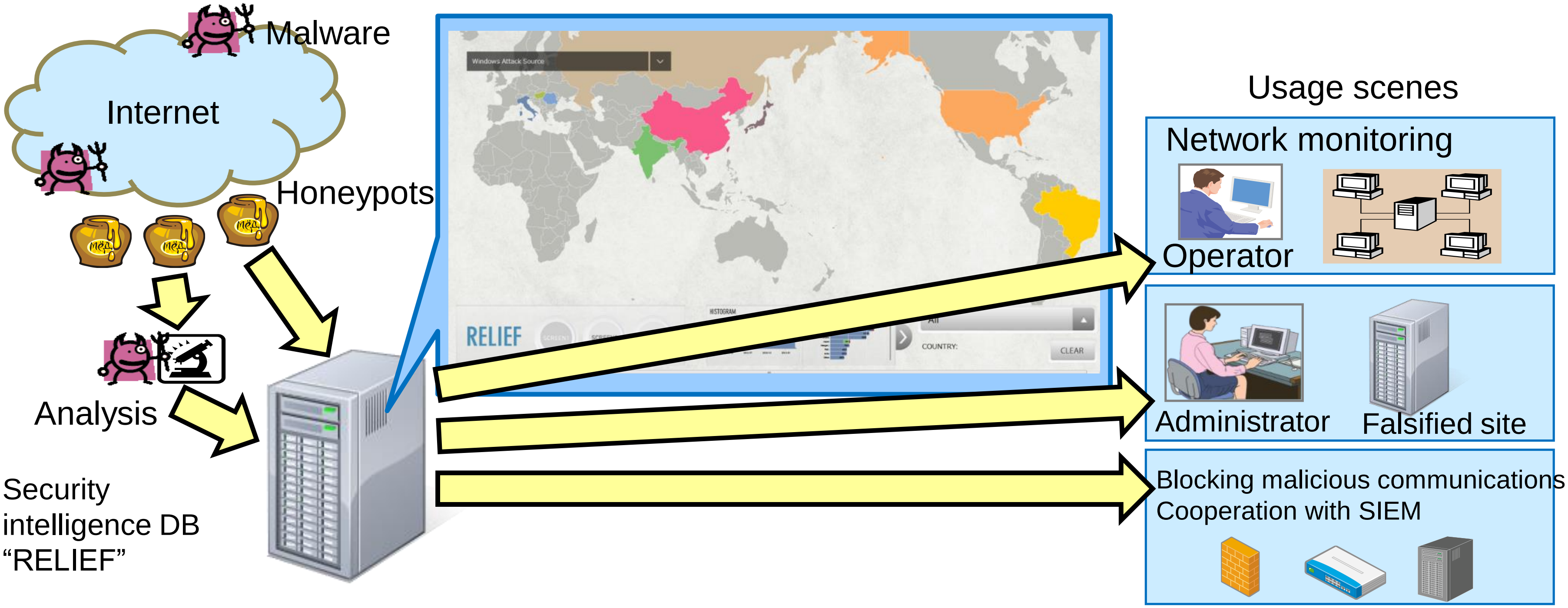
NTT R&D’s Anti-malware Technologies

- ◆ Detect/gather the latest attacks using “honeypot” sensors
- ◆ Analyze gathered data such as malware samples
- ◆ Construct an intelligence database of threat information
- ◆ Implement countermeasures such as access filtering



Security Intelligence DB “RELIEF”

- Analyze collected time-series data taking with various viewpoint such as nations, vulnerabilities
- Apply to countermeasures such as blocking malicious communications by using blacklists, alerting infected users or falsified web administrators



Malware

Internet

Honeypots

Analysis

Security intelligence DB “RELIEF”

Usage scenes

Network monitoring

Operator

Administrator

Falsified site

Blocking malicious communications
Cooperation with SIEM

Innovative R&D by NTT

Thank you!

NTT