Establishment of Secure Academic Cyberspace by Collaboration among Universities

- NII-SOCS (NII Security Operation Collaboration Services) -

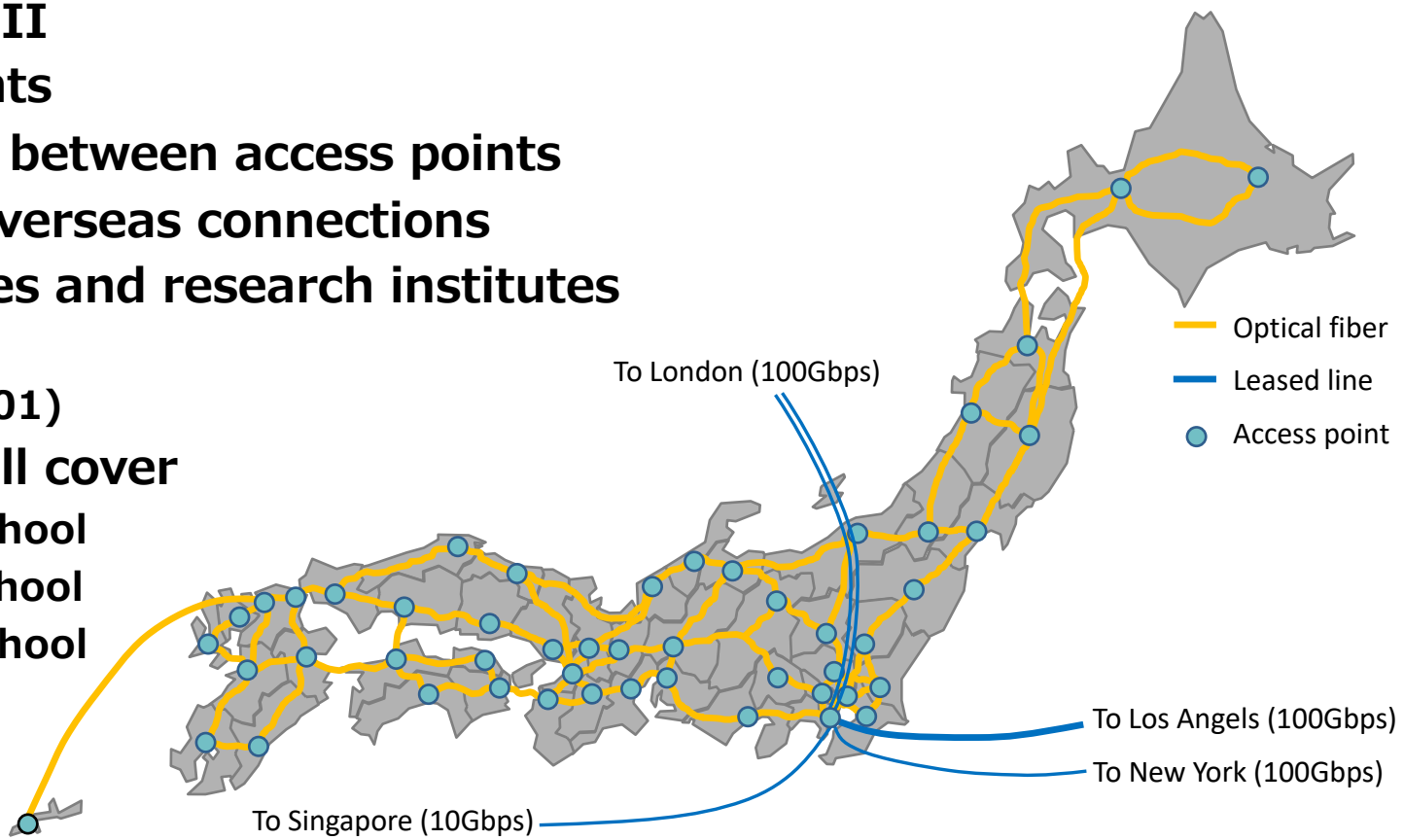
HIROKI TAKAKURA
DIRECTOR, CENTER FOR CYBERSECURITY RESEARCH AND DEVELOPMENT
NATIONAL INSTITUTE OF INFORMATICS

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Academic backbone network in Japan

NII

- **SINET5 (Science Information NETwork 5)**
  - **Operated by NII**
  - **50 access points**
  - **100Gbps links between access points**
  - **10-100Gbps overseas connections**
  - **910 universities and research institutes**
    - **100Gbps (16)**
    - **10-40Gbps (101)**
  - **Future plan will cover**
    - **Elementary school**
    - **Junior high school**
    - **Senior high school**



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Characteristics of academic network

NII

- Various types of devices are connected
  - Traditional computers
    - PC, servers, PDA, smartphones…
  - Research equipments
    - Telescope, micrscope, sensors…
      - Some of them are quite vulnerable
  - Building facilities
    - FA, IoT…
      - Most of them need direct connection to the Internet
        - » For research activities
- Ultra high speed
  - Over 10Gbps signle session, e.g., supercomputing
- Of course, IPv6!

Never worry about it

➡ Typical security systems cannot cover all of them.

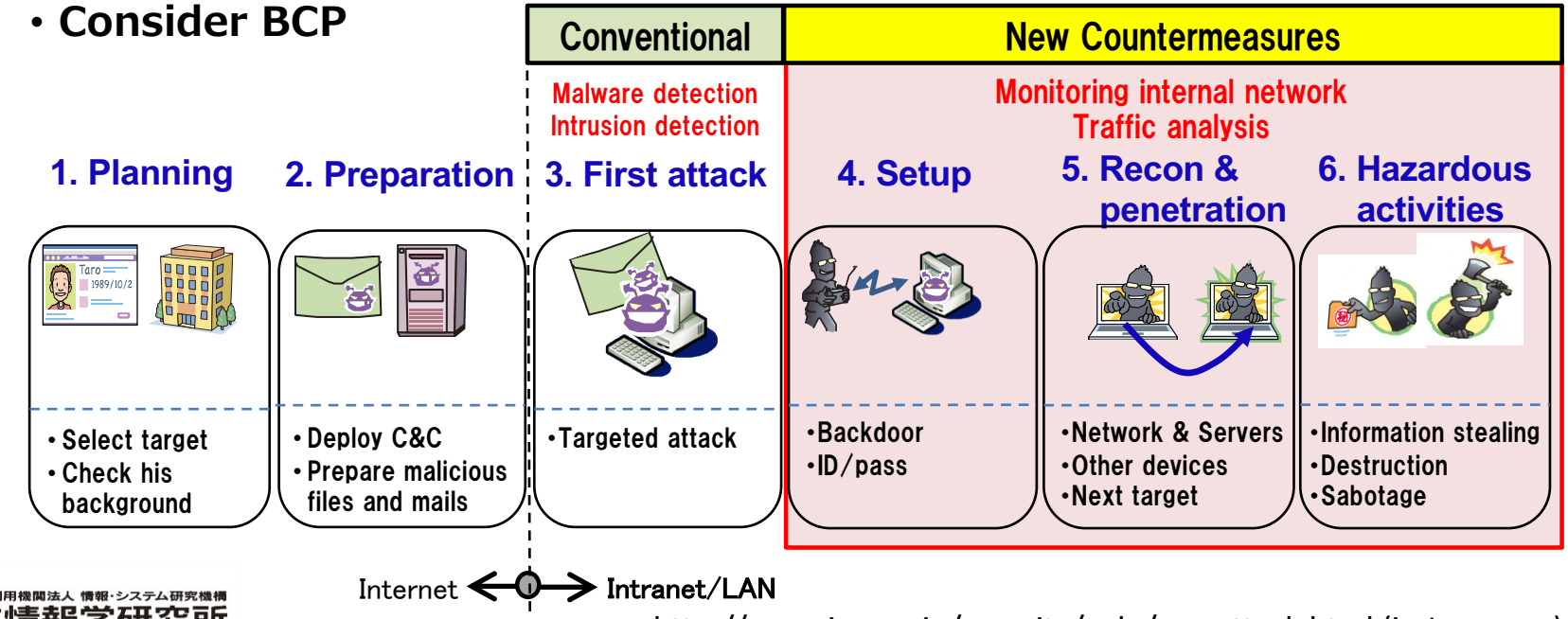
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Cyber security becomes mandatory for universities

- Basic Low for Cyber Security (2015)
  - All incorporated national universities should maintain adequate cyber security level on their network.
  - All incorporated administrative agencies must be monitored by Japanese gov.
    - Including all national research institutes.
- But, in universities
  - There are many students.
    - The Constitution of Japan prohibits governmental censorship.
    - Mixed traffic with researchers, faculties, students…and so on
  - Academic freedom must be preserved.
  - Too expensive cost is expected.
    - Wide bandwidth connection to SINET, e.g., 100Gbps
- Incorporated national universities have to protect by themselves
  - Capability to take proper action against cyber incident (in 5 years)

Adoption new countermeasure by Japanese government (2014)

- **Detect symptom of setup, reconnaissance or penetration**
  - Reveal all invisible activities before hazardous damage occurs
- **Analyze malicious activities while mitigation works effectively**
  - Damage control and degraded operation
    - Consider BCP



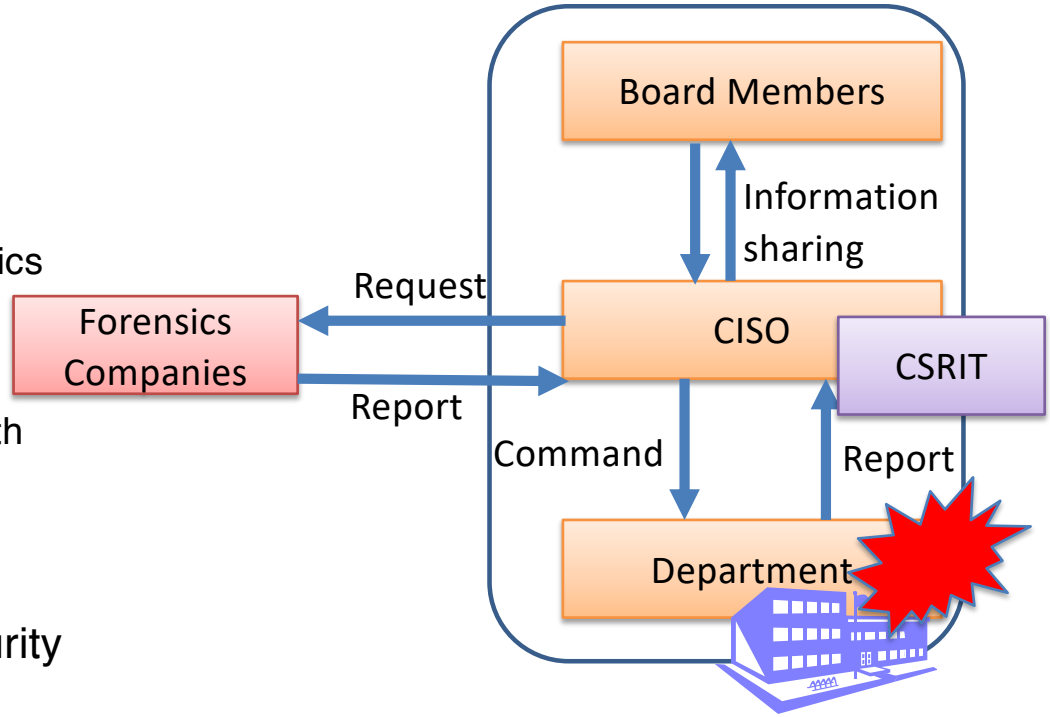
http://www.ipa.go.jp/security/vuln/newattack.html (in Japanese)

Requirement for adopting New countermeasure

- **Construction/operation of secure network** — NII-SOCS, Universities
  - Network segmentation and access control among segments.
    - Prohibit malware's activities on in-house network
    - Prepare for degraded operation (damage control)
- **Traps** — Universities and NII-SOCS
  - Dummy accounts, e.g., local admin, agent, manager…
  - Honeypots (optional)
- **Detection** — NII-SOCS
  - Log investigation
    - Login to dummy accounts, Access to honeypots
    - Alerts from security sensors
  - traffic analysis
    - Anomaly detection, Similarity analysis with typical C2 communication
- **Identification** — Universities and NII-SOCS
  - Risk level of attack
  - Attacker's target
- **Containment** — Universities
  - Quarantine all infected devices
  - Block all C2 communications

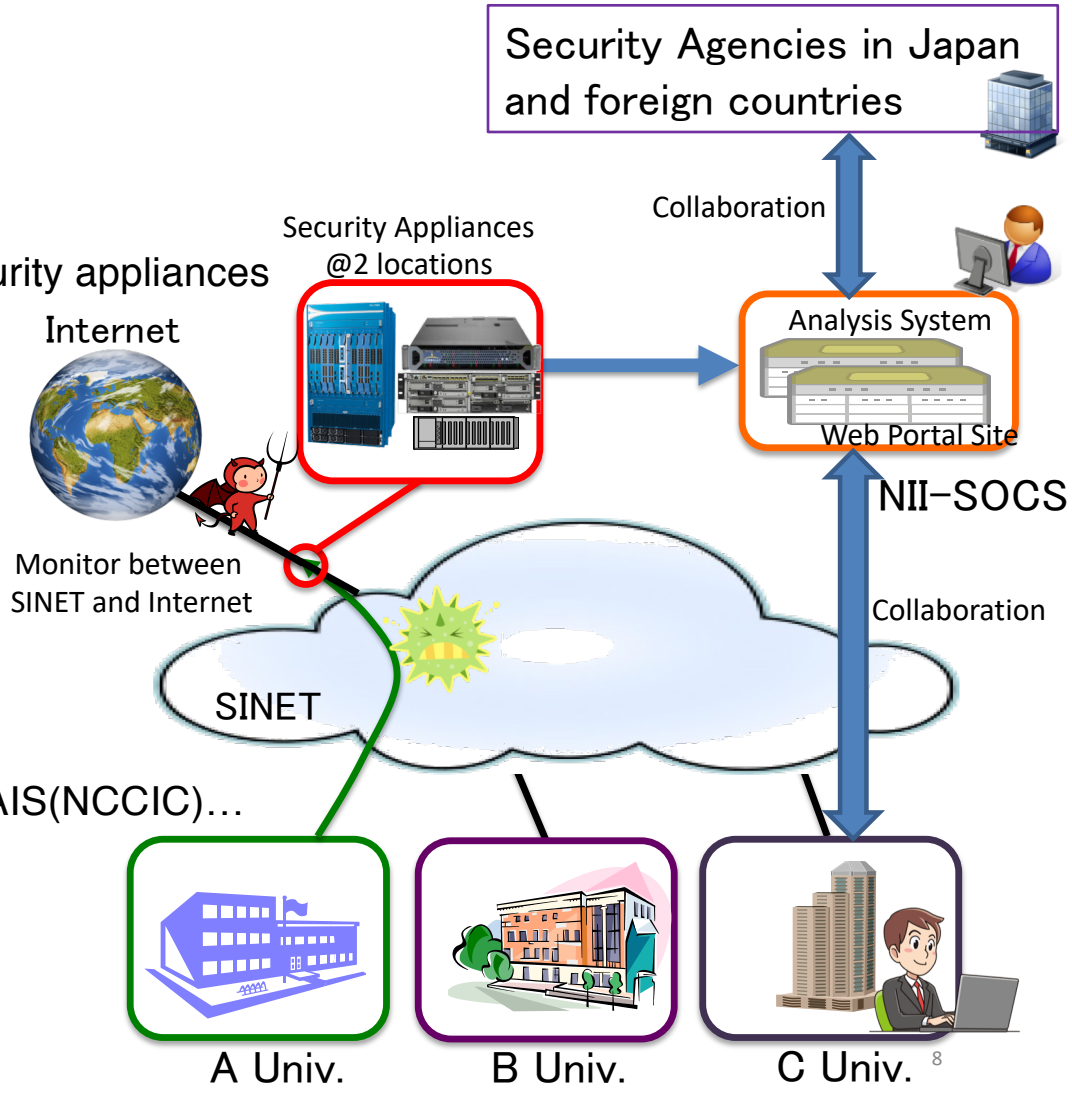
NII-SOCS provides education and training on cybersecurity by OJT

- Japanese gov. will require all national universities
  - Ability for cybersecurity management
    - Not incident response capability
- CISO should have ability as a coordinator
  - Act as a commander
    - Gives proper command to department
    - Negotiates with external companies, e.g., forensics
- CSIRT should support CISO
  - Act as an advisor
    - Provides several countermeasure candidates with pros/cons.
    - Also supports incident response and recovery
- Our goal
  - cultivate management capability for cybersecurity
  - not train security engineers



Basic Concept of NII-SOCS

- About 7M USD/year
  - 102 national universities
  - NII-SOCS (24/365)
    - Investigates alerts and sessions from security appliances
      - 171k alert/day, 860M session/day
    - Notifies dangerous alerts to universities
    - Provide advice for further investigation
    - Collaboration with security agencies
  - 4 types of security appliances
    - Paloalto: IDS with sandbox
    - Cisco FirePower: Signature-based IDS
    - Damballa CSP: DNS query investigation
    - LookingGlass: Reputation, e.g., ETPRO, AIS(NCCIC)…
- Analysis System and Web portals
  - Elasticsearch+Kibana, Splunk

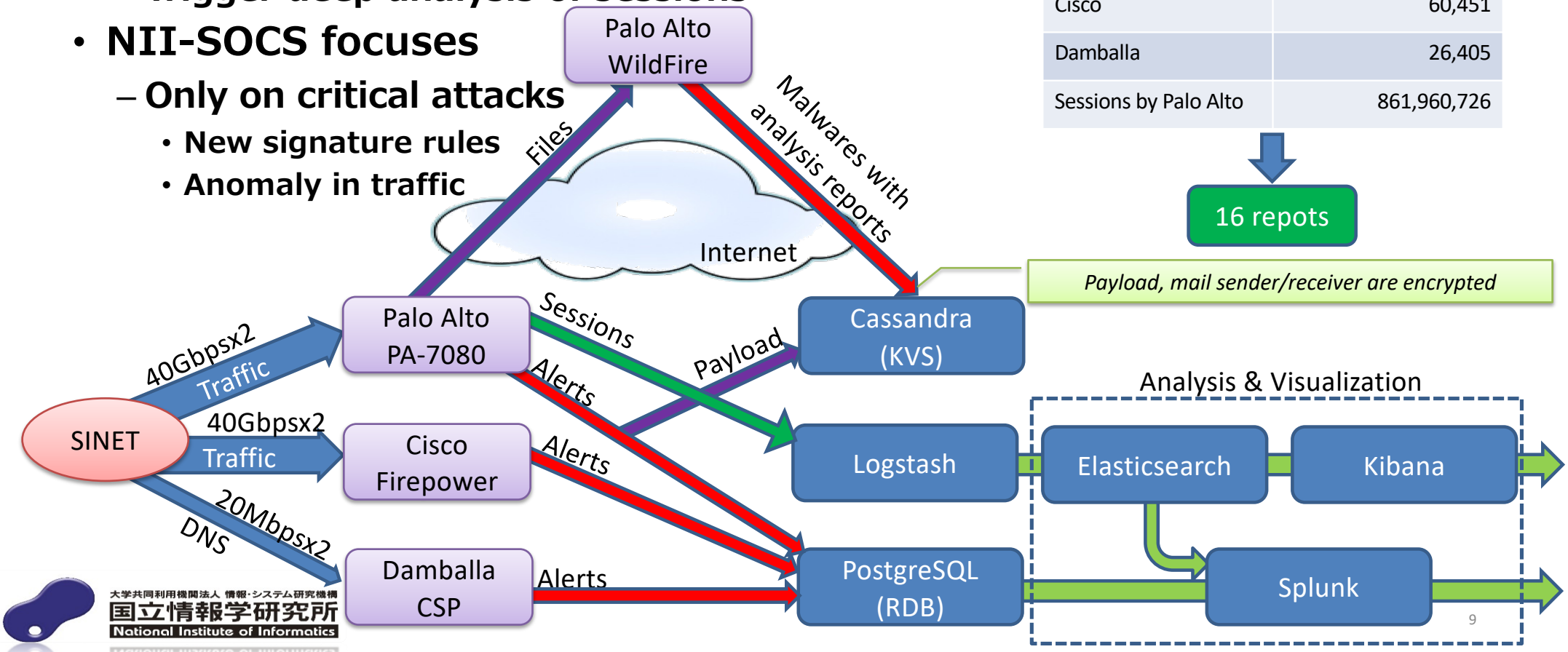


Basic Flow of Alert/Session Analysis

- **Brief analysis of alerts and sessions**
- **Indicator information**
  - **Trigger deep analysis of sessions**
- **NII-SOCS focuses**
  - **Only on critical attacks**
    - **New signature rules**
    - **Anomaly in traffic**

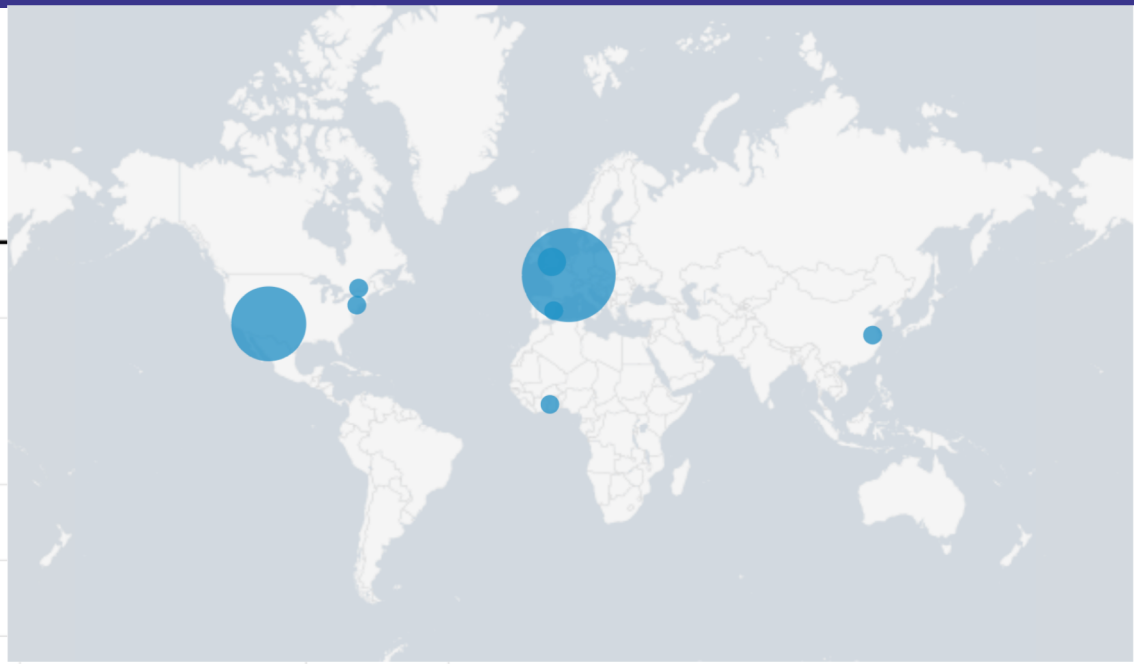
Daily statistics (average)

Sensors	# of alerts/sessions
Palo Alto	84,976
Cisco	60,451
Damballa	26,405
Sessions by Palo Alto	861,960,726



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

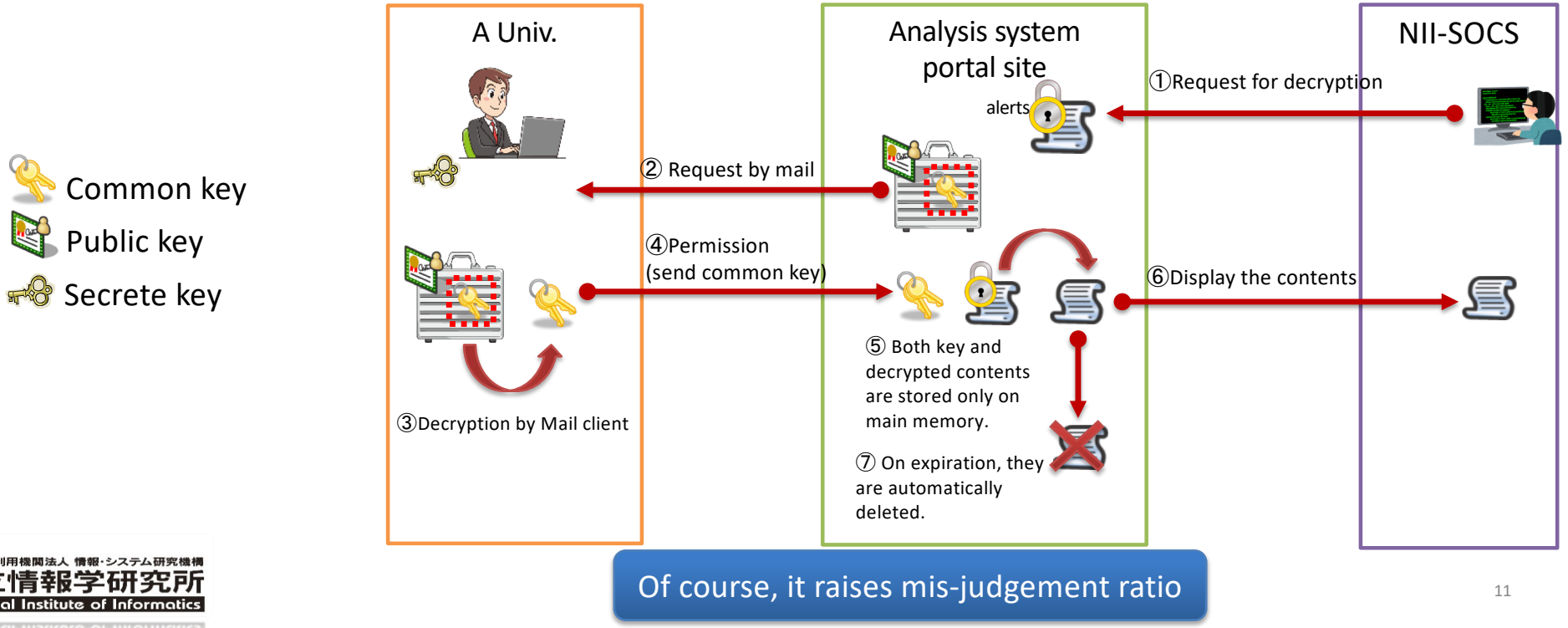
Example of Analysis



capture_time	source_ip	duration	concurrency	City	Country			
2019-04-18 06:41:10.255 2019-04-18 06:46:46.075	7.166	335.82	11	Paris	France			
2019-04-18 23:48:57.268 2019-04-18 23:51:47.804 2019-04-18 23:51:50.31 2019-04-18 23:52:46.389 2019-04-18 23:52:48.692		231.424	8		France			
2019-04-18 07:25:08.639 2019-04-18 07:27:13.298	153	124.659	12	Walnut	United States			
2019-04-18 01:49:17.555 2019-04-18 01:57:14.052	).60	476.497	7	Provo	United States			
2019-04-18 04:51:32.017 2019-04-18 04:51:42.83 2019-04-18 04:51:43.531	228	11.514	6		Ghana	19	14	1
2019-04-18 16:04:19.496 2019-04-18 16:04:20.097 2019-04-18 16:10:04.075 2019-04-18 16:10:04.275	3.62	344.779	17		Ukraine	18	8	1
2019-04-18 01:43:19.711 2019-04-18 01:43:39.536 2019-04-18 01:51:13.301	5.82	473.59	8	Algemesi	Spain	17	15	1

Consideration on secrecy of communication

- NII-SOCS
  - Security alerts may contain a part of contents of communication.
  - The contents are automatically encrypted by a common key and stored in DB.
  - The common key in DB is encrypted by university's public key.
    - Common key is replaced periodically (1 week - 1 month).



Of course, it raises mis-judgement ratio

We need pay attention to sessions

- **Many malwares start to use**
  - **encrypted communication, 21.44% in May 2017[1]**
  - **https, 37% in June 2017[2]**
- **C2 servers use**
  - **Well-known cloud services**
  - **Compromised company's web servers**
- **Also they use**
  - **Anonymized communication**
    - **VPN, open proxy, onion routing…**
- **Malware infection**
  - **Mostly occurs outside universities**
    - **NII-SOCS observes "patients" who have already show symptoms**
- **If we find many incident simultaneously**
  - **We have to assign priority to take countermeasure against them.**
    - **Effectively use the limited resources, e.g., personnel, sensors…**

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

(1) https://blogs.cisco.com/security/detecting-encrypted-malware-traffic-without-decryption
(2) https://www.cyren.com/blog/articles/over-one-third-of-malware-uses-https

Example (1)

Onion routing protocol seems to piggyback on SMTP server

src IP	dst IP	Application	src port	dst port	protocol	bytes sent	bytes received	packets sent	packets received
B.B.B.170	A.A.A.74	incomplete	54034	25	tcp	573	0	8	0
E.E.E.142	A.A.A.74	incomplete	53006	25	tcp	306	0	5	0
B.B.B.170	A.A.A.74	incomplete	54087	25	tcp	573	0	8	0
B.B.B.170	A.A.A.74	incomplete	54110	25	tcp	573	0	8	0
A.A.A.74	G.G.G.235	incomplete	62127	25	tcp	10179	0	23	0
A.A.A.74	H.H.H.26	incomplete	2843	25	tcp	19097	0	29	0
C.C.C.75	A.A.A.74	smtp	2742	25	tcp	608	1012	9	13
D.D.D.39	A.A.A.74	incomplete	16068	22	tcp	60	0	1	0
F.F.F.179	A.A.A.74	incomplete	18891	23	tcp	60	0	1	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	J.J.J.29	smtp	55684	25	tcp	13693	1606	25	17
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

A.A.A.74 SMTP server in an university

incomplete One way communication by malware

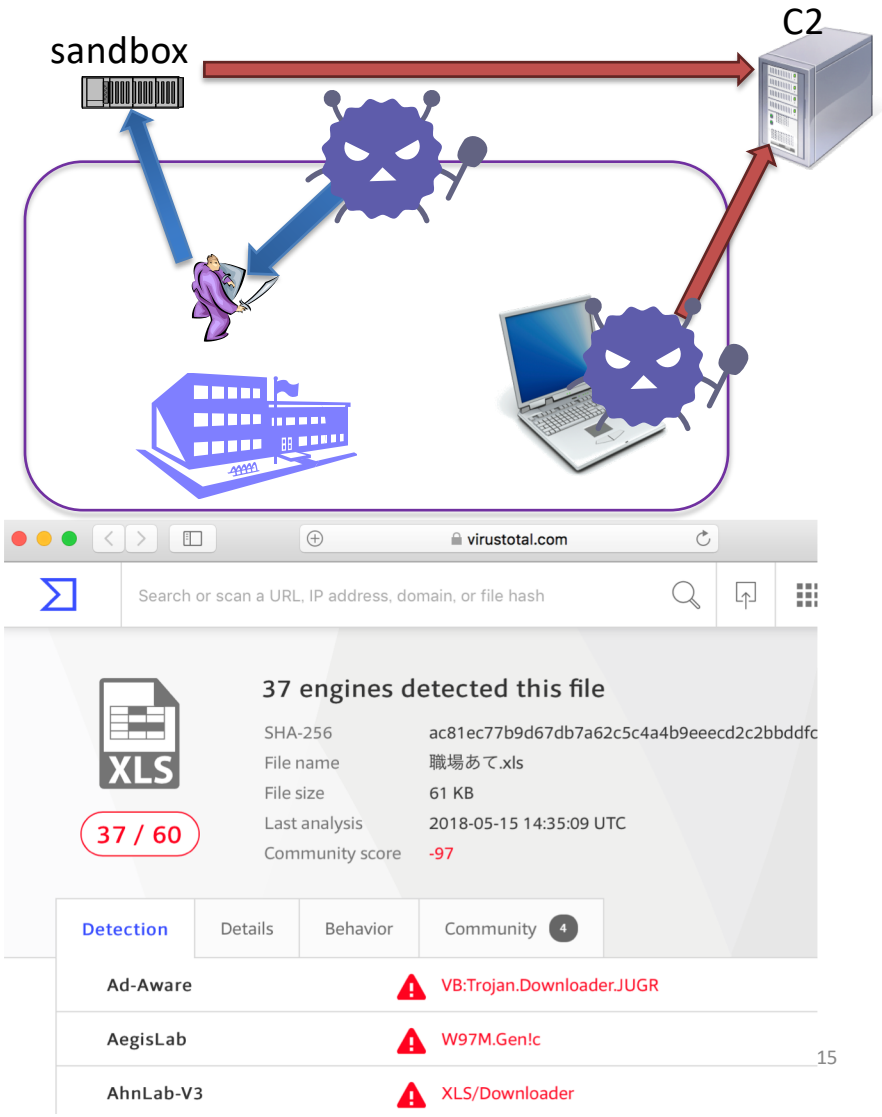
Example (2)

- **Prioritization on incident response**
  - **The most serious victim should be treated first.**

Date	Src IP	Dst IP	Src Port	Dst Port	Protocol	Sent(byte)	Rec. (byte)	Src Country	Dst Country
2018/5/◯ 09:19:28	A.B.C.D	W.X.Y.Z	49940	80	tcp	2283	353460	Japan	Russian Federation
2018/5/◯ 18:26:14	E.F.G.H	W.X.Y.Z	64464	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 19:07:37	E.F.G.H	W.X.Y.Z	50368	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 16:53:14	E.F.G.H	W.X.Y.Z	58072	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 17:45:15	E.F.G.H	W.X.Y.Z	61838	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 18:15:39	E.F.G.H	W.X.Y.Z	64279	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 19:59:12	E.F.G.H	W.X.Y.Z	53316	80	tcp	1154	23532	Japan	Russian Federation
2018/5/◯ 16:41:48	E.F.G.H	W.X.Y.Z	57399	80	tcp	307	14466	Japan	Russian Federation
2018/5/◯ 18:04:36	I.J.K.L	W.X.Y.Z	63829	80	tcp	307	14466	Japan	Russian Federation
2018/5/◯ 19:37:44	I.J.K.L	W.X.Y.Z	52110	80	tcp	307	14466	Japan	Russian Federation

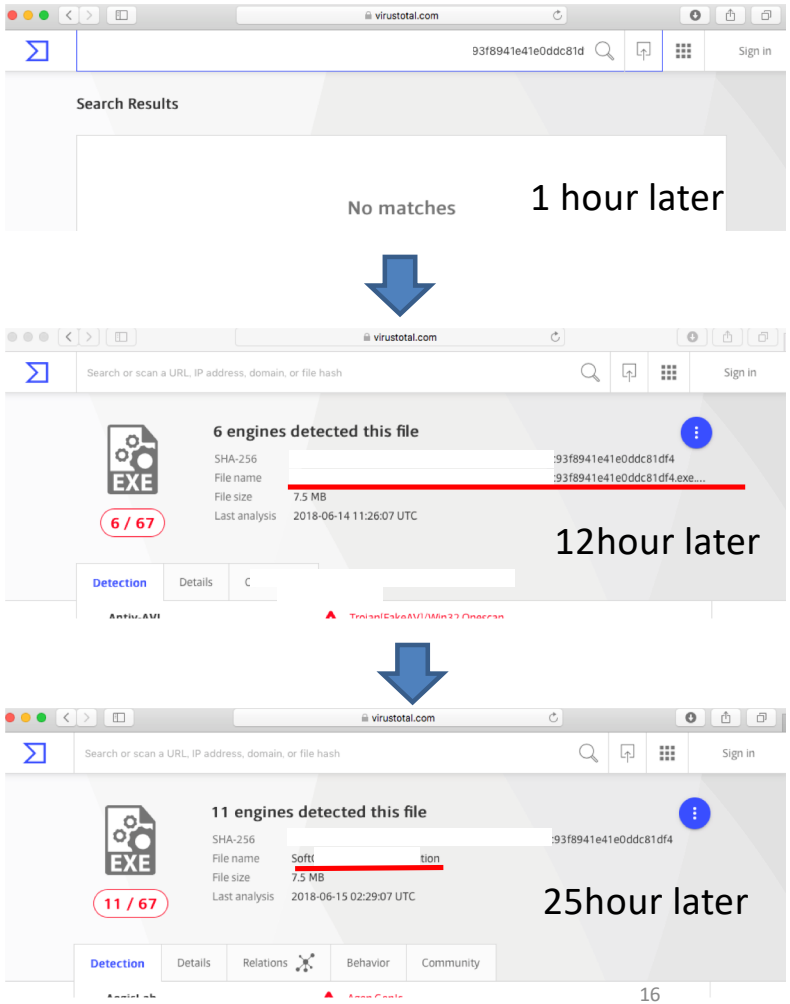
Example (3)

- Almost all malware infections
  - Occur outside universities
    - E.g., home, hotel, mobile environment
  - We cannot detect the initial step of the infections
- We analyze malware
  - By sandbox
    - Trace their behavior
      - Access pattern
        - » Download activity
      - Suspicious DNS query
  - Information sharing with universities
- We can trace suspicious activities
- Therefore we need to analyze sessions.



Example (4)

- **Targeted Attack**
  - Several professors received malicious mails
- **NII's sandbox detected the file**
  - During 1-3 hours, no AV could detect the file
    - We cannot not submit the file to VirusTotal.
- **12 hours, 25 hours…**
  - Several AV can detect the file
    - Sample file must be submitted for generating detection pattern
      - Who did submit the file?
- **From the result we judge the seriousness of the malware**



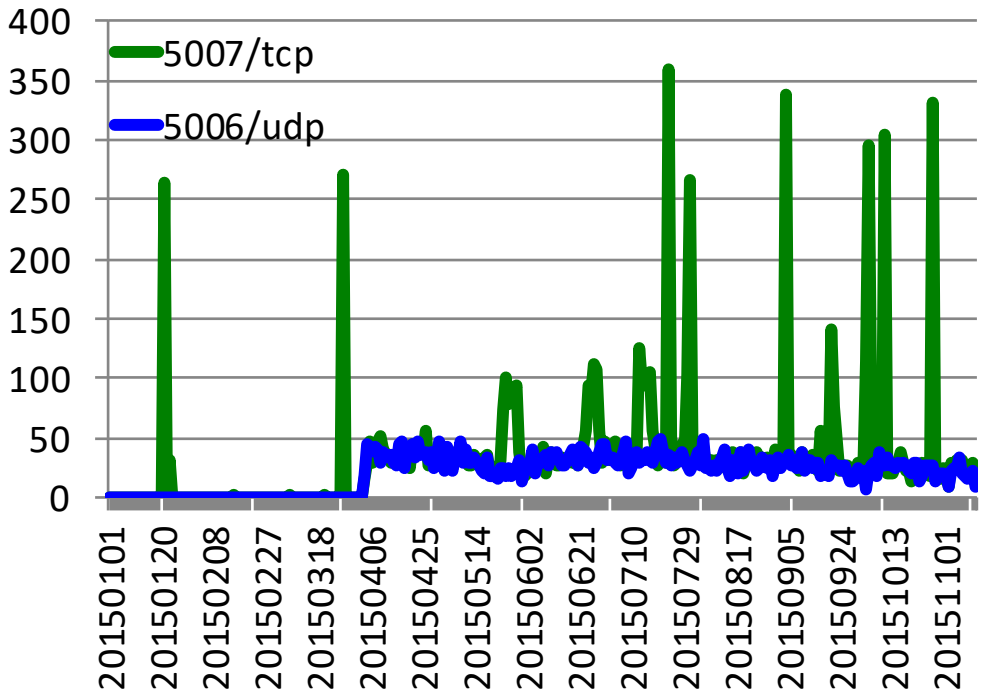
Trace Several Activities

- **Monitor accesses to sinkholes**
- **Monitor scan activities**
  - **By Shodan, Rapid7,…**
    - **Mainly focus on the change of their scan behavior**

Why do they want to find…

↓

IoT devices?

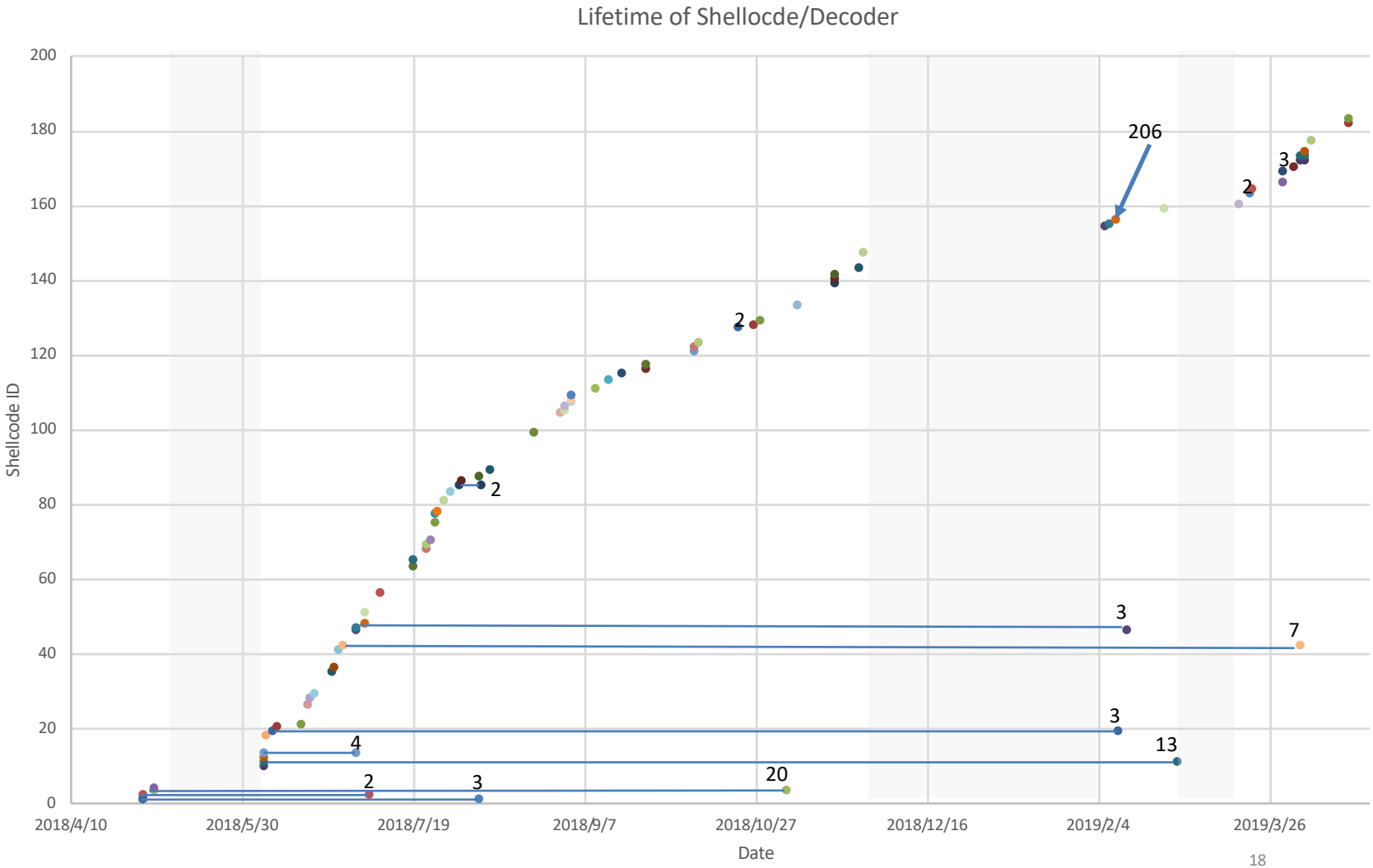


Port/Protocol	Count
81/tcp	639317
102/tcp	638848
444/tcp	637993
2222/tcp	637040
82/tcp	636701
9000/tcp	636534
6666/tcp	636482
80/tcp	358167
443/tcp	351648
53/udp	345561
8080/tcp	324982
3749/tcp	320330
25/tcp	320149
4782/tcp	320007

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

We also trace shellcodes and decoders used by remote attacks

- **Target CPUs**
  - AMD(x64)
  - AMD(x32)
  - IA32
  - MIPS
  - PPC
  - SPARC
- **Generate custom signature form frequently used codes**
  - **If no IDS alert, zero-day attack can be detected.**



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Information Sharing

- **NII-SOCS**
  - collects various types of information
    - from DarkWeb, SNS, Information exposure…
  - receives various types of indicator information
    - from JPCERT/CC, NISC, security venders in the world
      - Indirectly from foreign governments
  - receives the analysis report from universities
    - Malware: name, hash value, behavior
    - Suspicious domain name
    - Countermeasure: detection & containment
- **These kinds of information**
  - summarized
  - provided to universities
    - NII-SOCS acts as a hub of Academic ISAC among national universities.

NISC: National center for Incident response and Strategy for Cybersecurity

Benchmark Data and Malware Samples to Universities

- Alert and session information
  - Open to public
    - Sanitized IP addresses and timestamps
    - Hash value of encrypted contents which are included alerts
    - In accordance with KyotoData2006+ benchmark
      - which has been adopted by various research papers.
      - 1 hour data…2GB/day
- Malware samples
  - Universities which participate to NII-SOCS
    - Provided based on NDA and the regulation of Wassenaar Arrangement
      - Malware files
      - Analysis reports by our sandbox
- To stimulate research activity on cyber security

Conclusion

- **NII-SOCS**
  - **Encourages universities to realize secure networks**
  - **Shares cyber attack information with its risk level**
  - **Focus only on high risk attacks**
    - **Deep analysis of alerts and sessions**
  - **Trace suspicious activities to realize early warning**
    - **Sinkholes, scans, shellcode/decoder**
  - **Provide benchmark data for research community**
    - **Extension of Kyoto2016 for all researchers**
    - **Malware information for NII-SOCS members**