.jp's actions to cope with Kaminsky attack threats

Nov 5, 2008
ICANN Cairo ccNSO meeting

Shinta Sato
Japan Registry Services Co., Ltd.

Outline of JP domain

- .JP Domain Names
  - 1,054,356 registered domain names (2008 Nov 1)
  - Local presence required
- .JP Nameservers
  - Serve .JP zone and 300+ in-addr.arpa zones
    (except c.dns.jp, which only has .JP zone)
  - Serve about 1.5 billion queries per day

NS	IPv4	IPv6	Operator	Anycast
a.dns.jp	203.119.1.1	2001:dc4::1	JPRS	BGP anycast
b.dns.jp	202.12.30.131	Coming soon	JPNIC	N/A
c.dns.jp	204.74.112.245	2001:502:d399::245	JPRS	BGP anycast
d.dns.jp	210.138.175.244	2001:240::53	IIJ	IGP anycast
e.dns.jp	192.50.43.53	2001:200:c000::35	WIDE	BGP anycast
f.dns.jp	150.100.2.3	2001:2f8:0:100::153	SINET	N/A
g.dns.jp	203.119.40.1	-	JPRS	N/A

DNS related organizations/activities in Japan

- Organizations:
  - JPRS (Japan Registry Services)
    - http://jprs.jp/
    - .JP registry
  - JPNIC (Japan Network Information Center)
    - http://www.nic.ad.jp/
    - NIR of Japan
  - JPCERT/CC
    (Japan Computer Emergency Response Team Coordination Center)
    - http://www.jpcert.or.jp/
  - JAIPA (Japan Internet Providers Association)
    - http://www.jaipa.or.jp/
    - 180+ company members
- Users Groups
  - JANOG (Japan Network Operators' Group)
    - http://www.janog.gr.jp/
    - 5,500+ mailing-list members
  - DNSOPS.JP (DNS Operators' Group, Japan)
    - http://dnsops.jp/
    - 1,400+ mailing-list members

Brief summary of Kaminsky Attack

- New threats of DNS cache poisoning
  - Attacks are initiated without using exact target name
    - Ex. Use 001.example.jp instead of www.example.jp
  - Long TTL cannot protect the cache
    - Some implementation overrides the old data
  - See detailed explanations on the web
- How to protect the cache servers?
  - Apply the patches!!!
    - Many developers released source port randomization patch to decrease the possibility of the attacks
  - Discard queries from unwanted clients
    - Open recursive servers are troublesome in many cases

What has JPRS done

- Spread out the information to Japanese Internet users
  - Published immediate announcements on the web
    - http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html
    - http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning-update.html
  - Posted urgent announcements to the mailing lists
    - JANOG, DNSOPS.JP
  - Reported technical details
    - http://jpinfo.jp/topics-column/009.pdf

- Called registrars' attention to the vulnerability
  - At Technical Seminar for the registrars (23 July, 2008)

- Made analysis of the queries at a.dns.jp
  - To measure the progress of the patch applications
    - https://www.dns-oarc.net/files/workshop-2008/izuru.pdf
  - Created a list of hosts which are considered to be vulnerable

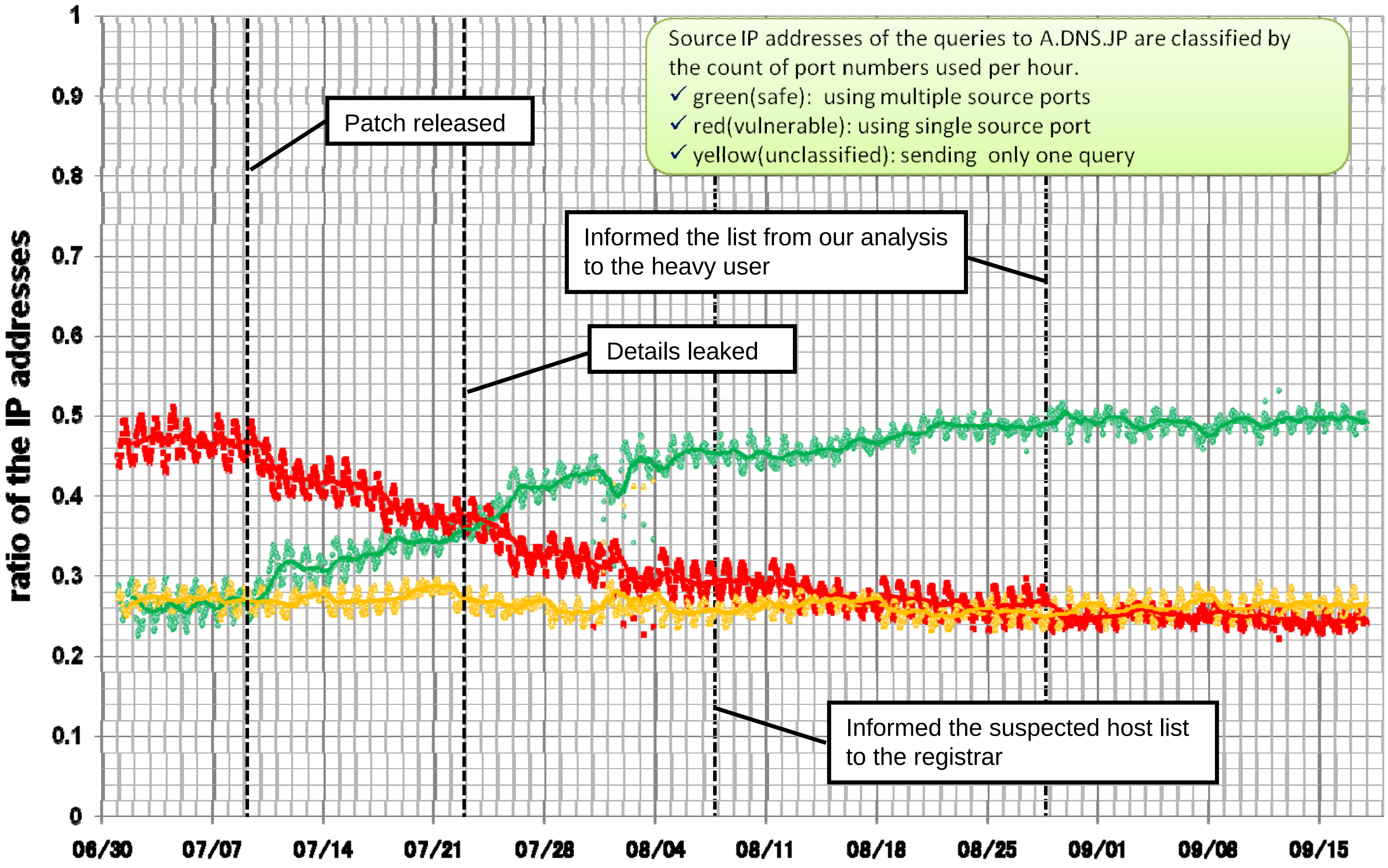
Actions with Related Organizations

- Cooperated with JPCERT/CC and JPNIC in raising awareness of the issue
  - Made collaborative announcements
  - Made specific announcements to their area of specialties
  - Suspected hosts were informed to the parties operating such hosts
    - data from JPCERT/CC
    - informed by JPRS and JPNIC
    - via registrars and IP address management agents
- Talked with large ISPs in Japan
  - Some registrars are also large ISPs
  - Through registry-registrar administrative channel
  - Using the list of suspected hosts known by a.dns.jp measurement
- Worked with JAIPA
  - Asked to distribute the announcements among JAIPA members
- Co-worked with closed security groups in Japan

Response from the field

- Internet news media
  - Many articles related to this threat were initiated by our announcements
- Internet community
  - JANOG ML
    - Was used to spread the announcements
    - Not so many discussions there
  - DNSOPS.JP ML
    - Some members had discussions
    - Information exchange among users had been done
- Other mass media
  - TV news by NHK (Japan’s sole public broadcaster)
  - Many articles are written in Internet related magazines

detected Safe/Vulnerable/Unclassified clients



Source IP addresses of the queries to A.DNS.JP are classified by the count of port numbers used per hour.
- ✓ green(safe): using multiple source ports
- ✓ red(vulnerable): using single source port
- ✓ yellow(unclassified): sending only one query

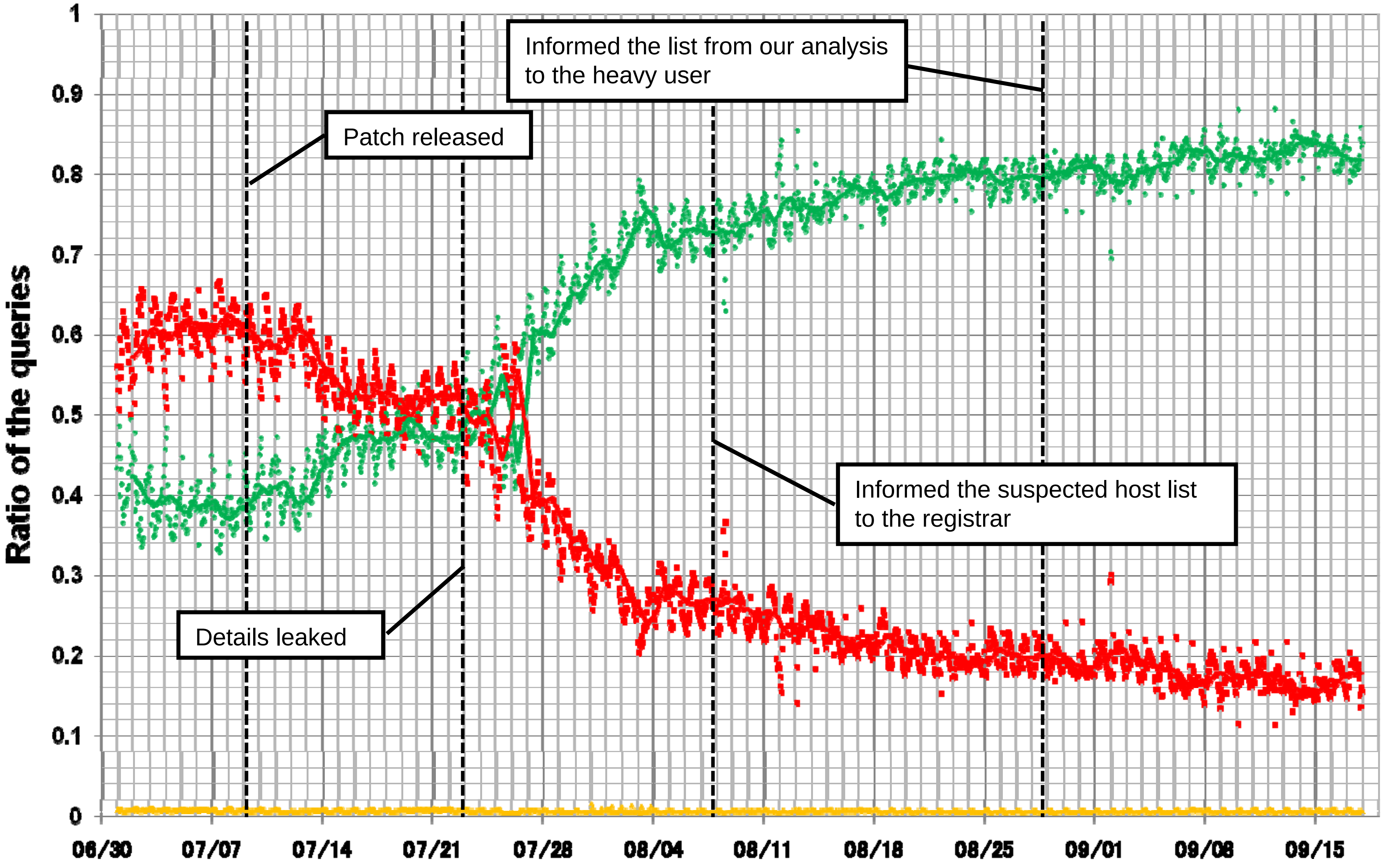
Patch released

Details leaked

Informed the list from our analysis to the heavy user

Informed the suspected host list to the registrar

detected queries from the Safe/Vulnerable/Unclassified clients



Patch released

Details leaked

Informed the list from our analysis to the heavy user

Informed the suspected host list to the registrar

What we’ve learned

- ISPs cannot apply patches immediately
  - Tend to spend time in investigating the side effects
- Operators need official announcements from somewhat related authorities
  - To convince their boss for taking an emergency patch action
  - JPRS actions along with JPNIC and JPCERT/CC were good support for them
  - Translation from English information needed
- Old announcements and presentations of the cache poisoning was reused and referred to by users
  - Keeping these kind of works and outputs to the community are important
  - JPRS is expected to act as DNS authority in Japan
- Communications between related parties/communities are important
  - On regular basis
  - Registrars, ISPs, CERT, media and so on
- 25% of the cache servers are still not protected

- Activities in your country?