Cyber Security Incident Trends in Japan

JPCERT/CC

Yukako Uchida / Shoko Nakai

JPCERT/CC is…

- The first CSIRT in Japan with 20+ years of experience (Founded in October, 1996)

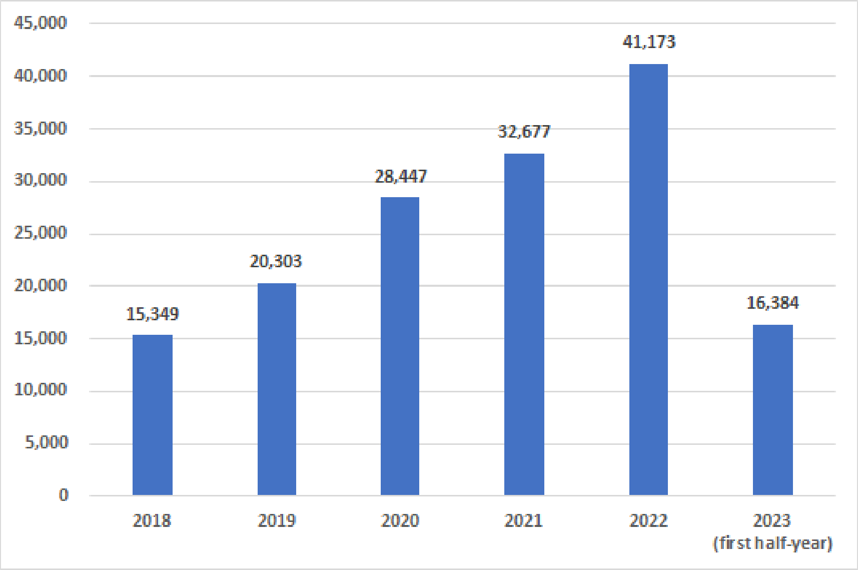
- A non-profit, non-governmental, and independent organization

- A national CSIRT of Japan
  - Funded by METI (Ministry of Economy, Trade and Industry)
  - Assigned as a **vulnerability handling organization** by METI

Number of incident reports (2018-2023)

- 16,384 reports have been received in the first half of 2023, showing a slight decrease compared to the same period in 2022.

- The number of incident reports continue to increase. We expect around the same or a fewer volume of events for 2023.

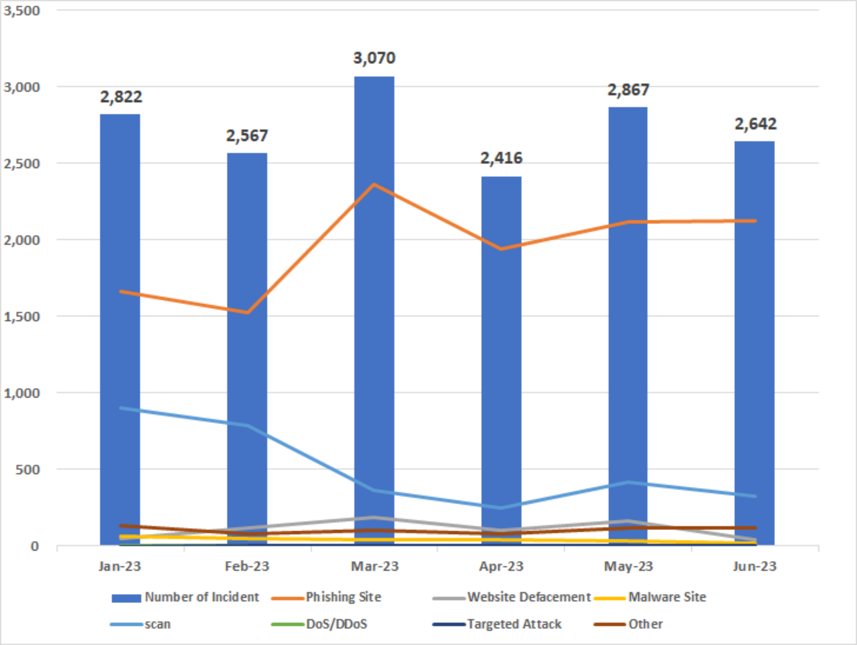


Incident breakdown in the first half 2023

- About 2,500 to 3,000 cases of incidents are handled each month.

- Phishing sites is the major incidents handled, followed by scan.

- The reports on phishing site remarkably increased in March.



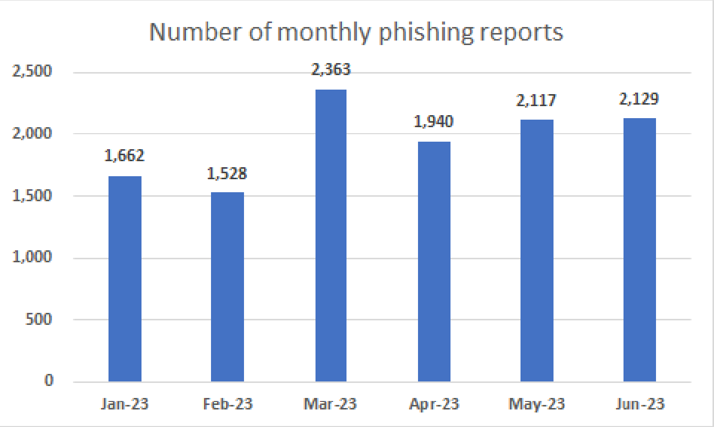
Incident cases

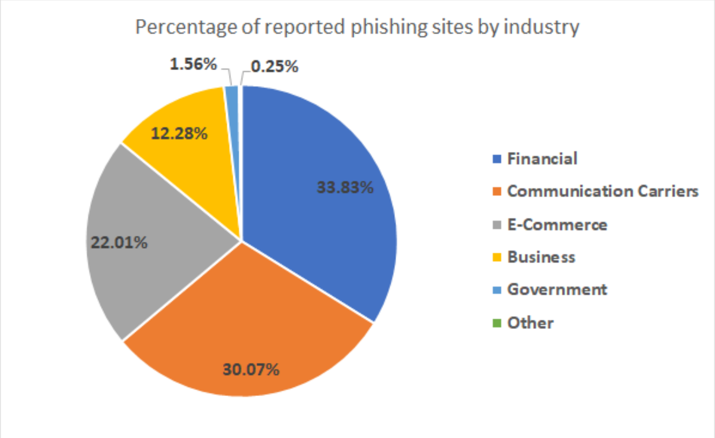
1） PHISHING SITE TRENDS
2） DNS WATER TORTURE ATTACKS

Phishing site trends in the first half 2023

- We receive about 2,000 reports on phishing sites.

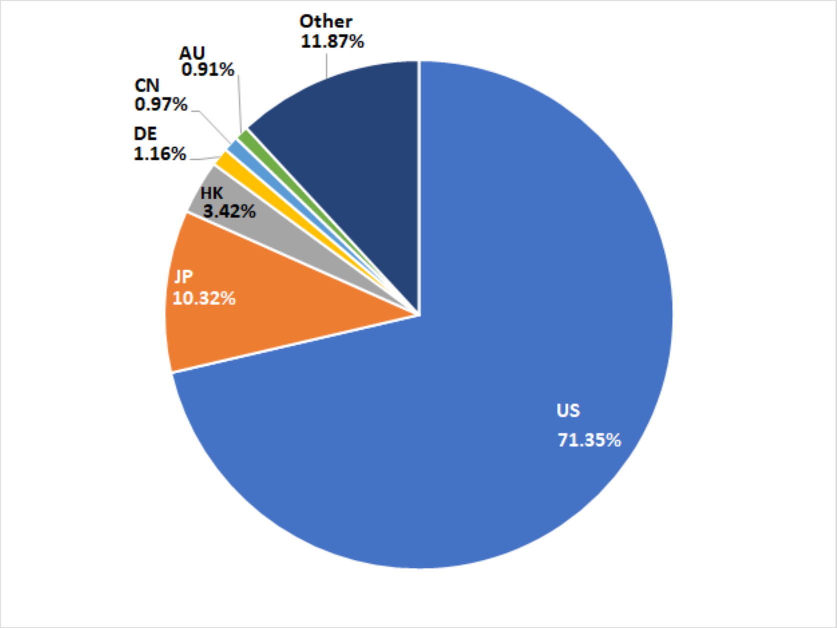
- Financial sector has been widely affected, and the brand/services impersonated keep changing each month.


Number of monthly phishing reports

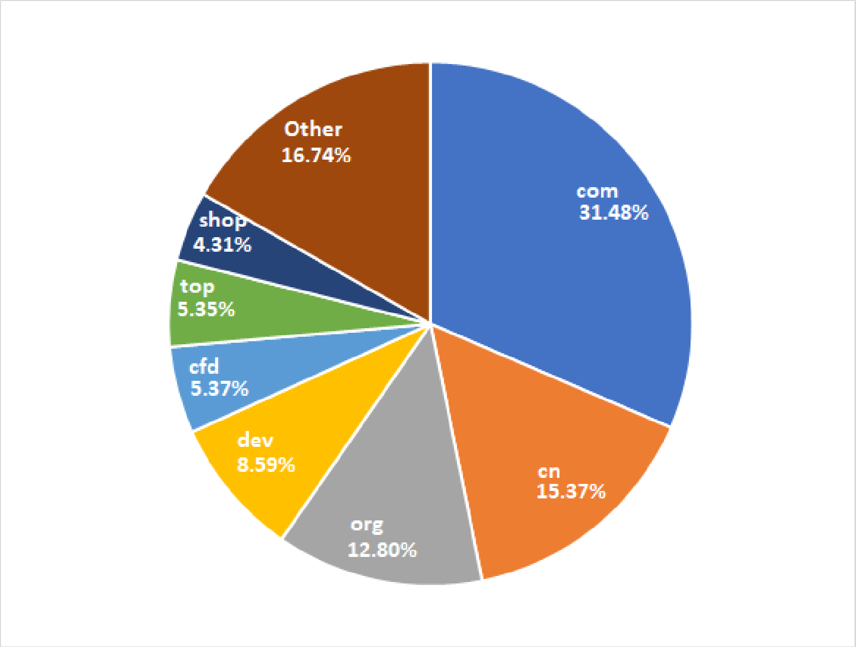

Percentage of reported phishing sites by industry

IP addresses and domains used for phishing sites

- Countries associated with IP addresses linked to phishing sites



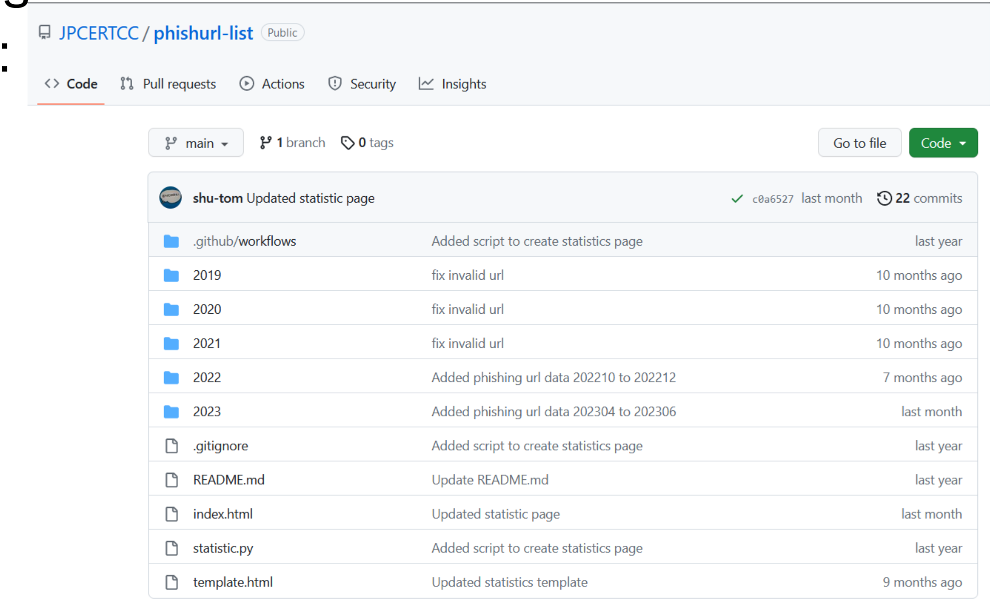
- Top Level Domain (TLD) based on phishing sites’ FQDN



Phishing URL dataset from JPCERT/CC

- JPCERT/CC publishes the details of reported phishing sites on the GitHub repository below:

Phishing URL dataset from JPCERT/CC
https://github.com/JPCERTCC/phishurl-list/



shu-tom Updated statistic page ✓ c0a6527 last month 22 commits

.github/workflows	Added script to create statistics page	last year
2019	fix invalid url	10 months ago
2020	fix invalid url	10 months ago
2021	fix invalid url	10 months ago
2022	Added phishing url data 202210 to 202212	7 months ago
2023	Added phishing url data 202304 to 202306	last month
.gitignore	Added script to create statistics page	last year
README.md	Update README.md	last year
index.html	Updated statistic page	last month
statistic.py	Added script to create statistics page	last year
template.html	Updated statistics template	9 months ago

DNS Water Torture Attack

- We are observing DNS water torture attacks (random subdomain attacks) from mid-March 2023.
  - JPCERT/CC domain was also targeted

Parts of attack details targeting JPCERT/CC domain

```
2023-07-08 21:46:53.570989 IP SourceOfAttack.39636 > OpenResolver.53: 19199+ A? amur.jpcert.or.jp. (35)
2023-07-08 21:46:55.153998 IP SourceOfAttack.39636 > OpenResolver.53: 52204+ A? chickadee.jpcert.or.jp. (40)
2023-07-08 21:47:00.651903 IP SourceOfAttack.39636 > OpenResolver.53: 9206+ A? cycle1.jpcert.or.jp. (37)
2023-07-08 21:47:02.548646 IP SourceOfAttack.39636 > OpenResolver.53: 11887+ A? mosaffa.jpcert.or.jp. (38)
2023-07-08 21:47:05.370698 IP SourceOfAttack.39636 > OpenResolver.53: 18118+ A? sokolova-nina.jpcert.or.jp. (44)
```

- Open resolvers are leveraged to carry out these attacks.

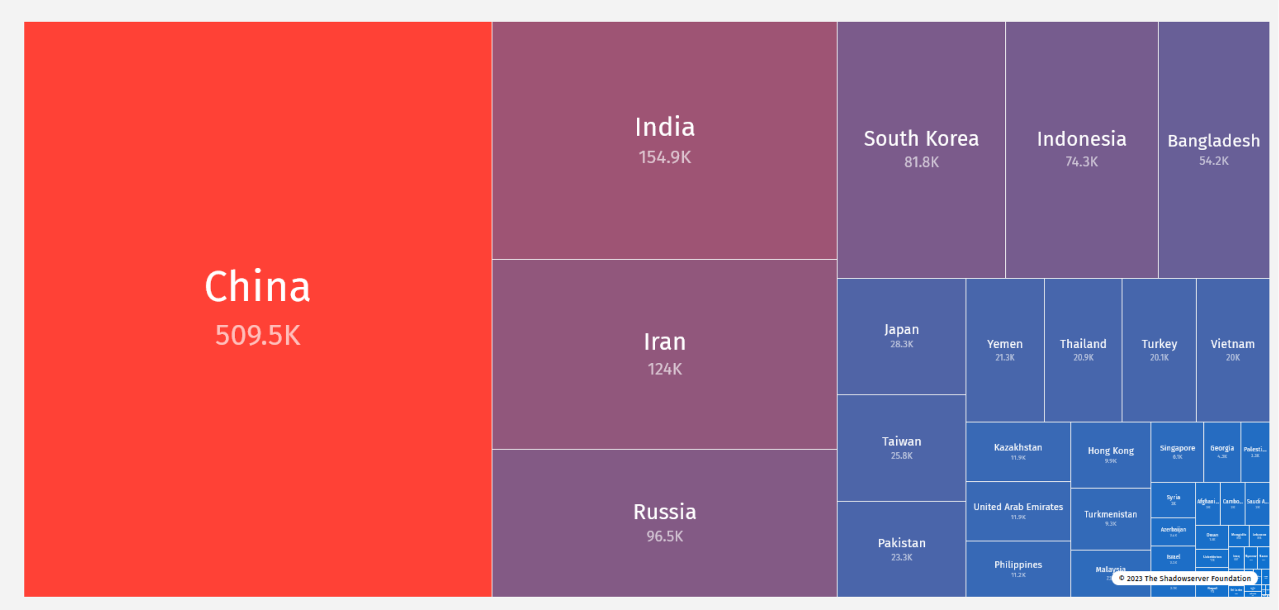
DNS Water Torture Attacks in Japan

- Several municipalities’ website have been attacked and resulted in temporary suspension
  - Impact: Website inaccessible
  - Duration: 1 to few hours

Date/Time	Duration (approx.)	Target	Target domain
2023/04/21 22:00 – 28:00	6 hours	Japan Railways	jr-odekake.net
2023/04/27 06:40 – 07:40	1 hour	JPCERT/CC	jpcert.or.jp
2023/04/28 15:30 – 21:30	6 hours	Kagoshima Prefecture	pref.kagoshima.jp.
2023/04/29 05:00 – 12:00	7 hour	Toyama Prefecture	pref.toyama.jp.
2023/04/29 20:45 – 21:45	1 hour	Kyoto Prefecture	city.uji.kyoto.jp town.wazuka.kyoto.jp etc.
2023/04/30 03:10 – 14:00	11 hours	Okinawa Prefecture	pref.okinawa.jp
2023/04/30 03:10 – 06:45	3.5 hours	Osaka Prefecture	pref.osaka.jp.
2023/05/01 14:30 – 22:15	8 hours	Navi Time (travel guide)	navitime.biz

Open Resolvers in Asia

- There are many open resolvers running in China, followed by India and Iran. Japan is in the 8th place, according to ShadowServer’s data. (As of 21 August 2023)



Reference：SHADOWSERVER Dashboard https://dashboard.shadowserver.org/

Publications

- **Security Alerts** https://www.jpcert.or.jp/english/at/2023.html
  - Information on widespread, emerging information security threats and their countermeasures, provided on an as-needed basis.
- **JVN – Japan Vulnerability Notes** https://jvn.jp/en/
  - Issued when necessary
- **Quarterly Report** https://www.jpcert.or.jp/english/menu_documents.html
  - Activity overview, Internet threat monitoring, incident handling
- **Blog** https://blogs.jpcert.or.jp/en/
  - JPCERT/CC activities and security trends
- **Twitter** https://twitter.com/jpcert_en
  - Blog and security alert updates
- **Github** https://github.com/JPCERTCC
  - Useful tools for incident analysis

Last but not least..

SAVE
THE
DATE
福
36TH ANNUAL
FIRST CONFERENCE
FUKUOKA
JUNE 9-14, 2024 JAPAN
BRIDGING
SECURITY
RESPONSE
GAPS

Thank you!