

DNS Abuse Techniques Matrix

~Matrix Introduction and Usage~

JPCERT Coordination Center
Incident Response Group
Shoko Nakai

What is DNS?

DNS stands for Domain Name System; a system developed to manage and operate domain names on the Internet.

- It is the most indispensable system for using the Internet.
- Just as an address to send a letter by mail, it is necessary to identify where the recipient is.

The DNS is used as an easy-to-remember Internet address.

(Reference : JPNIC <https://www.nic.ad.jp/ja/basics/beginners/dns.html>)

How DNS is used

■ When browsing websites

<https://www.jpccert.or.jp/> ➡ Complex

```
$ host www.jpccert.or.jp
www.jpccert.or.jp is an alias for d81drv6iivfiw.cloudfront.net.
d81drv6iivfiw.cloudfront.net has address 13.32.50.120
d81drv6iivfiw.cloudfront.net has address 13.32.50.45
d81drv6iivfiw.cloudfront.net has address 13.32.50.11
d81drv6iivfiw.cloudfront.net has address 13.32.50.72
```



■ When sending e-mail

TO: info@jpccert.or.jp ➡ Received at one of the following mail servers

```
jpccert.or.jp. 300 IN MX 20 mx02.jpccert.or.jp. (210.148.223.19)
jpccert.or.jp. 300 IN MX 10 mx01.jpccert.or.jp. (210.148.223.3)
```

How DNS is used

How DNS is used by attacker



Running for Phishing sites

Distribution of spam e-mails

Means of directing users to malware-infected sites

Malware's means of communication

Tools for DoS and DDoS attacks

Difficulties when responding to DNS-related incidents



Individuals have different levels of accumulated knowledge and expertise in DNS Abuse.

Few opportunities to share DNS Abuse expertise.

Miscommunication during response.

Differences in thinking about DNS abuse when collaborating with overseas operators.

Motivation for DNS Abuse Handling Documentation

If Japan doesn't have a document to refer to when dealing with DNS Abuse, then create one!

Let's document and preserve the know-how exchanged between the limited experts and businesses involved.

Let's follow the trend of DNS Abuse being discussed overseas and create an opportunity to start discussions and activities in Japan as well!

Global Trends Related to DNS Abuse

2019/10

Launch of DNS Abuse Framework
DNS Abuse Institute
(date unknown)

2020/05

Document Release
1) DNS Abuse Framework
“**Framework to Address Abuse**”

2021/03

Document Release
2) I&JPN
“**Toolkit DNS Level Action to Address Abuse**”
3) SSAC
“**SAC115**”

2022/01

Document Release
4) European Commission
“**Study on Domain Name System Abuse**”

2023

(1) Documents

Title.	Framework to Address Abuse
Organization	DNS Abuse Framework
Summary	<ul style="list-style-type: none">❑ 6 pages❑ DNS Abuse Explained in Five Categories<ul style="list-style-type: none">❑ Malware, Botnets, Phishing, Pharming, Spam (Spam is for Phishing Email distribution)❑ Views on the website content (if it has a negative impact on human life, take action)❑ Explanation of response flow for website content❑ Describes the role of trusted notifiers in the registry and registrar

(2) Documents

Title.	Toolkit DNS Level Action to Address Abuse
Organization	INTERNET & JURISDICTION POLICY NETWORK (I&JPN)
Summary	<ul style="list-style-type: none">❑ 48 pages.❑ Introduction divided into General Level and Technical Level❑ General Level<ul style="list-style-type: none">❑ Identification and communication of fraudulent content❑ Explanation of the evaluation of DNS-level responses in line with fraudulent content and the impact of such responses (LOCK, HOLD, REDIRECT, TRANSFER).❑ Technical Level<ul style="list-style-type: none">❑ Confirmation of the source of the report, evaluation of the content of the report, and explanation of the evaluation of the request❑ Explanation of the method for evaluating and determining the response process within the business❑ Mapping of DNS level support per DNS Abuse❑ DNS Abuse Workflow

(3) Documents

Title.	(SAC115) SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
Organization	ICANN Security and Stability Advisory Committee (SSAC)
Summary	<ul style="list-style-type: none">❑ 39 pages.❑ Definition of DNS Abuse and Website Content<ul style="list-style-type: none">❑ See The Framework to Address Abuse❑ Appropriate timing, response flow, and escalation in abuse response❑ About Evidence of Abuse<ul style="list-style-type: none">❑ Website screenshot (phishing, etc.)❑ MX records/ A, AAAA DNS records❑ Malware behavior (botnets, ransomware, etc.)❑ DNS Abuse Contact Information❑ Appendix: (DNS ecosystem, supported operators, related organization groups)

(4) Documents

Title.	Study on Domain Name System (DNS) abuse
Organization	European Commission
Summary	<ul style="list-style-type: none">❑ 173 pages❑ Domain space market, DNS ecosystem overview❑ Definition of DNS Abuse <p>Focus on the following three areas as Abuse</p> <ol style="list-style-type: none">1. Incidents with fraudulently registered domains2. Events in DNS operation3. Events related to website content (including unauthorized registration and infringing domains) <ul style="list-style-type: none">❑ DNS Abuse Damage (summary including hearings)❑ The Impact of IoT and 5G on DNS Abuse❑ Regulatory Framework for DNS Abuse<ul style="list-style-type: none">❑ World Level (EU, ICANN, etc.)❑ Community (I&JPN, DNS Abuse Framework, etc.)❑ Examples of measures in TLDs (gTLDs, ccTLDs)❑ Summary of Solutions for DNS Abuse

Steps to Completion

Scrutiny of overseas documents.



Translate into Japanese.



Japanese-language documents are checked within DNS operators and related parties.



Document Completed.

Completion and publication of a Japanese version DNS Abuse Techniques Matrix.

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix

4

Case Study

5

Concerns

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix

4

Case Study

5

Concerns

What is the Japanese version DNS Abuse Techniques Matrix?

■ Japanese translation of the document "**DNS Abuse Techniques Matrix**" published by the FIRST DNS Abuse SIG in 2023.

2019/10

Launch of DNS Abuse Framework
DNS Abuse Institute
(Inception date unknown)

2020/05

Document Release
1) DNS Abuse Framework
"Framework to Address Abuse"

2021/03

Document Release
2) I&JPN "Toolkit DNS Level Action to Address Abuse"
3) SSAC "SAC115"

2022/01

Document Release
4) European Commission "Study on Domain Name System Abuse"

2023

Documentation released
FIRST
DNS Abuse SIG
DNS Abuse Techniques Matrix

Features

While previous DNS abuse-related documents are often grouped together under the general categories of phishing, DDoS, etc., the actual factors and areas that need to be addressed are much more detailed.

- General categories classified by incident
 - phishing
 - defacement
 - DDoS
 - spam (unsolicited email messages)

Features

■ For example, phishing

Phishing is the act of using a real organization to fraudulently obtain personal information such as usernames, passwords, etc.

(Reference : Council of Anti-Phishing Japan https://www.antiphishing.jp/consumer/abt_phishing.html)

Many techniques are involved to carry out the phishing activities and acquire their objectives.

■ Possible methods/techniques

- Registration of malicious domains
- Registration of malicious subdomains
- Web server and content preparation
- Inducement by rewriting DNS information
- Prepare domain for phishing e-mails
- Sending spoofed e-mails

What is the Features of DNS Abuse Techniques Matrix?

Focusing on techniques rather than categories.

- Provide advice to incident response teams responding to incidents involving DNS abuse.
- Aim to complement existing efforts in DNS abuse investigation and research.

not covered (by)

Other techniques used in parallel with attacks involving the DNS.

- BGP Hijacking
- Things like TLS certificate spoofing

Scope related to the abuse of the DNS by malware.

- It does not cover, for example, dealing with malware used to generate DGA domains.

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix

4

Case Study

5

Concerns

Document Structure

22 pages (a volume that can be easily read)

■ Explanation of Terms

- Stakeholders
- Techniques
- Actions
 - detect
 - mitigate
 - prevent

■ Examples of Techniques

■ Abuse Matrix



Explanation of Terms

Stakeholders	<ul style="list-style-type: none">• 15 related businesses, organizations, and people• Description of each stakeholder is provided.
Techniques	<ul style="list-style-type: none">• 21 different techniques• Description of each technique is provided.
Actions	<p>Listed in 3 patterns of actions for each phase</p> <ul style="list-style-type: none">• Detect• Mitigate• Prevent

Explanation of Terms: Stakeholders

15 related businesses, organizations, and people

Registrars	Registries	Authoritative Operators
Domain name resellers	Recursive Operators	Network Operators
Application Service Provider	Hosting Provider	Threat Intelligence Provider
Device, OS, & Application Software Developers	Domain Registrants	End User
Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident Responder

Description of stakeholders (partial introduction)

- Registrars - an organization that allows registration of domains under a TLD - <https://www.icann.org/en/icann-acronyms-and-terms/registrar-en> for more information.
- Registries - organizations responsible for maintaining the database of domains for a TLD- <https://www.icann.org/en/icann-acronyms-and-terms/registry-en> for more information.
- Network Operator - Organizations operating an autonomous system (AS). We assume an organization with this capability is not running a recursive DNS server. This column means NetFlow and BGP data and excludes (as a matter of a clarity choice here) passive DNS.
- Hosting Provider - https://en.wikipedia.org/wiki/Web_hosting_service. If the hosting provider is a bulletproof hosting provider or otherwise complicit in providing attack infrastructure, then at best there is no good that will come from contacting them and at worst it will expose the team to reprisals.

Explanation of Terms: Techniques

21 different techniques

DGAs (Domain Generation Algorithms)	Domain name compromise	Lame delegations	DNS cache poisoning
DNS rebinding	DNS server compromise	Stub resolver hijacking	Local recursive resolver hijacking
On-path DNS attack	DoS against the DNS	NS as a vector for DoS	Dynamic DNS resolution (as obfuscation technique)
Dynamic DNS resolution: Fast flux (as obfuscation technique)	Infiltration and exfiltration via the DNS	Malicious registration of (effective) second level domains	Creation of malicious subdomains under dynamic DNS providers
Compromise of a non-DNS server to conduct abuse	Spoofing or otherwise using unregistered domain names	Spoofing of a registered domain	DNS tunneling
DNS beacon			

Description of Techniques (partial introduction)

- DGA (Domain Generation Algorithm) - See <https://attack.mitre.org/techniques/T1568/002/> for more information.
- Domain name compromise- The wrongfully taking control of a domain name from the rightful name holder. Compromised domains can be used for different kinds of malicious activity like sending spam or phishing, for distributing malware or as botnet command and control. For more information, see <https://www.icann.org/groups/ssac/documents/sac-007-en>.
- Lame delegations - Lame delegations occur as a result of expired nameserver domains allowing attackers to take control of the domain resolution by re-registering this expired nameserver domain. See <https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/> for more information.
- DNS cache poisoning -also known as DNS spoofing, is a type of cyber attack in which an attacker corrupts a DNS resolver's cache by injecting false DNS records, causing the resolver to records controlled by the attacker. For more information, see <https://capec.mitre.org/data/definitions/142.html>.

Explanation of Terms: Actions

Describes three patterns of conduct for each phase

detect

- Identify possible incident events
- Monitoring and detection, receipt of incident reports

prevent

- using DNS-specific steps, make it less likely incidents of this type will occur in the future.
- Knowledge transfer (including to internal IT teams); Vulnerability Response;

mitigate

- Contain the incident and restore safe operations
- Mitigation and Recovery

Examples of Techniques

■ JPCERT/CC

JPCERT/CC has published a list of phishing URLs that demonstrate examples of techniques including domain generation algorithms (DGAs) and malicious registrations of effective SLDs.

[Phishing URL dataset from JPCERT/CC](#)

■ U.S. Internal Revenue Service (IRS)

The IRS published a warning against SMS scams making use of malicious registration as well as spoofing the target organization.

[IRS reports significant increase in texting scams; warns taxpayers to remain vigilant](#)

■ Nominet

Nominet published an explanation of how dangling DNS entries can lead to vulnerability to the lame delegation and on-path DNS attack techniques.

[Dangling DNS is no laughing matter](#)

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix











4



Case Study

5

Concerns

How to see the Matrix

technique	stakeholders				
	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators
DGAs (Domain Generation Algorithms)	 <div data-bbox="440 467 658 565" style="border: 1px solid black; padding: 2px; width: fit-content;"> (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains) </div>				
Domain name compromise			 <div data-bbox="1045 699 1238 743" style="border: 1px solid black; padding: 2px; width: fit-content;"> lacks the capability </div>		

-  : The entity has the capability to
-  : The entity lacks the capability to

Matrix: Detection



Version 1.1 (Feb 9, 2023)

TLP:CLEAR

Detection

🟢 : The entity has the capability to detect

🔴 : The entity lacks the capability to detect

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrars	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	🟢 (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	🟢 (eSLDs only)	🟢 (eSLDs only, w/ analysis of customer domains)	🟢 (eSLDs only)	🟢 (Logs/ Passive DNS logging & analysis)	🔴	🟢	🔴	🟢	🔴	N/A (Registrant is Threat Actor Itself)	🔴	🟢 (Can engage registries and/or PSWG GAC)	🔴	🟢 (if outgoing queries logged)
Domain name compromise	🟢	🟢	🔴	🟢	🟢 (DNS RPZ + threat intelligence feeds)	🔴	🔴	🔴	🟢	🔴	🟢 (w/ proactive monitoring)	🔴	🟢	🔴	🔴 (Assuming external domain)
Lame delegations	🔴	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🟢 (w/ proactive monitoring)	🔴	🔴	🔴	🔴 (without historical delegation info)
DNS cache poisoning	🔴	🔴	🔴	🔴	🟢 (Validating DNSSEC at the recursive and enabling extended errors - RFC 8914)	🟢 (Flow analysis - NetFlow, Zeek)	🔴	🔴	🟢	🔴	🟢 (w/ proactive monitoring)	🔴	🔴	🔴	🔴 (Assuming external resolver is poisoned)
DNS rebinding	🔴	🔴	🔴	🔴	🟢 (pDNS analysis - DNS responses varying from	🟢 (Flow analysis -	🔴	🔴	🟢	🔴	🟢 (w/ proactive monitoring)	🔴	🔴	🔴	🟢

DNS Abuse Techniques Matrix
<https://www.first.org/global/sigs/dns/>

8 of 21

TLP:CLEAR

Matrix: Mitigation

Version 11 (Feb 9, 2023) **TLP:CLEAR**

Mitigation

✔ : The entity has the capability to mitigate
⊘ : The entity lacks the capability to mitigate

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✔ (updating status to onhold or changing name servers)	✔	⊘	✔ (updating status to onhold or changing name servers)	✔ (dns rpz)	⊘	⊘	⊘	⊘	⊘	N/A (Registrant is Threat Actor Itself)	⊘	✔ (Defensive registration, generate domains and share with registries)	⊘	✔ (blocking)
Domain name compromise	✔ (if compromise at the registrar level)	✔	✔	✔ (if compromise is at the reseller level)	✔	⊘	⊘	⊘	⊘	⊘	✔ (w/ appropriate clean up)	⊘	⊘	⊘	✔ (blocking)
Lame delegations	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔ (updating name servers)	⊘	⊘	⊘	⊘ (contact registrar, etc.)
DNS cache poisoning	⊘	⊘	✔	⊘	✔ (DNSSEC)	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘ (contact authoritative operator, etc.)
DNS rebinding	⊘	✔	⊘	⊘	⊘	✔ (BCP38, BGP blackhole attacker's IP netblock)	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔

DNS Abuse Techniques Matrix
<https://www.first.org/global/sigs/dns/> **TLP:CLEAR**

12 of 21

Matrix: Prevention

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

Prevention

✔ : The entity has the capability to prevent the threat
⊘ : The entity lacks the capability to prevent the threat

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✔ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✔ (eSLDs only)	✔ (if DG algorithm is known)	✔ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✔ (if DG algorithm is known, DNS RPZ + threat intelligence)	✔ (if DG algorithm is known)	⊘	⊘	⊘	⊘	N/A (registrant is threat actor itself)	⊘	✔	✔ Investigating DG Algorithm)	⊘
Domain name compromise	✔ (measures to prevent compromise of registrant account)	⊘	⊘	✔ (measures to prevent compromise of registrant account)	⊘	⊘	⊘	⊘	⊘	⊘	✔ (proactive measures to prevent compromise of registrant account)	⊘	✔	✔ (contact relevant stakeholders)	⊘
Lame delegations	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔ (good practices managing domain portfolio)	⊘	✔	✔ (contact relevant stakeholders)	⊘
DNS cache poisoning	⊘	⊘	⊘	⊘	✔ (DNSSEC validation enabled in the recursive)	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔	✔ (contact recursive operator or network operator clear/refresh cache)	⊘ (assuming cache is external to the org)

DNS Abuse Techniques Matrix
<https://www.first.org/global/sigs/dns/>

16 of 21

TLP:CLEAR

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix

4

Case Study

5

Concerns

How to Use the Matrix

Phishing



Phishing e-mail

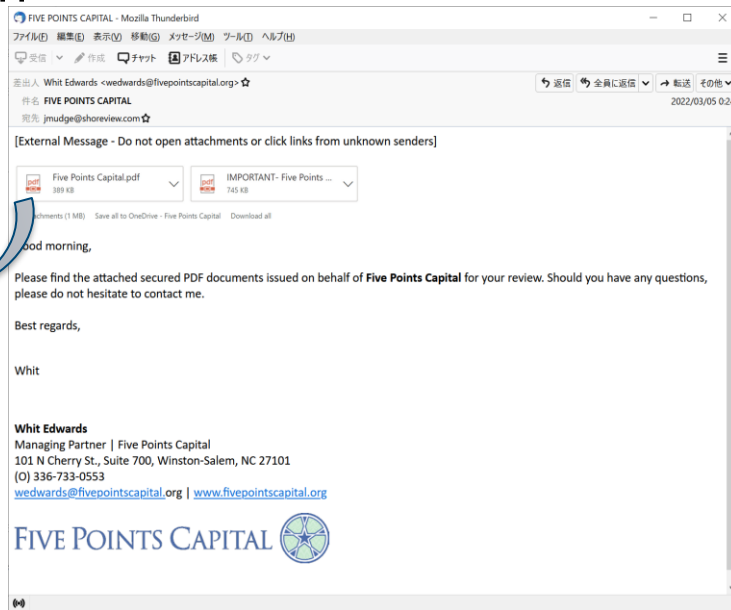
- Phishing e-mail impersonating Five Points Capital.
- Target domain name
 - (Correct) fivepointscapital.com
 - (False) fivepointscapital.org

Phishing e-mail Headers

```
Received: from 223404411203 named unknown by gmailapi.google.com with
HTTPREST; Fri, 4 Mar 2022 07:24:49 -0800
From: Whit Edwards <wedwards@fivepointscapital.org>
Date: Fri, 4 Mar 2022 07:24:49 -0800
Message-ID:
<CALYXdvkVcj3ttxy34VqKEgz_tmwEExjdLB1smvTjopMbU2zwaQ@mail.gm
ail.com>
Subject: FIVE POINTS CAPITAL
To: <xxxxxx@shoreview.com>
```

passive DNS information

```
:: bailiwick: fivepointscapital.org.
:: count: 1
:: first seen: 2022-03-04 15:11:31 -0000
:: last seen: 2022-03-04 15:11:31 -0000
fivepointscapital.org. in MX 1 aspmx.l.google.com.
```



Phishing e-mail

■ Technique: Spoofing of a registered domain

- Header-From Spoofing
- Spoofed domain that impersonates a legitimate domain

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
--	------------	------------	-------------------------	-----------------------	---------------------	-------------------	------------------------------	------------------	------------------------------	---	--------------------	----------	---	----------------	-------------------------------

Detection

Spoofing of a registered domain	⊗	⊙	⊗	⊗	⊙ (Analysis of DNS responses - RFC 8914)	⊗	⊙	⊙ (not bulletproof)	⊙	⊗	⊗ (unless using DMARC)	⊗	⊙	⊗	⊙ (assuming DMARC or maybe pDNS analysis)
---------------------------------	---	---	---	---	---	---	---	------------------------	---	---	---------------------------	---	---	---	--

Mitigation

Spoofing of a registered domain	⊙ (w/ analysis at point of creation or though the lifetime of the domains)	⊗	⊗	⊙ (w/ analysis at point of creation or though the lifetime of the domains)	⊙	⊗	⊗	⊙ (not bulletproof)	⊗	⊗	⊙ (filing report, UDRP, URS as appropriate)	⊗	⊗	⊗	⊗ (even if DMARC applies, does not stop the spoofing)
---------------------------------	---	---	---	---	---	---	---	------------------------	---	---	--	---	---	---	--

Prevention

Spoofing of a registered domain (for abuse)	⊙ (eSLDs only, analysis at point of creation)	⊗	⊙ (preventing resolution for the spoofing domains serviced)	⊙ (eSLDs only, analysis at point of creation)	⊗	⊗	⊗	⊙ (not bulletproof)	⊗	⊙	N/A (registrant is threat actor itself)	⊗	⊙	⊙ (share info for awareness)	⊗
---	--	---	--	--	---	---	---	------------------------	---	---	--	---	---	---------------------------------	---

Phishing site

<https://kuronekohelp.com/information>

The screenshot shows a phishing website for Yamato Transport. The page has a header with the company logo and navigation icons. The main content is a registration form titled "お届け先情報" (Delivery Address Information). A pink banner at the top of the form says "再配送するため、資料を更新してください。" (Please update the information for re-delivery). The form includes fields for name (姓 and 名), phone number (セイ, メイ, and 電話番号), birth date (年, 月, 日), address (ご住所), and email address. A sidebar on the left contains navigation icons for Home, Card, Campaign, Favorites, and Support.

<https://japan-japan-aeon.shop/index.php>

The screenshot shows a phishing website for AEON CARD. The page has a header with the AEON CARD logo and the text "暮らしのマネーサイト". The main content is a login page titled "ログイン" (Login). It features two columns: "イオンスクエアメンバーID" (Aeon Square Member ID) and "パスワード" (Password), and "スマートフォンでご利用の方" (For those who use the smartphone app). A blue "ログイン" button is at the bottom. A sidebar on the left contains navigation icons for Home, Card, Campaign, Favorites, and Support. A chat window is visible at the bottom, and a "重要なお知らせ" (Important Notice) banner is at the bottom of the page.

Phishing site

■ Technique: Malicious registration of (effective) second level domains

Registrars Registries Authoritative Operators Domain name resellers Recursive Operators Network Operators Application Service Provider Hosting Provider Threat Intelligence Provider Device, OS, & Application Software Developers Domain Registrants End User Law Enforcement and Public Safety Authorities CSIRTs / ISACs Incident responder (internal)

Detection

Malicious registration of (effective) second level domains	✔ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✔	✔ (depending on the strings)	✔ (pDNS analysis)	✘	✔	✘	✔	✘	N/A (Registrant is Threat Actor Itself)	✘	✔ (Contact registrar, escalate to registry)	✘	✘ (Can't detect the registration)
--	---	---	------------------------------	-------------------	---	---	---	---	---	---	---	---	---	-----------------------------------

Mitigation

Malicious registration of (effective) second level domains	✔ (updating status to onHold or changing name servers)	✔	✘	✔ (updating status to onHold or changing name servers)	✔	✘	✘	✘	✘	✘	N/A (Registrant is Threat Actor Itself)	✘	✔ (notify registrar/registry, domain seizure [LEA])	✘	✘ (cannot change registration itself)
--	--	---	---	--	---	---	---	---	---	---	---	---	---	---	---------------------------------------

Prevention

Malicious registration of (effective) second level domains	✔ (eSLDs only, analysis at point of creation)	✔	✘	✔ (eSLDs only, analysis at point of creation)	✘	✘	✘	✘	✘	✔	N/A (registrant is threat actor itself)	✘	✔ (notify registrar, escalate to registry)	✔ (contact relevant stakeholders)	✘
--	---	---	---	---	---	---	---	---	---	---	---	---	--	-----------------------------------	---

Prepare for phishing activities

- Prepare environment before starting phishing activity by tampering with DNS.
- Tampering with SPF authentication information in TXT records
 - ➡ Preparing to send a pretended authorized phishing e-mails

```
;; bailiwick: *****.jp.  
;; first seen: 2022-01-28 20:59:00 -0000  
;; last seen: 2022-01-28 20:59:00 -0000  
*****.jp. in TXT "v=spf1 ip4:133.242.52.116 ~all"  
*****.jp. in TXT "v=spf1 ip4:27.102.118.13/17 ~all"  
*****.jp. in TXT "v=spf1 a mx ptr a: *****.jp ip4:27.102.118.0/24 ?all"
```

- Add subdomain ➡ Prepare phishing site for operation

```
;; bailiwick: *****.jp.  
;; count: 93  
;; first seen: 2022-01-23 12:38:07 -0000  
;; last seen: 2022-01-29 03:26:55 -0000  
xserver-vps. *****.jp. in A 115.144.69.72
```


Prepare for phishing activities

Technique: Domain name compromise

Registrars Registries Authoritative Operators Domain name resellers Recursive Operators Network Operators Application Service Provider Hosting Provider Threat Intelligence Provider Device, OS, & Application Software Developers Domain Registrants End User Law Enforcement and Public Safety Authorities CSIRTs / ISACs Incident responder (internal)

Detection

Domain name compromise	✓	✓	✗	✓	✓ (DNS RPZ + threat intelligence feeds)	✗	✗	✗	✓	✗	✓ (w/ proactive monitoring)	✗	✓	✗	✗ (Assuming external domain)
------------------------	---	---	---	---	--	---	---	---	---	---	--------------------------------	---	---	---	---------------------------------

Mitigation

Domain name compromise (if compromise at the registrar level)	✓	✓	✓	✓ (if compromise is at the reseller level)	✓	✗	✗	✗	✗	✗	✓ (w/ appropriate clean up)	✗	✗	✗	✓ (blocking)
--	---	---	---	---	---	---	---	---	---	---	--------------------------------	---	---	---	-----------------

Prevention

Domain name compromise (measures to prevent compromise of registrant account)	✓	✗	✗	✓ (measures to prevent compromise of registrant account)	✗	✗	✗	✗	✗	✗	✓ (proactive measures to prevent compromise of registrant account)	✗	✓	✓ (contact relevant stakeholders)	✗
--	---	---	---	---	---	---	---	---	---	---	---	---	---	--------------------------------------	---

How to Use the Matrix

Other

- Lame Delegation
- Water Torture attack against authoritative DNS servers
- Cache poisoning by domain hijacking

Lame Delegation

Lame Delegation is a situation in which the DNS server registered in the upper zone at the time of delegation is not working properly for that domain for some reason.

(Reference : JPRS <https://jprs.jp/tech/notice/2003-05-20-dnsqc-lame-delegation.html>)

Domain Information: [Domain Information]
[Domain Name] *****.JP

[Registrant's name] ***** Corporation
[Registrant] *****

[Name Server] **ns-1926.awsdns-48.co.uk**
[Name Server] ns-309.awsdns-38.com
[Name Server] ns-1008.awsdns-62.net
[Name Server] ns-2000.awsdns-58.co.uk
[Signing Key].

[Date of registration] 2016/11/15
[Expiration date] 2023/11/30
[Status] Active
[Last Updated] 2022/12/01 01:05:08 (JST)

mismatch

```
$ dig @ns-309.awsdns-38.com *****.jp
```

```
:: AUTHORITY SECTION:
```

```
*****.jp. 172800 IN NS ns-1008.awsdns-62.net.  
*****.jp. 172800 IN NS ns-1268.awsdns-30.org.  
*****.jp. 172800 IN NS ns-2000.awsdns-58.co.uk.  
*****.jp. 172800 IN NS ns-309.awsdns-38.com.
```

```
$ dig @ns-1926.awsdns-48.co.uk *****.jp
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 24815  
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0  
:: WARNING: recursion requested but not available  
:: QUESTION SECTION:
```

```
. *****.jp. in A
```

ns-1926.awsdns-48.co.uk cannot resolve the name.

Lame Delegation

■ Technique: Lame Delegation

— Mainly addressed by Domain Registrants

Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
------------	------------	-------------------------	-----------------------	---------------------	-------------------	------------------------------	------------------	------------------------------	---	--------------------	----------	---	----------------	-------------------------------

Detection

Lame delegations	⊗	⊙	⊗	⊗	⊙	⊗	⊗	⊗	⊙	⊗	⊙ (w/ proactive monitoring)	⊗	⊗	⊗ (without historical delegation info)
------------------	---	---	---	---	---	---	---	---	---	---	--------------------------------	---	---	---

Mitigation

Lame delegations	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊙ (updating name servers)	⊗	⊗	⊗	⊗ (contact registrar, etc.)
------------------	---	---	---	---	---	---	---	---	---	------------------------------	---	---	---	--------------------------------

Prevention

Lame delegations	⊗	⊙	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊙ (good practices managing domain portfolio)	⊗	⊙	⊙ (contact relevant stakeholders)	⊗
------------------	---	---	---	---	---	---	---	---	---	---	---	---	--------------------------------------	---

Water Torture Attack against authoritative DNS servers

■ DNS Water Torture attack

- Using Open Resolver to execute attacks.
- Target is `jpcert.or.jp` authoritative DNS server.

Water Torture attack targeted JPCERT/CC domain

2023-07-08 21:46:53.570989 IP SourceOfAttack.39636 > Open Resolver.53: 19199+ A? amur.jpcert.or.jp. (35)

2023-07-08 21:46:55.153998 IP SourceOfAttack.39636 > Open Resolver.53: 52204+ A? chickadee.jpcert.or.jp. (40)

2023-07-08 21:47:00.651903 IP SourceOfAttack.39636 > Open Resolver.53: 9206+ A? cycle1.jpcert.or.jp. (37)

2023-07-08 21:47:02.548646 IP SourceOfAttack.39636 > Open Resolver.53: 11887+ A? mosaffa.jpcert.or.jp. (38)

2023-07-08 21:47:05.370698 IP SourceOfAttack.39636 > Open Resolver.53: 18118+ A? sokolova-nina.jpcert.or.jp. (44)

Water Torture attack against authoritative DNS servers

Technique: DNS as a vector for DoS

Registrars Registries Authoritative Operators Domain name resellers Recursive Operators Network Operators Application Service Provider Hosting Provider Threat Intelligence Provider Device, OS, & Application Software Developers Domain Registrants End User Law Enforcement and Public Safety Authorities CSIRTs / ISACs Incident responder (internal)

Detection

DNS as a vector for DoS	⊗	⊗	⊙ (if attack leverages)	⊗	⊙ (if attack targets the recursive or authoritative -	⊙ (Flow analysis -	⊗	⊗	⊗	⊙	⊗	⊗	⊙	⊗	⊙
-------------------------	---	---	----------------------------	---	--	-----------------------	---	---	---	---	---	---	---	---	---

Mitigation

DNS as a vector for DoS	⊗	⊙	⊙	⊗	⊙	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊙
-------------------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Prevention

DNS as a vector for DoS	⊗	⊗	⊙ (if the attack weaponizes the authoritative responses)	⊗	⊙ (ACL, rate-limiting etc)	⊗	⊗	⊗	⊗	⊙	⊗	⊙ (keep firmware up to date and proper configuration, etc)	⊙ (engage national-level CERT to identify DNS amplifiers)	⊙ (Coordination for open resolvers and infected machines)	⊙ (clean up infected machines)
-------------------------	---	---	---	---	-------------------------------	---	---	---	---	---	---	---	--	--	-----------------------------------

Cache poisoning by domain hijacking

- A situation in which an attacker corrupts a DNS resolver's cache by injecting false DNS records, causing the resolver to records controlled by the attacker.

Normal condition

```
whois :*****.com
Domain Name: *****.COM

Name Server: NS-1515.AWSDNS-61.ORG
Name Server: NS-1985.AWSDNS-56.CO.UK
Name Server: NS-405.AWSDNS-50.COM
Name Server: NS-650.AWSDNS-17.NET
```

After hijack

```
;; bailiwick: *****.com.
;; count: 1,686
;; first seen: 2020-05-30 15:43:14 -0000
;; last seen: 2020-06-01 16:04:04 -0000
coincheck.com. in NS ns-650.awsdns-017.net.
coincheck.com. in NS ns-1515.awsdns-061.org.
coincheck.com. in NS ns-1985.awsdns-056.co.uk.
```

NS-650.AWSDNS-17.NET	➔	ns-650.awsdns-017.net
NS-1515.AWSDNS-61.ORG	➔	ns-1515.awsdns-061.org.
NS-1985.AWSDNS-56.CO.UK	➔	ns-1985.awsdns-056.co.uk

Cache poisoning by domain hijacking

Technique: DNS Cache Poisoning

Registrars Registries Authoritative Operators Domain name resellers Recursive Operators Network Operators Application Service Provider Hosting Provider Threat Intelligence Provider Device, OS, & Application Software Developers Domain Registrants End User Law Enforcement and Public Safety Authorities CSIRTs / ISACs Incident responder (internal)

Detection

DNS cache poisoning	⊗	⊗	⊗	⊗	⊕ (Validating DNSSEC at the recursive and enabling extended errors - RFC 8914)	⊕ (Flow analysis - NetFlow, Zeek)	⊗	⊗	⊕	⊗	⊕ (w/ proactive monitoring)	⊗	⊗	⊗	⊗ (Assuming external resolver is poisoned)
---------------------	---	---	---	---	---	--------------------------------------	---	---	---	---	--------------------------------	---	---	---	---

Mitigation

DNS cache poisoning	⊗	⊗	⊕	⊗	⊕ (DNSSEC)	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗ (contact authoritative operator, etc.)
---------------------	---	---	---	---	---------------	---	---	---	---	---	---	---	---	---	---

Prevention

DNS cache poisoning	⊗	⊗	⊗	⊗	⊕ (DNSSEC validation enabled in the recursive)	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕ (contact recursive operator or network operator clear/refresh cache)	⊗ (assuming cache is external to the org)
---------------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--

Today's presentation

1

What is the Japanese version DNS Abuse Techniques Matrix?

2

Document Structure

3

How to see the Matrix

4

Case Study

5

Concerns

Concerns

In some cases, the scope of stakeholder responsibility varies by country or region.

Difficult to utilize this matrix under the provision of services by a business operator with malicious intent.

Difficult to utilize this matrix when addressing policy-related events.

Countermeasures will be updated and the matrix will need to be updated as well.

in the end

- **The DNS Abuse Techniques Matrix** has been compiled for incident responders and those investigating DNS abuse.
- As we investigate security incidents in depth, we are sure that many of them will involve the DNS, and we hope that **the DNS Abuse Techniques Matrix will be** of assistance in the investigation and in making adjustments.

Contact info:

JPCERT Coordination Center

- Email: pr@jpcert.or.jp
- <https://www.jpcert.or.jp/reference.html>

incident reporting

- Email: info@jpcert.or.jp
- <https://www.jpcert.or.jp/form/>

Incident Response Group

- Email: ir-info@jpcert.or.jp



Company names and product names mentioned in this document are trademarks or registered trademarks of their respective companies.

Thank you for your attention.



Reference Web site

- JPCERT/CC
 - [Matrix for Countering DNS Abuse Techniques](#)
 - [Phishing URL dataset from JPCERT/CC](#)
- FIRST DNS Abuse SIG
 - [DNS Abuse Technique Matrix](#)
- Framework to Address Abuse
 - [DNS Abuse Framework](#)
- ICANN
 - [SAC115 \(SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS\)](#)
- INTERNET & JURISDICTION POLICY NETWORK
 - [Toolkit DNS Level Action to Address](#)
- EU(European Union)
 - [Study on Domain Name System \(DNS\) abuse](#)
- U.S. Internal Revenue Service (IRS)
 - [IRS reports significant increase in texting scams; warns taxpayers to remain vigilant](#)
- Nominet
 - [Dangling DNS is no laughing matter](#)