



DNS Abuse SIG Update

TLP:WHITE

FIRST - DNS Abuse SIG Update

20.05.2020

Michael Hausding, Jonathan Matkowsky, John Todd

dns-abuse-sig@first.org

Mission of the DNS Abuse SIG

The Domain Name System (DNS) is a critical part of the Internet, including mapping domain names to IP addresses. Malicious threat actors use domain names, their corresponding technical resources, and other parts of the DNS infrastructure, including its protocols, for their malicious cyber operations. CERTs are confronted with reported DNS abuse on a continuous basis, and rely heavily on DNS analysis and infrastructure to protect their constituencies. Understanding the international customary norms applicable for detecting and mitigating DNS abuse from the perspective of the global incident response community is critical for the open Internet's stability, security and resiliency.

SIG Goals & Deliverables

- Common Language
- Classification Scheme
- Threat Actor TTPs
- Relevant stakeholders
- Mitigation Best Practices

Registrar Coalition Framework to Address Abuse*

DNS Abuse

- *Malware*
- *Botnet*
- *Phishing*
- *Pharming*
- Spam-- when it is a delivery mechanism for the above

Website Content Abuse

- CSMA
- Opioids
- Human trafficking
- Specific and credible incitements to violence

https://www.dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

Policy vs. Incident Response

Bridging the Gap

Current Policy

- Recipients of abuse notifications
- Limited to the Authoritative DNS (and not the full DNS ecosystem)

Incident Response

- Detection & Mitigation
- Prevention must take a holistic view of the DNS
- Analysis, including TTPs

TLP:WHITE

Abuse of the DNS:

Traffic that causes DNS servers or intermediate architecture involved in the transmission or processing of DNS services, or both, to be degraded or unavailable to third parties, or that causes unintended results in the service provided by DNS service operators or registry service providers.

Abuse via the DNS:

Harmful cyber activity that cannot take place without using the DNS, but where the threat actors' operations do not constitute abuse of the DNS

Mapping Incident Types to DNS-oriented Classifications and Actions

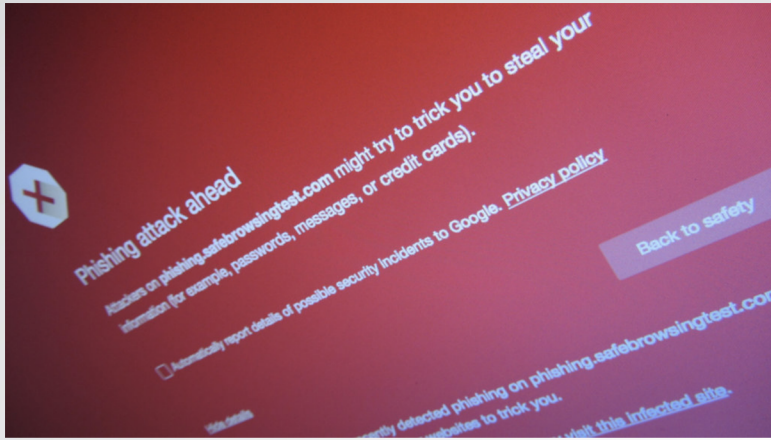
- Detection ability
- Mitigation ability
- Prevention ability
- Difficult to classify?
- Nature of access (acquired resource, intrusion, denial, n/a)
- Stakeholder and responder matrix

TLP:WHITE

Mapping Incidents to the DNS

A	B	C	E	F	G	H	I	J	K
Incident classification	Type of Incident Classification	Columns H-L Done	Abuse of the DNS	Abuse via the DNS	Detection via DNS	Mitigation through the DNS	Prevention through the DNS	Difficult to classify and confirm the incident	Nature of access to the DNS
Fraud									
	Intentional Trademark Infringement or Counterfeiting	<input type="checkbox"/>	No	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Acquired
	Intentional Unauthorized Use of Resources	<input type="checkbox"/>	Sometimes	Sometimes	Never	Sometimes	Sometimes	Sometimes	Intrusion
	Intentional (SIG) Copyright	<input type="checkbox"/>	Never	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Acquired
	Masquerade	<input type="checkbox"/>	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Intrusion, Acquired
	Phishing	<input type="checkbox"/>							
	Phishing: Compromised infrastructure intentionally used for Phishing (SIG)	<input type="checkbox"/>	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Intrusion
	Phishing: Fraudulently created domain that is currently exclusively being used to commit fraud under applicable law like Phishing (SIG)	<input type="checkbox"/>	Sometimes	Always	Always	Sometimes	Typically	Sometimes	Acquired

(work in progress)



Is Phishing DNS Abuse?

from the operational perspective of incident handlers

"Phishing warning" by Christiaan Colen is licensed with CC BY-SA 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/2.0/>

Sometimes

[Home](#)



 Financial Info

 Login eBanking

[Our company](#)

[Media](#)

[Investor Relations](#)

[Private Banking](#)

[Commercial banking](#)

[Asset Management](#)

Strong regional roots and an

This website uses cookies. By using this website, you consent to the use of cookies. For further information, please read our [Cookie Policy](#) and refer to our [Data Protection Policy](#).

I agree

Phishing: Domain Registration

Fraudulently registered domain that is currently exclusively being used to commit fraud under applicable law, like **Phishing**

Abuse of the DNS:	Sometimes
Abuse via the DNS:	Yes
Detection:	Yes
Mitigation:	Yes
Prevention:	Yes
Difficult:	Yes
Nature of Access:	Acquired

zimbra

Sign In

Username

Password

Show

Sign In

Stay signed in

Web App Version



Phishing: Compromise

Compromised
infrastructure
intentionally used
for **Phishing**

Abuse of the DNS: No

Abuse via the DNS: Yes

Detection: No

Mitigation:
Yes

Prevention:
Yes


Difficult:
Yes

Nature of Access: Intrusion

Einloggen

Einloggen

Benutzerdaten merken [Sie benötigen Hilfe?](#)

 Mit Facebook einloggen

Neu bei Netflix? [Jetzt registrieren](#)

Diese Seite ist durch Google reCAPTCHA abgesichert, um sicherzustellen, dass Sie kein Bot sind. [Weitere Infos.](#)

Phishing: DNS Resolver Hijacking

Attack on the DNS resolver path to redirect users to a fraudulent login page

Abuse of the DNS:	Yes
Abuse via the DNS:	Yes
Detection:	Yes
Mitigation:	No
Prevention:	No
Difficult:	No
Access:	Intrusion/Acquired

News	Topics	Information companies	Information individuals	Customs declaration	Documentation	The FCA
▼	▼	▼	▼	▼	▼	▼

Warning against phishing messages

Citizens have recently been receiving growing numbers of messages that supposedly originate from the Federal Customs Administration. The Federal Customs Administration is issuing a warning concerning these messages and recommends ignoring them and deleting them.

More and more private individuals and businesses are receiving so-called "phishing" messages in which fraudsters request payment using the name of the Federal Customs Administration. The recipients supposedly need to transfer money in order to receive a package they have ordered. The current phishing mails often feature "notification@ezv.admin.ch", "zoll-paket-dienste@schweiz-zoll.ch" or "zollauskunft@ezv-admin.ch" as the sender. In addition, the fraudsters use FCA logos without authorisation, create copycat documents, etc.

In light of this, the FCA would like to stress that it never sends payment requests by email or text message. It is therefore recommending that messages of this kind be ignored and deleted.

Phishing: Email only

Phishing emails being sent from a sender domain that is **not** registered and not in the DNS but used only in the from: header of phishing emails

Abuse of the DNS:	No
Abuse via the DNS:	No
Detection:	No
Mitigation:	Yes
Prevention:	Yes
Difficult:	No
Nature of Access:	No Access

Prevention through the DNS

- Register the domain
- Publish a SPF & DMARC Policy in the DNS

The screenshot displays the Hardenize Public Report for the domain schweiz-zoll.ch. The report is dated 18 May 2021 08:21 UTC. It provides a detailed overview of the domain's DNS configuration and email security status.

Domain

- ✓ Name servers
- ✓ DNSSEC
- ✗ CAA

Email

- ✗ Mail servers

SECURE TRANSPORT (SMTP)

- ✗ TLS
- ✗ Certificates
- ✗ MTA-STS
- ✗ TLS-RPT
- ✗ DANE

AUTHENTICATION AND POLICY

- ✓ SPF
- ✓ DMARC

DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling.

Test passed
Everything seems to be well configured. Well done.

DMARC Policy Information

Policy location: `_dmarc.schweiz-zoll.ch`

v	DMARC1
p	reject
sp	reject
pct	100
aspf	s

Analysis

DMARC policy found	Policy: v=DMARC1; p=reject;sp=reject;pct=100;aspf=s
Policy is valid	Host: _dmarc.schweiz-zoll.ch Good. You have a valid DMARC policy.

Some Takeaways

- *The DNS is a complex system from registration, authoritative and recursive resolvers that extends to the DNS resolver configuration and application*
- *Detection, mitigation and prevention can happen on any of these components*
- *Different actors can detect, mitigate and prevent DNS Abuse better than others for a specific incident*
- *Even incidents of the same type may have different detection, mitigation and prevention possibilities*

More Takeaways

- The relation between the DNS and Abuse is complex and cannot easily be described with “is DNS Abuse” or “is not DNS Abuse”
- No matter the definition of “DNS Abuse”, no single player can solve the problem as a whole
- Cooperation requires a common language to successfully combat abuse
- Operators are looking for a way to define abuse incidents that involve the DNS and relate them to a policy that allows them to act.
- Our work to date sharpens an understanding of DNS abuse to better map real-world events, which enables policy-makers to provide guidance to relevant stakeholders

Further work for the SIG:

- Extension of mitigation best practices - examples needed
- Continued discussion of mapping of ENISA mapping to DNS concepts
- Stakeholders will be able to create practical “checklists” for incident response, so that they understand where their role begins and where it ends.

Any FIRST member may join, others are welcome as well, requests must be approved by the SIG chairs.

<https://www.first.org/global/sigs/dns>