FIRST DNS Abuse SIG

TLP:WHITE

ICANN DNS Symposium 26.05.2020

Michael Hausding, Jonathan Matkowsky
co-chairs of the FIRST DNS Abuse SIG
dns-abuse-sig@first.org

About FIRST

FIRST is the Forum of Incident Response and Security Teams

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

https://first.org

TLP:WHITE

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.

TLP:WHITE

SIG Goals & Deliverables

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

TLP:WHITE

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

- Certain Recipients of abuse notifications
- Focused on 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.

TLP:WHITE

Abuse via the DNS:

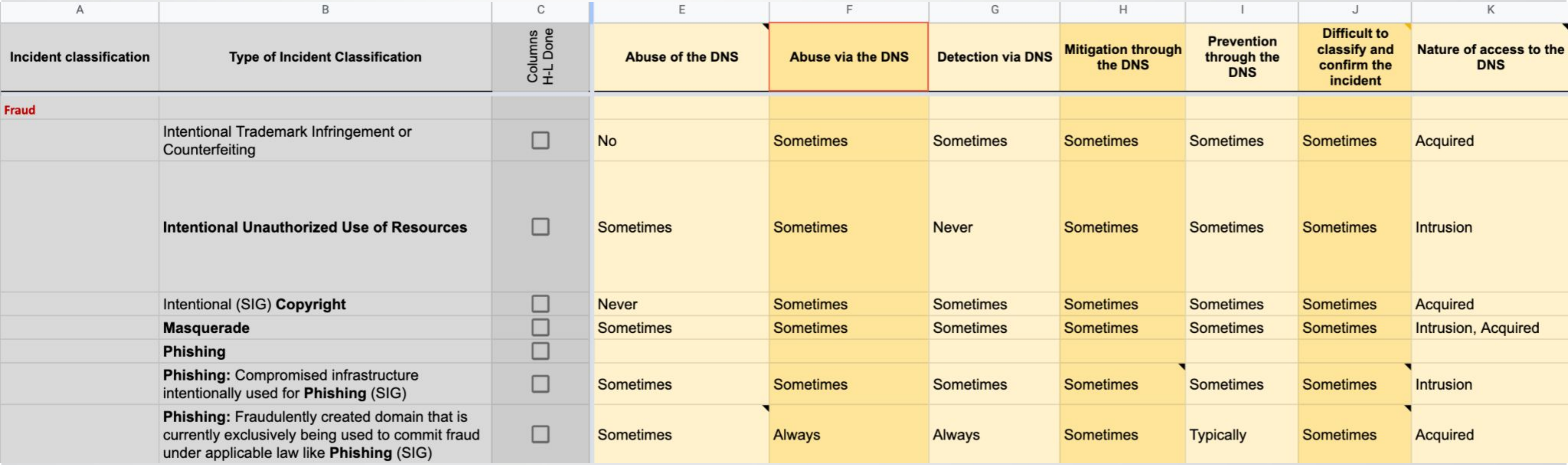
Harmful cyber activity that cannot take place without using the DNS, but where the threat actors' operations do not constitute abuse of the DNS

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

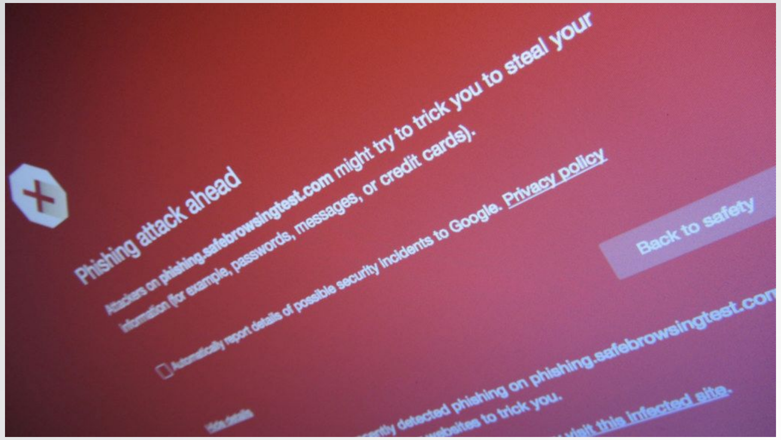
Mapping Incidents to the DNS



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	□	No	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Acquired
	Intentional Unauthorized Use of Resources	□	Sometimes	Sometimes	Never	Sometimes	Sometimes	Sometimes	Intrusion
	Intentional (SIG) **Copyright**	□	Never	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Acquired
	Masquerade	□	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Intrusion, Acquired
	Phishing	□							
	Phishing: Compromised infrastructure intentionally used for **Phishing** (SIG)	□	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)	□	Sometimes	Always	Always	Sometimes	Typically	Sometimes	Acquired

(work in progress)

TLP:WHITE


Phishing attack ahead

Attackers on phishing.safebrowsingtest.com might try to trick you to steal your information (for example, passwords, messages, or credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy

Back to safety

Hide details

ntly detected phishing on phishing.safebrowsingtest.com

websites to trick you.

visit this infected site.

Is Phishing DNS Abuse?

from the operational perspective of incident handlers

Sometimes

TLP:WHITE

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

TLP:WHITE

Further work for the SIG:

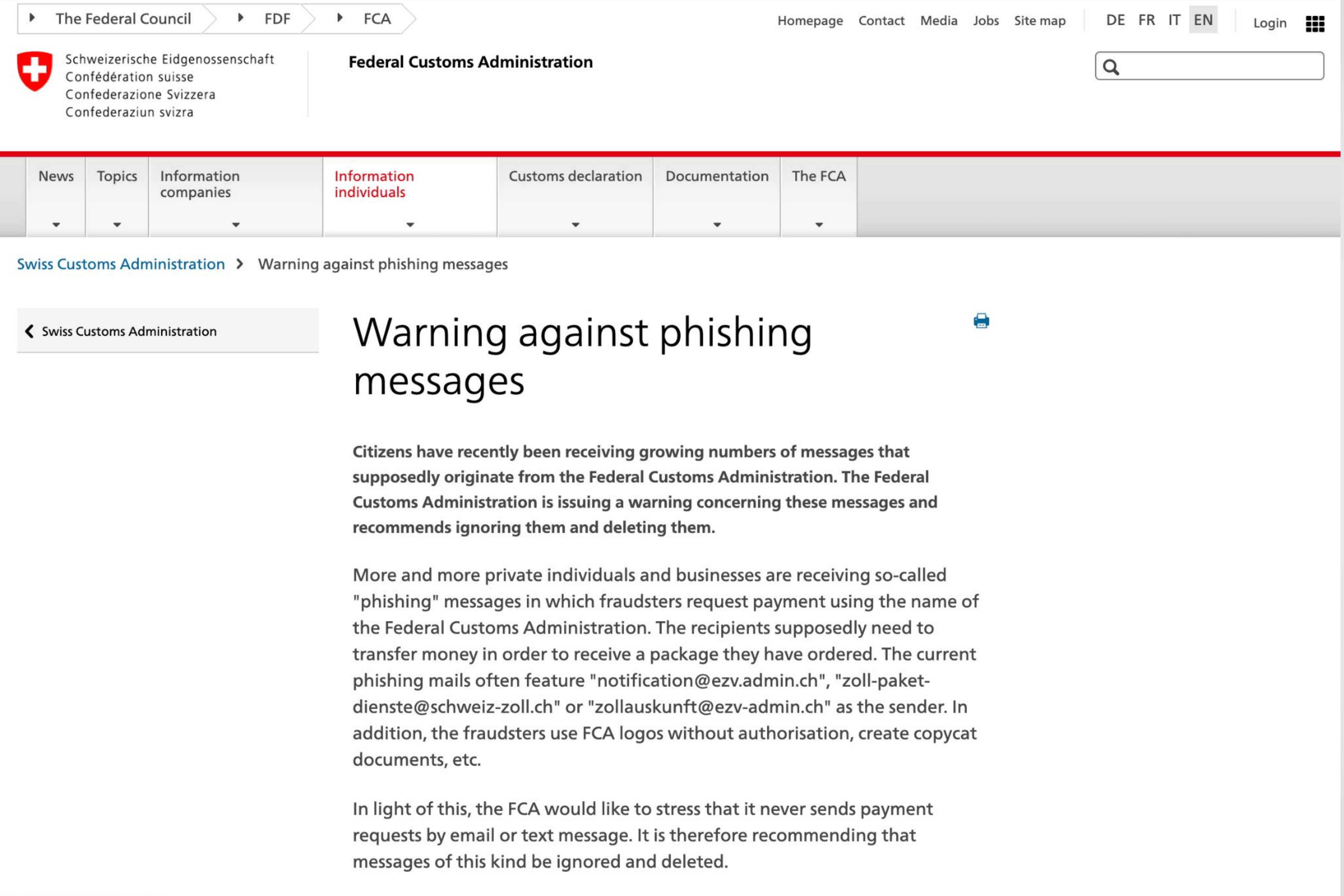
- Extension of mitigation best practices - examples needed
- Continued discussion of mapping ENISA taxonomy to DNS concepts
- Stakeholders will be able to create practical “checklists” for incident response, so that they understand where their role begins and where it ends.

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

Backup slides with example

TLP:WHITE



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.

https://www.ezv.admin.ch/ezv/en/home/teaser-homepage/focus-teaser/warning-against-fraudulent-messages.html

TLP:WHITE

Phishing: Email only

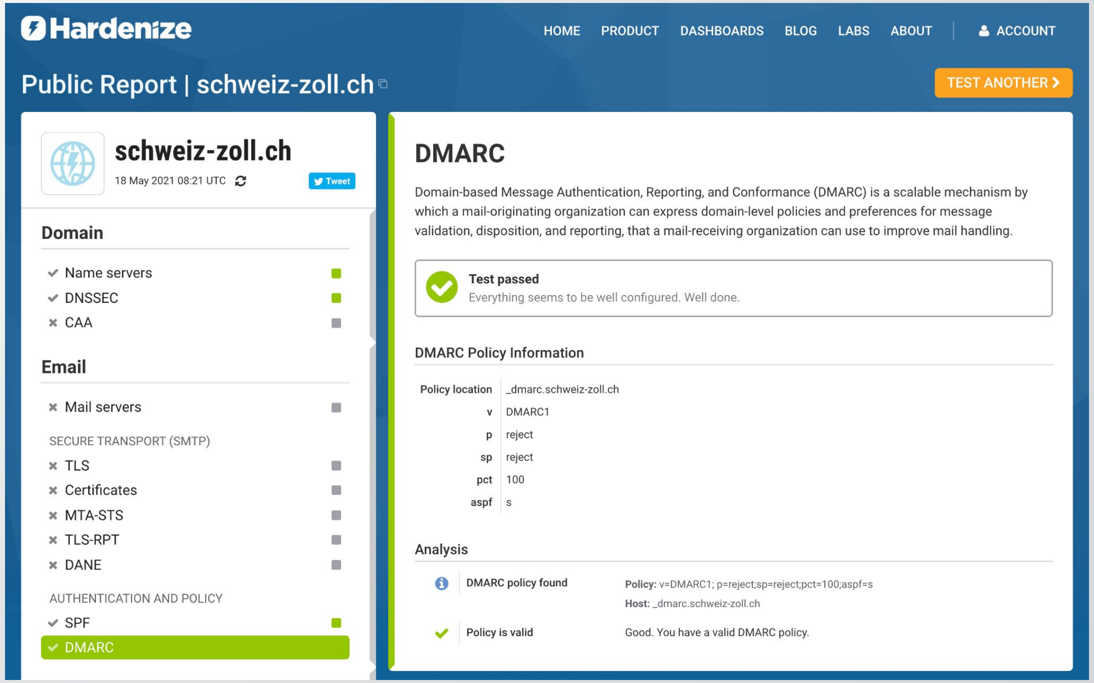
Phishing emails being sent from a sender domain that is **not** registered and not in the DNS but used only in the from: header of phishing emails

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

TLP:WHITE

Prevention through the DNS

- Register the domain
- Publish a SPF & DMARC Policy in the DNS to allow detection of email spoofing



Public Report | schweiz-zoll.ch

schweiz-zoll.ch

18 May 2021 08:21 UTC

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

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