Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Defence, Civil Protection and Sport DDPS
National Cyber Security Center NCSC

CH-3003 Bern, NCSC

Mrs. Sally Costerton
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Bern, 1st May 2024

Combatting internet abuse and applicability or RDRS

Dear Mrs. Costerton

The National Cyber Security Center of Switzerland (NCSC.ch) is the federal government's competence centre for cybersecurity. NCSC.ch is responsible for the implementation of Switzerland's National Cyber Strategy (NCS) and to ensure the cyber resilience of Switzerland. GovCERT.ch, which is the official national CERT mandated by the federal council, is part of NCSC.ch. GovCERT.ch conducts technical analysis to provide threat intelligence to critical infrastructure, economy and society, implements preventive technical measures with its partners (eg. telecommunication providers) and provides incident response services to national critical infrastructure.

Today, GovCERT.ch handles thousands of phishing reports per week[1]. In response to phishing threads, we send out takedown notices for phishing websites that have been confirmed as such by our tooling or by our analysts. The recipient of these takedown notices are corresponding network owners (i.e., hosting provider) that hosts the phishing content as well as the domain owner (domain registrant) that is responsible for a domain name. As the majority of the phishing websites identified by us are located on compromised websites, it is important that the responsible domain owner (registrant) gets notified about abuse in due time.

Due to the several hundred phishing websites detected and reported by us every week, we have to rely on automated reporting mechanisms to inform network and domain owners by email. To identify and obtain the appropriate email address we rely on public registration information through WHOIS and RDAP for both, IP addresses (to obtain the abuse mailbox of the corresponding network owner) and domain names (to obtain the registrant's email address).

Unfortunately, since 2018, domain registrant information is usually no longer published in the public accessible whois service (RDAP). As a result, we are no longer able to contact the owner of a domain (registrant) in an automated manner. In September 2022, ICANN announced that it has identified this as an issue and that it will work on a proper replacement. In November 2023, ICANN published a tool called RDRS which allows to request domain registration data for domain names.

With regards to the current situation and the tooling provided by ICANN, we would like to bring the following to your attention:

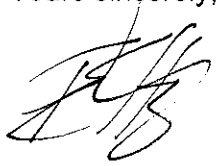
[1] See « Anti-Phishing Report 2023 », https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/anti-phishing-report-2023.html

- The current implementation introduced by ICANN (RDRS), although being a step in the right direction, does not suite our needs as it does **not allow automated notification of the domain registrant.** Subsequently, we do not consider ICANN' RDRS as a proper replacement for the public whois service (RDAP).
- We do strongly believe that the heaviest, most frequent users, including other authorities, security researchers and cyber threat analysts who need the non-public whois/RDAP data to fight abuse every, will not use RDRS. This is because the volume of the work won't allow to manually submit queries one by one. They are in a similar situation as we are since they too lost their ability to efficiently combat abuse related to the domain name system (DNS). We hope that the ICANN Board of Directors and the Generic Names Supporting Organization take this into account when considering the usability metrics of RDRS over time and during each month.
- From our understanding, the public whois service (RDAP) is no longer serving registrant information because of privacy issue. However, we want to outline that our purpose is not having access to the information **who** registered a domain name rather than **a way to contact an owner of a domain name** (registrant) and the sponsoring registrar in a scalable, **automated** way. For this purpose, we do not necessarily need to know who the registrant of a domain name is (impersonal contact data would already be sufficient).
- We increasingly observe domain names that in public whois (RDAP) have an email object (e.g. "Registrant Email") which does not contain an valid email address but point to a web form. In our opinion, this not only represents a misuse of the email object in public whois (RDAP) but also makes automated and scalable abuse reporting to corresponding domain owner (registrant) error prone and complicated at best and impossible at worst.

In a growing digital world, cyber threats represent a big challenge for internet society. As the organization that is responsible for coordinating the maintenance and procedures of the namespaces in the internet, I personally believe that ICANN plays a key role in enabling the internet society to battle abuse and making our digital future safer. I hope you are aware about these problems and its impact on internet security. I would like to encourage you to seek a discussion with the relevant stakeholders at ICANN to come up with a scalable solution that addresses the outlined problems and subsequently enable those of us of the internet society who fight for the good of the internet to do so.

Myself and my experts are looking forward to your response and are of course available to clarify any questions or a have a more in-depth discussion.

Yours sincerely,



Florian Schütz
Director NCSC

Copy to:
- Tripti Sinja, Chair
- Danko Jevtović, Vice-Chair

National Cyber Security Center NCSC
Florian Schütz
Schwarztorstrasse 59, 3003 Bern
florian.schuetz@ncsc.admin.ch
www.ncsc.admin.ch