topDNS Best Practice Series Part 3: How to Investigate Online Abuse with Free Tools

The topDNS webinar on "How to Investigate Online Abuse with Free Tools" was held on 10 August 2023. This was the third in a series of topDNS best practice webinars which showcase what the domain name industry is doing to fight DNS abuse. The webinar was moderated by Lars Steffen, Director International at eco – Association of the Internet Industry.

The specific aim of the webinar was to enable staff to conduct investigations using free tools. To support such staff, the core speaker at the webinar was:

- Theo Geurts, a Certified Information Privacy Professional (CIPP) and Governance Risk and Compliance (GRC) Officer at Realtime Register B.V. in the Netherlands

In commencing his input to the webinar, Theo Geurts indicated how, as a domain registrar, he proactively tackles problems related to abuse reports and investigations, going beyond the mere receipt of reports. To get to grips with these issues, he uses abuse reports to identify patterns, which he then turns into keywords. In so doing, Theo is of the strong view that using contextual keywords to distinguish between false positives and actual threats is of utmost importance.

As Theo informed the participants, on a daily basis he applies an export of all the new domain names that have been registered. He then uses a range of tools to analyze and identify patterns in these domain names associated with malicious activities. openSquat, for example, can quickly scan domain names for potential malicious behaviour. In addition, as he pointed out, urlscan is extremely valuable in enabling the bulk submission of domain names for scanning, and also facilitates a choice upon which country to scan from. In this regard, he provided an example as to how he had noted earlier that year how certain resells had a sudden high volume in Vietnamese registrations, with his consequent choice being to scan from Japan.

In order to identify phishing campaigns caused by cybercriminals, what is needed are external tools and a process in which every abuse report that is received is strictly documented and analysed. When records aren't defined and there is a need to dig a little deeper, Theo pointed out that switching to Pulsedive.com enables new data to be sent in and enables further enriched intelligence to be extracted: in his showcasing of Pulsedive in the webinar, Theo provided an example of how crucial the analysis of the domain names' SPF record could be.

Moving on, in his reference to cryptocurrency scams, Theo expressed the opinion that a particularly good approach is to undertake research with available images. In this regard, Intel Techniques offers a wide range of search tools. Theo also touched on detecting deep fakes,

such as sophisticated AI-generated videos which can convincingly mimic real people, making it increasingly difficult to distinguish fact from fiction. He recommended utilising tools to identify AI-generated images, and underscored the challenges and evolving nature of investigating online threats and the importance of adapting strategies to address emerging issues like deep fakes. In discussing the use of various search engines for research, he reported that his current preference is Google Images, followed by Yandex and TinEye.

A further tool that Theo regularly uses when he receives abuse reports is VirusTotal: this analyses suspicious files, domains, IPs and URLs to detect malware and other breaches. Theo also displayed how the tool CyberGordon can be used when scannings and investigations have already taken place: in entering the domain names that have been investigated, this tool quickly provides threat and risk information about observables like IP address or web domains.

Furthermore, when staff need to know aspects concerning the SSL certificate, a very powerful and transparent tool is Certificate Search. This provides staff with an opportunity to review SSL/TLS certificates that have been issued in their organisation's name, and offers a significant degree of information about the domain names.

Towards the end of the webinar, based on Lars' inquiry as to how the tool known as epieos gathers the information about LinkedIn accounts, Theo noted that this tool is connected to multiple APIs. The epieos tool not only checks email addresses, but it also returns which accounts are in use for that email address, which can be LinkedIn accounts, pornhub, github, etc; overall, it checks around eighty-eight digital services.

The webinar ended with a final question about the time spent on investigations. In this context, Theo noted that it varies due to his collaboration with law enforcement agencies and his daily research routine.

The following topDNS Best Practice Series will take place on 19 September 2023, covering the topic of "Recognising good practice in the DNS – towards positive, data-driven policy discussions".

List of tools

openSquat:	https://github.com/atenreiro/opensquat
urlscan:	https://urlscan.io
Pulsedive:	https://pulsedive.com
Intel Techniques:	https://inteltechniques.com/tools/Images.html
Google Images:	https://www.google.com/imghp
Yandex:	https://yandex.com
TinEye:	https://tineye.com/
VirusTotal:	https://www.virustotal.com
CyberGordon:	https://cybergordon.com
Certificate Search:	https://crt.sh
epieos:	https://epieos.com