



IMAGE: THE RECORD

Catalin Cimpanu | January 19, 2022

## EU wants to build its own DNS infrastructure with built-in filtering capabilities

Government

News

Technology



The European Union is interested in building its own recursive DNS service that will be made available to EU institutions and the general public for free.

The proposed service, named **DNS4EU**, is currently in a project planning phase, and the EU is looking for partners to help build a sprawling infrastructure to serve all its current 27 member states.

EU officials said they started looking into an EU-based centrally-managed DNS service after observing consolidation in the DNS market around a small handful of non-EU operators.

“The deployment of DNS4EU aims to address such consolidation of DNS resolution in the hands of few companies, which renders the resolution process itself vulnerable in case of significant events affecting one major provider,” officials said in [the DNS4EU infrastructure project](#) revealed last week.

But EU officials said that other factors also played a role in their decision to build DNS4EU, including cybersecurity and data privacy.

### DNS4EU to include powerful filtering capabilities

The EU said that DNS4EU would come with built-in filtering capabilities that will be able to block DNS name resolutions for bad domains, such as those hosting malware, phishing sites, or other cybersecurity threats.

This filtering capability would be built using threat intelligence feeds provided by trusted partners, such as national CERT teams, and could be used to defend organizations across Europe from common malicious threats.

It is unclear if DNS4EU usage would be mandatory for all EU or national government organizations, but if so, it would grant organizations like CERT-EU more power and the agility it needs to block cyber-attacks as soon as they are detected.

In addition, EU officials also want to use DNS4EU’s filtering system to also block access to other types of prohibited content, which they say could be done based on court orders. While officials didn’t go into details, this most likely refers to domains showing child sexual abuse materials and copyright-infringing (pirated) content.

The EU said the proposed DNS4EU system would also have to comply with all data processing laws, such as the GDPR, ensure that domain name resolution data is processed in Europe, and prohibit the sale or monetization of any personal data.

As for the technical details, DNS4EU would also have to support all modern DNS standards and technologies, such as DNSSEC, DoT, DoH, and also be IPv6 compliant.

Once launched, officials said the service would be available to anyone, including the private sector and home consumers, and not just for public institutions.

The company or companies that will be selected to build DNS4EU will also be tasked with creating and running a website with instructions on how users

The company or companies that will be selected to build DNS4EU will also be tasked with creating and running a website with instructions on how users could modify their devices' DNS settings to use DNS4EU servers for name resolutions.

## Commendable effort, but success will depend on many factors

"I think this is a necessary initiative within a strategy of digital sovereignty: Europeans should have the readily available option of a free EU-based public resolver, as an alternative to Google's current dominant service and other similar non-EU ones," [Vittorio Bertola](#), Head of Policy & Innovation at Open-Xchange, a company that provides email and DNS services, told *The Record* in an email today.

"Should Google's service become unavailable in Europe for any reason, those who currently use it should find an immediate replacement; moreover, given the CLOUD Act and the recent rulings on EU-US data export, using any service owned by a non-EU conglomerate is becoming impossible in GDPR compliance terms for many companies and especially public institutions," Bertola added.

"The mere existence of an effective alternative would already be an important achievement and a safety net for Europe, even if most users ordinarily continued to use other services."

However, Bertola also questions how DNS4EU will sustain itself in the long run, as the service has been prohibited from monetizing any of its users' data, nor will European network operators have any incentives for promoting the service, as it would be eventually cutting out a part of their profits.

"Another important topic will be that of compliance. Global resolvers claim not to be subject to any national blocking orders in Europe (e.g. against Pirate Bay or SciHub); in fact, being able to access illegal websites is one of the strongest drivers for users to drop their local ISP's resolver and move to a foreign global service," Bertola said.

"A European service won't be able to ignore the issue, though," he said.

"All in all, the effort by the Commission is commendable and many players will definitely consider bidding, but whether they will actually do so and whether this will be able to produce a change in the long term will depend on several factors that have still to be understood."



Tags

[DNS](#) [DNS filtering](#) [DNS4EU](#) [European Union](#)



Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

[< Previous article](#)

[Next article >](#)

### BRIEFS

**Red Cross begs hackers not to leak data of "highly vulnerable people"** | January 19, 2022

**Bipartisan bill would boost satellite cybersecurity** | January 19, 2022

**Man tasked with preventing fraud at DHS pleads guilty to defrauding the government** | January 14, 2022

**Hackers deface Ukrainian government websites** | January 14, 2022

**FCC proposes stricter data breach reporting rules** | January 12, 2022

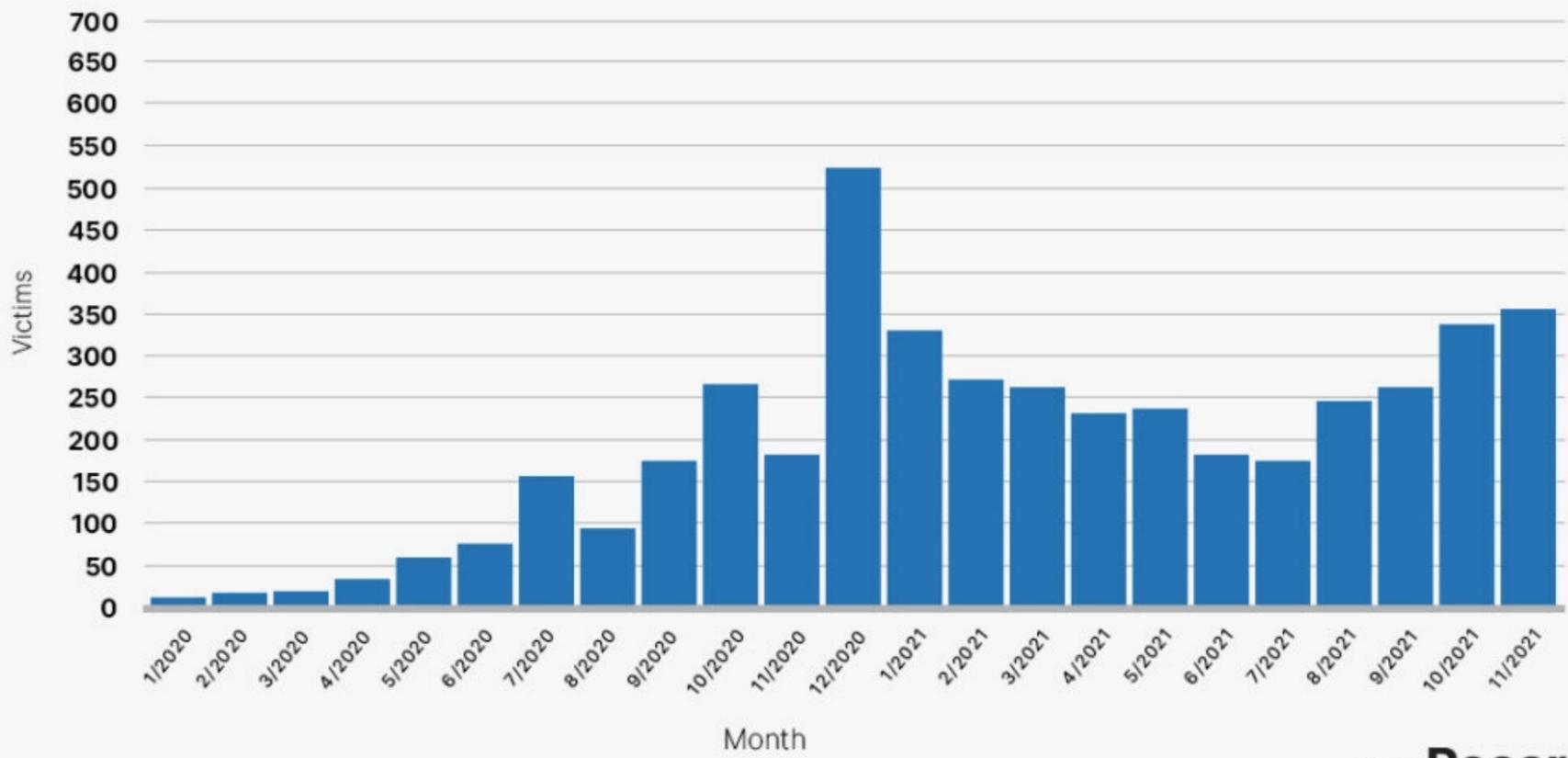
**Senate confirms NTIA head, but other cybersecurity nominations still on hold** | January 12, 2022

**Senate okays bill to promote cyber coordination between DHS, local governments** | January 12, 2022

**EA blames support staff for recent hacks of high-profile FIFA accounts** | January 11, 2022

### RANSOMWARE TRACKER: THE LATEST FIGURES [JANUARY 2022]

## Victim Data Released on Ransomware Extortion Sites



The Record.  
BY RECORDED FUTURE

© Recorded Future

[RANSOMWARE TRACKER: THE LATEST FIGURES \(JANUARY 2022\)](#)

The Record.  
BY RECORDED FUTURE



[About Us](#)   [Privacy Policy](#)

© Copyright 2022 | The Record by Recorded Future