Issue 1 - Year 8, May 2022

.eu Powered by EURid

Illustrated

.eu and Online Security

Dear reader,

At EURid, we believe that the provision of accurate data is an increasingly important tool in combatting fraudulent domain name use. Therefore, our main objective since the early days of .eu top-level domain has been to fight online abuse and ensure the quality of the data we publish.

In this issue of the .eu Illustrated you can read about the AI tool EURid is using to tackle cybercrime and our collaborations with organisations such as EUIPO and TaC. We also bring you tips on how to stay safe online, and testimonials from .eu users fighting online abuse in different fields.

Enjoy the read!
EURid team

Not in our domain: How EURid is using AI and global cooperation to tackle cybercrime

By Alastair Gill (a British journalist and editor focusing on geopolitics, culture and technology)

EURid is taking an innovative approach to help outwit cybercriminals, including a software solution that is helping to identify potentially malicious registrations at source.

Domain names are a key link in the chain that facilitates abusive online activity. If cybercriminals are able to register a domain name, they have a platform from which to target their victims, whether via phishing, spam, botnets, or malware.

Fighting domain name abuse is a constant challenge for EURid, which is an attractive domain for ambitious businesses looking to reach other markets and secure future growth: the .eu top-level domain represents 30 countries (EU and EEA member states), EEA citizens around the world and around 450 million people with one clear extension. A tempting opportunity for cybercriminals.

EURid's answer is the Abuse Prevention and Early Warning System (APEWS), a groundbreaking solution that uses AI and professionally curated incident lists to analyse domain name registrations and delay potentially abusive ones before they are able to carry out any attacks. EURid began working on the project in cooperation with KU Leuven in 2017, and APEWS finally went online in December 2019.

APEWS vs. abuse

If the APEWS system flags a domain name registration as possibly linked to misuse, it is placed on hold pending further verification before it is delegated to the .eu zone file. This means that any services attached to the domain name (such as a website or email) will not function until the registrant's identity has been fully corroborated.

"If we detect that a domain which has been registered shares some similarities with something that was abusive in the past, we ask the registrant about their identity – are you really the person that you say you are? Could you please identify yourself?" says Jordi Iparraguirre, Innovation Manager at EURid.

Suspicious cases are not only reviewed by EURid itself – the organisation also shares details of the registration with cybersecurity experts and law-enforcement bodies like Europol. But what makes a registration suspicious?

"We're not just looking at the domain name itself," explains Iparraguirre, whose role at EURid is to lead the development of new products and services so as to better serve .eu users. "We're looking at lots of metadata around that domain. The system is fed with lists of domains that for instance, have been used for spam or phishing in the past."

This kind of historical data helps the system to tag a registration as potentially abusive – even if the domain is not the same as a previous offender. In most cases further checks are necessary, says Iparraguirre, but "when you see sites that are selling counterfeit products, you can be almost certain. Or a clone of a bank webpage – we've seen that – or the tax office, then that's clear."

Some cyber criminals make amateurish attempts to prove their identity by submitting expired ID cards or retouching dates and information – “We’ve seen masters of Photoshop sending very interesting ‘proof’,” says Iparraguirre – but the people behind most suspicious registrations disappear and the registrations are subsequently suspended.

EURid is setting up systems so registrants can self-validate their identification using eIDAS (a European-wide system for electronic identification) or credit card, as well as other methods. EURid does not keep personal data, it simply checks whether the registrant’s identity has been validated by these trusted ID schemes.

Global events such as Covid-19 are a gift to abusers as they are usually impossible to predict, making it essential for cybersecurity bodies to react quickly to new threats. The coronavirus outbreak in 2020 and the ensuing global pandemic saw an explosion in fraudulent online activity as cybercriminals around the world seized upon the health crisis to exploit people’s fears by selling them fake tests, certificates, masks or sanitisers.

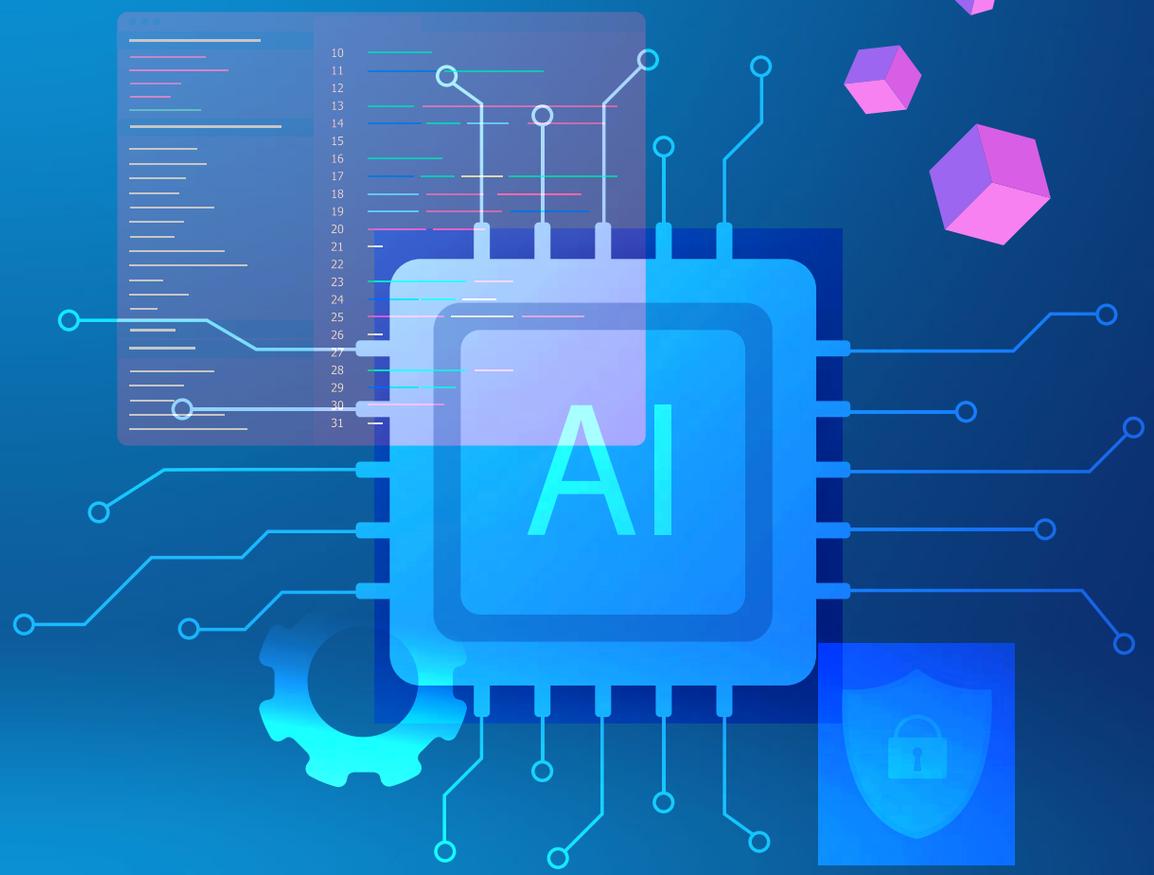
In response, EURid updated APEWS to protect end-users from potential misuse of domain names by programming it to perform additional checks if newly registered domain names contained keywords related to the pandemic.

Change is the challenge

According to Sameh Mannai, a data scientist and AI software developer at EURid, APEWS has shown excellent performance in detecting malicious campaigns – 80% recall [the proportion of actual positive labels correctly identified by the model] and 80% precision – but while it is capable of self-training, the system still requires input when cybercriminals suddenly alter their approach – as they often do.

“The main challenge is that the behaviour of abusers is continually changing, and the data is different, the performance of APEWS will naturally degrade over time and we have to feed the system with new data so that it can recover and improve its performance,” she explains.

“It needs to be constantly updated with new training data to remain accurate over time, but this is the case for most machine learning models. And this is what APEWS does: it automatically retrains regularly to catch up with these changes.”



Educating the younger generation

Beyond its own in-house projects, EURid collaborates actively with a number of other organisations on initiatives to combat online abuse. One is the Youth IGF, created and administered by TaC-Together against Cybercrime International, a global non-profit anti-cybercrime organisation based in Geneva and Paris. The main goal of the Youth IGF, which has been the leading youth movement on internet governance since 2011, is to help victims of internet crime and develop educational tools on online safety and cybersecurity for various stakeholder groups.

“As one of the partners of the Youth IGF, EURid is helping the Youth IGF to bring the voice of youth on the digital world to policy makers,” explains TaC founder and director Yuliya Morenets. “Cybersecurity is a strong focus of the Youth IGF’s work.”

By supporting the Youth IGF, EURid contributed to the implementation of innovative solutions like CyberVictim.Help, which provides victims of cybercrime with assistance.

“At the beginning of the pandemic, we launched CyberVictim.Help because cases were rising and there was a need to provide victims with an immediate response. Our trained Youth IGF Ambassadors made this real-time assistance possible, as they are located in different time zones and different linguistic regions.”

Protecting brands from abuse

When it comes to abuse prevention, businesses can also reduce risk by protecting their intellectual property rights at the European Union Intellectual Property Office (EUIPO).

EURid has collaborated closely with the EUIPO for several years and in 2020 it strengthened its efforts by helping users of the EU IP system to obtain trademark and domain name protection so that their brands are secure.
“We’re well aware of the risks entrepreneurs encounter when they launch and run their businesses,” says Ingrid Elisabeth BUFFOLO, director of EUIPO’s Customer Department.

“Here at the EUIPO we are fully committed to supporting EU business. For example, when a company registers a European trademark, the applicant can immediately access information in order to understand whether an identical or similar .eu domain name is already registered. Offering this information to a European trademark applicant will facilitate the registration of the company´s .eu domain name, avoiding cybersquatting or domain name abuse.”

An AI on the future

EURid is also working on a number of other applications of AI technology. It is developing automatic multilingual web page classification, and has implemented a system that offers new registrants a choice of alternative available domain names if the one they want is already registered.

Cyber criminals may be constantly improving their tactics, but EURid is showing that through the intelligent use of innovation and strategic alliances it is possible to stay one step ahead in the game.

Be safe online tips for SME`s

By Emily Taylor

Small and medium sized enterprises (SMEs) form the beating heart of the EU economy, representing 99% of businesses and employing 100 million people. Many SMEs are entwined in complex supply chains, meaning that a cyber-incident affecting one EU small business could have widespread impact. The Kaseya supply chain attack in 2021 affected organisations all over the world, interrupting 20% of Swedish retailers and kindergartens in New Zealand.

Cybersecurity should be an integral part of any SME's planning and risk management. Yet, for many, cybersecurity can feel daunting and management can be fearful of addressing the issue in case it requires money, time and skills that the business just doesn't have.

The good news is that by taking a few simple steps, SMEs can potentially avoid the majority of cyber incidents. You may not win prizes for your cyber security, but you improve your peace of mind and –as an added benefit–your GDPR compliance posture.

Here are three tips to help you improve your cyber security.

- Don't go it alone.

There are really good, practical guides to help SMEs, written by experts who understand the limited capacity and budgets of small businesses. ENISA's cybersecurity for SME's [https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes] is an example, and contains recommendations centred around people, processes and technical measures.

- Talk to your team

With limited resources, most SME's can't afford to hire dedicated cyber teams. Instead, you can raise awareness among your team, so that everyone is contributing to helping your business be better at cyber. If you succeed at making your team more aware of how to spot phishing and social engineering attacks, you could potentially avoid more than 80% of exploits.

- Simple technical steps

Three technical measures which are cheap or free can help to improve your cyber posture. Encourage your team to use unique, long passwords (three random words is current best practice advice), use password manager software with permissions to prevent your key people getting locked out of systems, update your software regularly and consider migrating your enterprise to cloud services. These straightforward measures are achievable and can help to move you onto a stronger footing.

Testimonials

betterinternetforkids.eu

Better Internet for **Kids**

Supporting the European Commission's strategy for a better internet for children, the key vision behind the Better Internet for Kids (BIK) platform is to create a safer and better internet for young people in Europe. In more practical terms, its mission is to foster the exchange of knowledge, expertise, resources, and best practices between key online safety stakeholders, including those that support children and young people when they go online (such as parents, carers, and educators), the European network of Safer Internet Centres (SICs), industry, policymakers, and the research community. It aims to foster a safe digital environment, increase access to high-quality content and services, step up awareness and empowerment, and fight against child sexual abuse and exploitation.

stoponlineviolence.eu

CYBERSAFE is a project funded by the European Union. Nine project partners from various European countries have developed and promoted an innovative experiential educational prevention programme – the CYBERSAFE Toolkit – that includes playful online tools, to address the issue of online violence against women and girls among young people in a classroom setting. CYBERSAFE promotes healthy relationships and gender equality online. The CYBERSAFE Toolkit provides information and tools to prepare and facilitate four workshops on the issues of gender-based online violence to raise awareness and encourage and support young people in safe and responsible online behavior.

CYBER SAFE

Yellowcube.eu

Founded in 2005, Yellow Cube is a multi-national, cybersecurity oriented, value added distribution group of companies with a local presence in 15 countries. Headquartered in Hungary, Yellow Cube has offices in Budapest, Bratislava, Bucharest, Warsaw, Kiev, and Ajka. With products covering both infrastructure and human security, Yellow Cube provides a wide range of solutions from basic cybersecurity hygiene to artificial intelligence-based advanced threat protection.

yellowcube

Myhealthmydata.eu

Launched in November 2016, MyHealthMyData (MHMD) is an H2020 Research and Innovation Action poised to build the first open biomedical information network based on the connection between organizations and the individual. MHMD's mission is the development of a blockchain-based data platform for biomedical data sharing, where hospitals will be encouraged to make duly anonymized health records available for research and industrial development, thus extracting maximum value from their database. At the same time, citizens will be given the opportunity to become the ultimate owners and controllers of their health data, by collecting it into personal data accounts for individual use and setting personalized dynamic consent options to grant, deny or revoke data access for different uses. The ultimate goal of Myhealthmydata.eu is improving the quality of healthcare, fostering clinical research and innovation and creating added value for the EU economy.

MY HEALTH
MY DATA

How to reduce the chance of falling prey to cybercriminals?

As with any crime, cybercrime does not seem real until you become a victim of it. Here are some useful tips to stay safe online:

Be careful when sharing personal information online

Change your passwords regularly

Use the strongest privacy settings offered by social media websites

Check your browser window for the “https” secure website indicator before entering credit card or bank details

Never click on links in emails from people that you do not know and be cautious opening links from people that you do know. It is safer to open your browser and type in the URL manually.

Make sure your computer’s antivirus software is up to date.

..eu ..ею ..ευ

The dots you can trust.

Published by EURid vzw | Telecomlaan 9, 1831 Diegem, Belgium | Tel. +32 (0)2 401 2750
www.eurid.eu | Editor Reelika Kirna | press@eurid.eu