Saving World Health Day: UNICC and Group-IB Take Down Scam Campaign Impersonating the World Health Organization

unicc.org/news/2021/04/29/unicc-and-group-ib-take-down-scam-campaign/

Maria Thomsen 29 April, 2021

UNICC, together with Group-IB, a global threat hunting and adversary-centric cyber intelligence company that specialises in investigating high-tech cybercrimes, detected and took down a massive multistage scam campaign circulating online on April 7, World Health Day. Scammers created a distributed network of 134 rogue websites impersonating the World Health Organization (WHO) on its health awareness day, encouraging users to take a fake survey with a promise of funds in return. The scheme targeted millions of users around the world with the goal of tricking them into visiting fraudulent third-party websites.

Group-IB Digital Risk Protection Team detected the campaign and reached out UNICC's Common Secure team as a trusted contact for cyber threat intelligence matters within the UN in order to assure that competent contacts with WHO are aware of its existence.

Group-IB Digital Risk Protection Team performed the takedown of all the scam domains. Group-IB researchers established that one scammer collective, codenamed DarkPath Scammers, is likely to be behind the campaign. The investigation is underway.

Cyber-hygiene for the Sustainable Development Goals

UNICC works with the World Health Organization and many other UN Agencies to deliver on their mandates, represented by the Sustainable Development Goals, a collection of 17 interlinked global goals designed to be a blueprint to achieve a better and more sustainable future for all. Whether it's health, eradication of poverty or hunger, rights for women and girls, actions to take on climate change, economic justice, sustainable cities and communities, or for peace and justice around the world, UNICC provides digital business solutions, including a threat intelligence network for over 30 UN Agencies and international organizations.

> *After warning us, we knew Group-IB was the team to deal with this World Health Day scam. They have the expertise and tools to get the job of takedown done, in short order.*
>
> *Bojan Simetic, Information Security Specialist, UNICC*

> *We are excited to cooperate with UNICC in the detection and elimination of scams deceiving people into thinking they are dealing with legitimate websites.*
>
> *Dmitry Tyunkin, Head of Group-IB Digital Risk Protection Team*

Detecting the Scam

On April 7, Group-IB alerted UNICC about a fake website impersonating WHO branding, where users were encouraged to answer a few simple questions to earn a 200 Euro reward on the occasion of World Health Day.

Once users answered questions, they were prompted to share links with their WhatsApp contacts. This way scammers tried to ensure the viral distribution of their multistage schema. Group-IB researchers discovered that users would see several fake Facebook comments about gifts commentators supposedly received. When they then hit the Share button they would unknowingly involve friends in the scam by sharing the link with them – instead of the promised reward – with a redirect to third-party fraudulent resources offering participation in another lucky draw.

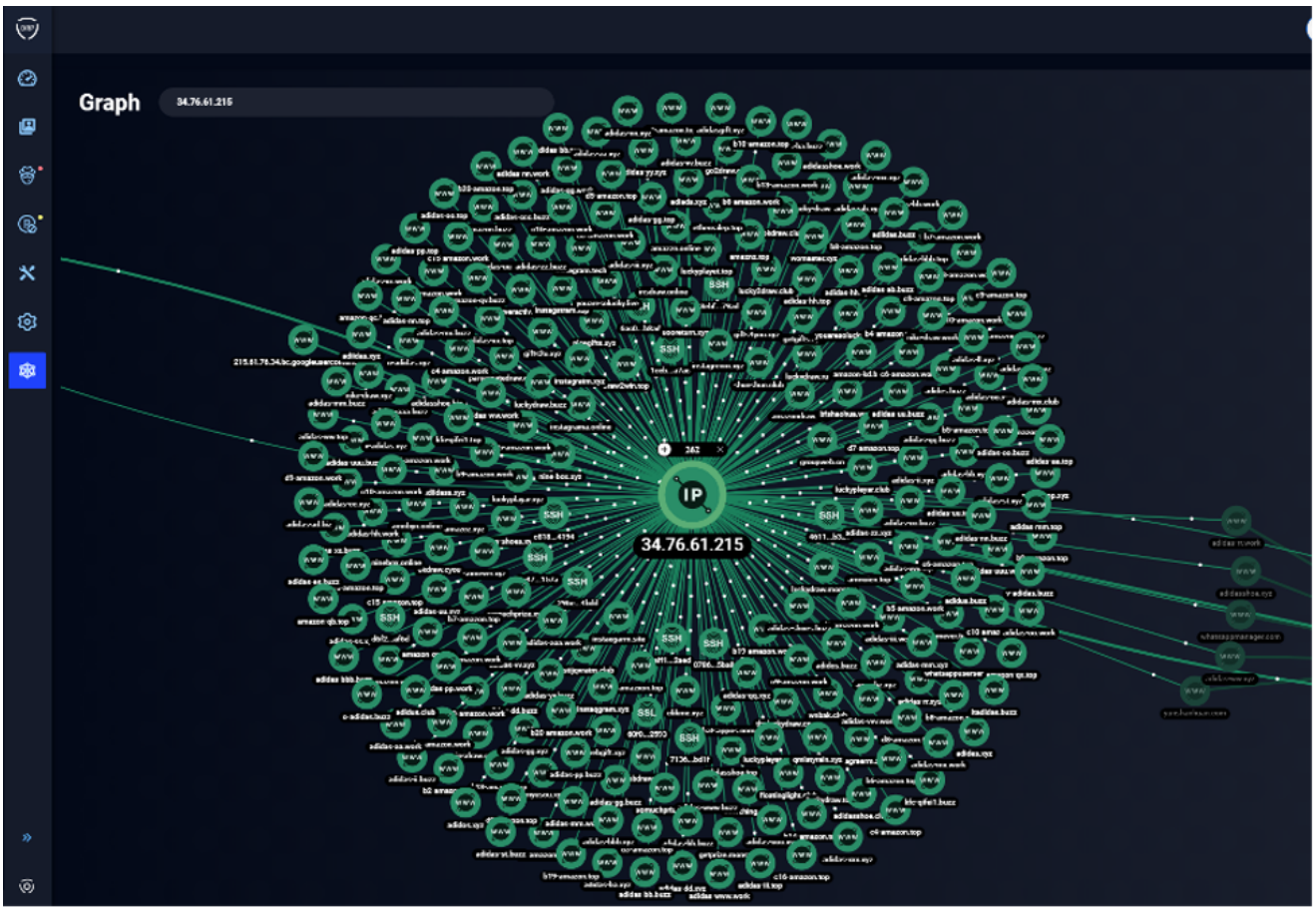
By this time in the scam routine WHO is no longer mentioned as users would visit a hookup website, inadvertently install an extension for their browsers or subscribe for paid services. In the worst-case scenario, users would end up on a malicious or a phishing website.

In addition to the multi-stage nature of the scam, which makes it harder to detect, victims saw customised content depending on their geolocation, user agents and language settings. For example, the currency of the reward would change depending on user location.

What the Scam Looked Like

Group-IB Digital Risk Protection team discovered that it was not a one-off, short-lived website impersonating the WHO brand, but rather a sophisticated distributed scam infrastructure that included a network of 134 almost-identical, connected domains hosting

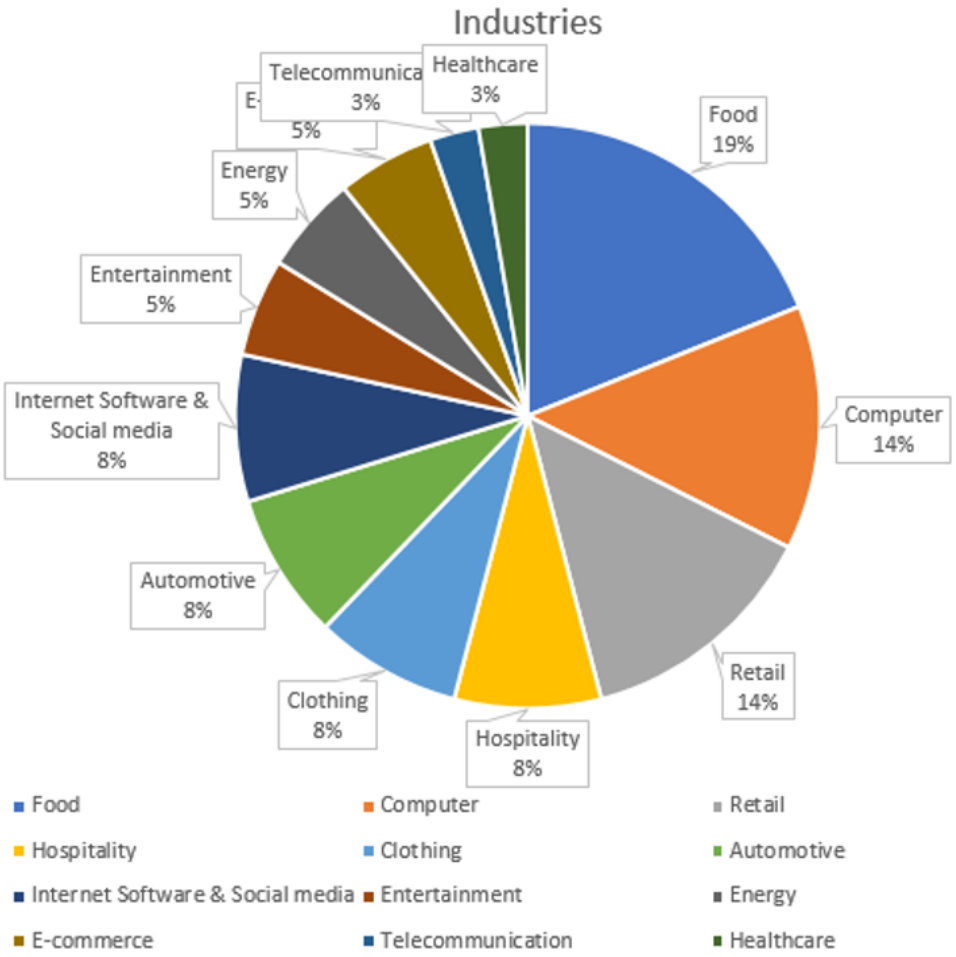
web pages exploiting the World Health Day theme. Within 48 hours upon discovery, Group-IB managed to block all the rogue domains.



Screenshot from Group-IB Digital Risk Protection Platform shows the network of 134 rogue websites impersonating the World Health Organization. Credit: Group-IB

Further investigation found that the 134 domains, identified and blocked by Group-IB, are part of a larger scam network, attributed to a single scammer collective.

Group-IB researchers discovered connections between the blocked 134 websites involved in the WHO scam and at least 500 other scam and phishing resources impersonating more than 50 well-known international food, sportswear, e-commerce, software, automotive, e nergy industry brands. The analysis of websites revealed that cybercriminals used scam kits, similar to phishing kits, which are sets of instruments for the creation and design of scam pages. One scam kit allows impersonating multiple brands at a time using the same template. Interestingly, after the takedown efforts by UNICC and Group-IB, the scammers stopped using the WHO branding across their whole network.



Brands impersonated by DarkPath Scammers. Breakdown by industries. Credit: Group-BI

Scam Syndicate

During the infrastructure analysis, Group-IB researchers examined the domains and other digital indicators and concluded that the whole network is likely to be maintained and controlled by a scammer collective codenamed DarkPath Scammers. Most of the domains with phishing and scam content are using CDN's (Content Delivery Networks) to hide IP-addresses of the real servers. Thanks to its proprietary Graph Analysis system, Group-IB researchers analysed dozens of SSL certificates, SSH keys, DNS and were able to track down malicious infrastructure, unveil the IP-addresses of the real servers where phishing content was stored and connect the domains into one distributed scam network. The scammers are using the same infrastructure configuration with its own traits and misconfigurations across all their servers. Group-IB continues to monitor the scammers' activity.

Most of the scam websites controlled by DarkPath Scammers remain active at the moment and keep targeting millions of users around the world. The scammers advertise their resources using email blasts, paid ads and in social media. According to Group-IB estimates, the scammers' whole network attracts around 200,000 users daily from the US, India, Russia and other locations.

Dmitry Tyunkin, Head of Group-IB Digital Risk Protection team in Amsterdam, noted that “many brands, however, still underestimate the impact of such scams on their businesses and customers. Most organizational approaches to eliminating brand abuse online seems a lot like tilting at windmills. They miss this continuous trend toward the use of multistage scams and distributed infrastructure. Scammers use smart, advanced technologies. They are successful due to the lack of comprehensive digital asset monitoring by brand owners.”

Organizations should carry out seamless online monitoring to promptly detect any cases of illicit use of their brands. Many institutions monitor only separate brand infringements, like phishing pages and domains but overlook other elements of fraudulent infrastructure. To see the comprehensive picture of all brand violations, companies should use Group-IB Digital Risk Protection solutions that will promptly eliminate all brand infringements online on a pre-trial basis without additional investment and lengthy litigation.

To avoid falling prey to this scheme, online users should carefully check the website they are interacting with. It is never redundant to check if the link you’re going to click on is identical to the domain of the organization’s official website since fraudsters often register domain names mimicking official ones. Stay suspicious of any website on which you plan to enter your data is a habit that must be developed by everyone willing to keep their money safe.