

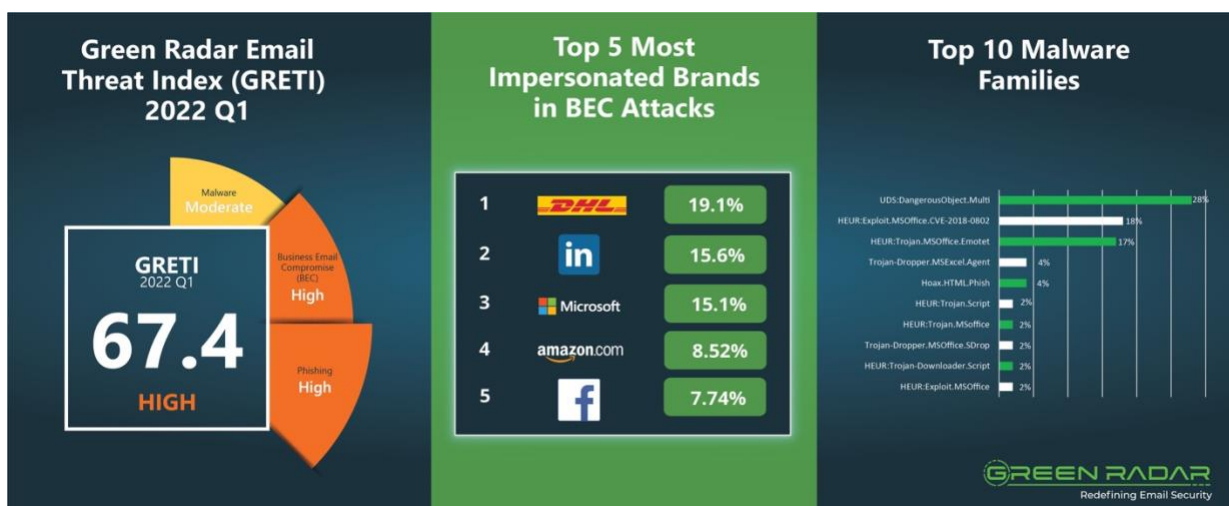
[For Immediate Release]



GREEN RADAR (HONG KONG) LIMITED

Green Radar Announces Email Threat Index for 2022Q1 “Phishing + QR Code” Is Becoming the Most Welcomed Exploit Favourite by Hackers

(Hong Kong, 28 April 2022) Green Radar (Hong Kong) Limited (“Green Radar” or “Company”) released the Green Radar Email Threat Index (“GRETI” or “Index”) for the first quarter of 2022. The Q1 Index scored 67.4, as compared with last quarter’s 65.9, reflected the email threat remained as an imminent risk and was ever growing. According to our analysis, the especially robust phishing and business email compromise (BEC) remained the ‘high’ risk ratings during the period. The quarterly report also reveals that the recent world events including the Russian-Ukrainian conflict and the fifth wave of COVID-19 pandemic in Hong Kong have become the topics of phishing emails that trick users who overlooked the email authenticity and fell prey to hackers.



DHL cements its top position on the list as the most impersonated brand and Facebook debuts on the list

According to the GRETI 2022Q1 Report, BEC attacks leaped from 16.3% last quarter to 52.5% this quarter. Green Radar Security Operations Center (SOC) statistics showed that the top three most impersonated brands are DHL, LinkedIn and Microsoft, which are the same as last quarter. On the other hand, Facebook debuted on the top five list which can be explained by the increased BEC attacks through Facebook. According to the emails intercepted by the SOC, a significant portion of BEC attacks was launched in the name of fundraising campaign for Ukraine, deceived the victims to donate for the country under siege by using their cryptocurrency wallets which would then be compromised for personal credentials and money loss. Corporates were also exposed to similar potential malicious threat.

UDS: DangerousObject.Multi ranked first among the top ten malware families, while HEUR: Exploit.MSOffice.CVE-2018-0802 jumped to the second place from sixth in last quarter, it was followed by HEUR: Trojan.MSOffice.Emotet. SOC also identified Sunseed, a malware targeting European Governments which gathers the whereabouts of Ukrainian refugees and important intelligence that relate to the Russian Government.

From "Volodymyr Zelenskyy" <retail@olympicssp.com> ☆
Subject: Support For Ukraine
Reply to: Support Ukraine <supp0rt4ukrainiens@gmail.com> ☆
To: jenniferhuo@ [REDACTED] ☆
3:28 am

Hello

Amidst the ongoing horrific War brought to us by the Russians. The Ukrainian government is embracing digital assets as it looks for ways to raise money for its military and its dying citizens, most especially our innocent kids.

We want to bring back hope to our land 🍪🍪

The Stand with the people of Ukraine movement now accepting cryptocurrency and other payment methods of donations as supports.

Please find below bitcoin wallet address:
3Dz6gXZJkSNeSPb8pq13GajPC8nEcZd5N6

**Donations are ongoing from 0.1 BTC - 100 BTC and above , We do not ask for a specific amount.
It's a free will donation !!..**

People of the world, We will never forget your support at this hard times, thanks 🍪

We Say No to War !!

We Say No to Destructions!!

We Say No to killing of Civilians !!

Thanks again.
Volodymyr Zelenskyy

For Ukrainians 🍪

(The Russian-Ukrainian War titled phishing email intercepted by Green Radar SOC)

Quishing: The hidden threat behind QR Code Scanning

Shadowed by the pandemic, Hong Kong people increases mobile payment usage to avoid physical contact in our daily life. Merchants tend to make use of QR codes (2 dimensional code) for the payment and promotion purpose by converting their website URLs, hyperlinks of their marketing materials, contact information or addresses to maximize visual effect. The automated ordering process at restaurants has become more common these days, which made QR code more popular. "Quishing" is a tactic that apply QR code in phishing attack, users will enter phishing websites by scanning malicious QR codes.

The statistics of the SOC, showed an increase of 30.2% in phishing attacks. "Quishing" combines the uniqueness of QR code to make successful phishing attacks. By analysing the recent "Quishing" incidents, we learnt that innovative hackers are bypassing email security gateways and the URL scanning feature of PCs' security gate. An U.S.-based cybersecurity company conducted a phishing assessment in September 2021 by sending an audio file in a phishing email, which was identified as a threat by the email security system. Interestingly, they successfully bypassed the security gate with another phishing email with QR code they sent one month later. This gives rise to "Quishing" as a new favourite hacking tactics given that QR code is solely an image that cannot trigger immediate attacks like hyperlink nor a malicious attachment, therefore, it becomes more challenging to identify as a threat by existing email security system.



Welcome to the world of travel with Cathay Pacific

Dear Customer,
Our aim is to always provide a service that is tailored to suit your needs every time you travel with Cathay Pacific.
We would love to hear your thoughts on your recent experience with us.

Please may we ask that you take a few minutes to complete a short questionnaire. The survey typically takes around 3 minutes to complete.

Your feedback is extremely important to us as it will assist us in improving the quality of our products and services.

As a reward , you will be credited cash and miles points .
To access the survey please scan the qr code below :



Thank you for your time.

Cathay Pacific

If you wish to be removed from any future customer research from us, please visit this link. Click here to [unsubscribe](#).

(Similar phishing email intercepted by Green Radar SOC in 2020)

Potential Threat of Quishing

SOC warns incautious scan on the QR code of phishing websites could provide hackers opportunity to compromise your personal accounts easily and lead to personal credentials leakage. With the fact that phishing technique is evolving, “Quishing” is a highly effective exploit tactics prior to actual malicious attack, as it is different nature compared with standard email protection (for instance, URL scan).

Mr. Kenneth Ma, Executive Vice President of Sales at Green Radar, commented, “It is expected that the significant increase of email attacks leveraging the fifth wave of COVID-19 pandemic in Hong Kong. Cyber criminals profit tirelessly from their so-called mind game to trick users. Following the increasing security awareness of enterprises and their staff, hackers plan their strategies ahead and exploit new loopholes. It is therefore essential for companies to keep updated on the latest threats nowadays. Green Radar continues its dedication to email security and staff awareness training as a part of effort to contribute to the industry and clients as a whole, and aim to tackle unknown threats for corporates with the valuable threat intelligence.”

About Green Radar

Green Radar redefines email security and enables organizations to focus on running their business. We operate a Managed Detection & Response (MDR) approach to protect organizations from email threats by combining big data with artificial intelligence, global threat intelligence and a team of cybersecurity experts to keep your inbox safe.

Green Radar is a member of Edvance International Holdings Limited (1410.HK), a leading cybersecurity and innovative technology company headquartered in Hong Kong.

Company website: <https://www.greenradar.com/>

For media enquiries, please contact:

Across Asia Communications Limited

Tango Chan/ Kent Lau

Tel: +852 9731 4992/ +852 9750 5105

Email: tango.chan@acrossasia.hk / kent.lau@acrossasia.hk

Green Radar (Hong Kong) Limited

Carol Yip/ Ruby Yeung

Tel: +852 3194 2266/ +852 3184 9432

Email: carol.yip@greenradar.com / ruby.yeung@edvanceintl.com

Issued by Green Radar (Hong Kong) Limited