[For Immediate release]

GREEN RADAR (HONG KONG) LIMITED

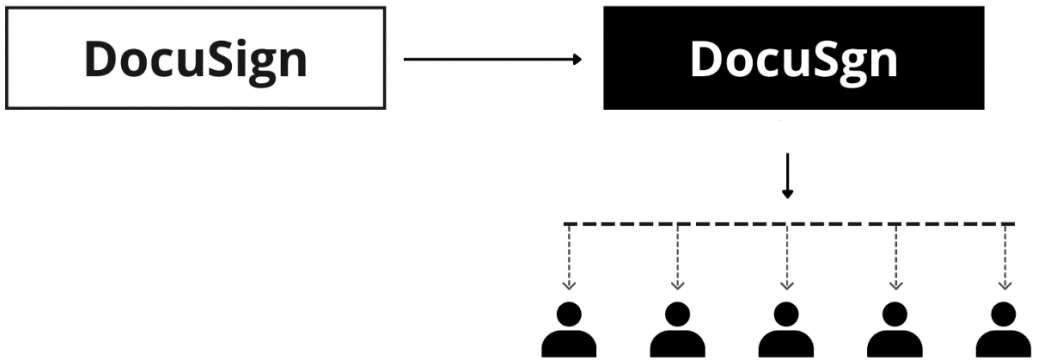
Green Radar Announces Email Threat Index for 1H 2023
ChatGPT reduces phishing costs for hackers; GR one step ahead by using AI

(25th July 2023, Hong Kong) Green Radar (Hong Kong) Limited ("Green Radar" or "Company") has released the Green Radar Email Threat Index ("GRETI" or "Index") for the first half of 2023. The index for the first half is 62.1 (the index released for 2022 was 64.3), the index reflects a moderate decrease compared to the last assessment, though the overall risk level remains 'High'. Compared to the same period last year, Green Radar observes an 1% increase in overall attack volume per email, showing that the overall attack volume is relatively stable. However, in actual terms the absolute increase in attack volume was 86% year on year and is a significant number. Of this volume, the Unknown / Zero Day attacks had increased by 33% vs the same time last year.

The rise of ChatGPT and other AI tools have facilitated hackers to create phishing emails and fake websites more efficiently, thereby lowers the barrier in launching cyber attacks. In another showing of hackers executes timely attacks, to the summer and holiday season promotions were impersonated with fake travel booking emails and websites to defraud credit cards and personal sensitive information. Green Radar's Email Security Operations Center (SOC) intercepted many related phishing emails, most of which were phishing on the grounds that the credit card usage was "suspicious".

LinkedIn ranks no. 1 for most impersonated brand, DocuSign on the list for the first time

According to GRETI statistics in this first half, business email compromise (BEC)attacks recorded a slight decrease over the same period last year. Though that is not to say that the threat is lessening, the top three most frequently counterfeited brands include: LinkedIn, Microsoft and Hang Seng Bank, with Facebook and DocuSign being the fourth and fifth respectively. It is no surprise that Facebook is enlisted, but DocuSign which debuted on the list is worth noting. Founded in 2003, DocuSign is an electronic signature service provider from the United States. It provides a cloud-based electronic signature platform to help enterprises or users quickly create and obtain legal and valid electronic signatures online. Hackers used illegal means to steal their customers' email addresses, forged a fake domain name "DocuSgn" (one letter i less than DocuSign), and disguised themselves as invoices from the financial department to send malicious emails to users. Using DocuSign's brand identity, it is easy to gain the trust of users. Therefore, users are tempted to click on the word documents containing malware without paying attention. In the absence of strong email security solution, this could bring loss to enterprises as their internal data could then be easily hacked.



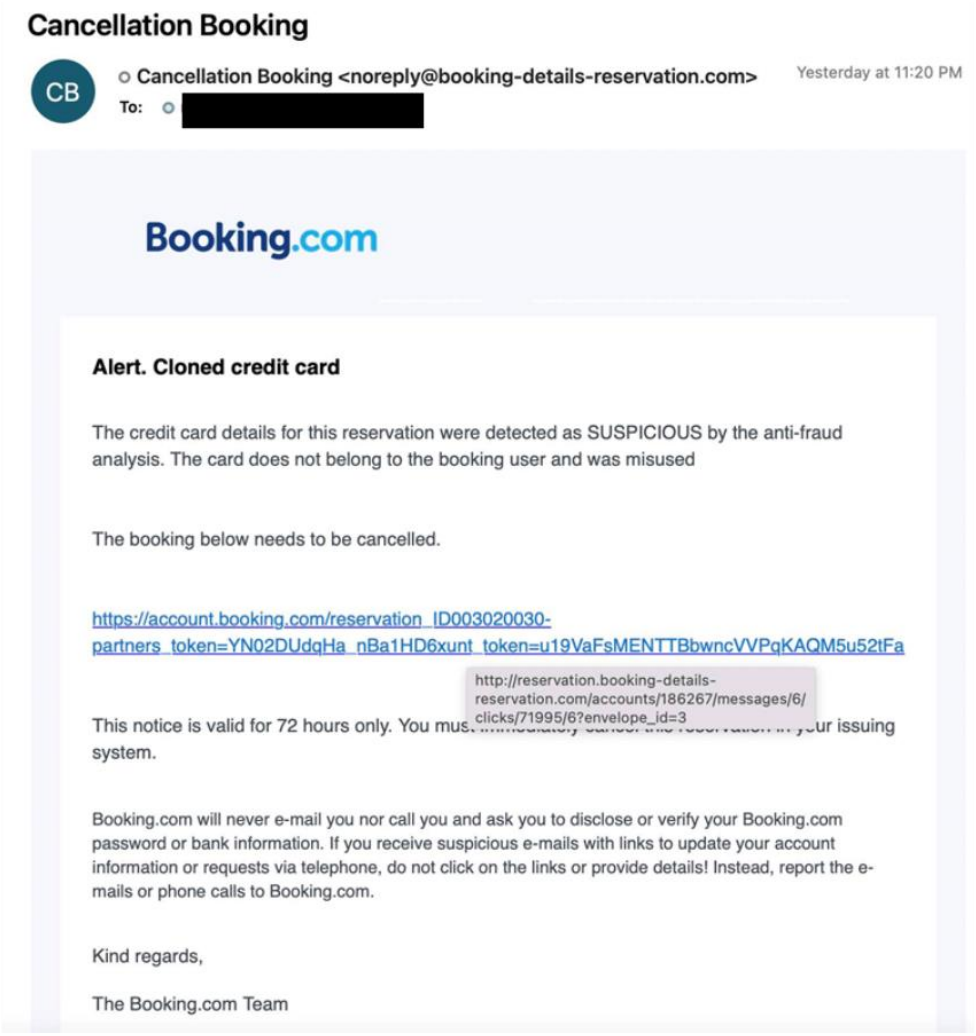
(Schematic diagram of hackers counterfeiting DocuSign)

HEUR:Hoax.HTML.Phish ranks first on the list of top ten malware families, with HEUR:Exploit.MSOffice the second. HEUR:Exploit.MSOffice.CVE-2018-0802 places third. Such ranking indicates that the software is popular among hackers and enterprises should pay more attention to it.

Hackers saw the right time to design phishing traps

With the easing of the epidemic and the recovery of tourism, hackers took advantage of the upsurge to send phishing emails to customers by impersonating travel booking websites. In the phishing case of booking.com, hackers defraud users of their online transaction information and impersonate "websites" to carry out phishing scams, claiming that the credit card usage was "suspicious" and the reservation would be cancelled. Riding on mental manipulation and users' anxiety after receiving these emails, hackers induce users to fall into their trap gradually by luring recipients to click on fake website links to steal their personal and credit card information. "This notice will be expired in 72 hours" and "booking.com will not send you an email or... verify your account password or bank details" are used to gain trust and add urgency.

Users should be viligent when responding over any links. It is essential to understand phishing threats and conduct appropriate awareness assessment training for enterprises, who with its ample staff of different levels of cyberthreat awareness are prime targets for hackers and potential returns high and worthwhile. Early preventions can eliminate potential threats and greatly reduce the risks of data leakage, ransomware, and financial frauds. Green Radar's grMail and grAssessment (phishing assessment services) can provide enterprises with the most appropriate email security solutions, increase employees' understanding of email threats, and become the gatekeepers of your enterprises.



(example of phishing email of hackers counterfeiting booking.com)

Mr. Francis Lee, Executive Vice President, Service Operations at Green Radar, said, "Cybercrime activities are becoming more and more frequent. The emergence of ChatGPT undoubtedly facilitates hackers by writing phishing content, as long as they weigh their words skillfully. Choosing a professional email security service provider with good quality builds the first line of defense to protect the enterprises and strengthen their protection barriers. For future development, we will continue to optimise the technical level of grMail, as well as adjusting and enhancing global and local threat intelligence, monitoring and interception capabilities by using our own developed AI (aidar^{TM}), so as to align with users' needs to defense."

About Green Radar

Green Radar redefines email security and enables organisations to focus on running their business. We take a Managed Detection & Response (MDR) approach to protect organisations 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 was recognised by market research company Frost & Sullivan in 2023 as a leader in email security market in Hong Kong and Singapore, leading the field in terms of technological comprehensiveness and innovation.

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

Website: https://www.greenradar.com/

For media enquiries, please contact:
Across Asia Communications Limited
Mr Adrian Wong / Mr Kent Lau
Tel： +852 6282 6412 / +852 9750 5105
Email: adrian.wong@acrossasia.hk / kent.lau@acrossasia.hk

Green Radar (Hong Kong) Limited
Ms Carol Yip
Tel: +852 3194 2266
Email: carol.yip@greenradar.com
Issued by Green Radar (Hong Kong) Limited