GREEN RADAR

GRETI ANNUAL REPORT 2023

Disclaimer

Publication Date: Feb 29, 2024

Green Radar, the Green Radar logo, greenradar.com and aidar™ are trademarks of Green Radar (Hong Kong) Limited. All third-party company names, products and services and their trademarks (including logos and icons) referenced by this document remain the property of their respective owners, and are used herein without intention of trademark infringements or implied endorsement or partnerships.

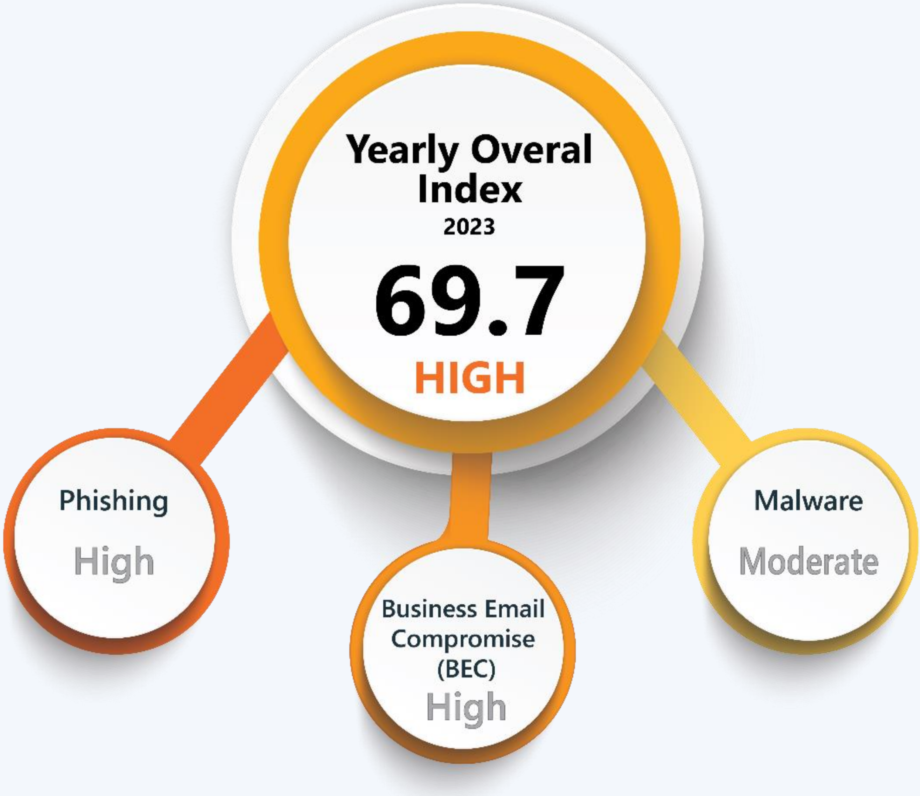
This document is current as of the initial date of publication and may be changed by Green Radar at any time. The report data and case examples cited are presented for illustrative purposes only.
Actual results may vary depending on specific configurations and operating conditions. The contents of this document have been prepared for general information only and are not, and should not be construed as, professional advice, service or opinion provided to the user.

Any market analysis, projections, estimates and similar information, including all statements of opinion and/or belief, contained herein are subject to inherent uncertainties and qualifications and are based on a number of assumptions. The factual information contained in this document has been obtained from multiple sources which are believed by Green Radar to be reliable and accurate as of the date of publication.

No representation or warranty, express or implied, is made as to the accuracy, completeness or reliability of the information contained in this report, and none of Green Radar and its affiliates, related entities, directors, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. Such information has not been independently verified. Any interested party should undertake their own inquiries as to the accuracy of the information. No part of this document may be copied or reproduced in any form or by any means without written permission by Green Radar.

Table of content

1. 2023 Annual Green Radar Email Threat Index (GRETI) Dashboard



2. About the Report

Throughout the last 12 months, Green Radar analyzed millions of phishing attacks and malicious email activities targeting enterprises, their employees, and brands. Green Radar Email Threat Index (GRETI) makes use of the data of 2023 to present key trends shaping the threat landscape. Results presented are extrapolated based on attack volume, frequency and impact levels riding on common malicious email activities. Security leaders and practitioners can use this information to better understand these threats and to take proactive measures to reduce risk.

Email attacks have been used extensively to carry out scams and initiate the most extensive breaches. In the last twelve months, famous organizations in Hong Kong had also experienced numerous infamous breaches where hundreds of gigabytes of data and entire client database information were removed. Subsequent blackmailing and ransom demands reflect the real dangers that no corporate would want to face, neither the brand reputation damage resulted. Other cases of AI-generated deep-faking were well reported that takes on a theme of phishing but could be proliferated in a near future.

Since email attacks primarily targets commercial organizations, holding it to ransom, attacks or fraudulent financial scams, it is imperative that they understand the current threat landscape, and thus making appropriate cybersecurity policies in securing their organizations. Readers must also consider the prevalent shortage in local IT and cybersecurity professionals' availability, making the fight to secure our infrastructure all the more challenging.

Core trends and figures shown in GRETI reports exclude malevolent emails from already-known sources, thus the focus is on malicious email activities that were not seen before and thus by-passing signature-based protections.

For details of GRETI measurements, please refer to Appendix A – GRETI Methodology and Risk Levels

3. Key Takeaways

- Exercise "Zero-Trust" caution and practice for all emails received, especially those that requires follow up actions.

- Threat Index – reflects the increased evasiveness and sophistication to bypass security devices, as well as the convincingness of the phishing emails to the recipients.

- AI gives you what you want! Phishing emails are increasingly AI created. It has evolved from writing generic contents to tailoring contents to an ever more refined group of intended recipients, thus making contents more contextual and authentic.

- Phishing emails continue to be the favoured method of initial breach, with numerous infamous attacks in 2023 that resulted in hundreds of gigabytes of data lost and entire business databases stolen, with the breached organization held to ransom and reputation in tatters.

- QR Code Phishing evolved to be ever more evasive to bypass defenses.

- Phishing emails, integrated with offline platforms that include call centers or deep-fake AI technologies could be devastating. Instructions to call a number or to join a Teams online conference would almost be indetectable by email security defenses but can oblige the recipient into taking fraudulent actions.

- Hackers make use of open platforms extensively to send out, and to host malicious phishing activities. This adds extra complexity for defenses to establish the legitimacy of all emails that make use of such platforms.

- Isolation technology, which prevents interaction with malicious emails, adoption is on the rise, with 18% of users now covered.

- Protecting the administrator account of email systems is paramount to preventing the most damaging BEC attacks, or to protect organizations from the most severe breaches.

- Threat awareness amongst local organizations is low, with over 33% recipients responding to phishing baits during exercises.

4. A Year of Deviously Smart Attacks

2023 was marked by a serious of high-profile infamous breaches. On the ground of the email security defenders, it could be observed that while traditional attack vectors are continuing to be erratic, a number of novel attack types were emerging and becoming popular in the last year, and likely to become mainstream in the coming year. Threat actors have learned and continue to devise ways to bypass traditional automated, and even intelligent email security platforms despite the increase in security tool spending and manpower, as well as investments in security awareness training efforts, and users still fall victim to well-crafted, socially engineered emails.

When reviewing emails, recipients should exercise extreme prudence: assume zero-trust on emails received and react objectively and verify the genuine nature of the email should actions be needed, including but not limited to enquire misunderstanding in account handling, open attachments, carry out managerial instructions, claim rewards or to verify accounts etc. With the nature of phishing emails becoming ever convincing and contextual to the recipient, it is ever easier to be entrapped.

Here we will review some of the latest techniques in phishing attack evasions.

4.1 AI-Generated Client Centric Contextualized Phishing Emails

While AI generated phishing email campaigns have been observed since the advent of AI, the way that phishing email content is written by AI is evolving. Content created by AI was generally generically written to convince a wide population, with natural language and wording. On its own, it is a simple read, and the context is generic to all recipients. However, in the past year, it could be observed that these emails are increasingly written for organizations. The context has evolved so that the gist of the email is relevant to the intended recipient.

These phishing emails were generated for industrial verticals, e.g. created for logistics, retail or financial industry, where a phishing email body contains industry specific information and uses timely industrial information. As these malicious emails were created for an intended group of recipients, these smart contents appear more relevant to the recipient. Even for those who are aware, they are more likely to appear as industrial graymail rather than malicious emails. In conjunction with traditional and evolving phishing techniques, these email poses a real threat in defeating traditional email security measures and deceiving its recipients. techniques, these email poses real threat in defeating traditional email security measures and deceives its recipients.

4.1.1 AI-Generated Attacks to get more efficient

While the most notable evolution of AI usage to generate Phishing email was noted. AI had essentially been exploited for malicious players to increase efficiency of generating phishing campaigns. At minimal, it could be observed that AI was used to create content, setup new domains as source and destination, setup phishing website with new URL and contents etc. Globally, technology like ChatGPT has been exploited by cybercriminals to generate unique content rapidly and in context of the recipient, elevating the sophistication of social engineering attacks and email threats to a new level. As further evolution, generative AI (like WormGPT and FraudGPT, etc) have been created by threat actors, with a view to deploy advanced attacks.

4.2 QR-Code Phishing Quishing Evolution

QR Code Phishing became popular a few years back, and it remains a deviously clever approach to bypass traditional defenses. Traditional QR Codes used in phishing emails were attached as images, so to bypass text-based scanning by defenses and thus have higher chance of success in getting through to the recipients. QR codes are more tightly integrated into mobile devices for easy reads and link redirection, and thus generally convenient for the unmindful recipients, especially those with mobile devices.

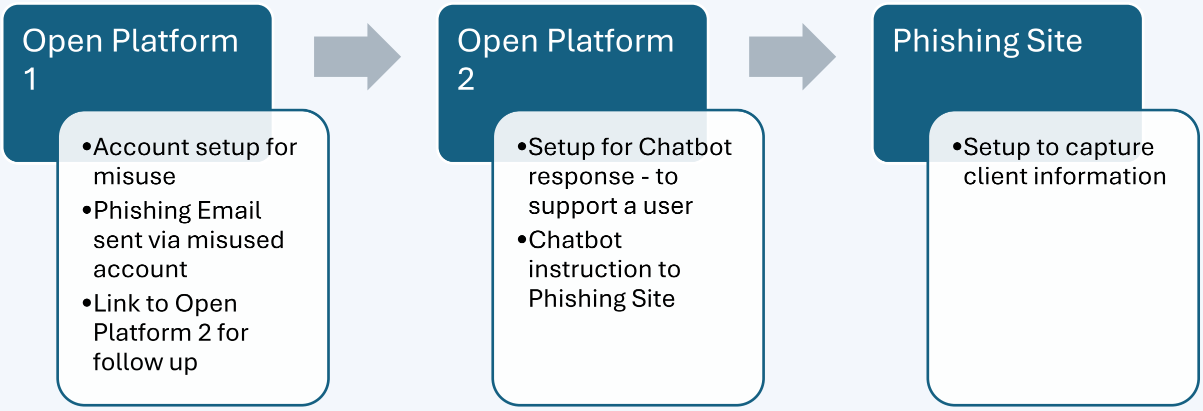
Unfortunately, Quishing remains popular and at minimum it accounts for a sizable portion of all phishing attacks. Defending against Quishing can be challenging due to the limited text content and heavy reliance on images – which are not often parsed by traditional security tools. The lack of threat indicators of compromise makes it difficult for legacy email security solutions to identify and ultimately lead the recipients to the phishing page.

However, the use of QR code in phishing emails has also evolved in the last year. Green Radar was one of the first players to bring out countermeasures that integrate QR code scanning into its defense layers to root out these attacks and evaluate the phishing site. Variations of QR code use, in terms of the image style, logo use, and even attached to PDF or document files attached to the emails etc were deployed to further evade against security measures, and these variations of Quishing threaten to bypass even smart defense platforms even if the base Quishing defense was already integrated. Twists and variations in the way that the QR code was embedded in phishing emails have continued to change and defense layers need to continuously keep up with these variations.

4.3 Open Platform Phishing Bypass

Generally, Phishing emails comprise of an innocuous looking body and a phishing link. Be it that the phishing link be a text-based URL or a QR code or other variations, email defenses generally scan to look for suspicious elements to identify it as potentially malicious. The email source, and actual destination of the phishing URL and QR Code are some of the more obvious elements to look for to verify its maliciousness.

In the last year, some phishing emails could be seen to be initiated from well known public cloud services platforms, with a redirect to another open cloud service platform, from which point the recipient is lead to the real phishing site:



Open Platform 1

- Account setup for misuse
- Phishing Email sent via misused account
- Link to Open Platform 2 for follow up

Open Platform 2

- Setup for Chatbot response - to support a user
- Chatbot instruction to Phishing Site

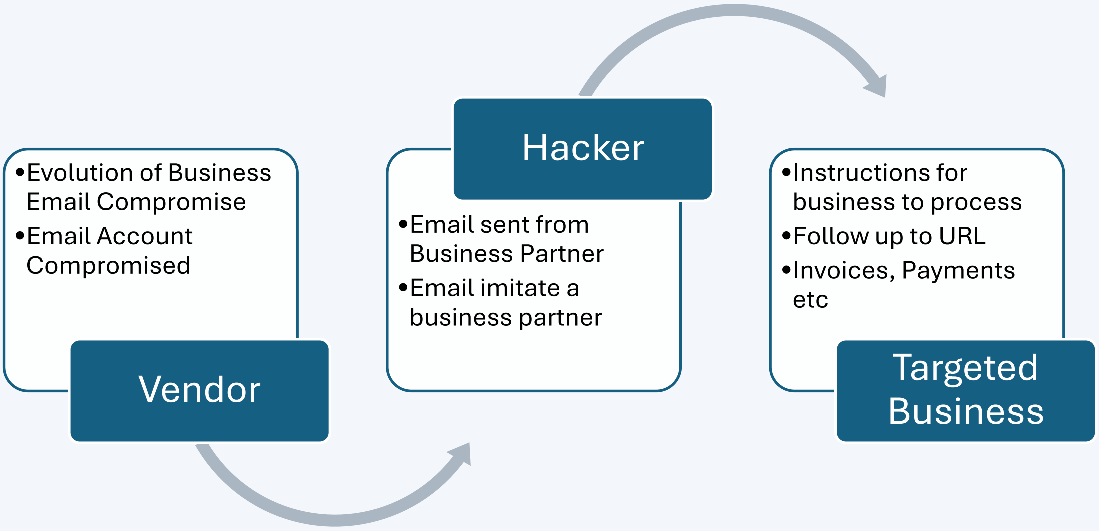
Phishing Site

- Setup to capture client information

This method of setting up phishing attacks could bypass, or at minimal, reduce the effectiveness of email security defenses because it removed some fundamental ways of identifying malicious emails by using a trusted email source, and a trusted URL destination. When used in conjunction with a well-crafted email, e.g. There is a problem with your online purchase account, please follow this link to discuss the issue with our support team (on a well-trusted social media platform), this could potentially bypass some of the most fundamental methods of identifying phishing email source and phishing URLs. When this is used in conjunction with a well-crafted socially engineered phishing email, the chance of getting to the recipient and for the recipient to follow the URL to the phishing site is significantly increased.

4.4 Vendor Email Compromise (VEC)

Vendor email compromise attacks have also seen an increase in frequency over the past year. Malicious players appear to have improvised on BEC and make use of the business partner network of the intended recipient to carry out similarly lethal attacks. Globally, 48% of organizations received a VEC attack in the first half of 2023 alone and a similar trend could be seen to be growing locally. This is an alarming observation given that these attacks require an initial compromise of a partner network, with the imitation of a vendor partner email also being seen in parallel.



- Evolution of Business Email Compromise
- Email Account Compromised

Vendor

Hacker

- Email sent from Business Partner
- Email imitate a business partner

- Instructions for business to process
- Follow up to URL
- Invoices, Payments etc

Targeted Business

These attacks are successful in part because they use or imitate real email accounts with previously established relationships to take advantage of expected financial transactions, and in similar fashions its impact to BEC, a successful breach could result in some of the worst impacts to the organizations. In an age of increased business transparency and extensive social media use, establishing the key VIPs in business relationships, or vendor relationships, is easy and can easily be imitated and exploited.

4.5 Payloadless Phishing & Offline Follow Ups

Another attack type gaining momentum over the past year is payloadless phishing, which could be executed filelessly or non-malware, and with or without URLs. Unlike traditional malware attacks sent via email, payloadless attacks operate without the need for a malicious executable file, making them stealthier and harder to detect by traditional email security tools. In most of these attacks, the email itself could contain no links or attachments but instead obliges the recipient to follow through with some said actions, e.g. to dispute a payment, or to retrieve certain online contents, or to join a video conference etc. Upon following up with these actions the recipient was ultimately deceived. A recent case involved the deep-fake characters of other company staff in a video conference call that resulted in the engaged staff being deceived in a devastating financial scam.

4.5.1 Clone Phishing (of well-known emails)

Evolving from imitating well known brands, clone phishing rides on emails that are regularly sent out from open platforms or service providers. Attackers essentially clone or copy such legitimate email and changes its content with its own phishing malware or URL. One such example detected this year was that hackers replicated a bank's regular notification email for the monthly statement, but the URL points to its own phishing website. The email itself is hard to distinguish from the original, short of close scrutiny of the URL, and if applicable the attachment.

4.6 Other methods of attempted Phishing By-pass

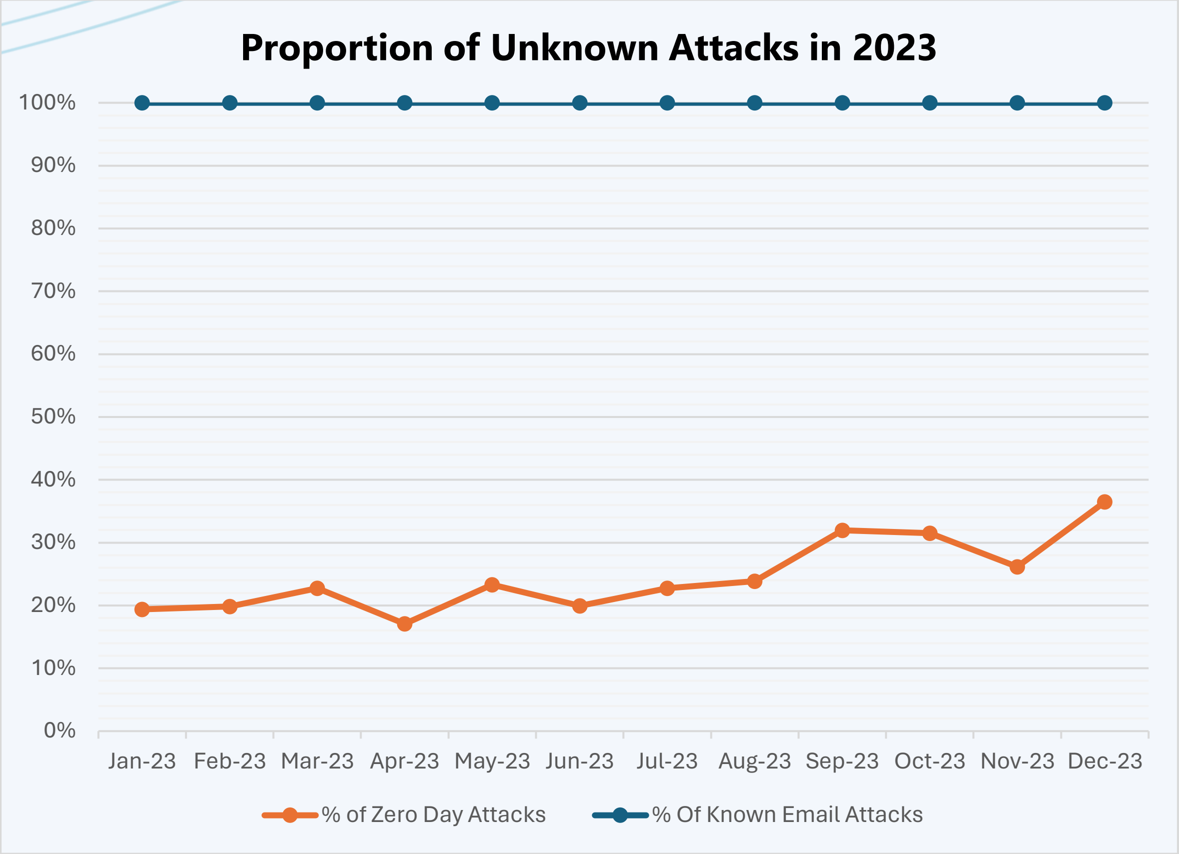
Throughout the last twelve months, various and indeed, inventive and innovative approach were observed to bypass phishing email security defences. In addition to the above outlined techniques, extensive use of password zipped or packaged files was used to attach malwares to phishing emails. Applying passwords to protect files often stops most email defences to scan the content of the attachment, however, in the case of phishing emails, the password is integrated into the email body message thus it includes instructions for the user to unzip or deviously worded as activation codes. This is further made complicated by embedding the password into the email as an image. Variations of this theme were observed throughout the year and email security defenses have to meticulously update its detection algorithm to keep up.

Another interesting technique observed includes an attack known as Right-to-Left Override, primarily used in attachments. Right-to-Left Override (RTLO) is a Unicode character that is used to control the directionality of text in bi-directional writing systems. It is represented by the character U+202E in Unicode.

When the RTLO character is inserted in a string of text, it causes the text to be displayed in reverse order from that point onward. Malicious actors can use RTLO to hide file extensions. For example, they might create a file named "documentfdp.exe" but insert the RTLO character before the "fdp.exe" part. The file would appear as "documentexe.pdf". Unsuspecting users might mistake it for a legitimate PDF document but instead execute the malware without realizing it.

5. A Trend that masks real Dangers

A cursory look at the pattern of Known and Unknown attacks appears to show that the Known attacks have been on the decline over the last year. Known attacks are more easily rooted out, unless the email security defence is minimal or out of date. Thus, known attacks, with known signatures or known sources etc, are unlikely to be able to get through to the recipients.



However, as can be seen here, the proportion of unknown attacks has increased over the year. In short, most users would have been subjected to almost twice as much of unknown, never-before-seen, or zero-day attacks from the beginning of the year to the end of the year. The security concern is not just in quantity but also in quality.

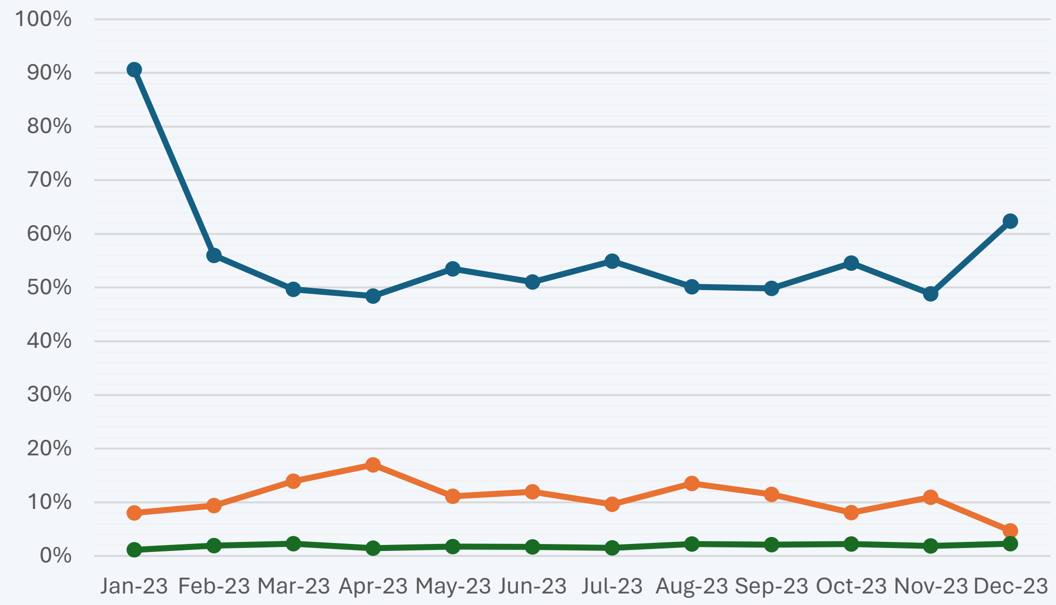
Attacks have been refined, both in quantity and quality. The relative quantitative low proportion of known attacks does not indicate a safe environment, the increasing level of unknown, zero-day attacks presents real threats. The volume of attack is less relevant when compared with the sophistication and the refined craftmanship of these evolving threats.

GRETI does not count the same zero-day email attack twice (Refer to Appendix B for details), and once an attack has been identified further attacks of the same characters are filtered out as Known attacks, thus even when the volume of attacks appears to be gentle rise throughout the year, it should be understood that recipients face new threats everyday, and that we should all consider this a constancy in email security world.

5.1 Key Attack Compositions

Attacks continue to be dominated by Phishing Emails throughout 2023:

Malicious Email Attack Composition throughout 2023

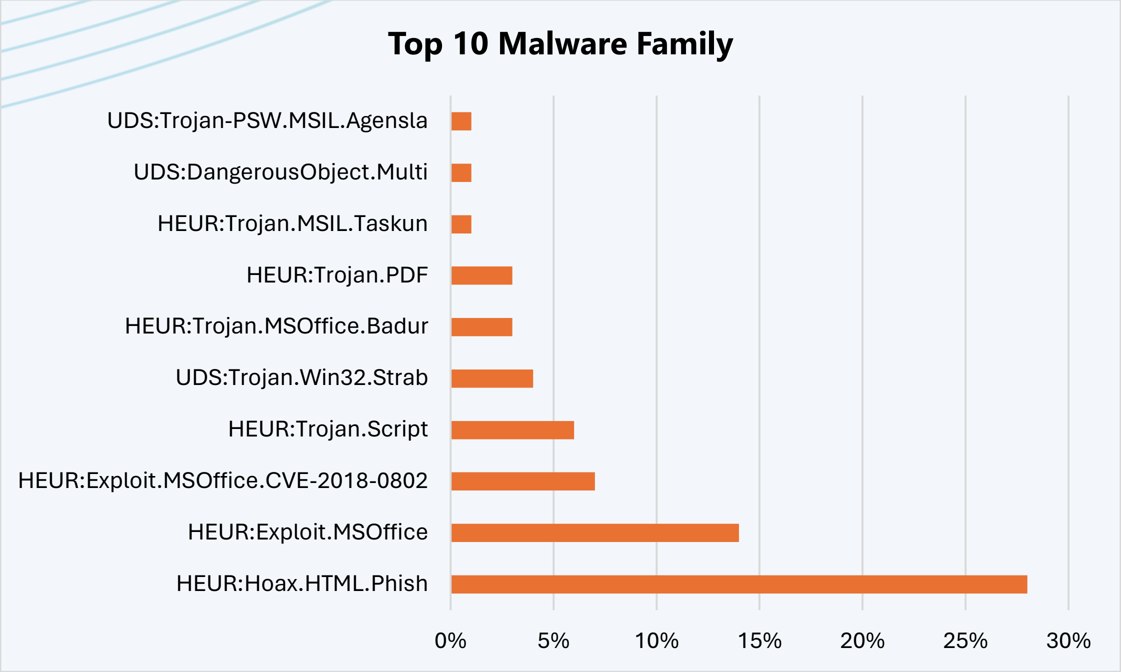


	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23
Phishing Emails	91%	56%	50%	48%	53%	51%	55%	50%	50%	55%	49%	62%
Malwares	8%	9%	14%	17%	11%	12%	10%	14%	11%	8%	11%	5%
BEC	1%	2%	2%	1%	2%	2%	1%	2%	2%	2%	2%	2%

It should be noted that, of most of the phishing techniques described, most are delivered through phishing emails.

5.2 Top malwares

It could be seen that there were multiple payload families being used throughout the last 12 months, with the HEUR:Trojan.Script.Generic being the most frequently spread malware.

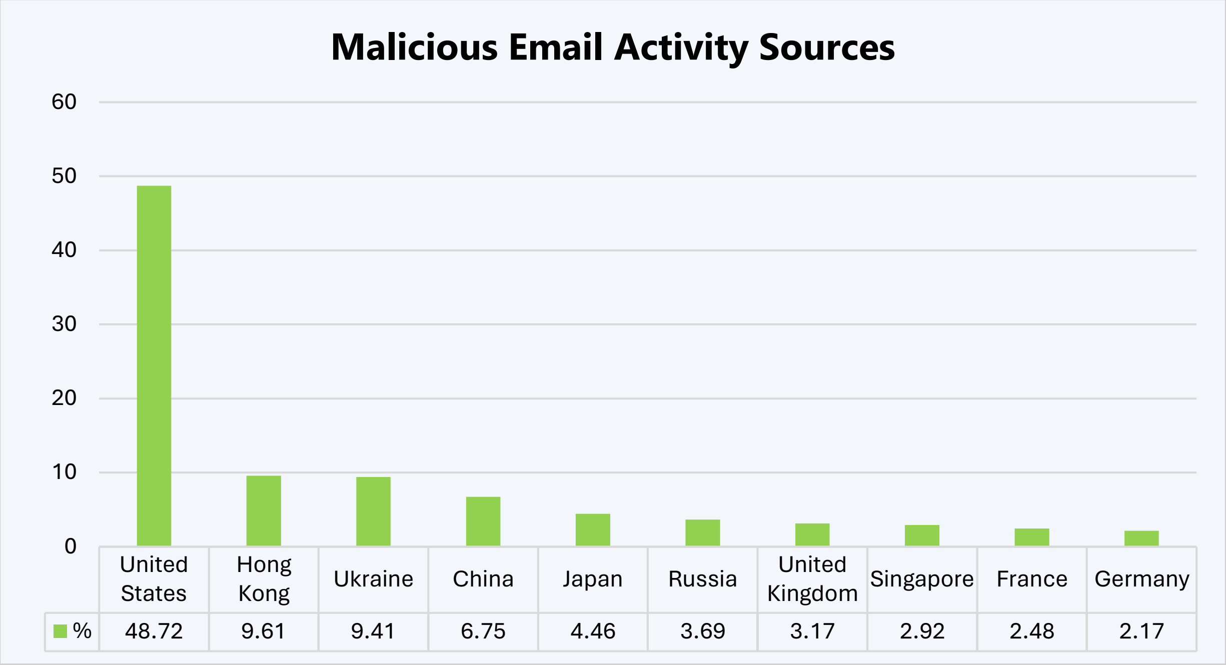


Variations in the family are designed to bypass known signatures, the continuously evolving malwares detected means that email defenses will be pushed further as evaluating attachments and malware consumes technical and security analyst resources. However, keeping up with mutating malware is an absolutely essential aspect of email defenses.

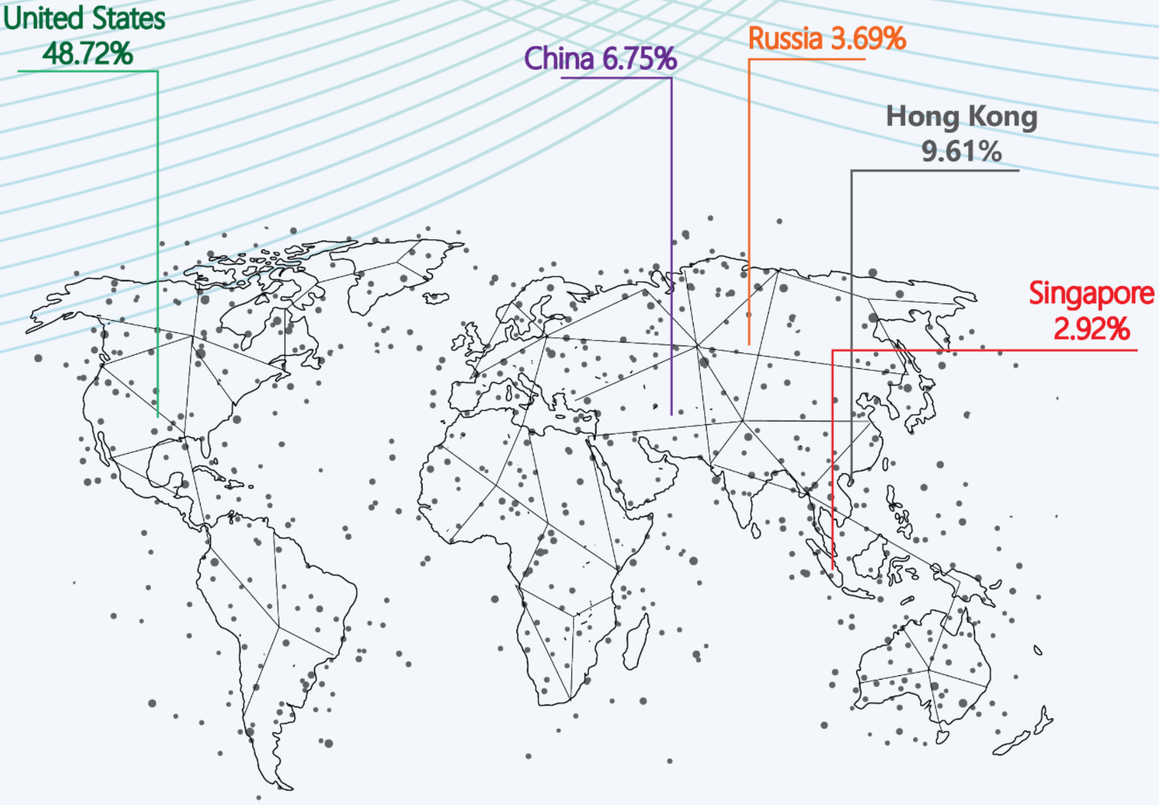
5.3 Where are Attacks Originating From?

From the perspective of Hong Kong & Singapore, the single largest origin of attacks continues to come from United States mailing servers. This is a relative increase of 40% versus last year. Again, this is not to say that malicious actors against Hong Kong & Singapore are from the US, though phishing attacks tend to ride on many well-known and familiar brands and that resources in US were used to initiate these attacks. There are plenty of well-recognized American products and services to choose from worldwide. Another alarming trend observed was Hong Kong initiated attacks went up to 9.6% versus 5.5% of last year, of all monitored malicious email activities.

Malicious Email Activity Sources



	United States	Hong Kong	Ukraine	China	Japan	Russia	United Kingdom	Singapore	France	Germany
🟩 %	48.72	9.61	9.41	6.75	4.46	3.69	3.17	2.92	2.48	2.17



Outside of the US initiated attacks, Hong Kong & Singapore is really exposed to a varied source of attacks, Ukraine, Russia, China, Japan, UK etc, it should be noted that Ukraine was never a major source of attacks against Hong Kong & Singapore in the past but has come up this year.

Hackers looking to successfully penetrate companies would desire to ride on familiarity for the highest chance of success. The exposure of Singapore to US and Asia in general, would define the design ideas of attacks it receives. It is not surprising that almost 10% of its attacks come from within, although it does mean that local users would likely face ever better disguised email attacks as hackers are riding on familiar local household names.

5.4 Most Impersonated Local Brands

On the global level, we still see DHL, Microsoft and LinkedIn continue to appear in the top spots over the past 12 months, with some shuffling in the orders. Hong Kong saw impersonated emails riding on Cathay Pacific, amongst other well-known and used brands, the use of Cathay Pacific as an impersonated brand seems to in part be related to a surge in traveling and the end of COVID restrictions. Singapore has been dominated by Telco and Financial Institutions as the favourite "go-to" brands for impersonated hacking, but Inland Revenue Authority was also seen to have been impersonated. It should be noted that the Inland Revenue Department of Hong Kong was also impersonated last year during taxation season.

Ranking	Global	Hong Kong	Singapore
1	DHL	SF EXPRESS 顺丰速运	LOUIS VUITTON
2	WeTransfer	国家税务总局 State Taxation Administration	Singtel
3	Meta	Hongkong Post 香港郵政	WeTransfer
4	Spotify	Spotify	DHL
5	amazon	LOUIS VUITTON	in

Over time, it could be seen that attackers are refining their techniques as well as the extensive impersonation of local brandings. The use of these brands is closer to home and for many local users, regular communications from these brands are the norm rather than the exception. All these point to the increased localized focus by malicious actors who would impersonate local brands for successful phishing campaigns. In conjunction with the increased sophistication in how the attacks aim to get around defenses, this makes the threats evermore real and closer to reaching their recipients.

6. Threat Mitigation and Safeguards

Malicious emails will always be around and continue to be an integral part of cybercrimes. Fundamentally it exploits weaknesses or curiosity in the recipient, resulting in the malicious actor reaping benefits. It takes just one weak link for an organization to be exploited.

However, safeguards against malicious emails have always been available technologically, from the anti-spam solutions of old to the anti-phishing and even managed detection and response services offered by Green Radar. Though, it must be emphasized that no technology can offer guaranteed safeguards.

Manned operation becomes an ever more important part of an effective email security platform. While facing innovative and never-before-seen techniques in email attacks, even with AI-assisted detection mechanisms, the timely intervention by security analysts is crucial to the accuracy of determining malevolence, and also to adapt the system to keep up.

A review of 2023 brings security practitioners to a reality that the industry had always known – phishing emails end with devastating attacks and breaches. It should almost be assumed that phishing emails could somehow get through to a member of staff in a corporation. Aside from strengthening perimeter email defenses, protecting the core of the organization is integral to a comprehensive defense strategy.

The general approach to better defend end users against malicious emails could be outlined in the following manners.

1. Email Filtering Technologies - Filter out harmful contents
2. Privileged Identity Management – Keep hackers out of critical systems or your email setup
2. Web Activity Isolation - Protect the recipient while accessing the online contents
3. Threat Awareness Training - Build up recipient awareness against likely malicious activities

6.1 Email Filtering Technologies – Aim for Zero-Trust Solutions

Email filtering technologies have been around for a long time and most organizations have it in one form or another. There are many options to choose from, all with different levels of technology integration and effectiveness. The key requirement is that emails received by end users should be clean and trustable.

The real-life challenge of running an email security solution is the operational costs, in terms of staff resources and expertise, where investigation is necessary against suspicious emails that are at the border of legitimacy. More advanced email security solutions with better technologies tend to filter better, while older technologies tend to tag-and-pass and thus mean more work for the operations team, who are obliged to investigate, release and, or follow up.

Managed Detection & Response services integrate the filtering technology with outsourcing services that investigate the suspicious emails, leaving the clients to receive clean emails only. They tend to profile for its locality and client, so that imitations of local brands and BEC would be more timely and promptly detected.

6.2 Privileged Identity Management Solutions – Protect the Core

Privileged Identity Management Solutions (PIM) have been around for a long time. However, it had mostly been exclusive to enterprises. PIM solutions secure critical infrastructure admin accounts with strong rotating passwords. Any serious breaches, such as the stealing of an entire database of data, requires some administrator access.

Implementing PIM solutions enhances clients with immediate benefits. The securing of the email administrator account reduces the chance of having email account information being compromised and thus adverts the worst form of BEC attacks. Should the organization’s perimeter be breached or a user and his laptop be compromised, PIM solutions help to stop hackers gaining access to the inner infrastructure and thus protect the database or other centralized critical assets from being stolen or compromised.

6.3 Web Isolation – Used by 18% of users

Around 18% of all organizations make use of some form of isolation technologies to safeguard their users while accessing potentially harmful contents, a slight increase from last year of 15%. Isolation technologies form quarantined pockets so that users can access web links and, or attachments safely. Any malicious activities would be nullified in the quarantined pocket.

It is imperative to understand that with the evolving evasiveness of phishing emails, organizations should take isolation technologies into serious consideration. Corporates that wish to exercise zero-trust against internet activities are powerless to enforce such directives without isolation technology in effect.

Even for those corporates that have deployed isolation technologies, it was found that up to 75% of users choose to bypass protection as part of email isolation. While bypassing isolation technology is not necessarily a negative indicator, it does indicate that users tend to believe that 75% of their email content, be it URL links or attachments, does not need to be protected. However, the adoption of isolation technology is low, though it is being adopted more widely over time.

Isolation technologies have their technological limitations. It cannot stop BEC or its recipients from reacting. BEC rides on fraud and its money is laundered and thus it is important to also consider PIM solutions as outlined. Emails and communications of such nature, even isolated, cannot stop the recipients from carrying out the sent instructions.

6.4 Threat Awareness & Training

Increasingly organizations are realizing that empowering users to be aware of potential cyber threats must become part of the overall cybersecurity strategy. While an increasing number of corporations are aware of the importance of these trainings, this is currently still in its infancy and these trainings are carried out in isolation rather than systematically or regularly.

To put this into perspective, over 30% of recipients and 90% of organizations would have responded to phishing emails during threat awareness exercises. This is a staggering high response rate to phishing baits and demonstrates a distressingly low threat awareness levels in the local environment.

7. Conclusion – Exercise “Zero-Trust”

In conclusion, it is important for security practitioners and business leaders to understand that malicious email attacks are and will continue to be an integral part of cybercrimes. Phishing emails could be engineered to initiate massive breaches. With the advent of AI, they are getting ever easier to manufacture and cheaper to execute. The dynamic nature of these threats demands continuous improvement and the adoption of cutting-edge AI-powered technologies to stay one step ahead. Organizations must stay informed, remain vigilant, and implement proactive measures to safeguard their data and prevent increasingly sophisticated attacks from entering their environments in 2024 and beyond.

Over the last twelve months, we could see that phishing emails have taken on new levels of smartness in their structure and their continuous evolution to try to bypass security defences. AI generated phishing, in its various ways of application has created phishing content that looks so much devious and more believable. It is important that email users should always practice zero-trust when it comes to reacting to emails.

Email security solutions are numerous and varied in its technology sophistication. The better the technology, the less there is to do for the operations team, who are tasked with analysing suspicious emails and releasing legitimate ones. In the climate of phishing attacks becoming increasingly wicked, the engineering sophistication vis-à-vis operational intervention should be utmost consideration for local enterprises. Managed Detection and Response services are better equipped technologically, and manned to take away this overhead, especially from smaller enterprises, while providing the best possible protection at a lower cost of ownership.

2024 will soon be seen to be more challenging than 2023. The slippery nature of phishing emails will continue, putting ever more pressure on security defenders. Cybercriminals will be out in force, taking advantage of a world of misinformation. Geopolitical factors in play making misinformation a way of life and another exploitable industry for them. Other forms of phishing outside emails, be it via phones or internet or SMS etc would continue to grow in its variety and volume. Thus, “trust no one” would be a good starting point when we go into 2024.

Appendix A - GRETI Methodology and Risk Level

What is the Green Radar Email Threat Index?

The Green Radar Email Threat Index (GRETI) is a annual measurement of the email threat landscape. It is constructed based on attack volume, frequency, and impact level of major email attack vectors, including phishing, Business Email Compromise (BEC), and malware. Huge volume of data is gathered from multiple threat intelligence sources, including the millions of emails that are screened daily by our proprietary artificial intelligence (AI) and machine learning engine aidar™, suspicious and novel attack events and attack methods captured by analysts at the Green Radar Security Operations Centers in Hong Kong and Singapore (SOCs), as well as global and local threat intelligence sources.

GRETI serves two main purposes:

- To keep companies and organizations informed on the level of risks they are exposed to in the latest threat environment and propose possible mitigation actions.
- Assist cybersecurity practitioners by providing insights and the latest trends on email threats so that they can develop appropriate protective measures.

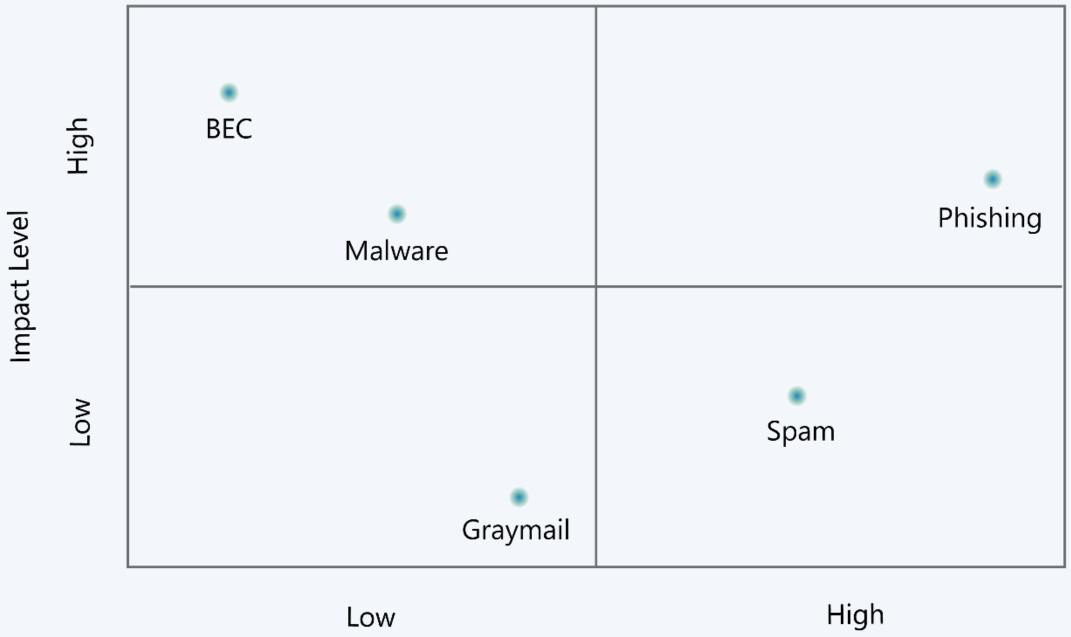
Email threats come in many forms, ranging from nuisance spam emails to highly sophisticated and tailored attacks. The GRETI focuses on the most prominent and impactful types of email threats as these have the potential to cause to most damage to organizations.

Less impactful or prevalent types of emails threats are excluded from the calculation of the GRETI.   When the different kinds of email threats emerge or evolve in the future, the components that form the GRETI will change to reflect the latest threat trends in future reports.

As shown in Figure 1, phishing, BEC and malware are included in the GRETI for this quarter due to their higher prevalence and impact level. We define Impact level as the magnitude of harm, such as the loss of information, information system availability and financial loss resulting from email threats.

Table 1 below outlines risk level with a general description of the possible impact and cautionary statements. The higher the email threat index, the more severe is the level of risks that organizations may be exposed to.

Notable Email Threats Captured by aidar™



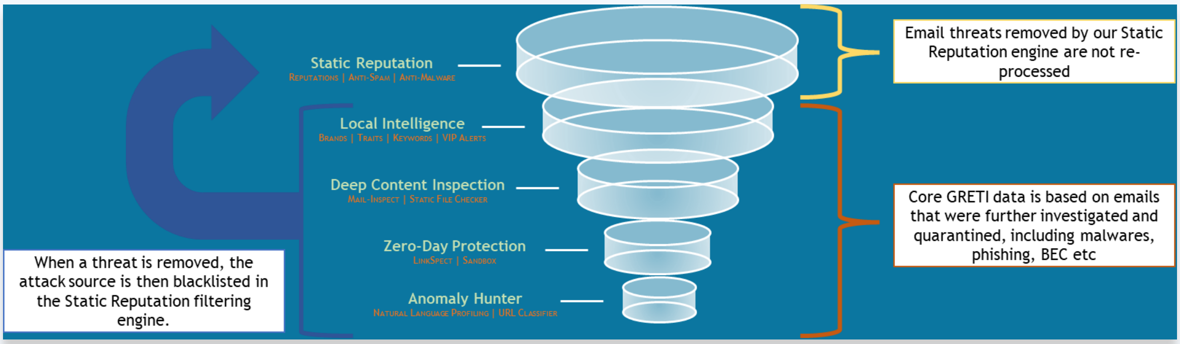
GRETI Risk Level

Risk Level	GRETI	Risk Impact	Cautionary Statement
Critical	80 -100	Attacks are known to cause widespread and severe damage with the potential to disrupt business operations	Immediate action is required to contain severity and damage. Additional controls to lower the risk level are to be implemented at the earliest opportunity.
High	60 - 79	Risk alert: attacks volumes and frequency are high, which might cause widespread and severe damage.	Continuous monitoring and immediate protective measures are required.
Moderate	40 – 59	General risk of phishing or other malicious activities spread. No significant impact has occurred.	Action required to make safe prior. Continuous monitoring of the controls is important.
Low	0 - 39	Threat risk is acceptable and manageable. No abnormal activity has occurred.	No additional actions are required. Routine activities are sufficient to prevent attacks effectively.

Appendix B – Green Radar grMail and how it affects GRETI – Focus on Unknown Threats Only

The detail analysis of zero-day email threats outlined in this paper is based on emails that were processed through the Green Radar email protection services (aka grMail) engine. The following diagram depicts how grMail works and which data set was used in the GRETI analysis.

grMail


Static Reputation
REPUTATIONS | ANTI-SPAM | ANTI-MALWARE
Local Intelligence
BRANDS | TRAITS | KEYWORDS | VIP ALERTS
Deep Content Inspection
MAIL-INSPECT | STATIC FILE CHECKER
Zero-Day Protection
LINKSPECT | SANDBOX
Anomaly Hunter
NATURAL LANGUAGE PROFILING | URL CLASSIFIER

Email threats removed by our Static Reputation engine are not re-processed

Core GRETI data is based on emails that were further investigated and quarantined, including malwares, phishing, BEC etc

When a threat is removed, the attack source is then blacklisted in the Static Reputation filtering engine.

Unknown threats captured by grMail becomes known threats. The source of the threat would then be added to the Static Reputation blacklisting engine. Should the attack repeats, it is rejected by the Static Reputation engine and thus will not go through the grMail engine again. The technical merit is obvious in that grMail will not process emails from the same source twice. However, for the purpose of GRETI, the importance is as follows:

Focus on Unknown or Evolving Threats – By evaluating threats and then blacklisting them, GRETI focuses and writes about threats that are worth scrutinizing only. In order to bypass the Static Reputation blacklisting engine, hackers at minimum must resend using different sources for persistent campaigns. The email threat can then be recorded as a separate attack. Thus, GRETI analyzes unknown or evasive attacks only as it does not multiple threat from the same source multiple times.

Concise Statistics – As GRETI does not count the same threat multiple times, the data is therefore consistent with either new or evasive attacks and only once for each such source. Thus, data and analysis is based on unique and uncluttered attack data only.

Analysis of Current Threat Landscape – By looking at the latest threats, and how they continue to evolve and trying to be evasive, GRETI keeps up with the latest threats that is most likely to get through general email protection products or solutions. GRETI therefore reflects email threats that are most likely to be effective in the timespan captioned.

grMail offers comprehensive email protection and is delivered through manned MDR staffed with cybersecurity professionals. It consistently detects new threats and keeps up with threats through continuous improvement in its detection and AI engines, which is augmented with manned operation and local intelligence.

Redefining Email Security

Green Radar (Hong Kong) Limited
25/F, Tower 1, The Millennity, 98 How Ming
Street, Kwun Tong Kowloon, Hong Kong
T: +852 3194 2200

Green Radar (Singapore) Pte. Ltd.
2 Sims Close #01-11/12,
Gemini@Sims Singapore 387298
T: +65 6248 0600

info@greenradar.com |www.greenradar.com

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 cyber security company headquartered in Hong Kong.