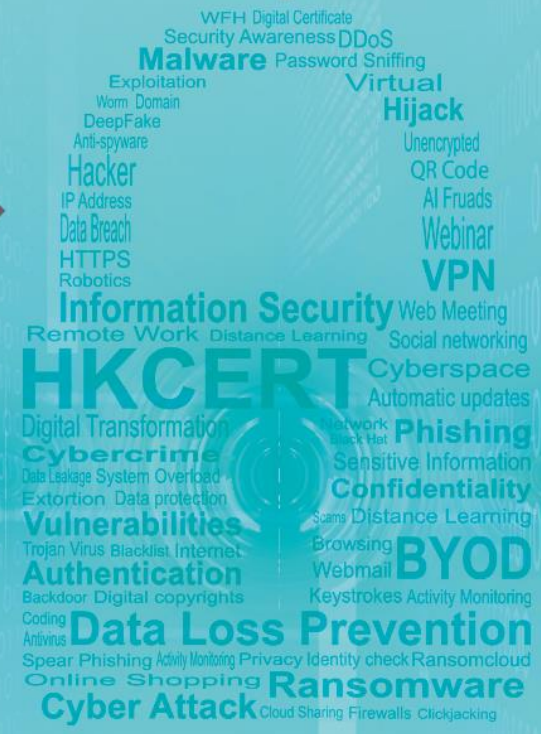
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report 2022 Q3

Release Date: Nov 2022



Foreword

Better Security Decision with Situational Awareness

Nowadays, many networked digital devices, such as computers, smartphones, tablets, are being compromised without the user's knowledge. The data on them may be mined and exposed every day, and even be used for various criminal activities.

The Hong Kong Security Watch Report aims to raise public awareness of the problem of compromised systems in Hong Kong, enabling them to make better decision in information security. The data in this quarterly report focuses on the activities of compromised systems in Hong Kong which suffer from, or have participated in various types of cyber-attacks, including web defacement, phishing, malware hosting, botnet command and control (C&C) centres or bots (Table 1). "Computers in Hong Kong" refer to those whose network geolocation is Hong Kong, or the top-level domain of their host name is ".hk". Also, this report will review major security incidents and explore hot security topics with easy-to-adopt security advice with an aim to improve public's information security posture and enhance their security resilience capabilities.

Capitalising on the Power of Global Intelligence

This report is the result of collaboration between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and global security researchers. Many security researchers could detect attacks against their own or clients' networks. Some will provide the collected information of IP addresses of attack source or web links of malicious activities to other information security organizations with an aim to collectively improve the overall security of the cyberspace. They have good practice in sanitizing personal identifiable data before sharing the information.

HKCERT collects and aggregates such data about Hong Kong from multiple information sources for analysis with the Information Feed Analysis System (IFAS), a system developed by HKCERT. The information sources (Appendix 1) are very diverse and reliable, providing a balanced reflection of the security status of Hong Kong.

HKCERT removes duplicated events reported by multiple sources and uses the following metrics for measurement to assure the quality of the statistics.

Type of Attack	Metric used
Defacement, Phishing, Malware Hosting	Security events on unique URLs within the reporting period
Botnet (Bots)	Maximum daily count of security events on unique IP addresses within the reporting period

Sources of information in IFAS

Event Type	Source	First introduced
Defacement	Zone - H	2013-04
Phishing	CleanMX - Phishing	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Botnet (Bots)	Shadowserver - microsoft_sinkhole_events	2021-06
Botnet (Bots)	Shadowserver - microsoft_sinkhole_http_events	2021-06
Botnet (Bots)	Shadowserver - sinkhole_http_events	2021-06
Botnet (Bots)	Shadowserver - sinkhole_events	2021-06
Botnet (Bots)	Shadowserver - honeypot_darknet_events	2021-06

Geolocation identification methods in IFAS

Method	First introduced	Last update
Maxmind	2013-04	2022-10

Better information better service

HKCERT will continue to enhance this report with more valuable information sources and more in-depth analysis and explore how to make best use of the data to enhance our services. Please send your feedback via email (hkcert@hkcert.org).

Limitations

Data collected for this report come from multiple sources with different collection periods, presentation formats and their own limitations. The statistics from the report should be used as a reference only and should neither be compared directly nor be regarded as a full picture of the reality.

Disclaimer

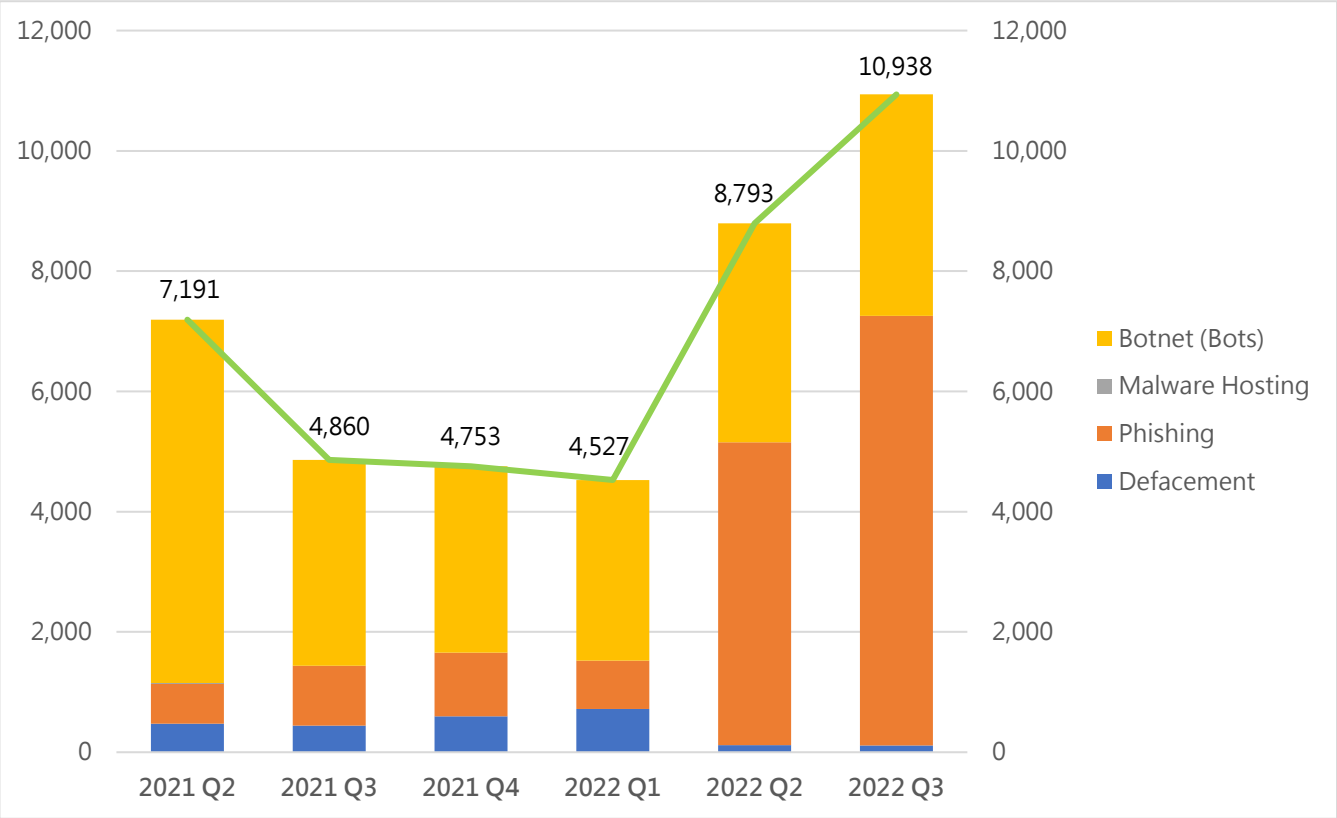
Data may be subject to update and correction without notice. We shall not have any liability, duty or obligation for or relating to the content and data contained herein, any errors, inaccuracies, omissions or delays in the content and data, or for any actions taken in reliance thereon. In no event shall we be liable for any special, incidental or consequential damages, arising out of the use of the content and data.

License

Highlight of the 2022 Q3 Report

Unique security events related to Hong Kong **Quarter-to-quarter**

10,938 **↑ 24%**



Event Type	2021 Q3	2021 Q4	2022 Q1	2022 Q2	2022 Q3	quarter-to-quarter
Defacement	**445**	**595**	**718**	**118**	**113**	**-4%**
Phishing	**993**	**1,061**	**806**	**5,033**	**7,141**	**+42%**
Botnet (Bots)	**3,422**	**3,097**	**3,003**	**3,642**	**3,684**	**+1%**
Total	**4,860**	**4,753**	**4,527**	**8,793**	**10,938**	**+24%**

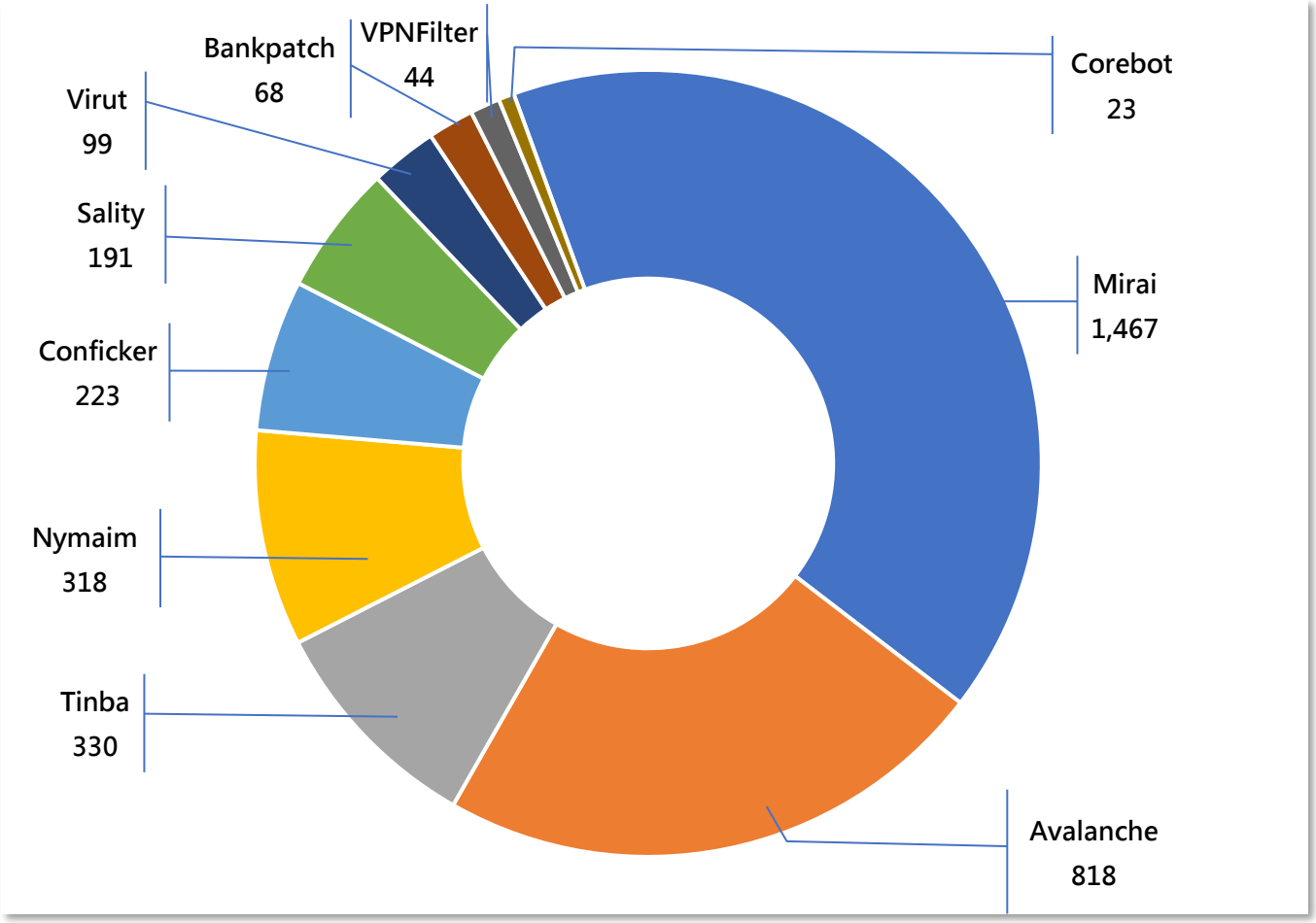
* The related data sources no longer provide botnet (control centre) information.
** The number of malware hosting event is zero in the past five quarters.

Major Botnet Families in Hong Kong Network

Mirai
1,467
↓ 5.1%

Avalanche
818
↑ 16.2%

Tinba	330	+42.2%
Nymaim	318	+43.2%
Conficker	223	-9.3%
Sality	191	-6.8%
Virut	99	-11.6%
Bankpatch	68	+88.9%
VPNFilter	44	-22.8%
Corebot	23	-42.5%



** Individual botnet's size is calculated from the maximum of the daily counts of unique IP address attempting to connect to the botnet in the reporting period. In other words, the real botnet size should be larger because not all bots are activated on the same day.*

Security Events Exceed 10,000 Again

Security events rose for two consecutive quarters, with the current reporting quarter being the first time since 2020 Q2 that the number of events has risen above 10,000. During the period, a change in security event landscape has also been observed. In particular, phishing events have replaced Botnet as the dominant source of security events in Hong Kong.

Among the 7,000+ phishing events detected in 2022 Q3, over 80% of their URLs shared similar patterns. They are constructed by a random string which ends with `page1.php` (e.g. `/k7OIMyJhEU/page1.php`, `/ic6oXx7P3s/page1.php`, `/uWBRvZ8quj/page1.php` or `/LAuCvx4R/page1.php`, etc.). According to email security specialists, most of these phishing websites are in Japanese and found to be related to fake credit card companies and banks, with an aim to steal credit card information. Hacker would send fake credit card usage notification email to the victims, and then lure them to click on the link of target phishing website.

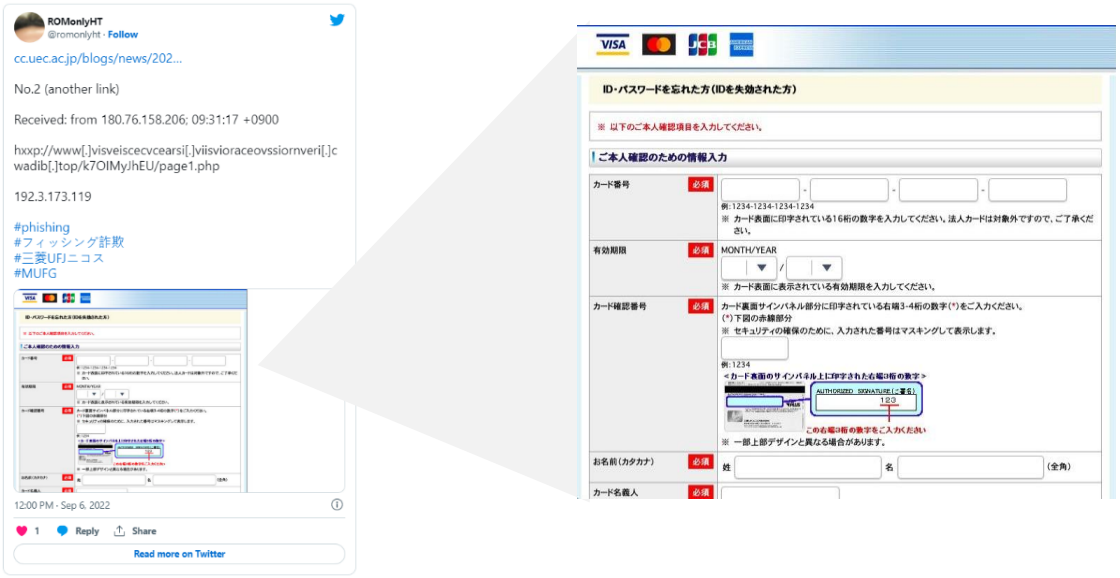
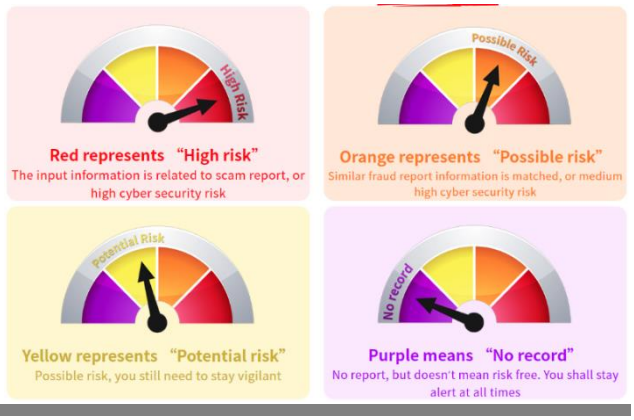


Image: https://twitter.com/romonlyht/status/1566999640054333441

At the time of writing, sample checking showed that these phishing sites have been either **taken down or inaccessible**. HKCERT would like to urge users to stay vigilant when providing sensitive information to any websites. Remember to check the spelling of URL to ensure it connects to legitimate website. If in doubt, leave the website and verify with the related organisation immediately.

How to Check the Website is Trustworthy?

Apart from the spelling of URL, a free search engine "Scameter" by CyberDefender of the Hong Kong Police supported by HKCERT is now available to help identify frauds and online pitfalls through email, URL or IP address, etc. The search result will be indicated in different colours:



> The search results will also provide fraud prevention tips, such as verifying the identity of the other party before making transactions or remittances, exercising caution when providing sensitive information, not opening suspicious links or attachments, and paying attention to local calls with the prefix +852, etc.

Email Security Tips

As mentioned, email is one of the main attack vectors for phishing attacks. When we receive suspicious emails, how can we know if the emails are from legitimate senders? Apart from checking the sender's email address, we can also look into the "email header" of the email. It contains important information such as the sending server, sending date, message ID, etc. Among them, 3 kinds of information namely Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication Reporting and Conformance (DMARC) provide valuable information for technical personnel to determine the authenticity of emails.

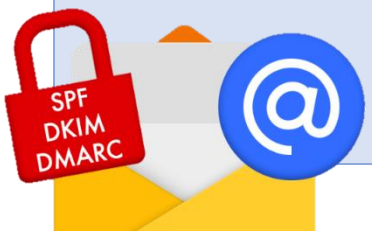
Headers Found

Header Name	Header Value
Authentication-Results	spf=pass ([redacted]) smtp.mailfrom=[redacted].com; dkim=pass ([redacted]) header.d=[redacted].com dmarc=bestguesspass

What are SPF, DKIM, and DMARC?

They are the technologies to tackle email spoofing and phishing. Organisations should review their email server settings to ensure they are properly configured to avoid their emails being misidentified as phishing emails.

Sender Policy Framework (SPF)	Specify the servers and domains authorized to send email on your organisation's behalf. • By verifying SPF, recipients can know that the message is from the senders' domain and whether they agree to send the message.
DomainKeys Identified Mail (DKIM)	Add a digital signature to every outgoing message so that the receiving server can confirm that the message really comes from your organization. • For example, when sending an email, the sender will add a DKIM digital signature (private key) to reduce the possibility of email being tampered with. The recipient will check the DKIM (public key) to ensure that it is the same as the original signed private key.
Domain-based Message Authentication Reporting and Conformance (DMARC)	If you send email that doesn't pass SPF or DKIM verification, you can use DMARC to instruct the receiving server what to do with the email. • DMARC can help with sending, quarantining, or rejecting when SPF and DKIM fail. However, outgoing emails are usually marked as "spam". Or, if DMARC is set to "reject", it means the emails that are not sent from the designated email server cannot be sent by using this email address. Therefore, system administrators should regularly review whether the settings of the email system comply with company policies.



Focus: Adopt Good Cyber Security Practices to Make AI Your Friends not Foes

Artificial intelligence (AI) has experienced a rapid growth in its adoption by businesses in recent years. According to the International Data Corporation, companies around the world plan to increase their spending on AI solutions (e.g., hardware, software, services, etc.) by 19.6% in 2022 to US$ 432.8 billion, and to exceed US$ 500 billion in 2023. As the application of AI becomes more diverse, greater attention must be attached to its associated security risks. Otherwise, it may end up doing more harm than benefits.

What is Artificial Intelligence?

AI is the simulation of human intelligence by machines. These "human intelligence" can include learning, problem-solving and pattern recognition etc. AI is currently undergoing a phase of vigorous development, such as the improvement of computing power, robotics and statistics, as well as the increasing volume of data. The application of AI is becoming more diverse: from its better-known applications like computer vision (e.g. pattern recognition, facial recognition) and natural language processing (e.g. machine translation, voice recognition), mimicking human cognitive behaviours such as cancer detection, to even analysis of legal cases and creative processes like poetry writing and art making. In the field of cyber security, AI can even be used to detect and identify malware.

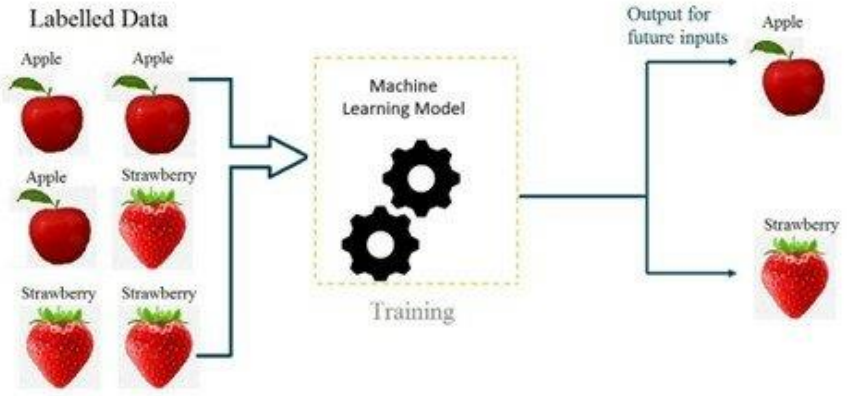
Supervised Learning

There are plenty of approaches to ML, with the most common one called Supervised Learning.

➢ Fundamentals of Supervised Learning

In supervised learning, a dataset is collected to train a mathematical model, where the dataset includes data of one or more inputs (or called features) and outputs (or called labels). By feeding this data into a model, it completes the algorithm to spit out outputs according to calculations with its parameters.

Figure 1: A Basic Scheme of a ML model with Images of Apples and Strawberries being the Features and the Word Associated with them ('apple' or 'strawberry') the Label.



Source: https://ai.plainenglish.io/introduction-to-machine-learning-2316e048ade3

Security Risks of AI-powered Services

For a start, as mentioned above, AI is powered by a large volume of data and computation. If these training data consist of sensitive personal information, leakage of training data can result in sensitive information disclosure. Also, as the collection of training data can come from various sources, AI-powered services are susceptible to the risk of cross-leakage. Moreover, if AI-powered services are being attacked, their adverse effects can be more serious than traditional ones. This is because multiple services might use the same machine learning model. If the model is being attacked, all services powered by that model will be affected as well. No matter we are the users of AI or not, the cyber security of AI affect everyone. Let us discuss how these risks can affect different stakeholders in two aspects: "Security Loopholes" and "Malicious Uses and Abuses".

Security Loopholes

➢ Membership Inference Attack

The inferencing of training data through reverse engineering on the machine learning model (i.e., "target model"). This way of attack is since the training model performs differently on seen and unseen data. One indicator is the difference in the confidence level it gives. By observing the behaviour of the output, we may be able to infer if a certain input data is a part of the training dataset.

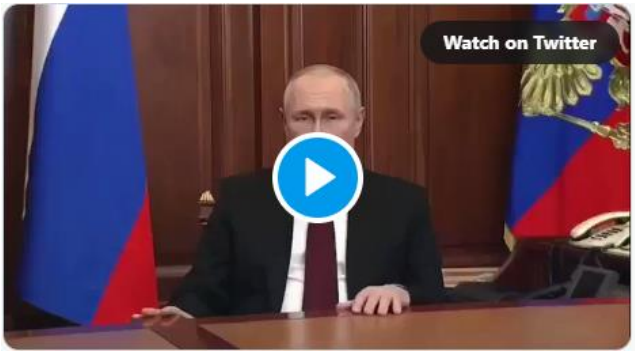
- **Adversarial Perturbation**
  It refers to provision of perturbed versions of inputs to the machine learning model to fool it. This type of attack is based on slight alteration of training data in order to decrease the accuracy of the model. There are two types: Evasion Attacks and Poisoning Attacks.

Malicious Uses and Abuses - Deepfake

It refers to the use of Deep Learning technology to create fake video/audio. This technology is most known in its video form, where the face in the video is swapped with another person's likeness. However, Deepfake could also be used to synthesize human voice in imitation of a particular person, and the realistic voice of the victim could be synthesized just by inputting a text script.

Deepfakes can even lip-sync the victim with an audio clip provided, meaning one video clip instead of two might be enough to make Deepfakes. Deepfake uses machine learning algorithms like the Autoencoder and the Generative Adversarial Network.

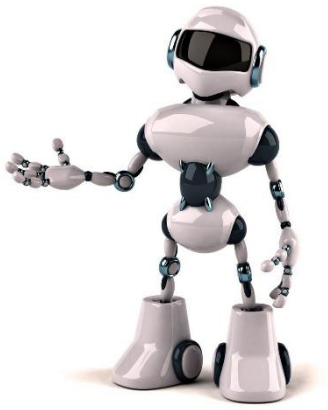
For example, in the 2022 Russian Invasion of Ukraine, the likeness of both presidents of Ukraine and Russia have been abused to produce Deepfake videos to spread rumours.



Source: https://www.youtube.com/watch?v=X17yrEV5sl4, https://twitter.com/sternenko/status/1504090918994993160?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504090918994993160%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Farticle%2Ffactcheck-putin-address-idUSL2N2VK1CC

Security Advice

- Select Appropriate Models to Prevent Membership Inference Attacks
- Validate Training Data Before Updating the Model to Prevent Adversarial Perturbations
- Improve Privileged Access Management (PAM) Policies
- Use Anti-Fake Tool to Protect from Deepfake
- Enhance understanding on deepfakes



Conclusion

As AI becomes increasingly powerful and ubiquitous, the weaponization of AI becomes more and more viable. Whether you are a user of AI or not, you may still be a victim of these attacks. Therefore, an understanding of the potential dangers of AI helps us stay vigilant, so that we may enjoy the benefits brought forth by AI, not in the expense of its security dangers.

For more information, please refer to HKCERT Security Blog
https://www.hkcert.org/blog/adopt-good-cyber-security-practices-to-make-ai-your-friends-not-foes

Analytical Report: Browser's Anti-phishing feature: What is it and how it helps to block phishing attack?

Over the past four years, HKCERT has handled an average of about 8,900 local cyber security incidents per year, with phishing attacks accounting for 48% of all incidents in 2021. Even globally, phishing attacks account for 36% of total security incidents.

What is the reason for the high volume of phishing attacks?

Phishing attacks are attributed to the low-cost yet highly effective and sophisticated nature of such attack. Nowadays technology makes it easy for hackers to build fake emails and websites, which are hard for the users to distinguish solely from the site layout. Apart from directly defrauding users' sensitive personal information, if attackers successfully obtain the credentials of any internal systems of the organizations (for example VPN or SaaS), they can then attempt to obtain sensitive information stored in the system or perform lateral movements (i.e., the process of an attacker progressively moving from the entry point to the rest of the network) and hack into other internal systems.

How to Prevent Phishing Attack

In addition to raising users' cyber security awareness (e.g., how to identify suspicious emails and URLs, proactively reporting suspicious URLs), anti-phishing functions are generally provided by anti-virus software and web browsers to block the access to suspicious websites for users and organizations.

Anti-Phishing Website Function and Engine

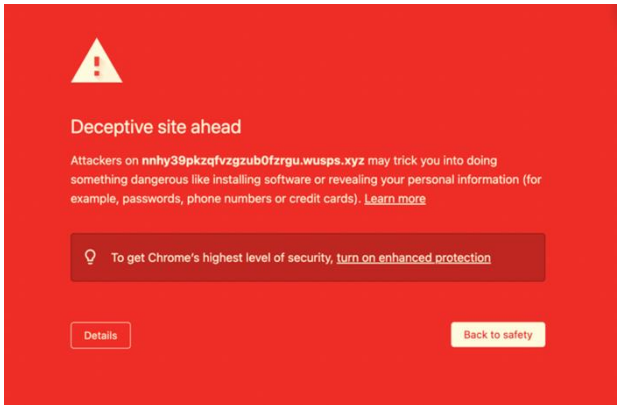
Acting as the gateway to websites, browser can detect and identify phishing URLs, making it one of an important defence mechanism. Common browsers usually come with a built-in anti-phishing website function. When the browser tries to access the page, the anti-phishing website engine will first compare and analyse the URL against the data in the database of the phishing website. If the analysis result is safe, the user can access the web page normally. Otherwise, a warning page will pop up to prevent the user from browsing.

Therefore, the comprehensiveness of the information in the database and the speed of update will have a significant impact on whether the browser can identify the phishing website. Some browser developers adopt the anti-phishing engine services from other browser developers. Below is a comparison of common browsers and the anti-phishing protection function:

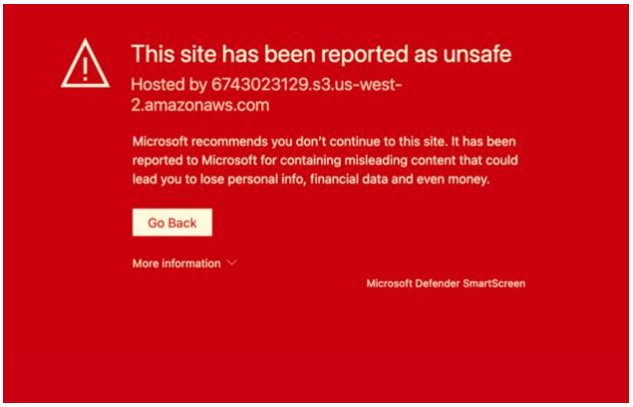
	Chrome	Edge	Safari	Brave	Firefox
Anti-phishing Function	Yes	Yes	Yes	Yes	Yes
Anti-phishing engine	Google Safe Browsing	Microsoft Defender SmartScreen	Google Safe Browsing	Google Safe Browsing	Google Safe Browsing

From the table above, the anti-phishing website engine is mainly divided into 2 groups: Google Safe Browsing and Microsoft Defender SmartScreen. Below is a sample warning displayed when these two engines identified a phishing site.

Google Safe Browsing



Microsoft Defender SmartScreen



Trends in phishing attacks in recent years

Phishing attack techniques have been evolving, and even the use of artificial intelligence customer service chatbot to obtain sensitive information from users. In light of this, HKCERT analysed and tested the performance of anti-phishing website function of common browsers.

Test Purpose

The purpose is to test the browser with default settings for end users, record the anti-phishing performance of common browsers in desktop and mobile platform.

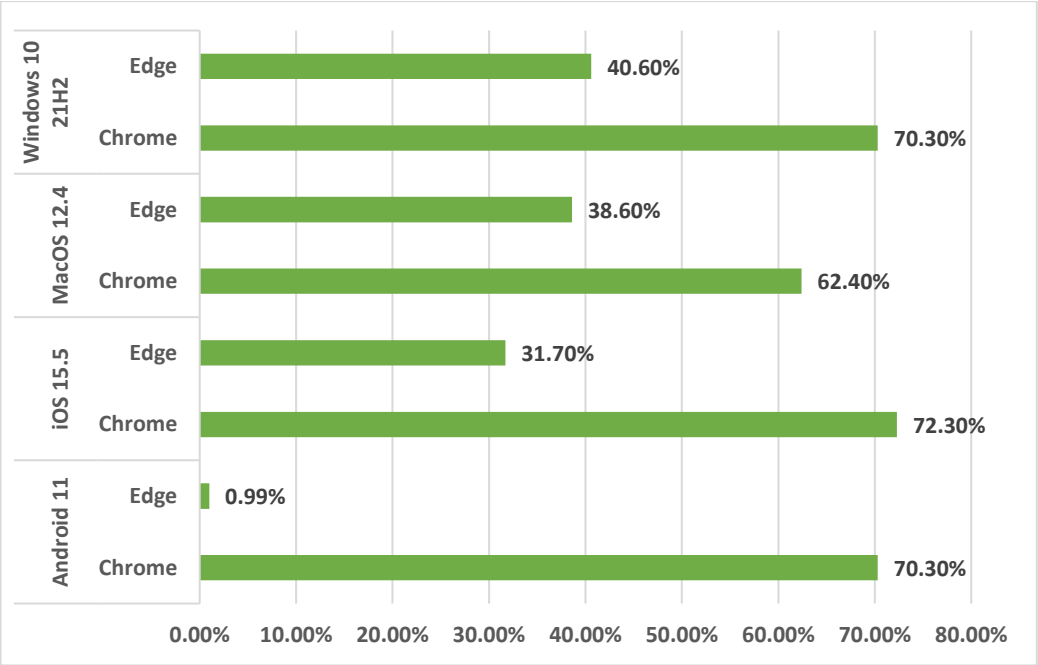
Test Method

For 14 consecutive working days (from July 11 to July 28), randomly select the latest phishing URLs published on that day. The URLs are provided by OpenPhish, which updates the list of phishing URL every twelve hours.

Testing Environment and Browsers Type

Since there are two anti-phishing engines used in common browsers, HKCERT chooses one of the browsers in each engine to test it on desktop and mobile platforms. To simulate the real usage of general users, all tested browsers use default security settings. The results are based on whether the browser, which acts as the first layer of defence, can block the phishing websites.

Result



1. The test results showed that Chrome achieved a higher success rate of blocking phishing websites across all platforms than Edge.
2. The same browser performs differently in the operating systems tested. This may have to with how the software vendor implements the anti-phishing website engine in specific platform.
3. Edge had a lowest success rate in Android. HKCERT has made inquiries with Microsoft in this regard and received a reply that the problem would be fixed in a future version of the SDK. Microsoft also stressed that the test conducted by HKCERT was based on Microsoft Defender Smartscreen's default settings, and the test results may be different if using its advised settings. It recommends users to contact the company for any inquiries.

Recommendation and Conclusion

HKCERT recommends Chrome users to enable Chrome browser Enhanced Protection to enhance the success rate of blocking phishing web pages. Since the anti-phishing function of the browser requires time to collect and analyse the phishing URLs, the successful detection rate of new phishing website would be lower. Users are advised to:

- Pay attention to the spelling of domain names of websites and check their authenticity.
- Do not assume a website that uses HTTPS is a legitimate site. A phishing site may also use HTTPS.
- Do not click any link or open any attachment casually and do verify the legitimacy of a website before providing any personal information.
- Do not log in to your account through a link provided by email or an unknown website. Use the bookmark function of browser to save the account login link instead.

In summary, the anti-phishing function is analogous to wearing a face mask in real life. It can prevent the infection of viruses (i.e., phishing attacks), but once the virus passes through the mask, it ultimately relies on the users' immune system (i.e., cyber security awareness) to protect oneself from virus infection.

For details, please refer to HKCERT Security Blog
https://www.hkcert.org/blog/browser-s-anti-phishing-feature-what-is-it-and-how-it-helps-to-block-phishing-attack

Security: Email Account Theft to Bypass MFA Protection

Microsoft researchers recently discovered a large-scale phishing campaign that steals users' email accounts even they have multi-factor authentication (MFA) enabled. Research shows that this type of phishing attack has been active since September 2021 and has attempted to target at least 10,000 organizations as of today.

Not difficult to understand, this technique is called Adversary-in-the-Middle (AiTM)

1. Hackers deploy proxy servers and fake websites, and then send phishing emails to target users.
2. The user believes that the fake email is legitimate and opens the fake website or attachment.
3. The user is redirected to the fake website which will request the user to enter email account and password to sign-in.
4. The user enters the account password and uses MFA to pass the authentication. The proxy server established by the hacker will redirect the information entered by the user to a legitimate website page, so that the user can log in successfully.
5. Meanwhile, the hacker has already intercepted the user's credentials and authentication information at the back end. The result is that the hacker would successfully invade the user's email account unnoticed.

Once the intrusion is successful, the hacker will search the user's mailbox for email conversations relating to payments or invoices, and then pretend to be the compromised account user to send fraudulent emails, such as asking the customer or colleagues to send money to the hacker's bank account.

In order to keep the compromised account user from noticing any suspicious emails, the hacker will delete the fraudulent emails, and establish inbox rules to hide the reply to emails of the fraudulent targets. For example, if a user's mailbox receives an email from a fraudulent target, it will be automatically deleted or moved to the archive folder and marked as read.

Although MFA can be bypassed, it remains very effective in preventing other attack methods. It is therefore best for the users to continue applying MFA for email account security.

HKCERT recommends that users

- Before providing login information, check the URL of the login page to ensure it is connected to the official login page
- Do not open suspicious emails or messages
- Do not open any website links or attachments in unknown emails
- Do not log in to your account through a link provided by email or an unknown website
- Check for suspicious inbox rules
- Use more advanced authentication technology, e.g., use hardware-based FIDO (Fast IDentity Online) password-free login authentication

-End-

Hong Kong Computer Emergency Response Team Coordination Centre
Tel.: 8105 6060
Email: hkcert@hkcert.org