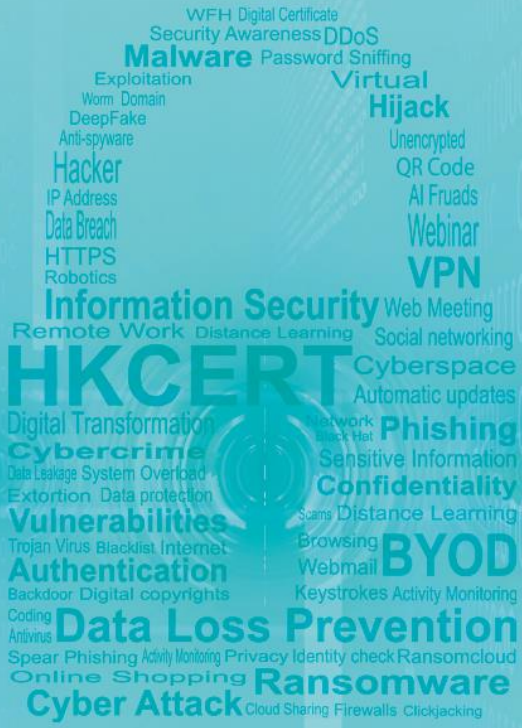
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report

2022 Q4

Release Date: Mar 2023


WFH Digital Certificate
Security Awareness DDoS
Malware Password Sniffing
Exploitation
Virtual
Worm Domain
Hijack
DeepFake
Anti-spyware
Unencrypted
Hacker
QR Code
IP Address
AI Fruads
Data Breach
Webinar
HTTPS
VPN
Robotics
Information Security Web Meeting
Remote Work Distance Learning Social networking
HKCERT
Cyberspace
Automatic updates
Digital Transformation
Network Black Hat Phishing
Cybercrime
Sensitive Information
Data Leakage System Overload
Confidentiality
Extortion Data protection
Scams Distance Learning
Vulnerabilities
Trojan Virus Blacklist Internet
Browsing
Webmail BYOD
Authentication
Backdoor Digital copyrights
Keystrokes Activity Monitoring
Coding
Antivirus Data Loss Prevention
Spear Phishing Activity Monitoring Privacy Identity check Ransomcloud
Online Shopping Ransomware
Cyber Attack Cloud Sharing Firewalls Clickjacking

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 and botnets. "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 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	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
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	2023-01

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

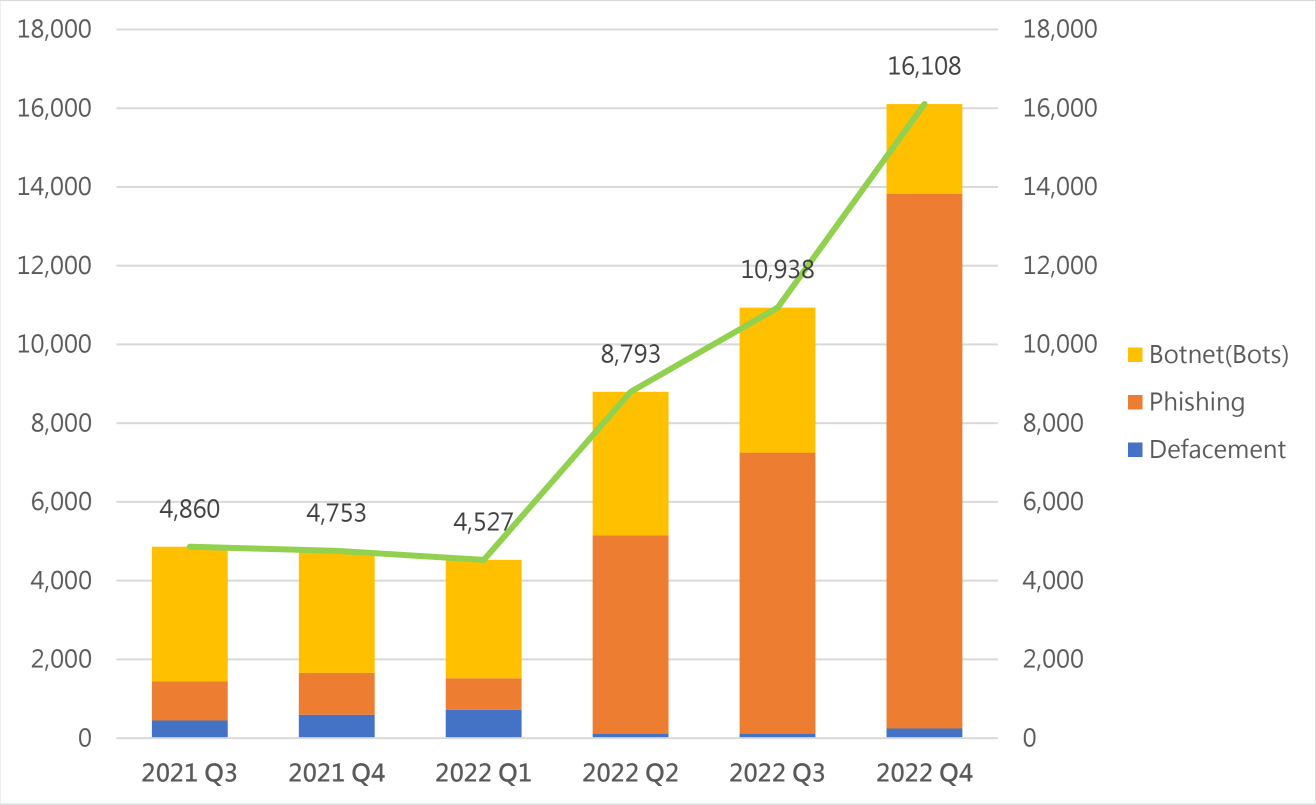
Highlights of the 2022 Q4 Report

Unique security events related to Hong Kong

16,108

Quarter-to-quarter

↑ 47%



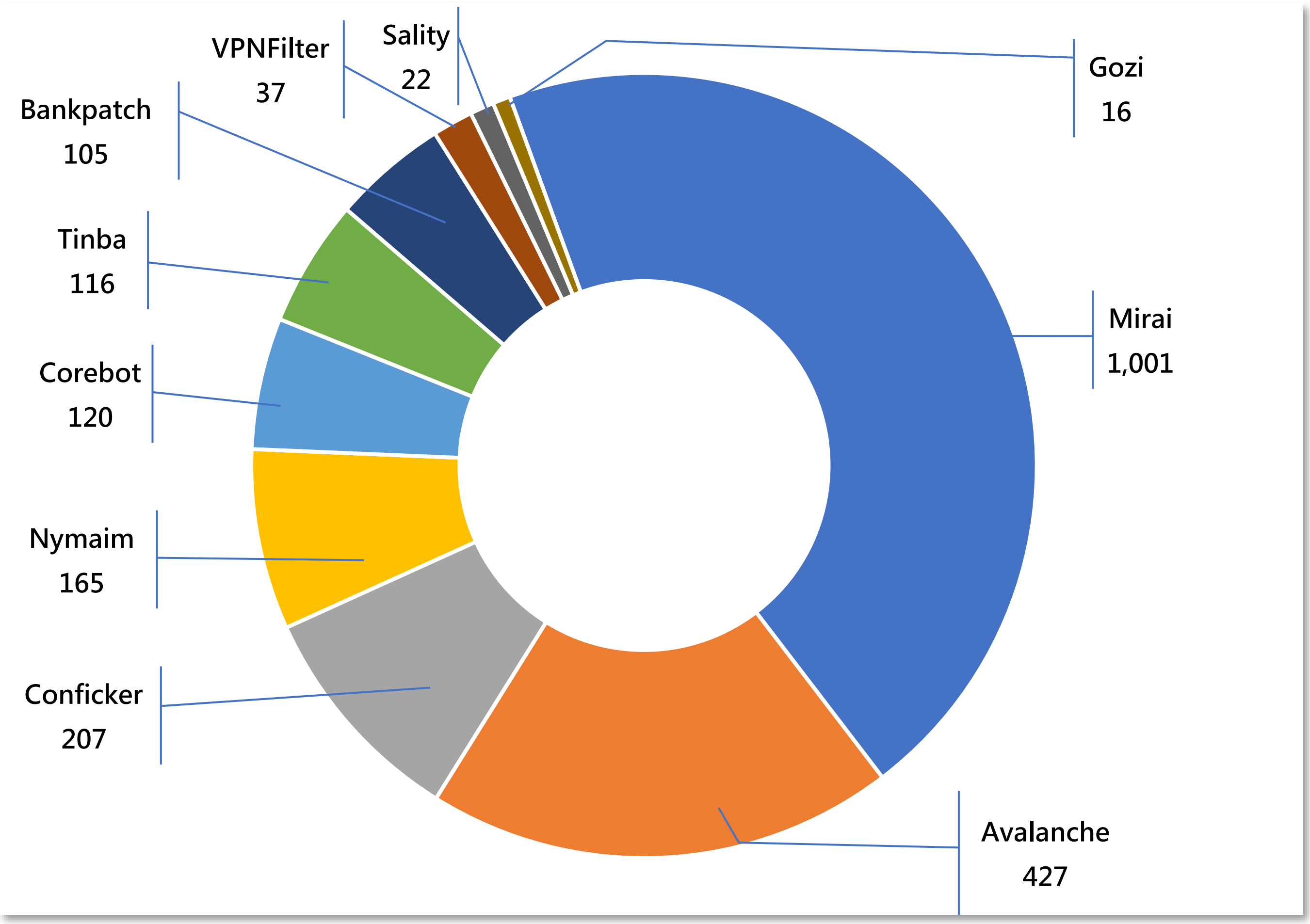
Event Type	2021 Q4	2022 Q1	2022 Q2	2022 Q3	2022 Q4	quarter-to-quarter
Defacement	595	718	118	113	249	+120%
Phishing	1,061	806	5,033	7,141	13,574	+90%
Botnet (Bots)	3,097	3,003	3,642	3,684	2,285	-38%
Total	4,753	4,527	8,793	10,938	16,108	+47%

Major Botnet Families in Hong Kong Network

Mirai
1,001
↓ 31.8%

Avalanche
427
↓ 47.8%

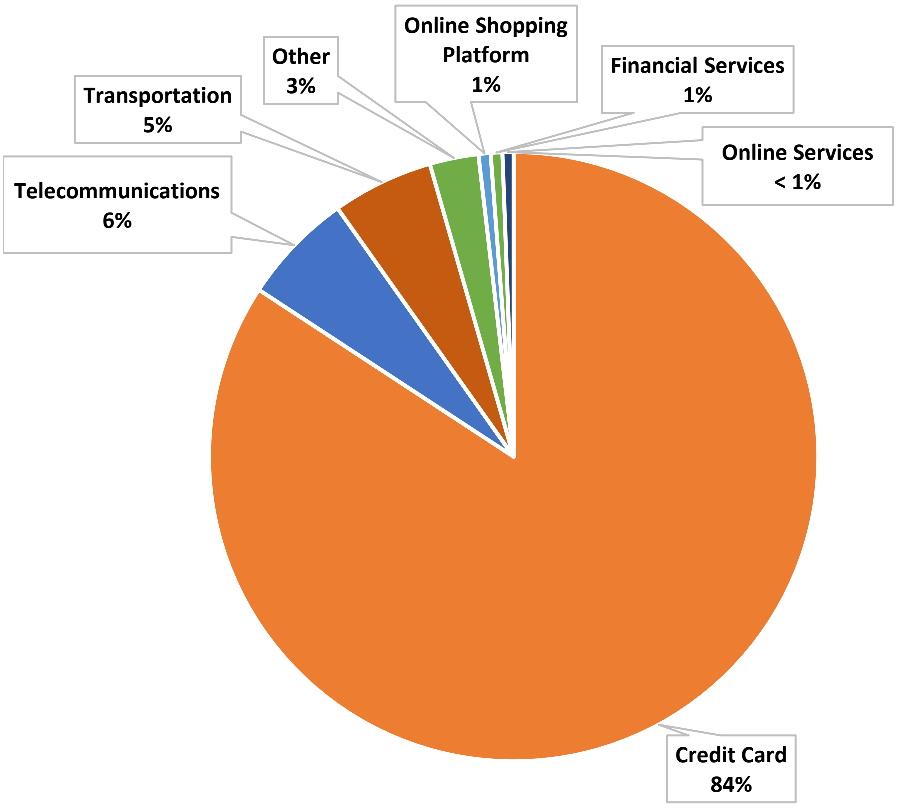
Conficker	207	-7.2%
Nymaim	165	-48.1%
Corebot	120	+421.7%
Tinba	116	-64.8%
Bankpatch	105	+54.4%
VPNFilter	37	-15.9%
Sality	22	-88.5%
Gozi	16	+14.3%



** 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 than in the report because not all bots are activated on the same day.*

Phishing Events Exceed 10,000! Public Must Be More Vigilant on Deception

Phishing events have risen for three consecutive quarters and have exceeded 10,000 for the first time, recording a quarter-on-quarter increase of 90% and a year-on-year increase of 11+ times. Data reported that 84% of the phishing websites were credit card websites; 6% and 5% were related to the telecommunications and transportation industries respectively. Although at the time of compiling the report, random testing have revealed that these websites have already been shut down or are no longer accessible, it is believed that hackers intend to defraud users' credit card information or other personal information through the websites for illegal purposes.

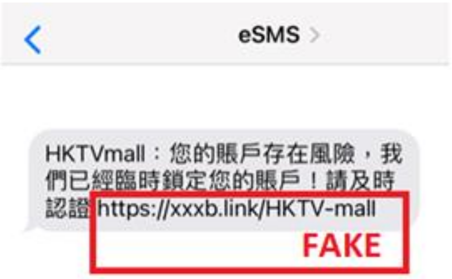


In general, the public holds the view that phishing websites are fake websites created by hackers being directed to through hyperlinks in emails, to lure the victims to enter relevant login names, passwords and other personal information. Hackers then use the information to carry out illegal activities, such as stealing deposits and borrowing money.

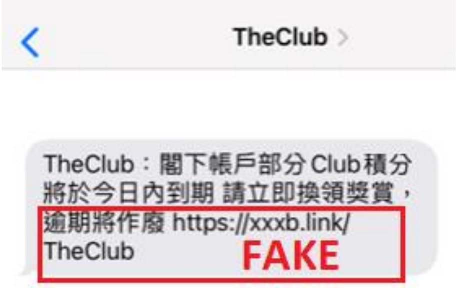
However, some members of the public recently reported to have received a text message from a supermarket chain on their phones, instructing them to click on a hyperlink in the message. The name on the text message was the name of the organisation, and the past messages were also the ones that the user had clicked into or used. So, is the phone broken? Are your phone being hacked? Or have hackers hacked the agency? These hackers' tactics have really made it difficult for the general public to differentiate and identify the source. Anyone who clicks on it carelessly will become the target of hackers. With hackers constantly updating such attacks to maximise their victims' count, HKCERT has compiled a short piece on their tactics in online shopping and areas for online shoppers to be vigilant in order not to fall into these phishing scams.

Phishing Instant Messages

The recent common phishing attack method is mainly to send malicious shortened URL links of the phishing sites through smartphone system built-in and third-party instant messaging apps. As most of those messaging apps allow for the setting up of the sender's name, the hackers could pretend to be a legitimate brand. Below are some examples of instant messages of attacks.


eSMS

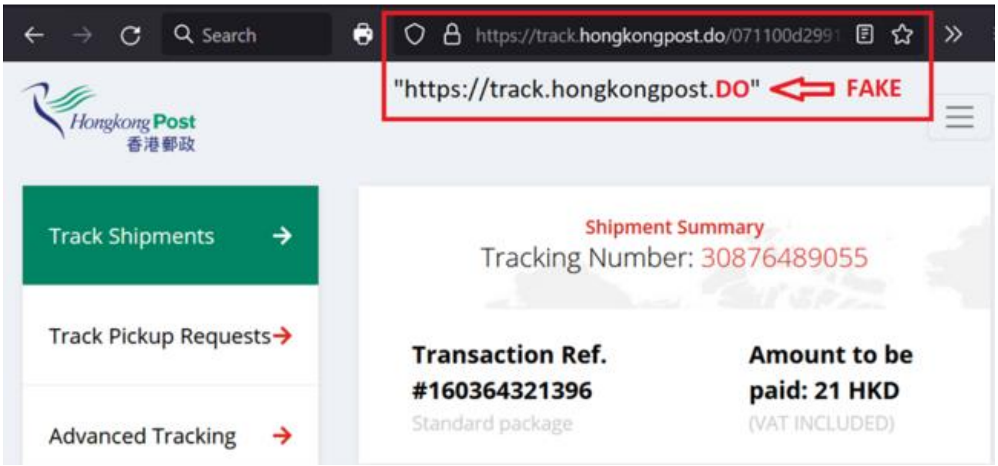
HKTVmall：您的賬戶存在風險，我們已經臨時鎖定您的賬戶！請及時認證 https://xxxb.link/HKTV-mall


TheClub

TheClub：閣下帳戶部分Club積分將於今日內到期 請立即換領獎賞，逾期將作廢 https://xxxb.link/TheClub

Phishing Sites with URLs similar to Legitimate Sites

To trick the victims into assuming the phishing sites were legitimate and proceeding to input information, the hackers would register domain names similar to the brand's legitimate website. Such an example is shown below, in which whereas the legitimate domain name of Hong Kong Post should be 'hongkongpost.hk', the hacker has hosted the phishing site with the domain name of 'hongkongpost[.]do'.



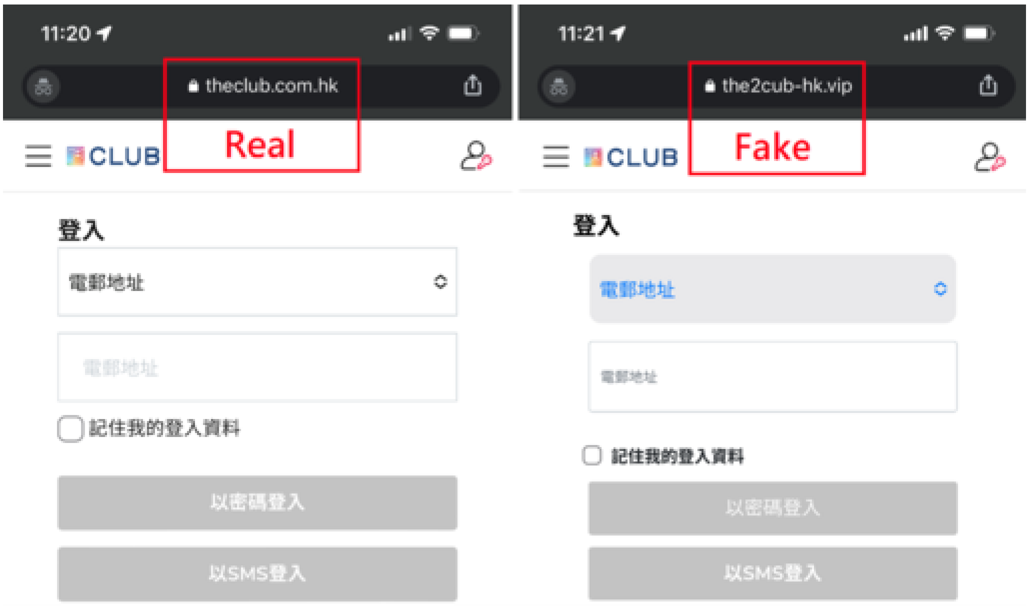
Shipment Summary
Tracking Number: 30876489055

Transaction Ref. #160364321396
Standard package

Amount to be paid: 21 HKD
(VAT INCLUDED)

Phishing Sites with Replication of Legitimate Sites

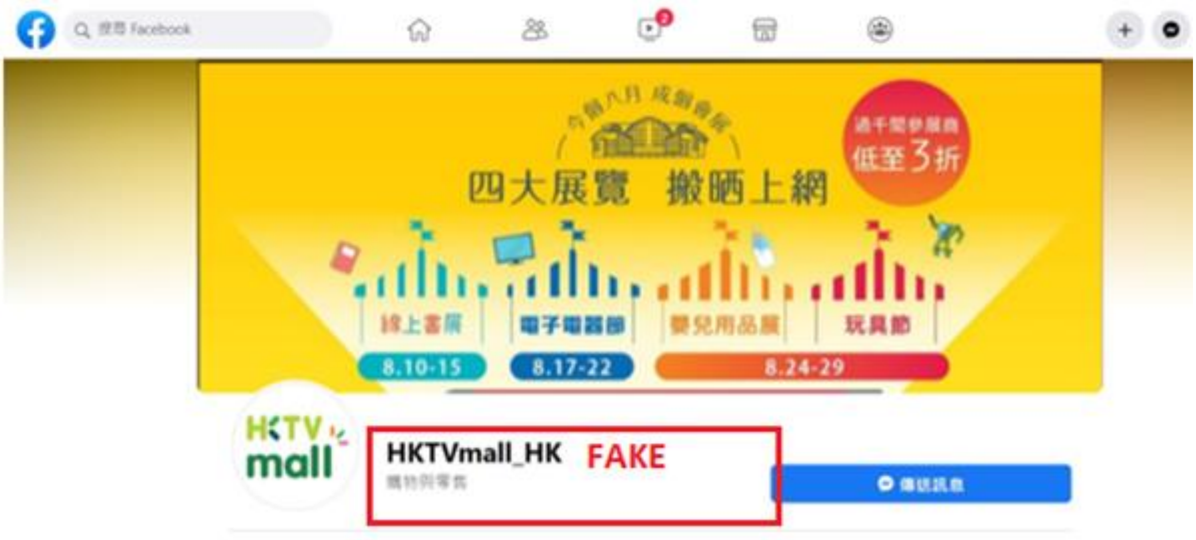
Besides having a domain name and a URL similar to those of a legitimate website, the hackers have recently been replicating part of the legitimate websites, such as the login pages. Since this technique would reduce the efforts for designing a new web interface of the phishing site, most hackers would usually change the backend of the web page after replicating from the legitimate website to fit their needs. This would make the users harder to verify whether the browsing page was legitimate.

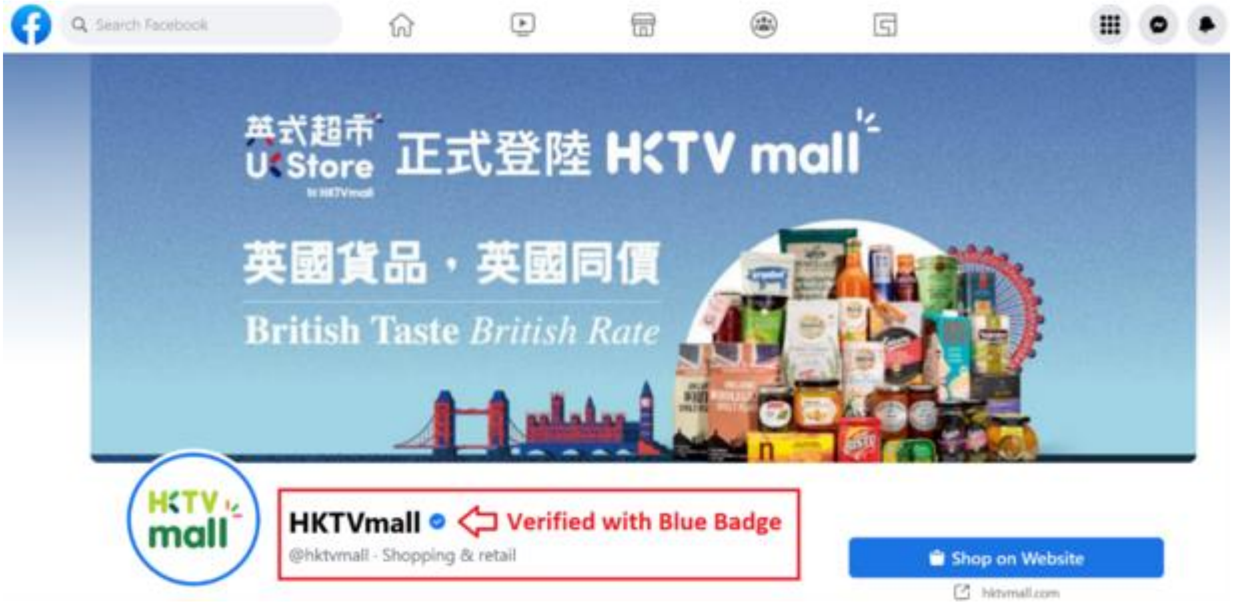


Phishing Page in Social Media Platform

With the widespread public use of social media platforms such as Facebook and Instagram, some hackers would create fake pages on these social media platforms. Most of them would publish some fake promotions on the page attached with links to the phishing sites.

The image below was a Facebook page of HKTVmall created by a hacker, where the design was similar to the official Facebook social media page of HKTVmall. The second image would be the genuine Facebook page of HKTVmall that is being verified by Facebook with a blue badge.

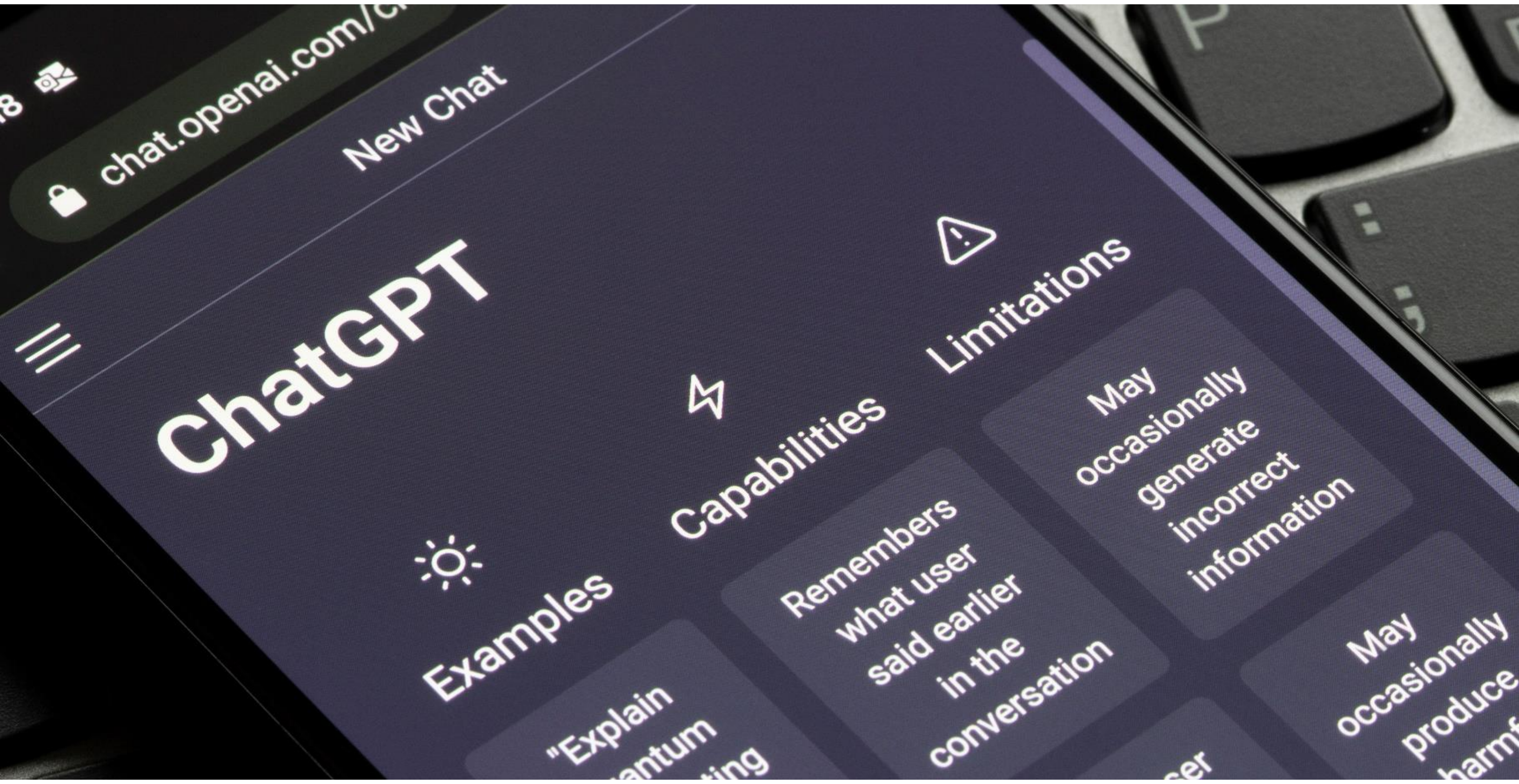




Tips for Safe Online Shopping

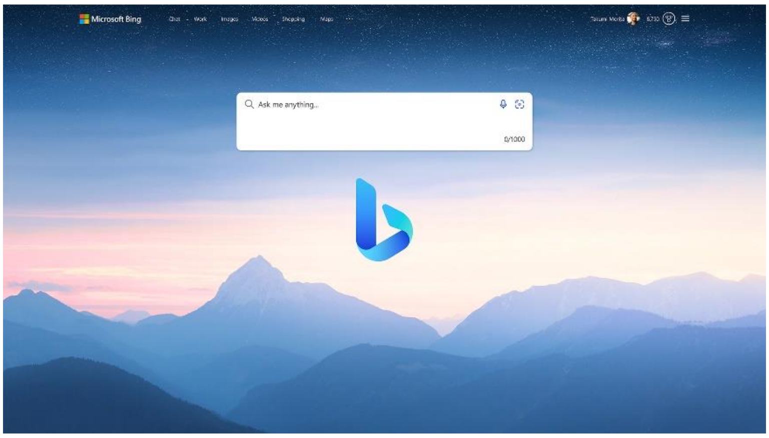
1. Don't click on any links or attachments from an unknown sender. Always enter the URL of the online shopping platform directly in your browser or use bookmarks. Be careful with the legitimacy of the links and emails. For example, check for spelling and grammatical errors in the URL, or whether the sender is trustworthy. If the website does not use HTTPS for encryption, please be careful and do not provide sensitive information.
2. Change the account password of the online shopping platform regularly. Use different passwords for different accounts to prevent from cascading impact if one of them is compromised.
3. Enable multi-factor authentications to enhance account security.
4. Place orders or check order status from the official website or mobile app only.
5. If you receive a suspicious email or instant message, please verify the details at official channels. Do not provide sensitive information to an unknown sender.
6. Check your online payment records regularly for suspicious transactions.
7. Verify the social media page of an online shop by using the social media verification badge function (Such as the Blue Badge in Facebook and Instagram);
8. Adopt anti-phishing feature in web browsers to help blocking phishing attacks; and
9. Use the free search engine “Scameter” of Cyberdefender.hk to identify frauds and online pitfalls through email, URL or IP address, etc.

Cyber Focus: Verify from Various Sources to Ensure Security When Searching for Answers with AI


chat.openai.com/c
New Chat
ChatGPT
Examples
Capabilities
Limitations
"Explain
antum
ing
Remembers what user said earlier in the conversation
May occasionally generate incorrect information
May occasionally produce harm
er

Recently, the artificial intelligence (AI) ChatBot, ChatGPT, has taken the Internet by storm. It is reported that the tool already has 100 million users. Most users say that compared with the traditional search engines which only rely on input queries to provide websites of highly relevance, ChatGPT allows users to ask questions in the format of a person-to-person dialogue and then output responses. In addition, the generated answers are very accurate with detailed explanations, saving the time to search for information after using search engines.

While its developer, OpenAI, says the current free ChatGPT is still in research preview, its popularity marks a major success in bringing AI and machine learning technology to the masses. Recently, major information technology companies have announced plans to integrate AI into their online services: for example, Microsoft will integrate AI technology more powerful than ChatGPT with Bing search engine and Edge browsers; another search engine giant Google will also incorporate its conversational AI service Bard in its products in the coming weeks. It can be seen that, in the near future, more AI technologies will be integrated into different online services and become more involved in our daily lives.



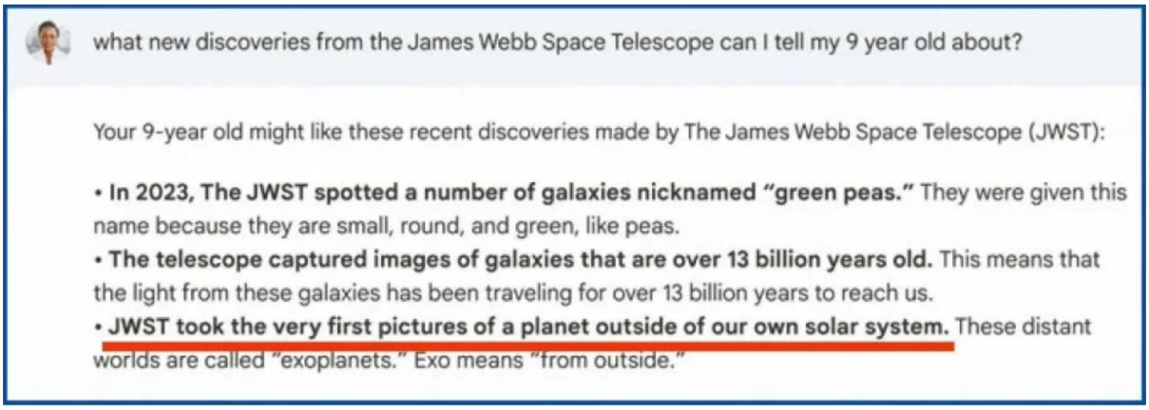
The wide applicability of AI, on the one hand, has made work or life more time-saving and convenient.

For example, some people have used ChatGPT to write programmes and articles faster and less error-prone, and the content of the articles generated is also rich and well-organised; but on the other hand, there have also been criminals who used ChatGPT to create phishing email content and even write malware. Although the system developer has added a security mechanism to prohibit the generation of malicious content, cyber criminals have developed evasion methods and sold them as a Crime-as-a-Service (CaaS). Therefore, the potential security issues cannot be ignored.

At the latest annual information security outlook briefing held in February 2023, HKCERT also predicted that attacks utilising AI and CaaS will be among the five major security risks in 2023. It even listed various possible scenarios of how criminals use AI to attack. On top the above-mentioned examples, AI fraud and poisoning of AI models are also included. In summary, risks involving AI are as follows:

- Data privacy and confidentiality: AI requires vast amounts of data for training, which can include sensitive information such as personal details, financial information and medical records. This may raise privacy concerns, as AI models may be able to access and generate sensitive information.

- Misinformation: AI may insert false or misleading information in order to produce coherent and smooth results. Users rely on such information without verification may be at risk of being convinced the misinformation. In addition, the accuracy of the message will also be affected by the training data it receives. For example, the training data of ChatGPT only goes up to 2021, so when asked about the most recent World Cup champion, it will answer France (2018 champion), not Argentina (2022 champion). Other examples of misinformation include a Google ad promoting its ChatBot Bard, which was found to contain misinformation in an answer to a question about the "James Webb Space Telescope."



what new discoveries from the James Webb Space Telescope can I tell my 9 year old about?

Your 9-year old might like these recent discoveries made by The James Webb Space Telescope (JWST):

• **In 2023, The JWST spotted a number of galaxies nicknamed "green peas."** They were given this name because they are small, round, and green, like peas.
• **The telescope captured images of galaxies that are over 13 billion years old.** This means that the light from these galaxies has been traveling for over 13 billion years to reach us.
• **JWST took the very first pictures of a planet outside of our own solar system.** These distant worlds are called "exoplanets." Exo means "from outside."

- Bias issues: AI training data may come from the Internet, some of its information may contain biases and discriminatory elements. This can lead to AI models producing biased and discriminatory responses. In addition, criminals can also use biased data to train AI models to generate malicious responses. This method is called Adversarial Perturbation.

- Copyright issues: It is important to consider the rights of third parties, for example, owners of any copyrighted material that may be involved in responses output by ChatGPT. Violation of the rights of others, including unauthorised use of their copyrighted material, may result in legal liability. Therefore, when using ChatGPT, please consider and respect the intellectual property rights of its developers and others, and ensure any use of ChatGPT responses complies with laws and regulations.

Actually, AI is a neutral tool and there is no right or wrong in itself. Just like when ChatGPT is asked if it has security risks, its final response is "However, it is important for users and developers to be aware of these security concerns and take appropriate measures to mitigate them." The ultimate responsibility must lie with the users. Finally, when using AI, please maintain a mentality of checking everything and verify facts from various sources.

HKCERT Security Tips: Always Keep System Security Up-to-Date to Prevent Customer Data from Becoming Phishing Feeds

Local photo printing chain, Fotomax, fell victim to a ransomware attack and malicious encryption of its database in October last year, resulting in the leakage of over 600,000 customer data, including name, gender, date of birth, phone number, email address, contact address and delivery address. The Office of the Privacy Commissioner for Personal Data recently published an investigation report into the incident which found the company to be in breach of the Personal Data (Privacy) Ordinance, thereby issuing an Enforcement Notice to Fotomax, directing it to remedy and prevent recurrence of the contravention.

Investigation

Fotomax purchased a firewall in 2018 and enabled its SSL VPN in the following year. Shortly afterwards, the firewall manufacturer announced the discovery of a security vulnerability in the SSL VPN function and urged users to disable it immediately until the operating system had been updated and all account passwords had been reset. It also recommended multi-factor authentication. However, Fotomax did not update the system immediately, which subsequently led to the system being hacked and leakage of customer data.

The incident reflects the importance of maintaining system security all the time. When learnt of potential threats, appropriate follow-up actions must be taken immediately, and any threats should never be treated lightly. Hence, system administrators should pay attention to the following advice to enhance system security:

1. To keep software, operating system, and anti-virus up-to-date and install security patches regularly, especially for systems exposed to the Internet (e.g., firewalls, VPN servers, etc.).
2. Avoid using end-of-life products.
3. Enable multi-factor authentication to protect network and system accounts.
4. Refer to HKCERT's Incident Response Guidelines for SMEs to establish and review security incident response plan.
5. Refer to the concept of zero trust and network segmentation to reduce the attack surface and the scope of affected network.
6. Back up all critical data, at least one local backup and one remote backup.
7. Encrypt all sensitive data.

Also, as the incident involves leakage of personal data, HKCERT believes that the data will be or has already been used for phishing attacks and scam incidents. The public is advised to pay extra attention to suspicious emails and calls. HKCERT also reminds enterprises and users:

1. To pay attention to the spelling of the URL, carefully check for errors or suspicious elements, and verify the authenticity of the website.
2. Not to assume that websites using the HTTPS protocol must be authentic and credible websites, and phishing websites can also use the HTTPS protocol.
3. Not to open any links or attachments at will and think twice before providing personal information.
4. To confirm the identity of the sender and the content before opening attachments and links in emails or instant messages;
5. To regularly update the login password and enable multi-factor authentication for each account.

In addition, if the public has doubts about the phone number, email address, website URL and IP address, they can use the "Scameter" (https://cyberdefender.hk/en-us/scameter/) by CyberDefender to check whether they are frauds/online pitfalls or not.

For more details, please refer to:
https://www.hkcert.org/blog/always-keep-system-security-up-to-date-to-prevent-customer-data-from-becoming-phishing-feeds

Analysis Report: Analysing AgentTesla Spyware

According to Israeli cyber security solution provider Check Point's "Global Threat Impact Index" monthly report published in early November, it was reported that AgentTesla continued to be one of the "Most Wanted Malwares" in the world, affecting over 7% of enterprises. In this regard, HKCERT collected a sample of AgentTesla to analyse its attack vector and operations. Security advice is also offered to help the public to protect against the threat.

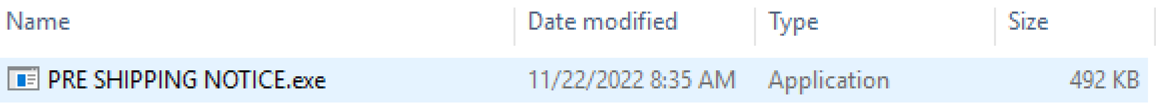
What is AgentTesla?

First appeared in 2014, AgentTesla is a spyware developed using .Net framework and designed for stealing user credentials. Hackers use this malware to spy on victims, intercept all user inputs in programs and browsers, and then transmit the information stolen to the Command-and-Control Server.

Investigate the Malicious Email Attachment

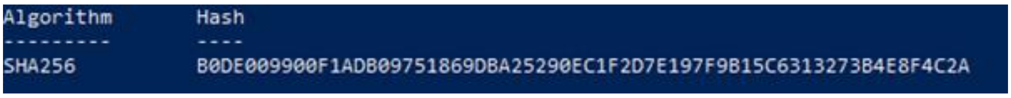
Hackers usually send phishing emails to lure victims to download and execute the malware. In the collected sample, hackers used an email attachment named "PRE SHIPPING NOTICE.zip" to try to guide victims to download and open it.

After downloading and opening the “PRE SHIPPING NOTICE.zip” file, a file named “PRE SHIPPING NOTICE.exe” was extracted.



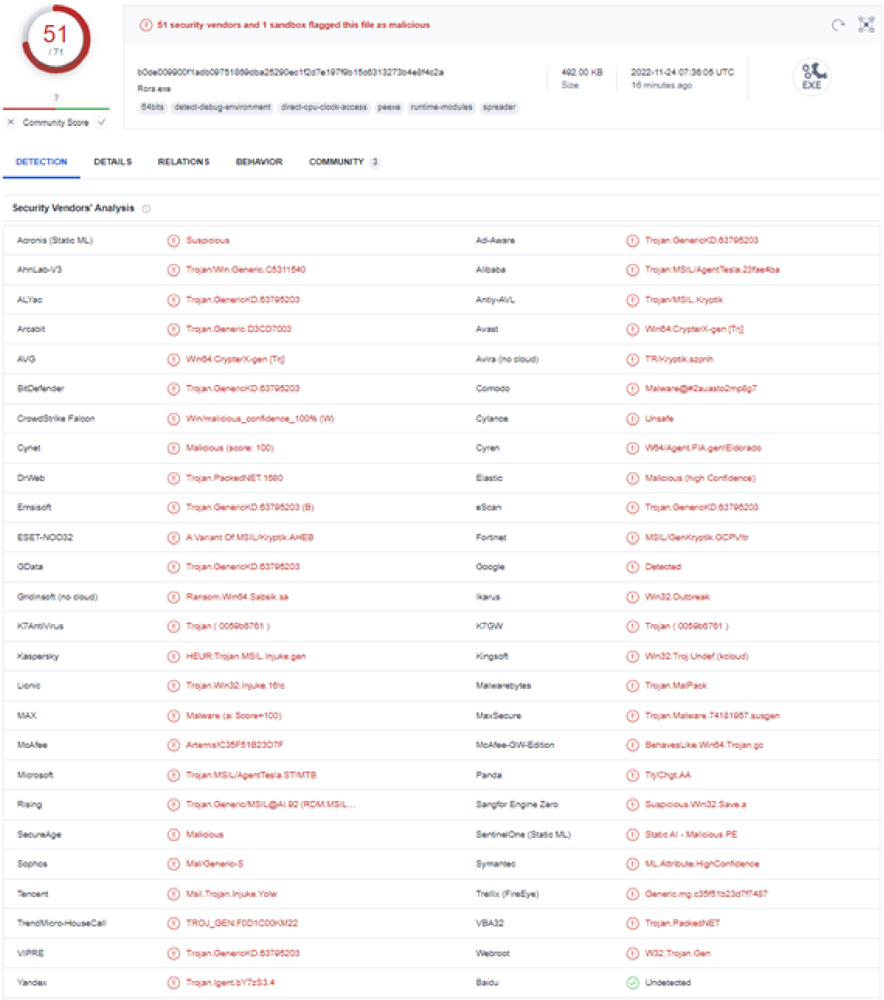
Name	Date modified	Type	Size
PRE SHIPPING NOTICE.exe	11/22/2022 8:35 AM	Application	492 KB

To check on VirusTotal website, a SHA256 hash value of the file is required. The PowerShell cmdlet Get-FileHash was executed to get the hash value of “PRE SHIPPING NOTICE.exe” which was uploaded to the VirusTotal.



```
Algorithm       Hash
---------       ----
SHA256          B0DE009900F1ADB09751869DBA25290EC1F2D7E197F9B15C6313273B4E8F4C2A
```

In the VirusTotal search result, 51 cyber security companies can identify the file as malware and AgentTesla.



51 security vendors and 1 sandbox flagged this file as malicious

b0de009900f1adb09751869dba25290ec1f2d7e197f9b15c6313273b4e8f4c2a
Rora.exe
64bits detect-debug-environment direct-cpu-clock-access peexe runtime-modules spreader

492.00 KB
Size

2022-11-24 07:36:06 UTC
16 minutes ago

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.GenericKD.63795203
AhnLab-V3	Trojan/Win.Generic.C5311540	Alibaba	Trojan:MSIL/AgentTesla.22fae4ba
ALYac	Trojan.GenericKD.63795203	Antiy-AVL	Trojan/MSIL.Kryptik
Arcabit	Trojan.Generic.D3CD7003	Avast	Win64:CrypterX-gen [Trj]
AVG	Win64:CrypterX-gen [Trj]	Avira (no cloud)	TR/Kryptik.szpnh
BitDefender	Trojan.GenericKD.63795203	Comodo	Malware@#2auasto2mp8g7
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W64/Agent.FIA.gen!Eldorado
DrWeb	Trojan.PackedNET.1680	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.GenericKD.63795203 (B)	eScan	Trojan.GenericKD.63795203
ESET-NOD32	A Variant Of MSIL/Kryptik.AHEB	Fortinet	MSIL/GenKryptik.GCPV!tr
GData	Trojan.GenericKD.63795203	Google	Detected
Gridinsoft (no cloud)	Ransom.Win64.Sabsik.sa	Ikarus	Win32.Outbreak
K7AntiVirus	Trojan (0059b6761)	K7GW	Trojan (0059b6761)
Kaspersky	HEUR:Trojan.MSIL.Injuke.gen	Kingsoft	Win32.Troj.Undef.(kcloud)
Lionic	Trojan.Win32.Injuke.16!c	Malwarebytes	Trojan.MalPack
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.74181967.susgen
McAfee	Artemis!C35F51B23D7F	McAfee-GW-Edition	BehavesLike.Win64.Trojan.gc
Microsoft	Trojan:MSIL/AgentTesla.STIMTB	Panda	Trj/Chgt.AA
Rising	Trojan.Generic/MSIL@AI.92 (RDM.MSIL...	Sangfor Engine Zero	Suspicious.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Msil.Trojan.Injuke.Yolw	Trellix (FireEye)	Generic.mg.c35f51b23d7f7487
TrendMicro-HouseCall	TROJ_GEN.F0D1C00KM22	VBA32	Trojan.PackedNET
VIPRE	Trojan.GenericKD.63795203	Webroot	W32.Trojan.Gen
Yandex	Trojan.Igent.bY7zS3.4	Baidu	Undetected

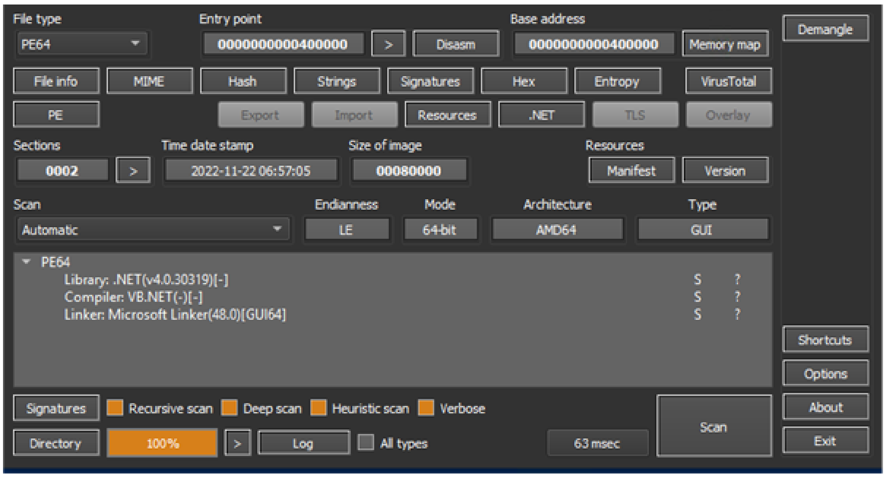
# Search conducted on 24 November 2022

Analysing “PRE SHIPPING NOTICE.exe”

It is determined the file “PRE SHIPPING NOTICE.exe” is an executable file developed by VB.NET. Also, it is noted that no software packing technique is applied to the file.

What is Software Packing?

Software packing is a method of compressing or encrypting an executable. Packing an executable will change the file signature in an attempt to avoid signature-based detection.

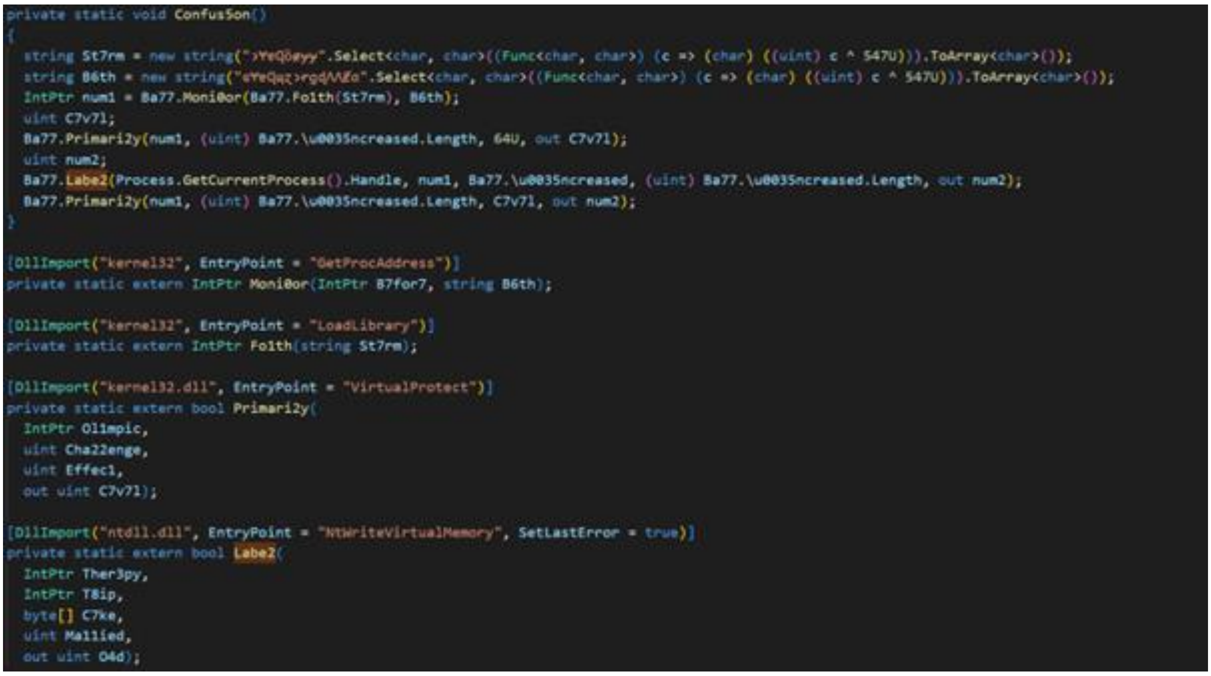


File type: PE64
Entry point: 0000000000400000
Base address: 0000000000400000
Sections: 0002
Time date stamp: 2022-11-22 06:57:05
Size of image: 00080000
Scan: Automatic
Endianness: LE
Mode: 64-bit
Architecture: AMD64
Type: GUI

```
PE64
    Library: .NET(v4.0.30319)[-]        S  ?
    Compiler: VB.NET(-)[-]              S  ?
    Linker: Microsoft Linker(48.0)[GUI64]  S  ?
```

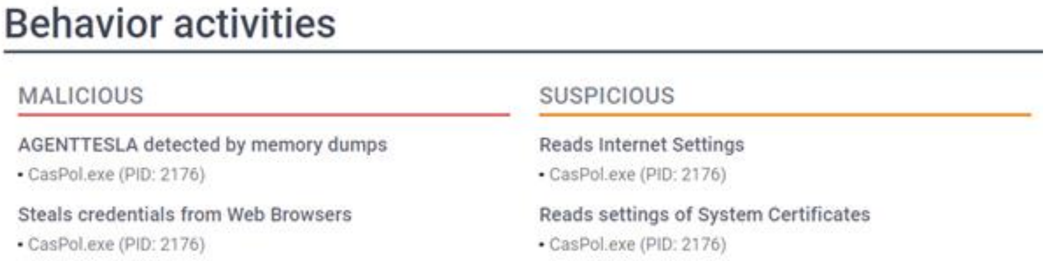
☑ Recursive scan ☑ Deep scan ☑ Heuristic scan ☑ Verbose
100%
□ All types
63 msec

Once the programming language used was determined, reverse engineering technique was applied to get the code of “PRE SHIPPING NOTICE.exe”. A part of the code of “PRE SHIPPING NOTICE.exe” has shown that AgentTesla is using Windows ntdll.dll to inject the payload.



```
private static void ConfusSon()
{
  string St7rm = new string("›YeQöeyy".Select<char, char>((Func<char, char>) (c => (char) ((uint) c ^ 547U))).ToArray<char>());
  string B6th = new string("eYeQqz›rgdWEo".Select<char, char>((Func<char, char>) (c => (char) ((uint) c ^ 547U))).ToArray<char>());
  IntPtr num1 = Ba77.Moni8or(Ba77.Fo1th(St7rm), B6th);
  uint C7v71;
  Ba77.Primari2y(num1, (uint) Ba77.\u0035ncreased.Length, 64U, out C7v71);
  uint num2;
  Ba77.Labe2(Process.GetCurrentProcess().Handle, num1, Ba77.\u0035ncreased, (uint) Ba77.\u0035ncreased.Length, out num2);
  Ba77.Primari2y(num1, (uint) Ba77.\u0035ncreased.Length, C7v71, out num2);
}

[DllImport("kernel32", EntryPoint = "GetProcAddress")]
private static extern IntPtr Moni8or(IntPtr B7for7, string B6th);

[DllImport("kernel32", EntryPoint = "LoadLibrary")]
private static extern IntPtr Fo1th(string St7rm);

[DllImport("kernel32.dll", EntryPoint = "VirtualProtect")]
private static extern bool Primari2y(
  IntPtr O11mpic,
  uint Cha22enge,
  uint Effec1,
  out uint C7v71);

[DllImport("ntdll.dll", EntryPoint = "NtWriteVirtualMemory", SetLastError = true)]
private static extern bool Labe2(
  IntPtr Ther3py,
  IntPtr T8ip,
  byte[] C7ke,
  uint Ma11ied,
  out uint O4d);
```

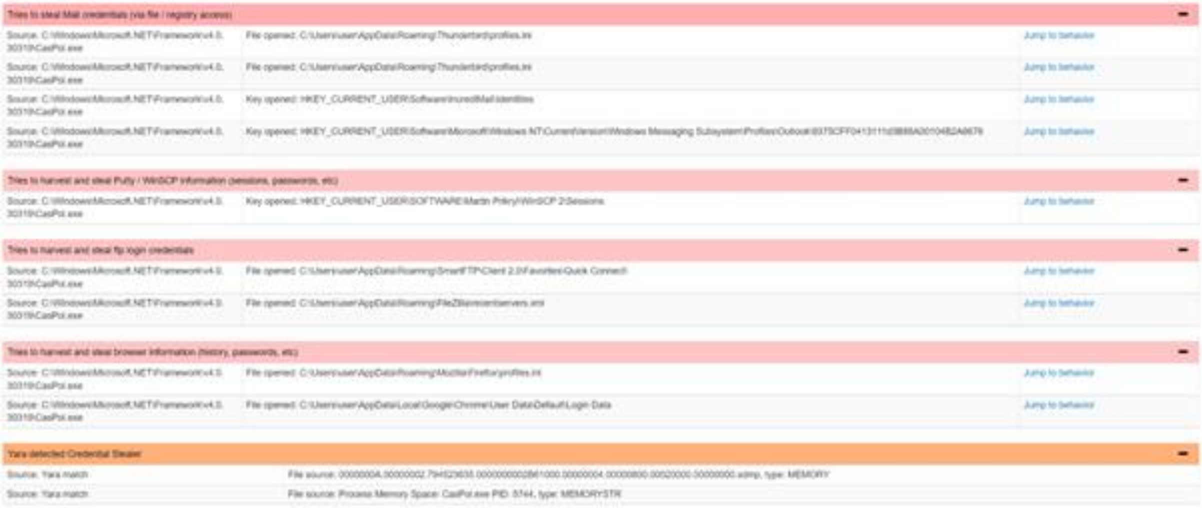
After the payload had been executed, the behaviour detection of AgentTesla on the victim computer showed that it will steal the computer setting, credentials of system and browsers.



Behavior activities

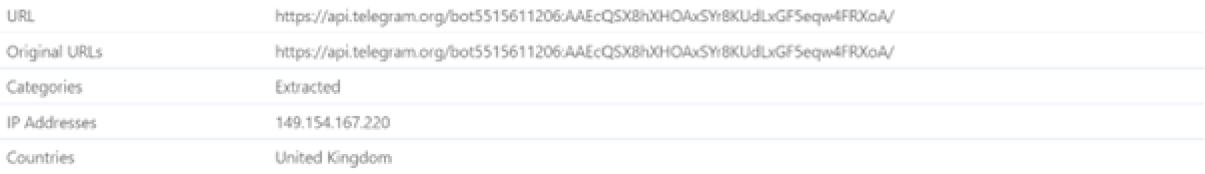
MALICIOUS	SUSPICIOUS
AGENTTESLA detected by memory dumps • CasPol.exe (PID: 2176)	Reads Internet Settings • CasPol.exe (PID: 2176)
Steals credentials from Web Browsers • CasPol.exe (PID: 2176)	Reads settings of System Certificates • CasPol.exe (PID: 2176)

Further deep dive into the stolen data using YARA malware research and detection tool found that it included mail profile setting (e.g. thunderbird, incredimail, MS Outlook), remote server credentials (e.g. WinSCP, FileZilla) and the login password stored in browsers (e.g. Firefox, Chrome)



Tries to steal Mail credentials (via file / registry access)		−
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Roaming\Thunderbird\profiles.ini	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Roaming\Thunderbird\profiles.ini	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	Key opened: HKEY_CURRENT_USER\Software\IncrediMail\Identities	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	Key opened: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	Jump to behavior
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)		−
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	Key opened: HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	Jump to behavior
Tries to harvest and steal ftp login credentials		−
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect\	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Roaming\FileZilla\recentservers.xml	Jump to behavior
Tries to harvest and steal browser information (history, passwords, etc)		−
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	Jump to behavior
Source: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	Jump to behavior
Yara detected Credential Stealer		−
Source: Yara match	File source: 0000000A.00000002.794523635.00000000028E1000.00000004.00000800.00020000.00000000.sdmp, type: MEMORY	
Source: Yara match	File source: Process Memory Space: CasPol.exe PID: 5744, type: MEMORYSTR	

AgentTesla would transfer the stolen data via Telegram API to the hacker’s Telegram account.



URL	https://api.telegram.org/bot5515611206:AAEcQSX8hXHOAxSYr8KUdLxGF5eqw4FRXoA/
Original URLs	https://api.telegram.org/bot5515611206:AAEcQSX8hXHOAxSYr8KUdLxGF5eqw4FRXoA/
Categories	Extracted
IP Addresses	149.154.167.220
Countries	United Kingdom

Security Advice

Malicious email is one of the spreading channels of AgentTesla. Moreover, different variants of AgentTesla have already appeared on the Internet. Hence, HKCERT recommends users to:

1. Always keep the system, software, and antivirus software up to date
2. Do not open unknown files, web pages and emails
3. Confirm the legitimacy of sender and the content of the email before opening the attachments and links in the email,
4. Check the file extension to avoid being misled by the file name. Do not open any executable file or Microsoft Office files with macros obtained from unknown source.
    a. Executable file extension: .exe, .vbs, .js, .bat, msi, .ps, psc1, .cmd, .wsf, .jar, .reg, etc.
    b. Microsoft Office files with macros can be contained in all kinds of Office files (e.g. .doc/.docm, .xls/.xlsm, .ppt/.pptm). Users are advised to disable all macros from auto-run in the security settings.
5. Use password management tools to manage the passwords instead of storing them on browsers.
6. Use lower privileged accounts for daily use instead of system administrator accounts.
7. Set up "multi-factor authentication" (MFA) to enhance the account security.

For more details, please refer to:
https://www.hkcert.org/blog/analysing-agenttesla-spyware

-End-

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