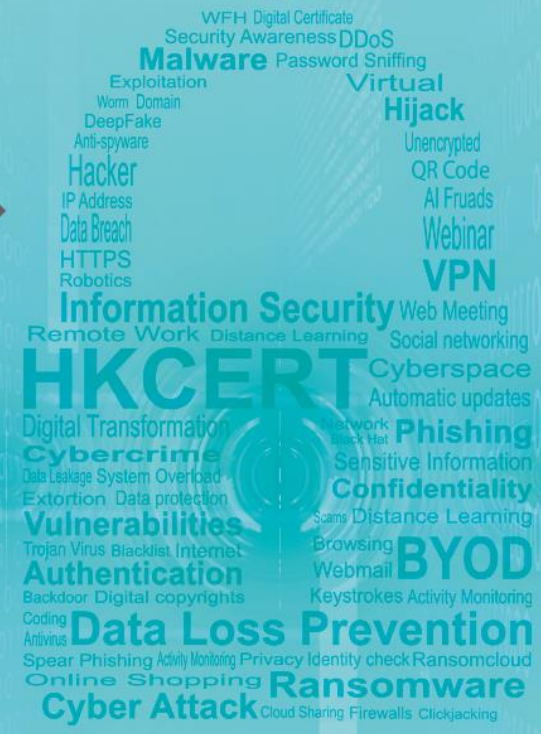
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report 2023 Q4

Release Date: Feb 2024



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 organisations 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	2023-11

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

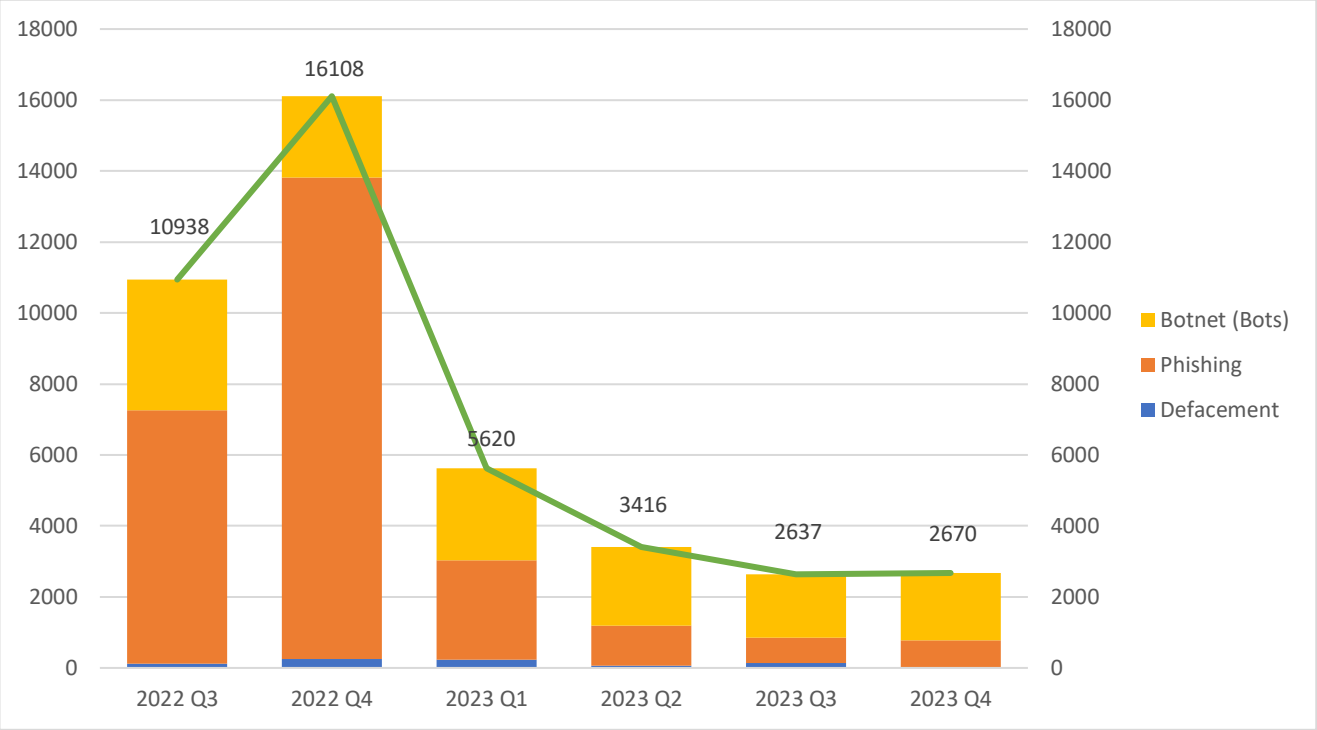
Highlights of the 2023 Q4 Report

Unique security events related to Hong Kong

2,670

Quarter-to-quarter

1.3%↑



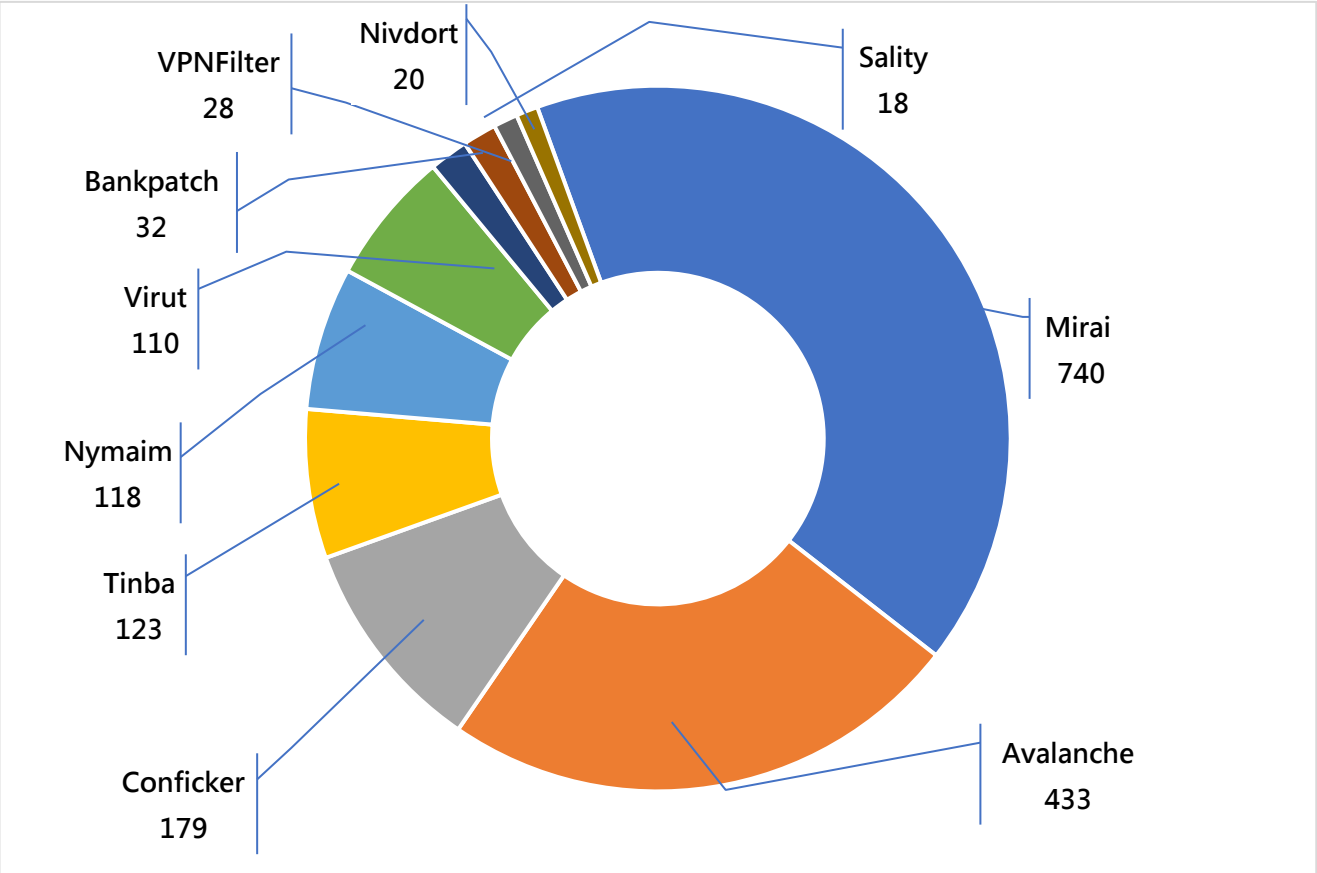
Event Type	2022 Q4	2023 Q1	2023 Q2	2023 Q3	2023 Q4	quarter-to-quarter
Defacement	249	233	69	132	31	-76.5%
Phishing	13,574	2,804	1,120	722	742	+2.8%
Botnet (Bots)	2,285	2,583	2,227	1,783	1,897	+6.4%
Total	16,108	5,620	3,416	2,637	2,670	+1.3%

Major Botnet Families in Hong Kong Network

Mirai
740
↓25.1%

Avalanche
433
↑111.2%

Conficker	179	+1.7%
Tinba	123	+15%
Nymaim	118	+68.6%
Virut	110	+3.8%
Bankpatch	32	+113.3%
VPNFilter	28	-3.4 %
Nivdort	20	+233.3%
Sality	18	-5.3%



** 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.*

Cyber Attacks Increased Slightly Quarter-on-Quarter, and the Public Needs to be Vigilant!

The security incident figures for the fourth quarter of 2023 were officially released. Phishing increased slightly this quarter by 2.8% compared to the previous quarter while botnets (zombie computers) also recorded a 6.4% increase. It was worth noting that the relevant figures only reflected attacks originating in Hong Kong and did not include overseas attacks targeting Hong Kong. If the hacker hosts the attack on an overseas server and attacks Hong Kong users, these types of cyber attacks will not be reflected in the numbers. The actual numbers were much higher. The number of security incidents handled by HKCERT also increased in the fourth quarter, indicating that hacker activities are still active in Hong Kong and the public needs to take more precautions.

2023 came to end. Let's review the major cyber attacks that occurred in Hong Kong in the past year. From March to April 2023, there were criminals to impersonate Hong Kong company reward programs and telecommunications providers, using smishing to trick victims into filling in sensitive information. Some victims even suffered from financial losses. Between August and September 2023, the systems of two institutions in Hong Kong were hacked and a large amount of sensitive information was stolen. One of the institutions was publicly extorted and threatened to leak the stolen data by hackers, demanding a huge ransom. In the end, the institution refused to pay the ransom and the hacker leaked the content. A large amount of sensitive information was leaked on the "dark web". Citizens faced with criminals using phishing attacks with search engine optimsation (SEO) . A large number of fake instant messaging software web pages appeared and was pinned to the top of search engine results. Many citizens' instant messaging software accounts were hijacked. Hong Kong's cyber security was sounding the alarm. During November 2023, phishing attacks were extended to social platforms by any means, pretending to be the pages of well-known local brands. Some criminals spread malicious apps through the instant messaging function of social platforms to steal sensitive bank information of victims.

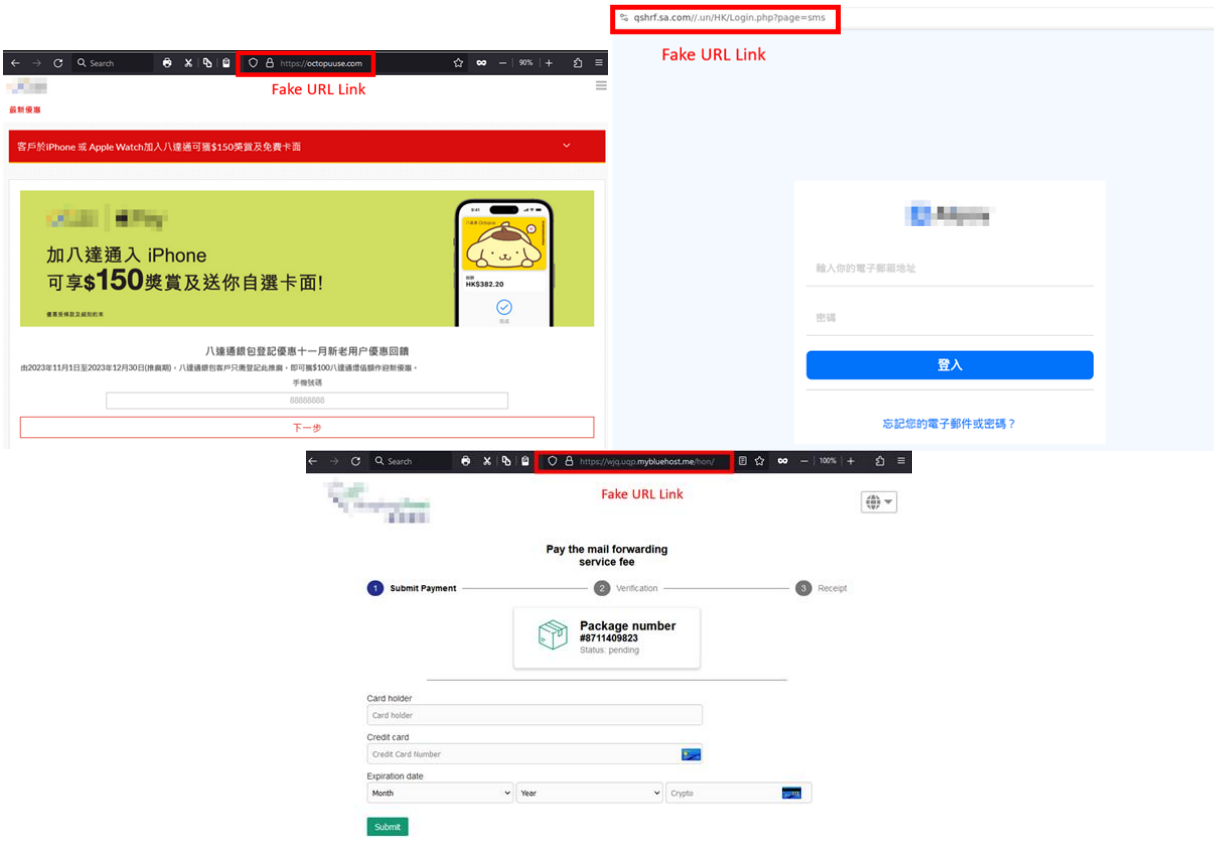
In 2023, many measures have also been implemented in terms of cyber security. After 23 February 2023, all users should complete real-name registration for their SIM cards with their telecommunications service providers. If the registration is not completed, they cannot be used anymore. On December 28, 2023, the first phase of the "Short Message Service (SMS) Sender Registration Scheme" was officially implemented. Telecommunications companies, banks and individual government departments have already participated. Measures will be extended to other industries. Both measures are aimed at combating phone scams.

Taking Security Best Practice During Festive Season

Online services have become more and more popular. We should stay vigilant on cyber security risks during the festive season while we enjoy the convenience.

Phishing Attacks

In addition to buy goods to be festive presents, people can pay for their trip online to receive sales and discounts for flights and hotels in the Internet. Hackers may find this as the opportunity to launch attacks towards the Internet users. From the hackers' point of view, launching phishing attacks would be low-cost and low-effort tactics when compared to launching other kinds of cyber attacks. Generally, people would easily get tricked and fall into the trap of phishing attacks because hackers can easily create phishing content that looks very similar to the official one, which is not easy to distinguish. From sending a phishing message or email, hackers aim to trick the targeted user to open a malicious URL link or even a malicious attachment that may contain malware. Recent phishing attacks in Hong Kong have been observed that hackers have been creating phishing pages impersonating local membership platforms. They were tricking users into entering login credentials on the phishing page and stealing sensitive information, such as credit card information, from the account after a successful login. Below is an example of recent discovered phishing webpage impersonating the common membership platforms in Hong Kong.



Besides of phishing websites, many fake travel and retail agencies have appeared on social media pages, offering a large number of discounts such as “Big Sale”, “Up to 70% off”, “Limited-time/Limited-quantity promotion at 90% off”, etc, to attract citizens to inquire and defraud them of their money and a large amount of personal information, including name, ID card, credit card information, phone number, and family information. How can citizens distinguish whether the social media pages and the contents of their advertising messages are genuine or not? In addition to paying attention to the blue verification badge or the blue tick mark, the number of likes and followers on the page, they can also keep an eye on the following points to prevent online shopping scams:

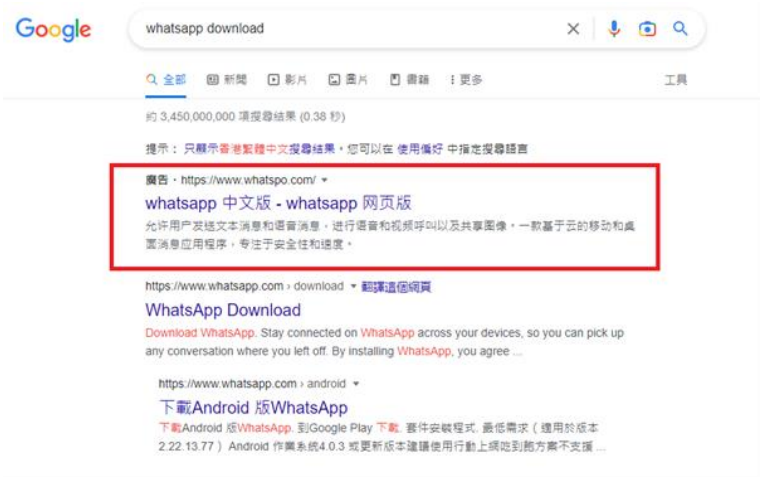
1. The pixels of the company logo or image are low: Most of the images used by hackers are obtained by screenshots or stolen from other websites, and they are not the original images, so the pixels are lower. In addition, citizens could use Google Images to search if similar photo was found on other websites.
2. Contact information is not detailed: The contact information displayed is not detailed, and the provided contact information is personal email or phone.
3. The location of the management personnel is overseas: Citizens can check the location of relevant management personnel through this path "About" > "Page transparency" on the page. If the location of some management personnel is different from the location of the page, it is necessary to be vigilant about the authenticity of the page.
4. Whether the page name is frequently changed and the establishment time: Fake pages often change their names and are established for a short period of time because their fraud methods are different each time.

Citizens can check the location of management personnel and establishment time through this path "About" > "Page transparency" on the page

5. The page only has a small number of posts: Most of the posts on fake pages are copied from the past one to two months.
6. Abnormal amount of likes/comments: Pay attention to whether the likes/comments come from countries outside the target group and whether the content of the comments is roughly the same.

Identify/Credential Theft

Other than launching phishing attacks to lure users to provide personal information, hackers could expand their scale of attacks if they successfully stole the users' login credentials. This let hackers to impersonate the user to launch attacks to their families and friends. Especially during holidays, it is not surprising to receive messages from friends with whom you rarely communicate, and therefore, our vigilance may be lowered. Hackers can launch identify attacks in various ways, including Adversary-in-the-middle (AiTM) Attacks, Fake Ads, Social Engineering Attacks, etc. Most hackers would aim to compromise a targeted user's account and perform malicious activities within the compromised account. The recent tactic of Identify Attack is that hackers would create fake WhatsApp login sites and push the malicious webpages to the top of the search results in search engines. If users carelessly browsed the malicious webpages and conducted login action, hackers could obtain the account session and gain access to all of the information in the WhatsApp account to launch further attacks.



Security Best Practices

To have safer travel and enjoy shopping with less worries in the digital era, people should consider following the security best practices below.

For security best practices when travelling abroad:

1. Use personal device to log into personal accounts and avoid using public devices;
2. Use trusted public Wi-Fi connections, avoid to connect to Wi-Fi hotspots with low security settings;
3. Check any malicious logins in your online accounts;
4. Check carefully when purchasing goods using mobile payments; verify the payment receiver and the amount before confirming and proceeding with the payment;
5. If required to access a webpage or scan QR code, verify if the URL of the website is legitimate before entering any information;
6. Do not open any links or attachments sent to overseas SIM cards. It might be related to phishing attacks;
7. If necessary, install applications only from official websites and app stores;
8. Do not charge your device at unknown public charging port to avoid Juice Jacking attacks;
9. Do not leave your device unattended; and
10. Power off your devices at home and office if they are no use, and power off your portable devices when it is not in use overnight during travel.

For security best practices when shopping online:

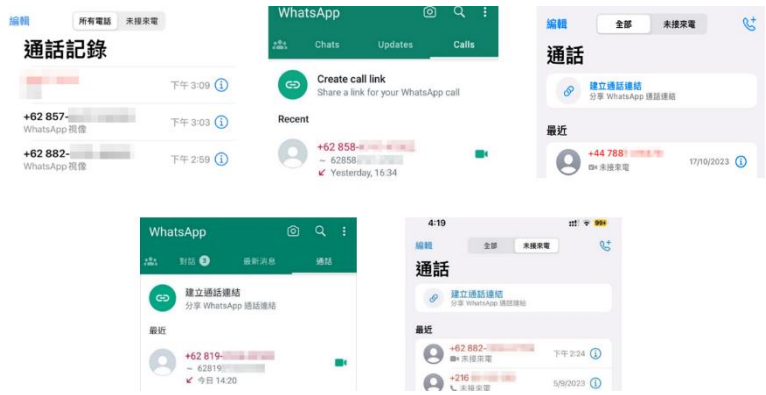
1. Don't click on any links or attachments from an unknown sender. Always enter the URL of the online shopping platform directly in your browser or use bookmarks. Be careful with the legitimacy of the links and emails. For example, check for spelling and grammatical errors in the URL, or whether the 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 a cascading impact if one of them is compromised;
3. If the platform supports multi-factor authentications, enable it to enhance security;

4. Place orders or check order status from the official website or mobile app only;
5. Do not save any sensitive information, such as credit card information, in online accounts;
6. Check your online payment records regularly for suspicious transactions;
7. 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;
8. Adopt anti-phishing features in web browsers to help block 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.

For more details, please refer to:
https://www.hkcert.org/blog/taking-security-best-practice-during-festive-season

Raise Public Awareness of Cyber Security:
Guard against Risks of Unknown WhatsApp Video Calls

With the advancement of technology, cyber security has become an important issue that cannot be ignored in our lives. Cyber-attacks have become increasingly sophisticated. Some citizens have reported to the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) that they have received suspicious WhatsApp video calls from strangers (using area codes such as +62 and +44), claiming to be from the police or banking institutions and even knowing the names of the victims. This has raised public concern about the risks of unknown video calls. This article aims to raise public awareness of cyber security and provide practical advice to guard against unknown video calls.



Why Attackers Initiate Video Calls than Voice Calls?

Personal Identity : Attackers may capture the appearance of citizens through video calls and relating the video or image capture to an identifiable individual through Internet search from Google, social media posts or online photo albums. Also, it can observe personal details in targets' backgrounds or appearances that can aid future social engineering or identity theft attacks.

Obtain Facial Information for Deepfake : Attackers may obtain the appearance and voice of citizens through video calls to create a highly realistic deepfake, which may be used in other fraudulent activities to your family members or friends.

Identity Impersonation for Illegal Activities : With both video and voice of the attackers is visible, it is easier for attackers to create an illusion with fake scene, background or costume, pretending to be from organizations like law enforcement or banks to sound legitimate and intimidating for financial scam.

Sense of Urgency : A video call makes the targets feel they need to respond quickly, leaving less time for critical thinking. This helps attackers maintain control of the interaction for scam.

What Are the Risks of Unknown Video Calls?

Scams : Attackers may attempt to engage in fraudulent activities through video calls, such as impersonating police officers or bank staff to obtain your personal information or money.

Privacy Breach : Strangers may use video calls to invade your privacy by secretly recording videos or taking photos for improper use or dissemination. In addition, careless use of the screen sharing function in WhatsApp increases the risk of data leakage (Right Image). For example, the user is using banking service or typing a password.

Practical Advice to Guard against Unknown Video Calls

Exercise Caution in Answering Calls : Maintain a cautious attitude towards video calls from unknown individuals. If you don't know the caller, you can choose not to answer or directly reject the call.

Avoid Disclosing Personal Information : Do not disclose sensitive personal information such as passwords or bank account numbers during unknown video calls. Legitimate institutions or their staff will not request such information through video calls.

Exercise Caution with File Downloads : Be cautious if a stranger request you to download or open a file during a video call. Only download files from trusted sources and scan them with secure antivirus software.

Discuss with Family and Friends : Discuss these risks with your family and friends, increase awareness of unknown video calls together, and provide mutual support and advice.

Configure Privacy Settings : Check the privacy options of your devices and applications to ensure that only authorized individuals can initiate video calls with you, or you can mute unknown callers (Open WhatsApp “Setting” > “Privacy” > “Calls” > enable “Sillence Unknown Callers”).

Cyber security is increasingly important, and guarding against the risks of unknown video calls is one of the challenges we must face. By following the practical advice provided in this article and maintaining vigilance, individuals can enhance cyber security and protect themselves from potential threats. Exercise caution in answering video calls from strangers, avoid disclosing sensitive personal information, be cautious with file downloads, configure privacy settings, and

For more details, please refer to:
https://www.hkcert.org/blog/raise-public-awareness-of-cyber-security-guard-against-risks-of-unknown-whatsapp-video-calls

Protecting Critical Infrastructures: IT/OT Convergence vs MITM Attacks

This blog has elaborated on the risks of the convergence of IT and OT systems, how Man-in-the-Middle (MITM) attacks are involved, and provided security best practices to mitigate them. We also highlight the importance of adopting a secure architecture to protect against cyber security threats and the need for security measures for IoT devices. By incorporating these points into daily practice, users can gain insights into the challenges and risks of IT/OT convergence and the actions that can be taken to mitigate these risks.

What is a Man-in-the-Middle (MITM) attack?

An attacker can use the MITM attack to intercept the communication between two devices, and gain control to perform malicious actions such as reading and writing data, or even execute commands. MITM attacks can be carried out through various methods, such as ARP spoofing, DNS spoofing, SSL stripping, etc.

IT/OT convergence

IT and OT systems aim to have different priorities for security considerations. While security on IT systems focuses on protecting user data, OT systems primarily emphasise system availability, physical safety during operations, and the completeness of data. Since most OT systems have longer lifecycles than IT systems, this may result in some legacy OT systems still running in factories. As OT systems are usually located in an isolated network environment, security has yet to be fully considered during the network design phase, resulting in a lack of protective measures and cyber defense.

A Cyber Security Case Study on IT/OT Convergence

Previously, HKCERT collaborated with Dr. LUO Xiapu, Professor of the Department of Computing at The Hong Kong Polytechnic University and his undergraduate student, Mr. TANG Ho Tim, to conduct a cyber security case study on standard Programmable Logic Controllers (PLCs) to raise public awareness of the importance of strengthening IoT security in critical infrastructures, explicitly focusing on MITM attacks.

Testing Target and Expected Outcomes
The test involved developing a light traffic system to create a testing environment. The simulated MITM attack aimed to show how attackers can intercept and change communication between the PLC and its components, potentially leading to unauthorised access and compromise of the system.

Testing Target

The test focused on the web server of the PLC system rather than the PLC itself, assuming that the web server features were enabled as the default.

Expected Outcomes

It was predicted that the test would identify security flaws like buffer overflows or command injection that could let an attacker run malicious code on the target machine to carry out an MITM attack.

Testing Environment and Equipment

The test was to simulate the scenario of using a PLC and remote controlling it through a web-based network environment. The devices used in the testing environment include:

Pre-setup Environment

- A powered-on PLC setup connected with traffic light bulbs and a network switch
- Setup PLC with web management feature and the settings remain with factory default

Hacker

- Laptop connecting with the network switch (Same network environment with PLC)
- The laptop has been installed and is running Windows 11 operating system and Burp Proxy software

Assumption

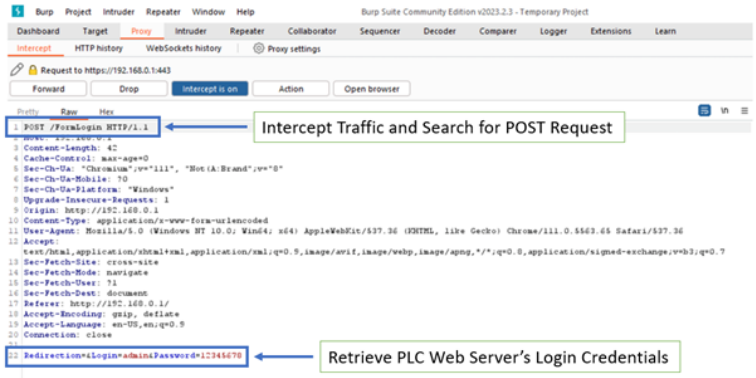
- The hacker hijacked and gained initial access to the internal network where the PLC was placed.

Testing Method and Steps to Simulate a MITM Attack

A simulation of a hacker launching a MITM attack would be separated into two steps – Reconnaissance and Weaponisation, in the use of Burp Proxy software:

Reconnaissance – Sniffing and Analysis of Network Traffic

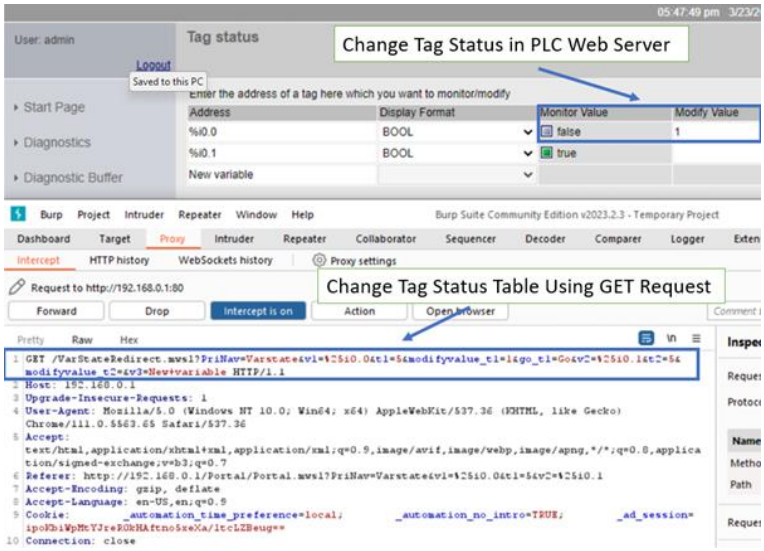
1. To prepare for launching MITM attacks, The hacker would set up a proxy and lure the user to connect through it.
2. The hacker uses the Burp Proxy to intercept traffic between the user's browser and the web server. A POST request is sent to the web server when the user tries to log in again.



3. The hacker views the login credentials displayed in Burp Proxy, showing encryption between the browser and PLC before sending the login credentials.

Weaponisation – Modify the Sniffed Network Traffics and Send Back to PLC

1. The hacker could change the intercepted packets by dropping or sending them out. By using Burp Proxy, the hacker could copy the intercepted requests and manipulate its session cookie to obtain control of the PLC.
2. To take control of the PLC, the hacker would send some manipulated requests with CURL - a simple command line tool to send custom web requests. Some customised web requests were tested and changed the state of the PLC successfully as shown below:
    - The hacker could change the tag status table to watch or alter the operation of the PLC system by sending a GET request.



- The hacker could change uploaded files by changing the file name or content by sending a POST request, causing them to become unavailable or infect other facilities or devices.

- The hacker could remove files by sending a GET request to change the file name from one to another or performing a brute force with a dictionary attack.

After performing the MITM attack, the findings were significant. The above findings proved how the hacker could use Burp Proxy to gain access to sensitive information, change CPU operations, and upload malicious code to the device. This showed that the hacker can successfully perform a MITM attack using the Burp Proxy software in the scenario of IT/OT convergence.

Other Risks Found in the Study

The study found both successful and risky findings. On one side, the project performed a replay attack on a web server and a dictionary attack on web applications. However, the study also found several vulnerabilities in the test PLC that pose significant risks. These vulnerabilities include the ability of an attacker to use the Industrial Exploitation Framework (ISF) to perform a replay attack on the test PLC. Additionally, the study proved how an attacker could use an injector tool to perform a Denial of Service (DOS) attack on the PLC.

Security Best Practices for Mitigating Risks in IT/OT Convergence

Organisations should take a proactive approach to cyber security to mitigate the risks associated with IT/OT convergence, explicitly focusing on mitigating Man-in-the-Middle (MITM) attacks. The following are some best practices that organisations should consider:

1. Conduct regular network and security assessments to find potential vulnerabilities and risks;
2. Develop a risk assessment report finding the risks associated with MITM attacks in their IT/OT convergence environment;
3. Formulate a strict implementation plan that addresses and prevents the identified security risks and vulnerabilities in the first place, such as implementing secure communication protocols, encryption, and strong authentication and access control measures;
4. Update operational policies to reflect new security measures and best practices for detecting and preventing possible attacks;
5. Adopt a secure architecture, such as the Purdue Reference Model or the "Zero Trust" architecture, with clear boundaries and strict access controls to prevent unauthorised access and limit the attack surface;
6. Use intrusion detection and prevention systems to watch network traffic and detect and prevent potential MITM attacks before they cause harm to IT/OT convergence systems:
7. Perform patch management to ensure that IT/OT convergence systems are regularly patched and updated to address known vulnerabilities;
8. Refer to HKCERT’s "IoT Security Best Practice Guidelines" to adopt security best practices in the use of IoT devices, and formulate the incident response plan in their environment by referring to HKCERT’s "Incident Response Guideline for SMEs".

Conclusion

Before converging IT and OT systems, sufficient preparations are required to reduce the risks. The lack of technical professionals with complete understanding of all the systems can make the convergence of IT and OT systems challenging. Therefore it is necessary to update the company's security, operation, and maintenance policies after the convergence.

It is important to note that the study focused on the web server of the PLC system rather than the PLC itself, assuming that the web management features are enabled as the default. Overall, this case study serves as a reminder of the importance of securing IT/OT convergence systems against potential cybersecurity incidents, particularly those related to MITM attacks.

For more details, please refer to:
https://www.hkcert.org/blog/protecting-critical-infrastructures-it-ot-convergence-vs-mitm-attacks

-End-

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