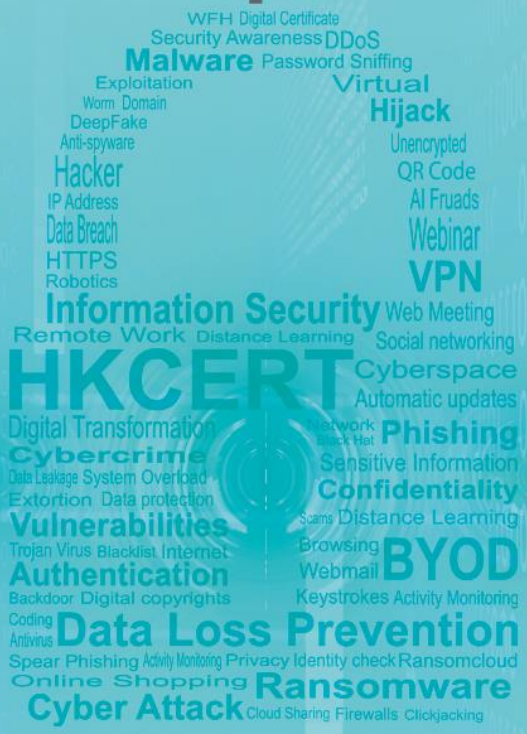
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report 2023 Q2

Release Date: Aug 2023



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 sanitising 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	2023-07

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

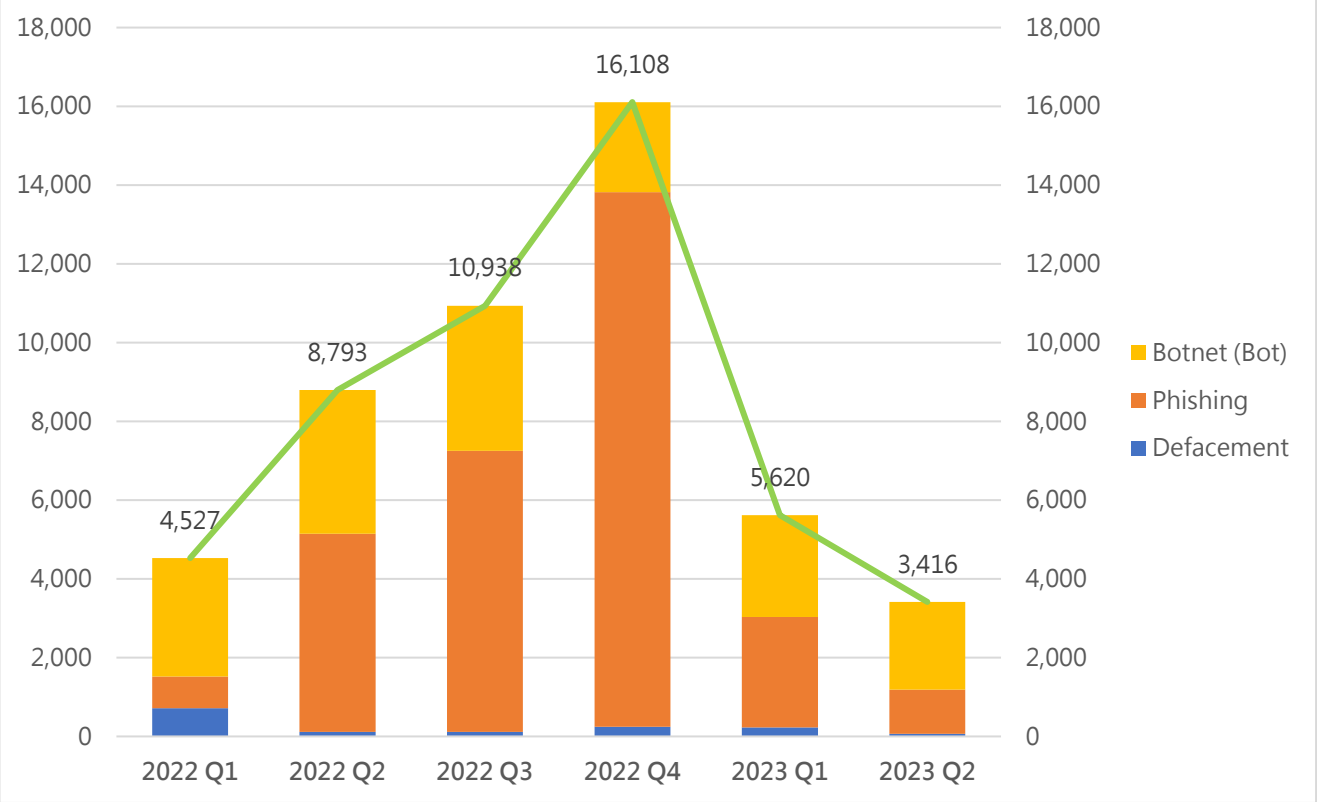
Highlights of the 2023 Q2 Report

Unique security events related to Hong Kong

3,416

Quarter-to-quarter

39.2%↓

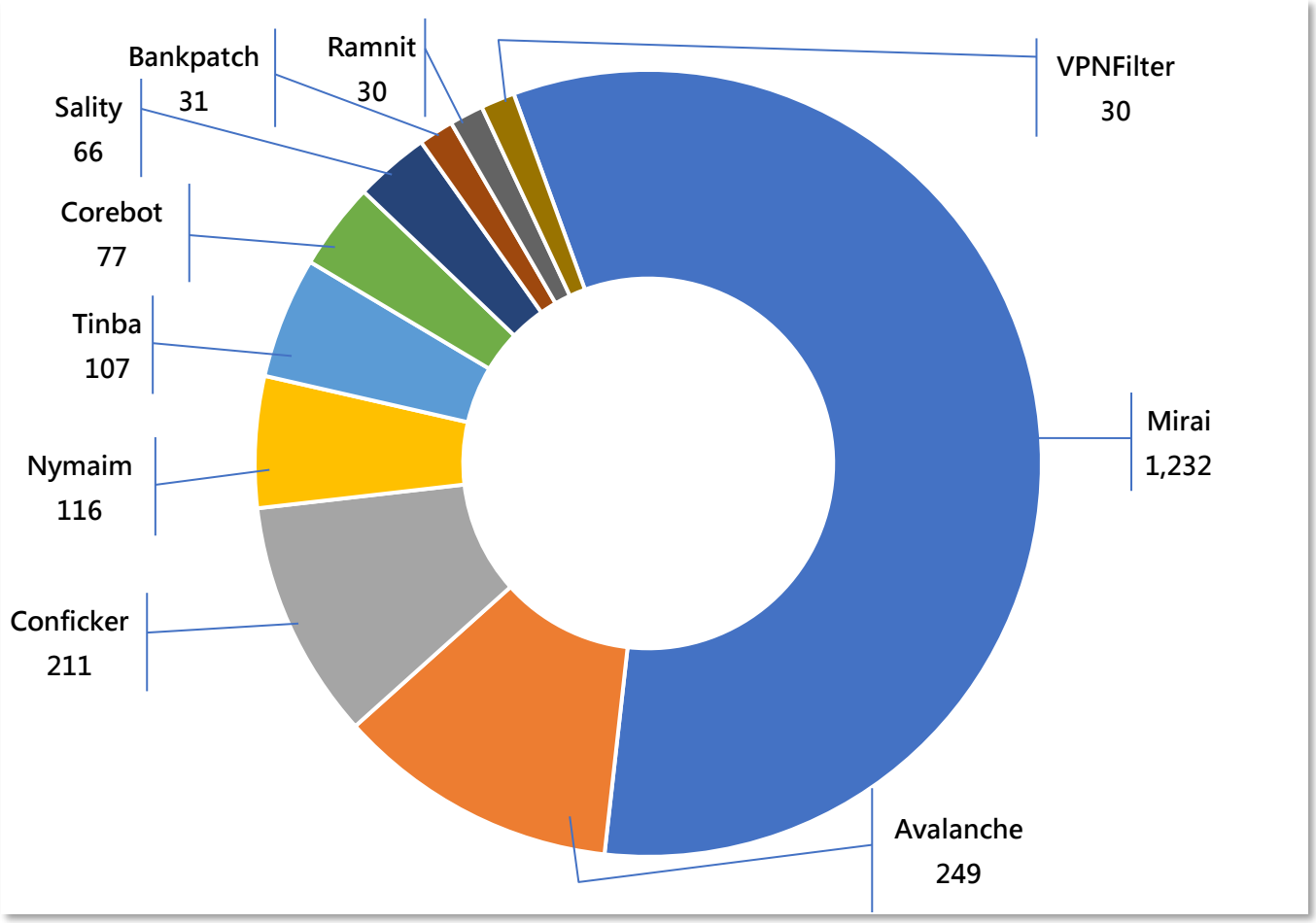


Event Type	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	quarter-to-quarter
Defacement	118	113	249	233	69	-70.4%
Phishing	5,033	7,141	13,574	2,804	1,120	-60.1%
Botnet (Bots)	3,642	3,684	2,285	2,583	2,227	-13.8%
Total	8,793	10,938	16,108	5,620	3,416	-39.2%

Major Botnet families in Hong Kong network

Mirai	1232 ↑ 53.8%
Avalanche	249 ↓ 61.4%

Conficker	211	+9.9%
Nymaim	116	-54.5%
Tinba	107	+114%
Corebot	77	-74.5%
Sality	66	+32%
Bankpatch	31	+47.6%
Ramnit	30	+500%
VPNFilter	30	-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 Attacks Decline for Two Consecutive Quarters! The Public is Still Advised to Remain Vigilant and Guard Against Deception!

The figures for the second quarter of 2023 regarding cyber incidents have been released. This quarter, phishing attacks have decreased by 60.1% compared to the previous quarter and by 77.7% compared to the same period last year. However, it is worth noting that the number only reflects the systems involved in phishing activities that are hosted in Hong Kong. In other words, hackers can set up phishing sites on overseas infrastructure systems and target users in Hong Kong. In addition, HKCERT has observed that there have been recent cases where criminals have used social media platforms such as WhatsApp, Facebook, LinkedIn and Instagram for fraudulent activities, aiming to deceive users and obtain their assets and personal information.

To protect the public from phishing attacks and safeguard their interests, HKCERT has provided some cyber security advice:

1. **Avoid clicking on suspicious links:** Do not click on links from unknown sources or suspicious emails, social media messages, text messages, or pop-ups. Before clicking on a link, carefully inspect it to ensure its legitimacy.

2. **Enhance password security:** Use strong passwords, change them regularly, and avoid using the same password on insecure websites. Use two-factor authentication (2FA) to enhance account security.

3. **Update and protect devices and software:** Regularly update operating systems, applications, and security software to ensure they have the latest security patches and protections.

4. **Handle personal information with caution:** Do not enter personal sensitive information on untrusted websites. When providing personal information, understand the purpose of the data being submitted.

5. **Respond to suspected phishing attacks:** If you suspect that an email or link is a phishing attack, do not click on the link or provide any personal or sensitive information. Report the email or link to relevant organisations or institutions to assist them in taking appropriate actions.

These recommendations can help the public stay vigilant and reduce the risk of falling victim to phishing attacks. Maintaining a strong sense of information security awareness and adopting good cyber security practises are key to online safety.

Image Source: 癲噹 DinDong Facebook Page
https://www.facebook.com/100044634960219/posts/pfbid02WBrHHP6DDJPYwtn9eUzghTbrGjsrrWZJckG5knNk8ondudzNBrWj4cYcF7KeVbX2l/?mibextid=cr9u03

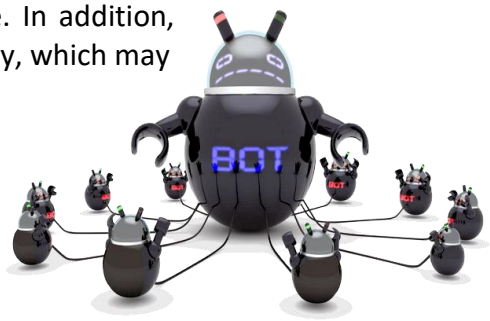
Mirai Botnets Experienced a Sharp Increase of 53.8%! Expert Analysis of the Possible Reasons Behind

Mirai is malicious software whose main function is to infect Internet of Things (IoT) devices, such as cameras, routers, and cars, and turn them into zombie devices or botnets that can be used to launch large-scale Distributed Denial-of-Service (DDoS) attacks. Mirai was first discovered in 2016, when major incidents included its targeting of Dyn, a domain name system service provider, which resulted in many large websites becoming inaccessible.

Reasons for the rise in Mirai attacks

The increase in Mirai cases may be related to the widespread use of IoT devices and a lack of security awareness, such as IP cameras installed in homes. Many IoT devices have low security, with issues such as weak default passwords and outdated software, making them easy targets for zombie network attacks. In addition, most IoT device users are not aware of their vulnerabilities and do not know how to protect their devices, making them easy to infect and use for attacks.

Another possible reason is that the source code for Mirai has been made public, allowing anyone to use it to create their own botnets and further expand its threat range. In addition, zombie network attacks have become a huge and profitable black industry, which may also encourage more criminals to use Mirai for attacks.

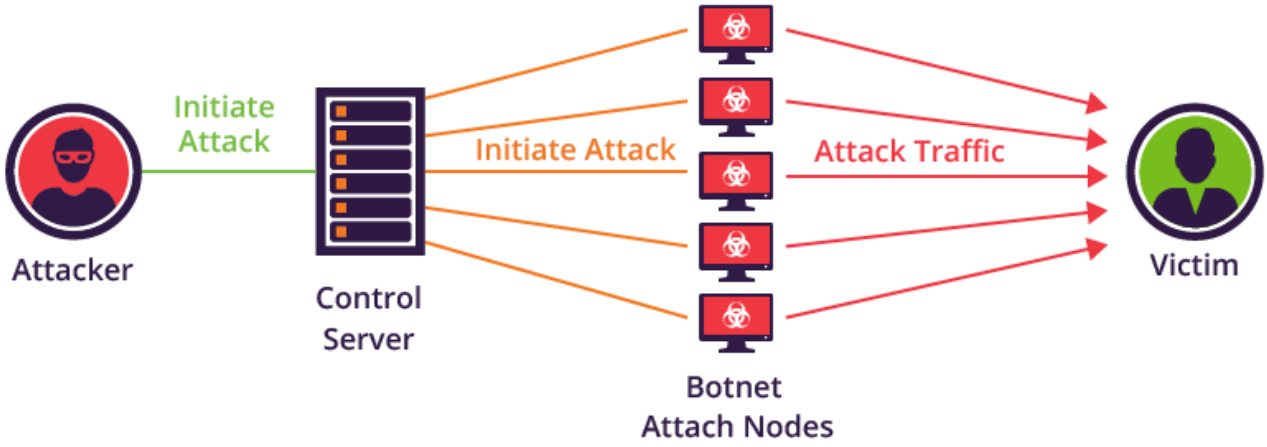


In addition to the widespread use of IoT devices and lack of security awareness, there are other reasons for the increase in Mirai attacks. For example, Mirai variants have begun to be used, such as IZ1H9, Satori, Miori, PureMasuta, IoTrooper, and Reaper.

How Mirai attacks work

When Mirai infects a device, it uses a predefined set of attack instructions, such as HTTP requests and TCP SYN flood attacks, to launch DDoS attacks. These attack instructions send a large number of requests to the target website or service, causing it to malfunction and stop service. Since Mirai can infect a large number of IoT devices, it can launch very large-scale attacks, causing serious damage to Internet infrastructure.

The way Mirai infects devices is usually through unpatched vulnerabilities or weak passwords for remote access, and then it installs malware on the device. Once infected, Mirai establishes a connection with the command-and-control (C&C) centre to receive attack instructions and execute attacks. The control centre can use anonymous networks, such as Tor, to make it harder to track or shut down. In addition, email attachments are also one of the ways of infection.



Recent network incidents related to Mirai

In mid-April of this year, according to the Palo Alto Networks threat research team Unit 42, a Mirai malware variant called IZ1H9 was found to be infecting Linux IoT devices and creating a large botnet for malicious activity. The malware first checked the target IP to avoid attacking Government networks, internet service providers, and larger tech companies to hide its location. In addition, another feature of IZ1H9 is that if the target device has become part of the botnet, it will terminate the device's running processes and start new ones.

In May of this year, the Mirai botnet was aggressively exploiting the CVE-2023-28771 vulnerability to launch large-scale attacks against Zyxel firewalls, allowing unauthenticated attackers to trigger remote code execution on the target system.

Security recommendations from HKCERT

To protect IoT devices from Mirai and other zombie network attacks, HKCERT recommends that users:

- **Use and regularly update complex passwords (such as mixing symbols, numbers, upper- and lower-case letters, and recommending a length of at least 12 characters)**
- **Update device software and firmware**
- **Restrict remote access to devices and take security measures such as closing unnecessary ports**
- **Conduct regular security checks**
- **Maintain network security awareness**

Education Activity: Campaign to promote anti-phishing messages in the community

“All-Out Anti-Phishing” Moving Showroom campaign just wrapped up its first season with great success!

HKCERT held the "'All-Out Anti-Phishing" promotion event from 26 June to 2 July, aimed at raising public awareness and prevention capabilities against phishing attacks, and strengthening the public's awareness of cyber security. The event also collaborated with local illustrator DinDong to promote anti-phishing messages through diverse means, helping more people understand the harm of phishing attacks and learn how to protect themselves and their families. The "All-Out Anti-Phishing Campaign" promotion vehicle covered multiple areas across Hong Kong during the event, including Wan Chai, Kwun Tong, and Tai Po, allowing citizens to learn about phishing techniques, harm, and prevention methods up close. At the same time, interactive games were set up on-site to make learning about cyber security more fun, and participants had the chance to win prizes.

Overall, the " All-Out Anti-Phishing Campaign" promotion event is an important activity aimed at improving the public's cyber security awareness and prevention capabilities, helping the public understand the harm of phishing attacks, and further strengthening their awareness of cyber security. The second season of the promotion vehicle campaign will be held soon, and details will be announced later on HKCERT's website and Facebook/LinkedIn pages.

"Smart City": HKCERT helps you gain insight into phishing with new games!

The fourth season of the "Smart City" roadshow organised by Office of the Government Chief Information Officer (OGCIO) has concluded successfully. HKCERT is honoured to once again be one of the participating organisations to introduce phishing and how to prevent it to the citizens. This time, HKCERT visited Yuen Long, Central, Tuen Mun, Chai Wan, and Tai Po to meet everyone! In addition to the popular "Phishing" game from the previous season, we also added a new game called "Insight into Phishing", hoping to use interesting and vivid ways to help more citizens understand that technology not only brings convenience to society but also has potential risks that citizen need to understand to avoid becoming hackers’ next target.

Security in the Digital Age: Protecting Your Connected world

The Internet of Things (IoT) refers to an interconnected system that includes physical devices, vehicles, buildings, and other objects embedded with sensors, software, and network connectivity, allowing them to collect and exchange data. The goal of IoT is to create a more efficient and connected world where devices and systems can communicate with each other, automate tasks, and improve overall performance. Examples of IoT devices include webcams, smart thermostats, wearable fitness trackers, and connected appliances like refrigerators and washing machines.

Any example of the IoT?

One popular application of IoT devices is Unmanned Aerial Vehicles (UAVs), also known as drones, in which the aircraft can be controlled to fly without a human pilot on board. They can be controlled by a computer or a remote controller. Drones have been widely used in various fields such as military weapons, cargo transportation, or search and rescue missions. The market for this field is enormous, attracting Government and commercial industries to invest in drone development. As a result, some commercial industries have started exploring the drone market, shifting from professional to economic markets, providing the public with low-cost drones. As the use of drones becomes more widespread, hackers can exploit them to carry out malicious activities, posing potential risks to public safety and privacy.

HKCERT has set IoT targeted attack as one of the top five information security risks for 2023. Previously, HKCERT collaborated with Dr LUO Xiapu, Associate Professor of the Department of Computing at The Hong Kong Polytechnic University and his undergraduate student, Mr SHAM Wing Chung, to conduct a cyber security study on drones to raise public awareness of drone and IoT security.

Application of Consumer Drones

Consumer drones have two types, namely simple "aircraft" and "aerial photography drone" equipped with a camera. They are usually remotely controlled via a remote controller and computer program and have different uses, shapes, and sizes, such as recording, assisting in search and rescue operations, scientific research, and agricultural monitoring, etc. Due to technological advances and cost reductions, they have become increasingly popular in recent years, and can be played by both adults and children. Additionally, hackers could potentially take control of the drone and use it to launch physical attacks, such as dropping a payload or ramming the drone into a target. This may affect people or property, causing serious injury. Therefore, this kind of equipment is used for further research.

Security Risks

Hacking methods generally target system vulnerabilities, users' personal credentials and encryption methods. Drones are controlled by commands sent by the controllers to the aircrafts, which receive and execute the commands and return system status and images to the controllers. Both are independent systems that operate through established network communication protocols and command operations. To hijack a drone, attackers can focus on several aspects, such as:

- Injecting malicious software into the controller or aircraft, or
- Intruding the aircraft through network communication

As the network communication methods of most IoT devices are similar (such as Wi-Fi and Bluetooth), this study will focus on this point to explore potential security risks that other IoT devices using similar connectivity methods may encounter.

Testing Target and Expected Results

Most drones on the market use Wi-Fi as their communication method. Wi-Fi de-authentication attack is a wireless network attack targeting communication between client devices and access points in a Wi-Fi network. The attack includes sending a de-authentication request to the access point, causing the client to disconnect from the network. This can be performed by hackers who have the necessary tools to send de-authentication frames within the Wi-Fi network range. This attack can be used to disrupt the normal operation of a Wi-Fi network, forcing clients to reconnect to the network while potentially revealing sensitive information such as login credentials or launching other types of attacks.

Target: To interrupt the user's device connects to the drone through Wi-Fi de-authentication.
Expected results: Control the drone movement and view the real-time image at the time.

Testing Method

Simulate a scenario where a normal user is using a drone, and another researcher playing the role as a hacker nearby, attempting to take control of the drone remotely.

Testing Environment and Equipment

The test was conducted in a typical indoor setting, and the equipment used was kept in the original factory setting. The devices used were:

User

- Drone (Education edition)
- Android smartphone with drone control software installed

Hacker

- Laptop with two network interface cards, running Windows 11 and Kali Linux (VirtualBox) operating systems

Testing Methods and Steps

User

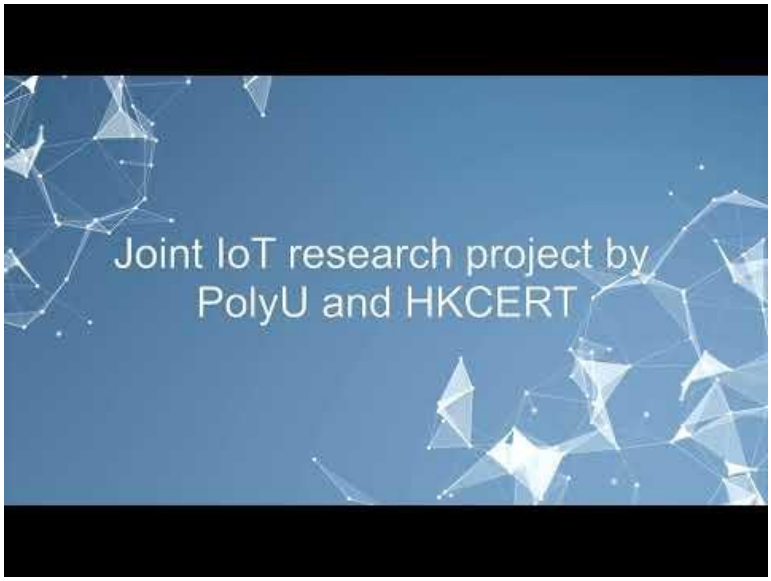
1. Start the drone
2. Use a smartphone to control drone flight and video recording

Hacker

1. Use the network scanning tool to scan all wireless networks in the field to obtain the MAC address of the drone
2. Execute Wi-Fi de-authentication commands to disconnect the user device from the drone
3. Connect the drone with a specific program
4. Fully control the drone and captured images

After testing, it only takes about 30 seconds for hackers to complete the attack and gain full control of the drone, including shutting down the drone engine. For detailed test clips, please refer to the following video.

Video Demo



Security Advice

Use complex passwords (such as a combination of symbols, numbers, upper- and lower-case letters, and recommending length of at least 12 characters), and set up two-factor authentication/multi-factor authentication as the user authentication method whenever possible. This will help prevent unauthorised access to user's drone control system. The study also attempted to successfully Brute Force short passwords within one minute, so complex passwords can reduce the chance of intrusion. In addition, it is recommended to change the SSID of the drone or other IoT devices before using it, as hackers can infer the brand and model of the product through the default SSID.

Other Suggestions

For personal users:

1. Keep the firmware of the drone up to date
   Regularly update the firmware of the drone to patch known vulnerabilities and ensure that the software of the drone is up to date.

2. Disable unnecessary features
   Reduce the attack surface, through which hackers could break into the system.

For manufacturers:

1. Encrypt the data of the drone
   Use encryption to protect the data transmitted between the drone and its control system. This will help prevent data theft or interception.

2. Set up two-factor authentication/multi-factor authentication as the user authentication method
   This will help prevent unauthorised access to your drone control system.

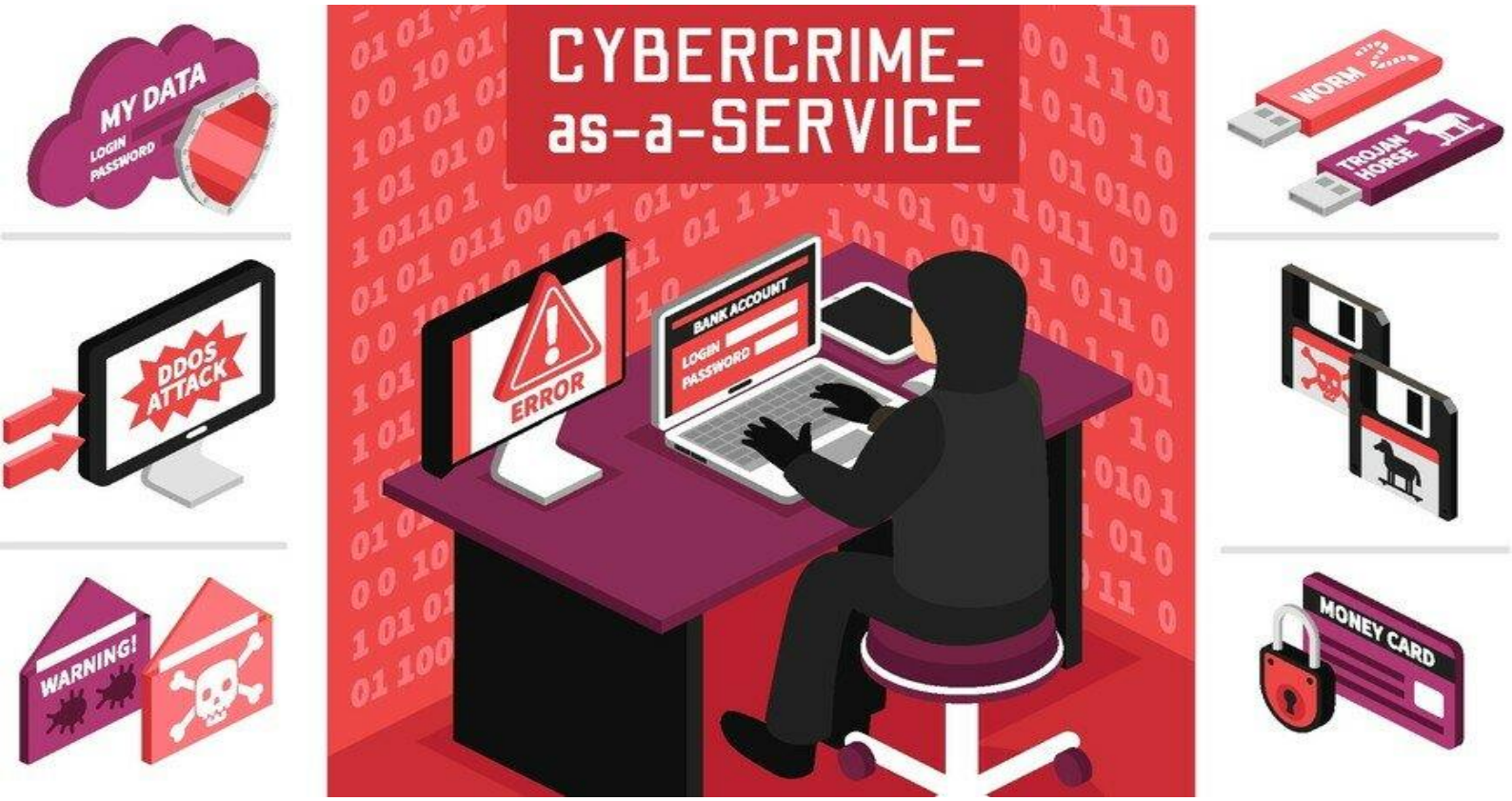
Conclusion

The rapid development of IoT nowadays brings convenience to users' lives, but it also lays hidden dangers to network security. Security issues of IoT devices may lead to malicious attacks, data leaks, privacy violations, and more. Therefore, ensuring the security of IoT devices is of paramount importance. To ensure the security of IoT devices, a series of measures need to be taken. First, it is necessary to use IoT devices with better security performance, and these devices must have complete security protection measures. Second, IoT devices require regular updates and maintenance to ensure their systems and software are up to date to avoid known security vulnerabilities. In addition, encryption is required to protect the communication of IoT devices to prevent data from being stolen or tampered with.

Finally, users should also pay attention to the protection of their privacy and security. Users should protect IoT devices with strong passwords, avoid using public wireless networks to connect IoT devices, and regularly check that IoT devices are working properly. To this end, HKCERT has released the *IoT Security Best Practice Guidelines* in 2020 to cover network security issues when using IoT devices. You may refer to the Guidelines as a reference.

For more details, please refer to:
https://www.hkcert.org/blog/iot-security-in-the-digital-age-protecting-your-connected-world

Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience



In today's digital age, we have come to rely on the Internet to provide us with unparalleled convenience, access to a wealth of information, and endless services at our fingertips. Unfortunately, not everyone uses the Internet for good and some even sell cybercriminal services online. HKCERT has set Cybercrime-as-a-Service (CaaS) as one of the top five information security risks for 2023. In this blog post, we will dive into the dark underbelly of the online world and explore what CaaS is, its business models, and how it has come to be. We will also provide examples of CaaS and discuss how you can protect yourself from falling victim to these nefarious schemes.

What is Cybercrime-as-a-Service (CaaS)?

CaaS refers to the trend where individuals or groups with malicious intent provide cybercriminal tools, infrastructure, and services to other criminals for a fee. In essence, CaaS has enabled even those with limited technical expertise to engage in sophisticated cyber attacks and other illicit online activities. This has led to the rapid growth and evolution of cybercrime, as it becomes increasingly accessible and profitable for aspiring criminals.

The Business Model of Cybercrime-as-a-Service

CaaS operates much like any other legitimate business, offering various products and services to a diverse clientele. The main difference, however, is that the customers of CaaS are other criminals, and the services provided are all designed to aid in the commission of cybercrimes. Some common offerings in the CaaS marketplace include:

- **Malware-as-a-Service:**
  This involves the development, distribution, and support of malicious software, such as ransomware, spyware, or Trojans, which can be used to infect devices and systems, steal sensitive data, or hold data hostage.
- **Exploit-as-a-Service:**
  Cybercriminals provide access to previously unknown security vulnerabilities (also known as zero-day exploits) or automated tools that can be used to exploit known vulnerabilities in software or systems.
- **Infrastructure-as-a-Service:**
  This service provides access to a network of compromised computers or servers (also known as botnets), which can be used to launch distributed denial-of-service (DDoS) attacks, send spam, or host malicious content.
- **Hacking-as-a-Service:**
  In this offering, skilled hackers are hired to breach targeted systems or networks, steal data, or sabotage systems on behalf of their clients.

Why Does Cybercrime-as-a-Service Arise?

The emergence of CaaS can be attributed to several factors. First and foremost, the rapid growth and widespread adoption of the Internet have provided fertile ground for cybercriminals to operate. The anonymity of the online world allows them to hide their identities and evade law enforcement, while the global reach of the Internet enables them to target victims anywhere in the world.

Secondly, the increasing complexity of technology and the expansion of the cyber security skills gap have created a demand for specialised cybercriminal services. As organisations invest in advanced security measures, traditional cybercriminals often find it difficult to keep up with the latest defences. This has given rise to a market for specialised services that can help them bypass these defences and achieve their nefarious goals.

Finally, the lucrative nature of cybercrime, coupled with the anonymity of the dark market, has attracted a growing number of individuals and groups to engage in these illegal activities. The CaaS model allows them to maximise their profits by monetising their skills and resources, while also making it easier for others to join the ranks of cybercriminals due to the lowered cost (e.g. skillset and infrastructure).

Examples of Cybercrime-as-a-Service in Detail

To better understand the threat posed by Cybercrime-as-a-Service, let's examine a few real-world examples:

- Ransomware-as-a-Service (RaaS): One of the most notorious examples of CaaS is the Ransomware-as-a-Service model. In this scheme, cybercriminals develop and distribute ransomware, which encrypts a victim's data and demands a ransom for its release.

  RaaS providers typically offer user-friendly platforms that allow aspiring criminals to customise the ransomware, set their ransom amounts, and manage their campaigns. Examples of RaaS platforms include GandCrab, REvil, and Cerber.

- DDoS-for-Hire Services: Distributed denial-of-service (DDoS) attacks are a common form of cyber attack that overwhelms targeted websites or networks by flooding them with an excessive amount of traffic.

  DDoS-for-Hire services provide access to botnets, which can be used to launch these attacks on demand. One such service, known as LizardStresser, was operated by the infamous Lizard Squad hacking group and was responsible for numerous high-profile attacks on gaming services and websites.

- Phishing-as-a-Service (PhaaS): Cybercriminals offer a user-friendly interface for even non-technical individuals to create and manage phishing campaigns. These services typically provide pre-built phishing templates, hosting services for the phishing sites, and tools to collect victims' data. Examples of PhaaS platforms include BulletProofLink, EvilProxy and etc

- Dark Web Marketplaces: The dark web is a part of the Internet that is not indexed by traditional search engines and requires special software to access. It is home to numerous marketplaces where cybercriminals can buy and sell various CaaS offerings, such as malware, exploits, or stolen data.

  One of the most well-known dark web marketplaces was the Silk Road (shutdown). Transactions are conducted with cryptocurrency. Although primarily known for drug trafficking, it also facilitated the trade of illegal digital goods and services.

Protecting Yourself from CaaS

As CaaS continues to grow and evolve, it is crucial for individuals and organisations to take proactive steps to protect themselves from these threats. Some recommendations for safeguarding your digital assets include:

- Do not engage in any cybercrimes. Do not access to dark web and its marketplace.
- Keep your software and systems up to date to minimise the risk of known vulnerabilities being exploited.
- Use strong, unique passwords for all your accounts and enable multi-factor authentication whenever possible.
- Regularly back up your data to ensure you can recover from a ransomware attack or other data loss incidents.
- Be cautious of phishing emails and avoid clicking on suspicious links or downloading unexpected attachments.
- Invest in comprehensive cyber security solutions, such as antivirus software, firewalls, and intrusion detection systems.

By staying informed about the latest cyber security threats from HKCERT and following best practices for securing your digital environment, you can significantly reduce the risk of falling victim to CaaS and help create a safer Internet for everyone.

For more details, please refer to:
https://www.hkcert.org/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience

-Ends-

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