



CYBER SECURITY NEWSLETTER

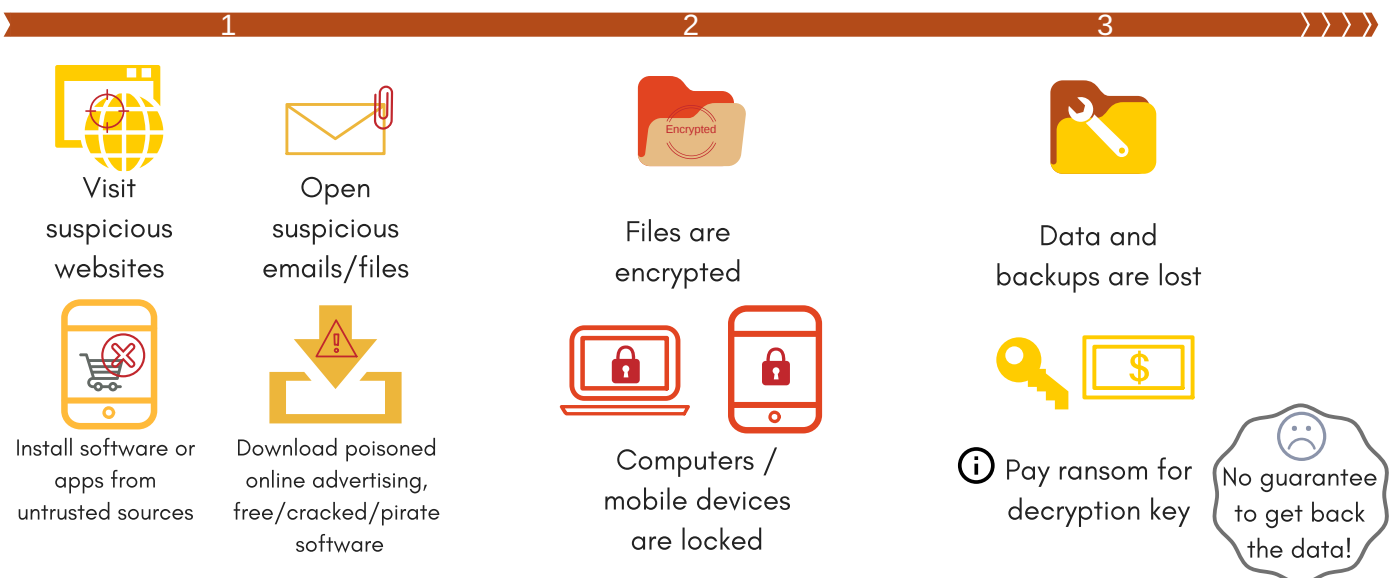


Feature Article

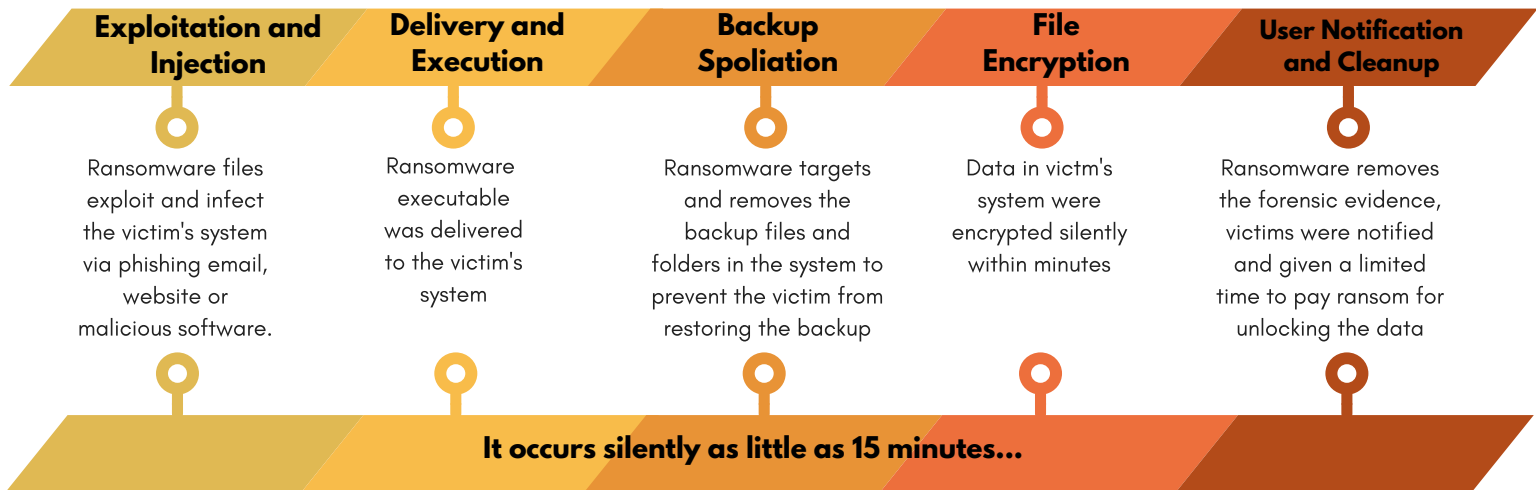
What is Ransomware?

A malware that kidnaps data on your computer or mobile device, and demands for a ransom payment to decrypt or unlock them.






How Ransomware works?



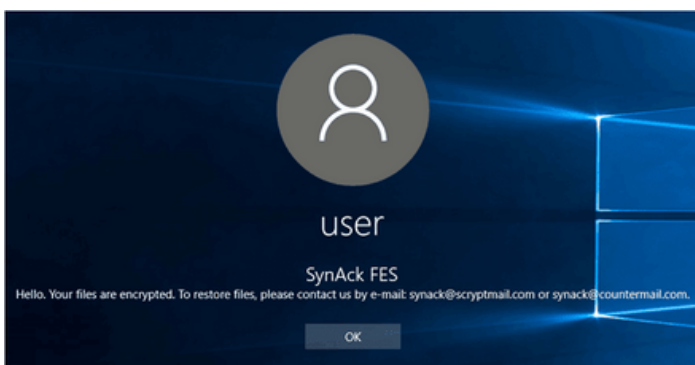
Ransomware Attack Timeline



What to do if infected?

-  **1 Disconnect Network**
Disconnect the infected computer/device from any network connections (wired, Wifi or Bluetooth).
-  **2 Unplug Storage**
Unplug any portable storage devices (USB and external hard drives).
-  **3 Determine Scope**
Check all accessible storage for any signs of encrypted files and the available backups. Copy any unencrypted files to separate clean storage immediately.
-  **4 Record Strain**
Use anti-virus to determine and record the strain of Ransomware for searching of recovery tools.
-  **5 Restore Backup**
Restore the most recent unencrypted backup to a separate "clean" computer / storage.
-  **6 Rebuild and Clean**
If possible, complete rebuild the whole computer / device from clean installation. Otherwise, use multiple anti-virus to scan and clean the Ransomware.

New style ransomware uses Process Doppelgänger Technique



Security researchers are reporting that a new and improved version of the SynAck ransomware, now uses the Process Doppelgänger technique.

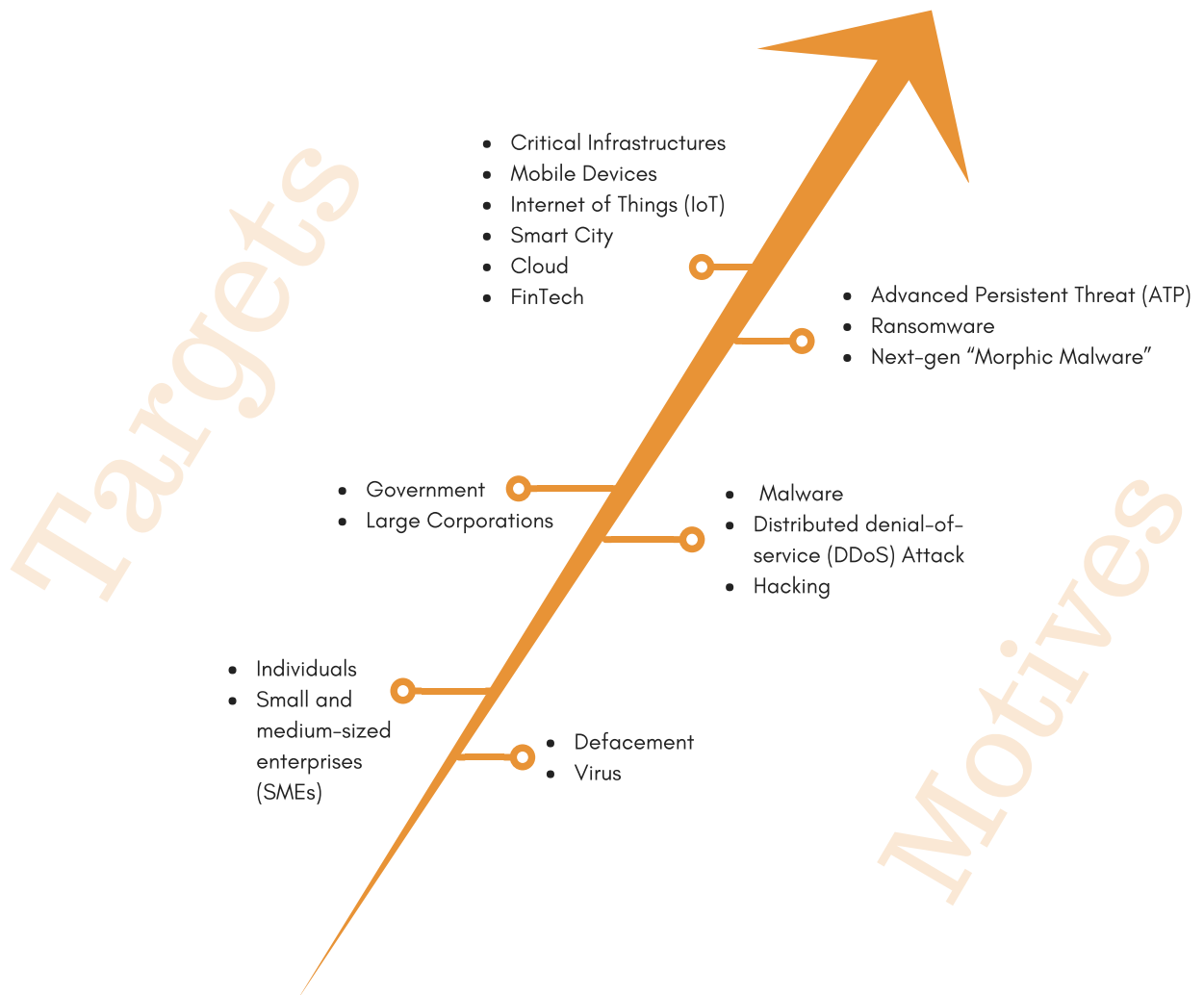
Process Doppelgänger is a code injection technique that abuses the Windows mechanism of NTFS transactions to create and hide malicious processes, in an attempt to avoid detection by antivirus software.

The technique is relatively new, being first presented at a security conference in December last year, but a few malware strains have already adopted it in their arsenal.

Finally, using the anti-malware software could protect your computer from SynAck and other ransoms.

Security Trend

Cyber Attack Trend



Cybercriminals are organized, well funded, and highly motivated. They are deploying advanced malware, leveraging cloud-based computing resources, and developing cutting edge tools based on AI and machine learning to not only circumvent advanced security defenses, but to also widen the scope and scale of their attacks. There are still wide-open, greenfield opportunities for enterprising criminals that are being driven by such things as cloud computing and IoT that are just waiting for the right tools to be compromised.

As a result, over the next couple of years, the Society will see the attack surface expand through the use of automation and tools that are able to make autonomous or semiautonomous decisions. The challenge is that we are at a very delicate moment in our transformation to a digital society and economy. Once we arrive at the singularity - when AI takes on a life of its own without human interaction - massive disruptions caused by autonomous malware could have devastating implications and permanently reshape our future.

Source:
Hong Kong Police Force
Fortiguard 2018

Tips and Tricks

How to Backup Your Smartphone?

You may be an iOS user or an Android user. Manufacturers provide a complete backup function, but busy Hongkongese, the backup will be forgotten. Unfortunately, if an accident on the smartphone, precious photos and videos are lost.

For this, today we introduce a tool that we hope will help you quickly and easily on backup your photos and videos.



SanDisk Ultra Dual Drive M3



Available from the Google Play store, the "SanDisk Memory Zone" app lets you view, access, and backup all the files from your phone's memory in one location.



SanDisk Connect Wireless Stick



Automatically backup photos and videos, set the app to automatically copy photos and videos from your camera roll to the drive when the drive is connected.

Be aware of using a USB stick, please make a USB encryption on the USB before use.

HSMC Threat Index

NSS reports the number of different threats at HSMC in April, 2018



BLOCKED WEBSITES BY CATEGORY

Malicious Websites
51,447 hits

Phishing
3,781 hits

DISCOVER, BLOCKED & CLEANED VIRUS / MALWARE

26 / 1500
PC

3 / 243
Server



PUA:WIN32/CANDYOPEN HACKTOOL:WIN32/KEYGEN
PUA:WIN32/ADVPCTWEAK TROJAN:WIN32/BITREP.A
TROJAN:VBS/MOVANIDE.A TROJAN:WIN32/OCCAMY.C
TROJAN:WIN32/SKEEYAH.A|BIT TROJAN:WIN32/VIGORF.A
HACKTOOL:WIN32/GENDOWS

ATTACK BY LOCATION

18,599 hits
China

News

Read more? Click the news headline

- [Close to 50,000 Minecraft accounts were infected with malware designed to reformat hard-drives and more](#)
- ["iTunes Wi-Fi Sync" feature could let attackers hijack your iPhone, iPad remotely](#)
- [Positive Technologies research: "Banking and Finance System were the most vulnerable web applications in 2017"](#)
- [Cybercriminals hijack router DNS to distribute Android banking trojan](#)
- [Twitter urges all users to change passwords](#)