UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

10 Q&A Cybercrimes and cyberattacks

Q&A

What is a cyberattack/cybercrime?

A cyberattack is an attack performed by a threat actor against an individual, network or organization's electronic device using digital techniques and tactics. They may include attempts to access data without permission, to disable shutdown services and/or access a website or network. According to UNODC, "the increased digitalization of society, compounded by the COVID-19 outbreak, has contributed to a recent 600% rise in cybercrimes in Southeast Asia."[1]

What is malware?

Malware is short for "malicious software." It is a term used to describe any software that has a malicious intention such as computer viruses, Trojans, adware, spyware, and ransomware.

What is ransomware?

Ransomware is a type of malware that encrypts a victim's data once it is infected. Then the threat actor, who controls the malware, asks for money in exchange for unlocking the victim's files. According to United Nations Office on Drugs and Crime (UNODC), in September 2021, a Malaysian web-hosting service was the target of a ransomware attack demanding US$900,000 in cryptocurrency. In May 2021, four subsidiaries of an international insurance company in Thailand, Malaysia, Hong Kong, and the Philippines were hit by a ransomware attack asking for US$20 million. Similar attacks also took place in September 2020 in Thailand, where computer systems and data of several hospitals, companies and organizations were encrypted and blocked.[2]

What is Distributed Denial of Service (DDoS)?

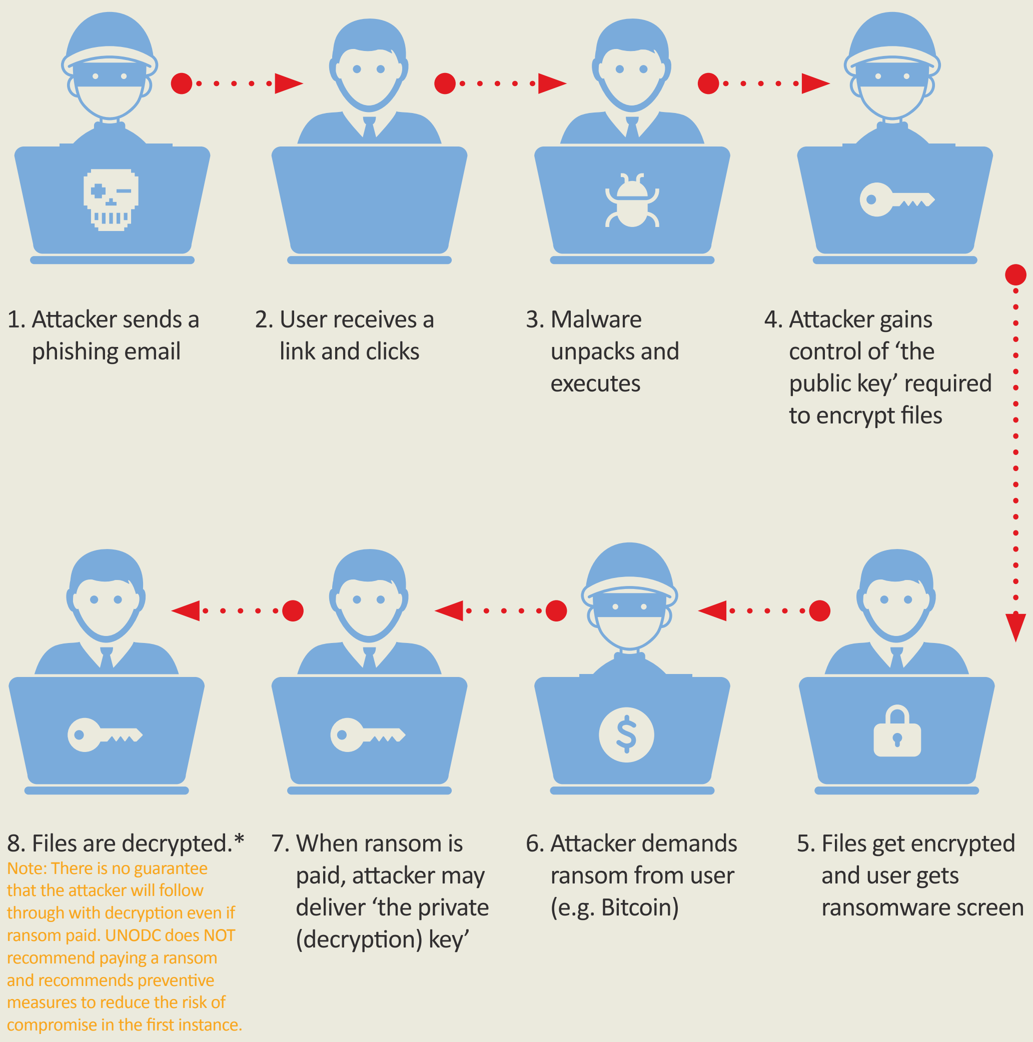
DDoS is a form of cyberattack that sends hundreds or thousands of requests to a target computer or website to disrupt its services, flooding it with requests and overwhelming the system. Threat actors do this by controlling a network of bots: or computers may do this by using infected malware. The command is sent by a "command and control" server to which target it will visit and access all at the same time, continuously.

How to protect your website against DDoS attacks?

You can protect your websites against DDoS attacks with the help of DDoS mitigation services. Companies such as Deflect, Cloudflare and Akamai, to name a few, are companies that provide DDoS protection.

DDoS protection services sit between the Internet and your website and filter all "bad" traffic as they pass through its network, only allowing legitimate or "good" traffic. By this filtering, websites are still able to process legitimate requests and keep their services online.

Anatomy of a ransomware attack



1. Attacker sends a phishing email

2. User receives a link and clicks

3. Malware unpacks and executes

4. Attacker gains control of 'the public key' required to encrypt files

5. Files get encrypted and user gets ransomware screen

6. Attacker demands ransom from user (e.g. Bitcoin)

7. When ransom is paid, attacker may deliver 'the private (decryption) key'

8. Files are decrypted.*

Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

Figure 1 UNODC, https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html

Note: References to external entities and websites are only indicative and should not be considered an OHCHR's endorsement to such entities and websites and the services provided by them. These references are provided, without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. Under no circumstances shall OHCHR be liable for any loss, damage, liability or expense incurred or suffered that is claimed to have resulted from the use of these websites. The use of these websites is at the user's sole risk. The external websites are not under the control of OHCHR, and OHCHR is not responsible for their content or any link contained in these sites.

[1] https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html.
[2] https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html.