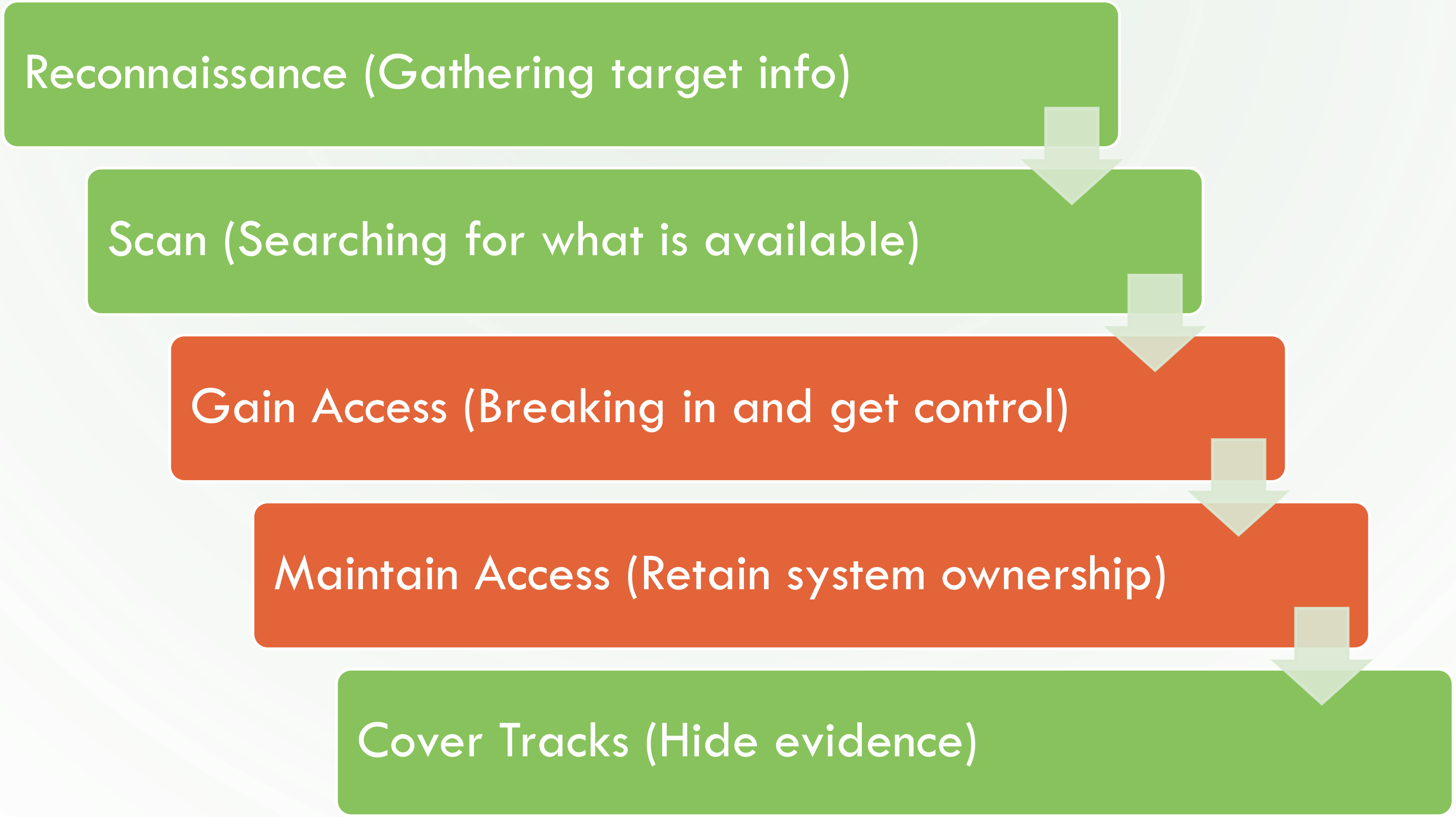
Ransomware

MODULE TOPICS

- What is Ransomware?
- Types of Ransomware
  - Locker Ransomware
  - Crypto Ransomware
  - Double Extortion Ransomware
- Ransomware as a Service (RaaS)
- Popular Ransomware Variants
- Notable Ransomware Victims
- Countermeasures

RECALL – PHASES OF HACKING



Reconnaissance (Gathering target info)

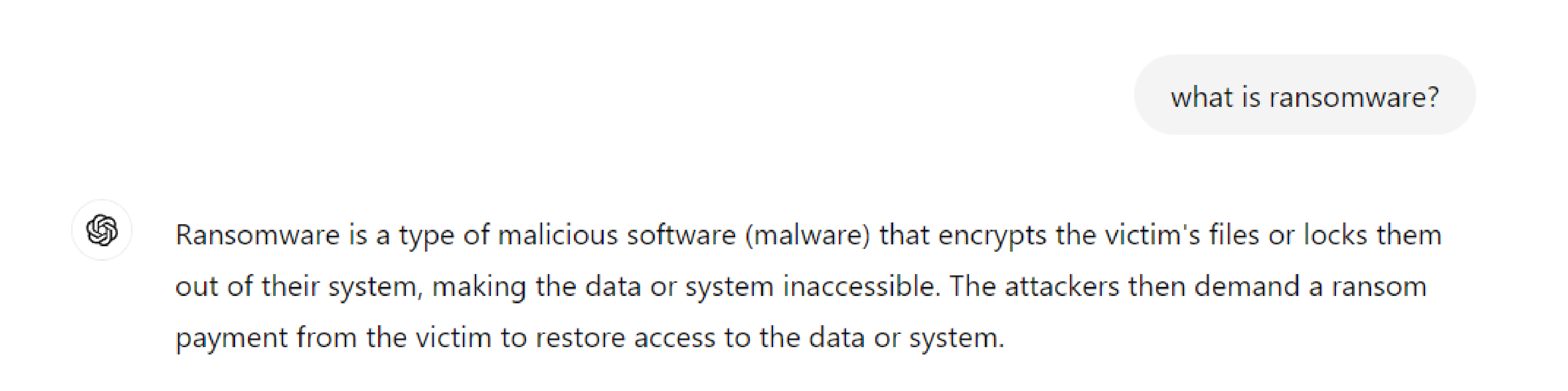
Scan (Searching for what is available)

Gain Access (Breaking in and get control)

Maintain Access (Retain system ownership)

Cover Tracks (Hide evidence)

WHAT IS RANSOMWARE?



what is ransomware?

Ransomware is a type of malicious software (malware) that encrypts the victim's files or locks them out of their system, making the data or system inaccessible. The attackers then demand a ransom payment from the victim to restore access to the data or system.

WHAT IS RANSOMWARE?

Ransomware is a type of malware attack that encrypts a victim’s data and prevents access until a ransom payment is made. Ransomware attackers often use social engineering techniques, such as phishing, to gain access to a victim’s environment. – Crowdstrike

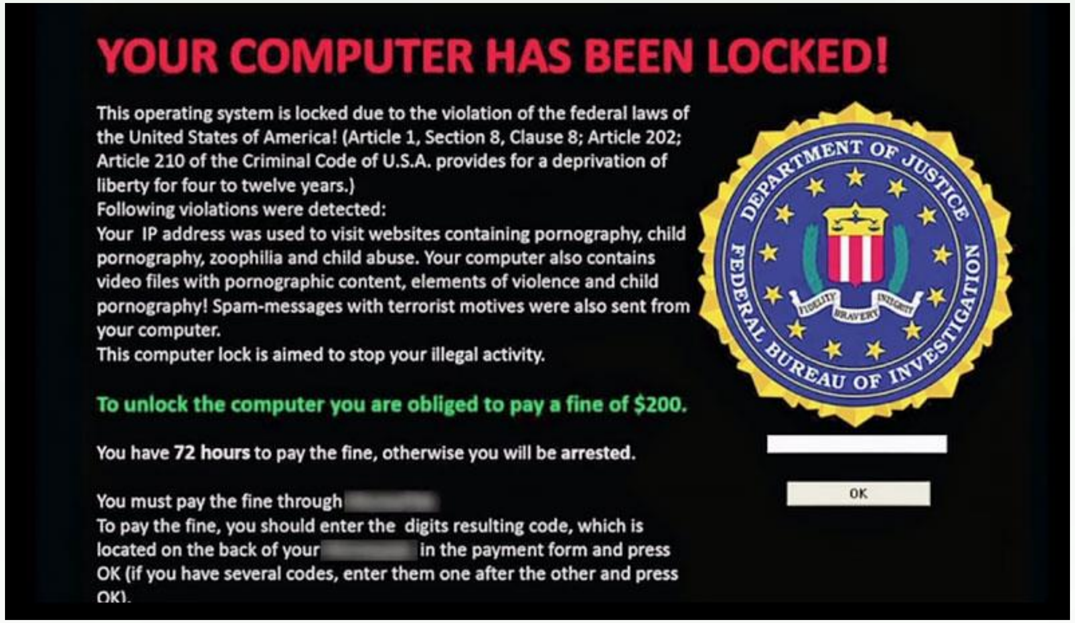
TYPES OF RANSOMWARE

- Locker Ransomware
- Crypto Ransomware
- Double Extortion Ransomware

TYPES OF RANSOMWARE

- Locker Ransomware

Locker ransomware's primary purpose is to lock a user's computer and solicit a ransom. The malware's core capabilities are geared toward this purpose.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

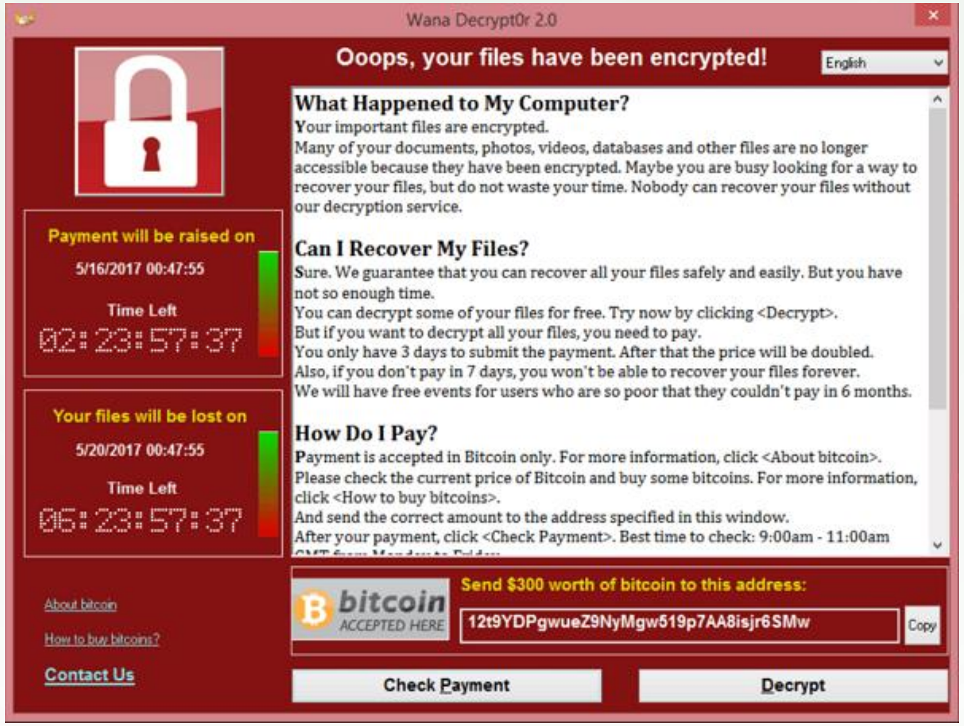
You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

TYPES OF RANSOMWARE

- CryptoRansomware

Crypto-ransomware is a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

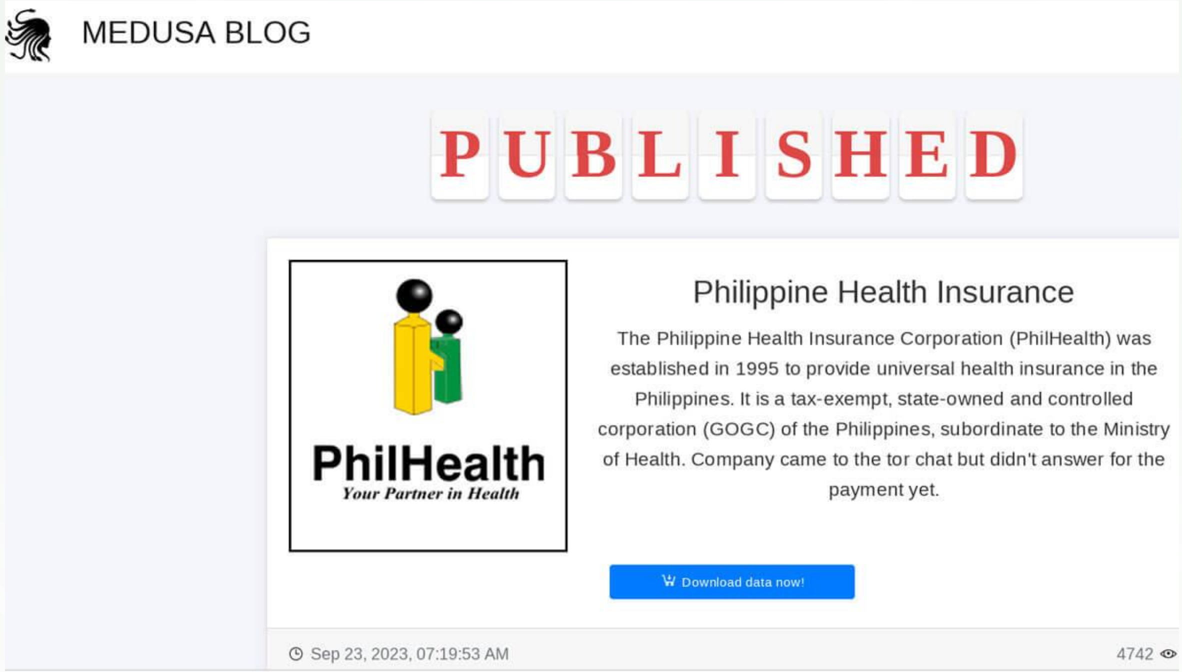
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

TYPES OF RANSOMWARE

- Double Extortion Ransomware

Double extortion ransomware is a type of cyberattack in which threat actors exfiltrate a victim's sensitive data in addition to encrypting it, giving the criminal additional leverage to collect ransom payments

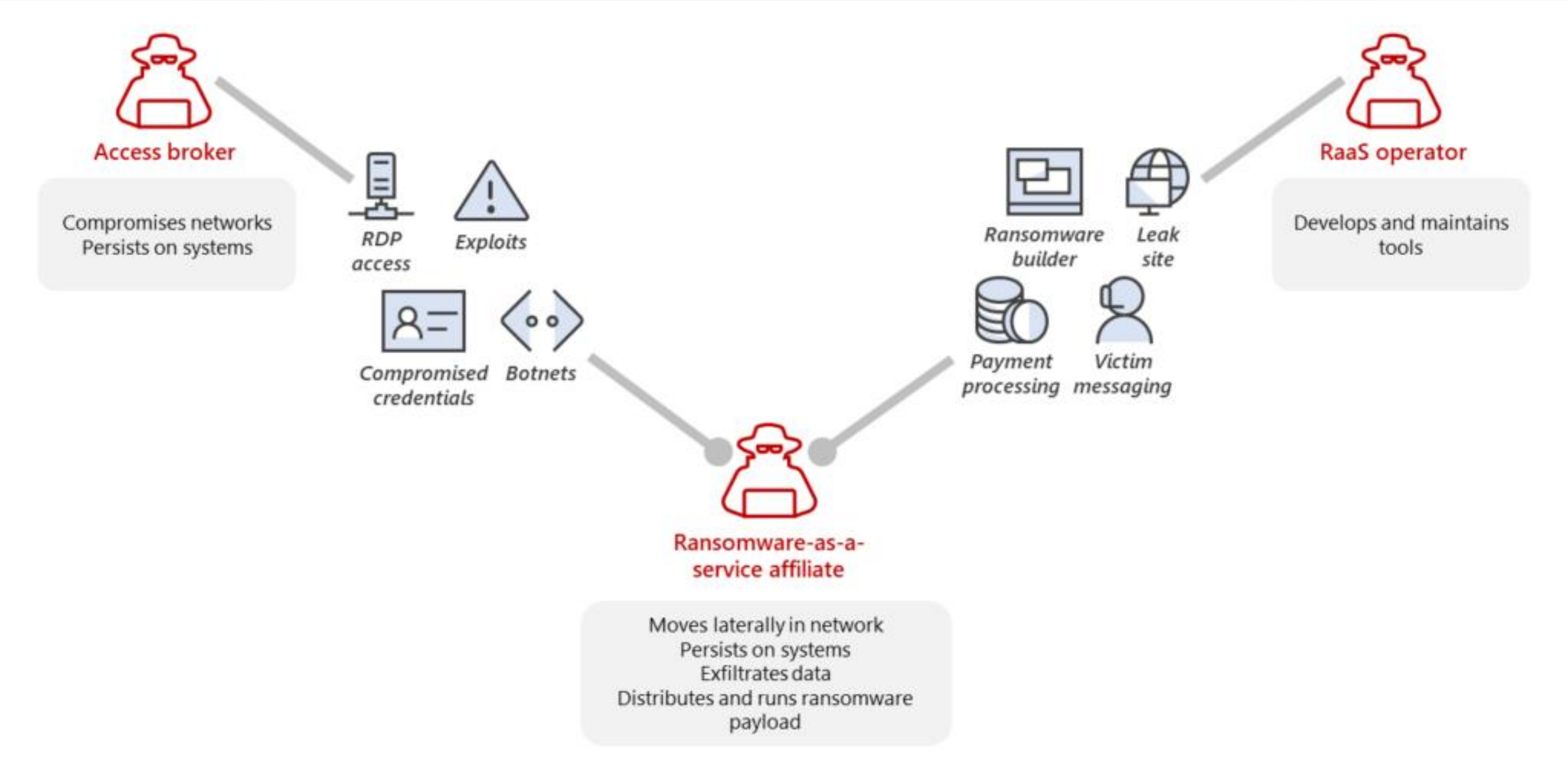

MEDUSA BLOG

PUBLISHED

Philippine Health Insurance

The Philippine Health Insurance Corporation (PhilHealth) was established in 1995 to provide universal health insurance in the Philippines. It is a tax-exempt, state-owned and controlled corporation (GOGC) of the Philippines, subordinate to the Ministry of Health. Company came to the tor chat but didn't answer for the payment yet.

RANSOMWARE AS A SERVICE (RAAS)



NOTABLE RANSOMWARE VARIANTS

- LockBit
- Revil
- BlackCat
- Lapsus$
- Conti

NOTABLE RANSOMWARE VICTIMS

- Las Vegas MGM Cyber-Attack 2023
- PhilHealth – 2023
- Nvidia Ransomware Attack 2022
- KASEYA RANSOMWARE ATTACK – JULY 2021
- Colonial Pipeline – 2021

DETECTION

- Behavioral Analysis
- Honeypots
- Heuristic Analysis
- File Integrity Monitoring (FIM)

COUNTERMEASURES

- Regular Backups
- Patch Management
- Security Awareness Training
- Endpoint Protection