



Defenxor

Safeguarding Your Business

Ransomware

Pengenalan dan Pencegahan

Dr. Toto A Atmojo

Agenda

01

Berbagai Jenis dan cara kerja
Malware



02

Ransomware



03

Pencegahan dan Penanganan
Ransomware





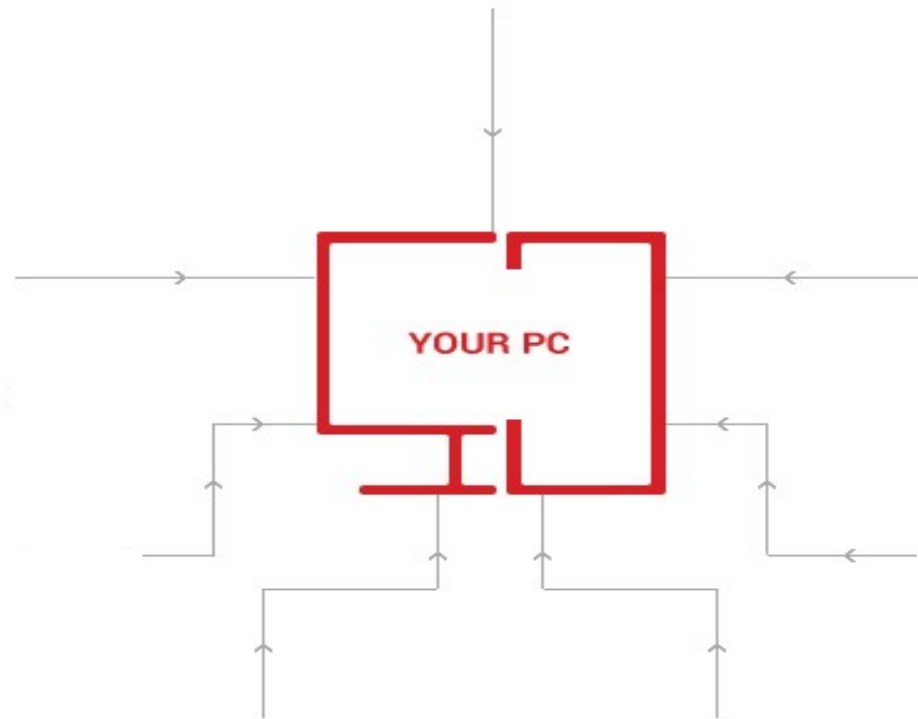
Berbagai Jenis & Cara Kerja Malware

Malware: Malicious Software



Software yang bertujuan merusak dan mengganggu, serta tidak diinginkan oleh pengguna.

Jenis Malware





Ransomware

Cybercriminal: Motif Ekonomi



Pembuat Malware
Bersenang-Senang



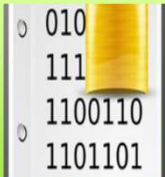
Pembuat Malware
Mendapatkan Uang

'Alat' yang dibutuhkan Hacker



Malware

- Virus
- Trojan / Bot



Alat untuk menyandera

- Enkripsi File
- Lock Operating System



Menyembunyikan identitas

- Jaringan TOR

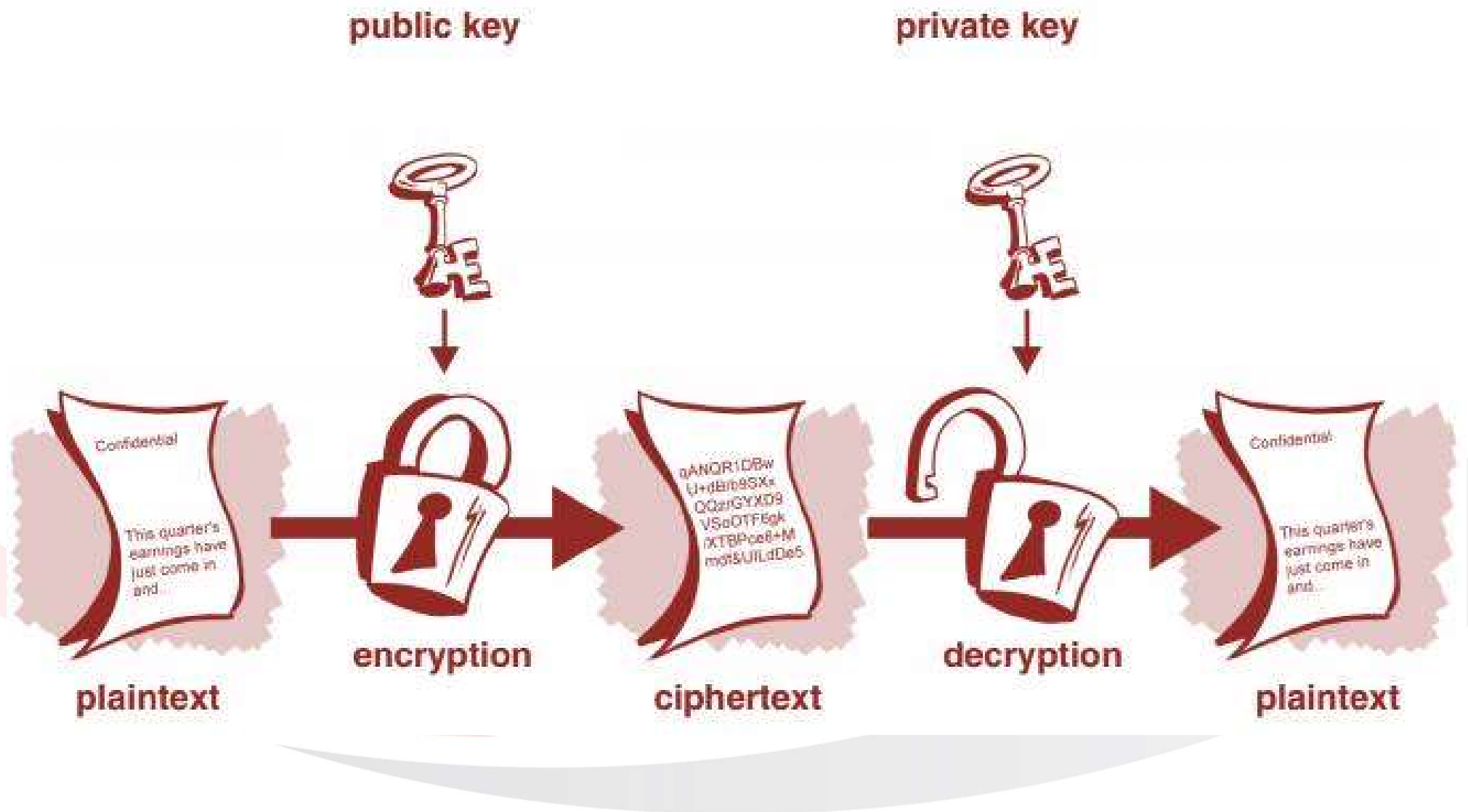


Mendapat Uang Secara 'Aman'

- Cryptocurrency
- Bitcoin, Ethereum, Litecoin, etc

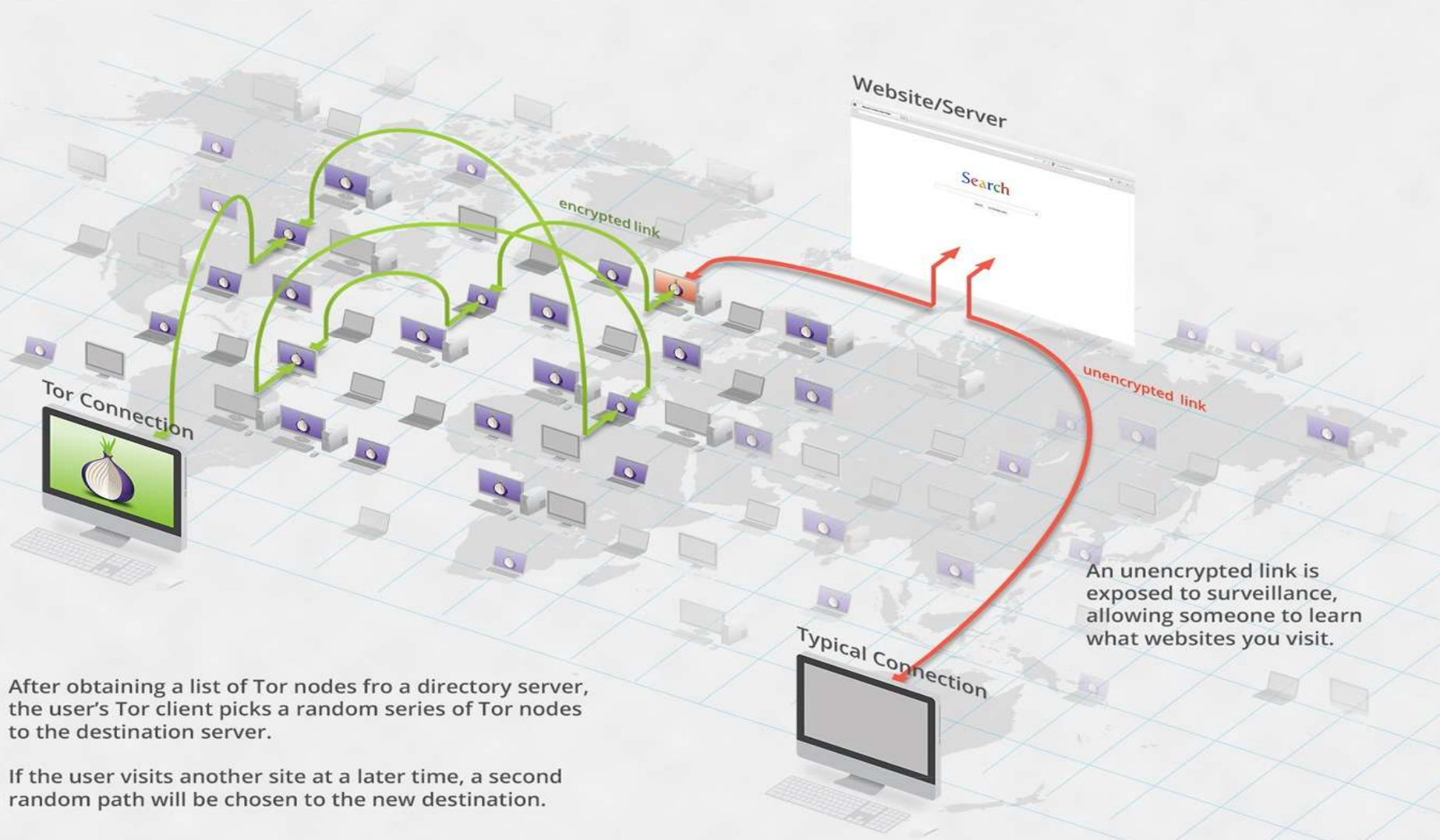


Bagaimana Enkripsi Bekerja?



Jaringan TOR (The Onion Ring)

How Tor Works:



Bitcoin: Mata Uang Digital yang Anonim

HOW TO USE BITCOINS

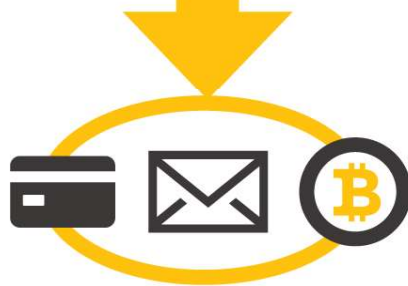


Download software to your computer or phone to set up a Bitcoin wallet. This gives you the basic facilities to send, receive and store Bitcoins



Your software will generate a unique string of letters and numbers: your Bitcoin address. The address isn't tied to your name or any other personal data, but it identifies you to the Bitcoin network. Give this address to anyone who needs to pay you

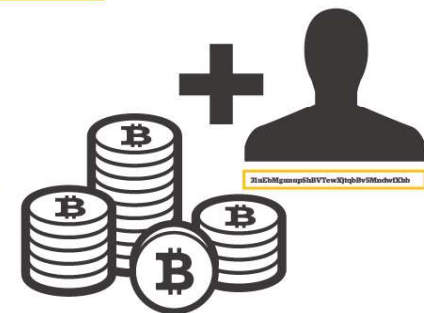
31uEbMgunupShBVtewXjtqbBv5MndwfXhb



Buy Bitcoins with a standard offline currency, either from another user or through a dedicated Bitcoin exchange. Your new digital funds are added to your wallet



The Bitcoin network authenticates transactions by recording them in the 'block chain' - the underlying code that preserves the integrity of the currency



Use your software to send payments to other addresses. Divisions as small as 100,000,000th of a Bitcoin are possible - a unit called a 'Satoshi', after the currency's enigmatic inventor

Penyebaran Ransomware



Email Attachment

- Notifikasi Invoice, Diskon Belanja, dll
- Target: Email personal & Perusahaan



Drive-by Download

- Terinfeksi saat mengakses website
- Teknik Watering Hole



Removable Media

- Memanfaatkan Fitur Autorun



Penyebaran Otomatis

- Memanfaatkan kelemahan OS

Malware Infection Index Asia Pacific 2016

Once Microsoft identifies new malware threats, malicious strains are investigated to understand their risks, origins and engineering, and how widespread their impact is. Here's a snapshot of the threat landscape in the region.

Top markets in Asia Pacific under malware threats:

Ranked by number of malware detections based on counts of machines

1	Pakistan	
2	Indonesia	
3	Bangladesh	
4	Nepal	
5	Vietnam	
6	Philippines	
7	Cambodia	
8	India	
9	Sri Lanka	
10	Thailand	
11	Malaysia	
12	Singapore	
13	Taiwan	
14	China	
15	Hong Kong	
16	Australia	
16	Korea	
18	New Zealand	
19	Japan	

"It takes an average of 200 days for organizations to find out they have been victims of cyber attacks."

Keshav Dhakad
Regional Director,
IP & Digital Crimes Unit,
Microsoft Asia

Most affected Least affected



Top 3 Encountered Malware

Gamarue
Skeeyah
Peals

Major Cyber Attacks



Malware

- Short for malicious software like Gamarue, Skeeyah and Peals, designed to cause damage to a single computer, server, or computer network, whether it's virus or spyware.



DDoS (Distributed Denial of Service)

- An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.



Identity Theft

- A crime in which an imposter obtains key pieces of personal information in order to impersonate someone else and gain access to sensitive data online.

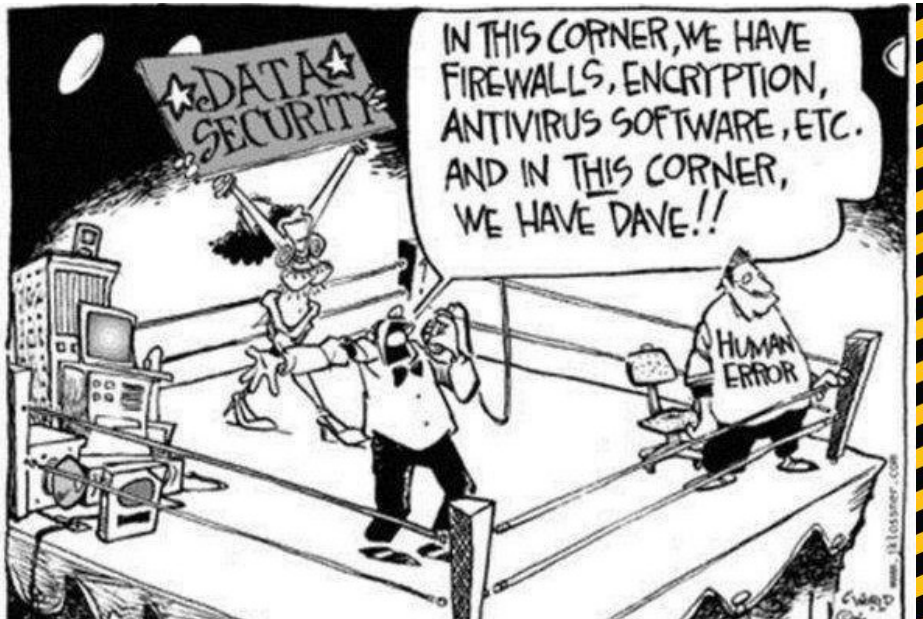
Infeksi Ransomware





Pencegahan & Penanganan Ransomware

Pencegahan Terhadap Ransomware



DOs and DON'Ts To Stay Safe From RANSOMWARE



What is ransomware?

A malware that kidnaps your computer or its data and demands money (ransom) in exchange.

HOW CAN YOU PROTECT YOURSELF?

An antidote to a ransomware infection has yet to be discovered. However, one can certainly avoid falling victim to it with the following practices:

BACK UP REGULARLY

Practice the 3-2-1 rule: Three backup copies of your data on two different media, and one of those copies in a secured separate location.

BOOKMARK WEBSITES

Bookmarking frequently visited and trusted websites will prevent you from typing in the wrong address.

VERIFY EMAIL SOURCES

Check the sender's email address against your contacts before opening any link or downloading anything from your email.

UPDATE YOUR SECURITY SOFTWARE

An up-to-date security software adds an extra layer of protection. Update it regularly so it can protect you against the latest ransomware variants.

DOs



Install all security updates for your computer.
Keep Automatic Updates enabled



Beware of emails that ask you to enable
'macros' to view the content



Always keep a secure backup of your
important data



Keep your antivirus software updated and
ensure you are using the latest version

DON'Ts



Do not click on links in unwanted
or unexpected emails



Do not download attachments
received in unknown emails



Do not click on pop-up ads
in unknown websites



Don't pay the ransom. There's no guarantee
that you will get your files back even if you do so

Bagaimana jika terinfeksi?

Ransomware?

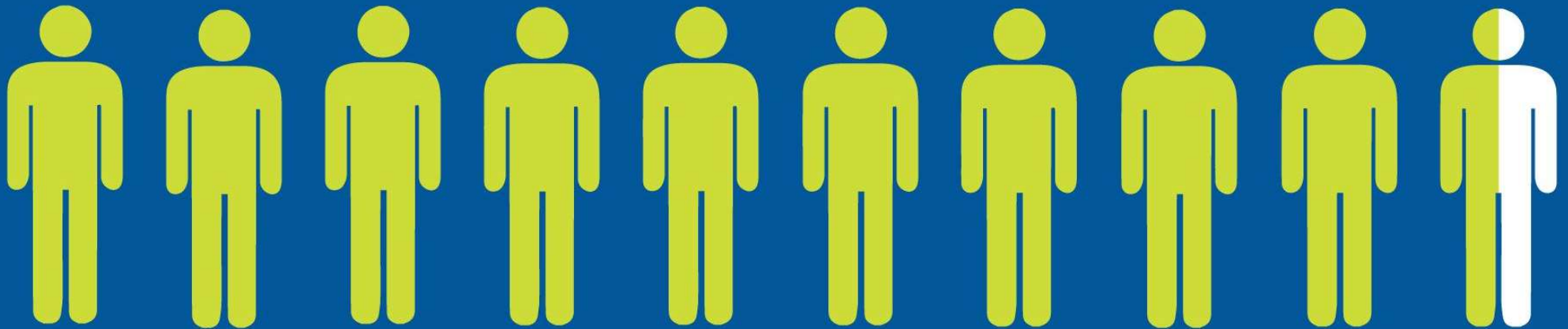
- Apakah benar Ransomware?
- Jenis>Nama Ransomware?

Kesadaran Pengguna

95%

of all successful cyber attacks
is caused by human error

Source: IBM Cyber Security Intelligence Index



Penggunaan TIK yang aman



Stay

Safe

Your Security is My Security



Defenxor

Safeguarding Your Business

Terima Kasih

www.defenxor.com