Defenxor

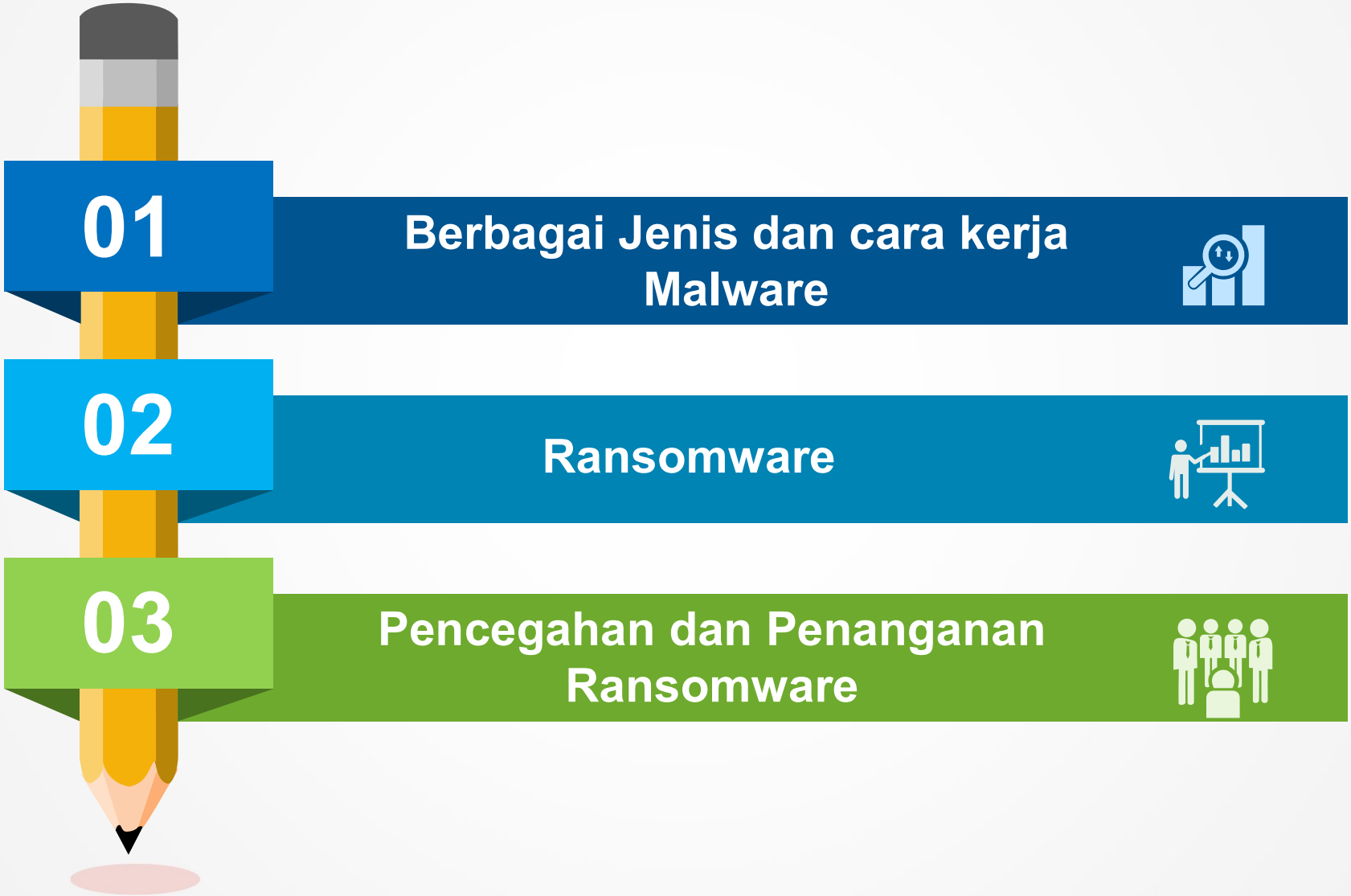
Safeguarding Your Business

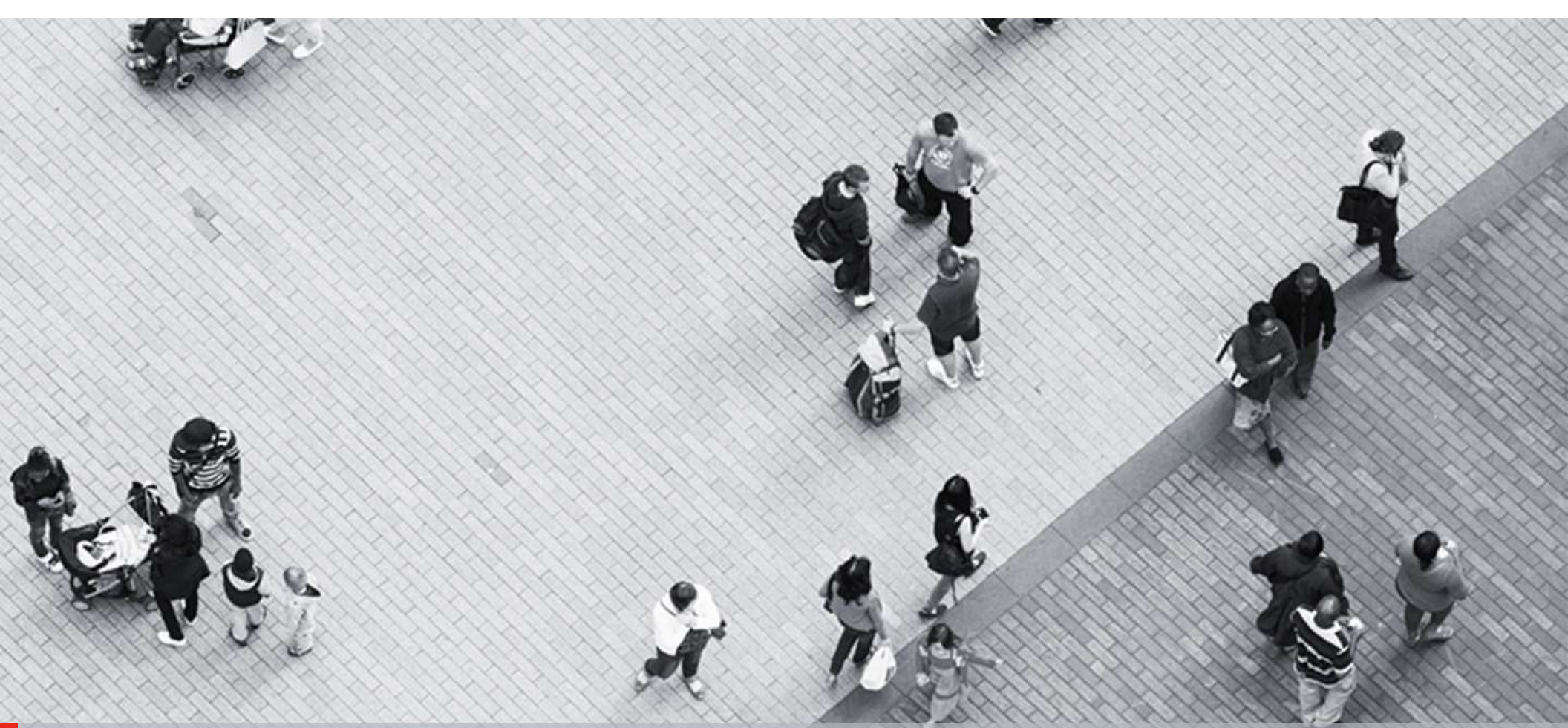
Ransomware

Pengenalan dan Pencegahan

Dr. Toto A Atmojo

Agenda


01
Berbagai Jenis dan cara kerja Malware
02
Ransomware
03
Pencegahan dan Penanganan Ransomware



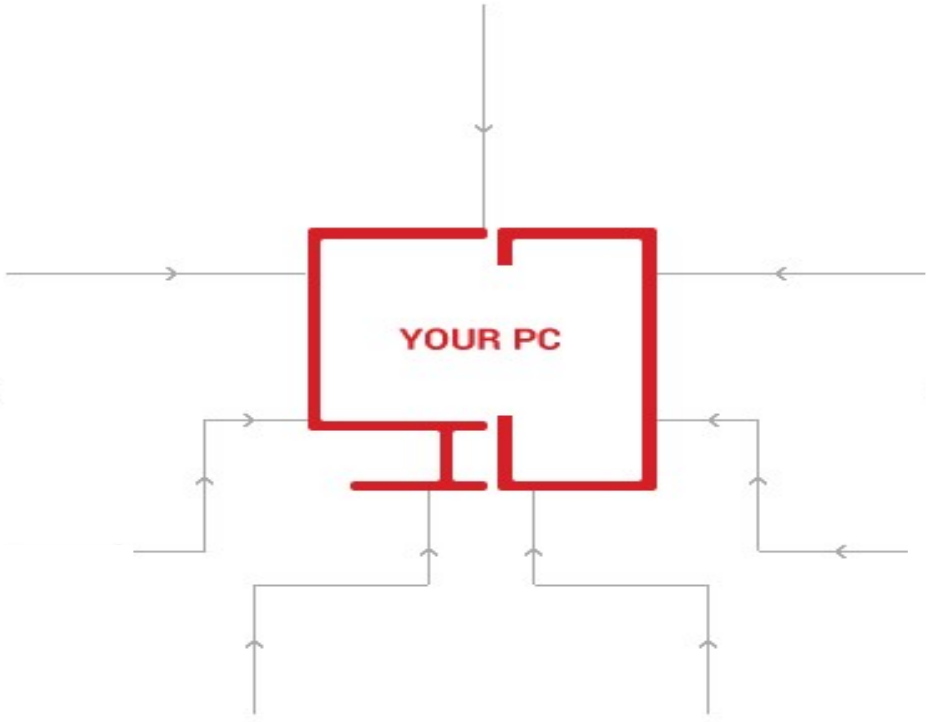
Berbagai Jenis & Cara Kerja Malware

Malware: Malicious Software

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

©2022 Defenxor. All rights reserved.

Jenis Malware



Ransomware

Cybercriminal: Motif Ekonomi

Pembuat Malware Bersenang-Senang

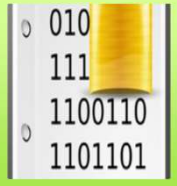
Pembuat Malware Mendapatkan Uang

©2022 Defenxor. All rights reserved.

’Alat’ yang dibutuhkan Hacker

Malware

- Virus
- Trojan / Bot



Alat untuk menyandera

- Enkripsi File
- Lock Operating System

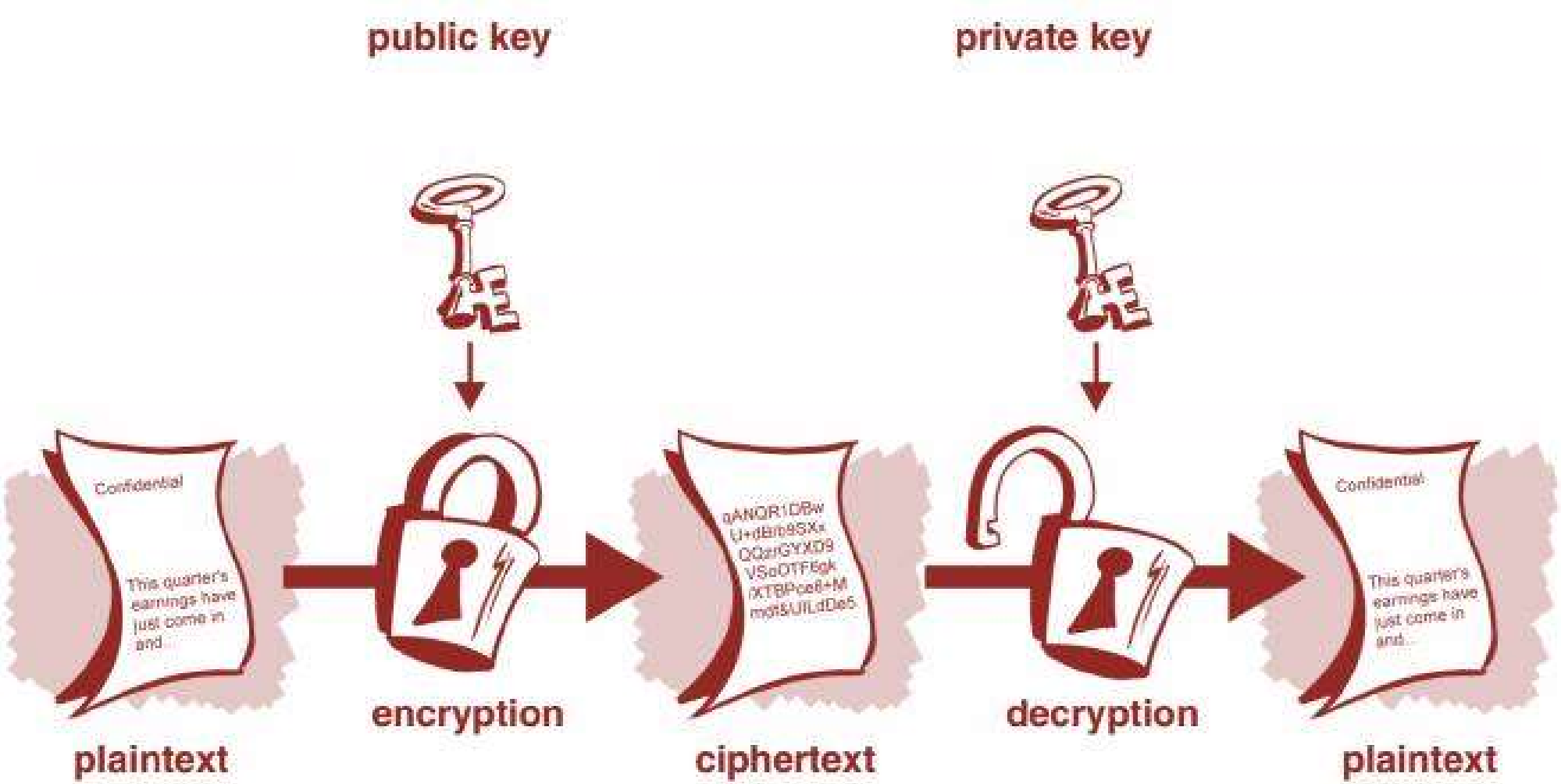
Menyembunyikan identitas

- Jaringan TOR

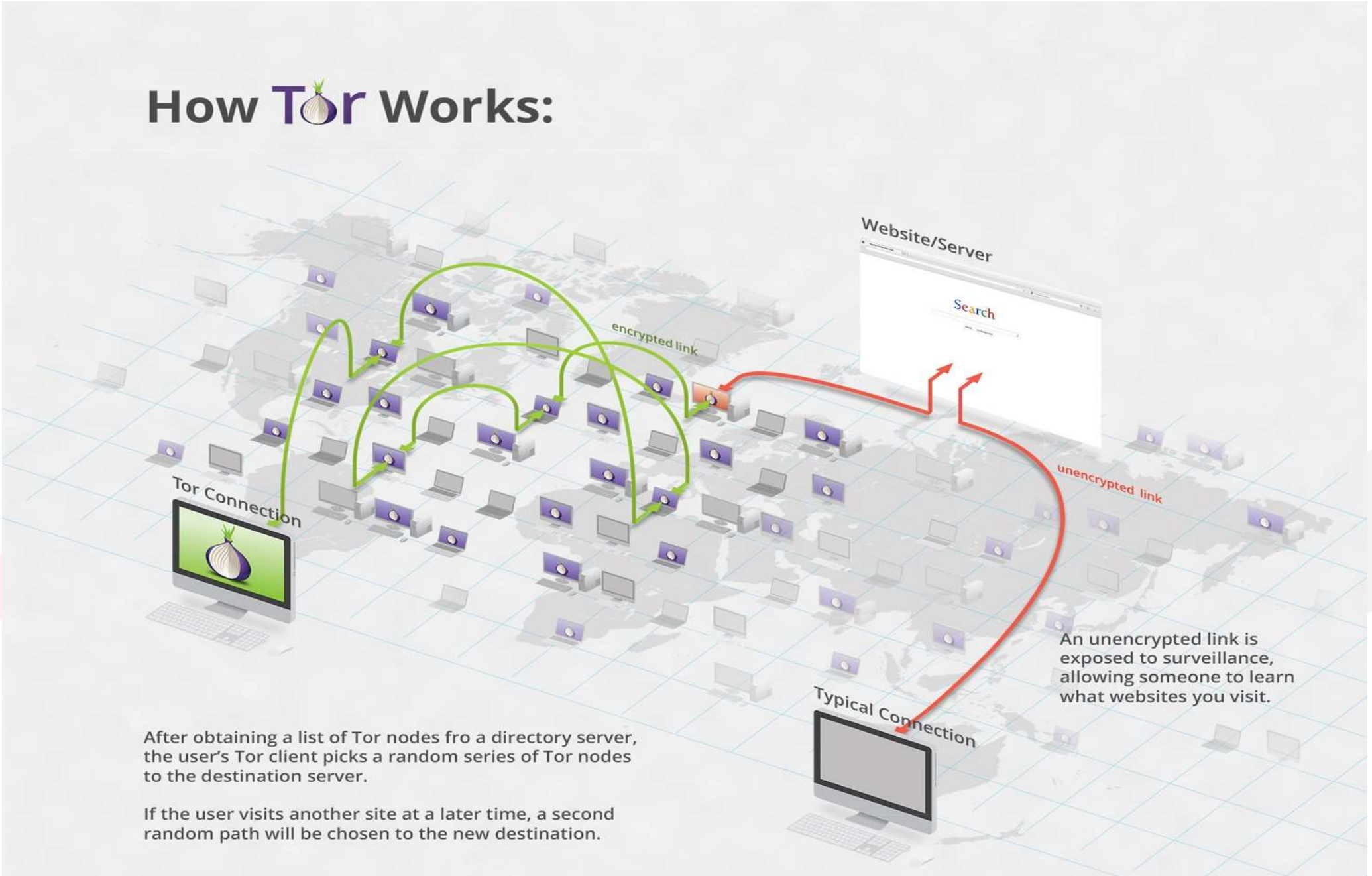
Mendapat Uang Secara ‘Aman’

- Cryptocurrency
- Bitcoin, Ethereum, Litecoin, etc

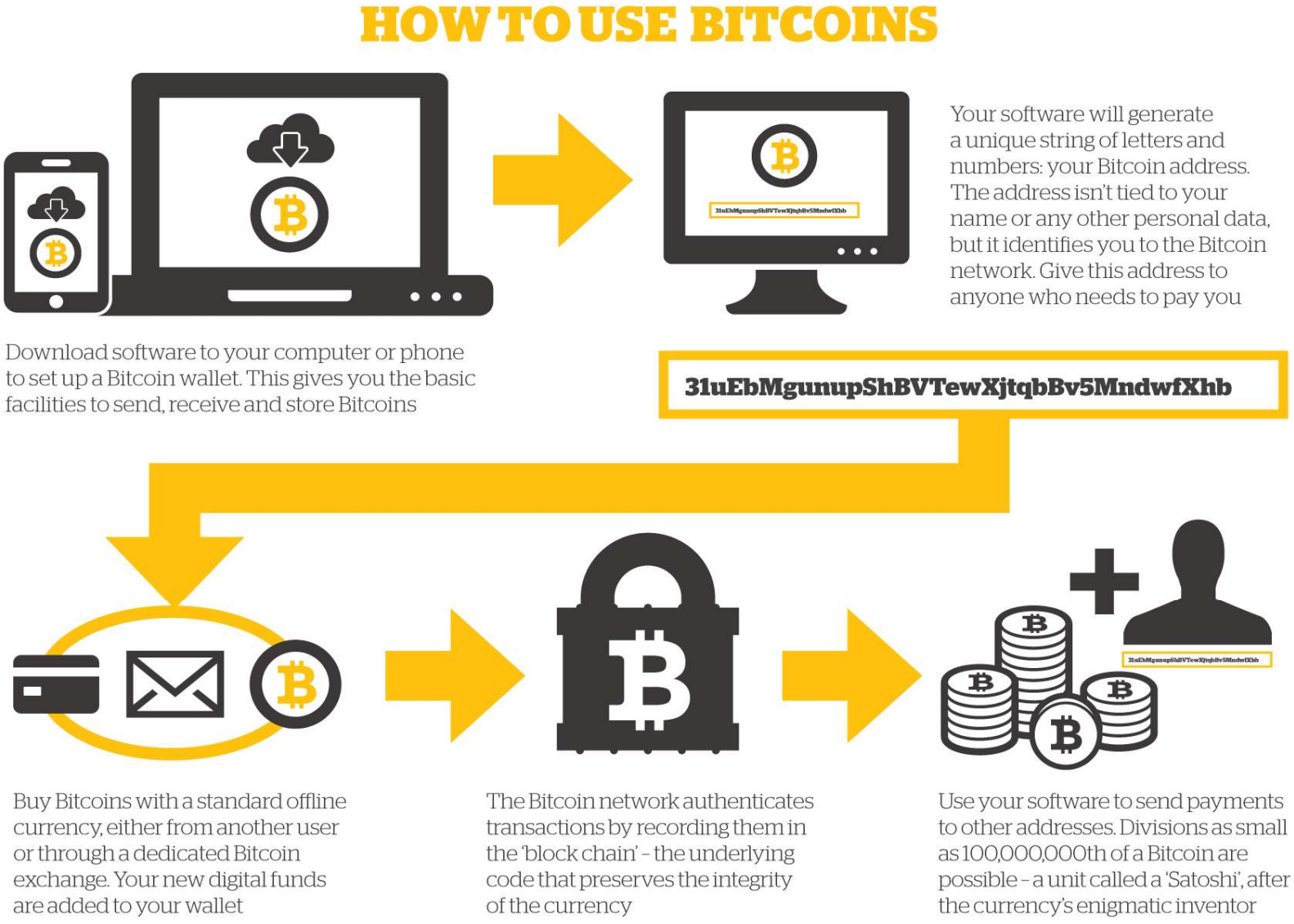
Bagaimana Enkripsi Bekerja?



Jaringan TOR (The Onion Ring)



Bitcoin: Mata Uang Digital yang Anonim



Penyebaran Ransomware

Email Attachment

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

Drive-by Download

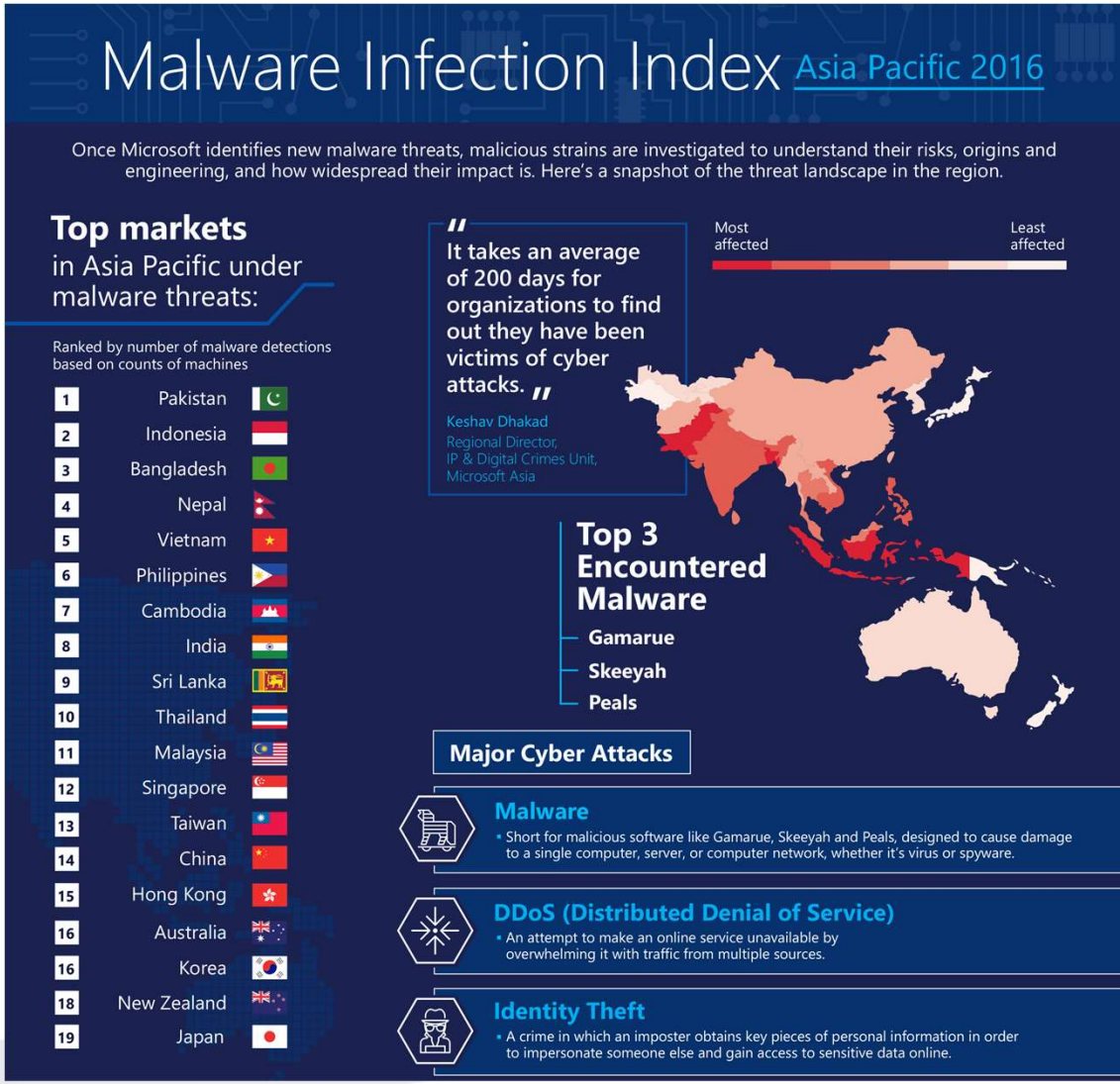
- Terinfeksi saat mengakses website
- Teknik Watering Hole

Removable Media

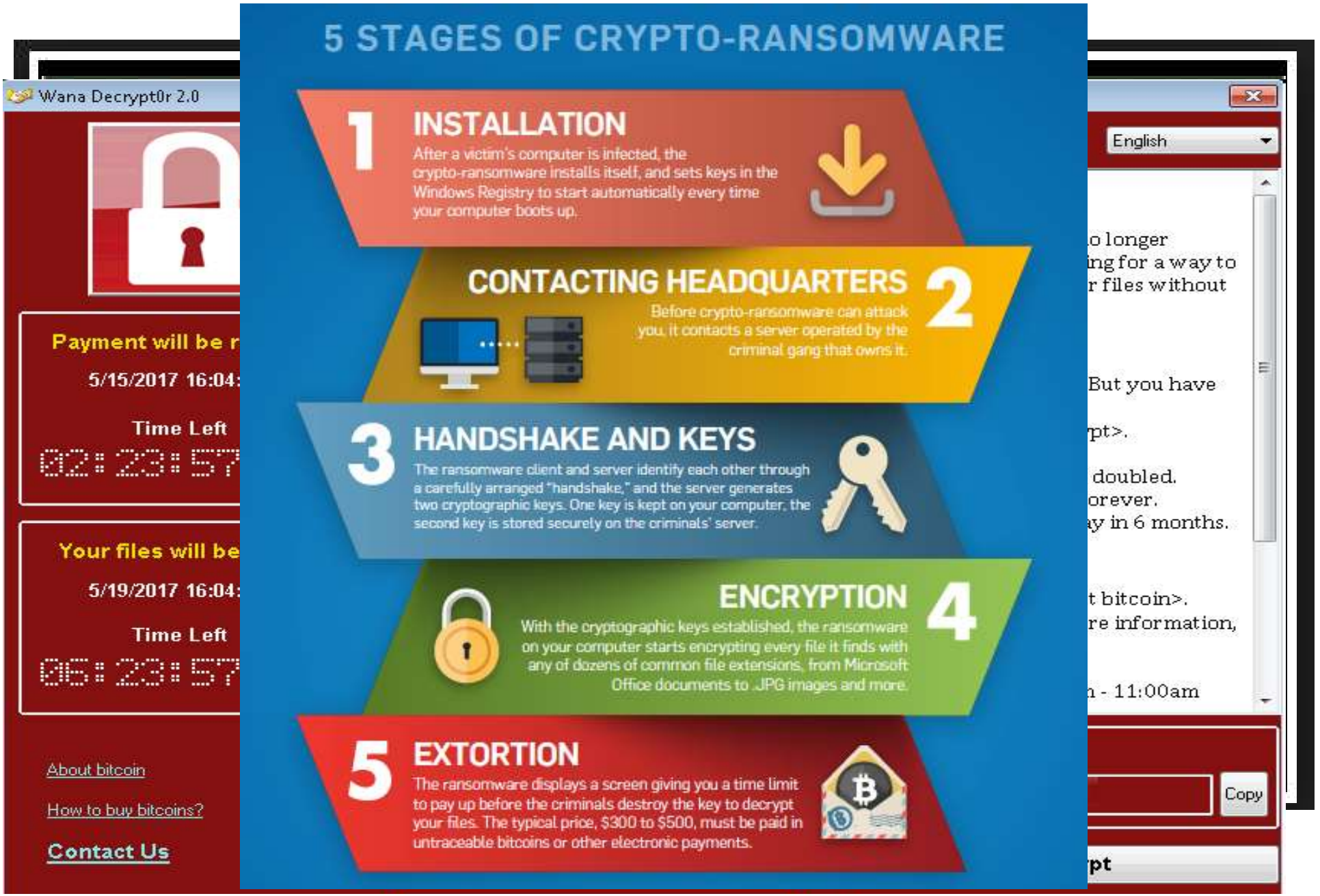
- Memanfaatkan Fitur Autorun

Penyebaran Otomatis

- Memanfaatkan kelemahan OS



Infeksi Ransomware



Pencegahan & Penanganan Ransomware

Pencegahan Terhadap Ransomware

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 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.

DOs	DON'Ts
Install all security updates for your computer. Keep Automatic Updates enabled	Do not click on links in unwanted or unexpected emails
Beware of emails that ask you to enable 'macros' to view the content	Do not download attachments received in unknown emails
Always keep a secure backup of your important data	Do not click on pop-up ads in unknown websites
Keep your antivirus software updated and ensure you are using the latest version	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?

©2022 Defenxor. All rights reserved.

Kesadaran Pengguna

©2022 Defenxor. All rights reserved.

Penggunaan TIK yang aman

Defenxor

Safeguarding Your Business

Terima Kasih

www.defenxor.com