Network Infrastructure and Information Security

Presented by Michael Takeuchi

23 July 2017, UHAMKA. Pharmacy & Science – East Jakarta (Klender)

About Me – Michael Takeuchi

- MikroTik Certified on MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E
- Work as Network Analyst at PT. Maxindo Mitra Solusi
- MikroTik Certified Consultant on www.mikrotik.com
- Ubiquiti Wireless Certified on UEWA and UBWA
- Not Hacker, Just Networker

Our Agenda

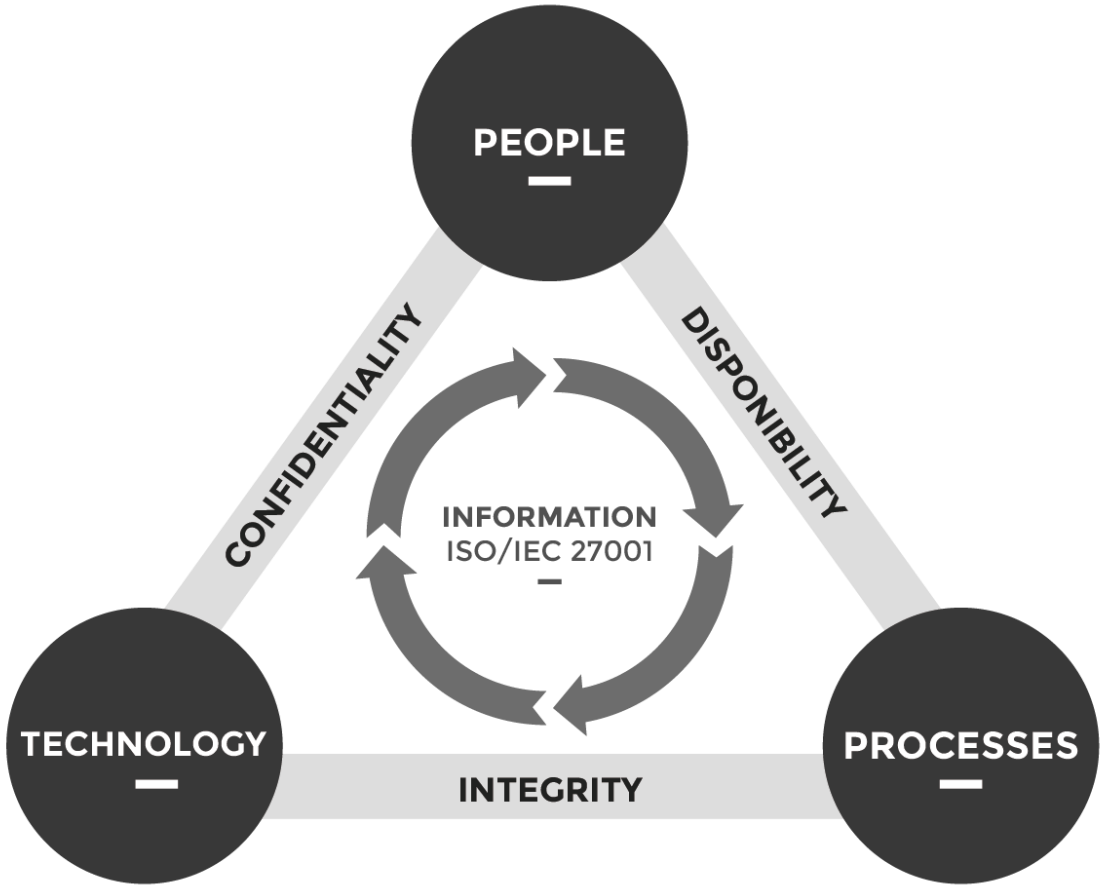
- Objective
- Chapter 1 – Information Security Baseline
- Chapter 2 – Introduction to Computer Network
- Chapter 3 – Computer Network Addressing
- Chapter 4 – Commonly Network Topology & Devices
- Chapter 5 – Cyber World, Cyber Crime, Cyber Warfare & Threats
- Chapter 6 – Introduce to “Ransomware Attack Trends 2017”
- Chapter 7 – How **WannaCry**pt Infecting Our Networks
- Chapter 8 – **WannaCry**pt Preventions & Conclusions
- Chapter 9 – End of The Presentation

Objective

- educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets
- understand how their actions can greatly impact the overall security position of an organization
- reinforce security policy and other information security practices that are supported by the organization
- helps minimize the cost of security incidents, helps accelerate the development
- of new application systems, and helps assure the consistent implementation of controls across an organization’s information systems

Chapter 1
Information Security Baseline

Information Security Baseline



Information Security Baseline

- **Confidentiality** attempts to prevent the intentional or unintentional unauthorized disclosured of information
- **Integrity** ensures that modifications are not made by unauthorized personnel or processes; unauthorized modifications are not made to data by authorized personnel or processes; and data is internally and externally consistent.
- **Availability** ensures the reliable and timely access to data or computing resources by the appropriate personnel.

Chapter 1 – Summary

- CIA (**Confidentiality, Integrity, Availability)** ini adalah 3 unsur utama dari keamanan informasi yang menjaga kerahasiaan, integritas data, dan ketersediaan layanan didalam sebuah organisasi yang harus dipahami oleh anggota dari organisasi tersebut agar terjaganya informasi didalam organisasi tersebut

Chapter 2
Introduction to Computer Network

What is Network?

- Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan **layanan (service)**.
- Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai media transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti **Hub, Bridge, Switch, Router, Gateway** sebagai peralatan interkoneksinya.

What is Network?

- Jaringan komputer adalah sebuah sistem yang terdiri dari dua atau lebih komputer yang saling terhubung satu sama lain melalui media transmisi atau media komunikasi sehingga dapat saling berbagi data, aplikasi maupun berbagi perangkat keras komputer.
- A computer network or data network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Chapter 2 – Summary

- Pada intinya jaringan komputer ini adalah teknologi yang dibangun bersama – sama digunakan untuk berkomunikasi secara digital dalam jarak jauh maupun dekat dengan cepat dibanding kita harus berkomunikasi secara tradisional

Chapter 3
Computer Network Addressing

Computer Network Address/IP Address

- Alamat IP (Internet Protocol Address atau sering disingkat IP) adalah deretan angka biner antara 32 bit (IPv4) sampai 128 bit (IPv6) yang dipakai sebagai **alamat identifikasi** untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32 bit (untuk IPv4 atau IP versi 4), dan 128 bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP.

Sistem pengalamatan IP ini terbagi menjadi dua, yakni:

- IP versi 4 (IPv4) – Dipakai Saat Ini
- IP versi 6 (IPv6) – Dipakai Saat Nanti

Perbandingan alamat IP versi 4 dan alamat IP versi 6

Kriteria	Alamat IP versi 4	Alamat IP versi 6
Panjang alamat	32 bit	128 bit
Jumlah total host (teoritis)	2^{32}=±4 miliar host	2^{128}
Menggunakan kelas alamat	Ya, kelas A, B, C, D, dan E. Belakangan tidak digunakan lagi, mengingat telah tidak relevan dengan perkembangan jaringan Internet yang pesat.	Tidak
Alamat multicast	Kelas D, yaitu **224.0.0.0/4**	Alamat *multicast IPv6*, yaitu **FF00:/8**
Alamat *broadcast*	Ada	Tidak ada
Alamat yang belum ditentukan	**0.0.0.0**	::
Alamat *loopback*	**127.0.0.1**	**::1**
Alamat IP publik	Alamat IP publik IPv4, yang ditetapkan oleh otoritas Internet (IANA)	Alamat IPv6 *unicast global*
Alamat IP pribadi	Alamat IP pribadi IPv4, yang ditetapkan oleh otoritas Internet	Alamat IPv6 *unicast site-local* (FEC0::/48)
Konfigurasi alamat otomatis	Ya (APIPA)	Alamat IPv6 *unicast link-local* (FE80::/64)
Representasi tekstual	*Dotted decimal format notation*	*Colon hexadecimal format notation*
Fungsi Prefiks	*Subnet mask* atau panjang prefiks	Panjang prefiks
Resolusi alamat DNS	*A Resource Record* (*Single A*)	*AAAA Resource Record* (*Quad A*)

IP Public & IP Private

- IP Public adalah IP yang beredar di Internet
- IP Private adalah IP yang digunakan didalam Jaringan Privat atau Pribadi yang tidak boleh digunakan di Internet dan juga sebaliknya pada jaringan privat kita tidak boleh menggunakan IP Public

- Jika kita mau terhubung keinternet kita harus memiliki IP Public yang dikenali di Internet, Check = https://www.whatismyip.com kok beda dengan IP yang terpasang di device kita? Check = **NAT Feature**
- Jaringan Internet Dibentuk Dengan **Routing**

Network Address Translation (NAT)

- NAT digunakan untuk mentranslasikan IP Private ke IP Public ataupun sebaliknya dari IP Public ke IP Private
- Dengan menggunakan NAT kita bisa menghemat penggunaan IP Public dunia karena setiap Host didalam 1 jaringan bisa diwakili oleh satu IP yang sudah ditranslasi dengan NAT
- Karena itu jika kita mau menggunakan server dengan IP Private kita harus mengaktifkan fitur **Port Forwarding** (FYI, Port Forwarding juga menggunakan fitur NAT untuk melakukannya)

Routing?

- Routing disini berarti kita memberikan arahan suatu paket dalam jaringan kita untuk menuju destinasinya dari asalnya (source)
- Routing atau pemberian jalur ini biasanya kita lakukan pada Perangkat Jaringan yang dinamakan Router
- Contoh: kita mengirimkan paket request http://www.google.com maka paket request kita akan diarahkan oleh router dengan rute yang sudah kita setup didalamnya
- Device kita melakukan **Routing?** (read: Fungsi Default Gateway)

IP Private

- Range 1 = 10.0.0.0 – 10.255.255.255
- Range 2 = 172.16.0.0 – 172.31.255.255
- Range 3 = 192.168.0.0 – 192.168.255.255

Reserved IP

https://en.wikipedia.org/wiki/Reserved_IP_addresses

- Reserved IP disini adalah IP yang sudah dibooking atau ditetapkan oleh IANA (Internet Assigned Number Authority) sehingga tidak bisa kita gunakan lagi
- Loh kok Range IP Private masuk? Jangan khawatir, untuk yang itu masih bisa digunakan didalam jaringan privat kita

Kelas A? Kelas B? Kelas C? Kelas D? Kelas E?

Kelas A = 0.0.0.0 – 127.255.255.255

Kelas B = 128.0.0.0 – 191.255.255.255

Kelas C = 192.0.0.0 – 223.255.255.255

Kelas D= 224.0.0.0 – 239.255.255.255

Kelas E = 240.0.0.0 – 255.255.255.255

- Tidak Berpengaruh karena kita sekarang sudah menggunakan yang namanya Classless Inter-Domain Routing (CIDR), kalau yang lama (Kelas A, Kelas B, Kelas C) itu namanya Classfull Addressing
- Kelas A – C digunakan untuk host
- Kelas D digunakan untuk multicast & Kelas E digunakan untuk eksperimen

Classless Inter-Domain Routing (CIDR)

- Adalah sebuah metode baru untuk IP Addressing, jika dulu kita memakai **Kelas** sekarang kita menggunakan CIDR yang ditandai dengan **/**
- Jika dahulu kita memakai Kelas, jumlah IP yang bisa digunakan sangat banyak sehingga tidak efesien sedangkan CIDR bisa meminimalisir penggunaan IP tersebut hingga 1 IP saja
- Kebanyakan Jaringan sekarang sudah menggunakan CIDR

Penggunaan CIDR

- Jika kita mempunyai 5 PC & 8 Smartphone maka kita membutuhkan 13 IP dan 1 IP sebagai **Gateway**, Maka kita membutuhkan 14 IP Saja dan 2 IP sebagai IP **Network ID** & **Broadcast** jadi 16 IP
- IP Network ID digunakan untuk Identitas Network Kita
- IP Broadcast digunakan ketika ada traffic **Broadcast** (IP ini tidak kita gunakan jika traffic kita unicast atau multicast)
- Gateway digunakan sebagai jalan keluar untuk kenetwork lain atau internet (tidak dibutuhkan jika kita hanya menginginkan komunikasi 1 network)
- Jika kita menggunakan CIDR /28 maka dengan begitu kita bisa mengeoptimalkan penggunaan IP tersebut dan bahkan kita bisa mencegah orang lain atau **HACKER** terhubung kedalam jaringan kita

CIDR Table

Subnet mask quick reference							
Host Bit length	math	Max hosts	Subnet mask	Mask octet	Binary mask	Mask length	Subnet length
0	2^0=	1	255.255.255.255	4	11111111	32	0
1	2^1=	2	255.255.255.254	4	11111110	31	1
2	2^2=	4	255.255.255.252	4	11111100	30	2
3	2^3=	8	255.255.255.248	4	11111000	29	3
4	2^4=	16	255.255.255.240	4	11110000	28	4
5	2^5=	32	255.255.255.224	4	11100000	27	5
6	2^6=	64	255.255.255.192	4	11000000	26	6
7	2^7=	128	255.255.255.128	4	10000000	25	7
8	2^8=	256	255.255.255.0	3	11111111	24	8
9	2^9=	512	255.255.254.0	3	11111110	23	9
10	2^10=	1024	255.255.252.0	3	11111100	22	10
11	2^11=	2048	255.255.248.0	3	11111000	21	11
12	2^12=	4096	255.255.240.0	3	11110000	20	12
13	2^13=	8192	255.255.224.0	3	11100000	19	13
14	2^14=	16384	255.255.192.0	3	11000000	18	14
15	2^15=	32768	255.255.128.0	3	10000000	17	15
16	2^16=	65536	255.255.0.0	2	11111111	16	16
17	2^17=	131072	255.254.0.0	2	11111110	15	17
18	2^18=	262144	255.252.0.0	2	11111100	14	18
19	2^19=	524288	255.248.0.0	2	11111000	13	19
20	2^20=	1048576	255.240.0.0	2	11110000	12	20
21	2^21=	2097152	255.224.0.0	2	11100000	11	21
22	2^22=	4194304	255.192.0.0	2	11000000	10	22
23	2^23=	8388608	255.128.0.0	2	10000000	9	23
24	2^24=	16777216	255.0.0.0	1	11111111	8	24

Example Test

- Carilah Range IP yang bisa digunakan, Network ID & Broadcast IP dari:

1. 192.168.10.0/28
2. 172.18.32.50/26
3. 10.20.30.40/25
4. 10.50.50.50/24

- Validasi Penulisan dan Sistem Pengalamatan IP Dibawah ini

1. 172.20.256.42/27 - Valid?
2. 2001::2/64 - Valid?
3. ::1/128 - Valid?

Example Test

- Sebuah ISP memiliki IP Public sebesar /24
  Untuk infrastructure jaringan, dibutuhkan 2 buah subnet /26
  Jika 1 pelanggan membutuhkan IP sebesar /29
  Berapakah pelanggan, berapakah jumlah pelanggan maksimum yang bisa dimiliki oleh ISP tersebut?

- Jawab (Lihat CIDR Table):

ISP memiliki subnet /24 = 256 IP, dibuat infrastruktur 2 buah yang punya subnet /26 = 64, maka 256 - 64 sejumlah 2 buah maka, 256 - 128, masih 128, jika tiap pelanggan punya akses /29 = 8 IP maka 128/8 = **16 Pelanggan**

Cara Cepat Subnetting (1)

- Contoh: 172.20.50.24/28

/28 memiliki maximal IP 16

1. Mencari Network = IP Oktet Terakhir (24) dibagi dengan maximal IP yang ada (16) maka menjadi 24/16 = **1**,xxxx (ambil depannya saja) + Max IP (16) sampai tidak melewati IP yang dihitung (bisa ditambah 1x sampai 16) – Hasil Pembagian (1) = 1 + 16 – 1 = 16, Maka Network ID = 172.20.50.**16**
2. Mencari Broadcast = Max IP (16) – 1 + Network ID (16) = **16**
   , Maka IP Broadcast = 172.20.50.**31**
3. Subnet Mask = 256 – Max IP (16) = **240**, Maka Subnet Mask = 255.255.255.**240**
4. Mencari Range Host = Diatas Network – Dibawah Broadcast

   172.20.50.17 – 172.20.50.30

Cara Cepat Subnetting (2)

- Contoh: 172.18.20.20/29

/28 memiliki maximal IP 16

1. Mencari Network = IP Oktet Terakhir (20) dibagi dengan maximal IP yang ada (8) maka menjadi 20/8 = **2**,xxxx (ambil depannya saja) + Max IP (8) sampai tidak melewati IP yang dihitung (bisa ditambah 2x sampai 16) – Hasil Pembagian (2) = 2 + 16 – 2 = 16, Maka Network ID = 172.18.20.**16**
2. Mencari Broadcast = Max IP (8) – 1 + Network ID (16) = **23** , Maka IP Broadcast = 172.18.20.**23**
3. Subnet Mask = 256 – Max IP (8) = **248**, Maka Subnet Mask = 255.255.255.**248**
4. Mencari Range Host = Diatas Network – Dibawah Broadcast

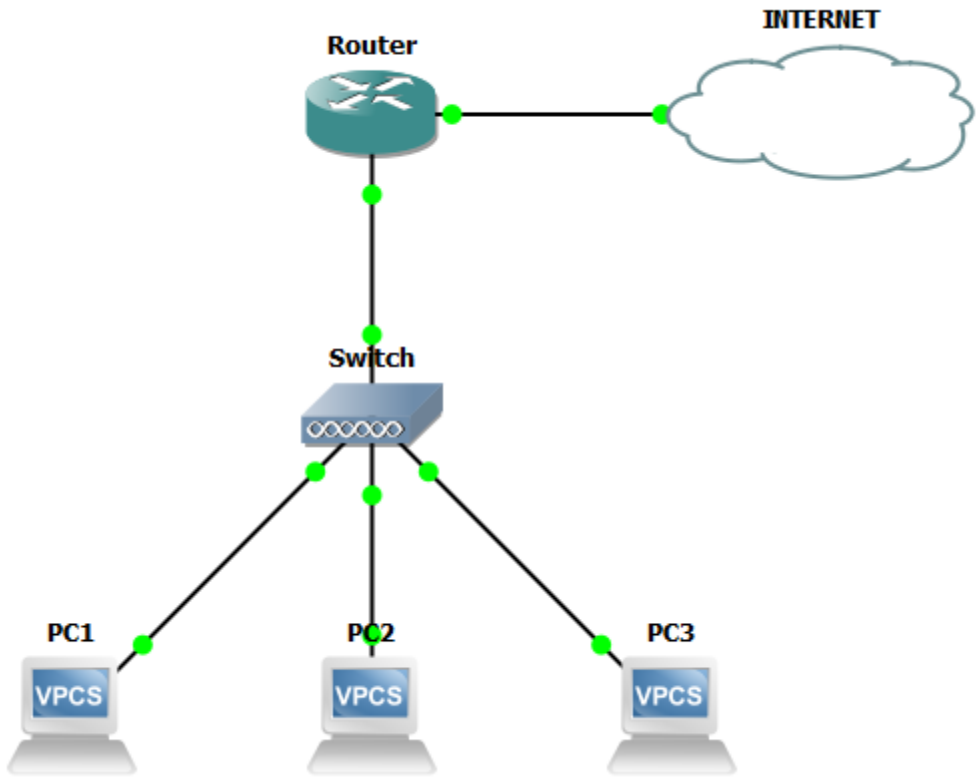
172.18.20.17 – 172.18.20.22

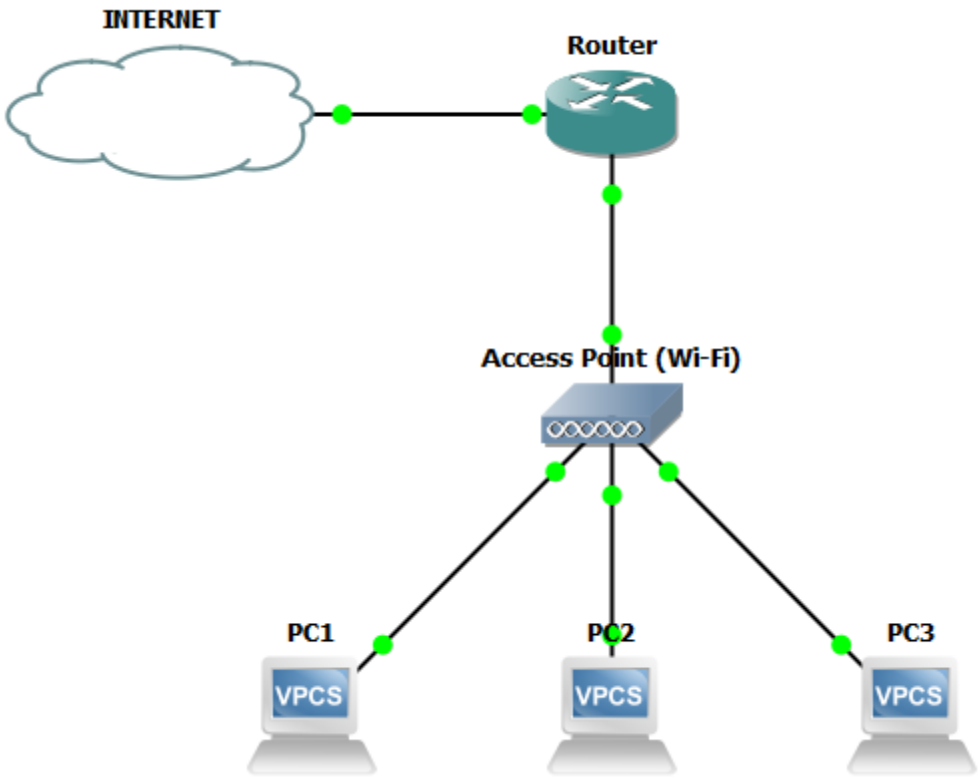
Chapter 3 Summary

- **Computer Network Address** atau biasa disebut **Alamat IP** adalah deretan angka biner sepanjang 32bit yang dipakai sebagai alamat **identifikasi** untuk tiap komputer host dalam jaringan Internet. Contoh:
  - **192.168.10.1** (11000000.10101000.00001010.00000001)
- Angka **192.168.10.1** adalah sebuah contoh alamat dari sebuah node (komputer) didalam sebuah jaringan komputer, IP address terdiri dari 4 blok dengan maximal angka 0 - 255
  - Blok 1 = 192
  - Blok 2 = 168
  - Blok 3 = 10
  - Blok 4 = 1
- Kenapa maximal 256? Karena panjang IP ini 32-bit/4 = 8bit (2^8 = **256**)
- Dan total sepanjang 2^32 = 4.294.967.296 atau bisa dihitung 256*256*256*256 = 2^32
- Challenge: Berapa IP Address anda?
- Cheat: http://jodies.de/ipcalc

Chapter 4
Commonly Network Topology & Devices

Commonly LAN Topology





Commonly Network Topology

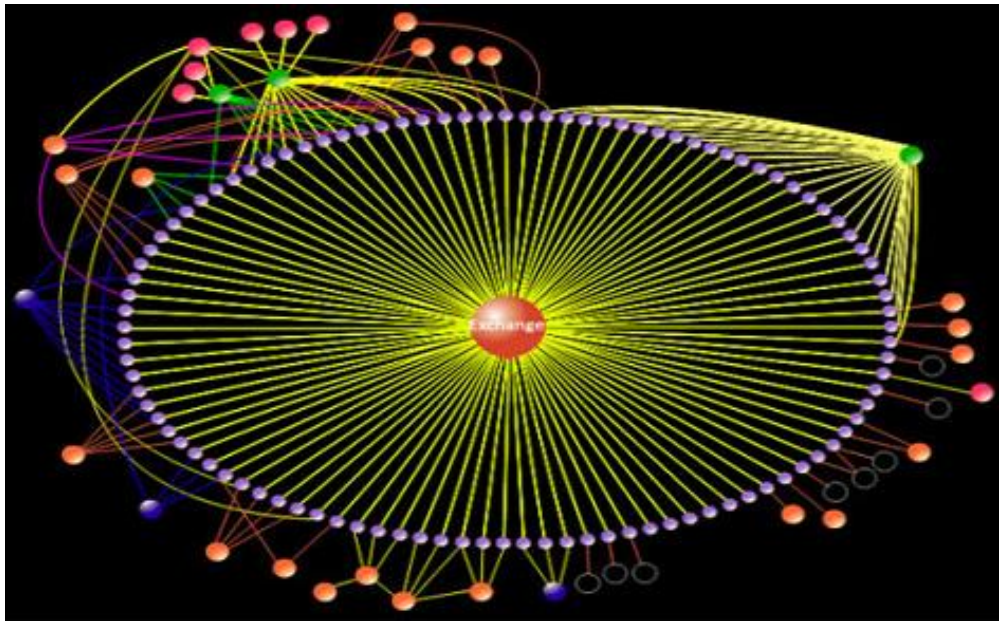
- Jaringan ini bisa kita ibaratkan sebagai rumah yang memiliki penghuni yang digambarkan sebagai **devices** (komputer, handphone, printer dan beberapa alat yang bisa berkomunikasi) yang pada umumnya dihubungkan melalui 1 alat yang disebut **switch** ataupun menggunakan **wireless** yang disebut **access point** dan jika kita ingin keluar kejaringan lain maka kita membutuhkan pintu **(router)**
- Untuk kabel bawah laut yang menghubungkan **DUNIA** bisa dilihat di http://www.submarinecablemap.com

Commonly Networking Devices & Function

- **Router** berfungsi sebagai penghubung 2 jaringan atau lebih untuk meneruskan data dari satu jaringan ke jaringan lainnya & router berbeda dengan switch.
- **Switch** berfungsi sebagai alat yang digunakan untuk menyatukan beberapa Host/Node/Devices menjadi satu jaringan menggunakan kabel.
- **Wireless Access Point** berfungsi mirip seperti switch, namun alat ini tidak memerlukan kabel dan data akan dihantarkan melalui udara

Chapter 4 – Summary

- Kita sudah berkenalan dengan jaringan SOHO (Small Office & Home) baik dengan alat maupun pengalamatan mereka
- Jaringan yang saya gambarkan dislide sebelumnya masih sederhana dan umum, dibawah ini saya lampirkan topologi dari OpenIXP/NiCE (National InterConnection Exchange)



Chapter 5
Cyber World, Cyber Crime, Cyber Warfare & Threats

Cyber World

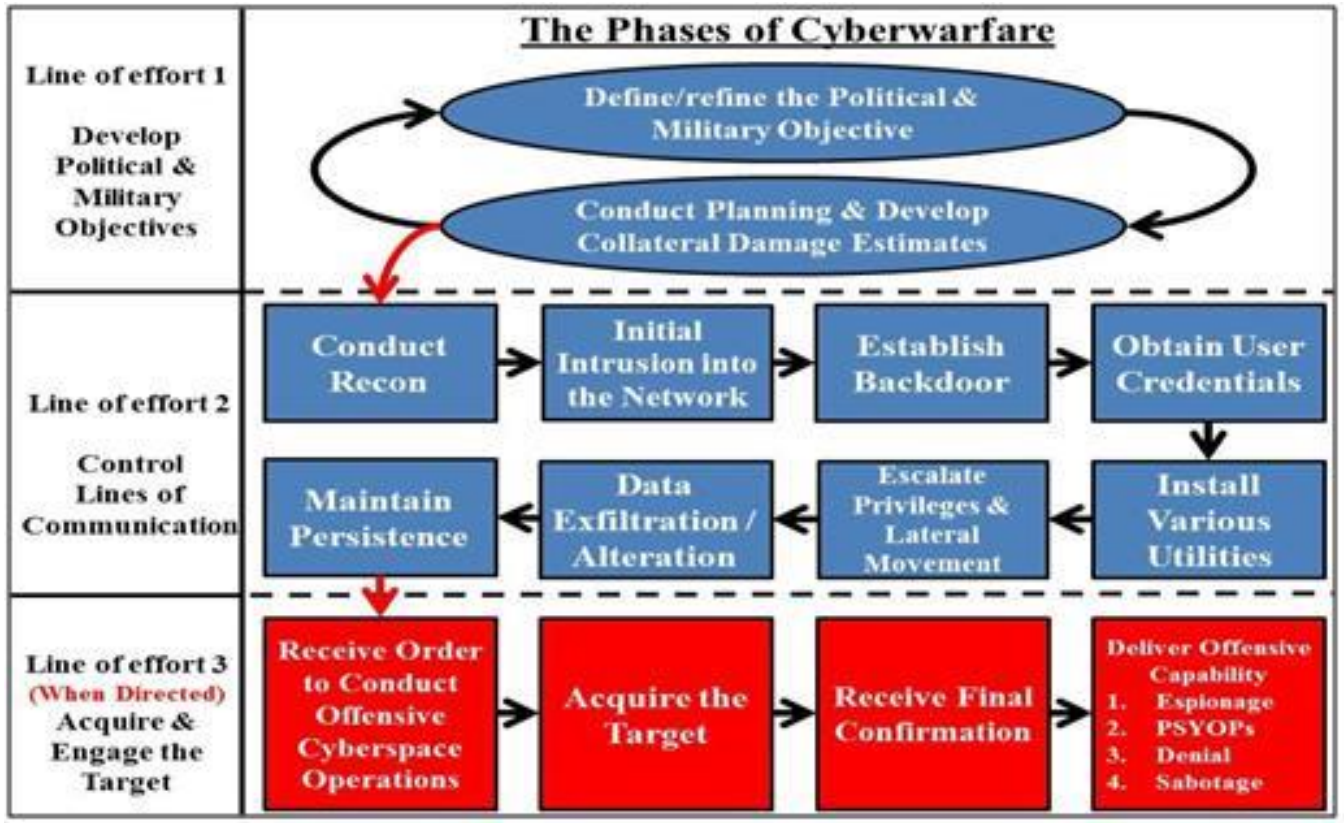
- adalah media elektronik dalam **jaringan komputer** yang banyak dipakai untuk keperluan komunikasi, **Dunia Maya/Cyber World** ini merupakan integrasi dari berbagai peralatan teknologi **komunikasi** dan **jaringan komputer** yang dapat menghubungkan peralatan komunikasi (komputer, telepon genggam, instrumentasi elektronik, dan lain-lain) yang tersebar di seluruh penjuru dunia.

Cyber Crime

- adalah istilah yang mengacu kepada **aktivitas kejahatan** dengan komputer atau **jaringan komputer** menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dll.

Cyber Warfare

- Cyber Warfare ini bisa kita artikan sebuah serangan dari pihak 1 ke pihak lainnya (perang)



Cyber Threats

- Cyber Threats atau ancaman yang ada didalam dunia maya ini ada berbagai macam, salah satunya:
  - Pencurian Data
  - Pemalsuan
  - Pornografi
  - Penipuan
  - Perang
  - Teror
  - Virus
  - **Penyandraan Data & Pemerasan (RANSOMWARE)**

Chapter 5 – Summary

- Cyber World/Dunia Maya: sebuah dunia digital yang dibangun diatas **jaringan komputer** dan digunakan untuk berkomunikasi
- Cyber Crime: Kejahatan dunia maya
- Cyber Warfare: Perang dunia maya
- Cyber Threats: Ancaman dunia maya

Chapter 6
Introduce to “Ransomware Attack Trends 2017”

Introduce to Ransomware

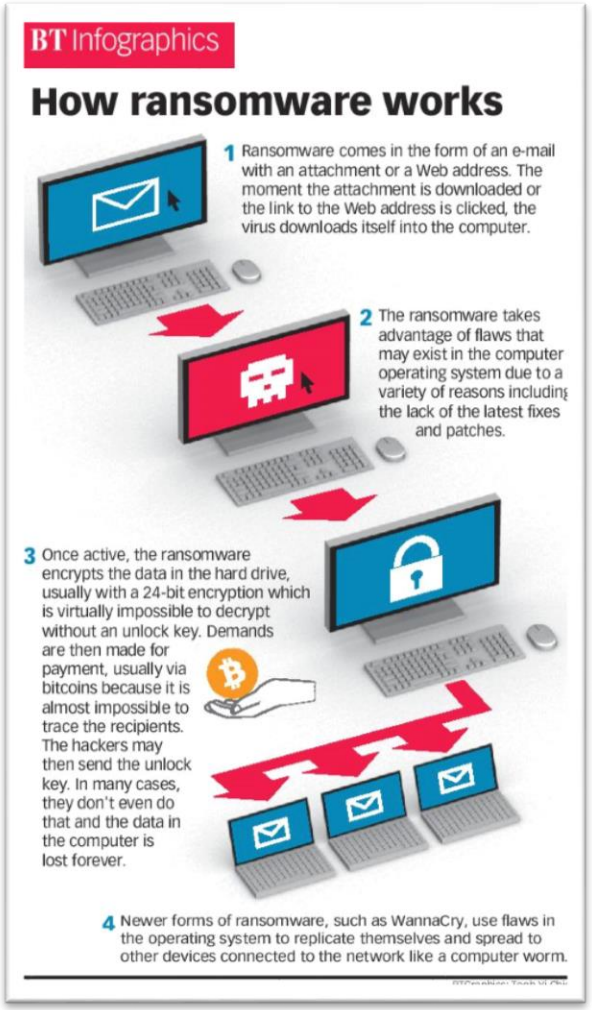
- **Perangkat pemeras** (*ransomware*) adalah jenis perangkat perusak yang dirancang untuk menghalangi akses kepada sistem komputer atau data hingga tebusan dibayar. Jenis yang sederhana bekerja dengan mengunci sistem dengan cara yang tidak sulit untuk ditangani oleh orang yang ahli, sedangkan jenis yang lebih canggih akan mengenkripsi berkas sehingga tidak dapat diakses. Serangan perangkat pemeras umumnya dilakukan melalui Trojan yang disamarkan sebagai berkas yang sahih.

  - Wikipedia Indonesia

Ransomware Trend Q2’2017 (**WannaCry**pt)

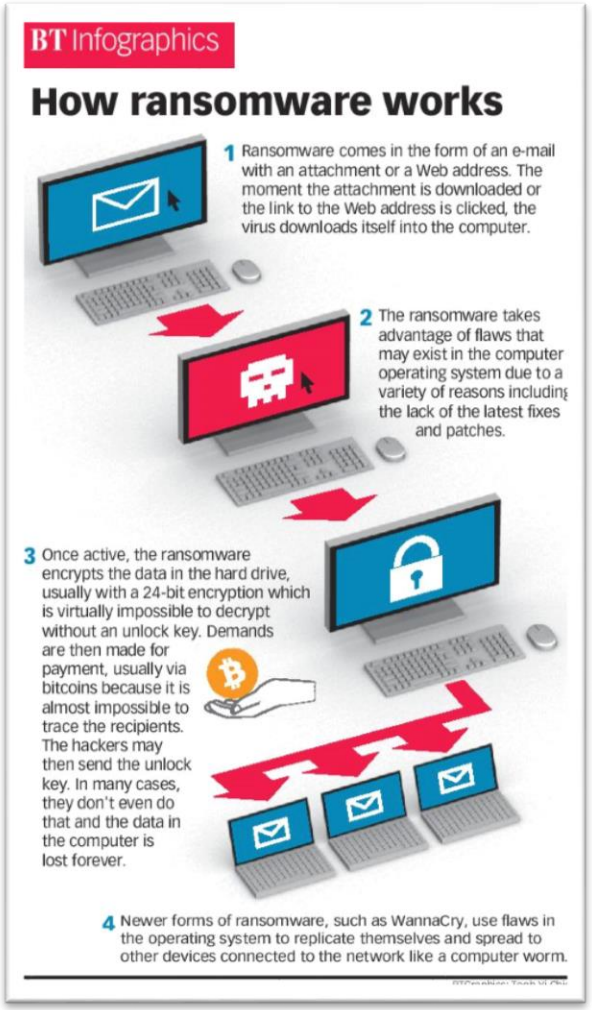
~~Ransomware~~ Trend Q3’2017 (Petya)

How They Works? (1)



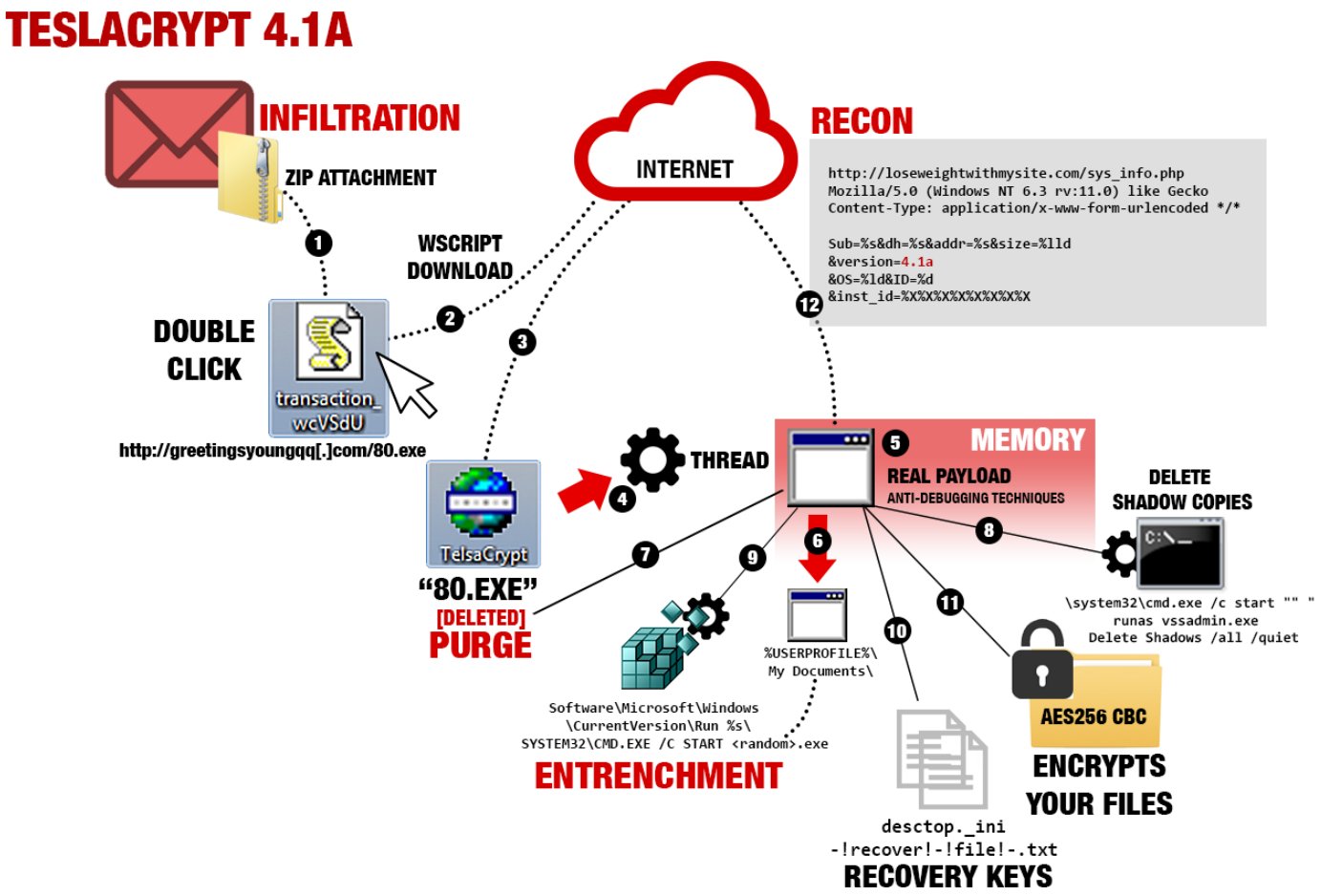
1. Ransomware comes in the form of an e-mail with an attachment or a web address. The momeny the attachment is downloaded or the link to the Web address is clicked, the virus downloads itself into the computer
2. The ransomware takes advantage of flaws that may exist in the computer operating system due to a variety of reasons including the lack of the latest fixes and patches

How They Works? (1)

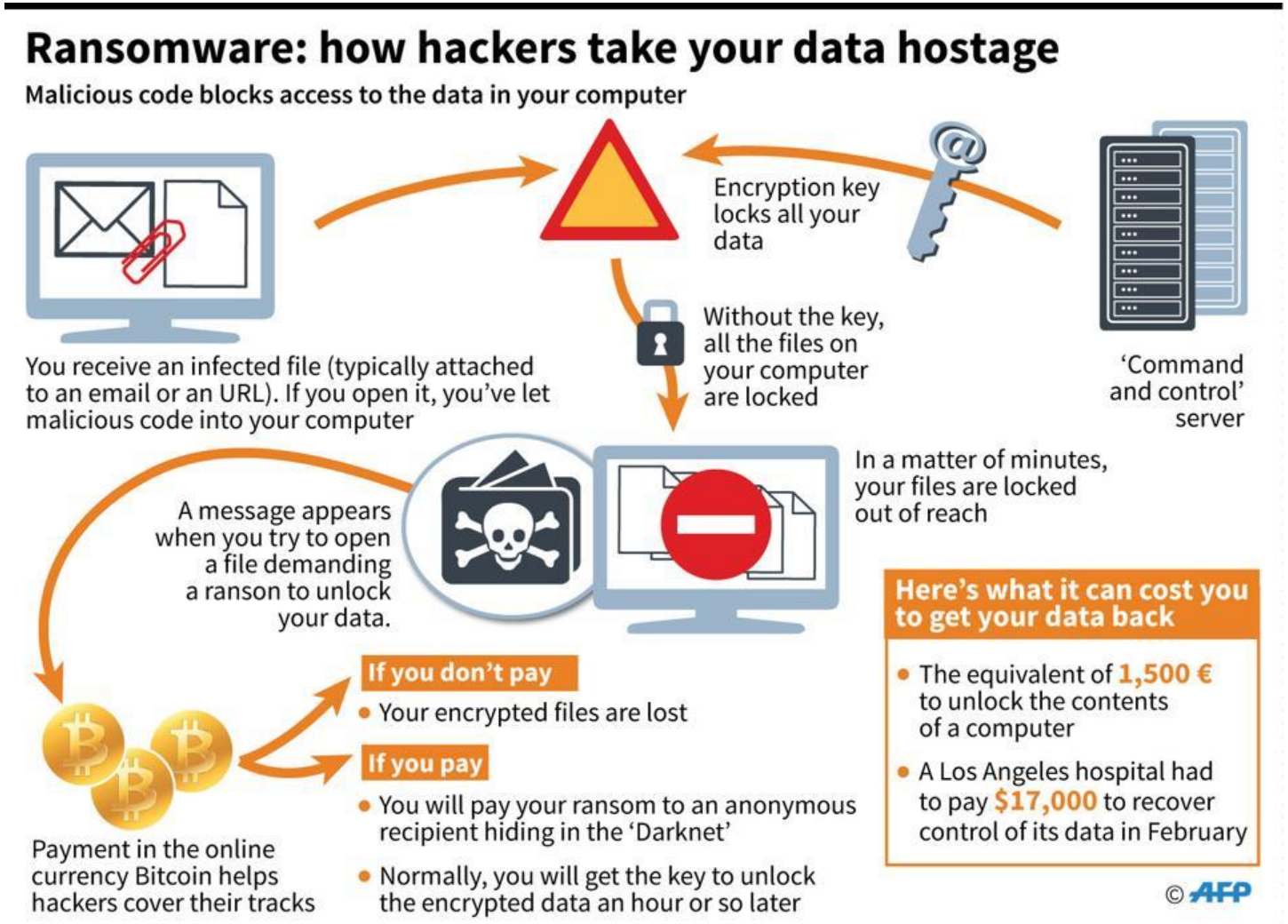


3. Once active, the ransomware encrypts the data in the hard drive, usually with a 24-bit encryption which is virtually impossible to decrypt without an unlock key. Demands are then made for payment, usually via bitcoins because it is almost impossible to trace the recipents. The hackers may then send the unlock key. In many cases, they don't even do that and the data in the computer is lost forever
4. Newer forms of ransomware, such as WannaCry, use flaws in the operating system to replicate themselves and spread to other devices connected to the network like a computer worm

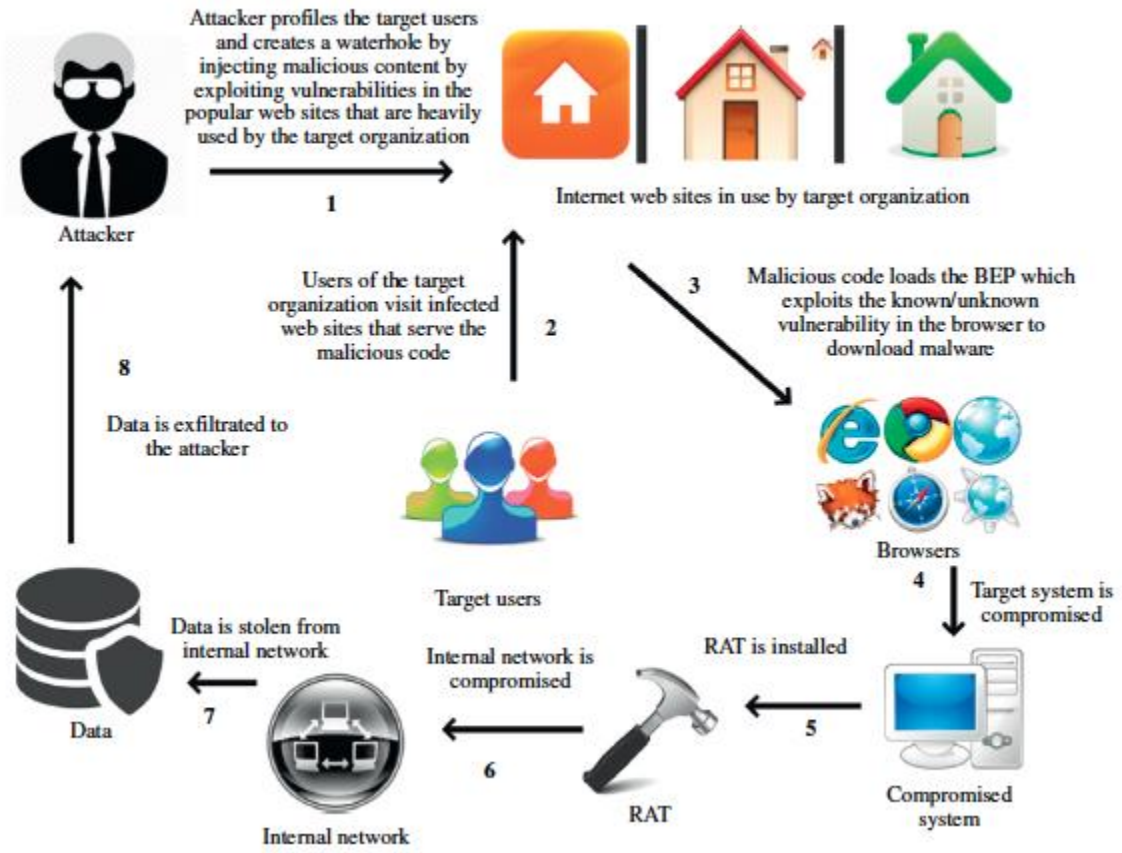
How They Works? (2)



How They Works? (3)



How They Works? (4)



Chapter 6 – Summary

- Banyak sekali refrensi cara kerja dari ransomware tersebut, namun dari itu semua bisa kita simpulkan bahwa tujuan utama dari ransomware ini adalah **Menyandra Data Kita** dan **Memeras** kita dengan **Uang**
- Dan dapat kita simpulkan juga bahwa ransomware ini masuk dan disisipkan melalui aplikasi yang kita download di **internet**
- Ketika ransomware ini sudah **ter-unduh/ter-download** dan **berjalan** maka ransomware ini akan **meng-enkripsi** semua data kita dan **memeras** kita dengan sejumlah **uang** yang dikirim melalui **bitcoin**
- Untuk ~~ransomware~~ **Petya** anda harus berhati – hati, karena ada rumor bahwa ini bukanlah ransomware melainkan malware yang menghapus bersih data anda meskipun anda sudah membayar dengan sejumlah uang
- Untuk ransomware jenis baru seperti **WannaCry**pt, mereka akan menyebar jaringan komputer kita dan akan merusak host lain melalui... (Lanjut Chapter 7)

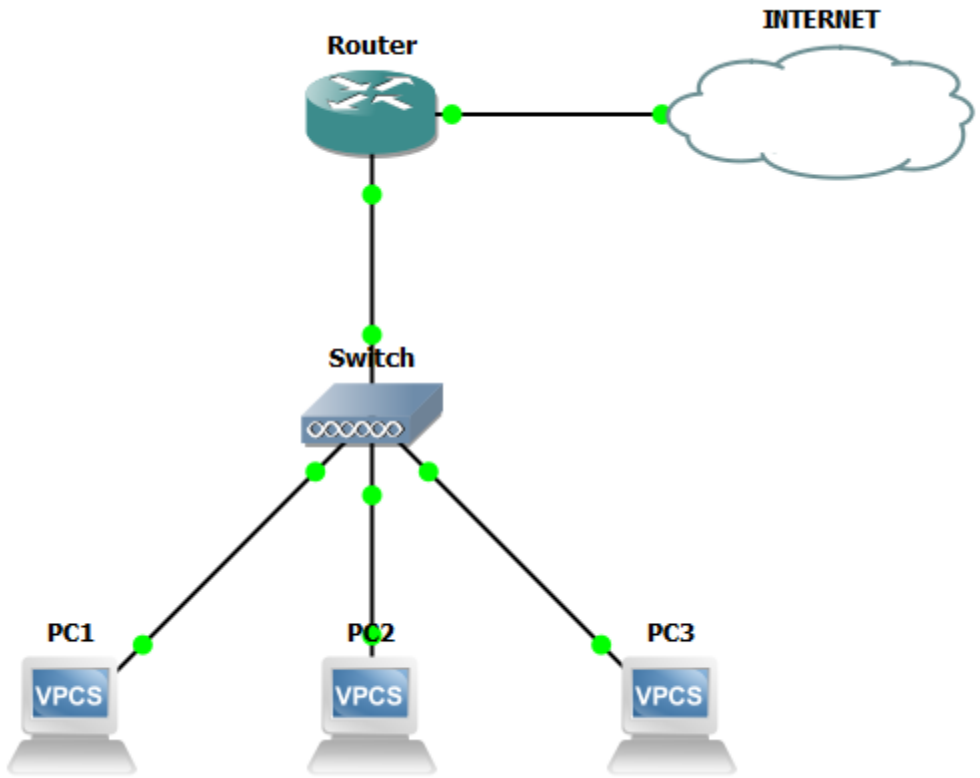
Chapter 7
How WannaCrypt Infecting Our Networks

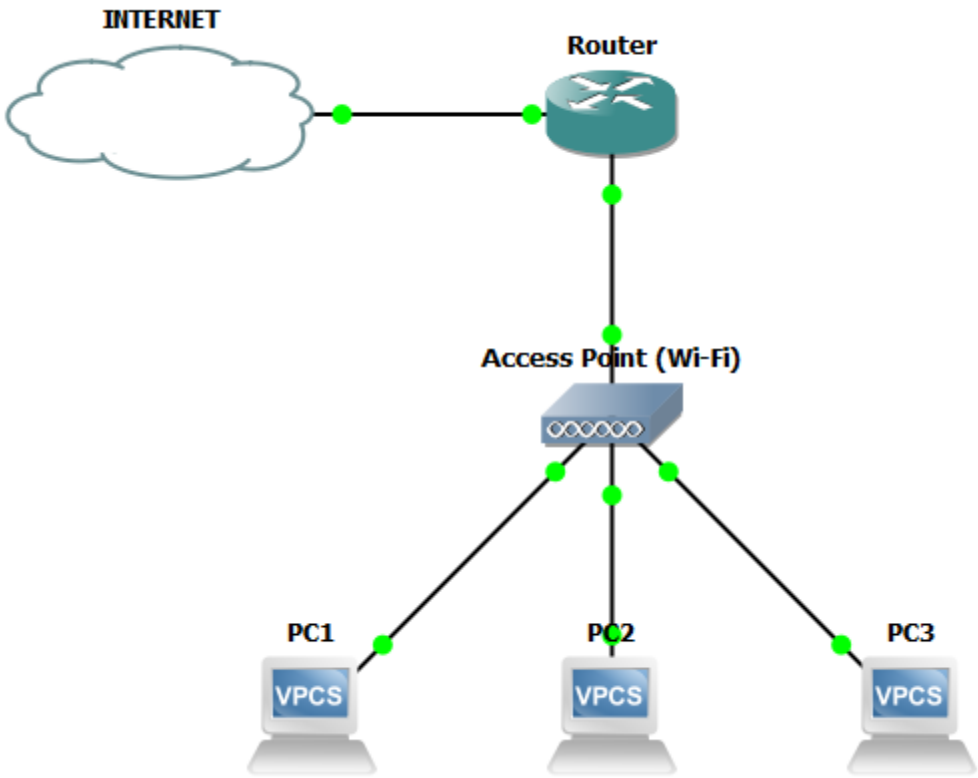
WannaCrypt?

- The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

  - Wikipedia

Back to Commonly LAN Topology



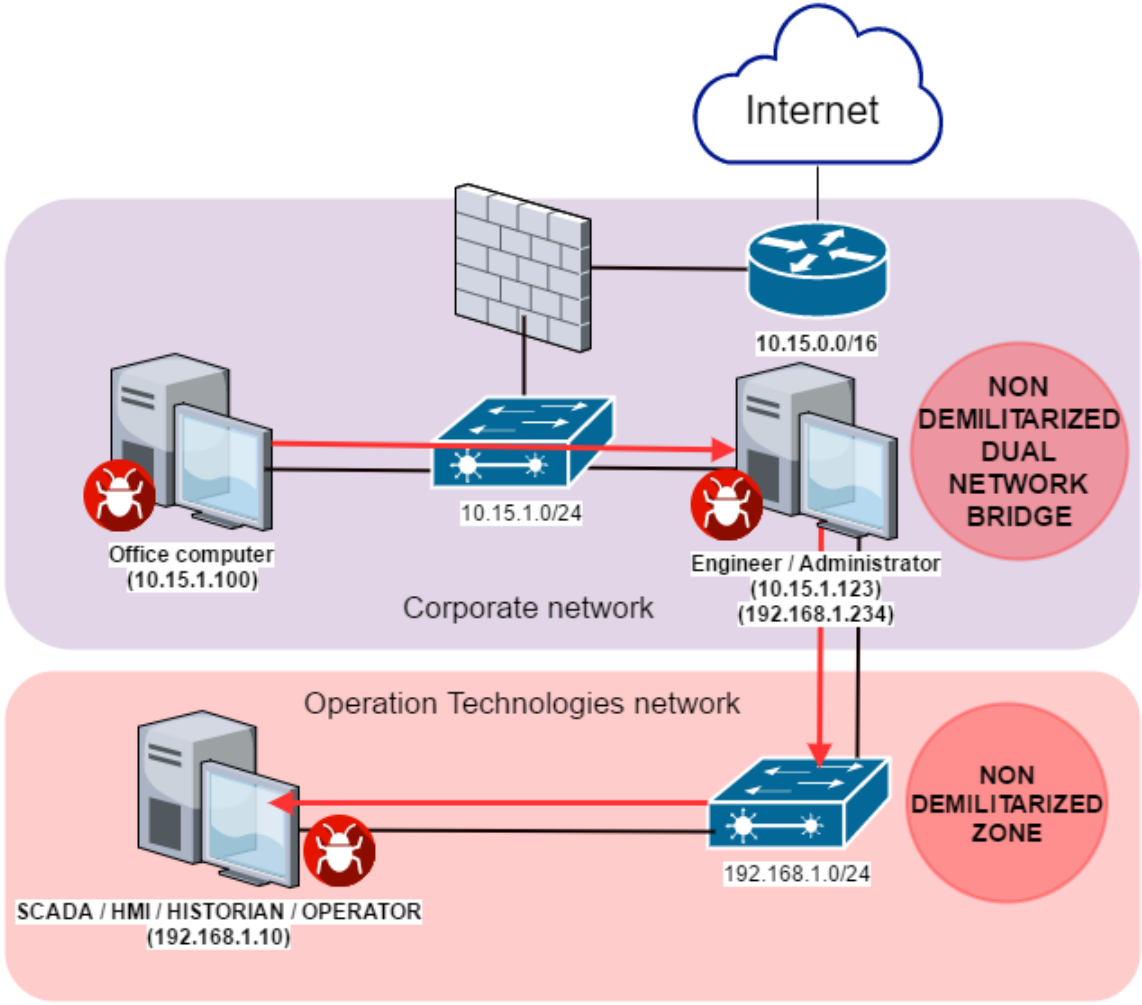


The Problem

- Commonly Network Administrator only do Filtering in Router
- The Ransomware Spread via The Switch, Not Passing the Router (For 1 Network)
- The Ransomware Spread via Remote Desktop Protocol (RDP for Remote Desktop)
- The Ransomware Spread via Server Message Block (SMB Protocol for File Sharing)
- Commonly Switch are no manageable and cannot be installed some firewall role inside

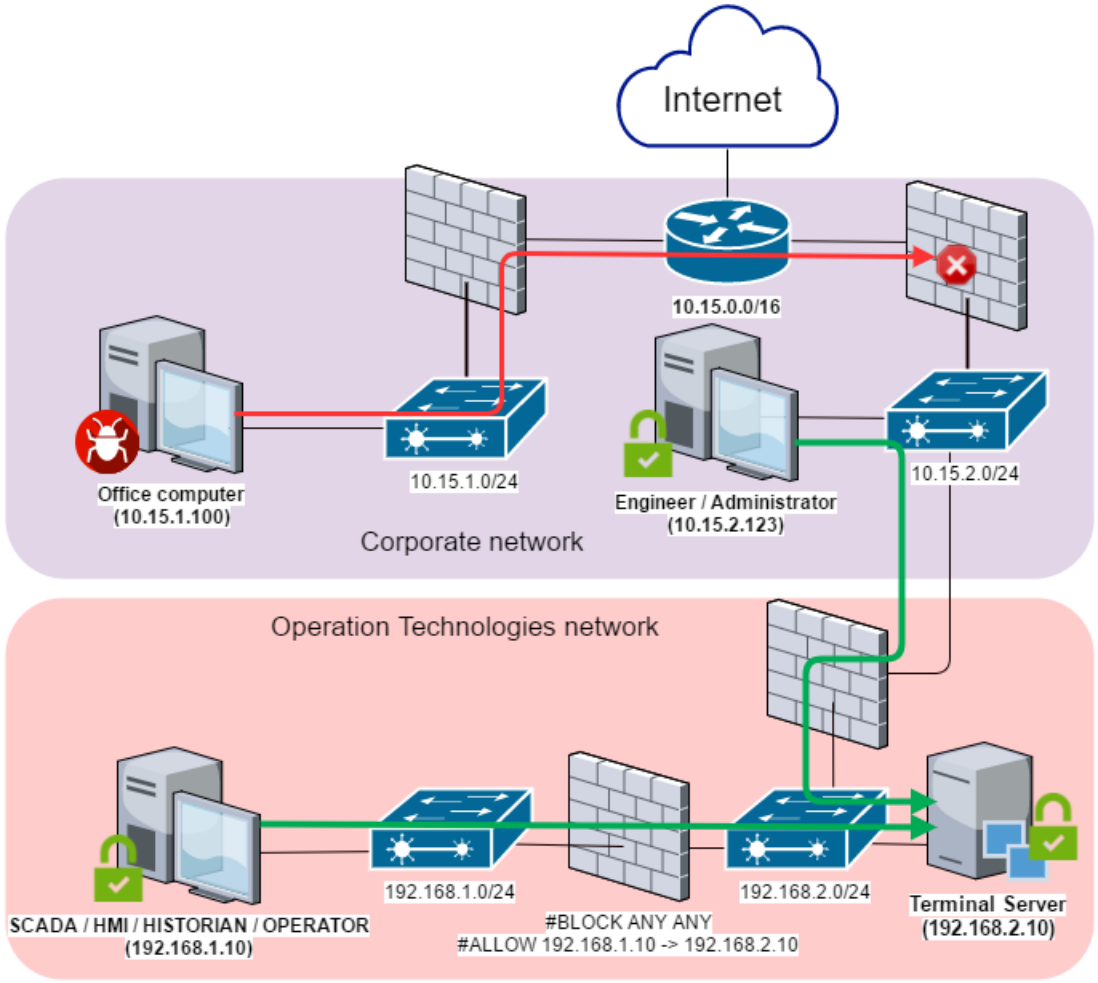
WannaCrypt Spreading Scenario (From Karspersky)

Use of computers acting as bridges between several networks



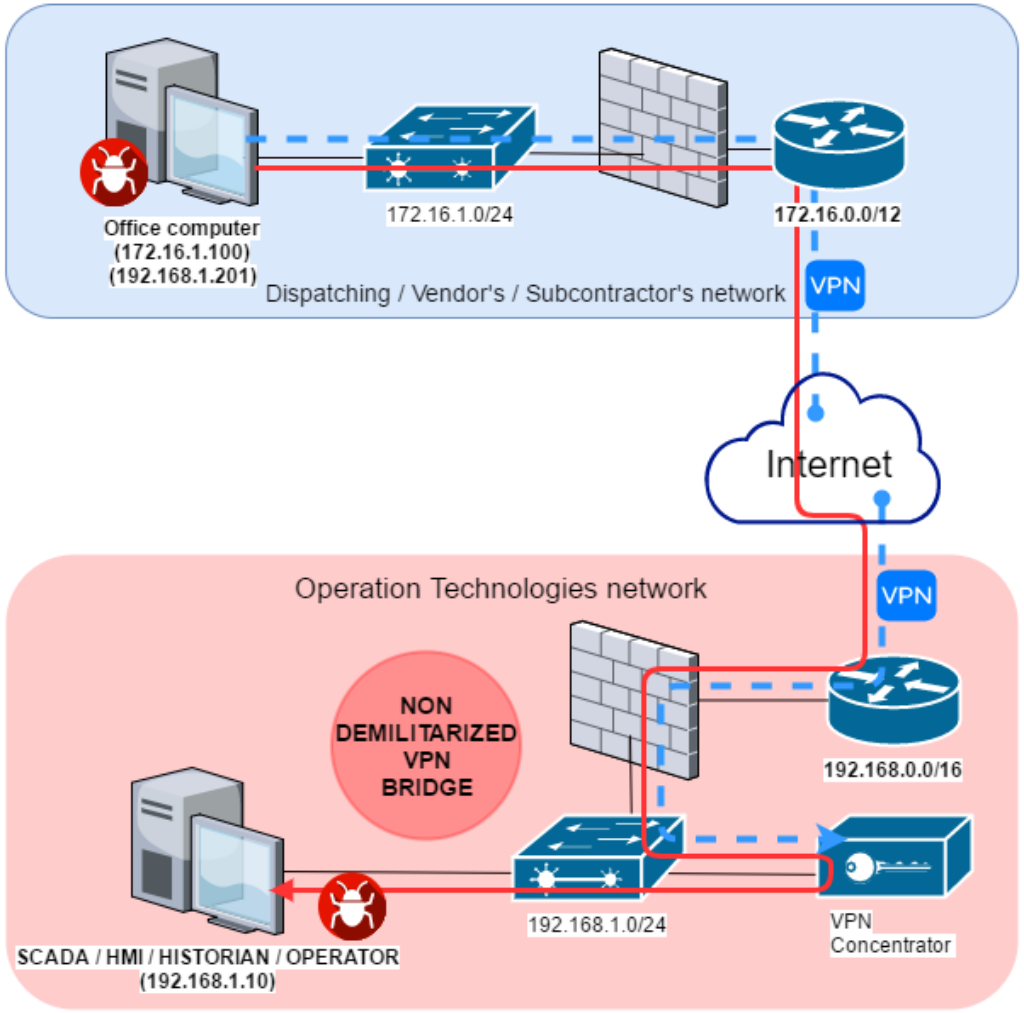
WannaCrypt Spreading Scenario (From Karspersky)

Connecting remote facilities



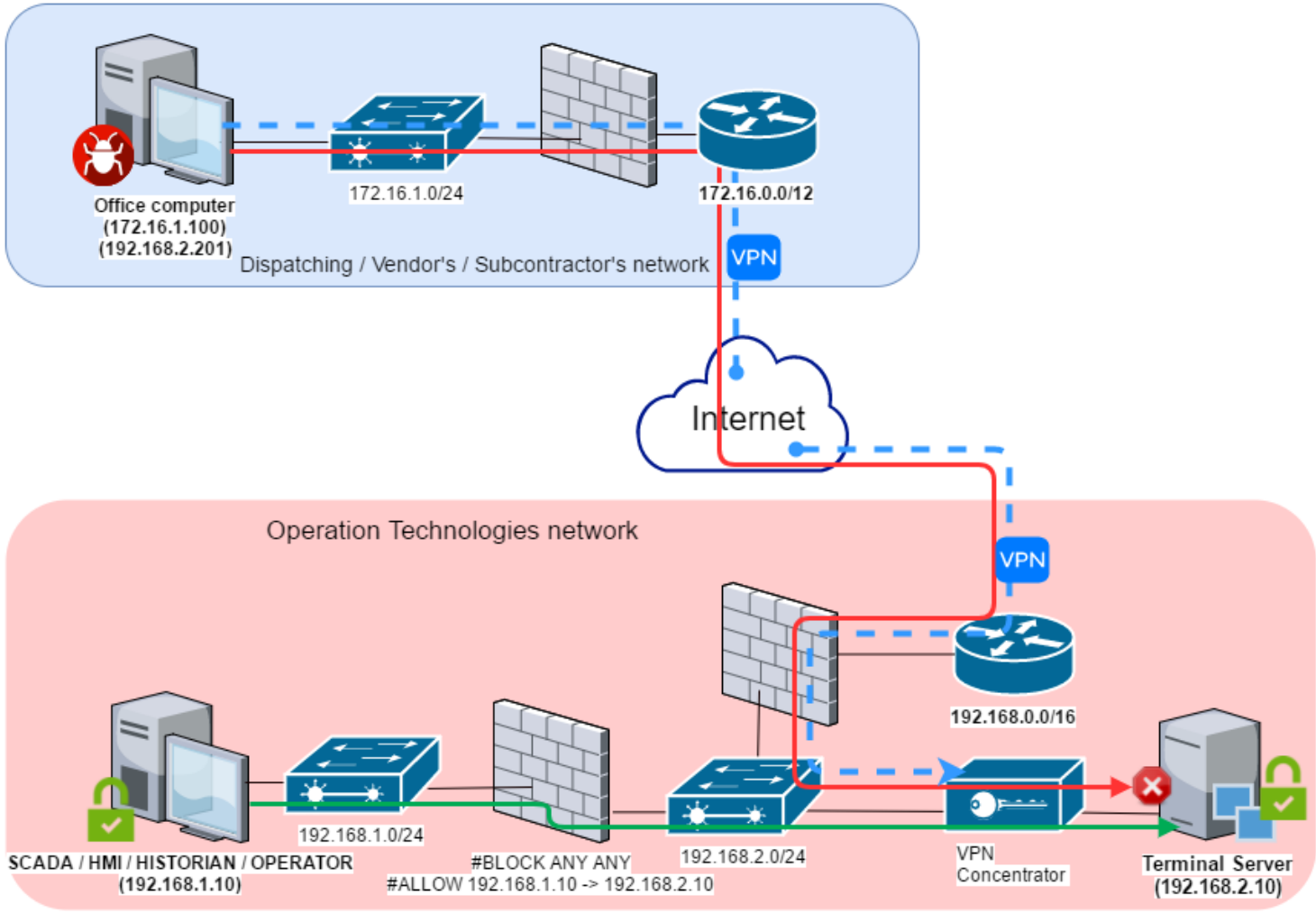
WannaCrypt Spreading Scenario (From Karspersky)

Connecting remote facilities



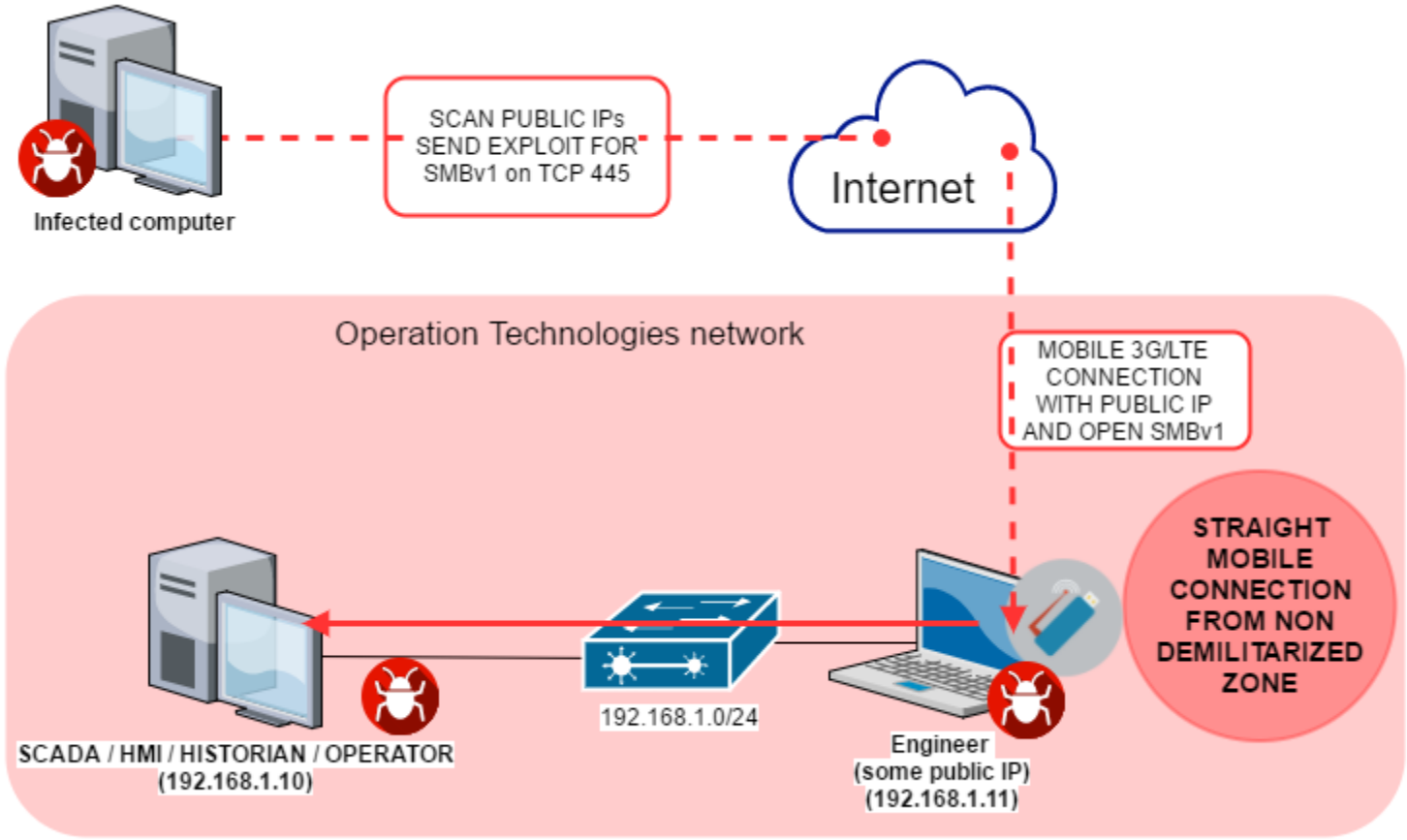
WannaCrypt Spreading Scenario (From Karspersky)

Connecting remote facilities



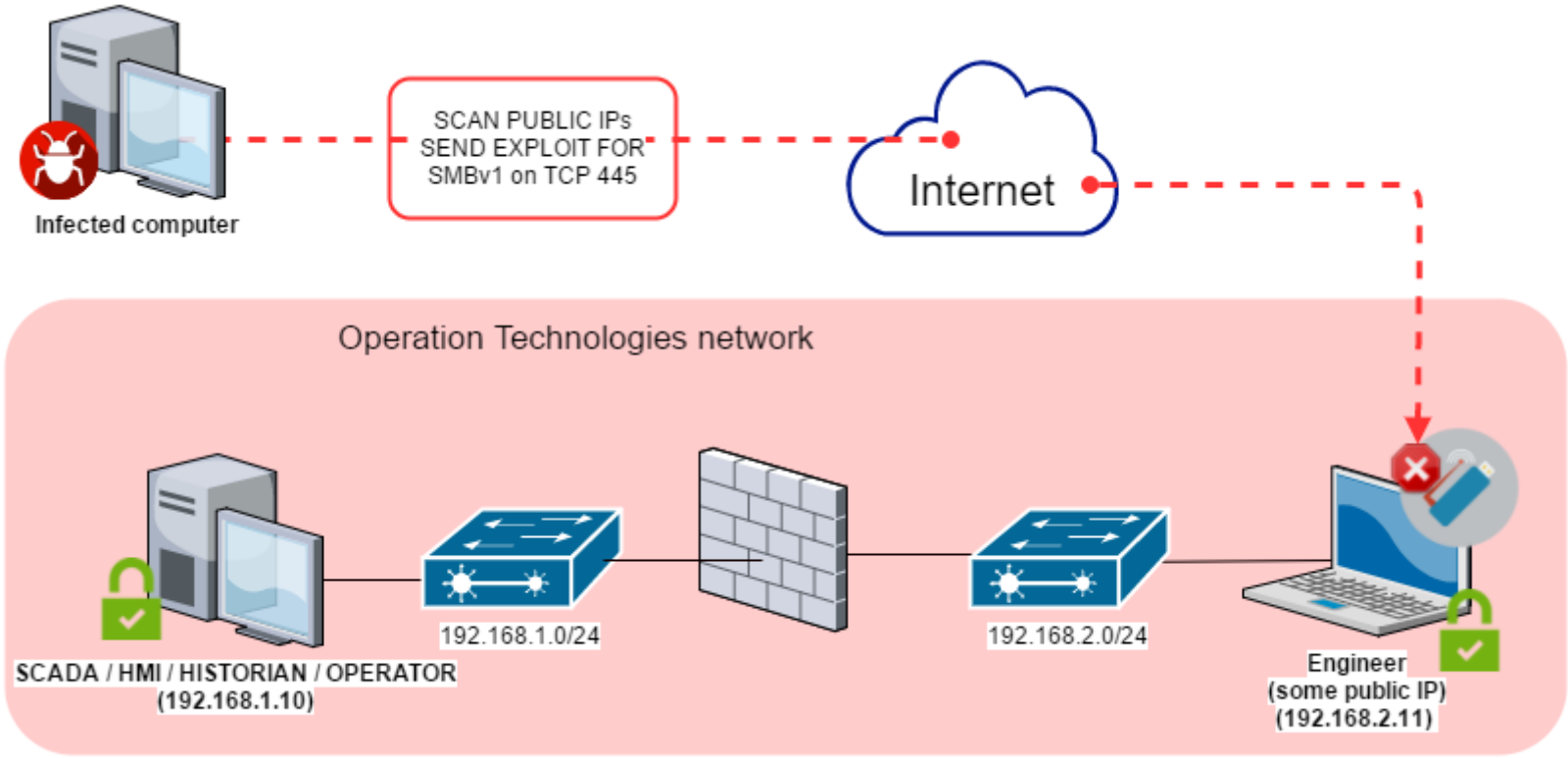
WannaCrypt Spreading Scenario (From Karspersky)

Using modems and mobile phones



WannaCrypt Spreading Scenario (From Karspersky)

Using modems and mobile phones



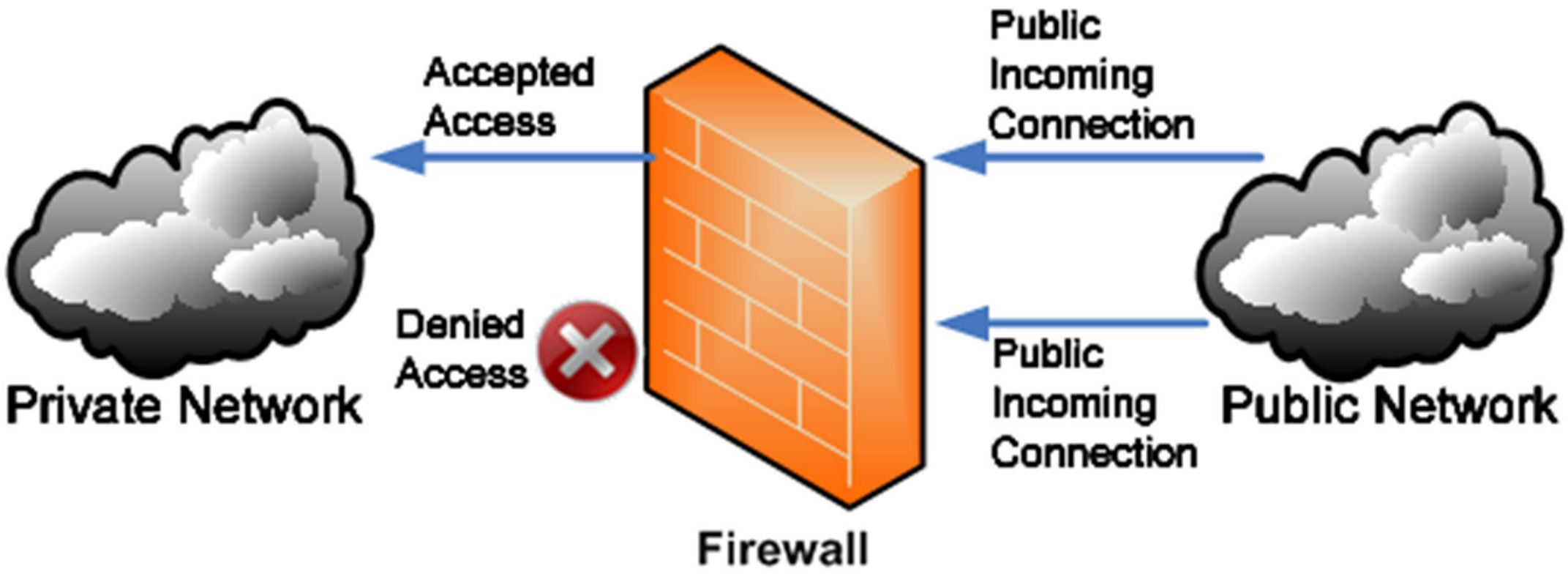
Chapter 7 – Summary

- Pada intinya, ransomware ini menyebar didalam jaringan yang didalamnya ada host yang sudah terinfeksi ransomware terlebih dahulu dan mulai menyebar melalui protokol file sharing (SMB) dan protokol remote desktop (RDP)
- Bisa tidak menyebar kejaringan lain? Jika tidak ada filtering? iya

Chapter 8
WannaCrypt Preventions & Conclusions

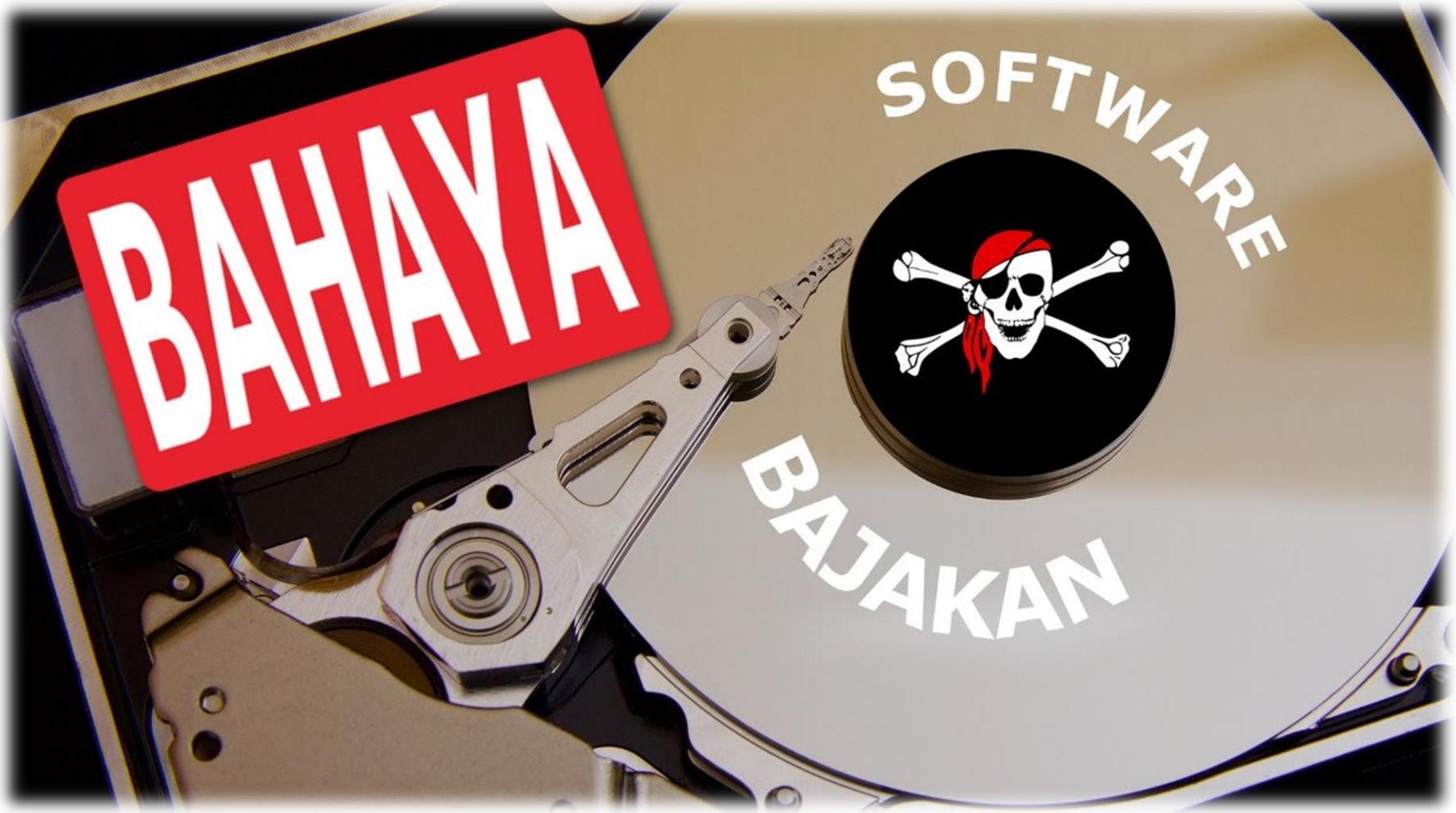
Ransomware Prevention

Ransomware Prevention



Ransomware Prevention

Ransomware Prevention



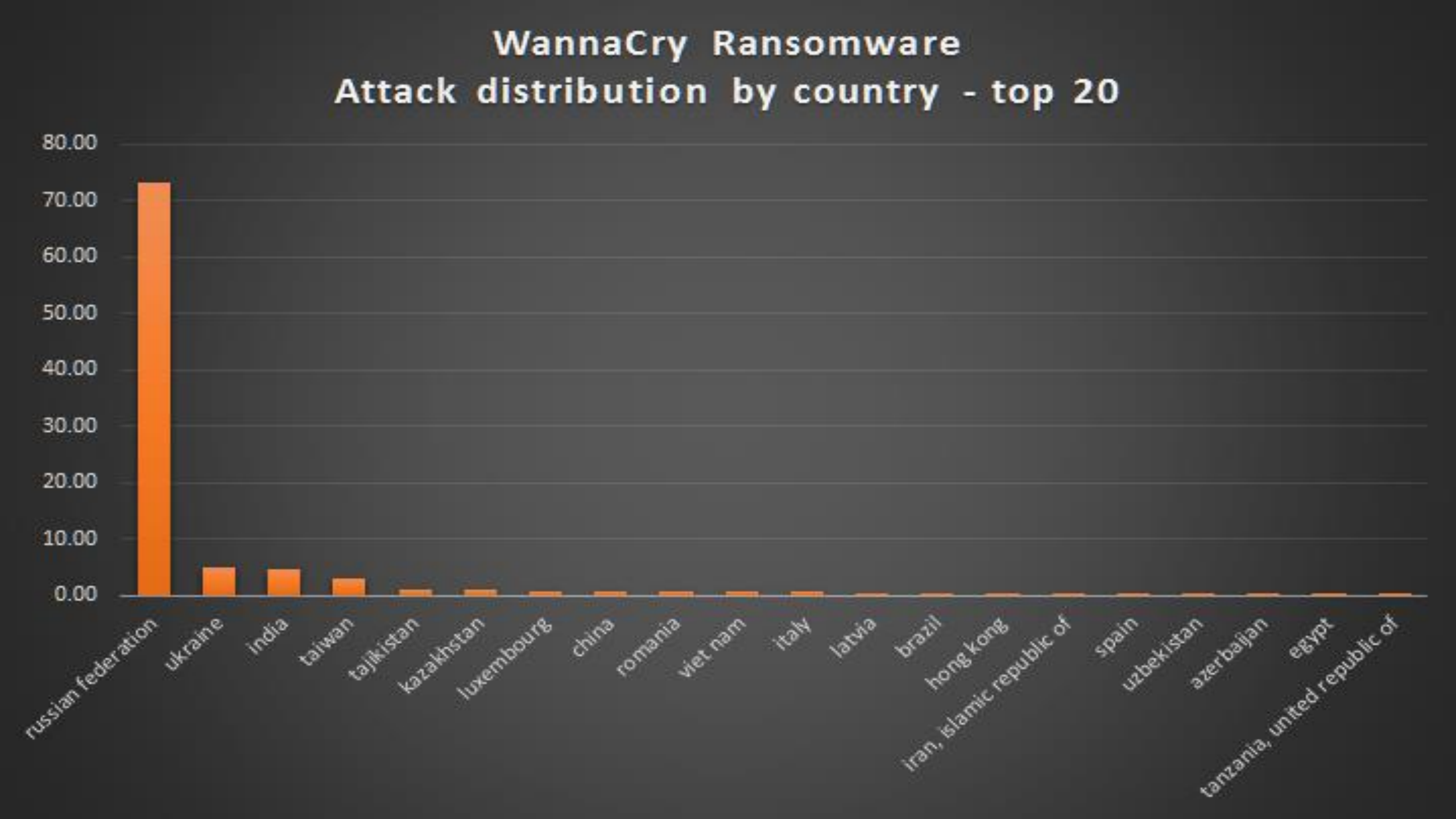
Ransomware Prevention

Ransomware Prevention

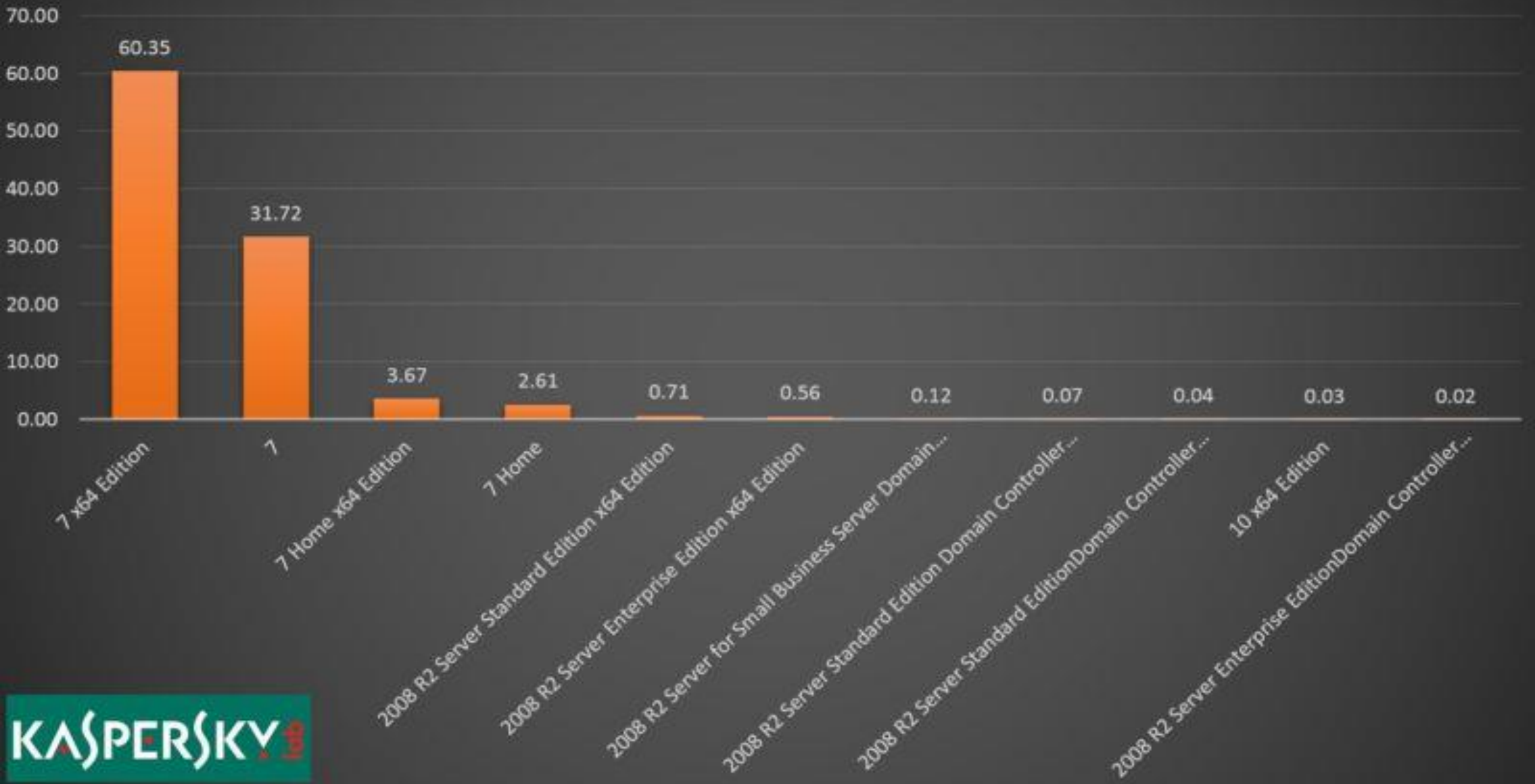
Ransomware Prevention

Ransomware Conclusions

- Ransomware ini telah membuktikan dirinya dengan dampak yang ditimbulkan, maka dari itu kita harus “meng-upgrade diri kita” namun bisa kita simpulkan melalui statistik yang saya dapatkan dari https://arstechnica.com dislide selanjutnya ini, bahwa penanganan dan respon masyarakat indonesia sudah cukup baik terhadap keamanan informasi namun ada baiknya kita tetap waspada setiap saat


WannaCry Ransomware
Attack distribution by country - top 20
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
russian federation
ukraine
india
taiwan
tajikistan
kazakhstan
luxembourg
china
romania
viet nam
italy
latvia
brazil
hong kong
iran, islamic republic of
spain
uzbekistan
azerbaijan
egypt
tanzania, united republic of

Wannacry: Affected Windows Versions by %



KASPERSKY

Chapter 8 – Summary

WannaCry

Screenshot of the ransom note left on an infected system

Date	12 May 2017 – 15 May 2017 (initial outbreak)[1]
Location	Worldwide
Also known as	Transformations: Wanna → Wana Cryptor → Crypt0r Cryptor → Decryptor Cryptor → Crypt → Cry Addition of "2.0" Short names: Wanna → WN → W Cry → CRY
Type	Cyberattack
Theme	Ransomware encrypting files with $300 – $600 demand (via bitcoin)
Cause	WannaCry worm
Outcome	Over 200,000 victims and more than 300,000 computers infected[2][3][4]

- Bisa kita simpulkan bahwa ransomware ini cukup berbahaya sehingga seluruh dunia yang terhubung kedalam jaringan ini terkena dampak darinya, kita tetap harus berhati – hati

Date	12 May 2017 – 15 May 2017 (initial outbreak)[1]
Location	Worldwide

WannaCry

Screenshot of the ransom note left on an infected system

Date	12 May 2017 – 15 May 2017 (initial outbreak)[1]
Location	Worldwide

Chapter 9
End of The Presentation

Additional Information

- Sebagian besar dari gambar didalam presentasi ini diambil dari internet (*Google Images, Wikipedia, Kaspersky, Ars Technica, dll.*)
- Presentasi ini dibuat untuk dipresentasikan didalam kegiatan "***XENOVOLUTION 3.0; Seminar IT***" yang bertemakan "***Improve cyber security for the better future***" dan disellenggarakan oleh **Badan Eksekutif Mahasiswa Fakultas Farmasi & Sains Universitas Muhammadiyah Prof Dr Hamka** pada tanggal **23 Juli 2017**

Additional Reads & Course

- https://ics-cert.kaspersky.com/reports/2017/06/22/wannacry-on-industrial-networks/
- Computer Network Certification (MikroTik, Cisco, UBNT, Juniper, dll)
- Computer Security Certification (OffSec, EC-Council, SANS, dll)
- https://mum.mikrotik.com/archive?lang=EN
- https://wiki.mikrotik.com/wiki/Main_Page
- http://www.juniper.net/documentation
- http://www.cisco.com/c/en/us/support/index.html
- http://www.ciscopress.com
- https://www.wikipedia.org
- https://www.youtube.com

Feel So Hard To Securing & Hardening Your Network?
Let Me Help You !
michael@takeuchi.id
http://www.facebook.com/mict404

Are we done? I don’t know ☺
humans always have unexpected things

One More Things !


Thank
you