



Keamanan Informasi dan Interoperabilitas Sistem Informasi RS dalam Era Endemi Covid-19 dan Revolusi Industri 4.0

Obrina Candra Briliyant, MT, CISA, CDPSE, CySA+, CSXF, ISO27001-LA, CyberOps
Politeknik Siber dan Sandi Negara, BSSN

Hospital Engineering Forum 2021
Indonesian Association Hospital Engineering



Curriculum Vitae

Nama: Obrina Candra Briliyant

Pendidikan:

- Akademi Sandi Negara
- Teknik Informatika ITB

Pengalaman bekerja :

- Lembaga Sandi Negara
- Kemenko Polhukam RI
- Badan Siber dan Sandi Negara

Pengalaman organisasi :

- ISACA Indonesia Chapter
- Ikatan Auditor Sistem Informasi Indonesia

OUTLINE

01 Lanskap Ancaman

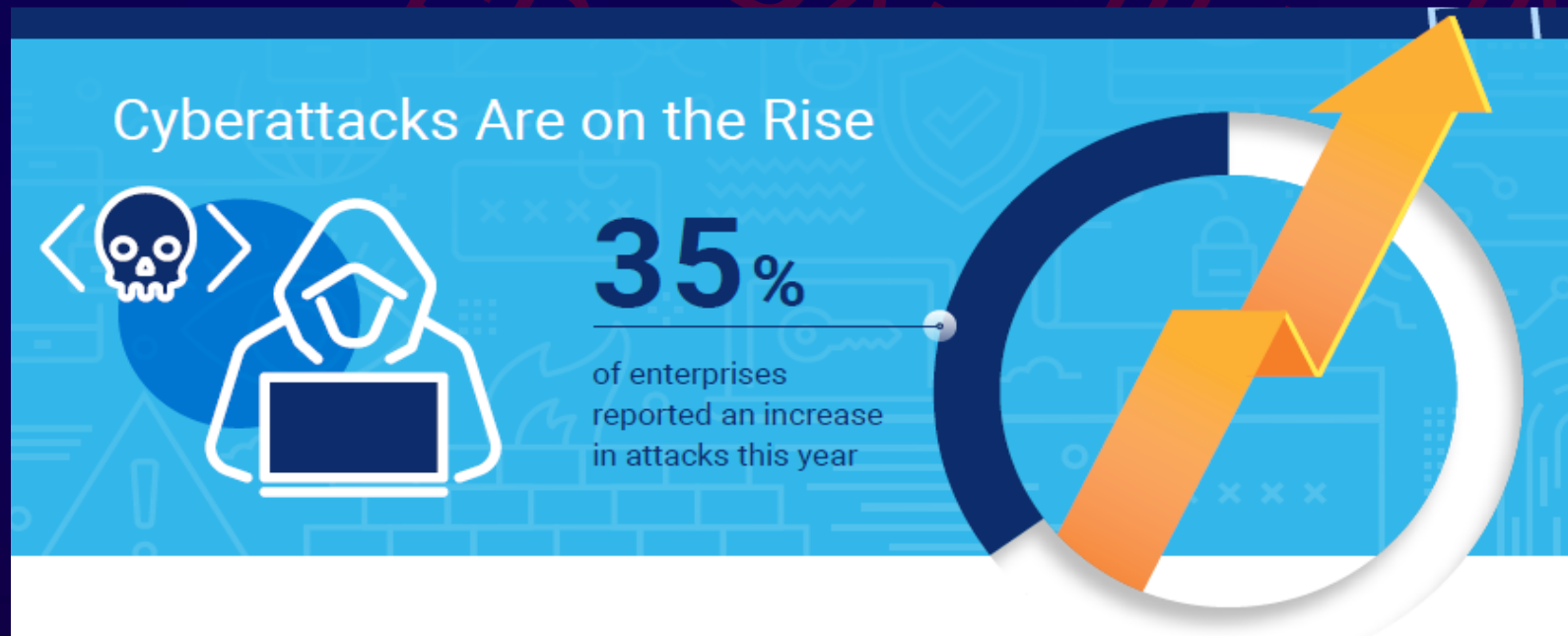
02 Tantangan 4.0

03 Rekomendasi

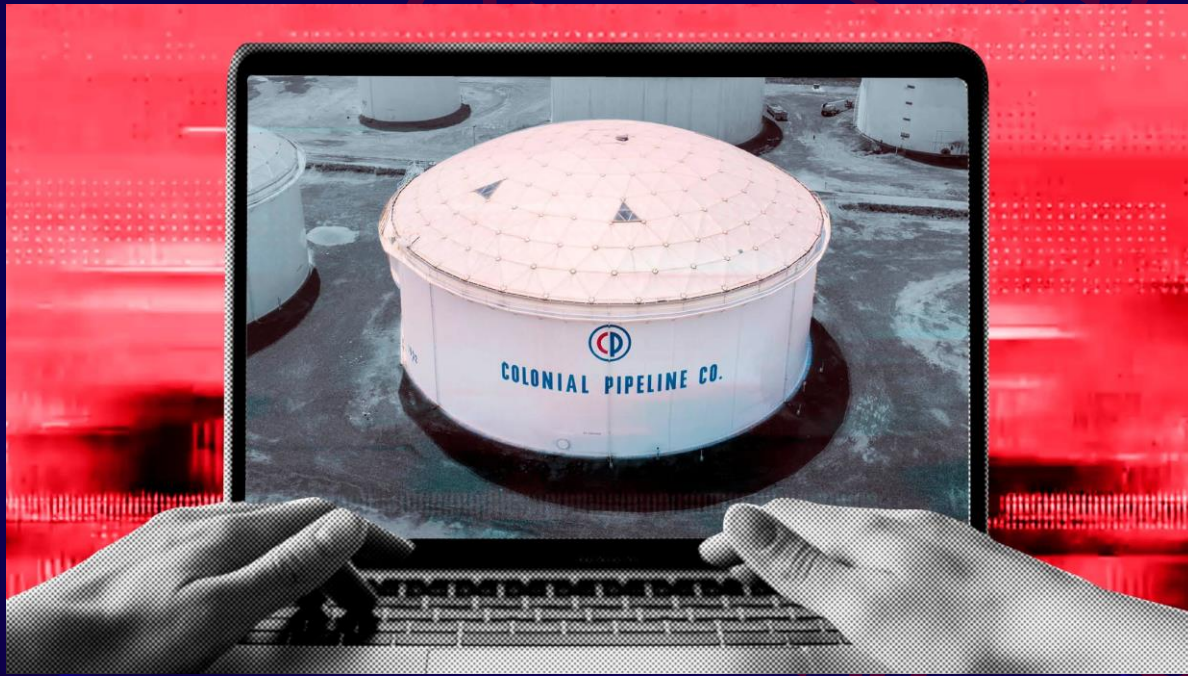
DIS
DIS
1

Lanskap Ancaman

ISACA *State of Cybersecurity 2021* melihat pada tren ancaman, dampak pandemi pada program keamanan, serta pentingnya menilai kematangan *cybersecurity*. Banyak dari temuan ini akan memperkuat tantangan lama & baru yang dihadapi organisasi di tengah pandemi global yang sedang berlangsung dan aktor ancaman oportunistik.



- 1 dari 3 organisasi mengalami lebih banyak serangan siber tahun ini
- tiga poin lebih tinggi dari tahun lalu



- di mana ada konektivitas, ada risiko serangan siber
- Serangan langsung pada teknologi operasional (OT/ICS, SCADA) jarang terjadi karena sistem ini biasanya lebih terlindungi
- Kemungkinan besar peretas memperoleh akses ke sistem komputer melalui sisi administratif bisnis

Some of the biggest attacks we've seen all started with an email

- Colonial Pipeline dilaporkan membayar US\$4,4 juta sebagai tebusan kepada para aktor DarkSide.
- Perusahaan memiliki asuransi cyber dengan Lloyd's dan Beazley, yang menanggungnya setidaknya US\$15 juta.
- Pada 2019, Norsk Hydro menerima US\$20,2 juta dalam asuransi siber dari AIG.
- Laporan keamanan tahun 2020 dari Cybereason menunjukkan bahwa 80% organisasi yang membayar uang tebusan, mengalami serangan kedua.



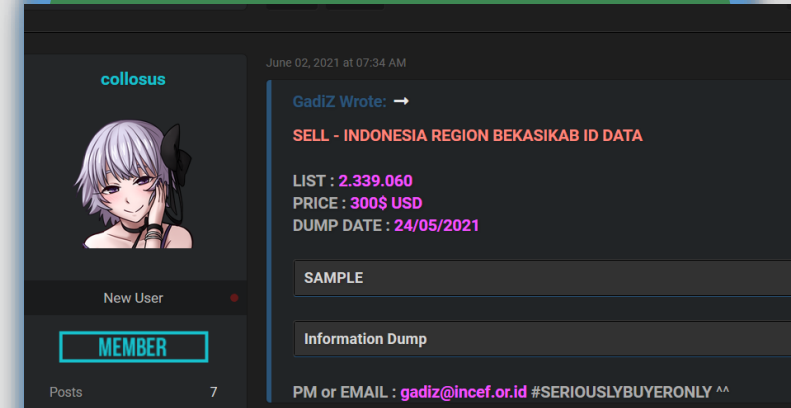
INSIDEN SIBER DI INDONESIA



Isu kebocoran data warga Indonesia yang diduga merupakan data BPJS Kesehatan pertama kali mencuat di media sosial pada **Kamis (20/5/2021)**. Data itu dipublikasikan dan dijual di salah satu forum online.



Juli 2021, Data nasabah asuransi BRI Life diduga bocor dan dijual di darkweb. Dalam unggahan sampel data, disertakan screenshot yang berisi data milik nasabah BRI Life, seperti KTP hingga rekam medis. Ditemukan bukti beberapa komputer milik karyawan BRI Life telah menjadi sarana hacker dalam melakukan pembobolan data ini.



Mei – Juni 2021, serangkaian laporan penjualan data hasil breach beberapa pemerintah daerah dan BUMD bermunculan di darkweb. Penjual mengklaim menjual data pribadi berupa nik, kk, dan nama ibu kandung.

Most Frequent Cyberattacks

experienced by respondents are:

- 1 14% Social engineering
- 2 10% Advanced persistent threat (APT)
- 3 9% Ransomware
- 3 9% Unpatched system
- 4 8% Denial of service (DoS)
- 4 8% Security misconfiguration



Top 5 of attacks are the same as last year

GLOBAL RANSOMWARE INCIDENTS



Top 5 Ransomware Actors Impacting Global HPH Sector 2021

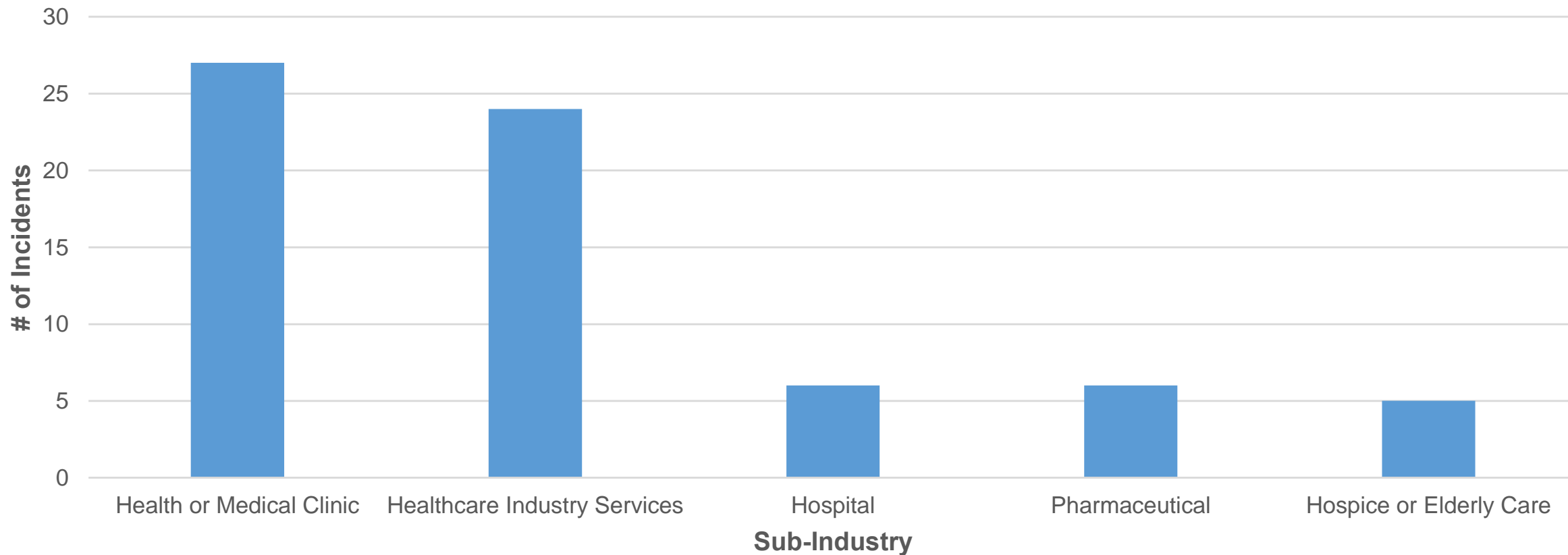
Place	RaaS Name	Number of Incidents
1	Avaddon RaaS Operator(s)	16
2	Conti RaaS Operator(s)	16
3	REvil/Sodinokibi RaaS Operator(s)	7
4	Mespinoza/Pysa RaaS Operator(s)	6
5	Babyk RaaS Operator(s)	5

RaaS -> Ransomware as a Service

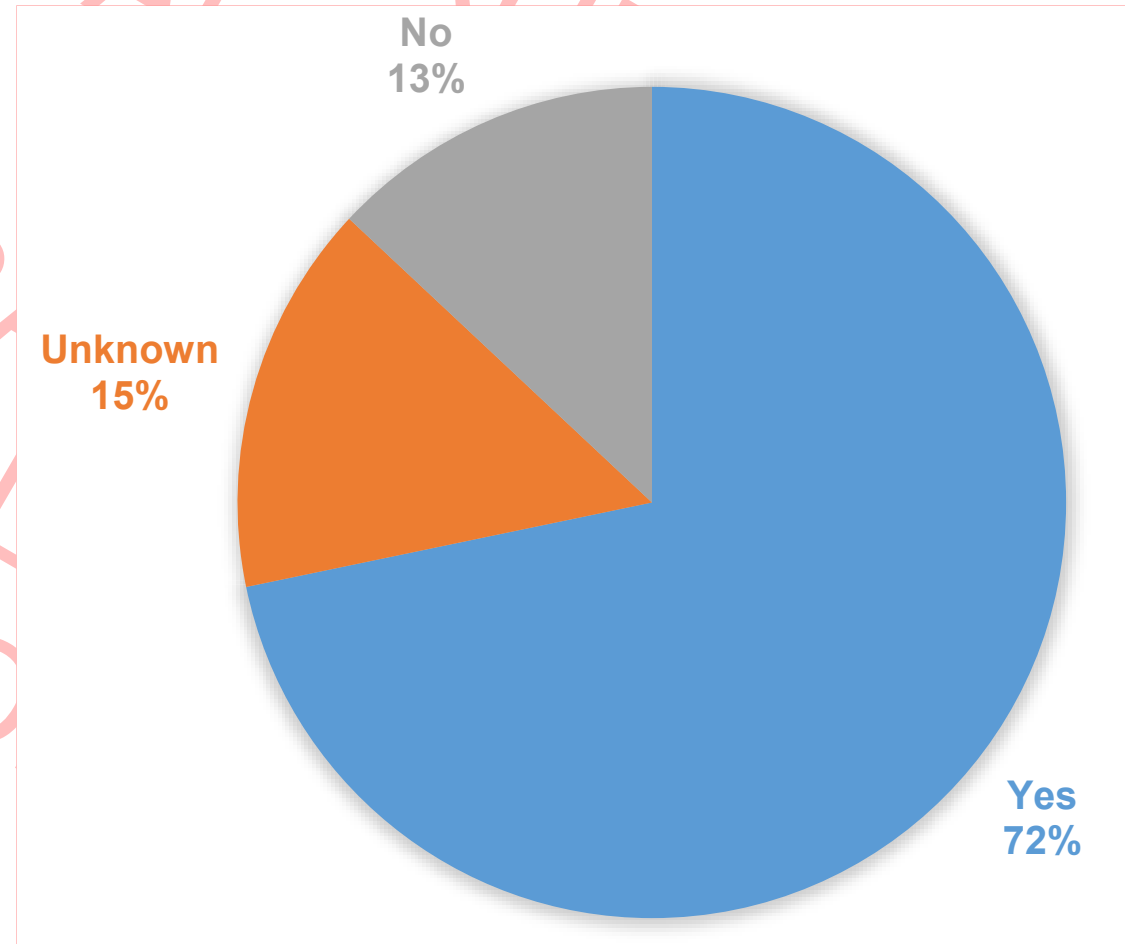
<https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf>

- Health Sector Cybersecurity Coordination Center (HC3) dibuat oleh Departemen Kesehatan AS untuk membantu perlindungan informasi kesehatan (e-PHI) di seluruh Sektor Kesehatan dan Kesehatan Masyarakat/*Health and Public Health Sector* (HPH).
- Karena daya tarik sektor HPH bagi pelaku ransomware, tim HC3 memberikan perhatian khusus pada tren ransomware.
- HC3 telah melacak total **82** insiden ransomware yang berdampak pada sektor perawatan kesehatan di seluruh dunia sepanjang tahun 2021 ini, per 25 Mei 2021.
- Temuan didasarkan terutama pada pengamatan blog aktor ransomware, tetapi juga pelaporan media sumber terbuka dan *breach notification*.

Top 5 HPH Victim Sectors Impacted by Ransomware Globally 2021



INSIDEN RANSOMWARE HPH 2021: APAKAH DATA DIBOCORKAN PELAKU?



Serangan terhadap Sistem Kesehatan Irlandia



- Departemen Kesehatan Irlandia dan Eksekutif Layanan Kesehatan (HSE) diserang oleh ransomware Conti pada Mei 2021
- Penasihat klinis nasional HSE Dr. Vida Hamilton mengatakan hal itu "mempengaruhi setiap aspek perawatan pasien"
- Gangguan paling berdampak terhadap layanan rawat inap dan layanan penerbitan akta kelahiran dan kematian
- Fasilitas kesehatan terpaksa kembali menggunakan dokumentasi kertas
- Data pasien dirilis secara online

<https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf>

Malware

CryptoWall—has a new strain ransomware among others, with a price of \$39 per infection, which produces a profit of \$100 for the victim.

<https://www.trendmicro.com/vinfo/threats/ransomware-as-a-service>

Indonesian Association

Ransomware FileCrypter Rodando Windows , Android ,IOS,OSX, Linux,

Preço USD:3.000.00 ou 9 BTC. bitcoin. Por semana: Aluguel Semanal.
Encripta Todos Arquivos do Sistema , Seja as extensões , jpg,png,gif,pdf,txt,sql,doc,
xls,html,htm,xhtml,sql,bmp.php que estiver no sistema

Metodos de Encriptação 3DES AES DES RC4 ,

Resgate via Bitcoin .

Inclui Painel Completo Mostrando Quantidades de Pcs Infectados , Resgatados com Pagamentos ,
Não Resgatados E Valor Total Dos Resgates .

PROFIT FROM

HIGH INFECTION RATES
Since [redacted] bundled with his little brother [redacted] can't do his evil work without administrative privileges, [redacted] launches when those can't be obtained.
[redacted] does a low level encryption of the disk, which is a completely new technique in ransomware, acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR
As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multiple addresses, where no one (including us) can rip you off.
For more informations see our FAQ.

FREE CRYPTING SERVICE
We provide you FUD crypted binaries, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.
Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.

EASY ADMINISTRATION
Administrative Tasks like viewing the latest infections, setting the ransom price or encrypting your binary can be done with an clean and simple web-interface.
We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

Announcements

2016-03-18: I've got three stolen authenticode certificates for sale. The highest bid wins. It's OK to bid just for one and the end of the auction is not determined yet. Details: One (whole-chain) SHA1 and two SHA256, one SHA256 is valid until early 2018, the others are valid until late 2018, they aren't issued to the same name and I would use them for my service instead if they wouldn't be valid for that long. All three are valid for signing applications and kernel drivers up to Windows 10. (It's possible to load kernel drivers by the use of each certificate even on Windows 10. Thank you, old cross-certificates! It might be possible that the SHA1 certificate won't work for windows versions higher than Vista at any time.)
2016-03-31: I need help with cracking a faulty RSA(-MP) modulus (because of a bug) for a victim. I need the RSA decryption key. Please see "changes.txt" for more informations.
2016-04-16: @Microsoft: Please could you explain me two things: 1.: Why do you call my ransomware "Sarete"? 2.: What sense could it make for you to silently delete the readme files created by my ransomware on Windows 10 (Defender)?

Informations

The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been payed.
Decryptor links: **Decryptor interface**, **Decryptor demo page & chat with others**
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, readme filename, readme content and an unique hidden service address. Please see **this file** for rudimentary informations about the victims page template and contact me.
Fee: at least 5% (choosable).
Fixed BTC/USD rate: 451.74 USD.
Number of victims (excluding demo victims): 1891
Payed (excluding demo victims; automatically updated): 20 (1.06%)
Incomplete payments (excluding demo victims; manually updated): 3
FAQ: **faq.html**

Technical summary

My Encryptor works fully offline and uses a combination of RC6-32/20/256 and RSA-2048. Every file has its own key.
Encryptor RaaS is signed by my free file signing service. It's using stolen authenticode certificates. SHA256 only.
File extensions, which are being encrypted: **extensions.txt**
Changes: **changes.txt**
Minimum support: Windows XP, i686.
Version: 2016-05-11_1

Detection rates

Unsigned Encryptor Detection Rate (NoDistribute, as at 2016-05-11): **235** (Ikarus and Trend Micro)
Notice: My ransomware might be detected by Twister, AhnLab and/or Qihoo360.

Please enter your bitcoin address

Use my donation bitcoin address for demonstration purposes only. It'll then act like the victim has already payed.

Bitcoin address:
12PCLkRtA5RyYnD72kMvT9cKtU6

Continue

File signing service

Free PE (Windows executable) file signing service. Please donate! SHA256 (no Win7) only.

Botnets & Malware Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

Stampado Ransomware - You always wanted a Ransomware but never wanted to pay hundreds of dollars for it? - This list is for you! :)

Stampado is a (cheap and easy to manage) ransomware, developed by me and my team. E...

Sold by **The_Rainmaker** - 2 sold since Jul 12, 2016 **Vendor Level 1** **Trust Level 5**

	Features	Features	Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

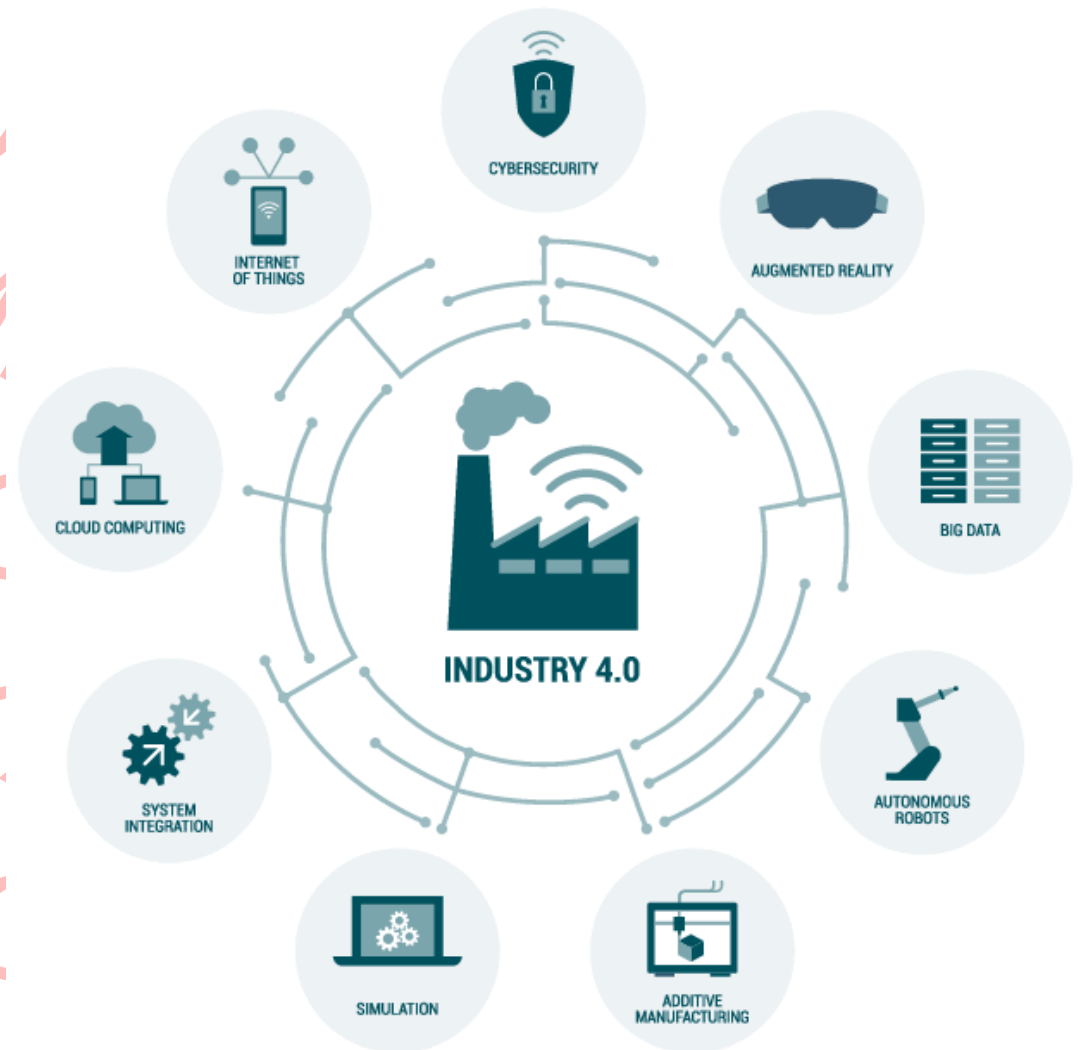
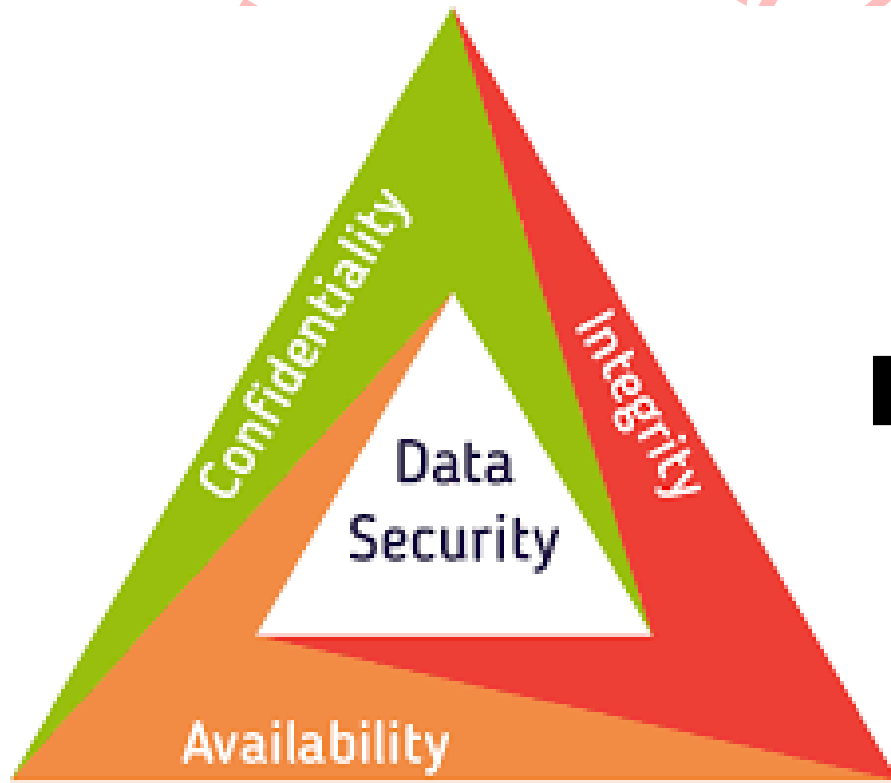
DIS

DI

2

Tantangan 4.0

the devil is in the details



Healthcare IT Challenges

Healthcare telah mengalami modernisasi TI yang signifikan. Berikut 4 tantangan Keamanan Data pada *Healthcare* :

- 1. Integrasi jaringan.** Di sisi bisnis *healthcare*, ada banyak merger dan akuisisi, atau adopsi alkes berbasis elektronik/bahkan IP. Sayangnya, hal ini sering menyebabkan masalah integrasi jaringan dan visibilitas jaringan.
- 2. Perawatan pasien jarak jauh.** Penelitian terbaru menunjukkan bahwa 71% dari semua penyedia *healthcare* menggunakan alat kesehatan jarak jauh atau pengobatan jarak jauh untuk terhubung dengan pasien.
- 3. Kepatuhan terhadap Regulasi/Standar.** Indonesia belum memiliki regulasi khusus untuk PHI, namun data rekam kesehatan WNI dilindungi sesuai UU 24/2013 ttg Adminduk pasal 84. AS memiliki HIPAA (*Health Insurance Portability and Accountability Act of 1996*) yang sangat ketat dalam masalah seperti *breach* informasi pribadi pasien yang melanggar hukum, dan setiap insiden *data breach* yang dapat berakibat denda besar atau kerusakan reputasi yang signifikan.
- 4. Perencanaan respon insiden siber.** Memiliki rencana untuk menangani ransomware sangat penting untuk organisasi *healthcare*. Meskipun enkripsi dan *backup* penting, itu mungkin tidak cukup. Organisasi yang *comply* terhadap standar seperti HIPAA atau ISO 27001 akan melihat manfaat terbesar.

Pasal 84

- (1) Data Pribadi Penduduk yang harus dilindungi memuat:

a. keterangan . . .



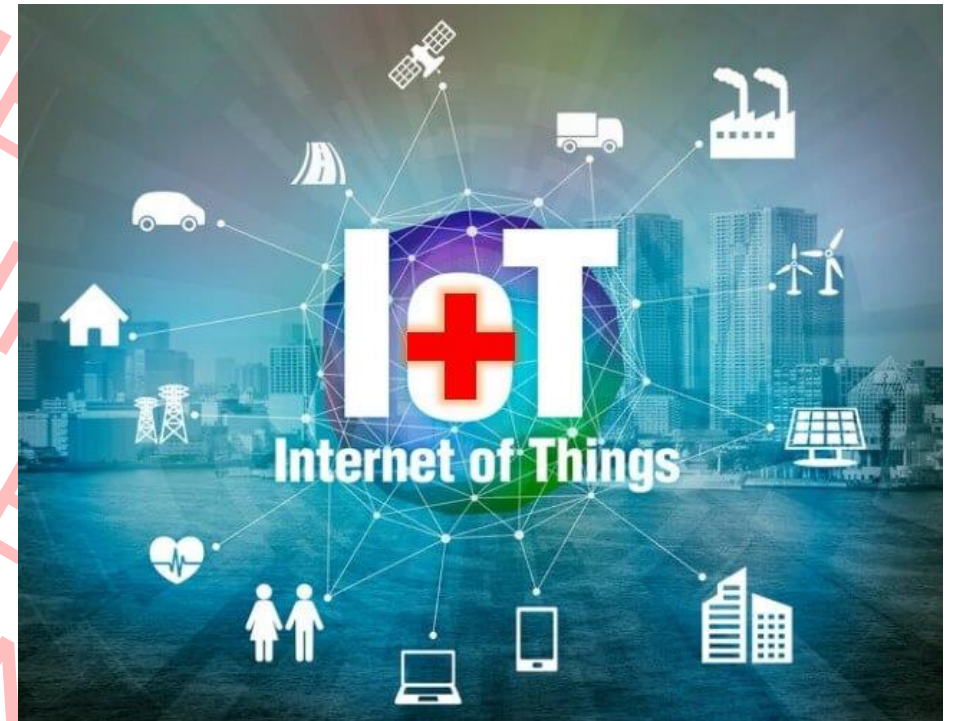
PRESIDEN
REPUBLIK INDONESIA

- 21 -

- a. keterangan tentang cacat fisik dan/atau mental;
- b. sidik jari;
- c. iris mata;
- d. tanda tangan; dan
- e. elemen data lainnya yang merupakan aib seseorang.

The Rise of IoTs

- Dalam banyak hal, sistem IoT sangat mirip dengan tubuh manusia – sistem besar dan kompleks yang selalu aktif.
- Mari kita gunakan serangan jantung sebagai analogi. Kita semua tahu bahwa serangan jantung bisa menjadi bencana besar. Meskipun serangan jantung biasanya terjadi secara tiba-tiba, kondisi yang memungkinkannya sebenarnya membutuhkan waktu berhari-hari, berbulan-bulan atau bahkan bertahun-tahun untuk terbentuk.
- Jika kita dapat secara terus menerus, otomatis dan cerdas memantau jantung dan tubuh, kita dapat mendeteksi tanda-tanda awal masalah dan mengambil tindakan pencegahan untuk menghindari serangan jantung.
- Sayangnya, banyak Unit TIK organisasi tidak memiliki informasi serupa di jaringan IoT. Sebagian besar rumah sakit tidak memiliki informasi terkini tentang jenis perangkat IoT apa yang mereka miliki, apalagi berapa banyak perangkat ini yang terhubung ke jaringan mereka. Jadi, visibilitas perangkat IoT adalah **tugas pertama** untuk setiap organisasi.



Securing the Connecting Doors

- *MyHealthEDo* walaupun tuju
- Masalah akse dari keamana
- API (applicati memungkinkan ketiga, dan m tersedia di m
- Tetapi ancam menjadi lebih kompleks.

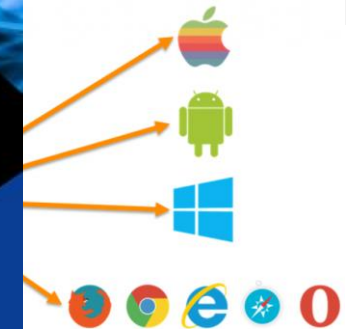
PEDOMAN KEAMANAN

MICROSERVICE DAN APPLICATION PROGRAMMING INTERFACE (API)

Berdasarkan:
NIST SP 800-204 (2019)
OWASP API Security Top 10 (2019)

my
health
data

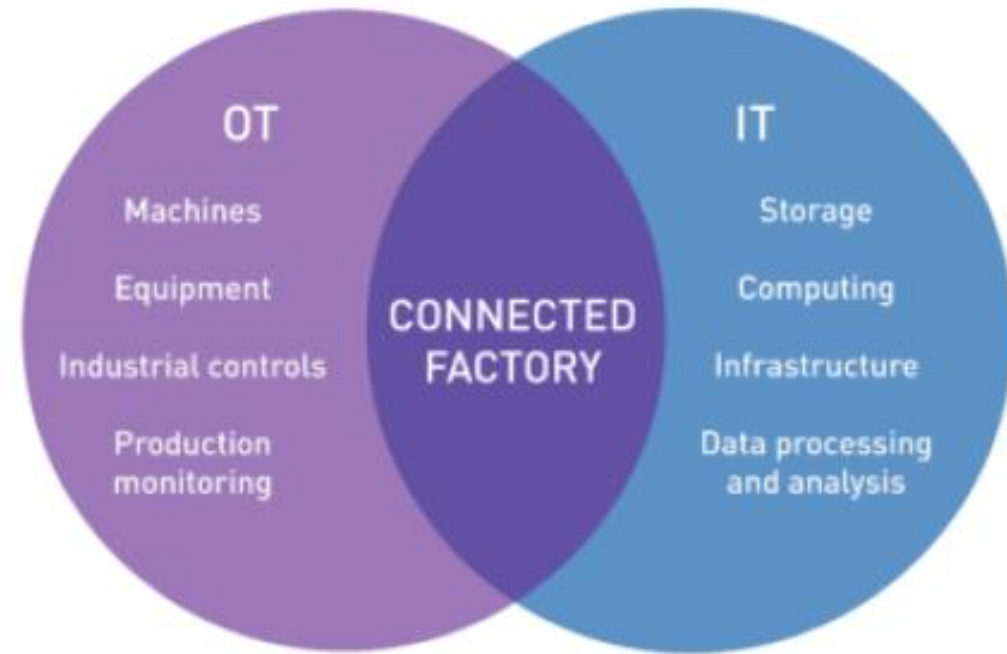
patients access and share
r healthcare data



PeduliLindungi

Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift

- Cloud dan Shadow IT memberi dampak attack vector baru
- Konvergensi OT → IT, e.g. *Building Automation System (BAS)*, Robotik, *Medical Devices Data System (MDDS)*
- Keamanan TI konvensional masih berbasis Perimeter



<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/healthcare-securitythree-paradoxes-and-the-need-for-a-paradigm-shift>

DIS

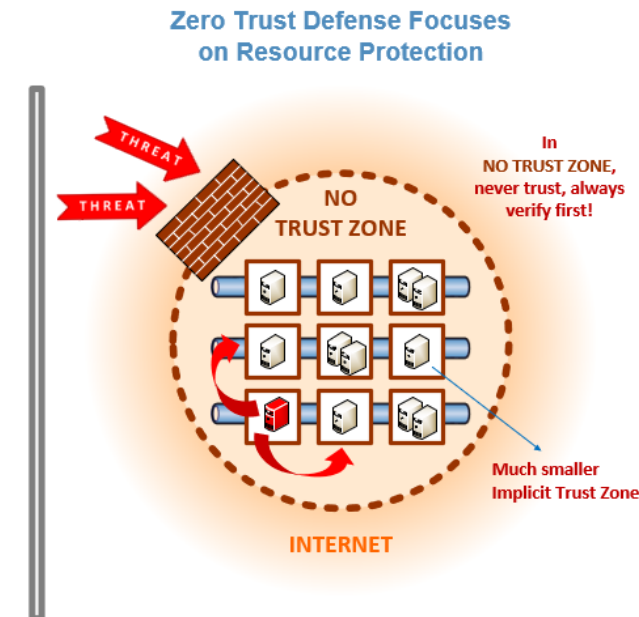
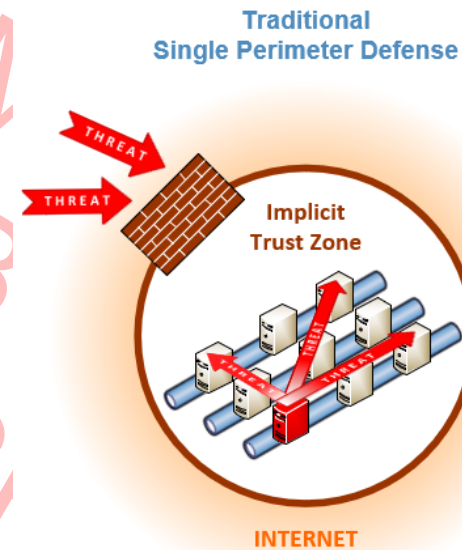
DI

3

Rekomendasi

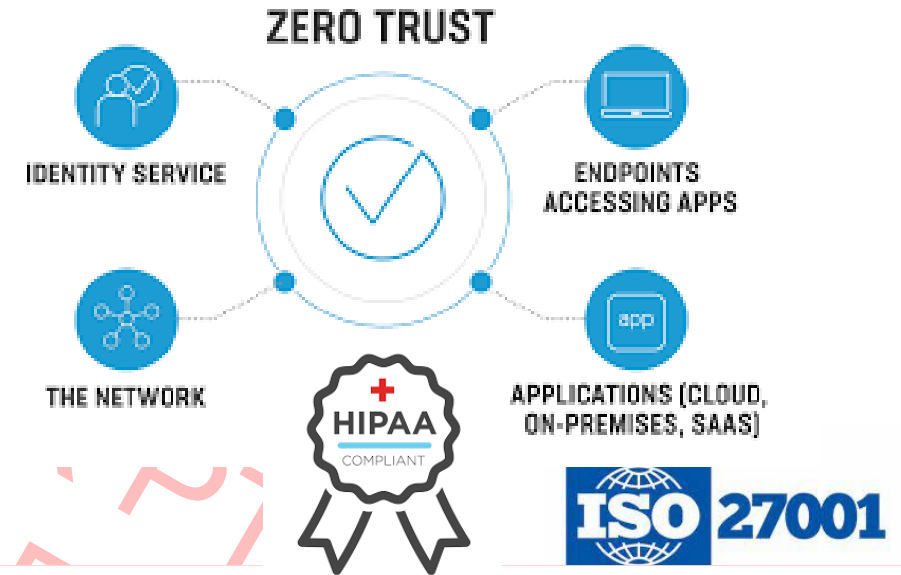
TAKEAWAYS

- Dalam ekosistem di mana sistem TI tradisional berdampingan dengan sistem *shadow IT* (BYOD, mobile apps, GDocs) dan sistem manajemen data lainnya (cloud, MDDS, SCADA), perlindungan data dan infrastruktur penting harus ditangani dari sudut pandang yang berbeda.
- Metafora yang tepat mungkin adalah kota terbuka dengan sejumlah bangunan kritis, bukan benteng ber dinding. Tujuan keamanan tidak lagi pertahanan benteng, melainkan perlindungan bangunan kritis dalam suatu kota terbuka.
- Semua teknologi informasi dan otomatisasi di rumah sakit harus menjadi pertimbangan. Keamanan harus meliputi TI tradisional, cloud, alkes, otomatisasi bangunan, dan *shadow IT* lainnya.



Rekomendasi

1. **Raise Awareness.** Manusia – yaitu pengguna akhir – akan selalu menjadi mata rantai terlemah.
2. **Govern your Security.** Organisasi/fungsi keamanan TI akan menjadi ujung tombak program keamanan anda.
3. **Apply Zero Trust.** Pergeseran keamanan konvensional berbasis perimeter ke arah keamanan berbasis hak akses merupakan kondisi ideal.
4. **Invest in Predictive Analysis.** Platform *Cyber Threat Intelligence* (CTI) dapat menyediakan analisis *real-time* tentang deteksi dan respon insiden. Kerjasama sektoral juga menjadi kunci kesuksesan keamanan.



3-2-1 Backup Rule



X3

Maintain at least 3 copies of your data



X2

Keep 2 copies stored at separate locations



X1

Store at least 1 copy at an off-site location



Thank You

“SECARA
“LINE”

