### Kenali Model Bisnis Dalam Kejahatan Siber Modern

#### Security Awareness Purposes

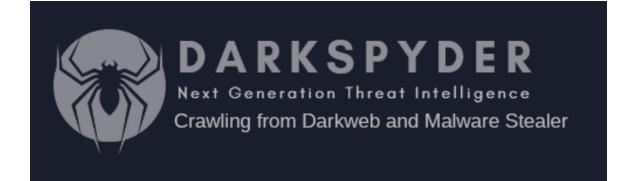
Pemerintah Kota Jakarta Barat Edisi ke-18 tanggal 21 November 2024

supported by:



#### Who Am I?











- 18 Tahun sebagai professional di bidang Cybersecurity dan Information Security
- CISO of Darkspyder, salah satu Perusahaan Cyber Threat Intelligence berbasis di Netherland
- CISO of Quantumshield, salah satu anak Perusahaan Konglomerasi di bidang Cybersecurity di Indonesia
- VP of Technology (act) Xignature, Digital Trust Company (PSrE) di Indonesia
- Senior IT Security Consultant of SciEngines, salah satu Perusahaan yang berfokus di bidang Crypto Analysis dan Massive Parallel Computing di Jerman
- Sebelumnya bekerja di Badan Siber dan Sandi Negara selama 14 tahun sebagai cybersecurity professional (Training, Pentest, Cybersecurity Assessment dan SOC team)



#### **DISCLAIMER**

- Dalam keadaan apapun, presentasi ini tidak boleh dianggap sebagai panduan untuk bertindak.
- Presentasi ini hanya berfungsi sebagai tinjauan umum pasar kejahatan dunia maya.
- Aktivitas yang dijelaskan dalam presentasi ini merupakan tindak pidana menurut Kitab Undang-Undang Hukum Pidana di banyak negara!

## SPYDER

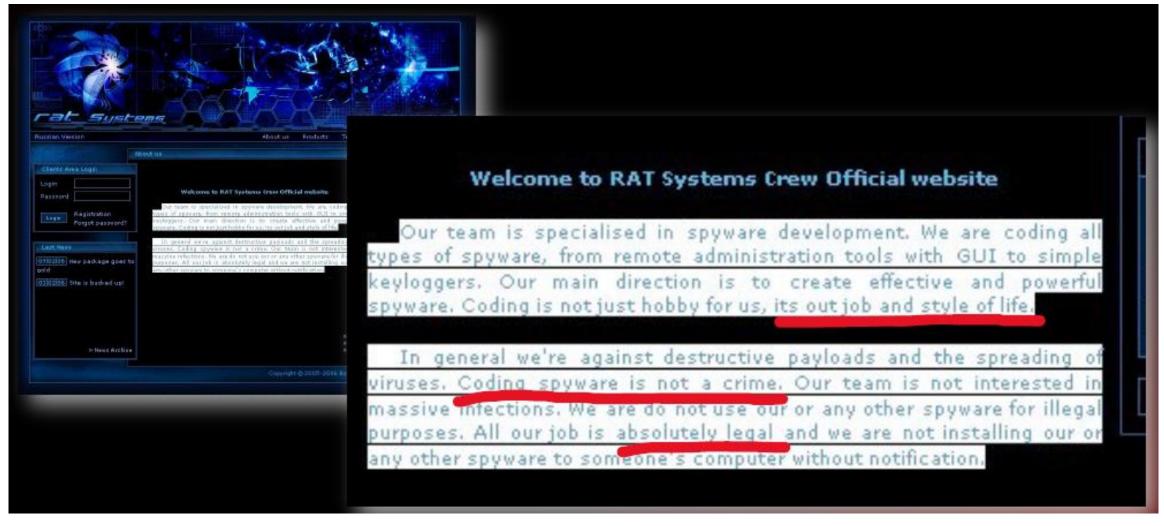
#### Bapak hacker ya?



Hey, I am a Cybersecurity Profesional not a cyber gang!



# Hacking sebagai sebuah fenomena tidak dapat dikalahkan



#### Who is Mr. Hacker?







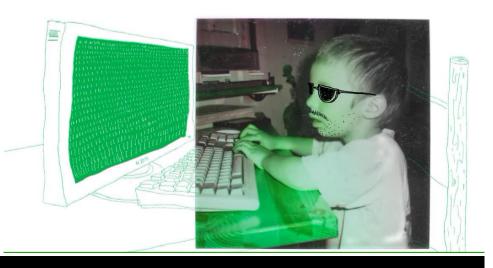


Tidak memiliki kemampuan untuk menulis program atau mengeksploitasi



#### Senang mencoba

Tujuan mereka semata-mata hanya untuk membuat orang lain terkesan, atau agar namanya dikenal komunitas penggemar komputer atau peretas



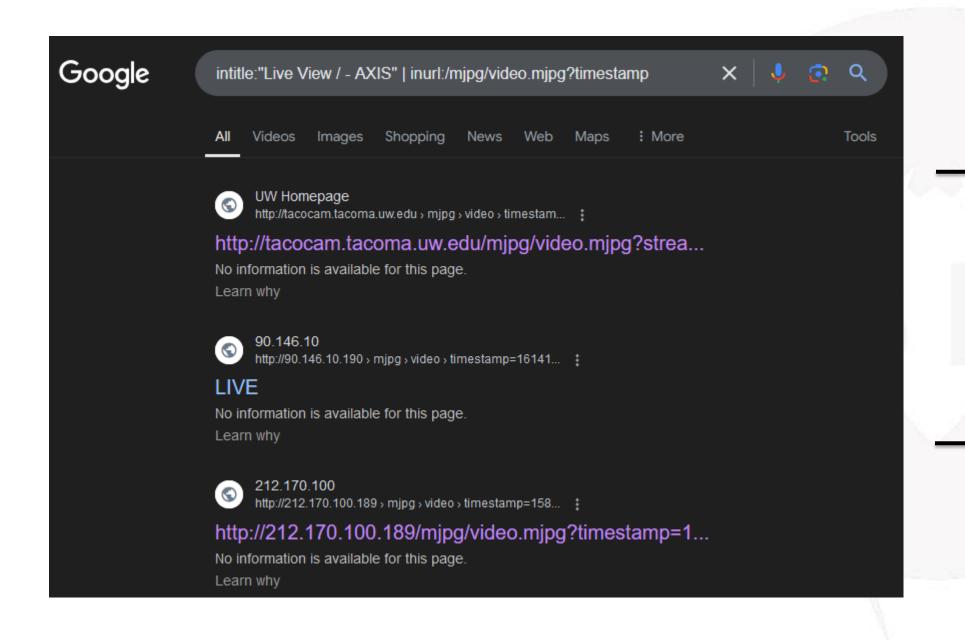
#### skid

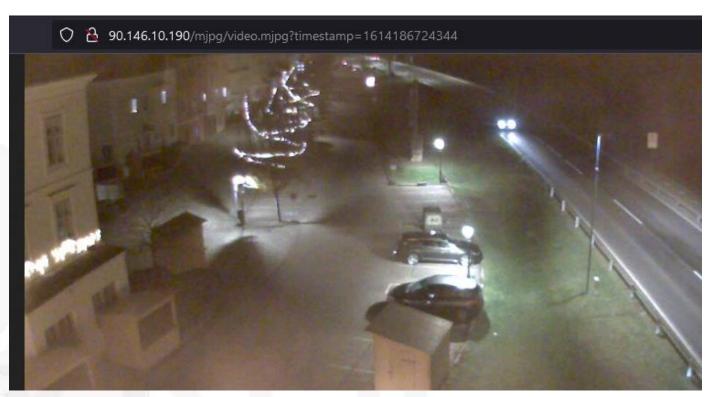
Script Kiddies menggunakan skrip atau program yang dikembangkan orang lain untuk menyerang sistem komputer dan jaringan

intitle:"Live View / - AXIS" | inurl:/mjpg/video.mjpg?timestamp
intitle:"DEVICE" "Real-time IP Camera Monitoring System"



#### intitle:"Live View / - AXIS" | inurl:/mjpg/video.mjpg?timestamp



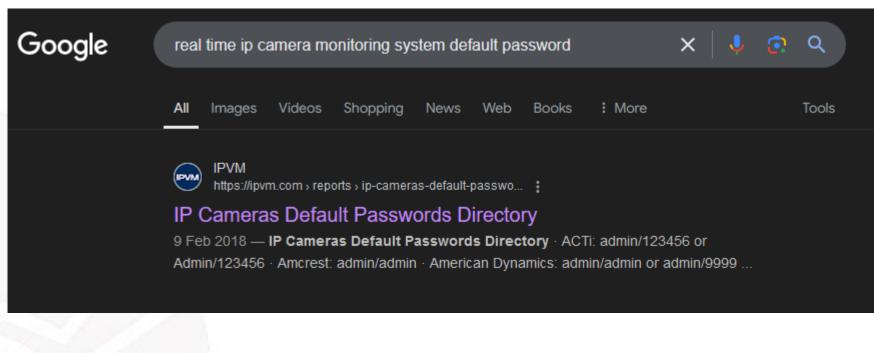


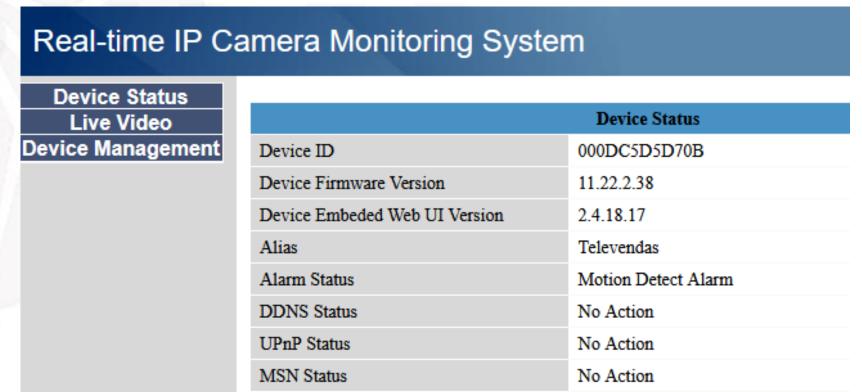




#### intitle: "DEVICE" "Real-time IP Camera Monitoring System"







Coba yang paling mudah: User:admin / Password:123456



#### Script Kiddies.

Mereka ingin membuktikan kepada semua orang bahwa mereka mampu melakukan sesuatu. Hal ini sudah melekat pada sifat manusia dan tidak dapat dihilangkan.





#### **Hacktivists**











#### Hacking

Menggunakan computer atau internet

#### Activism

Mengungkap ketidak adilan di ranah politik, social dan agama

#### Hacktivism

tindakan meretas, atau membobol sistem komputer, untuk tujuan bermotif politik atau sosial



Hacktivist adalah kelompok penjahat yang bersatu untuk melakukan serangan siber



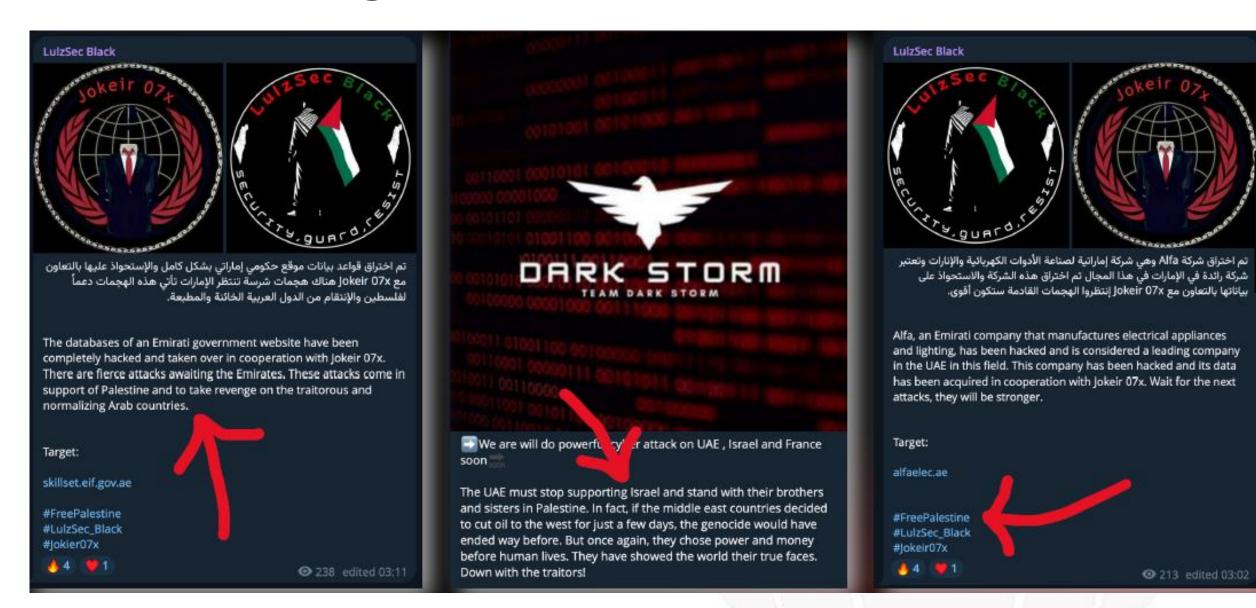
#### **Hacktivists**

Mereka ingin hidup di dunia yang sempurna. Ini adalah khayalan dan tidak dapat dicapai!

Mereka didorong oleh politik, ideologi, agama, social, yang hampir mustahil dikalahkan.

# ) ARKSPYDER

#### Contoh serangan Hacktivist



Prediksi. Para hacktivist membentuk aliansi dan saling bertukar target serangan, alat, teknik, taktik, dan peluang.



On the 19th of August we launched a devastating attack targeting the infrastructure of Saudi Arabia. One of the primary targets was the Arab National Bank (ANB), where we successfully disrupted the banking service portal for over seven hours.

The attacks we launch are powerful, lethal and advanced that belong to the fourth generation. Despite the fact that Saudi Arabia spends high amounts on protective firewalls/ WAF's/ DDoS Protection, they still remain incapable of stopping our attacks.

At this moment, a new and comprehensive attack is being prepared against the Saudi infrastructure, including financial and banking services.

🕠 🎤 Hello Saudi government 🖐 , I hope you are entertained by our attack this week and also hello to the princess Mohammed ben Salmane:) we're sure you like your new Jewish family.

♦ بتاريخ 19/08/2024، قمنا بتنفيذ هجوم مدمر استهدف البنية التحتية للمملكة · العربية السعودية، وكان من أبرز الأهداف البنك العربي الوطني (Arab National Bank)، حيث تم تعطيل بوابة الخدمات المصرفية لأكثر من سبع ساعات.

> • نوعية الهجمات التي نه المملكة تصرف الملايين عا 🌑 حاليًا، يتم التحضير له،

بما في ذلك الخدمات المال

or "terrorists"; instead, we would become symbols of progress and

This is the law of the new world, the law of the strong who rule over the weak. But we are neither the strong nor the weak... We are the kings of the game, the armies of the oppressed and wronged. Our mission is not to establish justice in life, for that is a relative concept, but our mission is to silence those who think they are something when they are nothing. Where some of our attacks are labeled as criminal activity, we label it as the voices of freedom.

➤ The result? We would be hailed as national heroes, champions

privileges beyond imagination. We would benefit financially and

challenge). We would have connections with business leaders and

politicians and no one would call us "a gang of criminal hackers"

of freedom and democracy, fighting terrorism and gaining

live lives free from risks and troubles (although we love a

Terrorism is a year-long genocide.

- Terrorism is the rape of lands without any right.
- Terrorism is the destruction of childhood dreams.
- Terrorism is accusing us of terrorism without a court or legal
- Terrorism is the right of white people and foreigners to international protection and diplomatic law, while people with brown and black skin are marginalized.
- · Terrorism is destroying the homes of the innocent and the dreams of children.

🔯 🌉 🎇 In the end, you are the terrorists.

Note: Our group does not carry out attacks for money. That is a cheap media tactic to tarnish our great names. Our enemies will taste severe torment.



justice.



Not for

money

We'd like to announce GhostSec's leave from the financial motivation "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed. The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!

What will remain? At the moment we will continue to keep our private channel and chat room available and will be running a discount from today until may 23rd, Get lifetime access to the private channel and chat room for \$400 \$250 ONLY until may 23rd. We may also plan soon to make and provide a hacking course/package though we are still debating on making this hack like a ghost course.

Thank you for your constant support, love and understanding. We are very excited to continue and put all focus into our work in changing the world to becoming a better place!

Fight for something you believe in and truly find it for yourself.

Chase your own freedom, dreams and goals. Then Pass it on to the future.

Hack the planet!!
We Run Shit Cause We Can!
~GhostSec0

Para aktivis peretas mulai tidak hanya fokus pada serangan DDoS dan kebocoran data, tetapi sekarang mereka juga menggunakan metode ransomware untuk menarik perhatian pada tujuan mereka atau untuk mendanai operasi mereka.

- Earned enough and can now "relax"
- Return to hacktivism
- Will teach new hackers on private courses





### **Advance Persistent Threat (APT)**

Advanced Persistent Threat (APT) adalah jenis serangan siber yang ditargetkan dan dilakukan secara berkelanjutan oleh pihak yang memiliki sumber daya dan keahlian tinggi.



Hidden Cobra atau Labyrinth Chollima. Dari korea utara. Kelompok ini dikenal karena strategi mereka yang mencakup pencurian data dan informasi bernilai tinggi, dengan motif yang melibatkan keuntungan finansial, spionase, dan sabotase. Keterlibatan pemerintah Korea Utara dalam aktivitas Lazarus menambahkan dimensi geopolitik yang signifikan pada ancaman yang mereka timbulkan.



Winnti, yang juga dikenal dengan nama Blackfly atau Wicked Panda, merupakan salah satu contoh Advanced Persistent Threat yang diduga terkait dengan Tiongkok. Aktif sejak tahun 2010, kelompok ini dikenal karena operasi mereka yang bertujuan untuk pencurian informasi dan spionase.







SECURITY OF

India's maples, 19th Delini, Chilli Choan, FU Quing, and ISMS Late are all part of a Children hacking group boson as MT 45, and SARSON.

In August 15, 2019, a Grand Sury or the District of Columbia returned an indictional agency Chinese nationals DIANG resonal and Stift Districts on charges including bioauthorped Abress to Presided Computers, Applicables Sentity TheRi, Ricco Lauridening, and littre Fraud. These charges primarily Identified from allegals activity terysting ligh technology and Adeo Jersing compenses, and a United Kingdom object.

On Regard 11, 2000, a Grand Sury in the District of Columbia intermed on indichment against Chinera nationals QBNs Choice, Pol Quang, and JSANG Light on charges including Recketsering, Impress sandading, Prisust, Identity TheRt, and Molecul Electrics Prisust. These interpress them from their elleged unsulfatorized computer infrastructure entitle employed by Changity 460 Reduces Technology Complete. The definitions allegated conducted augusty chain attacks to gain providenced across to operation to technology Complete the extract Elegating Standards of compenses reconsisting a brasis areas of industries to include across to operation the extract England Standards of compenses reconsisting a brasis areas of industries to include across to describe the extract Elegating Standards Industries to Standards Industries In

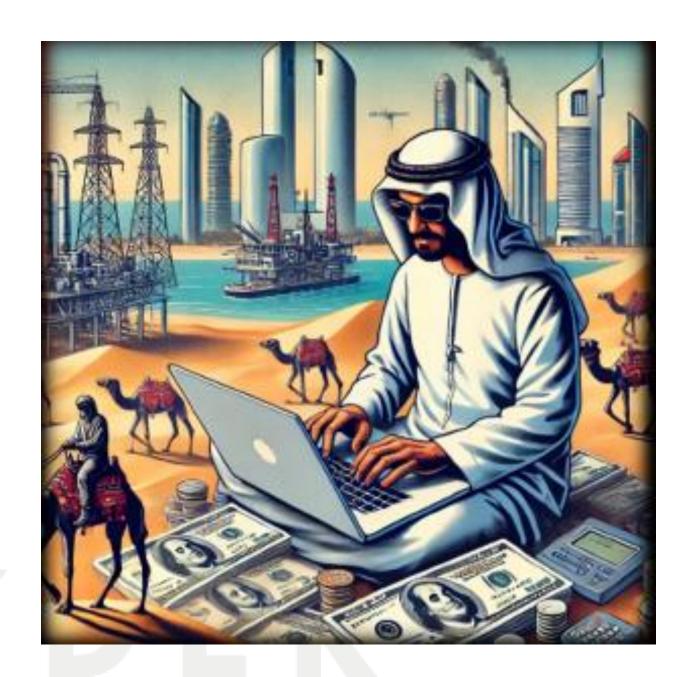
If you have any information concerning these individuals, please context your local FEE office, or the nearest American Emileory or Consolute.

Field Office: Vision region D.C.

man fit and



Mereka menghasilkan uang. Uang tidak terkalahkan selama masih ada, dan akan selalu ada! Kita dapat mencoba mengendalikan dan memblokir arus keuangan, serta menghukum perantaranya.





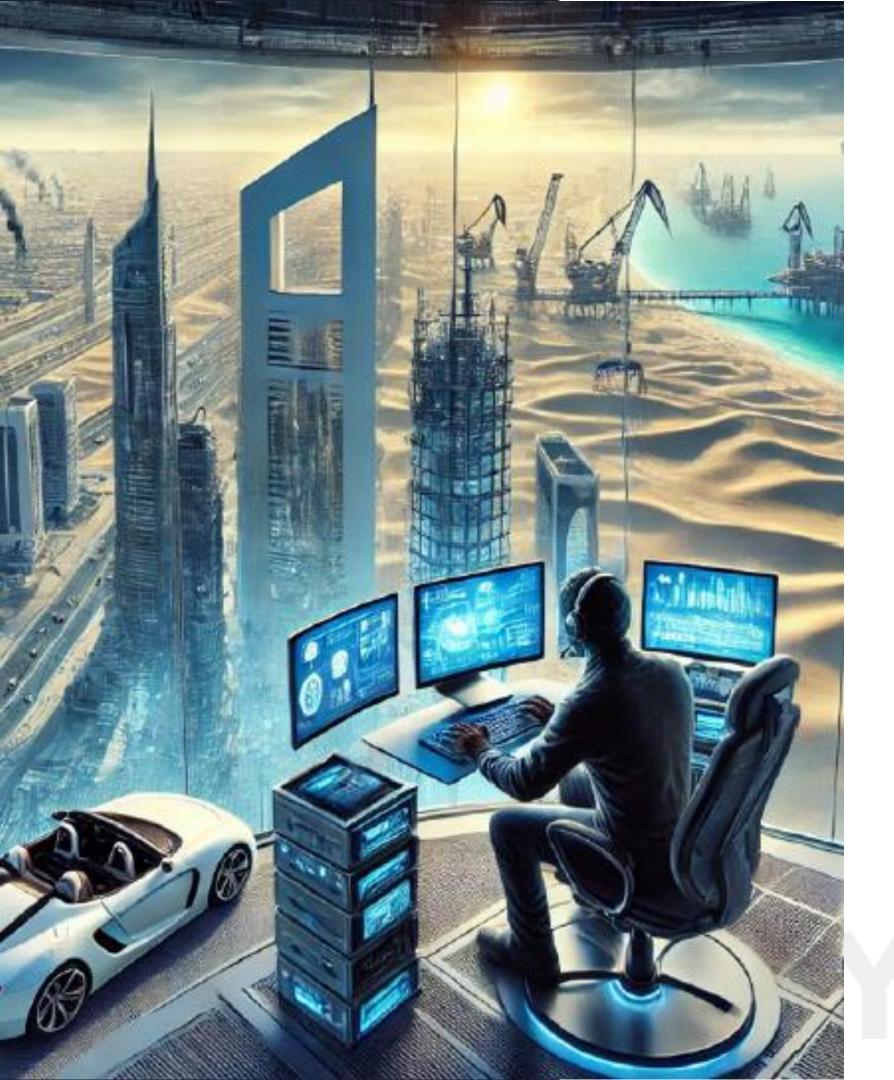


### **State-Sponsored Hackers**



Hacker yang didukung oleh pemerintah atau entitas negara untuk melakukan serangan cyber terhadap target pemerintah, militer, atau bisnis asing. Tujuannya dapat berkisar dari mencuri rahasia negara hingga sabotase infrastruktur kritis.

Mereka mengabdi pada negara. Pengabdian pada negara akan terus berlanjut selama negara masih ada! Kita juga tidak boleh melupakan intelijen dan operasi khusus di dunia maya!



Namun bagaimana jika kita melihat kejahatan dunia maya dari sudut pandang bisnis dan pasar?!



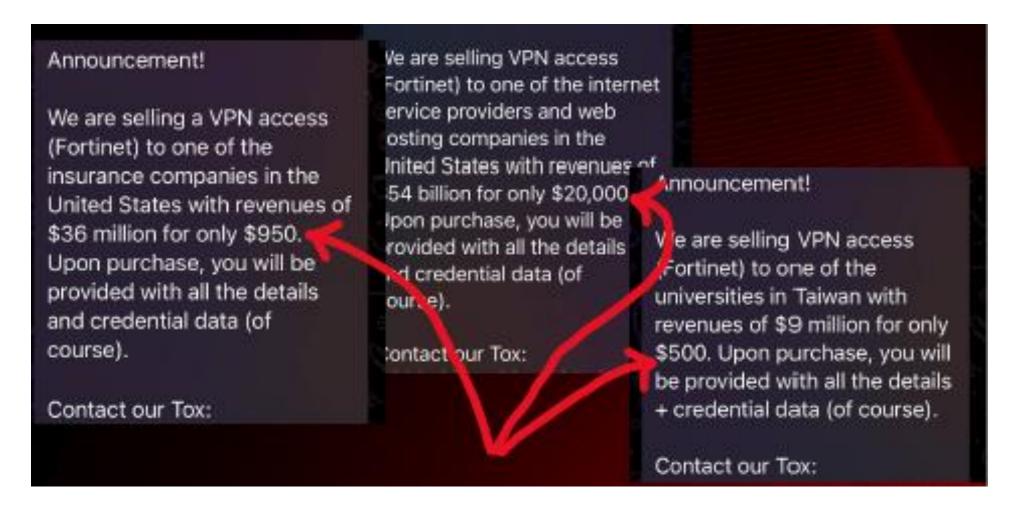
### Pertumbuhan laba

merupakan tujuan dari setiap bisnis, dan dicapai dengan meningkatkan pendapatan dan mengurangi biaya.

# Dan kejahatan dunia maya tidak terkecuali!!!



## **Cybercrime Products**



- Software for unauthorized access (RATs,
- ransomware, etc.)
- Vulnerabilities
- Software for exploiting vulnerabilities (exploits)
- cryptors, obfuscators
- Databases of stolen information (insider data, personal data, payment cards, etc.)
- Internet traffic
- Botnets



# Cybercrime Services model is better!

- Spam distribution and Malware development
   Credit card and
- Conducting DDoS attacks
- Data theft
- Detection testing
- Re-encryption
- Abuse-resistant hosting
- VPN services
- Botnet rental

- Malware development
   Hiring droppers
- Credit card and account verification
- Data verification
- Search engine optimization
- Criminal arbitration
- Money laundering
- Fake website development
- Hiring hackers

- Mules / droppers
- Call center
- Crypto-analytical services
- CAPTCHA bypass
- Background checks
- Card cloning
- Fake ATMs
- Forging documents

## Model layanan berkembang



- Destroying a competitor's business
- Digital twins and deepfakes
- Hacker universities
- Creating a hacker marketplace in the darknet
- Advertising in the darknet
- Access to video cameras
- Tracking a person's movement through video cameras
- Commissioned defamation (slander)



## Prediction

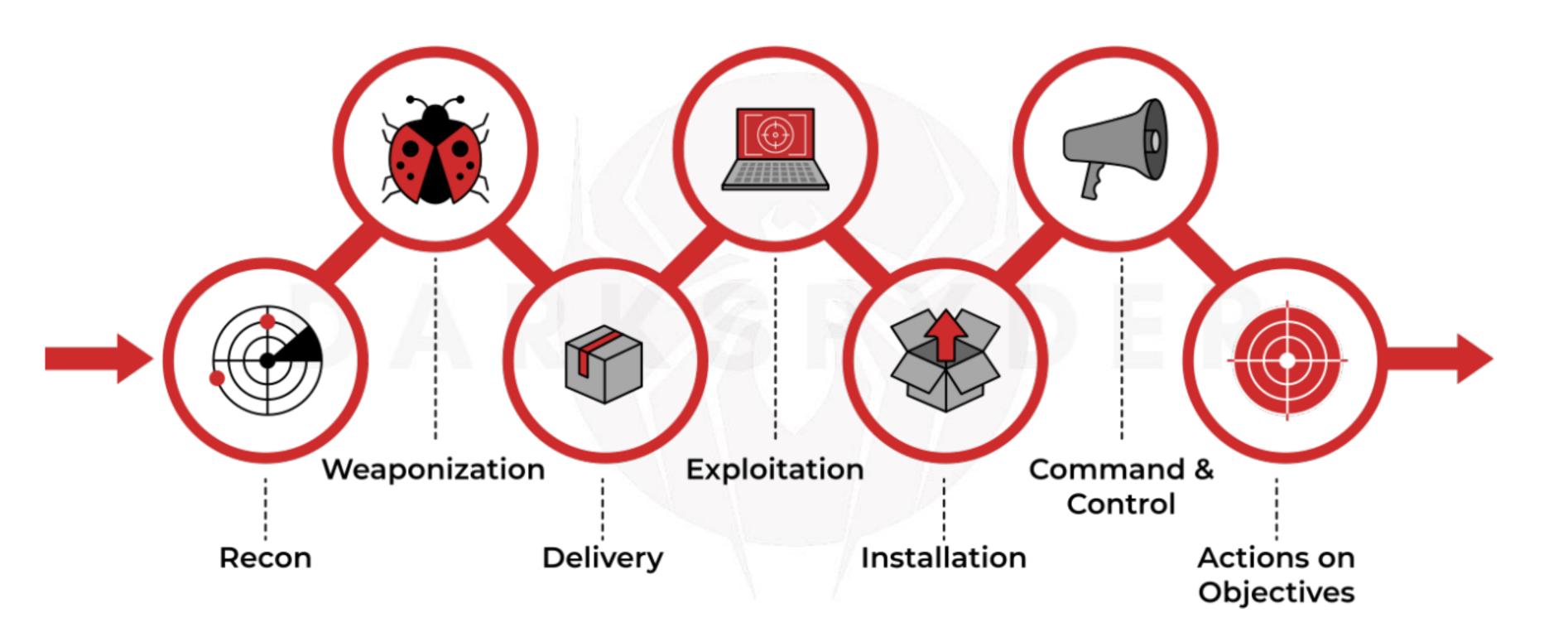
Growth in the number of hacker services based on the XaaS model:

- Ransomware-as-a-Service
- DDoS-as-a-Service
- Phishing-as-a-Service
- Cybercrime-as-a-Service
- Anything-as-a-Service











- Pasar cybercrime sama seperti pasar cybersecurity, tetapi dengan momok yang negatif
- Kejahatan dunia maya akan terus berkembang
- Pemantauan model bisnis baru memungkinkan kita untuk mengantisipasi apa yang akan digunakan oleh penjahat dunia maya dan bersiap untuk menghadapinya terlebih dahulu
- Pentingnya memiliki dan menggunakan layanan Threat Intelijen yang canggih

