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?

Xignature

SciEngines
massively parallel computing

- 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)

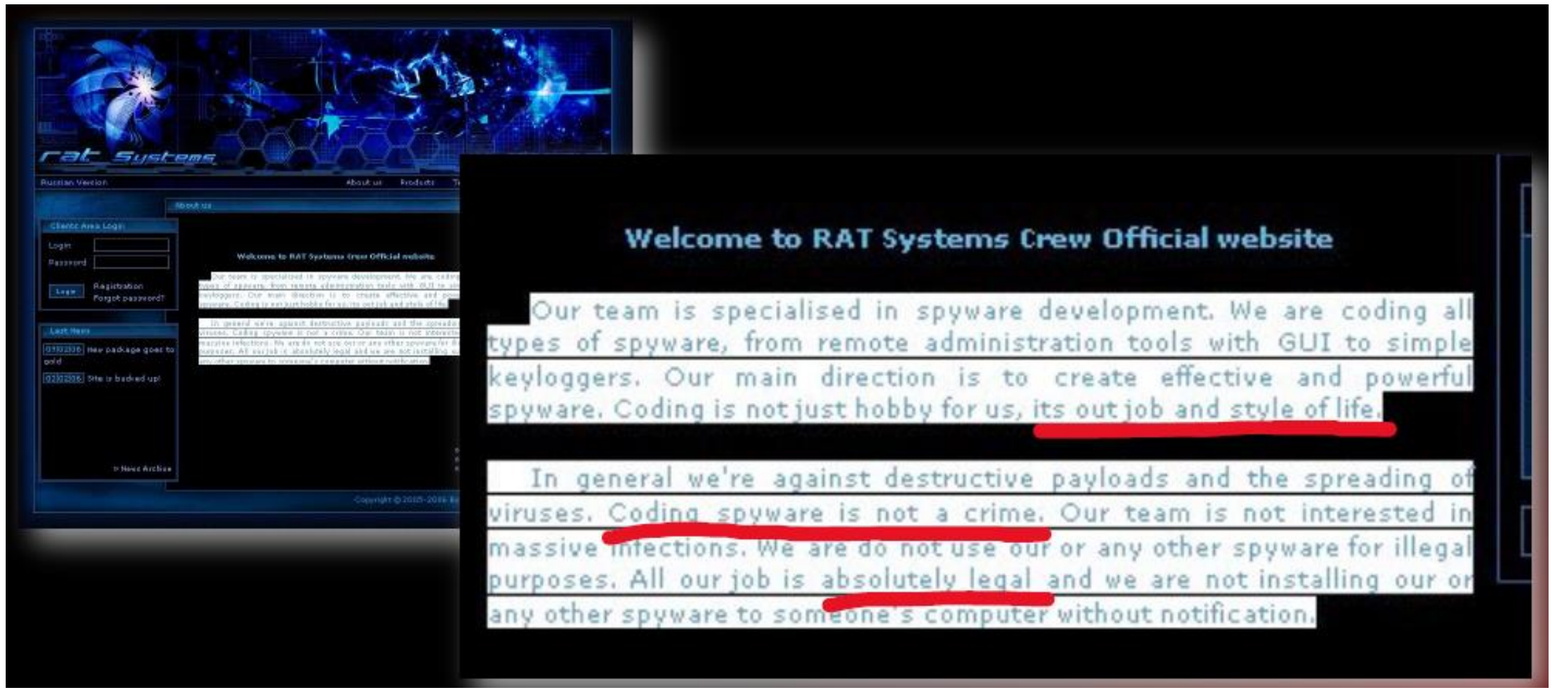
DISCLAIMER

- 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!

Bapak hacker ya?

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

Hacking sebagai sebuah fenomena **tidak dapat dikalahkan**



Who is Mr. Hacker?

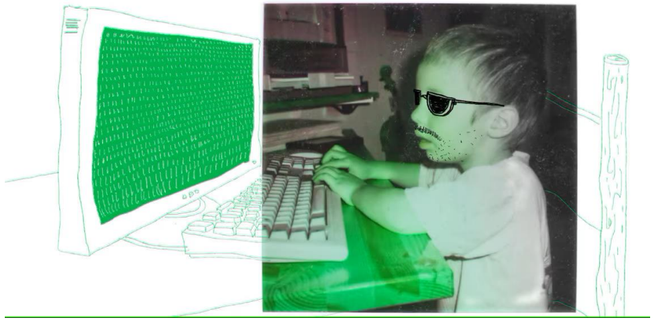
Script Kiddies

Baru belajar

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

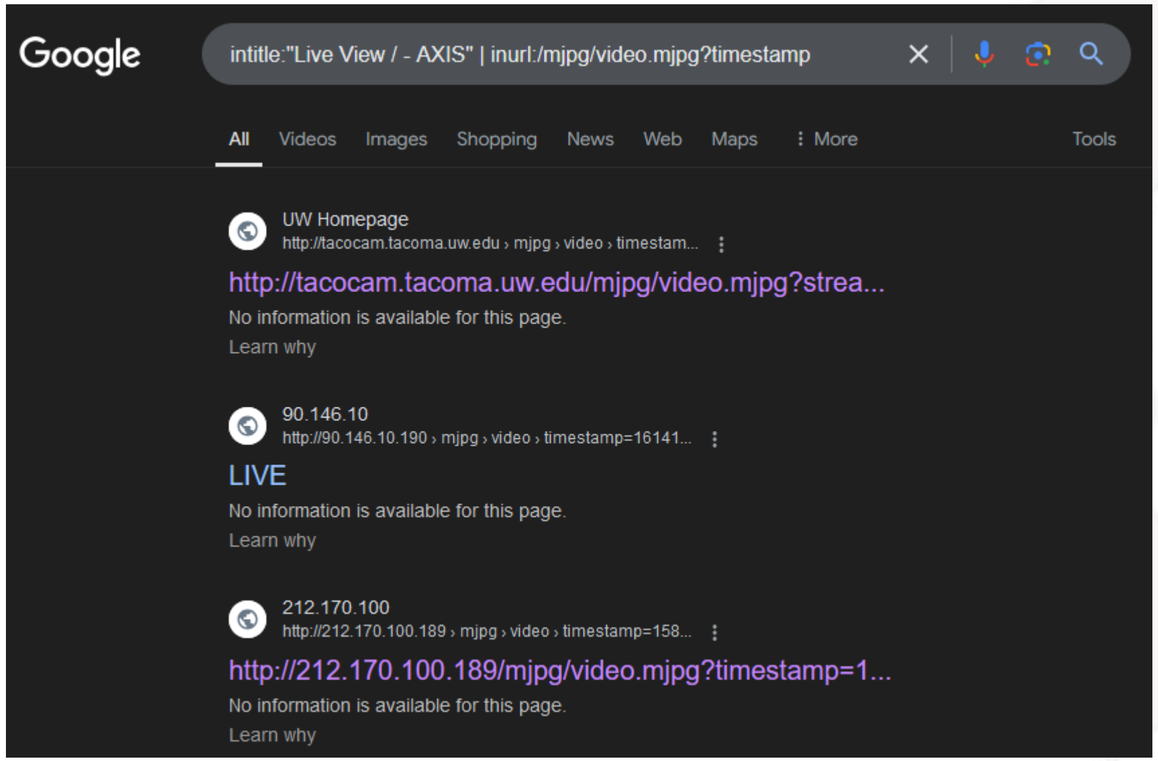


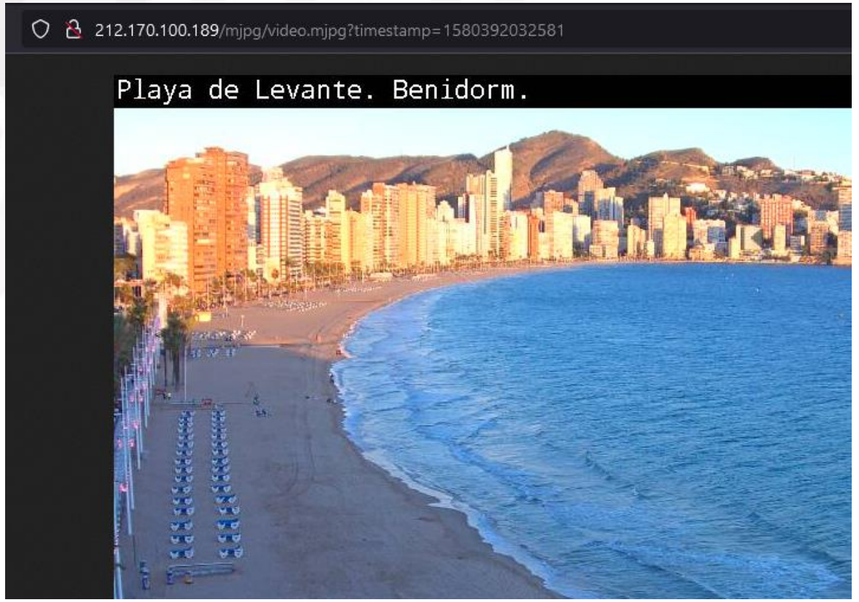
skid

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

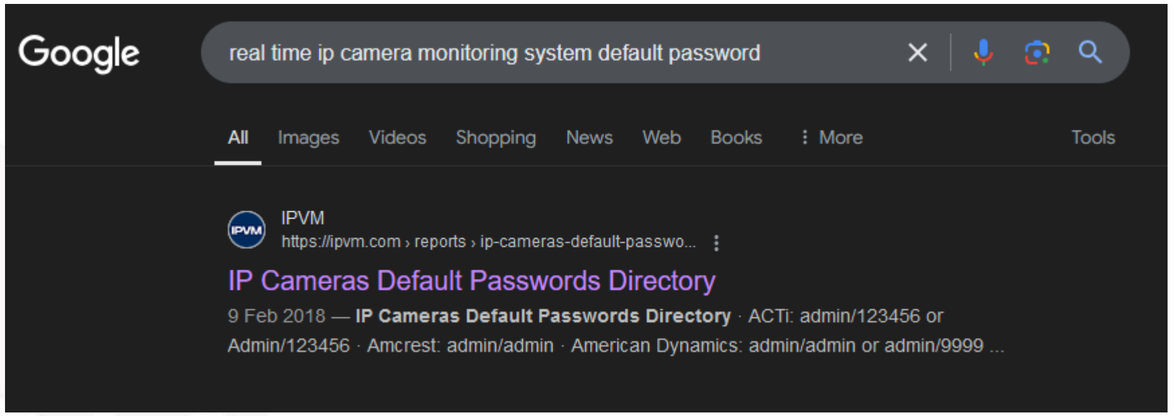
```
intitle:"Live View / - AXIS" | inurl:/mjpg/video.mjpg?timestamp
intitle:"DEVICE" "Real-time IP Camera Monitoring System"
```

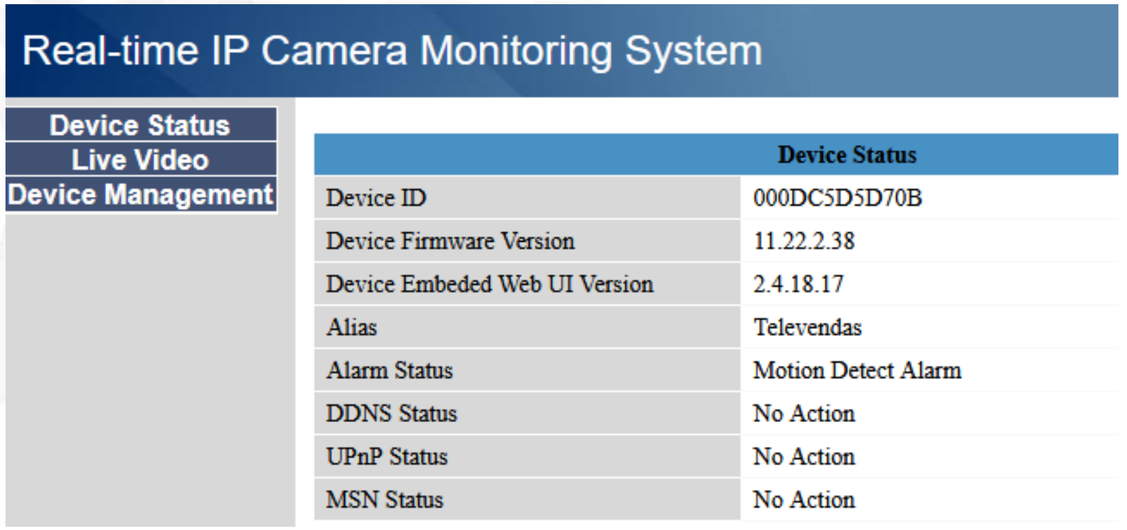
intitle:"Live View / - AXIS" | inurl:/mjpg/video.mjpg?timestamp





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.**

Who is Mr. Hacker?

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

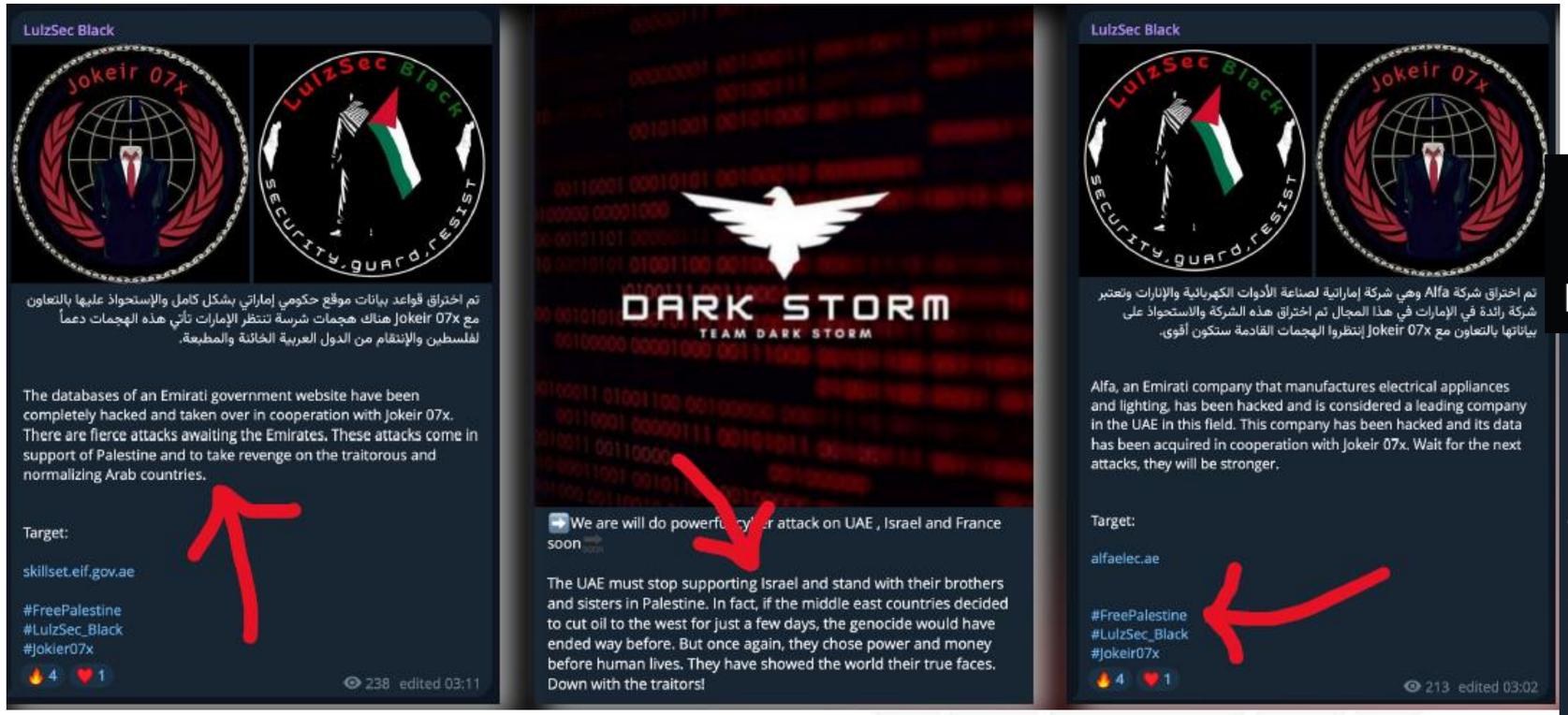
Hacktivist adalah kelompok penjahat yang bersatu **untuk melakukan serangan siber**

Hacktivists

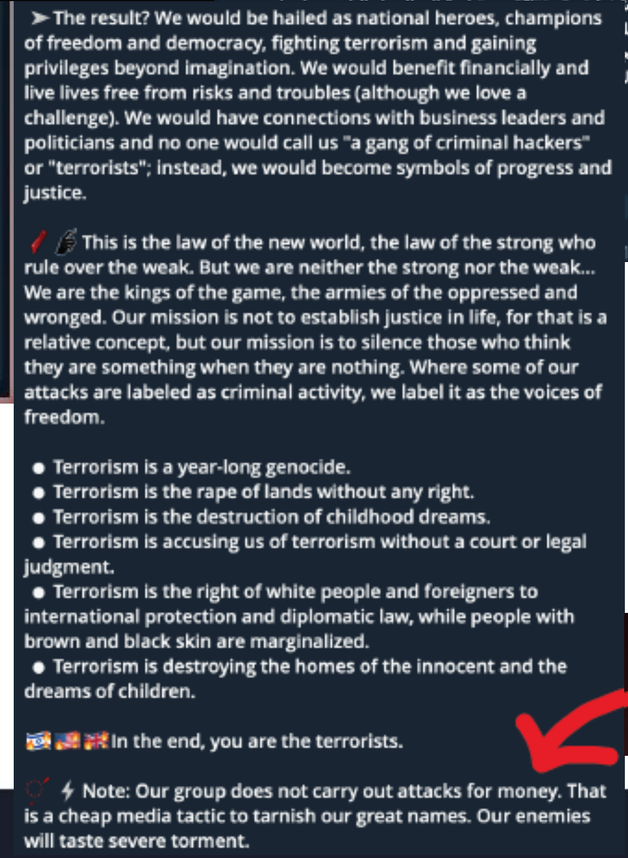
Mereka ingin hidup di dunia yang sempurna.
Ini adalah khayalan dan tidak dapat dicapai!

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

Contoh serangan Hacktivist



Ideology



Not for money

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

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

Who is Mr. Hacker?

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.

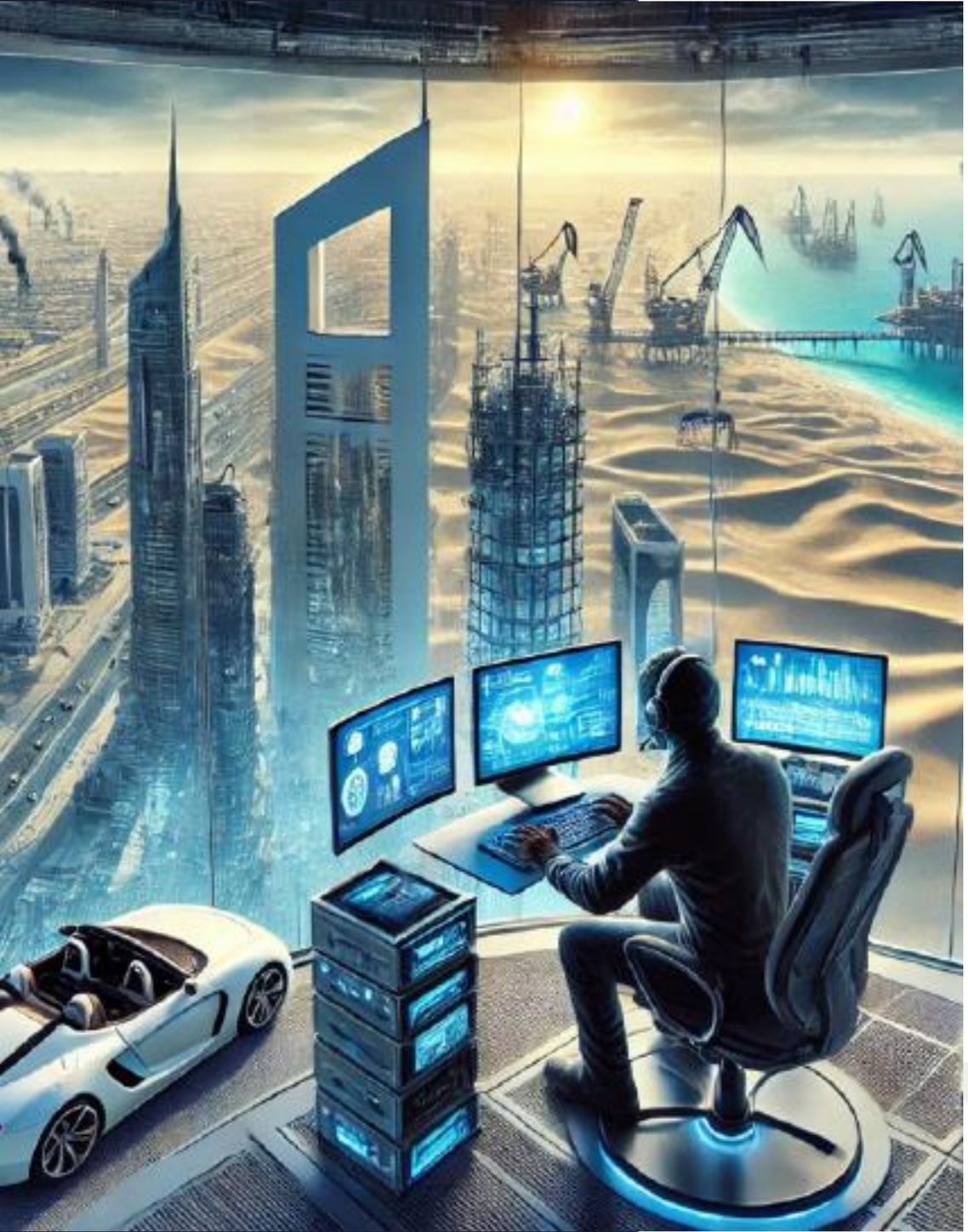
Winnti, yang juga dikenal dengan nama *Blackfly* atau *Wicked Panda*, merupakan salah satu contoh *Advanced Persistent Threat* yang diduga terkait dengan Tiongkok. Aktif sejak tahun 2010, kelompok ini dikenal karena operasi mereka yang bertujuan untuk pencurian informasi dan spionase.

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!



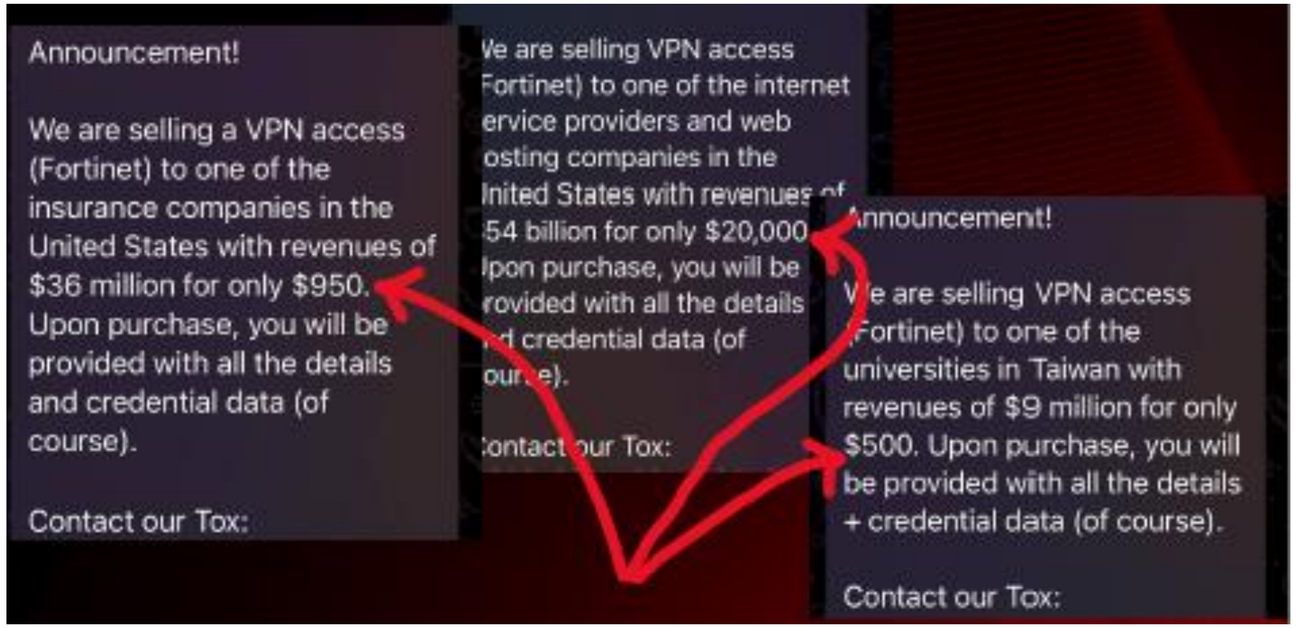
Namun bagaimana jika kita melihat kejahatan dunia maya dari sudut pandang bisnis dan pasar?!

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 phishing
- Conducting DDoS attacks
- Data theft
- Detection testing
- Re-encryption
- Abuse-resistant hosting
- VPN services
- Botnet rental
- Malware development
- Credit card and account verification
- Data verification
- Search engine optimization
- Criminal arbitration
- Money laundering
- Fake website development
- Hiring hackers
- Hiring droppers
- Mules / droppers
- Call center
- Crypto-analytical services
- CAPTCHA bypass
- Background checks
- Card cloning
- Fake ATMs
- Forging documents

Model layanan berkembang

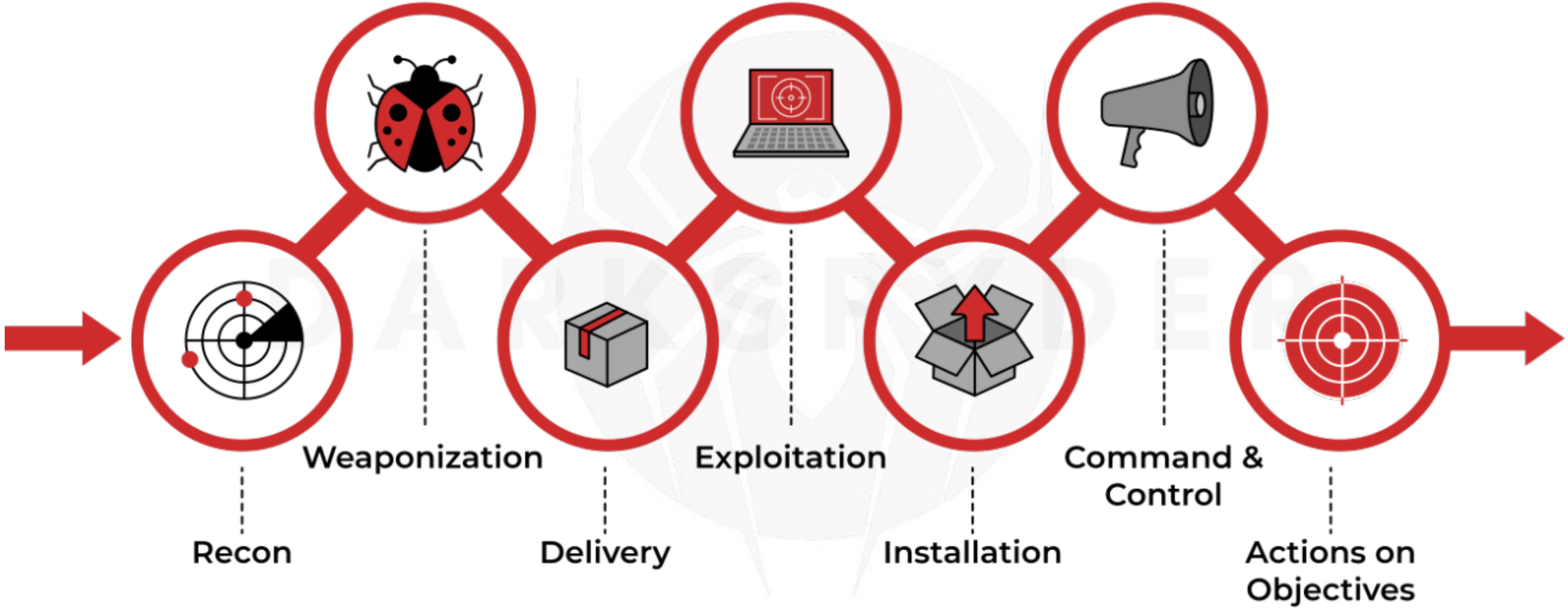
- Destroying a competitor's business
- Digital twins and deepfakes
- Hacker universities
- Creating a hacker marketplace in the darknet
- Advertising in the darknet
- Access to video cameras
- Tracking a person's movement through video cameras
- Commissioned defamation (slander)

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

Cyber Kill Chain



- 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

Crawling Us: sales[at]darkspyder.com

Dubai

New York

Moscow

Singapore

Doha

Indonesia

Next Generation Threat Intelligence