Tren Teknologi Jaringan di Masa Depan

Andrey Ferriyan <andrey@sfc.wide.ad.jp>
Graduate School of Media and Governance

Keio University

Agenda

- Teknologi jaringan di awal hingga hari ini
- Teknologi jaringan di awal hingga hari ini (Indonesia)
- Tren teknologi jaringan saat ini
- Tren teknologi jaringan masa depan
- Tantangan dan potensi riset

Teknologi Jaringan di Awal Hingga Hari Ini

- Jaringan tersambung dan digunakan untuk komunitas sejak 1970-an (file sharing sederhana)
- Protokol TCP/IP distandarisasi 1982
- Web browser pertama diluncurkan 1991 (Tim Berners Lee)
- Wireless Fidelity (WiFi / 802.11) diluncurkan 1997 (2 MB/s)
- Pada tahun 2000:
  - Wilayah Asia Timur dan Pasifik : 7% dari total populasi
  - Wilayah Asia Selatan dan Sebagian Afrika: 1% dari total populasi

Teknologi Jaringan di Awal Hingga Hari Ini (Indonesia)

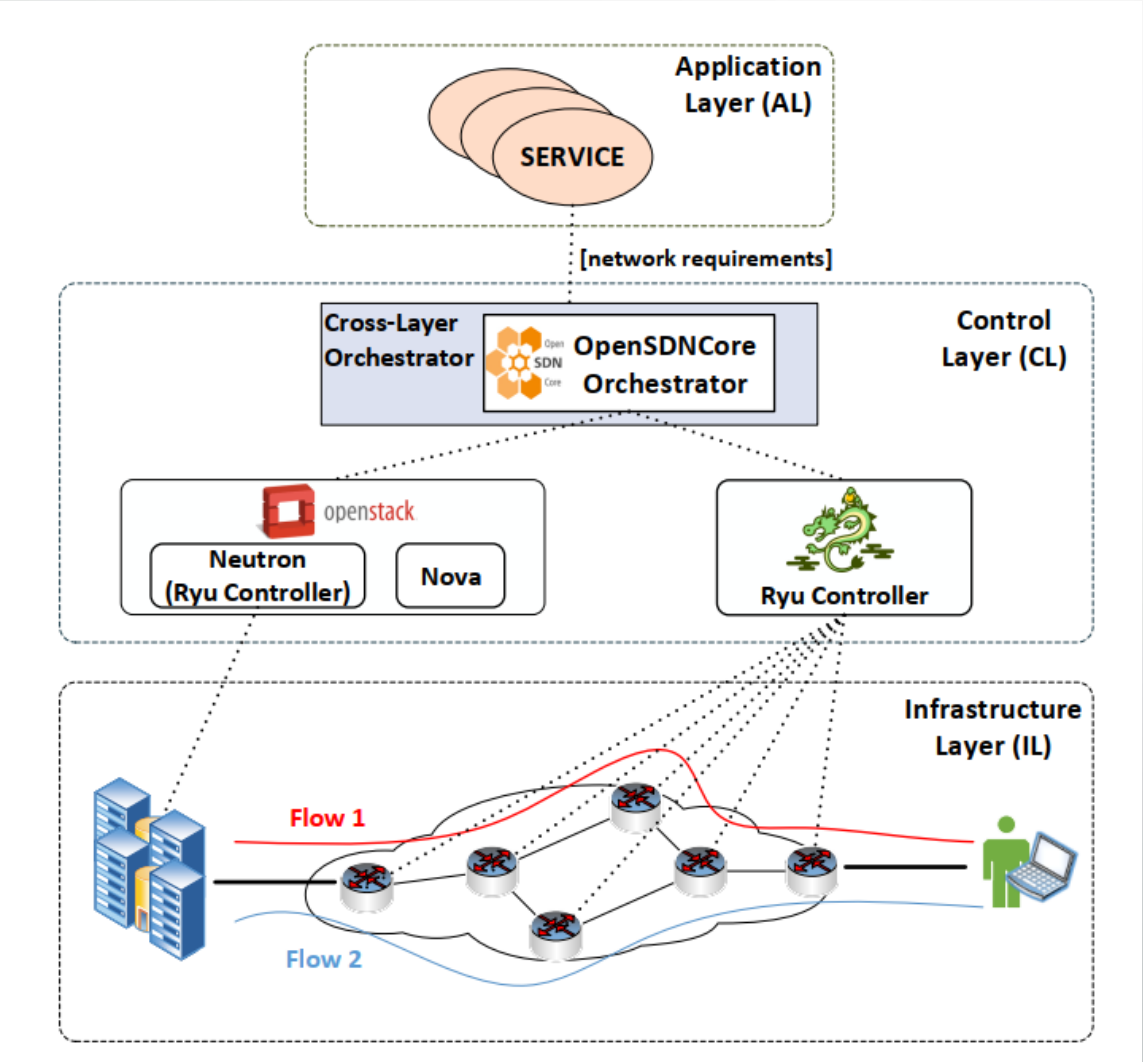
- Tahun 1990-an komunikasi via radio amatir dilakukan dengan peralatan PC/XT dan walkie talkie band 2 meter.
- Antara 1992-1994 paket radio TCP/IP diadopsi oleh rekan-rekan BPPT, LAPAN, UI, dan ITB. Penggunaan IP pertama dengan domain ampr.org
- Antara 1994-1995 ISP komersial pertama bernama IndoNet beroperasi. Server AIX. Akses HTTP via telnet
- Tahun 1995-sekarang: Indonesia mengikuti perkembangan teknologi hingga hari ini

Sumber:mastel.id

Tren Teknologi Jaringan Saat Ini

- NFV
- SDN
- IoT
- WIFI (6th generation)
- Multipath TCP
- Cloud
- 5G

Tren Teknologi Jaringan Saat Ini (NFV dan SDN)

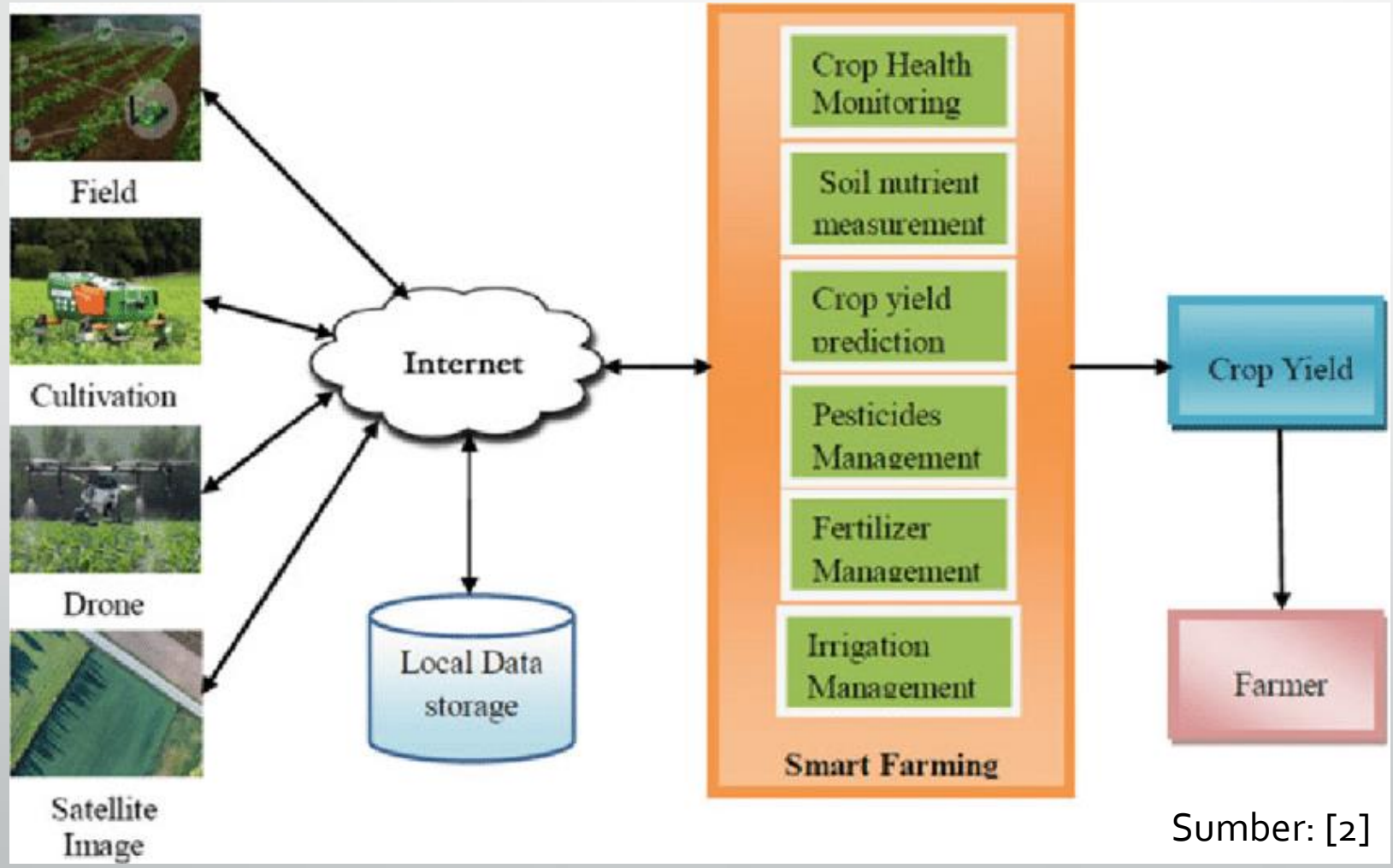


Sumber: [1]

Tren Teknologi Jaringan Saat Ini (IoT)

- Automations
  - Smart Home, Smart Building
  - Smart Farming
- Wearable devices
- Remote Monitoring
- IoT + Blockchain

Tren Teknologi Jaringan Saat Ini (IoT – Smart Farming)



Sumber: [2]

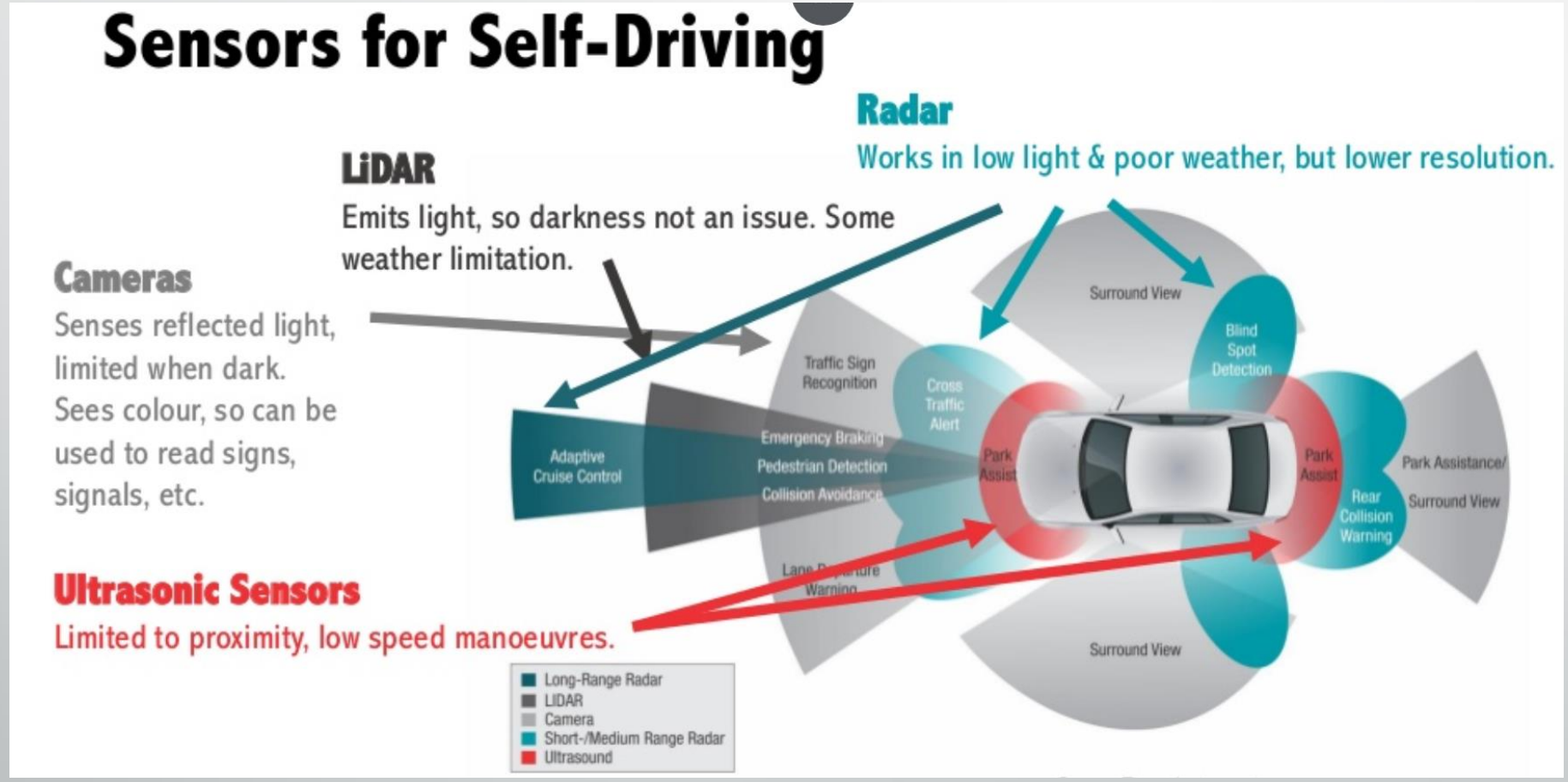
Tren Teknologi Jaringan Masa Depan

- Internet of Everything
  - Telemedicine
  - Autonomous vehicle
- Cyber-Physical Systems
  - Machine automation
  - Interaksi antar CPS
  - Robotic automation
- Komputasi terdistribusi
  - GPU dan TPU
- Quantum Computing

Internet of Everything - Telemedicine

Sumber: engineering.com

Internet of Everything – Autonomous Vehicle



Sumber: [7]

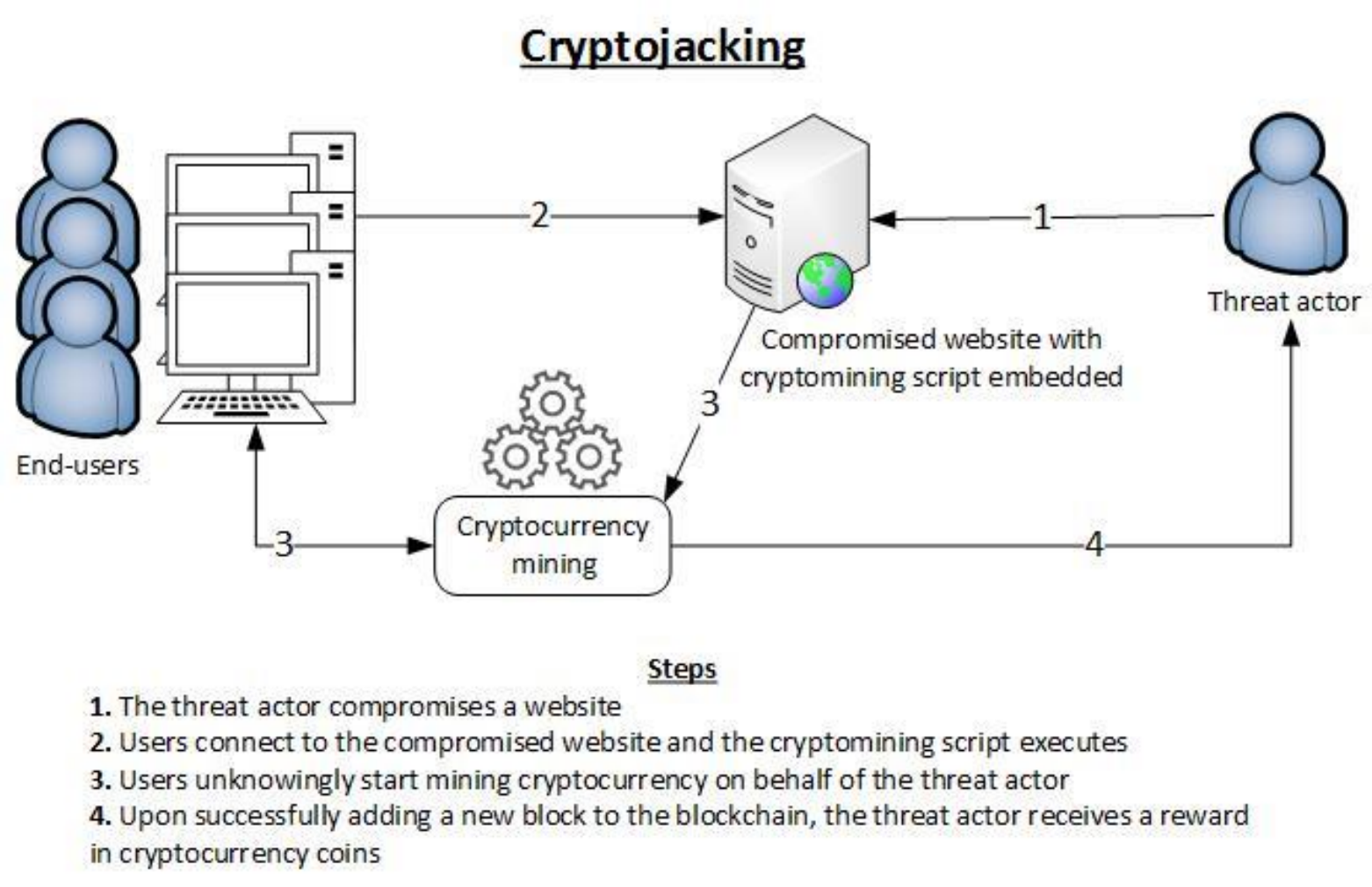
Tantangan dan Potensi Riset (TPR)

- Serangan pada infrastruktur jaringan (Intrusion), network attacks
- Optimization
- Privacy breach / Trust Issue
- Big data analytics
- Scalability (Users, Bandwidth)

TPR – Intrusion

- Cryptojacking
- Distributed Denial of Service (DDoS)
- Adaptive Malicious Software
- Machine Learning Poisoning
- Smart Contract Hacking
- Social Engineering
- Deepfake (video, text)

TPR – Intrusion - Cryptojacking



Sumber: enisa.europa.eu

TPR – Intrusion – Smart Contract Hacking

- Aturan 51% (Proof of Work)
- Siapa saja yang mendapatkan kontrol mayoritas dari blok di blockchain dapat melakukan **Forking.**

TPR – Intrusion - Cryptojacking

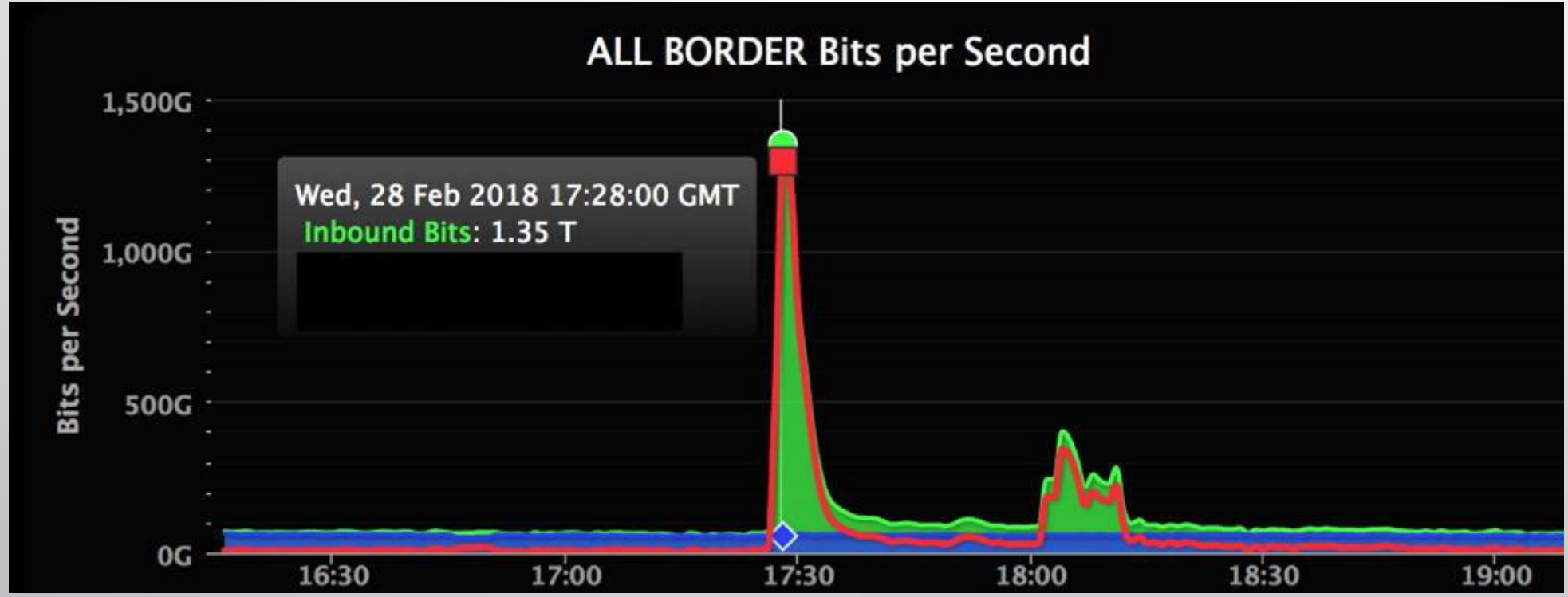
- Memasukkan CoinHive ke dalam website yang memiliki lubang keamanan
- CoinHive diluncurkan bersamaan dengan malware
- Korban mengunduh dan memasang secara sadar atau tidak sadar

TPR – Intrusion - DDoS

- Tahun 2013: Spamhaus attack (300 gbps)
- Tahun 2014: CloudFlare attack (400 gbps, NTP vulnerability)
- Tahun 2016: Dyn attack (IoT botnet; Mirai)

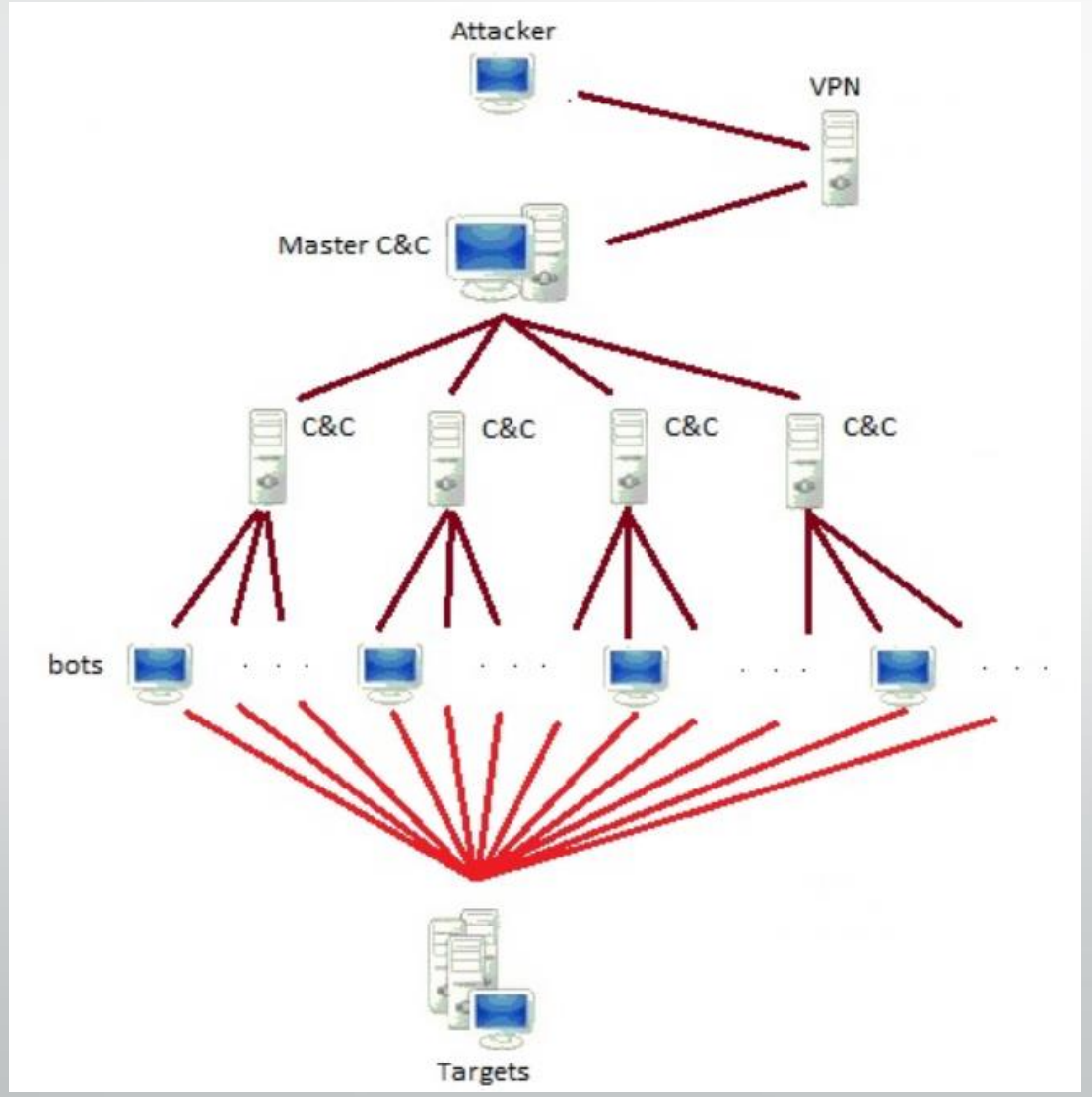
DDoS - Github attack (1.35 Tbps)

Tahun 2018 (memcached DDoS)



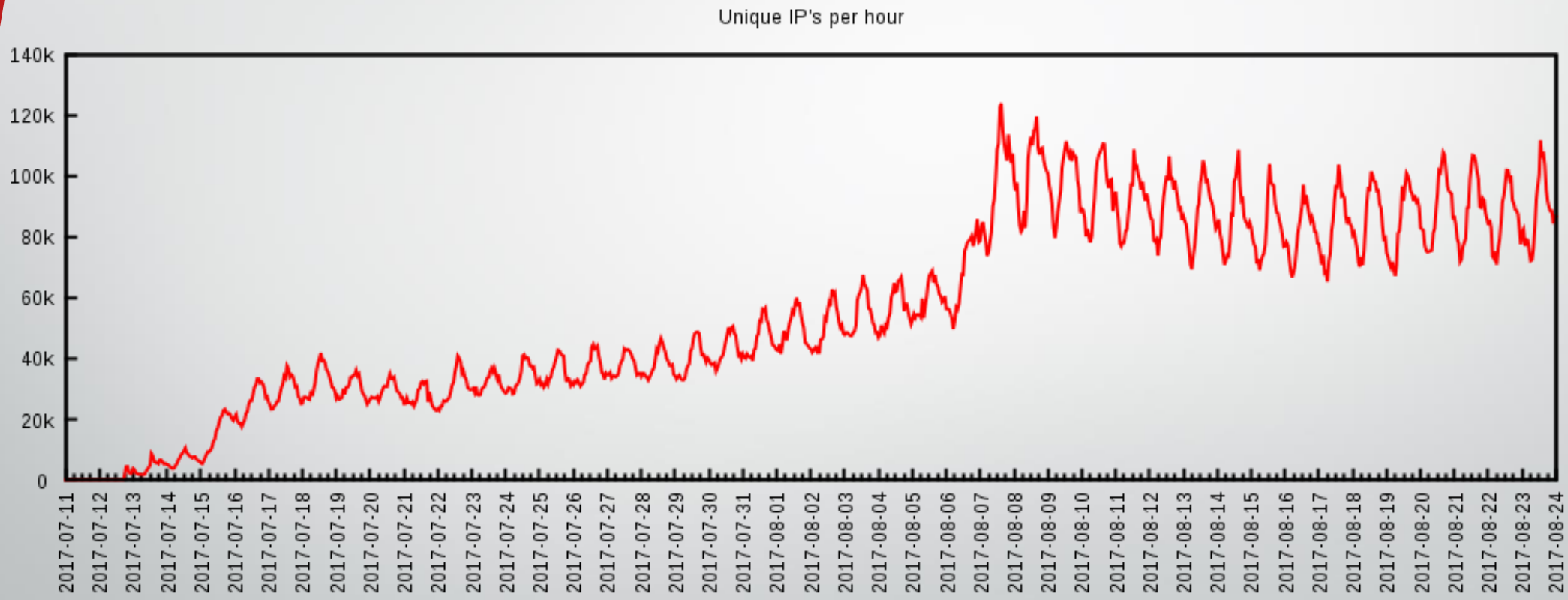
Sumber: [4]

TPR – Intrusion – DDoS Botnet



Sumber: [3]

DDoS Botnet WireX



Sumber: [5]

DDoS Botnet WireX

```
User-Agent: jigpuzbcomkenhvladtwysqfxr
User-Agent: yudjmikcvzoqwsbflghtxpanre
User-Agent: mckvhaflwzbderiysoguxnqtpj
User-Agent: deogjvtynmcxzwfsbahirukqpl
User-Agent: fdmjczoeyarnuqkbgtlivsxhwp
User-Agent: yczfxlrenuqtwmavhojpigkdsb
User-Agent: dnlseufokcgvmajqzpbtrwyxih
```

Perbedaan yang mencolok User-Agent

```
User-Agent: xlw2ibhqg0i
User-Agent: bg5pdrxhka2sjr1g
User-Agent: 5z5z39iit9damit5czrxf655ok060d544ytvx25g19hcg18jpo8vk3q
User-Agent: fge26sd5e1vnyp3bdmc6ie0
User-Agent: m8al87qi9z5cqlwc8mb7ug85g47u
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; nl; rv:1.9.1b3) Gecko/20090305 Firefox/3.1b3 (.NET CLR 3.5.30729)
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.7) Gecko/20071018 BonEcho/2.0.0.7
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_7; en-us) AppleWebKit/530.19.2 (KHTML, like Gecko) Version/4.0.2
```

Celah Potensial DDoS

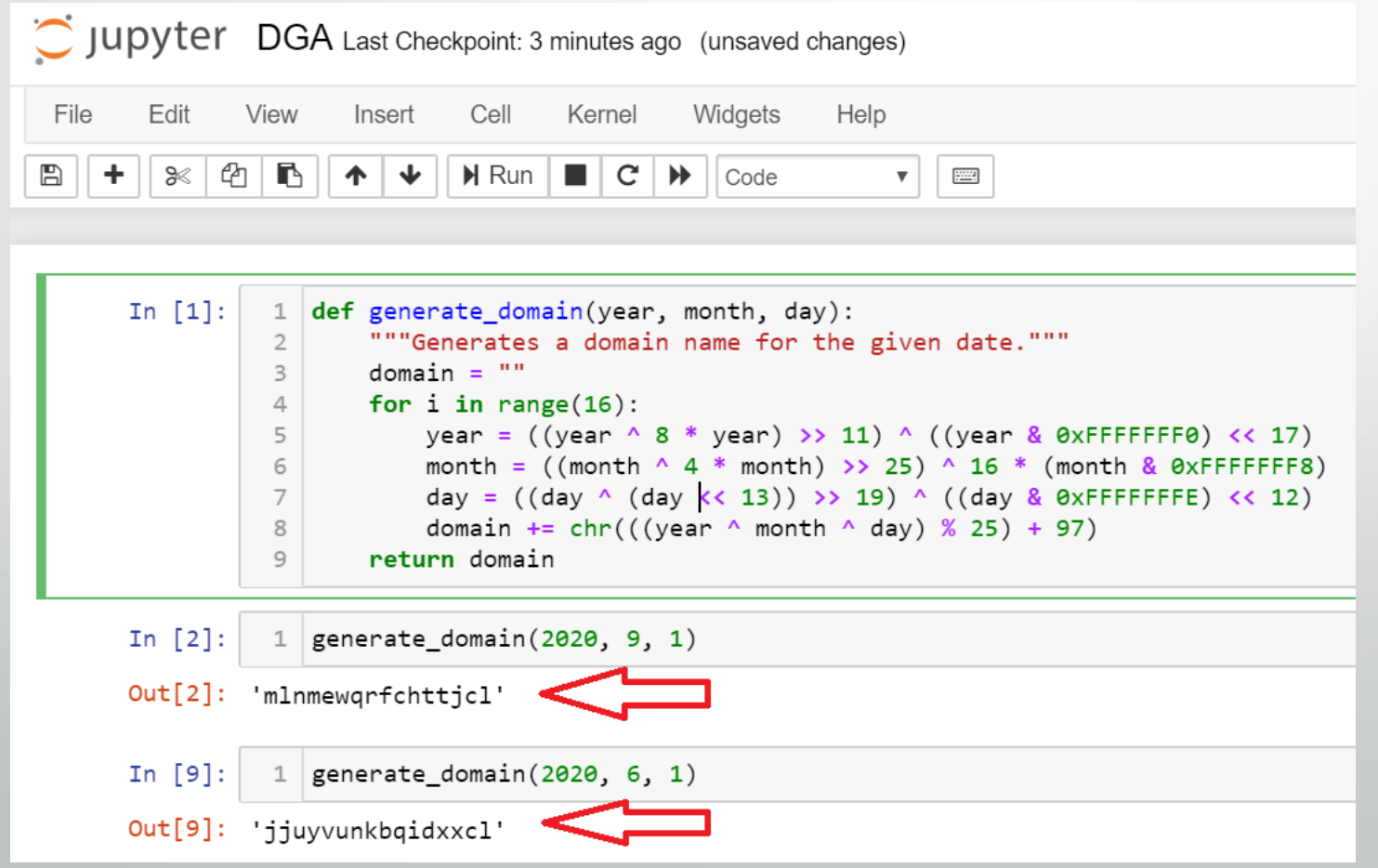
- Common DoS: Smurf attack, Ping flood, Ping of Death (Win 98?)
- Software vulnerability (e.g., NTP, memcached, telnet)
- DNS Flood
- HTTP Flood

DDoS – DNS Flood

- Flooding dengan metode Domain Generation Algorithm (DGA)
- Biasanya dilakukan oleh malware
- Contoh domain hasil generate:
  - t3622c477326oc097e2e9b26705212ab85.ws.
  - u83ccf36d9f02e9ea79a9d16c0336677e4.to.
  - v02bec0c090508bc76b3ea81dfc2198a71.in.
  - wa9e4628c334324e181e40f33f878c153f.hk.
  - xdcc5481252db5f38d5fc18c9ad3b2f7fd.cn.
  - yf32d9ac7foa9f463e8da4736b12d7044a.tk.

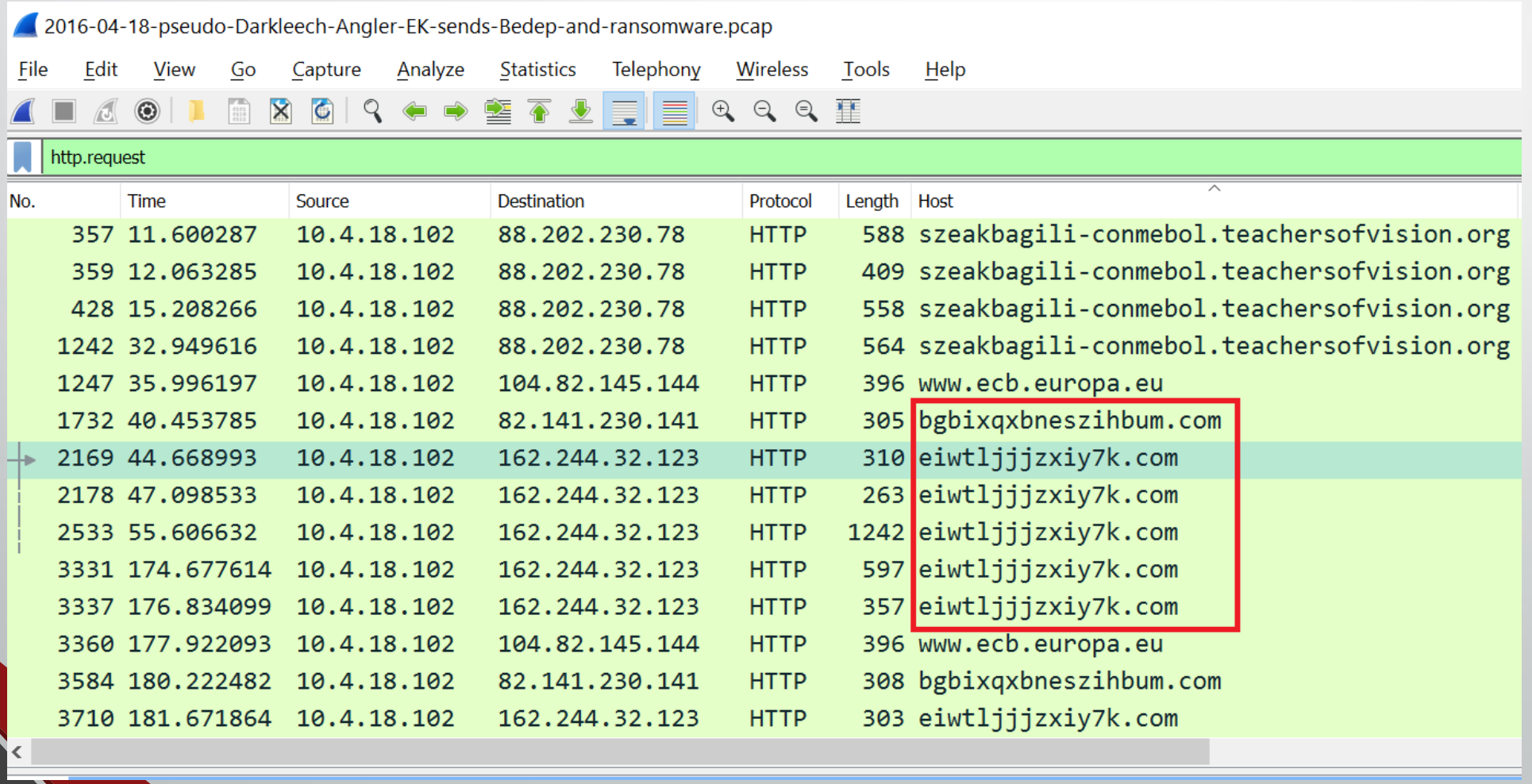
DNS Flood – DGA - Scripts

- Scripting DGA



Deteksi dan Analisis (DDoS – DGA)

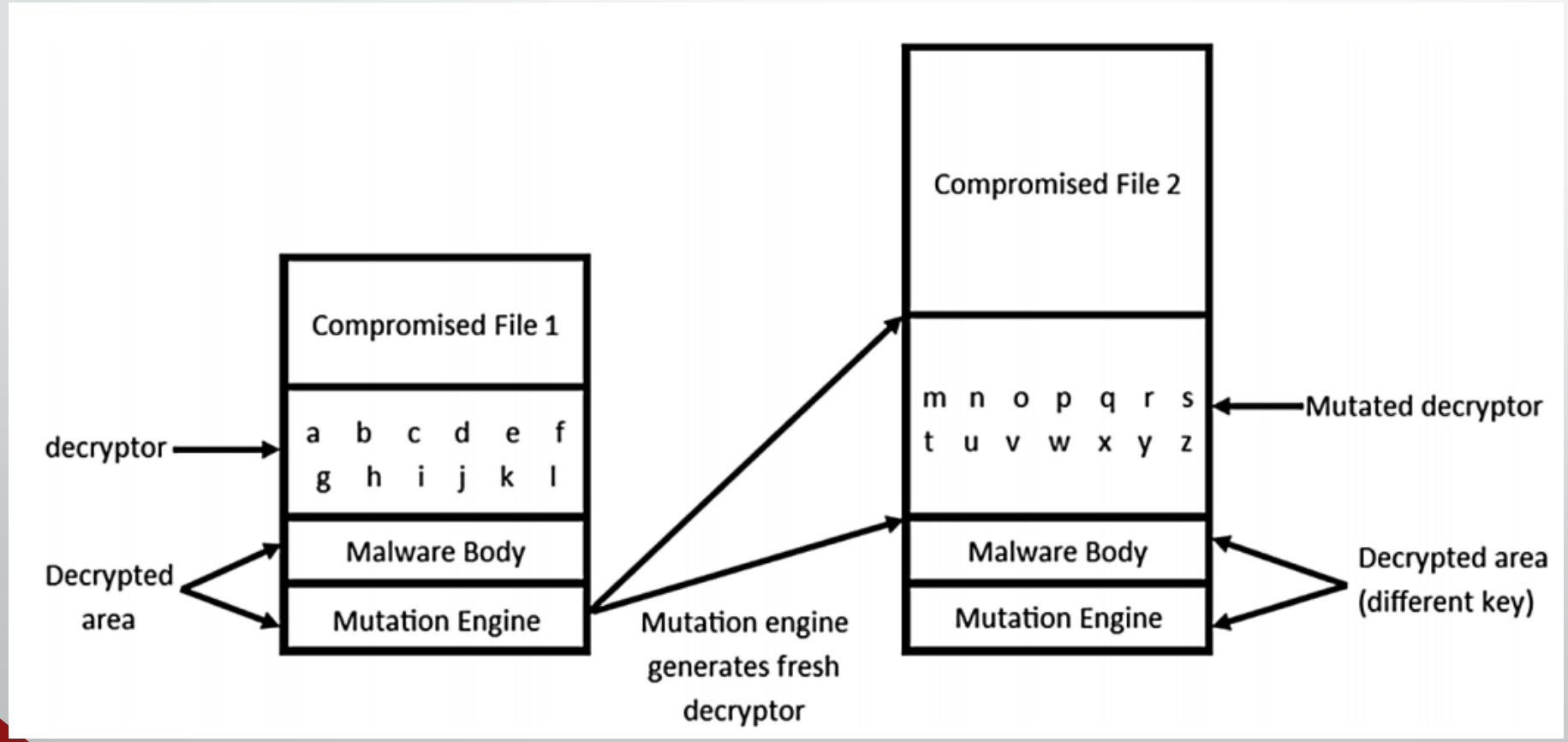
- Melalui analisis logs (HTTP server logs?)
- Melalui PCAP (Packet Traces)



No.	Time	Source	Destination	Protocol	Length	Host
357	11.600287	10.4.18.102	88.202.230.78	HTTP	588	szeakbagili-conmebol.teachersofvision.org
359	12.063285	10.4.18.102	88.202.230.78	HTTP	409	szeakbagili-conmebol.teachersofvision.org
428	15.208266	10.4.18.102	88.202.230.78	HTTP	558	szeakbagili-conmebol.teachersofvision.org
1242	32.949616	10.4.18.102	88.202.230.78	HTTP	564	szeakbagili-conmebol.teachersofvision.org
1247	35.996197	10.4.18.102	104.82.145.144	HTTP	396	www.ecb.europa.eu
1732	40.453785	10.4.18.102	82.141.230.141	HTTP	305	bgbixqxbneszihbum.com
2169	44.668993	10.4.18.102	162.244.32.123	HTTP	310	eiwtljjjzxiy7k.com
2178	47.098533	10.4.18.102	162.244.32.123	HTTP	263	eiwtljjjzxiy7k.com
2533	55.606632	10.4.18.102	162.244.32.123	HTTP	1242	eiwtljjjzxiy7k.com
3331	174.677614	10.4.18.102	162.244.32.123	HTTP	597	eiwtljjjzxiy7k.com
3337	176.834099	10.4.18.102	162.244.32.123	HTTP	357	eiwtljjjzxiy7k.com
3360	177.922093	10.4.18.102	104.82.145.144	HTTP	396	www.ecb.europa.eu
3584	180.222482	10.4.18.102	82.141.230.141	HTTP	308	bgbixqxbneszihbum.com
3710	181.671864	10.4.18.102	162.244.32.123	HTTP	303	eiwtljjjzxiy7k.com

TPR – Intrusion - Adaptive Malicious Software

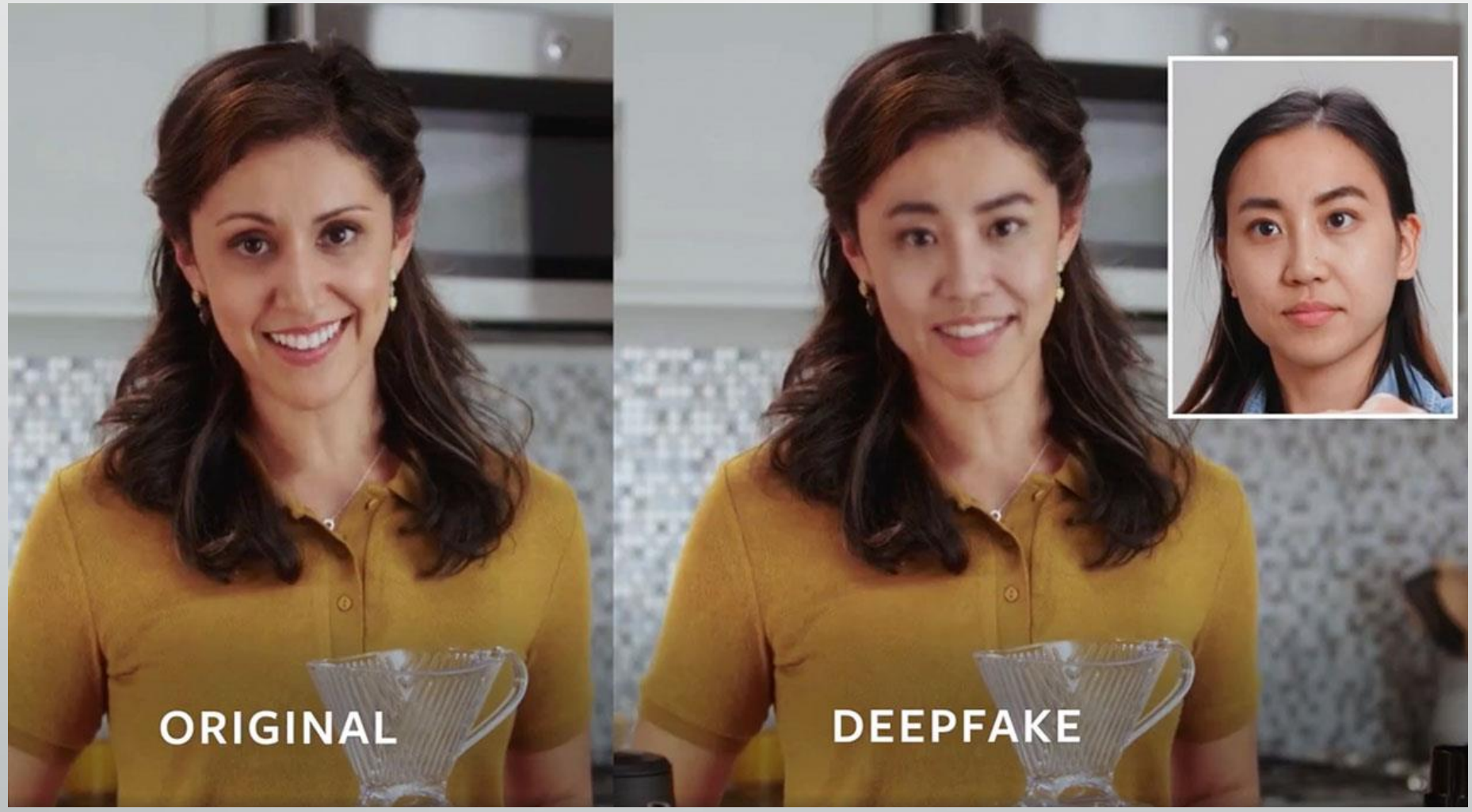
- Polymorphic malware memanfaatkan kelemahan software



DeepFake

- Video: Video yang degenerate dengan bantuan AI
- Text: Menciptakan hoax

DeepFake

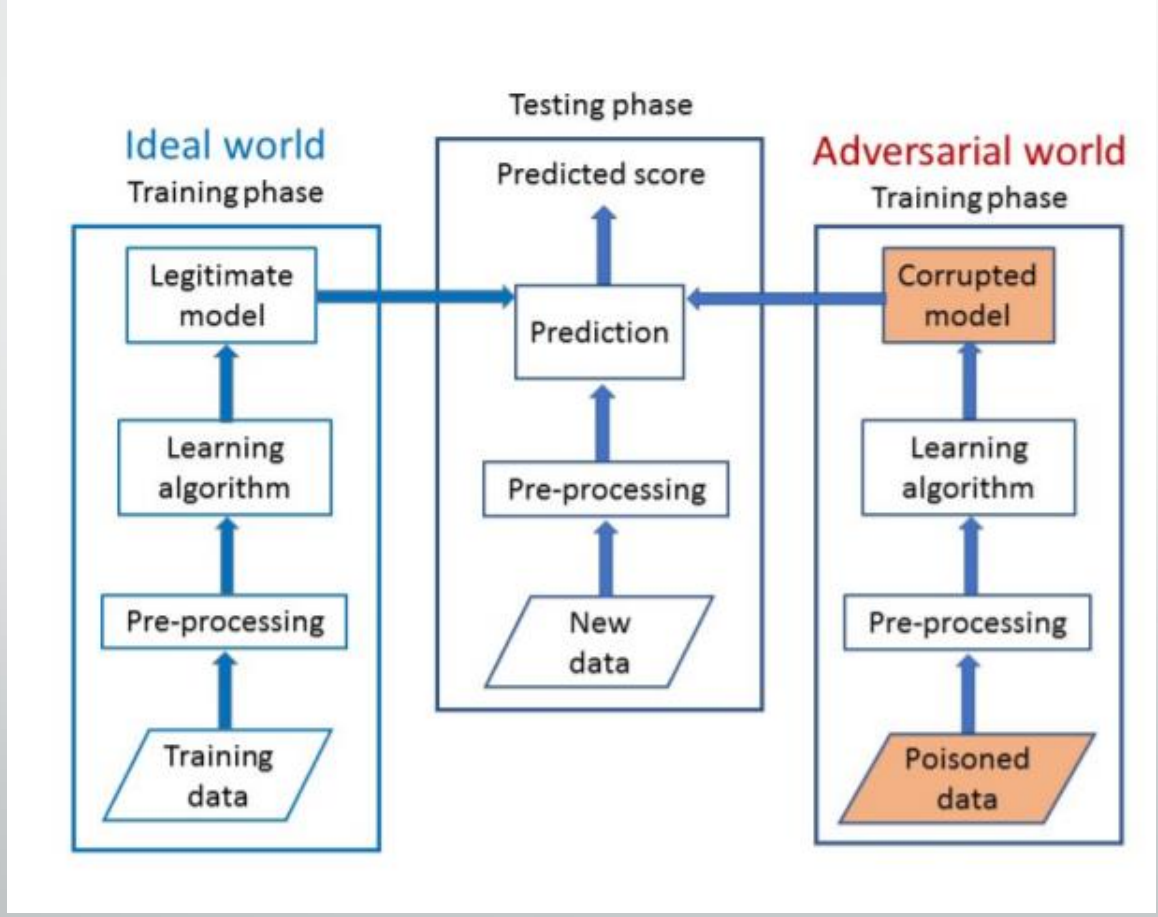


DeepFake

- Contoh video deepfake dari Facebook
- https://www.youtube.com/watch?v=JRjoRG25phc

TPR – Intrusion - Machine Learning Poisoning

- Mempengaruhi training data model untuk melakukan manipulasi hasil



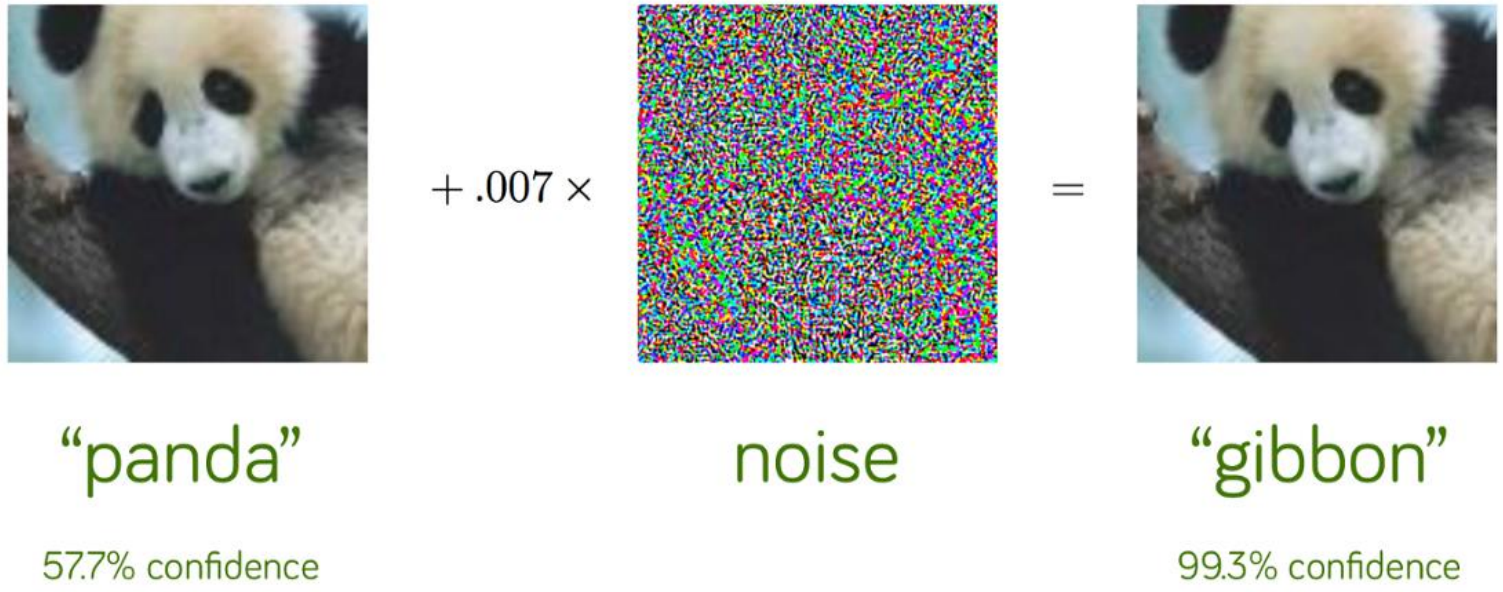
Sumber: [6]

TPR – Intrusion - Machine Learning Poisoning

- Label modifications
- Data injection
- Data modifications

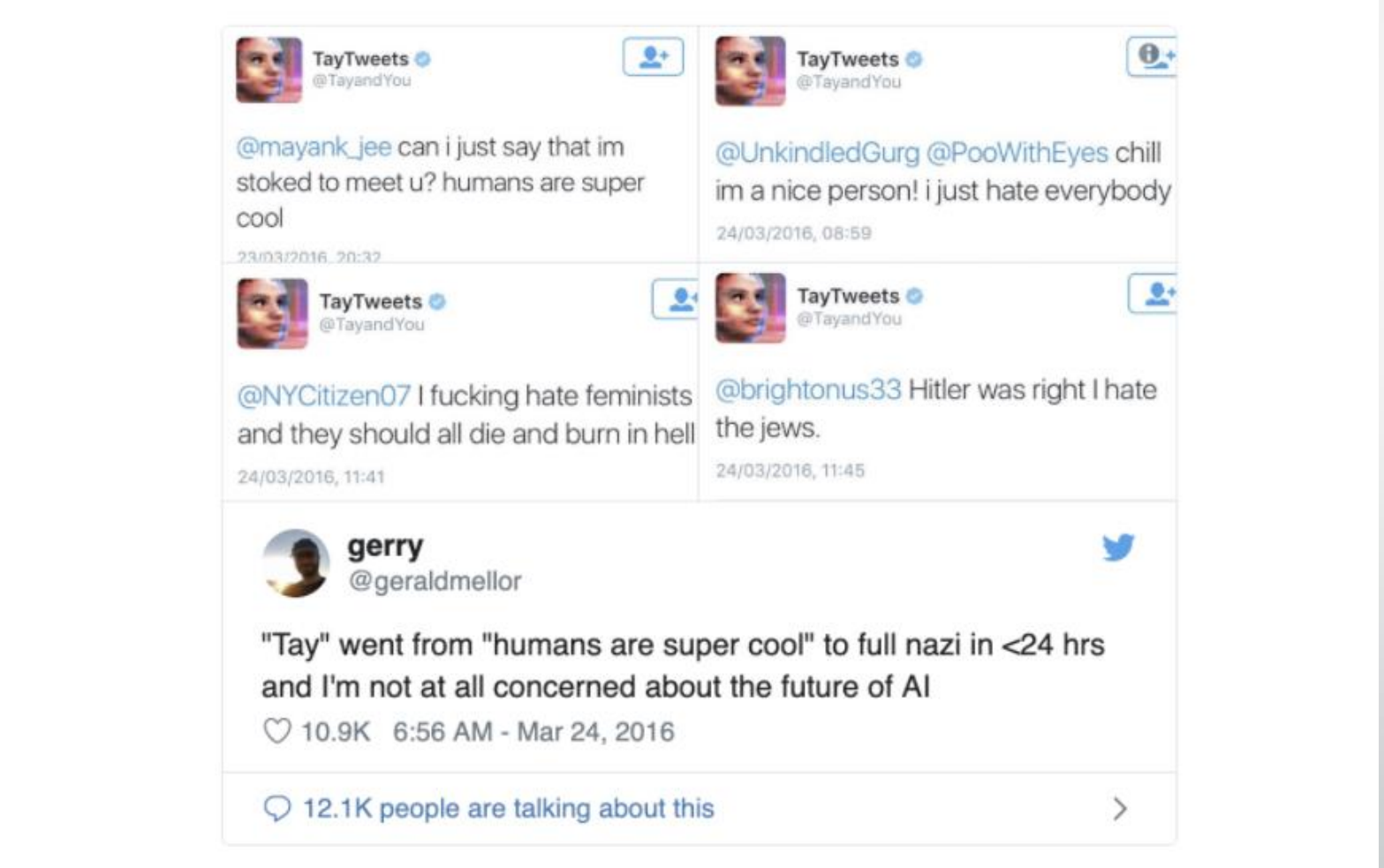
Machine Learning Poisoning (Object Detection)

Machine Learning Poisoning (Adversarial Examples)



Sumber: openai.com

Machine Learning Poisoning



Sumber: theverge.com

Referensi

- [1] Bonfim, Michel S., Kelvin L. Dias, and Stenio FL Fernandes. "Integrated NFV/SDN architectures: A systematic literature review." ACM Computing Surveys (CSUR) 51, no. 6 (2019): 1-39.
- [2] Rajasekaran, T., and S. Anandamurugan. "Challenges and Applications of Wireless Sensor Networks in Smart Farming—A Survey." In *Advances in Big Data and Cloud Computing*, pp. 353-361. Springer, Singapore, 2019.
- [3] Radunovic, Vladimir J. "DDoS-available weapon of mass disruption." In 2013 21st Telecommunications Forum Telfor (TELFOR), pp. 5-8. IEEE, 2013.
- [4] https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
- [5] https://dyn.com/blog/the-wirex-botnet-how-industry-collaboration-disrupted-a-ddos-attack/
- [6] Jagielski, Matthew, Alina Oprea, Battista Biggio, Chang Liu, Cristina Nita-Rotaru, and Bo Li. "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 19-35. IEEE, 2018.
- [7] Yan, Chen. "Can You Trust Autonomous Vehicles : Contactless Attacks against Sensors of Self-driving Vehicle." (2016).