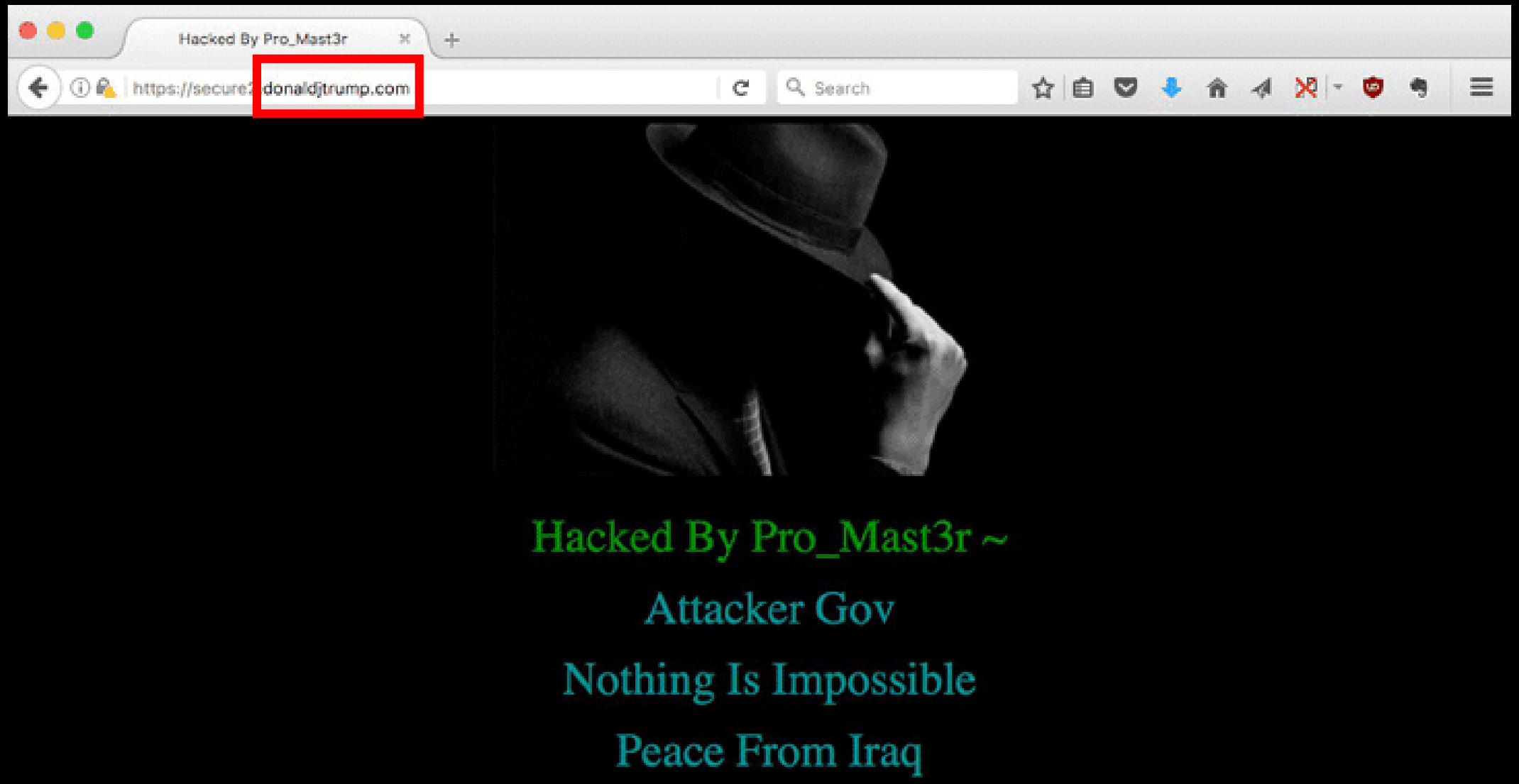

Hacked By Pro_Mast3r
https://secure3.donaldjtrump.com
Search
Hacked By Pro_Mast3r ~
Attacker Gov
Nothing Is Impossible
Peace From Iraq

Anatomy of an attack..

Cel: firma Aupticon
Branża: technologie, R&D, self-driving cars

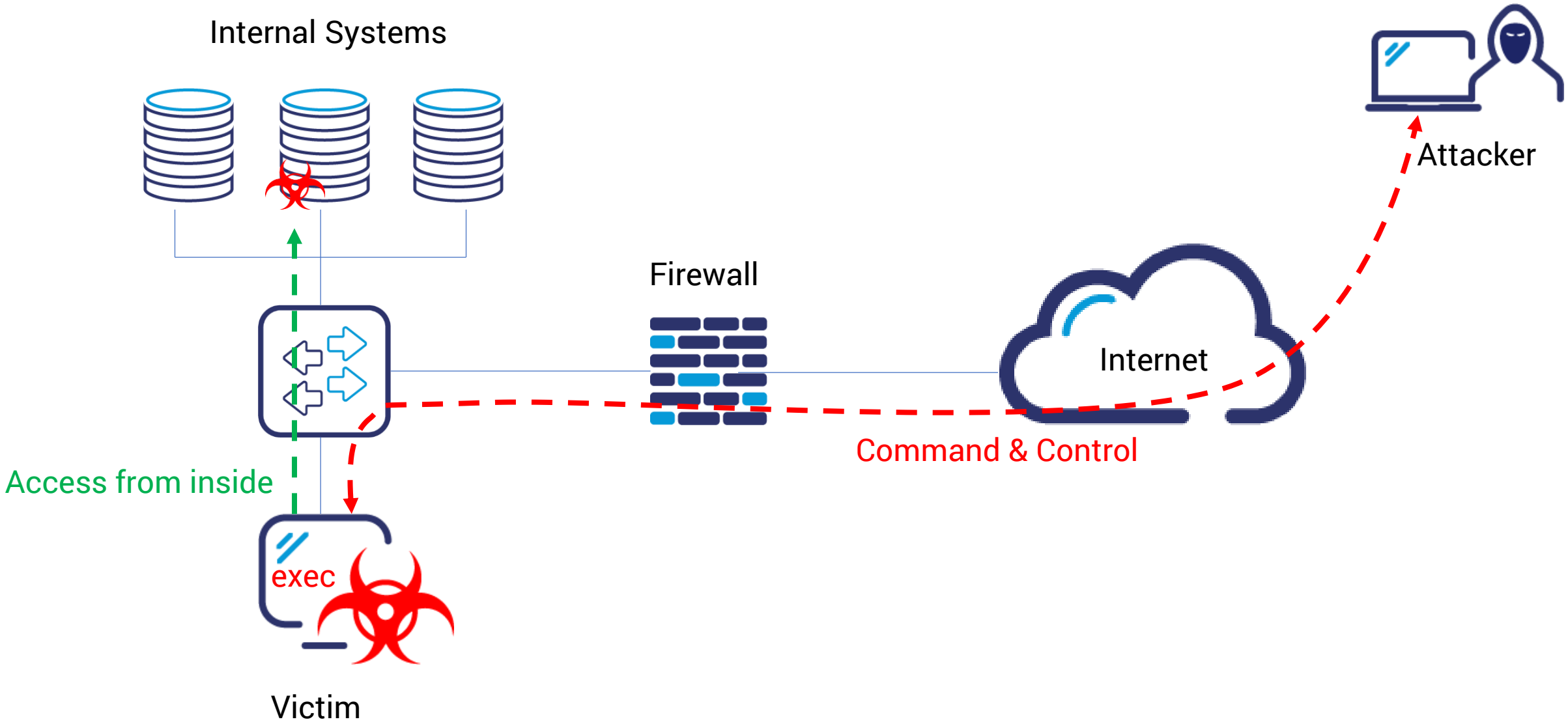
Firma Aupticon została zdestabilizowana, zaszyfrowano treści, wstrzymano systemy

Ale zacznijmy od początku

#1 Reconnaissance aka RECON

#2 Initial compromise

#3 Command and control (C&C)


Internal Systems
Attacker
Firewall
Internet
Command & Control
Access from inside
exec
Victim

#4 Toolset installation

cracks

Scanners

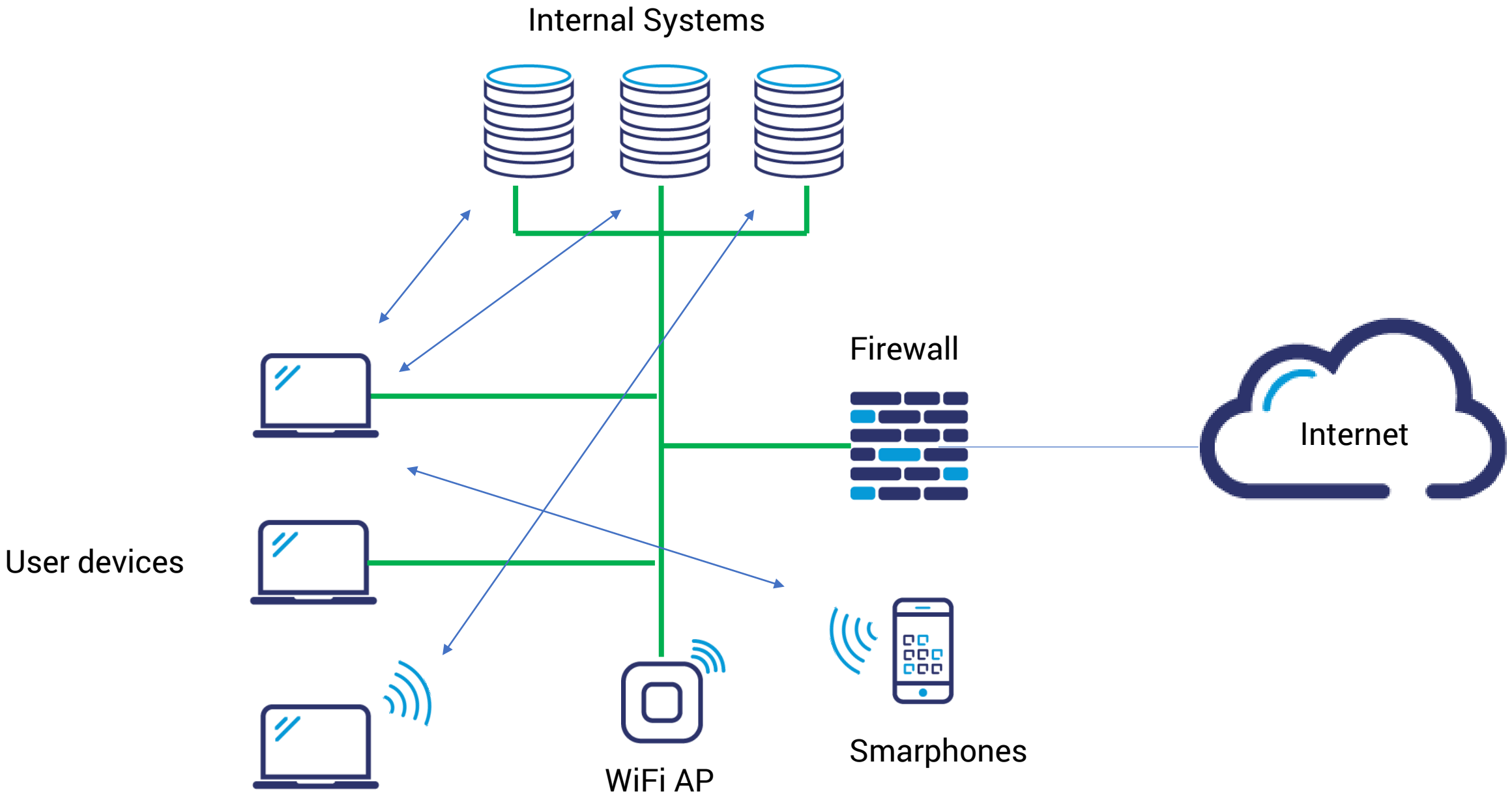
Scripts

sniffers

decryptors

Spoofing deamons

#5 Czym jest flat network ?


Internal Systems
Firewall
Internet
User devices
WiFi AP
Smarphones

Co możemy zrobić na poziomie sieci?

Łakome kąski:

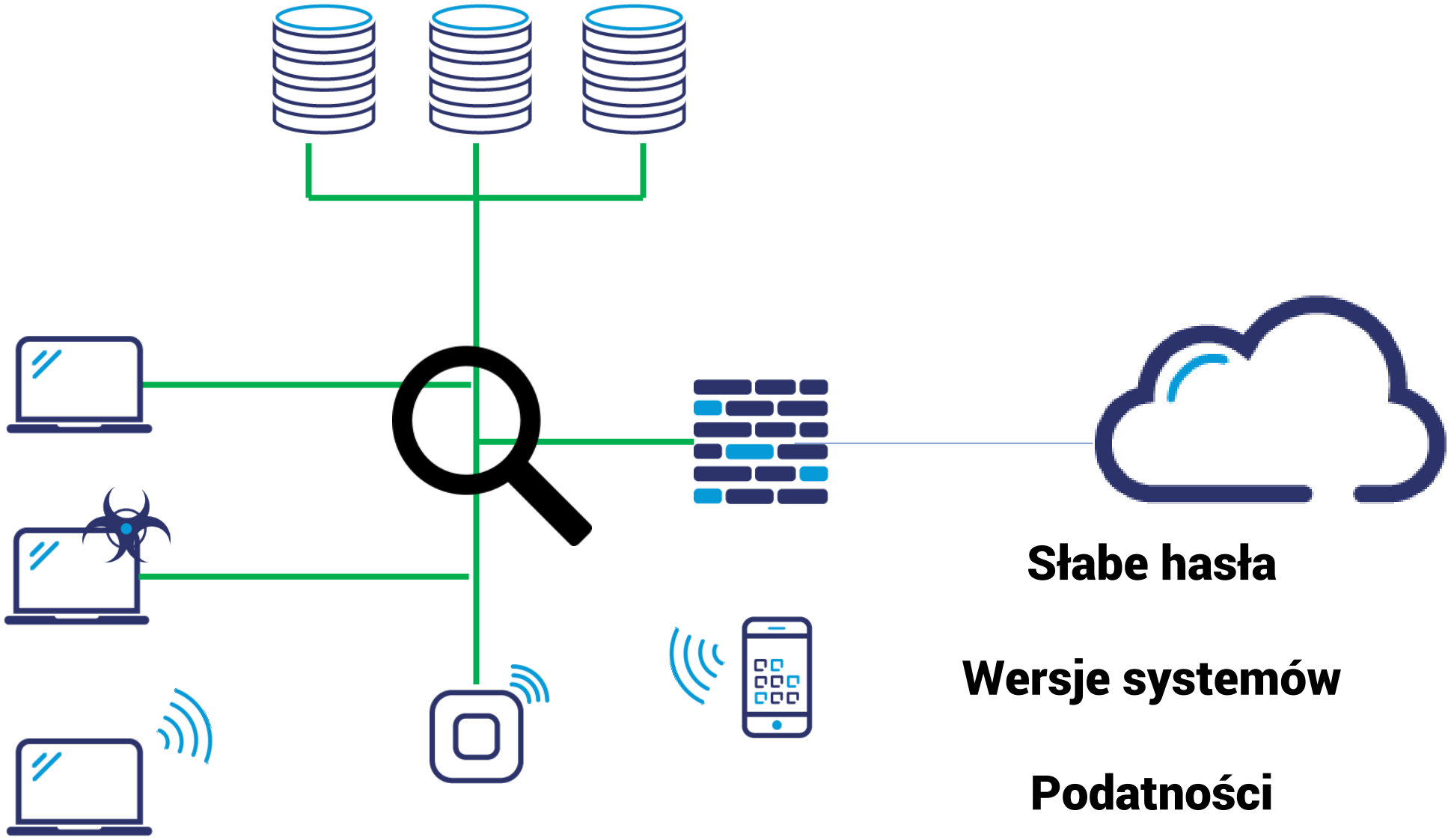
#Know how

#Lista klientów

#Payroll / Wynagrodzenia

#Corruption / Disruption

Skanujemy sieć uzyskując listę podatności i systemów

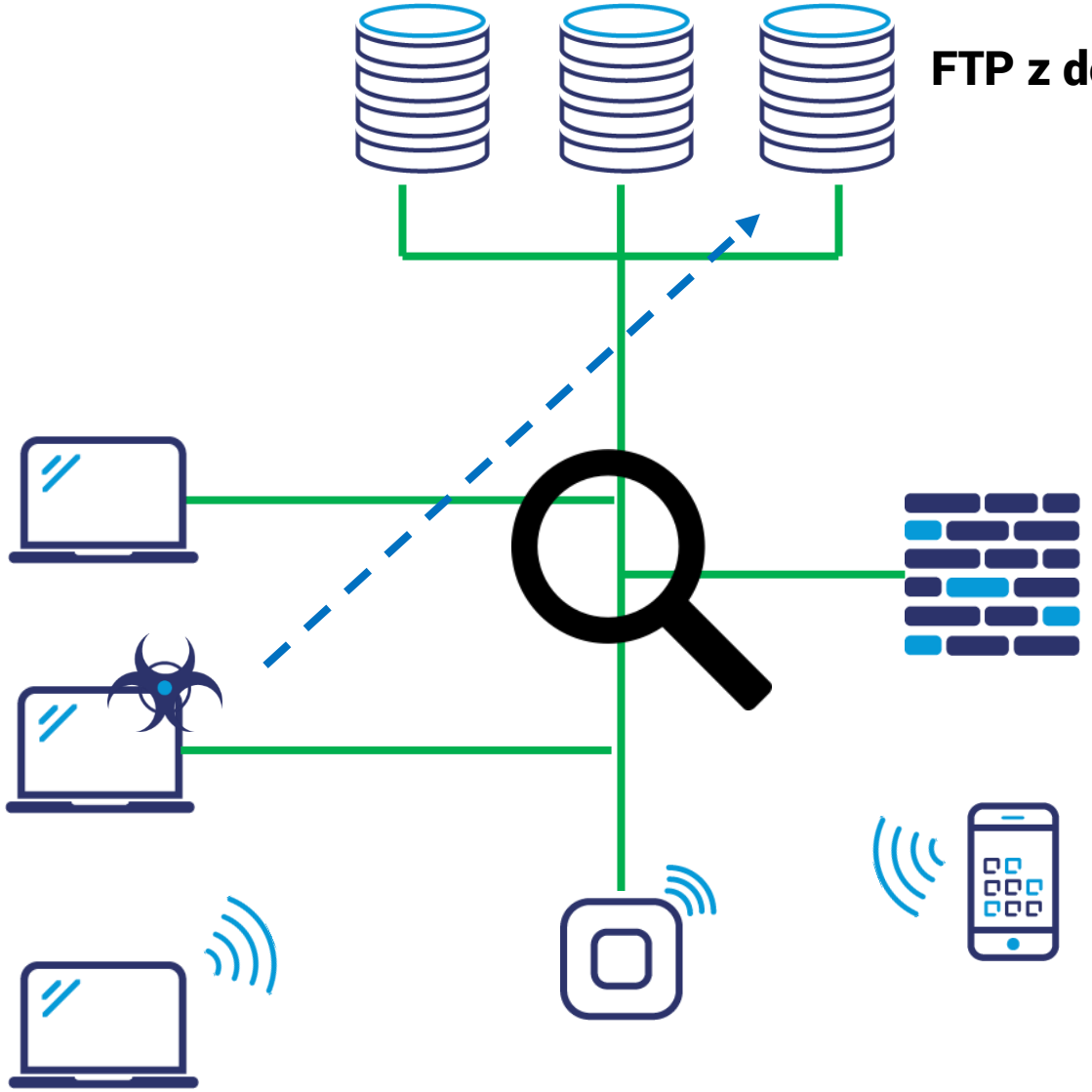


Słabe hasła

Wersje systemów

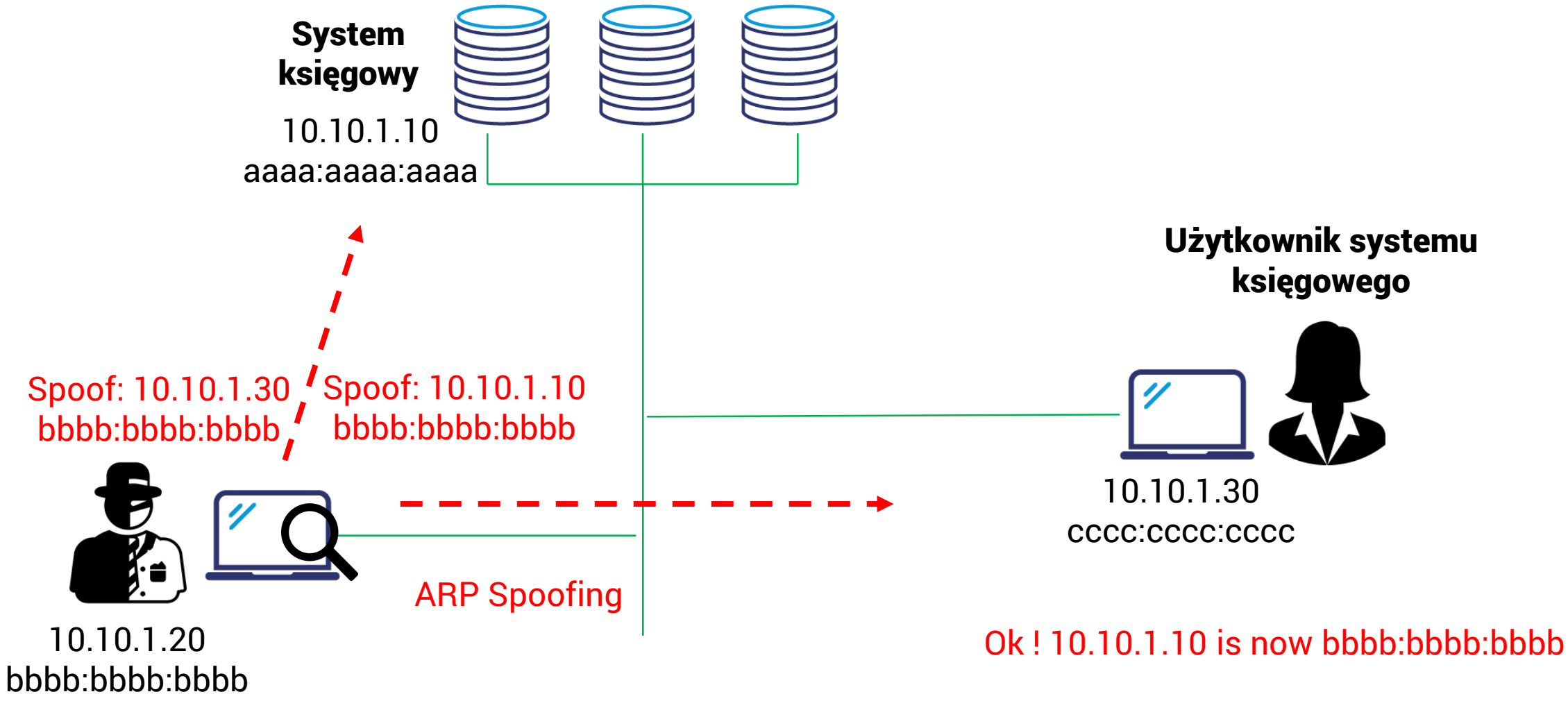
Podatności

Z know how było łatwo – hasło admin/admin123



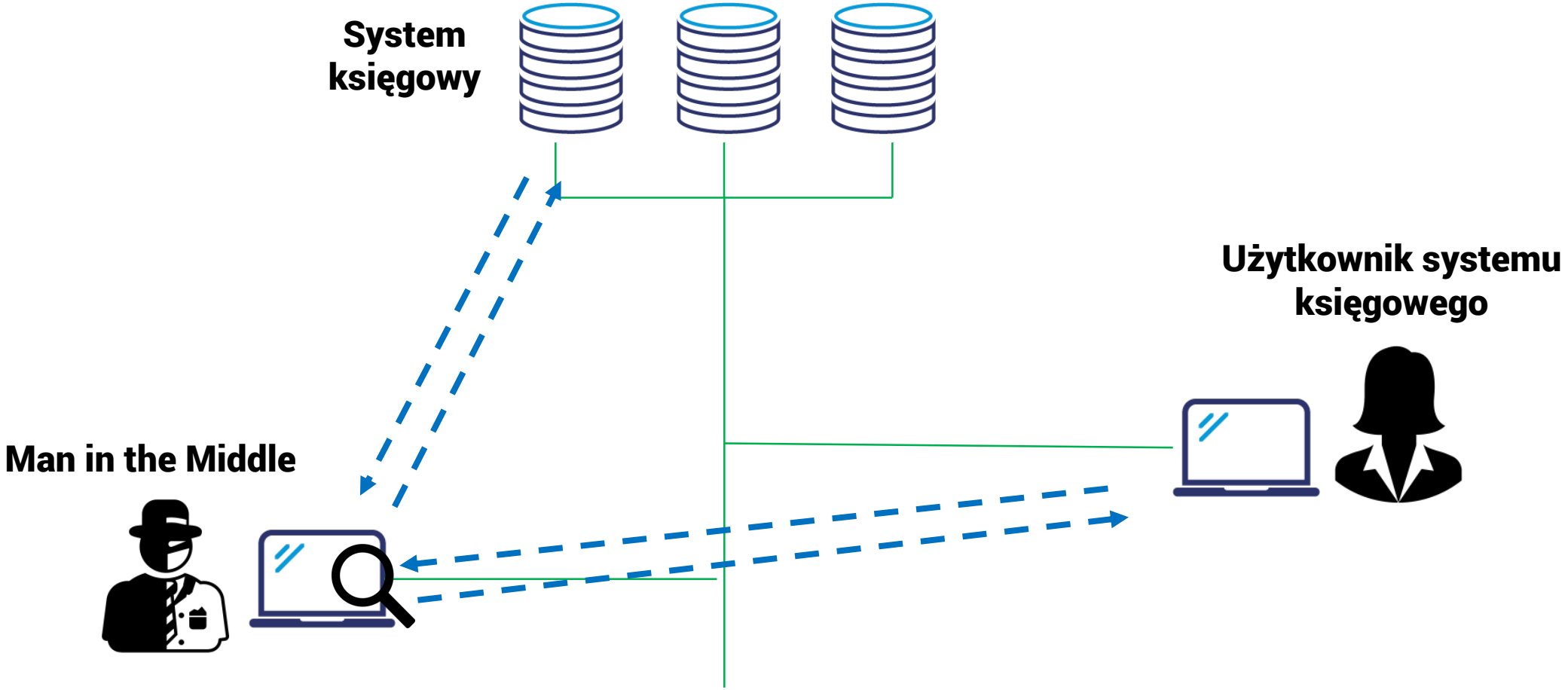
Dictionary attack

Ok, znaleźliśmy system księgowy, ale hasło jest silne...



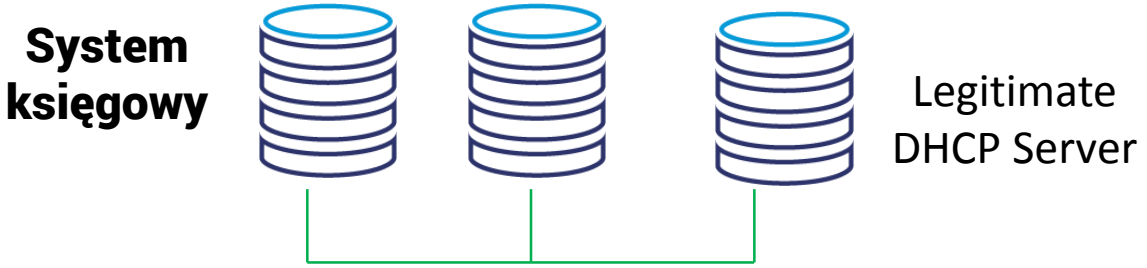
Jak nazywa się atak, w którym atakujący znajduje się na ścieżce między nadawcą, a odbiorcą?

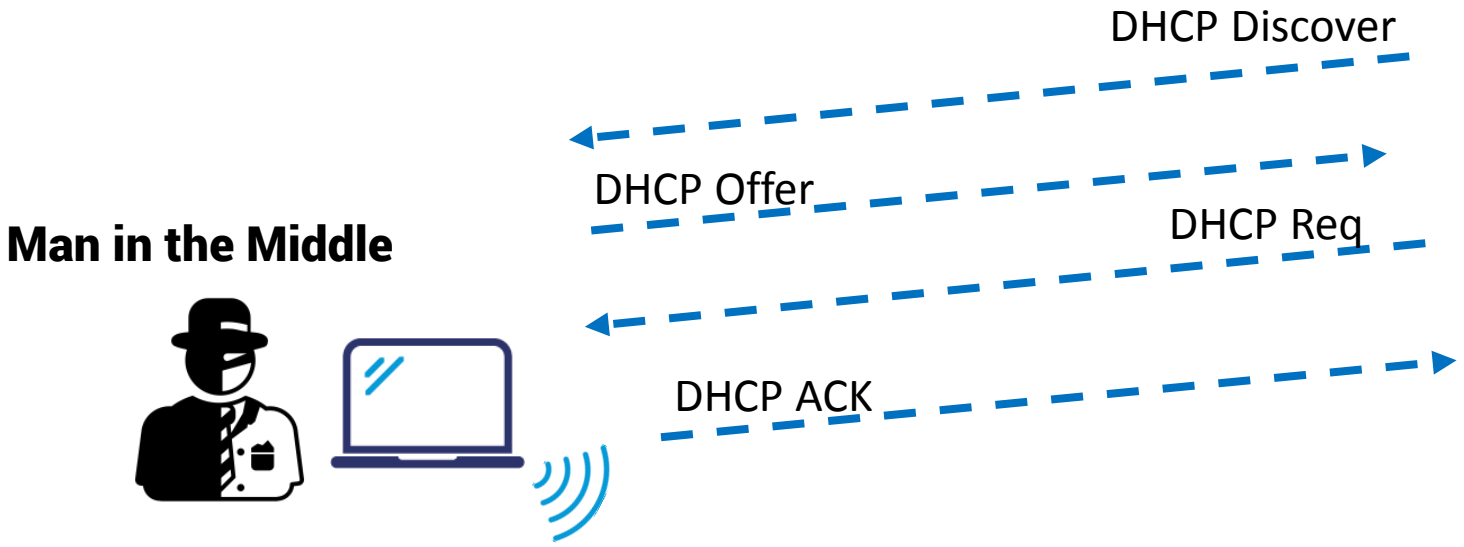
Teraz system księgowy myśli, że użytkownik jest pod nowym MAC, i odwrotnie...



Przyglądamy się ruchowi i po kilku minutach mamy użytkownika i hasło !

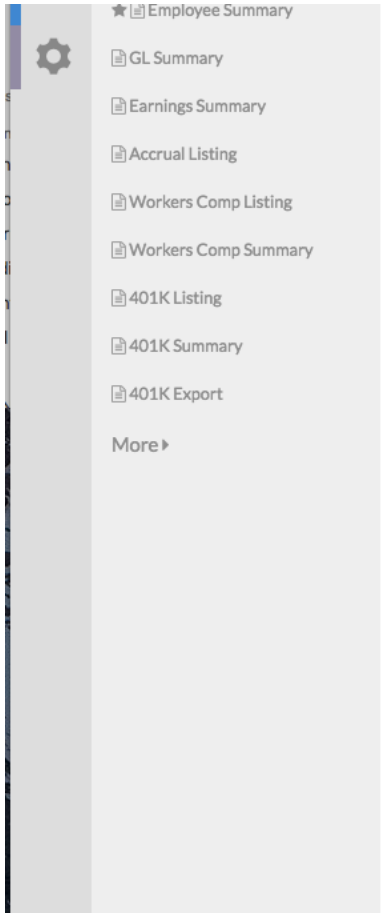
Inny przykład MITM aplikowany łatwo w sieciach Wifi 802.11 – DHCP + DNS spoofing





Czy jesteście pewni, że DNS, który dostajecie w ramach Hot Spot, nie jest podstawiony?

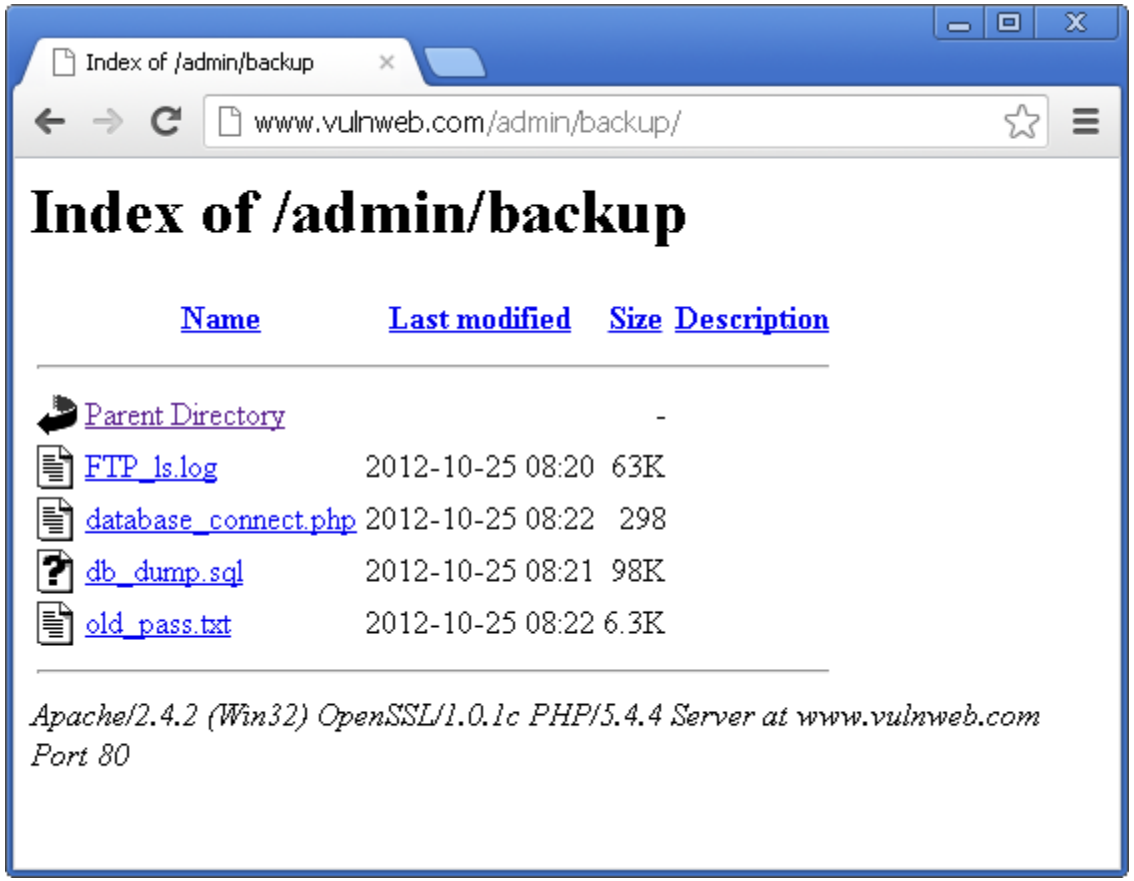
Czemu oni tyle zarabiają?



Number of results: 39

Run	Num	Date	Name	Gross	Withholding	Employer	Deductions	Net
73	22222..	4/28/2017	Jenni Barn	$20,000.00	$8,314.87	$42.00	$0.00	$11,685.13
73	DD23...	4/28/2017	Bill Curran	$4,000.00	$1,420.48	$346.20	$1,000.00	$1,579.52
73	22222..	4/28/2017	Will Curran	$200.00	$0.00	$0.00	$0.00	$200.00
73	DD23...	4/28/2017	TJ Diamond	$290.00	$48.01	$22.19	$0.00	$241.99
73	22222..	4/28/2017	John Does	$8,000.00	$3,051.10	$612.00	$0.00	$4,948.90
73	DD23...	4/28/2017	Bertram Gilfoyle	$2,800.00	$373.38	$233.75	$1,100.00	$1,326.62
73	22222..	4/28/2017	Darryl Hannah	$8,200.00	$3,405.22	$627.30	$100.00	$4,694.78
73	22222..	4/28/2017	Theodore Iles	$100.00	$9.90	$13.75	$0.00	$90.10
73	22222..	4/28/2017	Mark Matters	$385.00	$62.77	$52.94	$0.00	$322.23
73	22222..	4/28/2017	Andre Amesley	$750.00	$155.57	$103.13	$0.00	$594.43
73	DD24...	4/28/2017	Arden Miles	$1,040.00	$172.72	$13.63	$100.00	$767.28
73	22222..	4/28/2017	John Smith	$2,630.00	$347.57	$201.20	$600.00	$1,682.43
73	22222..	4/28/2017	Angela Thomas	$1,750.00	$487.81	$139.43	$3.00	$1,259.19
72	22222..	4/28/2017	Jenni Barn	$20,000.00	$8,314.87	$42.00	$0.00	$11,685.13
72	DD22...	4/28/2017	Bill Curran	$4,000.00	$1,420.48	$413.20	$1,000.00	$1,579.52
72	22222..	4/28/2017	Will Curran	$200.00	$0.00	$0.00	$0.00	$200.00
72	DD22...	4/28/2017	TJ Diamond	$290.00	$48.01	$22.19	$0.00	$241.99
72	22222..	4/28/2017	John Does	$8,000.00	$3,051.10	$612.00	$0.00	$4,948.90
72	DD22...	4/28/2017	Bertram Gilfoyle	$2,800.00	$373.38	$233.75	$1,100.00	$1,326.62
72	22222..	4/28/2017	Darryl Hannah	$8,200.00	$3,405.22	$627.30	$100.00	$4,694.78

Z listą klientów to było tak... path traversal



Łakome kąski – co mamy?:

#Know how ✓

#Lista klientów ✓

#Payroll / Wynagrodzenia ✓

#Corruption / Disruption

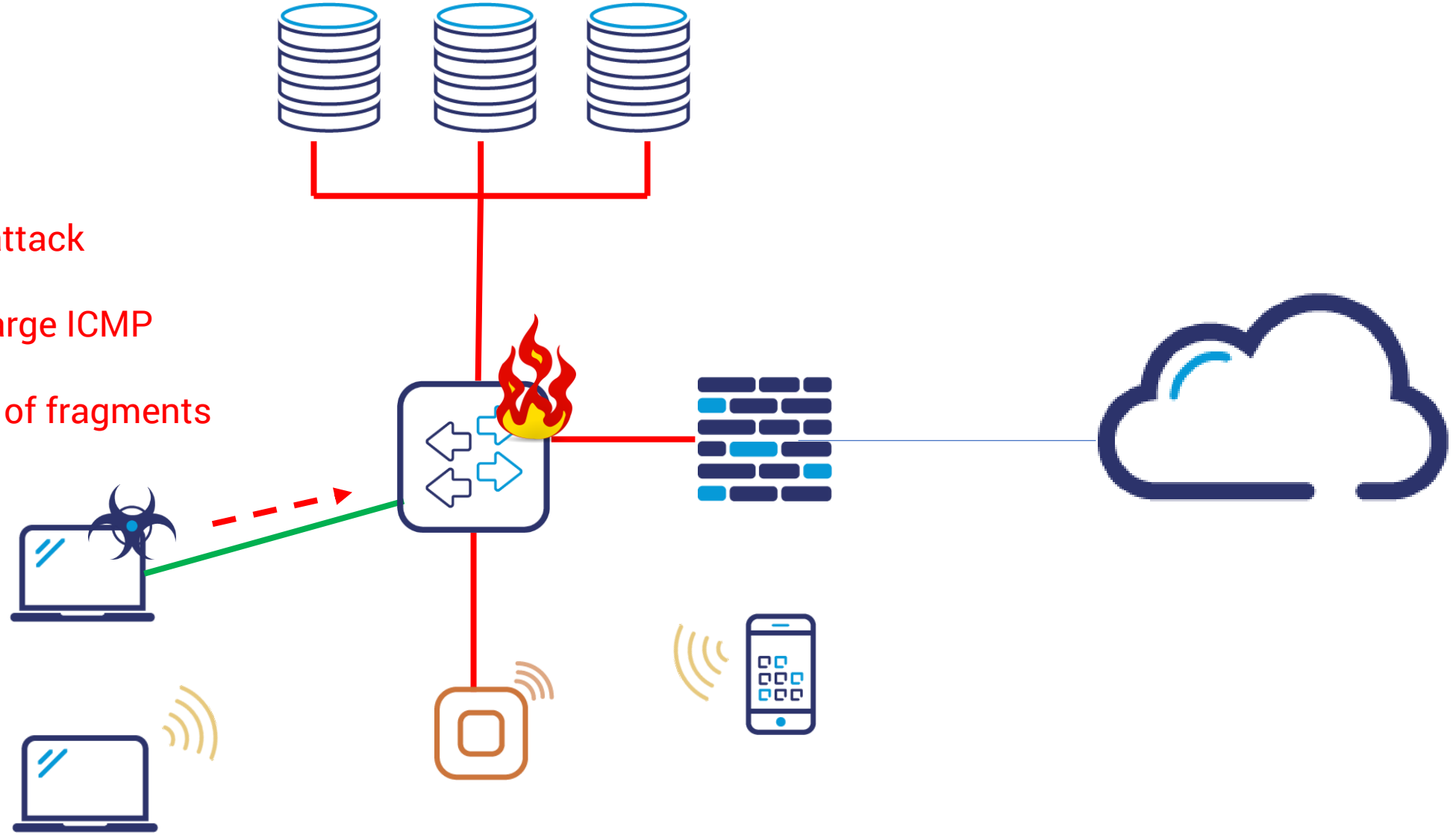
Destabilizacja sieci i systemów

Denial of Service na urządzenia sieciowe

CPU attack

Sending large ICMP

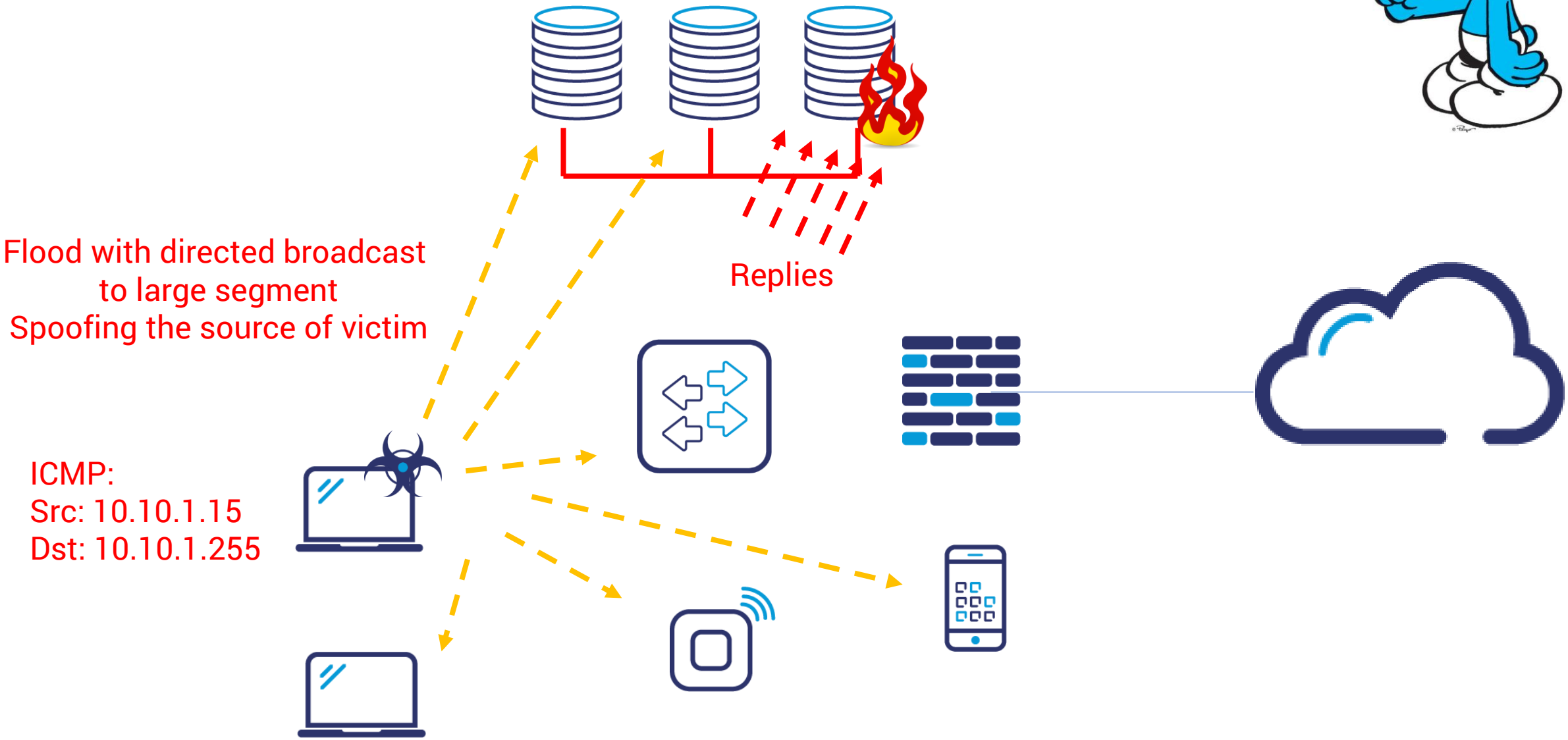
Large volume of fragments



Jak nazywa się atak, w którym w kierunku ofiary wysyłany jest strumień pakietów typu ICMP?

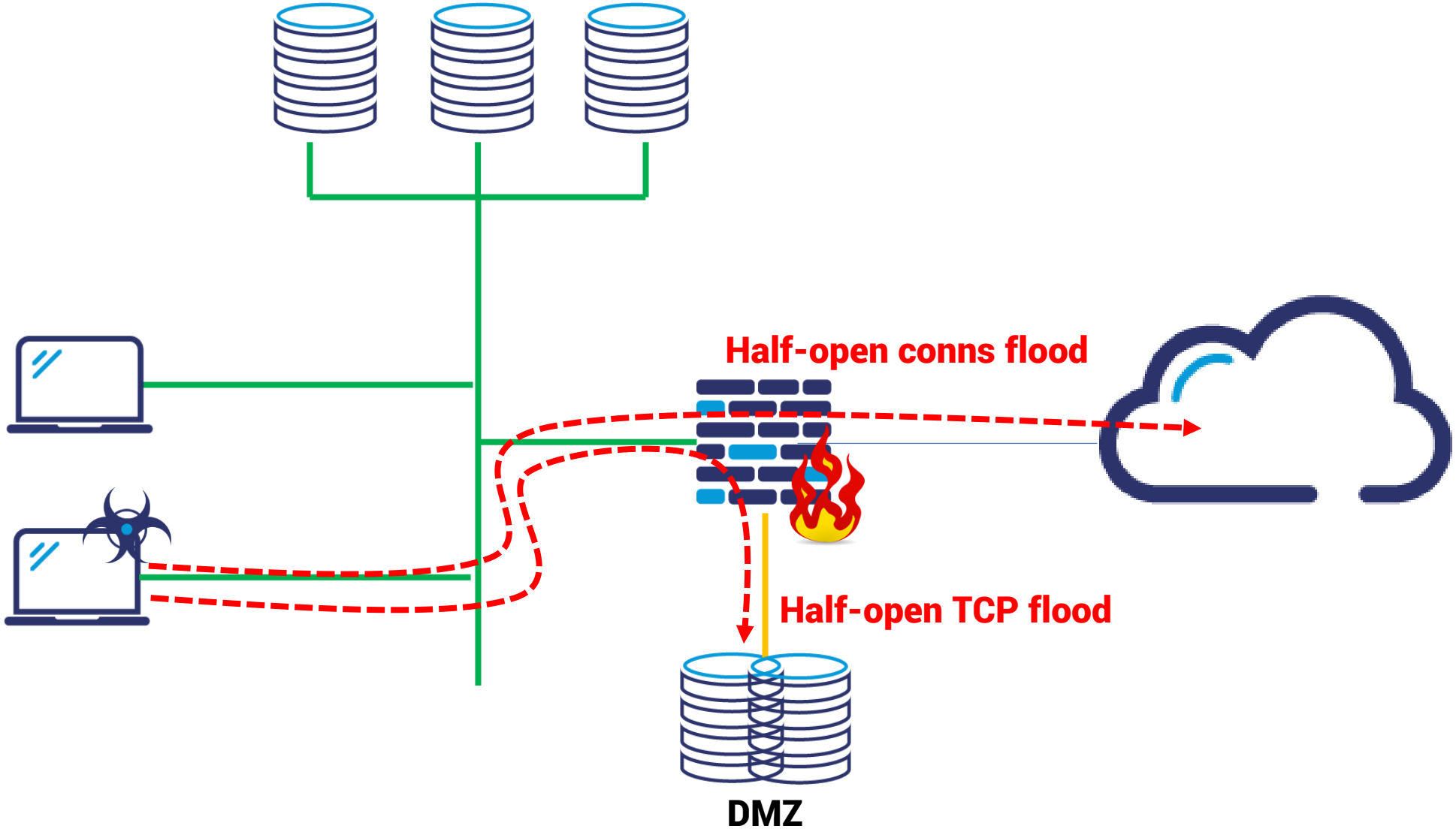
Wewnętrzny DDoS wycelowany w system

DDoS na poziomie sieci – smurf attack



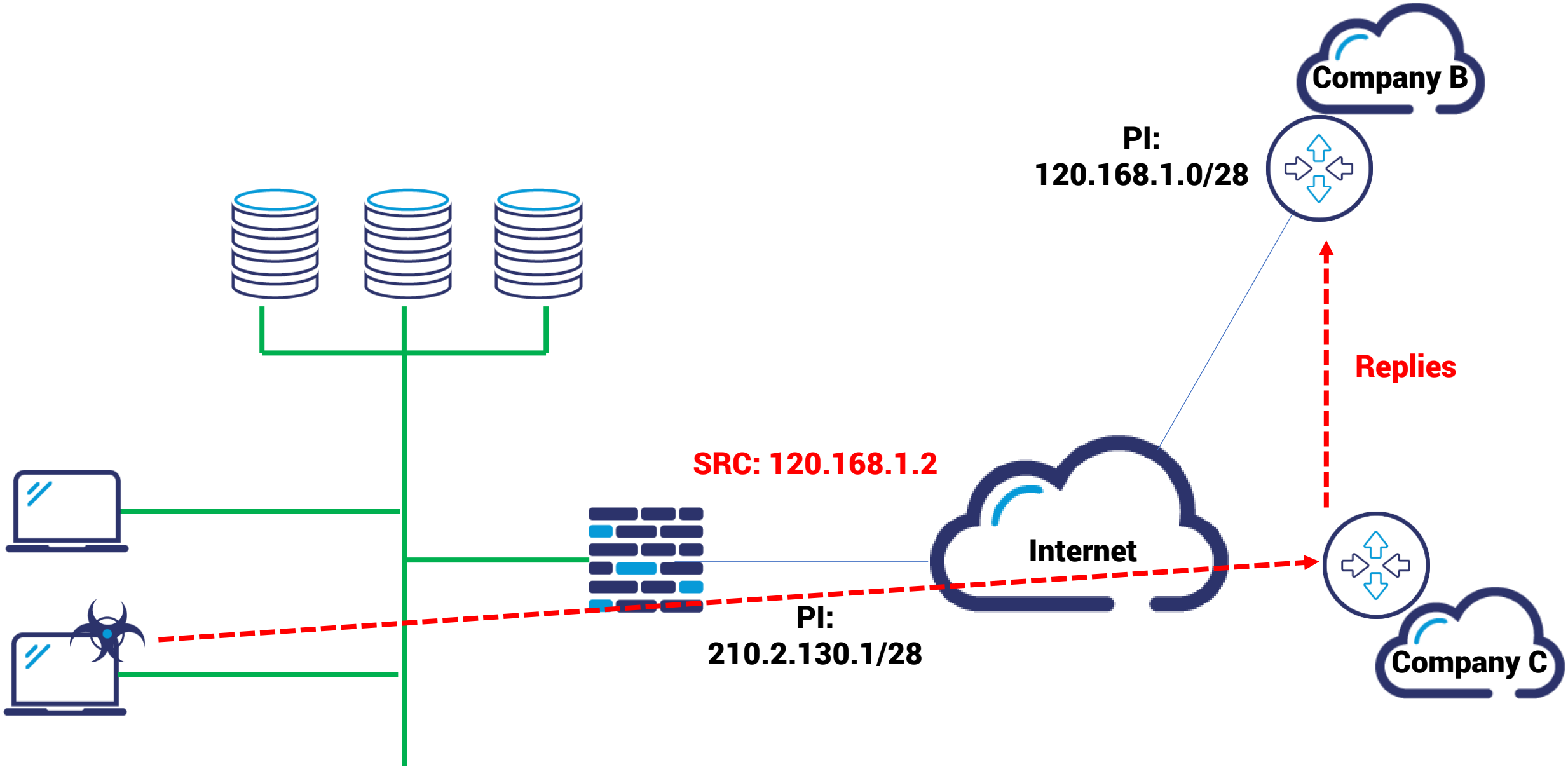
Distributed DoS na e-commerce

E-commerce DDoS od środka

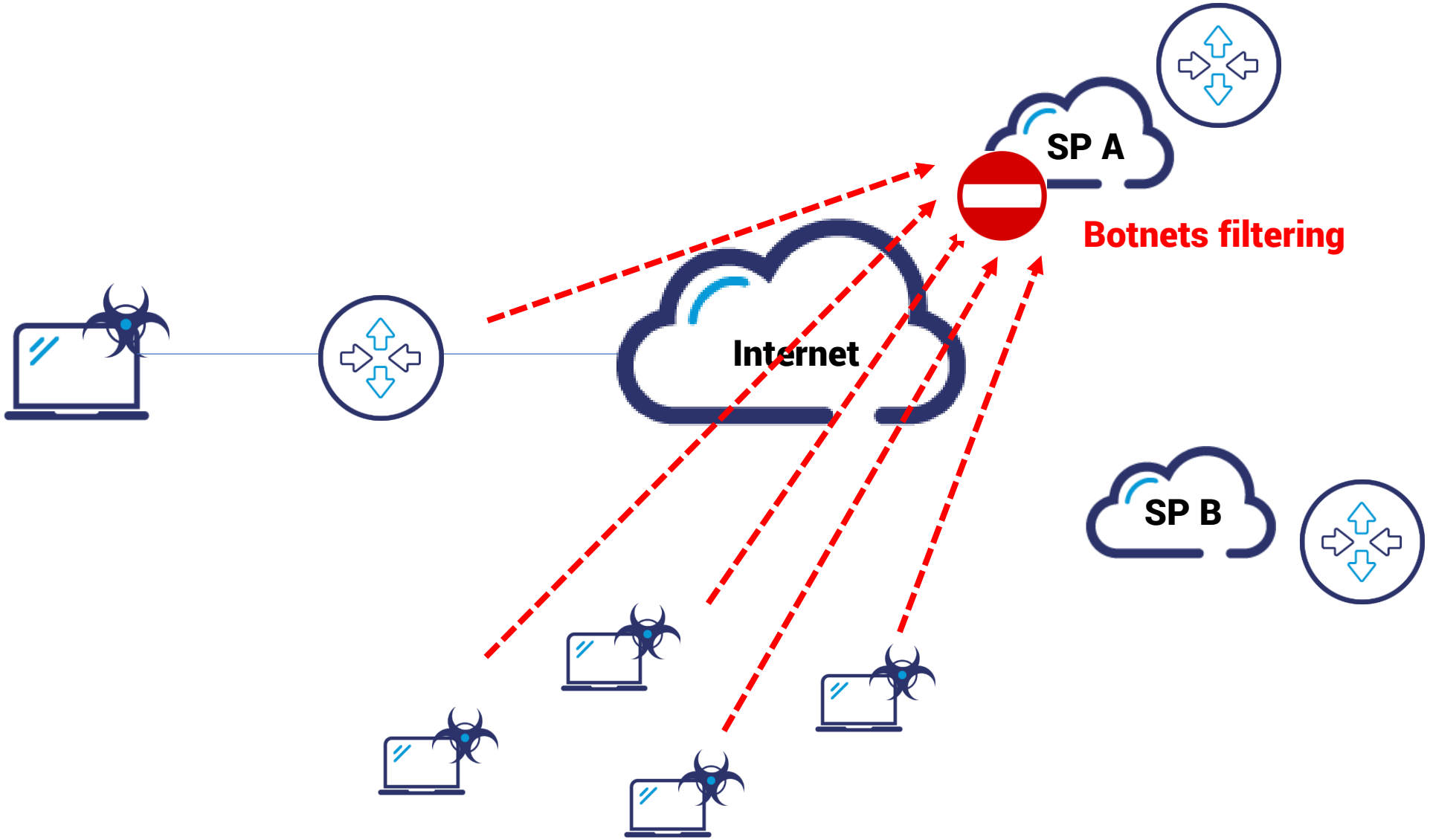


Blacklisting, czyli problem z reputacją

Source spoofing - blacklisting

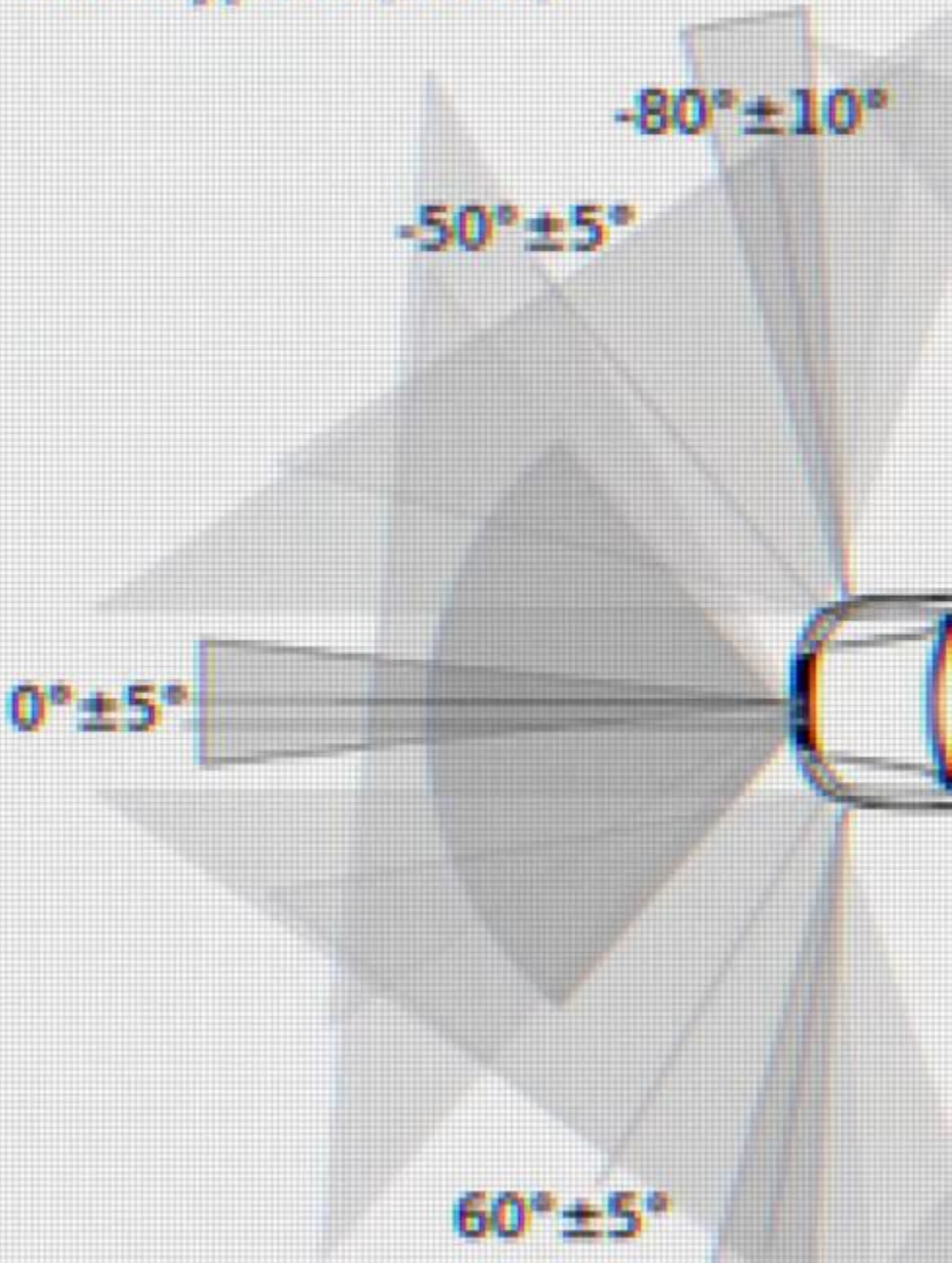


Botnets & RTBF



A nasz bohater szyfruje dane kompletnie destabilizując prace firmy

Ibeo LUX (110°)
SMS Typ 31 (100°)



Czy jest jakaś odpowiedź na te ataki?

ARP Spoofing vs Dynamic ARP inspection

Scanning vs VLAN segmentation

Network infra DoS vs CoPP/CoPPr

TCP flood vs firewall inspection

Botnets vs firewall + RTBH

Source spoofing vs uRPF + iACL

Network level DDoS (Smurf) vs IPSG

Malware vs Anti-malware + NGIPS

Jak planować karierę?

1 milion miejsc pracy w cybersecurity w 2016

https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#2767db1b27ea

„ ...Every year in the U.S., 40,000 jobs for information security analysts go unfilled…”
- Forbes

Specjalizacje

Network Security Engineering
5 – 9k PLN netto

Application Security Tester
6 – 12k PLN netto

Chief Security Officer
14 – 20k PLN netto

Systems Security Architect
9 – 14k PLN netto

Network Security Tester
6 – 11k PLN netto

Cybersecurity Analyst
9 – 16k PLN netto

Więcej techniki i szkoleń na

www.grandmetric.com