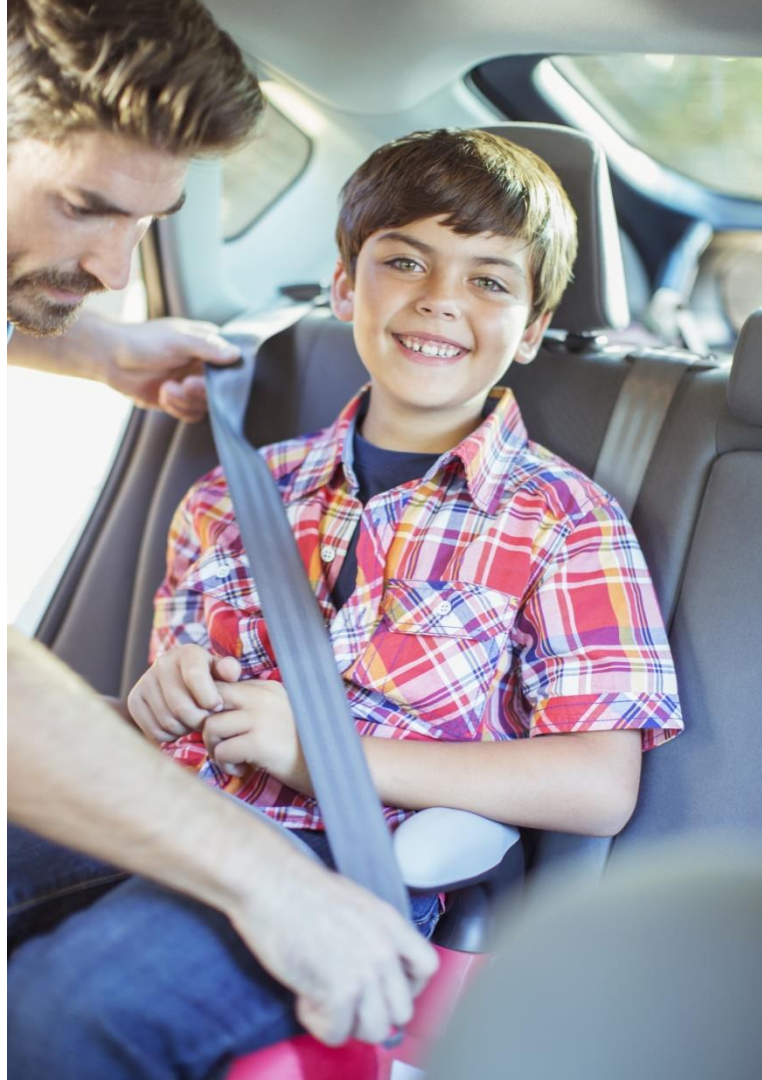


Raport CERT Orange Polska za rok 2017



sieć
#1



Interaktywna mapa zagrożeń w Polsce

Mapa zagrożeń w czasie rzeczywistym – jak ją czytać?

- Ataki, których celem jest Polska
- Typy ataków
- Kraje źródłowe ataków
- Najczęstsze zagrożenia

Mapa

Większość ataków unieszkodliwiamy zanim dotrą do naszych klientów

2 filary bezpieczeństwa



- **Doskonalenie narzędzi ochrony**

Większość ataków unieszkodliwiamy zanim dotrą do naszych klientów

Nowość! CyberTarcza:
atomatyczna blokada phishingu

- **Świadomy użytkownik – połowa sukcesu**

@CERT_OPL

Mapa zagrożeń

Raport CERT Orange Polska

TOP 3 trendy 2017



Wzrost ataków na urządzenia mobilne –

już 25%
wszystkich

Socjotechnika
coraz doskonalsza –

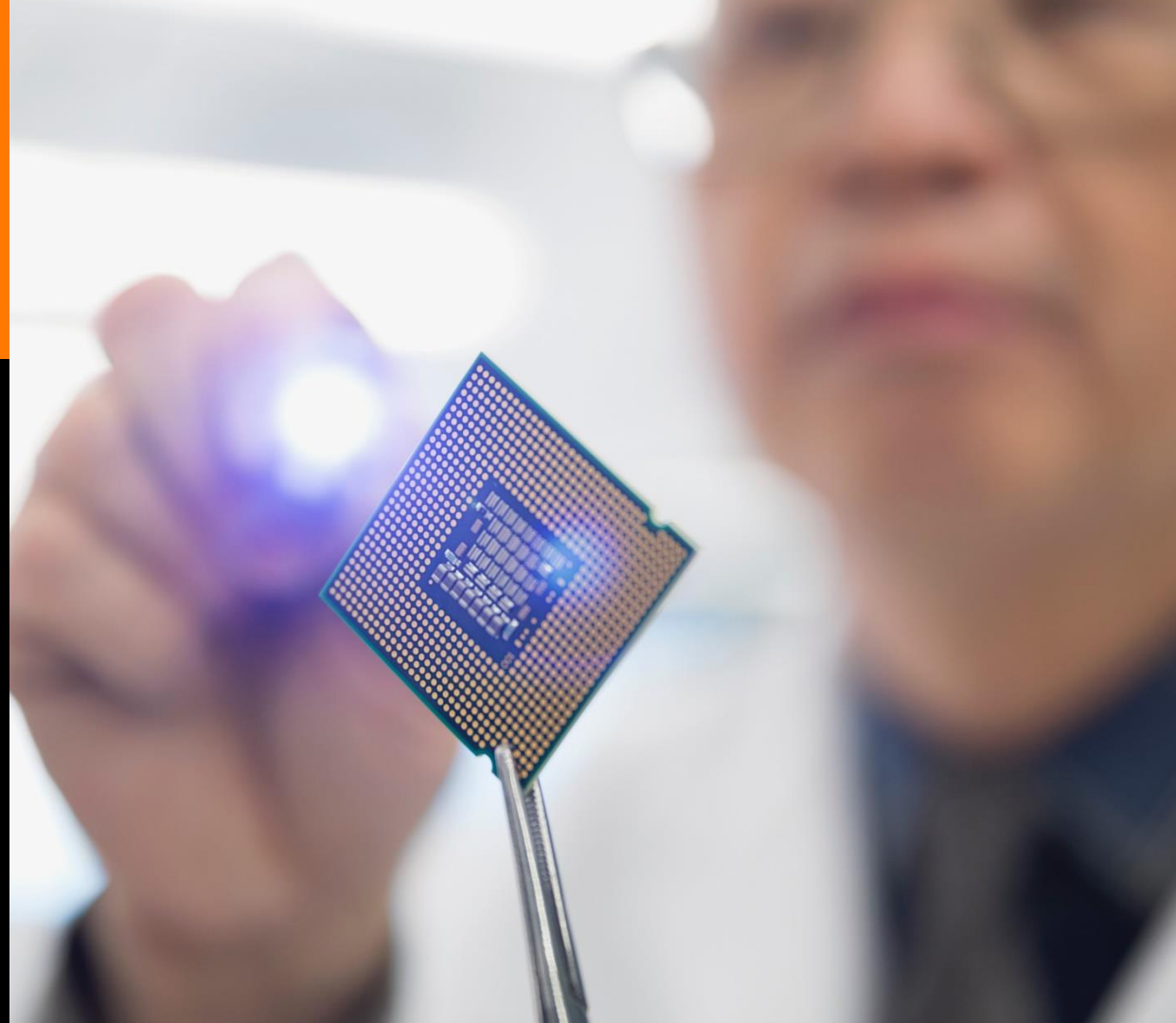
phishing

Ataki DDoS
wciąż groźne:

177 Gbps

W przyszłości...

**Sztuczna
inteligencja:
narzędzie
ochrony,
ale także
zagrożenie?**



Cyber ataki 2017



WannaCry

- Atak wykorzystujący exploit EternalBlue, kojarzony z amerykańską NSA
- Zainfekowane komputery w niemal 150 krajach, głównie w Rosji
- Czy to ransomware ? okup zaledwie 200 tys. dolarów

NotPetya

- Teoretycznie ransomware, najprawdopodobniej wiper
- Cel ataku: Ukraina, rozprzestrzenił się względu na globalne firmy z siedzibą na Ukrainie

Główne powody ataków:

zacieranie śladów po innych działaniach cyberprzestępców



Co się działo w naszej sieci?



48,9%

Obrażliwe
I nielegalne treści

19,5%

Dostępność
zasobów

14,7%

Próby włamań



4,6%

5,5%

Złośliwe
oprogramowanie

6,9%

Gromadzenie informacji

2,9%
Oszustwa sieciowe

0,4%
Poufność
i integralność decyzji

0,4%
Włamania sieciowe

0,9%
Inne

Statystyki 2017 – internet stacjonarny i mobilny

TOP 3 złośliwego
oprogramowania
– sieć stacjonarna

- Trojan
- Backdoor
- Ransomware



TOP 3 złośliwego
oprogramowania
– sieć mobilna

- Adware
- Trojan
- Malwaretising



Średnia miesięczna
liczba użytkowników
dotkniętych złośliwym
oprogramowaniem:

ponad **80 tys.**
użytkowników
sieci stacjonarnej

ponad **10 tys.**
użytkowników
sieci mobilnej (IPv6)

Statystyki 2017

– CyberTarcza

TOP 3 ochronionych przez CyberTarczę klientów z podziałem na kategorię zagrożeń:

Ransomware – ponad

119 tys.

Trojan – ponad

72 tys.

Exploitkit – ponad

61 tys.

CyberTarcza
ochroniła
w 2017 roku
ponad

324 tys.
klientów









- backdoor
- banker
- exploitkit
- mobile
- ransomware
- spyware
- trojan
- worm

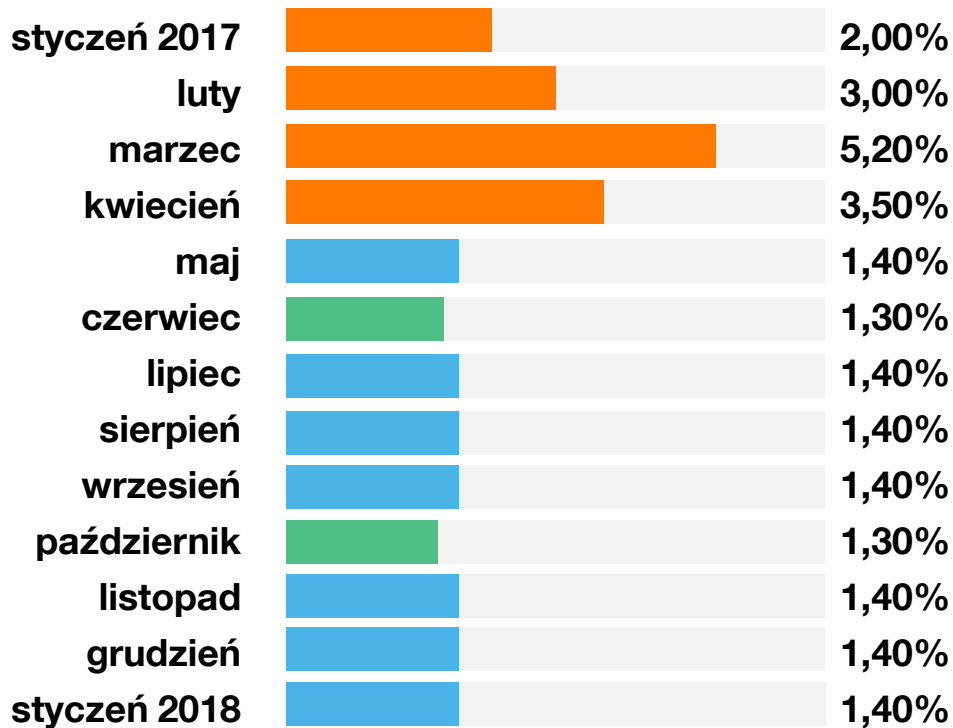
Sieć Orange Polska – jesteśmy coraz bardziej skuteczni

Dzięki rozwojowi CyberTarczy skuteczniej chronimy klientów:
coraz więcej zagrożeń
CyberTarcza blokuje automatycznie

Miesięcznie:

	Zdarzenia	Anomalie	Incydenty
2017	 ^{ponad} 10 mld 	147 tys.	 1000 
2016	 ^{blisko} 9 mld	170 tys.	 1400
2015	^{blisko} 6 mld	150 tys.	1700

Case studies



1.

**Atak na urządzenia
naszych klientów
botnet Mirai,
blokada portu 7547**



2. Największy atak wolumetryczny (DDoS) 2017

- Skierowany na pojedynczy adres IP klienta Neostrody
- Średni wolumen ataku: ponad 100 Gbps przez ponad 20 minut
- Maksymalna wartość: niemal 180 Gbps
- Atak automatycznie wykryty i zneutralizowany przez systemy monitorujące Orange Polska



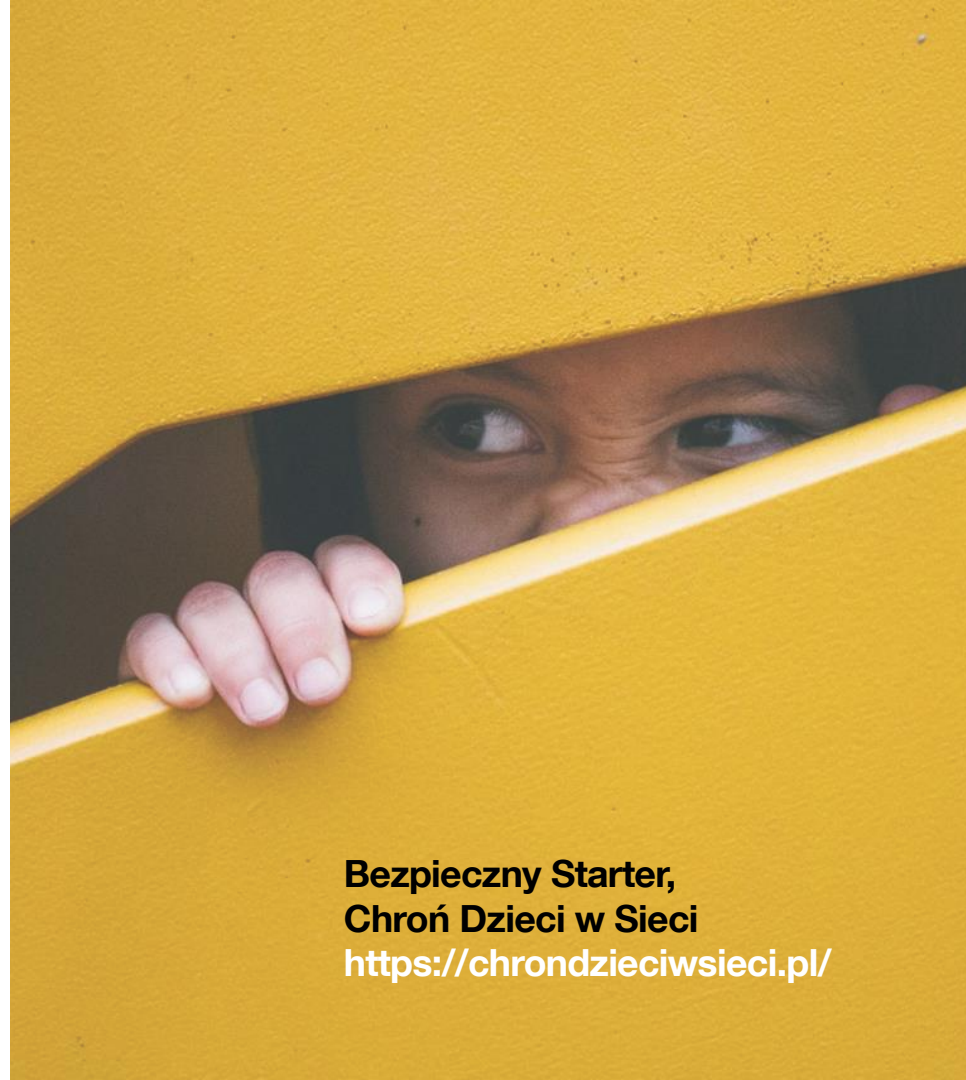
Cyberprzestępcy zmieniają metody działania

- Mniej spektakularnych i długich ataków DDoS - krótsze są bardziej opłacalne
- Kwitnie czarny cyber rynek – podaż botnetów przekracza popyt na ich usługi (!)
- Phishing – maile „od kurierów”, „faktury za usługi”, nawet „dokumenty rozwodowe”
- Wiadomość e-mail – najłatwiejsza droga do oszustwa
- Socjotechnika w mediach społecznościowych
- Profilowanie ataków na konkretne grupy użytkowników (np. grupy zawodowe)



Digital natives: co robią dzieci w sieci

- **Niemal 16 milionów** zablokowanych odwołań do stron pornograficznych
- **Ponad 100 milionów** zablokowanych przekierowań na strony związane ze złośliwym oprogramowaniem, spamem i phishingiem
- **1374 dzieci** nie zdołało wejść na strony o treściach pedofilskich



Bezpieczny Starter,
Chroń Dzieci w Sieci
<https://chrondzieciwsieci.pl/>

Nowe rozwiązania dla większego bezpieczeństwa

- Automatyczne blokowanie stron phishingowych przez CyberTarczę
- Mapa zagrożeń – budowanie świadomości
- Statystyki zagrożeń mobilnych w czasie rzeczywistym na cert.orange.pl
- Orange Polska członkiem MANRS
- Testujemy mobilną Cybertarczę



Edukacja



Fundacja



Raport CERT
Orange Polska



twitter
CERT OPL

www.cert.orange.pl

Dzieci

– zadbaj o trudne hasło, nikomu go nie pokazuj, nie pisz o sobie prywatnych rzeczy w sieci.

Młodzież

– korzystaj świadomie z mediów społecznościowych. Pamiętaj, to co wrzucone do sieci tam pozostaje. W sieci nie jesteś anonimowy.

Dorośli

– pomyśl, zanim klikniesz. Analizuj podejrzane maile.

Seniorzy

– nie bój się internetu. Nie wierz we wszystko, co piszą.

Co nas czeka w roku **2018** – **nowe zagrożenia**



Wykorzystywanie
zasobów
użytkowników do
kopania
kryptowaluty

Wykorzystanie
podatności
sprzętowo-
programowych
w infrastrukturze
środków
wirtualnych

Phishing i
ransomware –
ulepszanie metod
i socjotechniki

Internet Rzeczy,
wirtualizacja
sieci

Sztuczna
Inteligencja,
Machine Learning

A woman with long dark hair is shown in profile, looking through a large, black telescope. The telescope has the word "SIGHT" embossed on its side. The background is a bright, hazy sunset or sunrise over a landscape. The overall mood is one of looking forward and seeking new horizons.

**Co nas czeka
w roku 2018
– nowe możliwości
ochrony**

**Nacisk na
budowanie
świadomości
użytkowników**

**Sztuczna
Inteligencja,
Machine
Learning –
nowe narzędzie
ochrony**

**Nowe
funkcjonalności
CyberTarczy**

Raport CERT Orange Polska za rok 2017

Bezpieczeństwo

Raport
CERT Orange Polska
za rok 2017

Uśmiechnij się.
Razem będzie
bezpieczniej.

sieć
#1

