Jak ograniczyć zagrożenie związane ze zjawiskiem “credential abuse”?

Bartlomiej Jakubowski – Solutions Engineer II, CISSP, CCSP

Agenda

- O firmie Akamai
- Co to jest „credential abuse”?
- Techniki i sposoby zapobiegania, historie z pierwszej linii frontu
- Podsumowanie

Akamai makes the Internet

Fast, Reliable and Secure.

Jesteśmy wiodącym dostawcą usług Content Delivery Network (CDN). Dostarczamy, optymalizujemy i zabezpieczamy treści dostępne online i aplikacje biznesowe

DANE STATYSTYCZNE:

$2.2B	6,000+	6,000+
Dochódu	Pracowników	Klientów

NASZA HISTORIA:

Rok założenia 1998, firma zakorzeniona w MIT — Rozwiązujemy problem przeciążenia Internetu za pomocą matematyki, nie Hardware'u.


Ufa nam:
7 z 10 największych banków na świecie
27 z 30 największych banków w Stanach Zjednoczonych
Ponad 150 banków na całym świecie

Inteligentna Platforma Akamai (HTTP+HTTPS+DNS)

230,000+ Serwerów

1600+ Sieciach

130+ Państw na 7 Kontynentach

Do 30% całego ruchu webowego

46 Tbps ruchu

Centra „Scrubbingowe” (wszystkie protokoły)

7 Centr

4 Kontynenty

3.6 Tbps dedykowanej pojemności na ataki DDoS

Talent

5 SoC’ów – 180 Inżynierów

350 Inżynierów Bezpieczeństwa

Zespól R&D

Zespól CERT

Analiza Danych

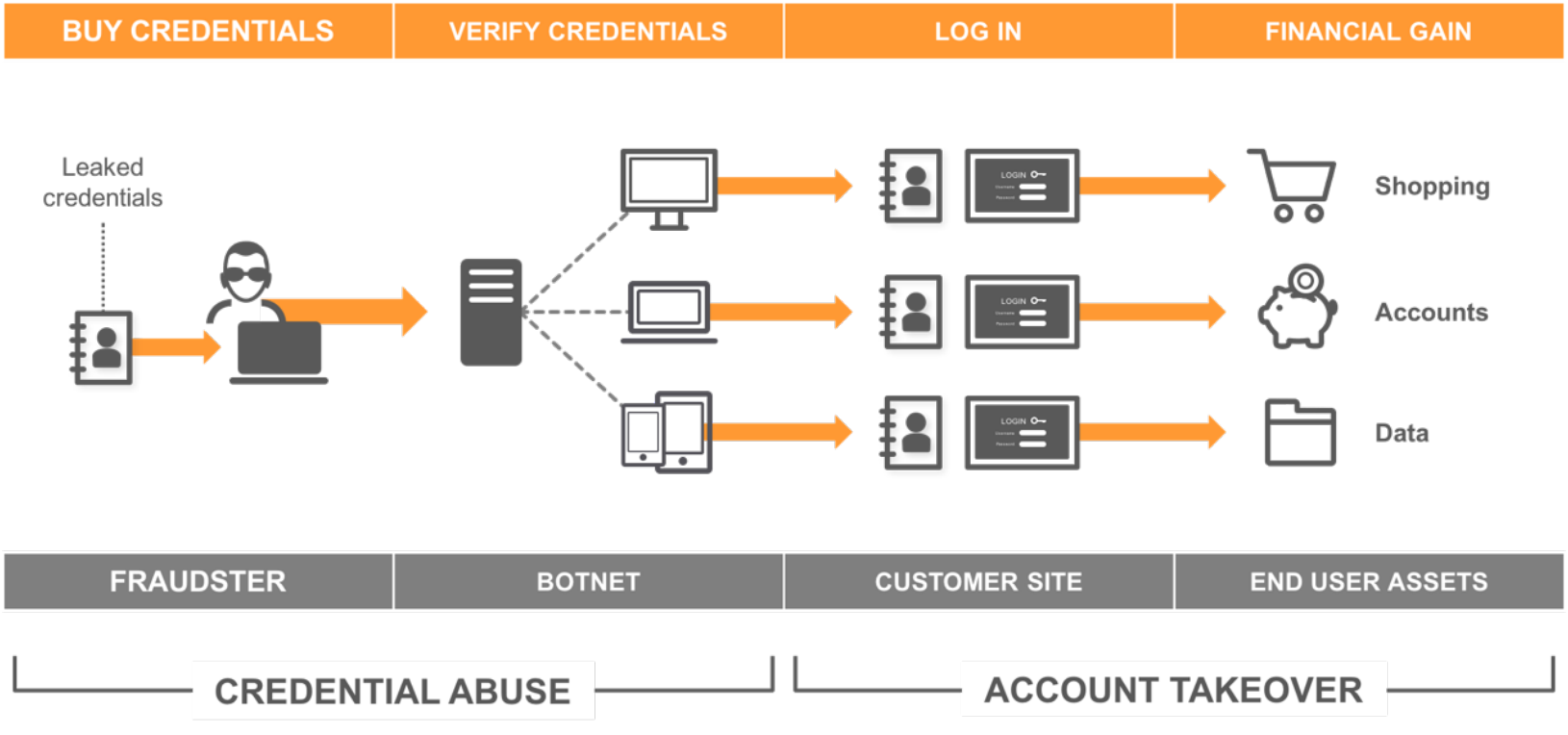
2 biliony hitów dziennie

Dziesiątki milionów unikatowych adresów IP dziennie

600 000 logów na sekundę

2 PB danych z ostatnich 45 dni

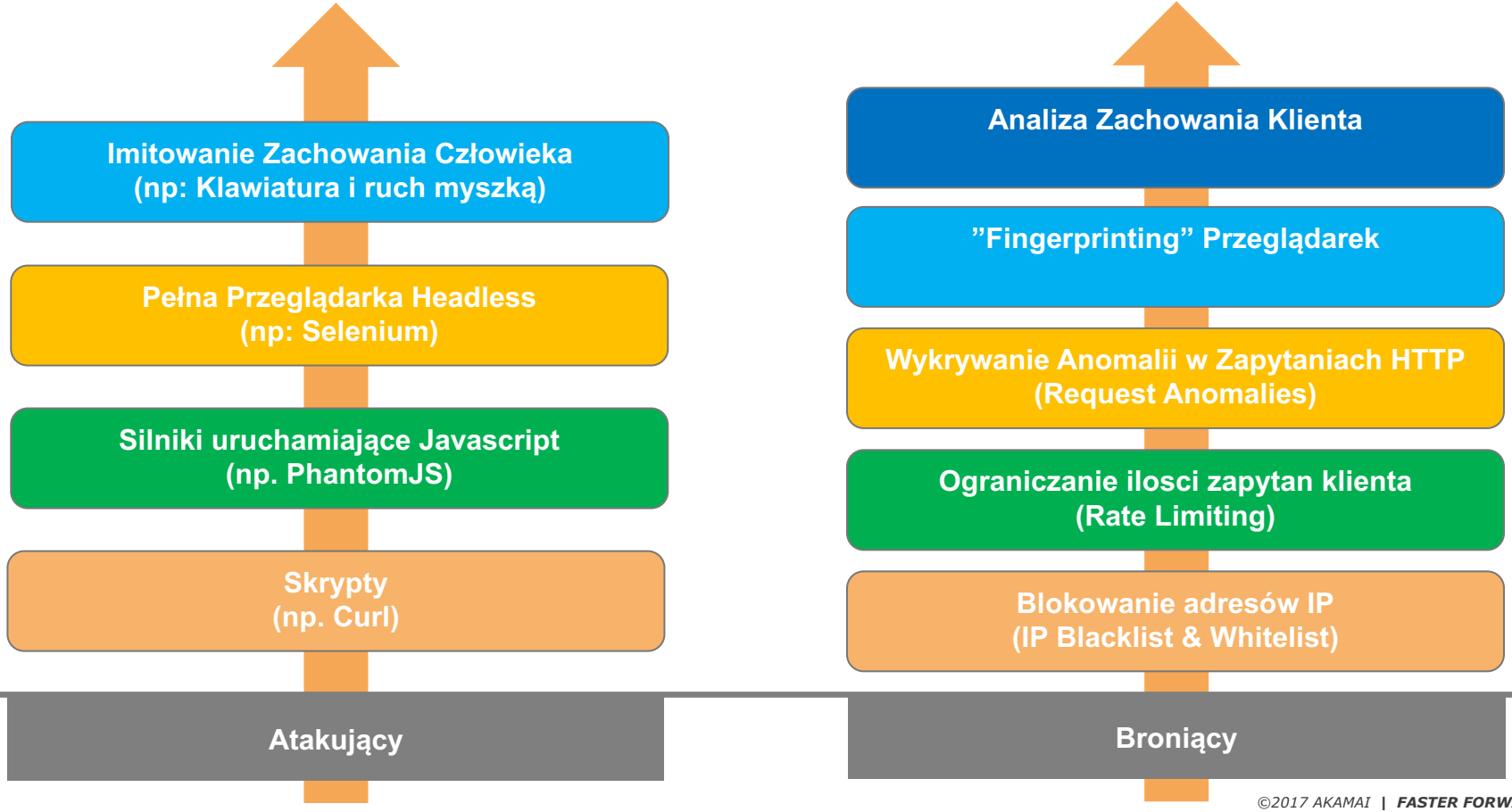
Co to jest ”credential abuse”



Według Naszego Zespołu Threat Research

30% wszystkich transakcji logowania to "credential abuse”

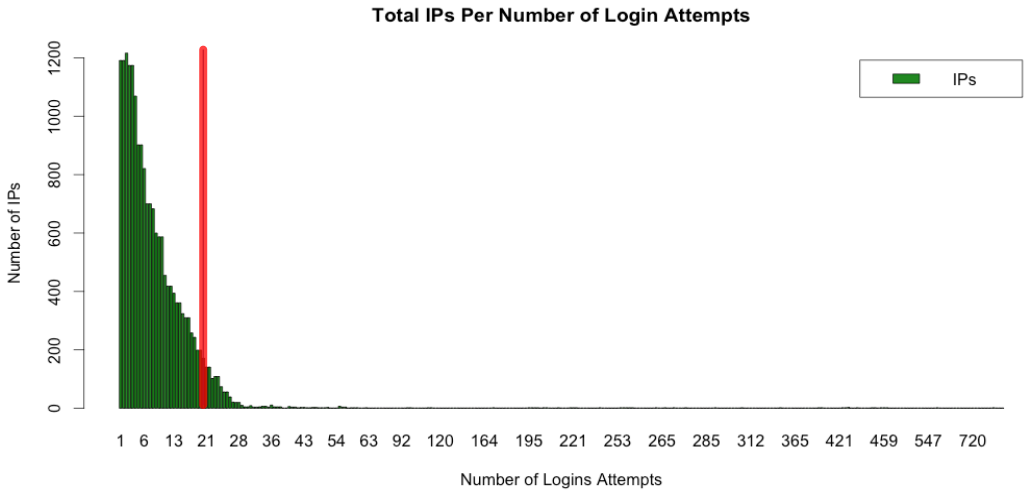
Zaawansowanie i determinacja: Atakujący kontra Broniący



Statystyka

Analiza „Big Data” Cloud Security Intelligence:

- 167 kampanii ”credential abuse” (na przestrzeni miesiąca)
- 400000 adresów IP (średnia na dzień)
- ~25% wszystkich adresów IP było “jednorazowych”
- ~70% wszystkich adresów IP uczestniczyło w kampanii 1 dzień
- Login API jest 3.7x częściej atakowany niż login webowy

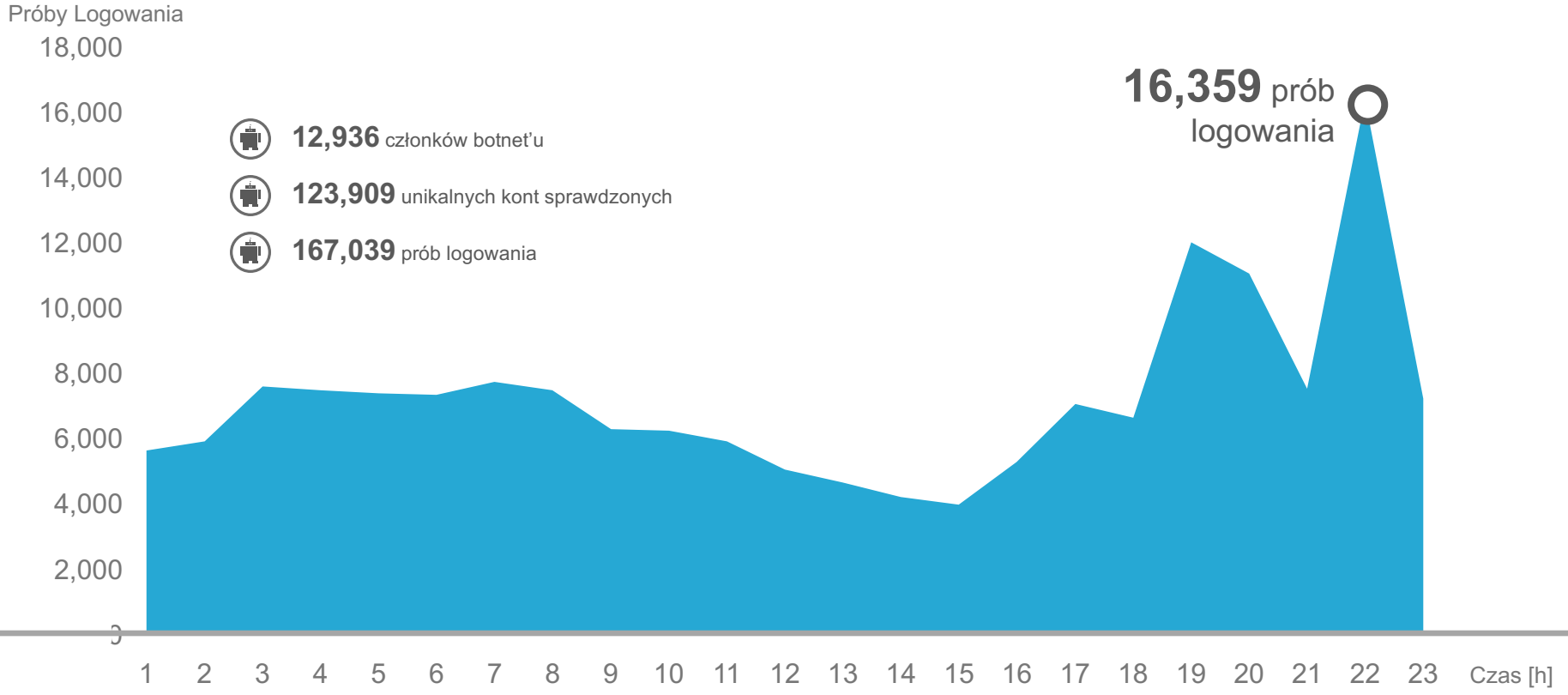


Dlaczego walka z “Credential Abuse” jest trudna?

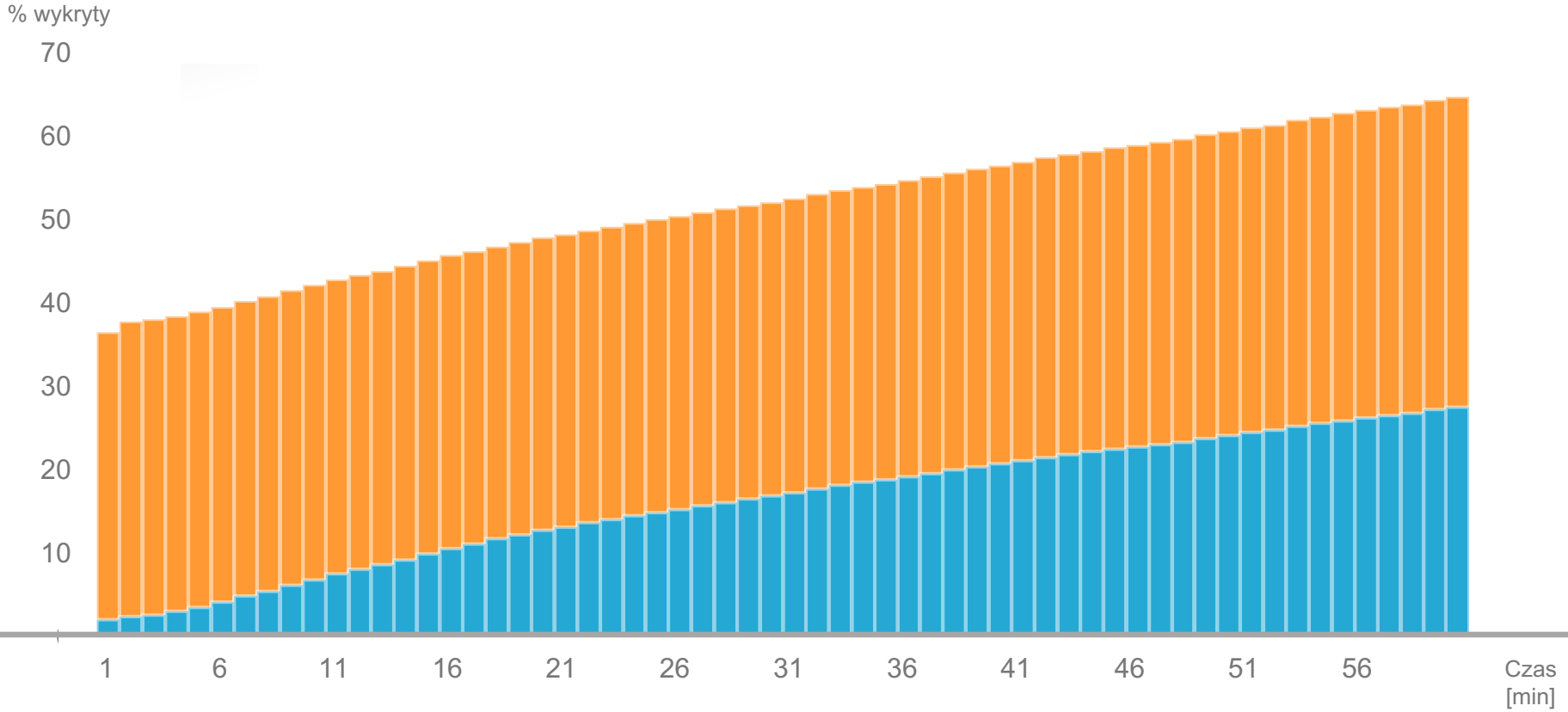
Atakujący obchodzą obecne zabezpieczenia:

- Powolny Atak– 25% botów jest wykorzystywanych tylko raz
- Zmasowany Atak – Miliony zapytań
- Działa na warstwie aplikacyjnej, nie do rozpoznania na niższych warstwach
- Informacje przesyłane są tajne – Nazwy użytkowników i hasła
- Informacje przysłane są zaszyfrowane
- Login API jest 3.7x częściej atakowany niż login webowy

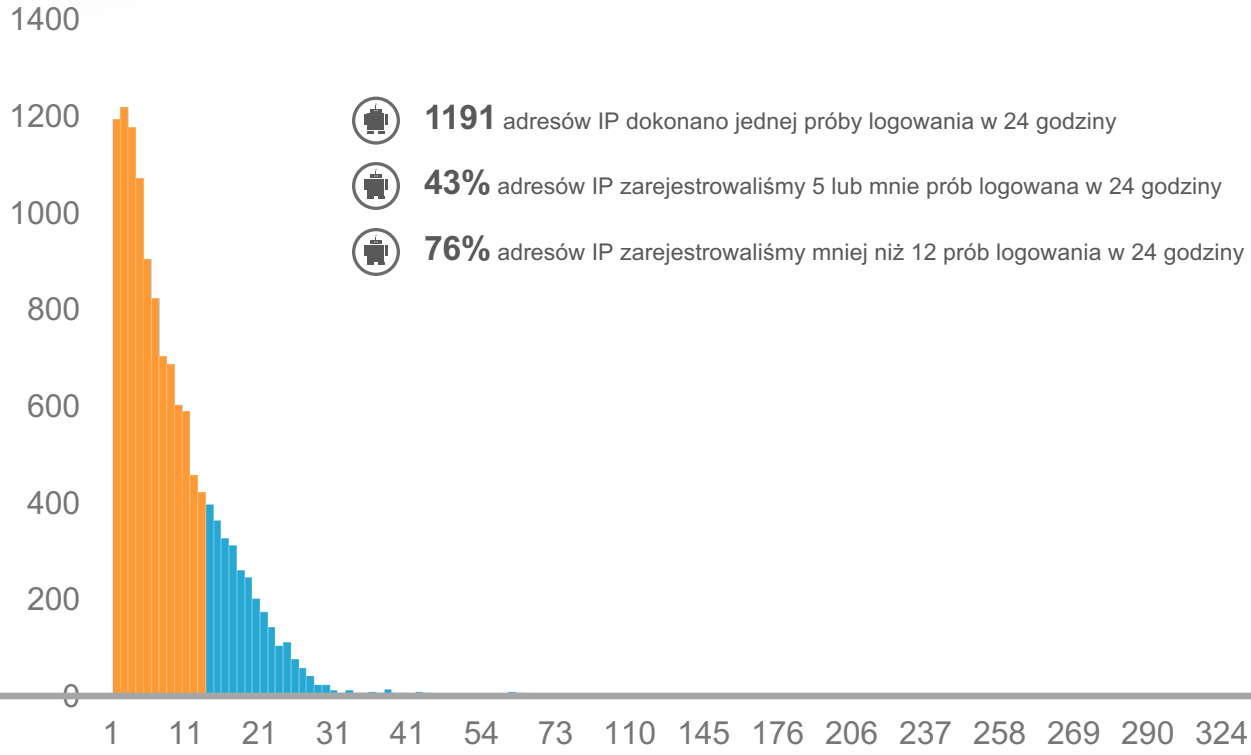
Perspektywa jednej aplikacji - kampania ”credential abuse”



Perspektywa jednej aplikacji - jaką cześć wykryjemy



Perspektywa jednej aplikacji - Ilość prób logowania wciągu 24h

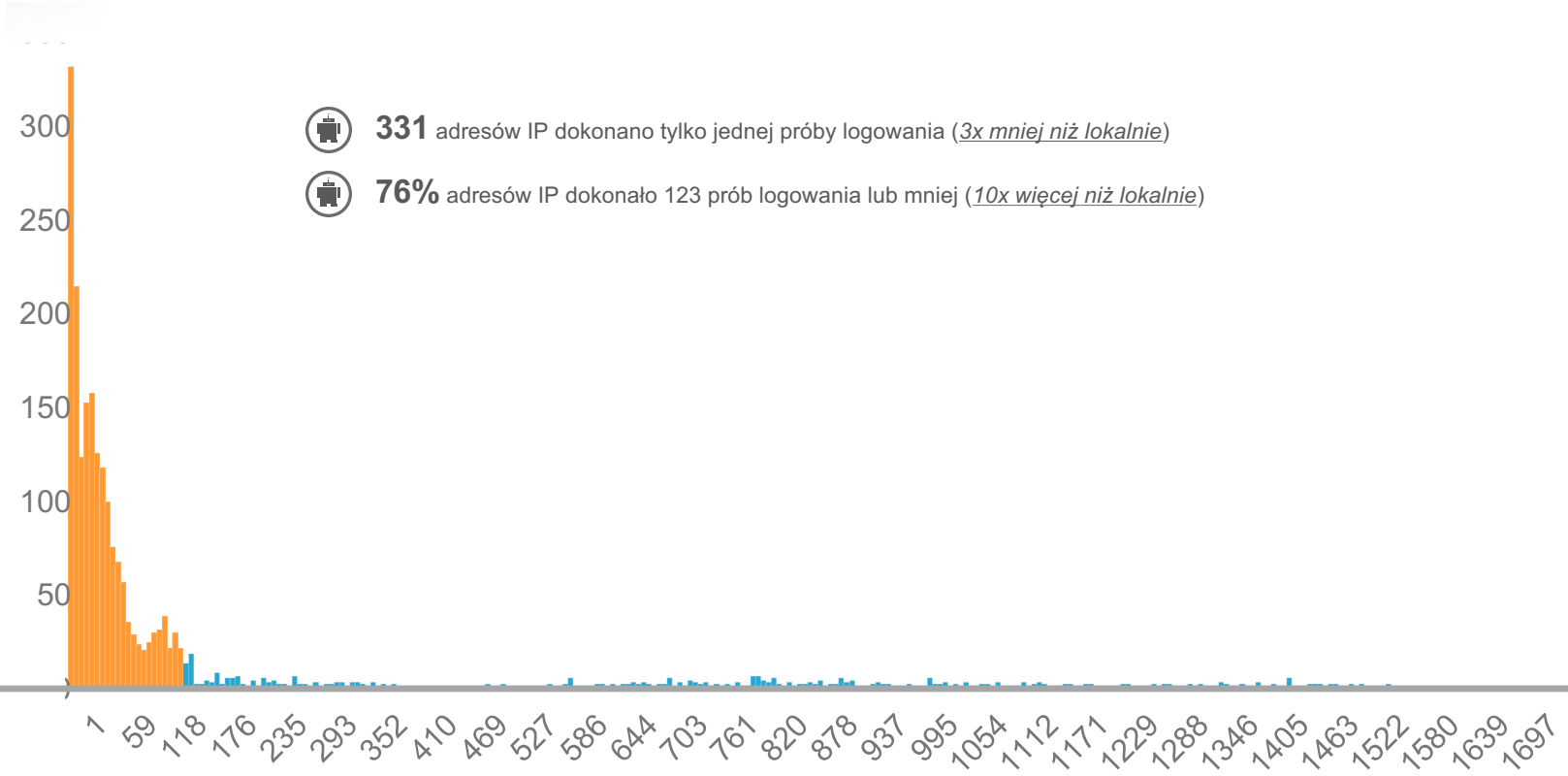


1191 adresów IP dokonano jednej próby logowania w 24 godziny

43% adresów IP zarejestrowaliśmy 5 lub mnie prób logowana w 24 godziny

76% adresów IP zarejestrowaliśmy mniej niż 12 prób logowania w 24 godziny

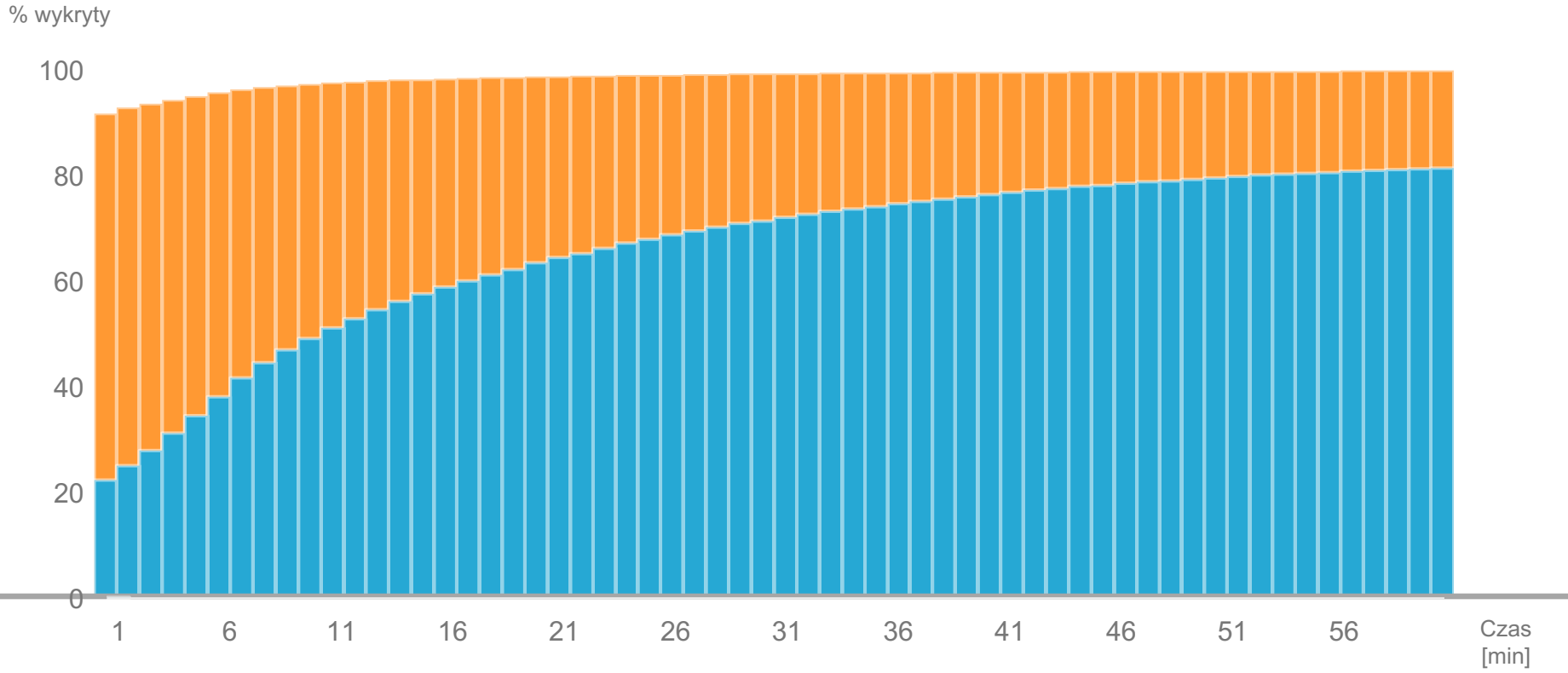
Perspektywa globalna – Ilość prób logowania wciągu 24h



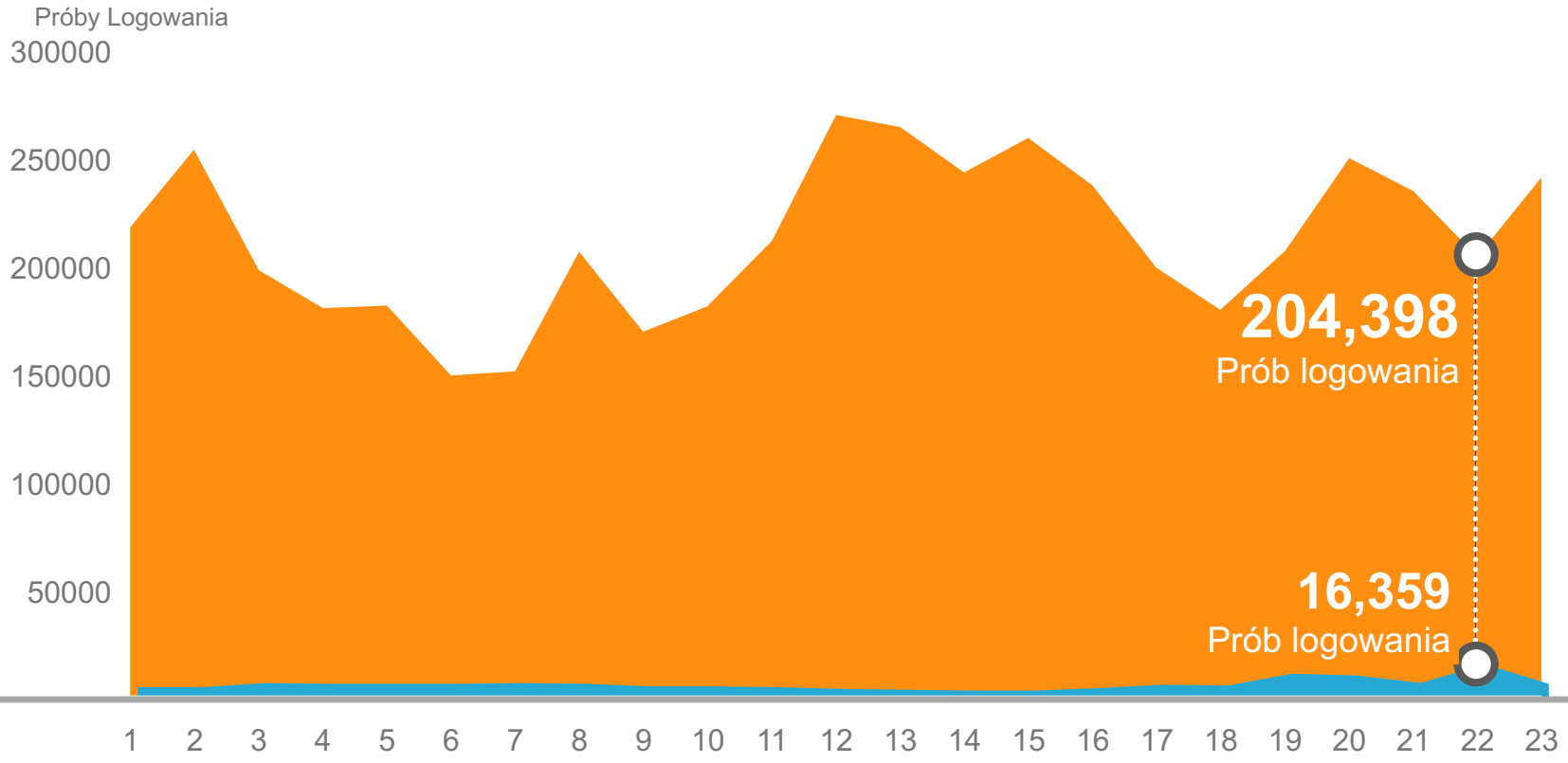
331 adresów IP dokonano tylko jednej próby logowania (*3x mniej niż lokalnie*)

76% adresów IP dokonało 123 prób logowania lub mniej (*10x więcej niż lokalnie*)

Perspektywa globalna - jaką cześć wykryjemy



Perspektywa Globalna – kampania “credential abuse”



Podsumowanie

- Jak wielkim problemem jest “credential abuse” dla instytucji/firmy?
- Ile instytucja/firma chce/może zainwestować w przeciwdziałanie zjawisku?
- Strategie broniących I atakujących będą ewoluować z biegiem czasu.

Pytania?

Więcej Informacji:
http://www.StateOfTheInternet.com
https://blogs.akamai.com/

Bartlomiej Jakubowski – Solutions Engineer II
bjakubow@akamai.com

Dziękujemy!

Zapraszamy do naszego stoiska


Akamai
FASTER FORWARD