HP Sure Click Enterprise

POWERED BY Bromium

Chroń się przed nieznanymi zagrożeniami.

Ponad 5 miliardów otwartych załączników do wiadomości e-mail, stron internetowych i pobranych plików - brak zgłoszonych naruszeń.[1]

Zagrożenia wyeliminowane przez HP Sure Click w IV kwartale 2020 r.[2]

1.4%
wzrost izolowanych zagrożeń

32,005 zagrożeń zostało odizolowanych przez HP Sure Click po ominięciu innych zabezpieczeń.

8.8 dni

Średni czas potrzebny innym producentom do wykrycia dotychczas nieznanego złośliwego oprogramowania przechwyconego na maszynach wirtualnych.

29,1% nowych lub nieznanych zagrożeń

Zagrożenia, które były nowe lub nieznane w czasie, gdy zostały wyizolowane.

848 typów złośliwego oprogramowania

Trojany	66.4%
Exploity	12.7%
Downloadery	5.3%
Wykradające info z PC	3.6%
Narzędzia hakerskie	2.2%
Inne	9.8%

HP Sure Click wykrył 848 typów złośliwego oprogramowania, wśród których najczęstsze były "konie trojańskie".

73% pozytywnych wyników

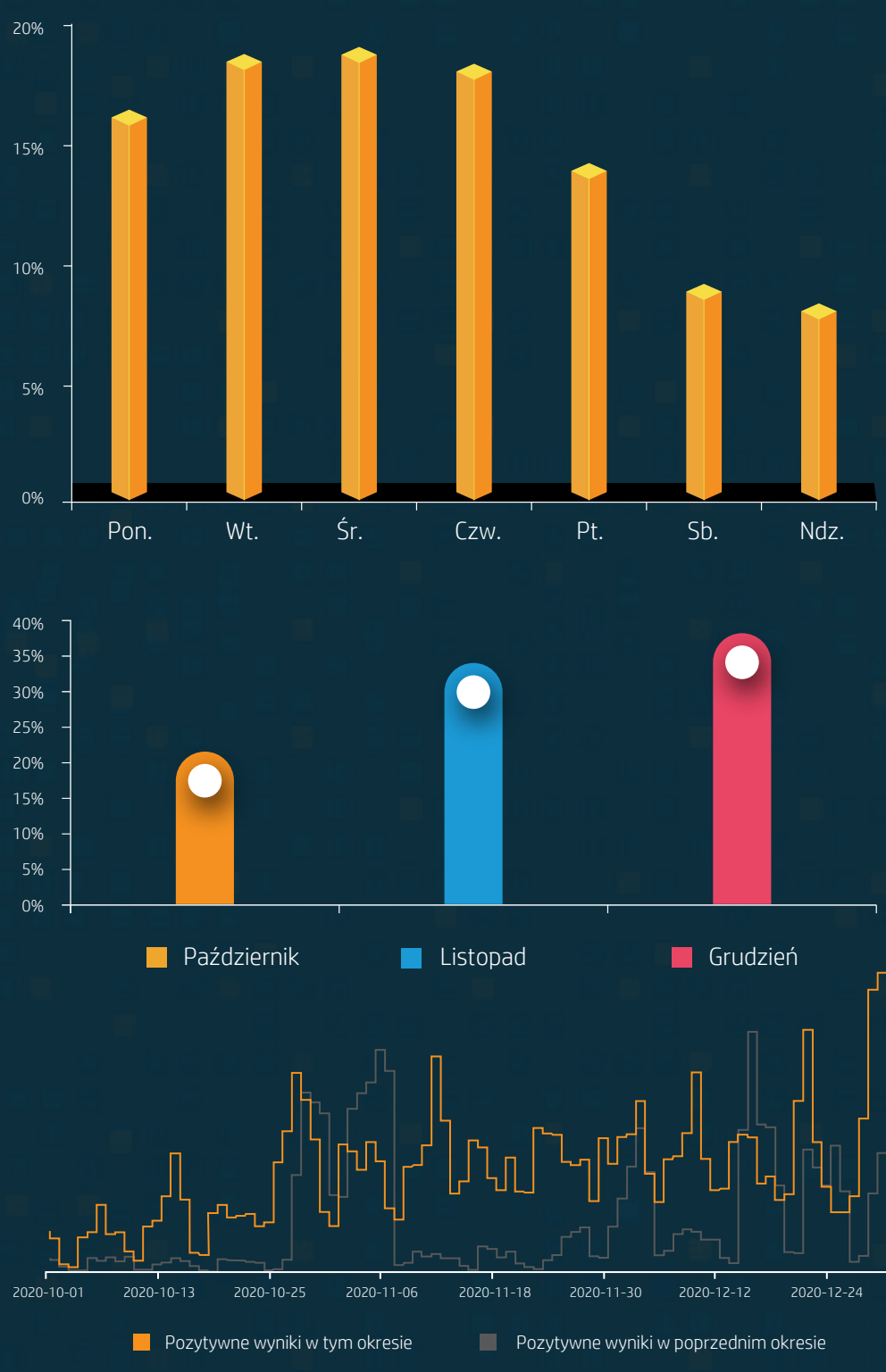
23,364 z 32,005 alertów zostało potwierdzonych jako złośliwe oprogramowanie po dalszej analizie. Pozostałe dotyczyły podejrzanych zachowań.

88% naruszeń bezpieczeństwa za pośrednictwem poczty elektronicznej

Email	88%	Sieć	12%

Do infekcji szkodliwym oprogramowaniem dochodziło najczęściej poprzez załączniki w poczcie e-mail.

Podział według czasu



Według dnia

Do większości ataków dochodziło w środy.

Według miesiąca

Największą liczbę ataków odnotowano w grudniu.

Październik 2020	:	27.5%
Listopad 2020	:	35.1%
Grudzień 2020	:	37.4%

Wykres przedstawia liczbę zagrożeń dla każdego dnia w IV kwartale 2020 r., w porównaniu z poprzednim okresem.

Według zastosowania

Wykres przedstawia najważniejsze aplikacje i typy plików wykorzystywane przez zagrożenia, które zostały wyizolowane przez HP Sure Click.

Przeczytaj pełny raport

Więcej o Sure Click Enterprise

Przypisy:
1. Założenia oparte na wewnętrznej analizie HP dotyczącej spostrzeżeń zgłaszanych przez klientów i zainstalowanej bazy.
2. Dane te obejmują klientów HP Sure Click, którzy wyrazili zgodę na udostępnianie swoich danych o zagrożeniach firmie HP.
3. Zagrożenia niezidentyfikowane przez wykrywanie oparte na sygnaturach hash w czasie izolacji.