Uważaj na linki wyłudzające dane i pieniądze – ciągle rośnie liczba oszustw w internecie

Kategoria: Styl życia
Opublikowano: piątek, 10, maj 2024 09:23
Alicja Cisowska
Odsłony: 1492

Liderem na liście cyberzagrożeń wciąż pozostaje phishing, oparty na coraz bardziej wyrafinowanej socjotechnice. W 2023 roku polscy internauci często klikali w linki zachęcające do szybkich i zyskownych inwestycji, ale też kierujące do fałszywych stron sklepów, kurierów czy promocji – wynika z nowego raportu CERT Orange Polska. Nadal bardzo popularne jest również tzw. oszustwo na kupującego, powiązane z portalami aukcyjnymi i zakupowymi, a ponad 40-proc. wzrost zanotowało oprogramowanie szpiegowskie: przede wszystkim Agent Tesla, który był jednym z dominujących zagrożeń w skrzynkach polskich internautów. – *Przewidujemy, że takie ataki będą się nasilały* – mówi Robert Grabowski, szef zespołu CERT Orange Polska.

CERT Orange Polska opublikował raport za 2023 rok. Wynika z niego, że krajobraz tych zagrożeń mocno się zmienił. W 2014 roku numer jeden w klasyfikacji zagrożeń z ok. 40-proc. udziałem stanowił spam, czyli niechciane wiadomości zapychające elektroniczną skrzynkę, a phishing stanowił raptem 1 proc. incydentów zarejestrowanych przez CERT Orange Polska.

W ostatnich latach coraz większą rolę w atakach odgrywa socjotechnika. Cyberprzestępcy dążą do zmanipulowania użytkownika w taki sposób, żeby sam pobrał i uruchomił niebezpieczny plik. Temu służy właśnie phishing czy tzw. malvertisment, czyli reklamy, w których umieszczane są linki prowadzące do złośliwych stron. Z najnowszego raportu CERT Orange Polska wynika, że w ubiegłym roku systemy bezpieczeństwa operatora zablokowały ponad 360 tys. fałszywych stron internetowych, co oznacza aż trzykrotny wzrost r/r. W linki prowadzące do takich stron, stworzonych przez oszustów, kliknęło ok. 5,5 mln Polaków. Dzięki blokadzie CyberTarczy uniknęli oni utraty danych czy oszczędności.

Do topowych zagrożeń, którymi wabieni są użytkownicy sieci, poza fałszywymi inwestycjami, należą także fałszywe linki do płatności i wciąż popularne tzw. oszustwo na kupującego (18 proc.), zwykle powiązane z portalami aukcyjnymi i zakupowymi, gdzie kupującym wysyłane są linki (zazwyczaj poprzez WhatsApp) do rzekomej strony z odbiorem pieniędzy za sprzedawany przedmiot. Ten sposób kradzieży to też zdecydowany lider, jeśli chodzi o liczbę tworzonych w tym celu fałszywych, zablokowanych stron. Eksperci wskazują, że użytkownicy często klikają także w fałszywe panele logowania do Facebooka, fałszywe sklepy czy linki w SMS/RCS związane z kuponami do znanych sklepów, poprawą adresu przesyłki czy zgubionym smartfonem.

Ataki DDoS stanowiły w ubiegłym roku 17,9 proc. incydentów.

Liczba ataków o wolumenie powyżej 10 Gbps wzrosła dwukrotnie (z 3,8 do 7,7 proc.), podobnie jak liczba ataków o najmniejszym wolumenie – poniżej 0,2 Gbps (z 24,3 do 40,8 proc.). Natomiast rekordowy atak z 2014 roku, który wynosił 93 Gbps, dzisiaj nie wzbudza większych emocji (ataki powyżej 100 Gbps to obecnie codzienność). Ubiegłoroczny rekord to 543 Gbps, czyli atak blisko sześciokrotnie mocniejszy niż ten sprzed dekady.

W kategorii złośliwego oprogramowania największy, aż 40-proc. przyrost dotyczył oprogramowania szpiegowskiego (spyware), które wykrada wrażliwe dane z urządzeń ofiar. Eksperci CERT Orange Polska wskazują, że pod tym względem ubiegły rok należał do malware'a Agent Tesla. Był jednym z najpopularniejszych i dominujących zagrożeń w skrzynkach polskich internautów. To złośliwe narzędzie, określane jako RAT (Remote Access Trojan), które umożliwia cyberprzestępcy zdalny dostęp do zainfekowanego komputera. Po raz pierwszy zostało wykryte w 2014 roku i początkowo miało bardzo ubogie funkcje. Po wielu latach rozbudowy kodu i pomysłów twórców ostatecznie stało się jednym z

Phoca PDF

bardzo popularnych złośliwych oprogramowań na rynku cyberprzestępców. Obecna wersja jest w stanie w pełni szpiegować system ofiary, przechwytywać poufne dane uwierzytelniające, a także działania użytkownika poprzez nagrywanie jego ekranu. Dodatkowo dysponuje funkcją keyloggera, rejestrującą klawisze naciskane przez użytkownika, umożliwia też kradzież danych uwierzytelniających z przeglądarek i klientów poczty.

Eksperci w trendach na 2024 rok wymieniają także wykorzystanie sztucznej inteligencji do typowania potencjalnych ofiar ataków. Mechanizmy oparte na AI będą tworzyć skuteczne kampanie dezinformacyjne, bo będą coraz lepiej „szkolone" do tworzenia deepfake'ów i ataków socjotechnicznych. Dezinformacja oparta na AI będzie w tym roku o tyle groźna, że może być wykorzystywana w trakcie kampanii wyborczych.

Cyberbezpieczeństwo stanowi coraz większe wyzwanie nie tylko dla indywidualnych użytkowników sieci, ale też firm i instytucji. Dlatego, jak wskazują eksperci, kluczowe znaczenie ma regularne badanie firmowych zabezpieczeń i podatności.

Źródło: Newseria

Phoca PDF