Bitdefender

Badania Bitdefendera pokazują, że niewielu internautów uważa się za cel cyberprzestępców

12.07.2024

Według raportu Bitdefender 2024 Consumer Cybersecurity Assessment Report większość konsumentów nie uważa, że są rzeczywistym celem cyberprzestępców. Jednak jedna czwarta z nich przyznaje, że doświadczyła incydentu bezpieczeństwa w ciągu ostatniego roku – liczba ta prawdopodobnie dotyczy tylko osób, które faktycznie wiedzą, że do niego doszło.

Czy uważasz, że jesteś celem cyberprzestępców?

Internauci z reguły mają trudności ze zrozumieniem, jak, kiedy, dlaczego i czy w ogóle są celem ataku. Zdecydowana większość (75,7%) albo nie wierzy, że jest celem ataku, albo nie jest pewna. I podczas gdy jedna czwarta (24,3%) uważa, że mogą paść ofiarą cyberprzestępców, ponad jedna trzecia (37,1%) jest przekonana, że hakerzy nie chcą ich dopaść.

Internauci nie są do końca w błędzie, nie uważając się za lukratywny cel dla cyberprzestępców. Tylko ułamek ataków hakerskich jest w rzeczywistości wymierzony w konkretną osobę – na przykład ataki spyware skierowane na znane osobistości, takie jak politycy, obrońcy wolności słowa, dysydenci, dziennikarze, gwiazdy itp.

Targetowanie występuje również w atakach socjotechnicznych, ale głównie w końcowych etapach, gdy osoba została już zwabiona i zidentyfikowana jako potencjalna ofiara. W większości przypadków zwykli ludzie nie są indywidualnie atakowani przez cyberprzestępców. Nie oznacza to jednak, że nie staną się celem w pewnym momencie.

Większość ataków jest nieselektywna

Jak zauważa zespół Bitdefender w swoim raporcie, niekoniecznie trzeba być na celowniku cyberprzestępców, aby paść ofiarą cyberataku. Większość kampanii cyberprzestępczych jest bezładna. Atakujący zazwyczaj wykorzystują:

- Dane wyciekłe z naruszeń danych, a następnie atakują swoje ofiary, stosując taktykę „spray and pray".

- Doxxing, aby zebrać dane o ofierze i skontaktować się z nią za pośrednictwem mediów społecznościowych

- Numery telefonów z baz spamu i kontaktują się z celem telefonicznie, SMS-em lub za pomocą wiadomości tekstowej.

Badania Bitdefendera pokazują, że niewielu internautów uważa się za cel cyberprzestępców

Większość ataków zaczyna się bez rozróżnienia na lukratywne cele, a rzeczywiste ukierunkowanie następuje w końcowych etapach ataku, gdy oszust zna imię ofiary, jej numer telefonu, adres e-mail i kontaktuje się z nią bezpośrednio.

Oszustwa związane z odzyskiwaniem kryptowalut

FBI wydało komunikat w ramach usługi publicznej, informując graczy na rynku kryptowalut, aby mieli oczy szeroko otwarte, ponieważ oszuści wzmagają swoją aktywność. W pierwszym ostrzeżeniu w zeszłym roku agencja zwróciła uwagę na wzrost liczby schematów odzyskiwania kryptowalut, których celem są ofiary, które już straciły kryptowalutę w wyniku oszustwa, przekrętów lub kradzieży. Teraz biuro twierdzi, że zauważyło nową taktykę przestępczą wykorzystywaną do dalszego oszukiwania ofiar oszustw kryptowalutowych: fikcyjne kancelarie prawne wabią ofiary, których portfele kryptowalutowe zostały już opróżnione przez oszustów, twierdząc, że zajmują się sprawą, aby odzyskać ich cenne zasoby – za opłatą.

Podszywanie się pod rząd

Oszuści telefoniczni podszywają się pod agentów federalnych i proszą o gotówkę, kryptowalutę lub karty podarunkowe.

Jak wynika z komunikatu opublikowanego w czerwcu przez amerykańską Agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), oszustwa polegające na podszywaniu się pod inne

osoby są coraz powszechniejsze. Często wykorzystywane są w nich nazwiska i tytuły pracowników rządowych.

„Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) jest świadoma niedawnych oszustów podszywających się pod agencję. Przypominamy, że pracownicy CISA nigdy nie skontaktują się z Tobą z prośbą o przelew pieniędzy, gotówki, kryptowaluty ani o użycie kart podarunkowych i nigdy nie poinstruują Cię, abyś zachował rozmowę w tajemnicy" – czytamy w notatce.

Jak poinformowała w kwietniu Federalna Komisja Handlu, Amerykanie stracili w zeszłym roku ponad miliard dolarów z powodu oszustów podszywających się pod przedsiębiorstwa lub agencje rządowe.

Oszustwa żerujące na osobach starszych

Targetowanie niekoniecznie występuje indywidualnie. Wiele oszustw ma na celu całe grupy demograficzne znane jako szczególnie dojrzałe do zbierania.

Prokuratorzy w USA uznali dwóch oszustów za winnych przestępstwa polegającego na masowej wysyłce mailingowej poprzez sprzedaż danych konsumentów oszustom, którzy następnie kierowali fałszywe nagrody do bezbronnych obywateli. Para – która posiadała mnóstwo informacji o konsumentach, w tym sposoby kierowania do konkretnych osób – sprzedawała listy docelowe konsumentów i ich adresy sprawcom oszustw, którzy kontaktowali się z ofiarami za pomocą fałszywych listów obiecujących nagrody pieniężne. Obaj mogą zostać skazani na 20 lat

więzienia.

Oszustwa związane z pomocą techniczną również żerują na tej wrażliwej grupie demograficznej. Japońskie władze biorą sprawę w swoje ręce, stosując nową taktykę walki z zagrożeniem, umieszczając fałszywe karty płatnicze w sklepach typu convenience.

Fałszywe oferty pracy

Oszuści często atakują internauci fałszywymi ofertami pracy, których celem jest kradzież pieniędzy. FBI zauważyło ostatnio wzrost liczby oszustw tego typu, w których oszuści „oferują ofiarom fałszywe prace zdalne, zazwyczaj obejmujące stosunkowo proste zadanie, takie jak ocenianie restauracji lub „optymalizowanie" usługi poprzez wielokrotne klikanie przycisku", zgodnie z notatką prasową FBI. Podszywając się pod agencję zatrudnienia lub rekrutacyjną, oszuści zazwyczaj kontaktują się z ofiarami za pomocą wiadomości tekstowych lub telefonicznie.

„Wyniki badania Bitdefender wskazują, że oszustwa polegające na przesyłaniu wiadomości tekstowych stanowią najczęstsze zagrożenie cybernetyczne, z jakim stykają się obecnie konsumenci. Oszuści wymyślają mylącą strukturę wynagrodzeń, która wymaga od ofiar dokonywania płatności w kryptowalutach, aby zarobić więcej pieniędzy lub „odblokować" pracę, a płatności trafiają bezpośrednio do oszusta. Ofiary są kierowane do fałszywego interfejsu, który wyświetla fałszywe zarobki, z których żadne nie są dostępne do wypłaty. Dlatego to niezwykle istotne, aby zachować czujność oraz zabezpieczyć swoje urządzenia za pomocą skutecznego systemu antywirusowego, który

został wyposażony w moduł antyphishingowy” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/badania-bitdefendera-pokazuja-ze-niewielu-internautow-uwaza-sie-za-cel-cyberprzestepcow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 12.07.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.