Bitdefender

Ataki BEC w 2023 r.: na co powinny uważać firmy i banki?

25.05.2023

Ataki Business Email Compromise (BEC) są cyberniebezpieczeństwami, które mają jeden z największych wpływów finansowych w ostatnich latach. BEC stały się tak znaczącymi cyberatakami, głównie dlatego, że opierają się na wykorzystaniu ludzkich słabości i omijają tradycyjne środki bezpieczeństwa antywirusowego, co prowadzi do znacznych strat finansowych dla firm i instytucji. Według FBI tylko w 2022 roku ataki BEC doprowadziły do strat w wysokości 2,7 miliarda dolarów. Biorąc pod uwagę, że liczba ataków BEC wzrosła w 2022 r. o 81%, jasne jest, że organizacje muszą być przygotowane na stawienie czoła temu zagrożeniu także w roku 2023.

Spośród branż najczęściej atakowanych przez BEC sektor finansowy oraz branża logistyczna zostały najbardziej dotknięte, a FBI ostrzega, że celem ataków BEC są teraz dostawy żywności. Biorąc pod uwagę zachęty finansowe, ataki BEC nie wydają się słabnąć, a napastnicy

znajdują nowe sposoby na przeprowadzanie skutecznych ataków.

Dlatego w tym artykule zagłębimy się w ewolucję ataków BEC i przedstawimy podstawowe informacje, o których organizacje muszą wiedzieć, aby chronić się przed tym rosnącym zagrożeniem.

Jak rozwijają się ataki BEC?

Ataki Business Email Compromise (BEC), znane również jako oszustwa CEO lub ataki man-in-the-mail, to wyrafinowane oszustwa wymierzone w firmy realizujące przelewy bankowe. Ataki te często polegają na tym, że cyberprzestępca podszywa się pod wysoko postawionego dyrektora lub zaufanego partnera, aby nakłonić pracowników do przelania środków i poufnych informacji, takich jak dane konta bankowego. Techniki stosowane w atakach BEC są różne, ale często opierają się w dużym stopniu na inżynierii społecznej i wykorzystują ludzkie słabości, w tym zaufanie i autorytet.

Chociaż może się wydawać, że ataki oparte na wiadomościach e-mail wychodzą z mody, tak nie jest. Zgodnie z raportem firmy Bitdefender z 2023 roku aż 25% kadry kierowniczej nadal nie zna podstawowych zasad cyberbezpieczeństwa i bezpiecznego postępowania z mailami.

Zasadniczo ataki BEC są zaawansowaną formą phishingu. Cyberprzestępcy przeprowadzają masowe kampanie phishingowe, wysyłając fałszywe wiadomości e-mail do dużej liczby potencjalnych ofiar. Dzięki narzędziom sztucznej inteligencji kampanie te stają się

coraz bardziej wyrafinowane. Chatboty oparte na sztucznej inteligencji, takie jak ChatGPT, są wykorzystywane do generowania wiarygodnych treści e-maili, które nie mają wielu typowych wskazówek, takich jak dziwny język lub słaba gramatyka.

Innym pojawiającym się trendem w atakach BEC jest wykorzystywanie deepfake'ów – generowanych przez sztuczną inteligencję filmów, obrazów lub głosów, które są podobne do prawdziwej osoby, pod którą się podszywają. Korzystając z technologii deepfake, osoby atakujące mogą naśladować głos dyrektora generalnego lub innego kierownika wyższego szczebla podczas spotkania, dodając tym atakom dodatkową warstwę wiarygodności.

Co ciekawe wykorzystywanie technologii deepfake do przeporwadzania kampanii phsihingowych nie jest czymś czysto hipotetycznym, ponieważ takie ataki rzeczywiście się zdarzają. W 2019 roku brytyjska firma energetyczna straciła 243 000 dolarów, gdy dyrektor generalny został oszukany przez hakera, który wykorzystał technologię deepfake do naśladowania głosu innych pracowników firmy. Ponieważ ataki BEC wciąż ewoluują, organizacje muszą być na bieżąco informowane o tych trendach i inwestować w zaawansowane środki bezpieczeństwa w celu obrony przed tym rosnącym zagrożeniem.

Jak ostatnie wydarzenia w branży bankowej mogą doprowadzić do większej liczby ataków BEC?

Branża finansowa została wstrząśnięta ostatnimi wydarzeniami związanymi z serią upadłości wielkich banków. Silicon Valley Bank i

Signature Bank upadły, a First Republic Bank musiał zostać uratowany przez JP Morgan, aby uniknąć podobnego losu. Stworzyło to bardzo napięte środowisko i odciągnęło uwagę oraz zmniejszyło zasoby przeznaczone na zapewnienie odpowiedniego cyberbezpieczeństwa, co może prowadzić do niepotrzebnego ryzyka dla mniejszych i lokalnych banków, na które cyberkompromis prawdopodobnie najbardziej wpłynie.

Oszuści pogarszają sytuację, wykorzystując niepewność i przeprowadzając różne ataki phishingowe i BEC. Oszuści kupili już domeny powiązane z SVB i Signature w nadziei na próbę kradzieży informacji finansowych, podczas gdy inni, bardziej nikczemni hakerzy kontaktowali się z klientami banków, których dotyczy problem, lub klientami klientów SVB, podszywając się pod organizację i prosząc o dane konta bankowego .

Podczas gdy największe banki najprawdopodobniej przetrwają takie ataki bez większych perturbacji, to mniejsze banki mogą ponieść znacznie gorsze konsekwencje, jeśli zostaną dotknięte atakami BEC. Nie tylko stracą środki w wyniku ataku, ale mogą być narażeni na ryzyko wycofania środków przez deponentów ze względu na wpływ cyberataku na ich reputację. Może to zaostrzyć problemy, które doprowadziły do upadku SVB i Signature Bank.

Jak organizacje finansowe mogą się bronić?

Budowa silnej kultury bezpieczeństwa i świadomości ma kluczowe znaczenie w walce z atakami BEC. Ze względu na charakter tych ataków pracownicy często stanowią zarówno pierwszą, jak i ostatnią linię

obrony. Nawet przy solidnych środkach bezpieczeństwa pojedynczy błąd w ocenie przez obojętnego lub niedbałego pracownika może doprowadzić do udanego ataku.

„Jednym z kluczowych kroków jest kultywowanie wysokiego poziomu czujności wśród pracowników. Regularne, ciągłe szkolenia w zakresie bezpieczeństwa mogą pomóc im dostrzec charakterystyczne oznaki ataków BEC, takie jak prośby o nietypowe przelewy bankowe lub pilne żądania, które omijają normalne procedury. Symulowane ćwiczenia phishingowe mogą być również przydatne we wzmacnianiu tego szkolenia, dając pracownikom praktyczne doświadczenie w identyfikowaniu prób ataków i reagowaniu na nie" – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Ważne jest również, aby wiedzieć, że jednorazowe szkolenie w zakresie świadomości bezpieczeństwa nie wystarczy, zwłaszcza iż obserwujemy ewolucję tych ataków i zmianę taktyki. Ciągłe szkolenie w zakresie bezpieczeństwa może zapewnić, że Twoi pracownicy będą świadomi tych nowych metod ataku, zanim zobaczą je w praktyce. Jednak nie wszyscy pracownicy mogą być tak otwarci, więc upewnij się, że budujesz kulturę bezpieczeństwa w całej organizacji, która obejmie twoje wysiłki.

Wiele organizacji uznało również za pomocne wdrożenie narzędzi i rozwiązań technicznych od dostawców, którzy automatycznie oznaczają lub wskazują wiadomości e-mail z zewnętrznych źródeł. Opcje te mogą pomóc w ochronie przed atakami za pośrednictwem poczty e-mail i obejmują:

Rozwiązania antywirusowe zabezpieczające pocztę e-mail: te narzędzia mogą skanować przychodzące wiadomości e-mail w poszukiwaniu oznak phishingu lub ataków BEC, takich jak podejrzane załączniki, adresy URL.

Monitorowanie domen: obserwując aktywność związaną z rejestracją domen, usługi te mogą ostrzegać, jeśli ktoś zarejestruje domenę, która bardzo przypomina Twoją własną — powszechna taktyka w atakach BEC.

Narzędzia bezpieczeństwa sieci: te narzędzia mogą pomóc wykryć nietypową aktywność w sieci, potencjalnie identyfikując trwający atak BEC.

Inwestycja w te narzędzia i strategie może znacznie wzmocnić obronę antywirusową Twojej organizacji przed atakami BEC. Należy jednak pamiętać, że żaden pojedynczy środek nie jest niezawodny. Wielowarstwowe podejście łączące zabezpieczenia techniczne z silną świadomością bezpieczeństwa jest często najskuteczniejszym sposobem ochrony przed tymi wyrafinowanymi atakami.

Źródło: https://bitdefender.pl/ataki-bec-w-2023-r-na-co-powinny-uwazac-firmy-i-banki/

Data udostępnienia: 25.05.2023

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.