Wiadomość e-mail: klikaj z ostrożnością

Jak się chronić przed phishingiem, oszustwem i innymi podstępami

cisco

Spis treści

Wprowadzenie

W zeszłym roku spam obchodził swoje 40 urodziny. Tak, to było w 1978 roku, kiedy Gary Thuerk, szef marketingu w Digital Equipment Corporation, rozesłał pierwszą wiadomość spam do 393 odbiorców w oryginalnej sieci ARPANET, aby zareklamować nowy produkt. Nic dziwnego, że ówczesna wiadomość spotkała się z równie miłym przyjęciem, jak dzisiejszy spam. Thuerk otrzymał ostrą reprymendę i polecenie, aby nigdy więcej tego nie robić.

Gdyby to było tak proste także dzisiaj. Czterdzieści lat później spam gwałtownie zyskał na popularności, zalewając nasze skrzynki niechcianymi ofertami lekarstw, produktów dietetycznych i ofertami pracy. To jednak nie wszystko; dołączyli do niego jego daleko bardziej niebezpieczni kuzyni: phishing i złośliwe oprogramowanie. Phishing powstał ponad 30 lat temu, a złośliwe oprogramowanie również może się poszczycić kilkoma dekadami historii rozsyłania poprzez pocztę e-mail.

Dziś możemy ze smutkiem stwierdzić, że wiele wiadomości e-mail to niechciany spam – lub gorzej. Ilości są oszałamiające: 85% wszystkich wiadomości e-mail wysłanych w kwietniu 2019 roku to spam, zgodnie z informacjami dostarczonymi przez grupę Talos. Ilość niechcianych wiadomości również rośnie; w kwietniu spam pobił rekord ostatnich 15 miesięcy.

Nadawca a odbiorca

Można stwierdzić, że wiadomość e-mail jest sformatowana w niemal idealnym formacie dla oszustów. Wiadomość e-mail zmusza użytkownika do przeczytania i dokonania oceny tego, co otrzymał, a następnie podjęcia decyzji, co w konsekwencji kliknie lub otworzy. Odpowiednia dawka inżynierii społecznej, która wykorzysta dobrą naturę użytkownika, może go pchnąć do działania.

Właśnie ona odpowiada za to, że poczta jest coraz popularniejszym sposobem na dostarczenie złośliwego oprogramowania oraz że tak trudno jest się przed nim systematycznie bronić. Rzadko, jeśli w ogóle, atak za pośrednictwem poczty e-mail omija użytkownika. Mimo że łącza URL prowadzące do niebezpiecznych lub złośliwych stron wykorzystujących ataki typu exploit kit są popularne, są one uzależnione od użytkownika, który najpierw musi kliknąć dane łącze w wiadomości e-mail.

Co to oznacza dla firm

Nic dziwnego, że poczta e-mail jest jednym z głównych wyzwań, które spędzają sen z powiek specjalistom ds. cyberbezpieczeństwa. W naszym najnowszym badaniu porównawczym bezpieczeństwa cybernetycznego, dowiedzieliśmy się, że 56% liderów cyberbezpieczeństwa uważa, że obrona przed zachowaniami użytkowników, takimi jak kliknięcie złośliwego łącza w wiadomościach e-mail, jest bardzo lub bardzo trudna. Ta odpowiedź plasuje się wyżej niż jakiekolwiek inne zagrożenie związane z bezpieczeństwem: wyżej niż dane w publicznej chmurze, wyżej niż używanie urządzeń mobilnych.

Uwagę specjalistów ds. cyberbezpieczeństwa przyciąga także częstotliwość tego rodzaju ataków. Przykładowo 42% ankietowanych opanowywało incydenty związane z otwarciem złośliwego spamu w firmie. 36% ankietowanych przeciwdziałało podobnym incydentom w wyniku kradzieży danych poprzez phishing. Zgodnie z danymi naszej ankiety porównawczej specjalistów ds. cyberbezpieczeństwa, największe zagrożenie dla firm związane jest z pocztą e-mail.

W osobnym badaniu, zamówionym przez Cisco i wykonanym przez ESG w 2018 roku, 70% respondentów stwierdziło, że ochrona przed zagrożeniem poczty e-mail staje się coraz trudniejsza. W kwestii skutków ataków poprzez pocztę e-mail 75% ankietowanych stwierdziło, że w znaczący sposób ucierpiała zdolność operacyjna, a 47% zadeklarowało poważne straty finansowe.

Wymagana odpowiedź

Jak zabezpieczyć coś, co jest koniecznym narzędziem i stanowi ryzyko? Wiele firm uważa, że przeniesienie się do chmury stanowi rozwiązanie tego problemu. Jednak chmura nie jest złotym środkiem na zagrożenie poczty e-mail. W większości przypadków to po prostu przerzucanie problemu w inne miejsce. Problemy z bezpieczeństwem nie znikają, lecz zostają.

Istnieje kilka sposobów na zminimalizowanie zagrożeń związanych z pocztą e-mail. W tym dokumencie omówimy współczesny krajobraz zagrożeń, robiąc przegląd najpopularniejszych rodzajów ataków poprzez pocztę e-mail. Rozłożymy na części pierwsze ich przebieg, cele oraz infrastrukturę, która za nimi stoi. Omówimy, co możesz zrobić, aby zapewnić swojej firmie bezpieczeństwo, a także w jaki sposób identyfikować zagrożenia przenoszone przez pocztę e-mail, z którymi spotykają się użytkownicy.

„Przeciętnie w ciągu dnia otrzymujemy około 412 000 wiadomości e-mail, z których 266 000 nawet nie dochodzi do naszych silników SMTP, ponieważ Talos blokuje je w oparciu o globalne informacje o zagrożeniach."

Milind Samant, dyrektor ds. bezpieczeństwa, SUNY Old Westbury

„Firmy muszą zrównoważyć bezpieczeństwo i ryzyko biznesowe oraz doświadczenie użytkownika. Po uzyskaniu takiej równowagi potrzebny jest program, który stosuje ochronę poprzez aktywną reakcję w przypadku wystąpienia niebezpieczeństwa. W rzeczywistości nie da się uniknąć popełniania błędów przez ludzi, a dziś mamy do czynienia z wielomiliardową branżą, która na te błędy liczy. Należy zaplanować plan działania na wypadek, gdy ktoś popełni błąd, aby móc szybko na niego reagować. Każdego dnia odkrywamy udane próby obejścia naszych zapór bezpieczeństwa z powodu ludzkiego błędu lub dedykowanych agentów. Celem tych ataków są nasze zasoby lub słabe punkty oprogramowania; każdego dnia sprawdzamy, czy nasze narzędzia aktywnego wykrywania i reagowania znajdują i powstrzymują ataki. Dlatego właśnie wiem, że mamy w pełni działający program bezpieczeństwa."

Steve Martino, Wiceprezes, Dyrektor ds. cyberbezpieczeństwa, Cisco

Dzisiejszy krajobraz zagrożeń poczty e-mail i phishingu

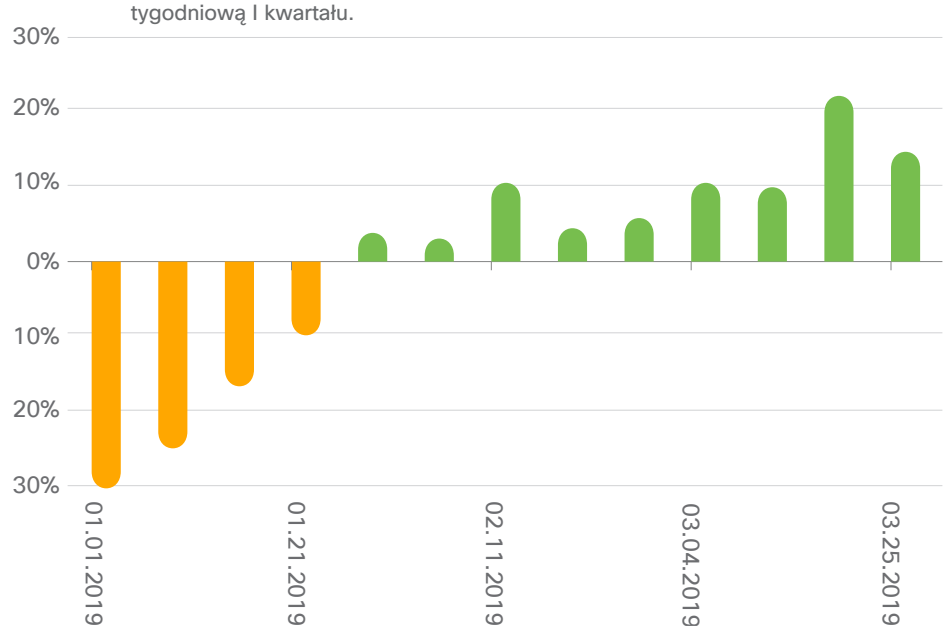
Zagrożenia powodowane przez pocztę e-mail są liczne. Zgodnie z raportem dot. śledztw w sprawie naruszeń bezpieczeństwa firmy Verizon z roku 2018, w którym Cisco wzięło udział, poczta e-mail to najpopularniejszy wektor rozprowadzania złośliwego oprogramowania (92,4%) i phishingu (96%). Wystarczy, że zareagujesz na niewłaściwą wiadomość e-mail i możesz paść ofiarą kryptokopalni, kradzieży danych logowania lub, jeśli dasz się nabrać na oszustwo, kradzieży dużych pieniędzy. Zeskaluj to na rozmiar przedsiębiorstwa, a okaże się, że niewłaściwa wiadomość e-mail może siać spustoszenie.

Jak często użytkownicy dają się nabrać na oszustwa e-mail? Zapytajmy specjalistów z Duo Security. Kilka lat temu zespół utworzył darmowe narzędzie Duo Insight, które pozwala użytkownikom na tworzenie własnych fałszywych kampanii phishingowych i testowanie ich w swojej organizacji, aby sprawdzić, kto da się nabrać, a kto nie.

Niestety wiele osób daje się wciągnąć w pułapkę. Zgodnie z raportem Zaufany dostęp z 2018 roku firmy Duo, 62% uruchomionych kampanii symulujących phishing przechwyciło minimalnie jeden zestaw danych logowania użytkownika. Spośród wszystkich adresatów prawie jedna czwarta z nich kliknęła łącze phishingowe w wiadomości. Połowa z nich wprowadziła dane uwierzytelniające na fałszywej stronie.

Po takim sukcesie nic dziwnego, że poczta e-mail stanowi tak popularny cel kampanii phishingowych. Co więcej, wydaje się, że działalność phishingowa zwiększa swoje możliwości, o ile weźmiemy pod uwagę liczbę nowych domen phishingowych zidentyfikowanych przez Cisco Umbrella. Wzięliśmy średnią tygodniową w pierwszym kwartale 2019, a następnie porównaliśmy ją ze średnią każdego tygodnia. Wyniki przedstawione na rys. 1 pokazują, że podczas gdy rok zaczął się powoli, później nastąpił wzrost częstotliwości tworzenia nowych domen aż o 64%, porównując pierwszy tydzień z ostatnim tego kwartału.

Rysunek 1 Nowe tygodniowe domeny phishingowe w porównaniu ze średnią tygodniową I kwartału.



Źródło: Cisco Umbrella

Najczęstsze rodzaje ataków przez pocztę e-mail

Poniżej znajduje się analiza najczęstszych oszustw opartych na wiadomościach e-mail z dnia dzisiejszego. Łap laptopa, otwórz skrzynkę i wyobraź sobie, że czekają tam na Ciebie następujące nieprzeczytane wiadomości.

Phishing za pomocą programu Office 365

Nadawcą wiadomości wydaje się Microsoft. W treści czytamy, że Twój adres e-mail powiązany z Office 365 zostanie odłączony z powodu błędu lub naruszenia zasad. Jedynym sposobem, aby temu zapobiec, jest zweryfikowanie adresu pod podanym łączem.

To próba wyłudzenia danych logowania do Office 365. Wiadomości e-mail i łącza URL mogą nawet wyglądać podobnie do tego, czego można by oczekiwać w związku z Office 365, na przykład: micros0ftsupport@hotmail.com. Jeśli klikniesz łącze, zostaniesz przeniesiony na wyglądającą na oficjalną stronę logowania, która zażąda Twojego adresu e-mail i hasła.

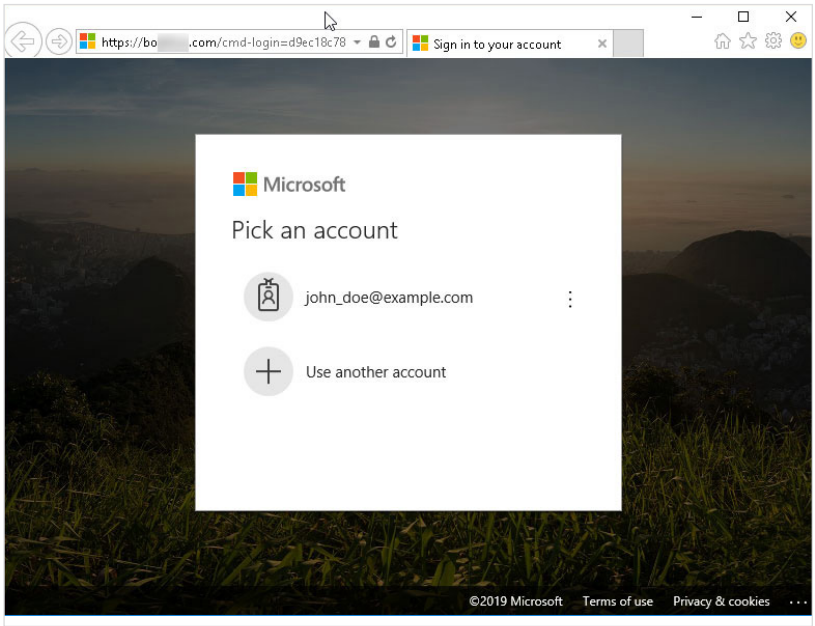
Jednak strona ta jest fałszywa. Kiedy oszuści pozyskają Twoje poświadczenia, mogą próbować logować się do innych powiązanych usług Microsoftu, a także ukraść Twoje kontakty. Jedną z powszechnych metod jest zalogowanie się na konto e-mail ofiary i rozesłanie osobom ze skrzynki adresowej nieformalnej wiadomości (np. Temat: DW), która zawiera kolejne phishingowe łącze URL.

Ataków tego rodzaju jest coraz więcej. Według danych opublikowanych przez naszych partnerów z Agari w raporcie nt. oszustw e-mailowych i trendów kradzieży tożsamości z II kwartału 2019 roku, 27% zaawansowanych ataków poprzez wiadomość e-mail jest rozsyłanych z kont pocztowych, na które się wcześniej włamano. To wzrost o 7 punktów procentowych w porównaniu z rokiem 2018, gdy 20% ataków phishingowych pochodziło z przejętych kont.

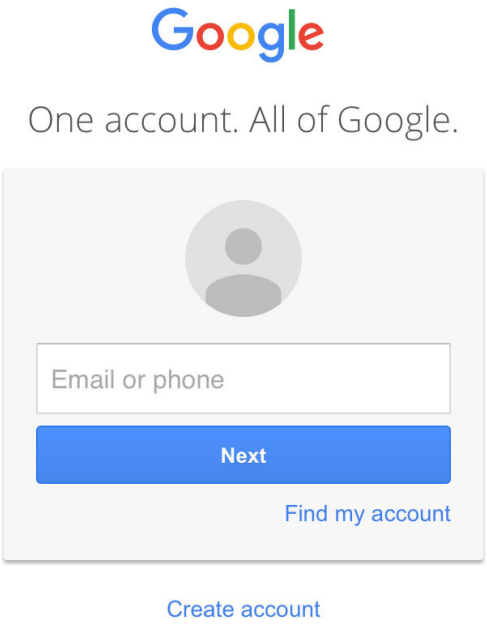
Celem jest nie tylko Office 365. Podobne ataki phishingowe zaobserwowano w usługach e-mailowych w chmurze, jak na przykład w Gmailu i G Suite. Biorąc pod uwagę popularność kont Google i to, jak często są one wykorzystywane do logowania się do różnych stron w całym Internecie, nic dziwnego, że cyberprzestępcy stworzyli phishingowe strony również w tym obszarze.

Podobne ataki phishingowe zaobserwowano w usługach e-mailowych w chmurze, jak na przykład Gmail i G Suite.

Rysunek 2 Strona phishingowa celowo zaprojektowana tak, aby wyglądała jak strona logowania firmy Microsoft.



Rysunek 3 Przykład logowania do konta Google. Czy umiesz odróżnić prawdziwą stronę od fałszywej?



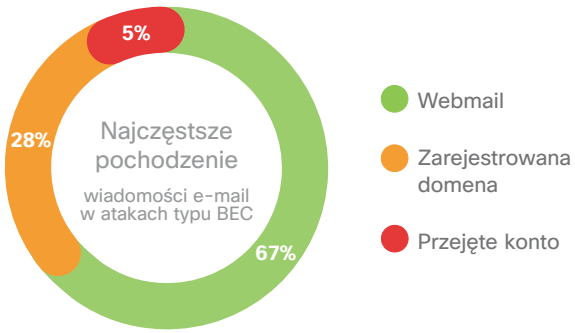
Naruszenia zabezpieczeń biznesowej poczty e-mail

W tym tygodniu odbywa się szczyt wielkich firm i oprócz małej liczby osób, które zapewniają działanie krytycznych funkcji, w biurze nie ma nikogo. Jesteś członkiem działu finansowego i częścią podstawowego składu, który jest na miejscu. Nagle w Twojej skrzynce pojawia się wiadomość e-mail, która wygląda, jakby wysłał ją dyrektor finansowy o tytule: „Przekroczono termin płatnosci". W wiadomości napisano, że płatność, która miała wyjść w zeszłym tygodniu, nie została wykonana, co może skutkować zakłóceniem w łańcuchu dostaw firmy. Dołączone są instrukcje dotyczące wykonania przelewu. Nadawca kończy wiadomość, pisząc, że skontaktuje się z Tobą w ciągu godziny.

To właśnie jest najbardziej typowe naruszenie bezpieczeństwa biznesu (BEC). Oszustwa typu BEC są formą oszustw dokonywanych za pośrednictwem wiadomości e-mail, w której cyberprzestępca podszywa się pod kierownika wyższego szczebla i próbuje nakłonić odbiorcę do wykonania zadania biznesowego w celu popełnienia nielegalnego czynu, jak na przykład przesłania mu pieniędzy. Zdarza się, że cyberprzestępcy posuwają się do dzwonienia do danej osoby i udawania kierownika. Wydaje się, że to działa. Zgodnie z internetowym centrum Internet Crime Complaint (IC3), z powodu oszustw typu BEC w 2018 roku w Stanach Zjednoczonych odnotowano straty w wysokości 1,3 mld USD.

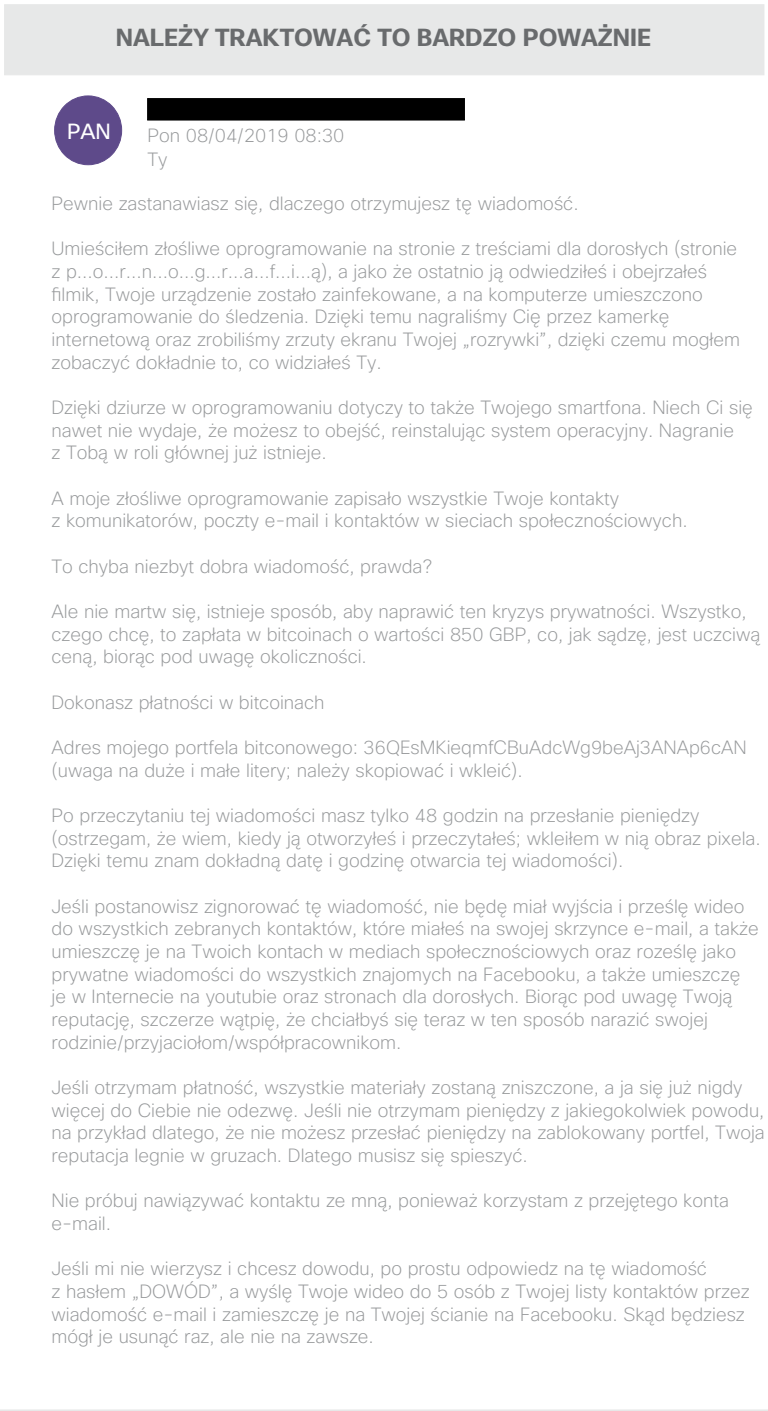
Wydawać by się mogło, że cyberprzestępcy wykorzystają przejęte konta w oszustwach typu BEC, jak to miało miejsce przy oszustwach phishingowych Office 365. Nieoczekiwanie, jak wynika z raportu nt. oszustw e-mailowych i trendów kradzieży tożsamości z II kwartału 2019 roku firmy Agari, tylko 5% tego rodzaju oszustw faktycznie z nich korzysta. Dwie trzecie ataków wciąż używa darmowych kont e-mailowych do rozsyłania ataków, natomiast pozostałe 28% atakuje poprzez zarejestrowane domeny. Ten ostatni poziom personalizacji dotyczy także treści wiadomości; zgodnie z informacjami Agari aż w jednej piątej wiadomości typu BEC zawarte jest imię docelowego odbiorcy.

Rysunek 4 Pochodzenie ataków typu BEC poprzez e-mail.



Źródło: Dane Agari, Inc.

Rysunek 5 Niedawny przypadek cyfrowego haraczu.



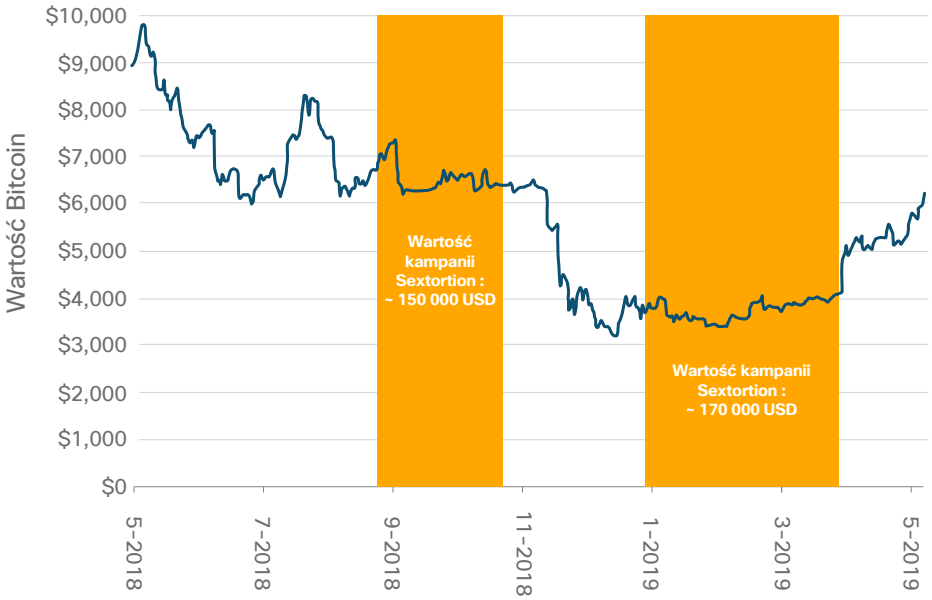
Cyfrowy haracz

W skrzynce odbiorczej pojawia się wiadomość o tytule: **„NALEŻY TRAKTOWAĆ TO BARDZO POWAŻNIE".** Nadawca wiadomości twierdzi, że włamał się na stronę zawierającą treści dla dorosłych, którą odwiedziłeś. Co więcej, twierdzi, że nagrywał Cię Twoją własną kamerką internetową, wraz z wideo, które w tym czasie oglądałeś. Poza tym, nadawca twierdzi, że uzyskał dostęp do Twoich kontaktów i prześle wszystkie materiały wraz z nagraniami, jeśli nie zapłacisz setek, o ile nie tysięcy, dolarów w bitcoinach.

To właśnie cyfrowy haracz. Jedyną rzeczą, która odróżnia go od bardziej tradycyjnych scenariuszy wyłudzenia pieniędzy jest fakt, że wszystkie twierdzenia są całkowicie zmyślone. Cyberprzestępcy nie przejęli strony internetowej, nie nagrali Ciebie, ani nie mają Twojej listy kontaktów. Po prostu mają nadzieję, że nakłonią Cię do uwierzenia, że to prawda.

Wiele form tego rodzaju oszustw omawiamy w naszym artykule na blogu Zagrożenie miesiąca, Pieniądze albo życie: oszustwa cyfrowych haraczy.

Rysunek 6 Porównanie wartości bitcoina (USD) do udziału w kampaniach haraczy seksualnych.



Źródło: Cisco Talos

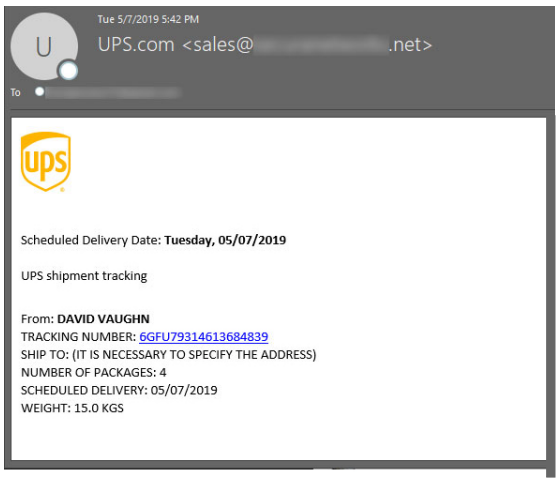
To interesujący podstęp i lukratywny interes dla cyberprzestępców: przychody uzyskane z kampanii cyfrowych haraczy osiągnęły poziom liczb sześciocyfrowych pod koniec 2018 roku. Jednak zgodnie z najnowszą analizą grupy Talos Cisco, obejmującą okres od stycznia do marca 2019 roku, zyski zmalały. I tak jednak wzrost i spadek tych zysków jest luźno powiązany z wartością bitcoina, a więc i spadkiem jego wartości. Jako że w chwili obecnej wartość bitcoina zdaje się wzrastać, jesteśmy ciekawi, czy to samo zjawisko zaobserwujemy w zyskach z cyfrowych haraczy.

Spam dot. przesyłek i faktur

„Nie pamiętam, żebym kupował subskrypcję na tę aplikację mobilną", myślisz. A to właśnie zdaje się twierdzić treść wiadomości: subskrypcja do końca życia w, powiedzmy, klubie filmowym. Trzymaj się, lokalizacja zakupu widniejąca na fakturze to Sri Lanka. A ty nawet nie mieszkasz w Sri Lance. „To musi być jakiś błąd", myślisz, szybko otwierając załączonego PDF-a, aby to sprawdzić.

Niestety ten PDF zawierał oprogramowanie, w wyniku którego pobrałeś na swoje urządzenie Emoteta. Oszustwa wyglądają różnie, ale zazwyczaj ich temat dotyczy paczki, której nie zamawiałeś, faktury za coś, czego nie kupiłeś lub comiesięcznej opłaty za subskrypcję lub usługę, na którą się nie zapisałeś. To może skutkować wieloma oszustwami, od kradzieży danych logowania do banku aż po zainstalowanie kryptokopalni.

Rysunek 7 Wiadomość e-mail z Emotetem, udająca wiadomość od firmy UPS.



Rysunek 8 Niedawny przykład oszustwa związanego z zaliczką.

Pan Christoper A. Wray

DW

Dyrektor Federalnego Biura Śledczego (FBI)
Do: [redacted]
Odpowiedz: [redacted]

Do: Beneficjent.

Zgodnie z etyką biura, wprowadzenie jest zawsze bardzo ważne przy nawiązaniu pierwszego kontaktu. Nazywam się Christopher A. Wray i jestem dyrektorem Federalnego Biura Śledczego (FBI). Niniejsze oficjalne memorandum ma na celu poinformowanie Państwa, że odkryliśmy, że pewni urzędnicy pracujący dla rządu Stanów Zjednoczonych próbowali wykraść Państwa środki poprzez nieoficjalny kanał. Odkryliśmy to właśnie dzisiaj, dzięki tajnym agentom, pracującym dla Działu dyscyplinarnego FBI po zatrzymaniu podejrzanego.

Wspomniany podejrzany został zatrzymany dziś rano na międzynarodowym lotnisku w Dulles, w trakcie próby ucieczki z terytorium USA z dużą ilością gotówki. Zgodnie z rozporządzeniem dot. prania brudnych pieniędzy w Stanach Zjednoczonych, taka ilość gotówki nie może być wywieziona ze Stanów Zjednoczonych, ponieważ stanowi to przestępstwo i jest karalne zgodnie z przepisami ustawy o praniu brudnych pieniędzy z roku 1982 Stanów Zjednoczonych Ameryki. Rozporządzenie to obowiązuje w większości państw rozwiniętych w celu powstrzymania terroryzmu i prania brudnych pieniędzy.

Ze zgromadzonych w dziale informacji wynika, że rzekome środki należą do Państwa, natomiast ich przesłanie zostało umyślnie opóźnione, ponieważ odpowiedzialni za to zadanie urzędnicy doszukują się tutaj pewnych nieprawidłowości, co jest całkowicie sprzeczne z zasadami etycznymi jakiejkolwiek instytucji płatniczej. Obecnie wspomniane środki znajdują się pod kontrolą banku i mogę Państwa zapewnić, że zostaną niezwłocznie zwolnione, pod warunkiem, że okażą się Państwo uczciwi. Dlatego prosimy o ułatwienie współpracy na każdym etapie, ponieważ bardzo uważnie przyglądamy się tej transakcji w celu uniknięcia nieuczciwych osób.

W dniu dzisiejszym 9 maja 2019 roku poleciliśmy kierownictwu banku wypłacenie Państwu wspomnianych środków, jako udokumentowanemu beneficjentowi, ponieważ posiadamy cenne informacje/dokumenty, które dowodzą, że wspomniane środki naprawdę do Państwa należą. W każdym razie konieczne jest przesłanie nam poniżej wymienionych informacji (w celu oficjalnej weryfikacji).

1. Imię, drugie imię i nazwisko.
2. Wiek.
3. Zawód.
4. Stan cywilny.
5. Bezpośredni numer telefonu/faksu.
6. Adres zamieszkania.

Oczekujemy natychmiastowego spełnienia tego oficjalnego obowiązku w celu wypłaty należności przez bank.

Oficjalnie podpisał

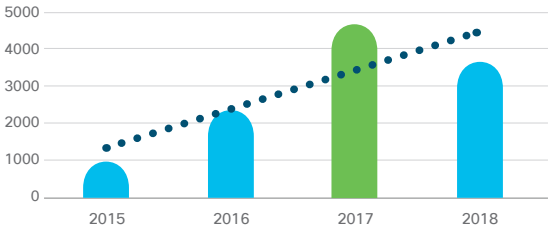
Pan Christoper A. Wray
Dyrektor Federalnego Biura Śledczego (FBI)

Oszustwa dot. zaliczek

Nie każdego dnia otrzymujesz wiadomość od FBI. To jeszcze rzadsze niż otrzymanie wiadomości informującej o oczekującym przelewie na 10,5 mln USD! Wszystko, co musisz zrobić, to odpowiedzieć na tę wiadomość, a oni poinstruują Cię, co należy zrobić, aby otrzymać przelew.

To klasyczne oszustwo związane z zaliczką. Jak sama nazwa wskazuje, oszuści będą prosić o zaliczkę, zanim wyślą Ci obiecane pieniądze – pieniądze, które nigdy się na Twoim koncie nie pojawią. To także jeden ze starszych rodzajów oszustw e-mailowych, który przybiera różne formy od lat, począwszy od księcia z zagranicy, który chce się podzielić bogactwem po podmioty udzielające pożyczek osobom spłacającym wysokie kredyty. A mimo to oszustwa nadal istnieją, a amerykańskie biuro Better Business Bureau (BBB) każdego roku otrzymuje informacje o tysiącach wiadomości e-mail tego rodzaju .

Rysunek 9 Oszustwa związane z wyłudzeniem zaliczki zgłaszane do biura BBB w ciągu roku.
(Suma rodzajów oszustw związanych z zaliczkami, wymianą pieniędzy w Nigerii/w innym kraju, romansem, pomocą z kredytem/umorzeniem długu, inwestycją oraz podróżami/wakacjami).



Źródło: Better Business Bureau

Złośliwe oprogramowanie w poczcie e-mail

Spora część złośliwego oprogramowania jest nadal dostarczana za pośrednictwem poczty e-mail. Kiedyś było to bardziej widoczne, ponieważ pliki .exe były dołączone bezpośrednio do wiadomości e-mail. Lecz kiedy użytkownicy nauczyli się, że otwieranie pliku programu dołączonego do wiadomości nie jest bezpieczne, cyberprzestępcy zmienili taktykę.

Obecnie dużo bardziej prawdopodobne jest, że złośliwe oprogramowanie zostanie przesłane bezpośrednio albo przez mniej podejrzane załączniki, takie jak powszechnie używane dokumenty biznesowe lub poprzez łącza URL zawarte w treści wiadomości – wszystkie będące regularnie wysyłane w normalnej, prawdziwej komunikacji e-mailowej. Celem tych zabiegów jest ominięcie tradycyjnego skanowania wiadomości e-mail, które wyłapałoby i wrzuciło do kwarantanny wiadomości z plikami binarnymi lub inne rzadko przesyłane załączniki.

Rzuca się to w oczy, gdy przeanalizuje się zaznaczone załączniki wiadomości e-mail w tym roku (w okresie od stycznia do kwietnia 2019). Pliki binarne stanowią mniej niż 2% wszystkich złośliwych załączników – to nie tylko pliki .exe, ale także wszystkie pliki binarne. Jest to dość duża zmiana w porównaniu do lat ubiegłych, gdy pliki .exe, Java lub Flash były regularnie spotykane. Co więcej, pliki Java i Flash tak bardzo wypadły z łask, że jeśli dodamy je do plików binarnych, nadal otrzymujemy zaledwie 1,99% załączników.

Pliki archiwalne, takie jak pliki .zip to niemal jedna trzecia załączników i cztery z dziesięciu najbardziej popularnych rodzajów plików wykorzystywanych przez cyberprzestępców.

Tabela 1 Rodzaje złośliwych załączników.

Typ	Wartość procentowa
Biuro	42,8%
Pliki archiwalne	31,2%
Skrypt	14,1%
PDF	9,9%
Plik binarny	1,77%
Java	0,22%
Flash	0,0003%

Źródło: informacje grupy Talos

Najczęściej spotykane rodzaje załączników to po prostu pliki, które są przesyłane w biurze każdego dnia – dwa z pięciu złośliwych plików to dokumenty pakietu Microsoft Office.

Jakiego rodzaju załączniki wybierają cyberprzestępcy? Pliki archiwalne, takie jak pliki .zip to niemal jedna trzecia załączników i cztery z dziesięciu najbardziej popularnych rodzajów plików. Skrypty takie jak pliki .js stanowią 14,1%. Odnotowaliśmy wysoki wzrost obecności tego rodzaju skryptów od ostatniej analizy rodzajów załączników w Corocznym Raporcie nt. Cyberbezpieczeństwa 2018 (ACR), kiedy pliki .js, wraz z plikami XML i HTML, stanowiły zaledwie 1% rozszerzeń złośliwych plików.

Ich występowanie wśród złośliwych załączników nadal rośnie, dochodząc już prawie do 5% od momentu publikacji raportu ACR 2018. Dorzućmy do tej mieszanki pliki PDF i okaże się, że ponad połowa wszystkich złośliwych załączników to regularnie używane rodzaje dokumentów, wszechobecne w nowoczesnym miejscu pracy.

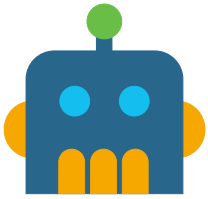
Tabela 2 Top 10 złośliwych rozszerzeń plików w wiadomościach e-mail.

Rozszerzenie pliku	Wartość procentowa
.doc	41,8%
.zip	26,3%
.js	14,0%
.pdf	9,9%
.rar	3,9%
.exe	1,7%
.docx	0,8%
.ace	0,5%
.gz	0,5%
.xlsx	0,2%

Źródło: informacje grupy Talos

Infrastruktura dostarczania poczty e-mail

Zajrzyjmy za kulisy, pomijając rodzaje wiadomości e-mail lub ich treść i przyjrzyjmy się sposobowi dystrybucji wiadomości e-mail. Istnieją dwie podstawowe metody, które oszuści wykorzystują do rozesłania kampanii spamu: botnety lub narzędzia do rozsyłania masowych wiadomości.



Botnety

Botnety spamu są zdecydowanie głównym winowajcą, odpowiedzialnym za większość rozsyłanego obecnie spamu. Poniżej znajdują się najważniejsze botnety rozsyłające spam.

Necurs

Botnet Necrus pojawił się pierwszy raz w 2012 roku i rozprzestrzenił różnorodne zagrożenia, od Zeusa po oprogramowanie ransomware. Mimo że jego aktywność wzbudzała duże zainteresowanie w przeszłości, dziś wydaje się, że Necrus znika, przynajmniej z nagłówków gazet. Jednak botnet ten nadal jest bardzo aktywny. W rzeczywistości botnet Necrus to główne narzędzie dystrybucji wielu oszustw, w tym cyfrowych haraczy.

Aby uzyskać więcej informacji na temat Necrusa, zapoznaj się z analizą Wiele macek botnetu Necrus, przeprowadzoną przez grupę Talos Cisco.

Emotet

Znaczna część spamu rozsyłanego przez Emoteta wpada pod kategorię przesyłek i faktur. Emotet to modułowe złośliwe oprogramowanie, zawierające wtyczkę typu spambot. Biorąc pod uwagę sposób, w jaki cyberprzestępcy stojący za Emotetem zarabiają pieniądze, wykorzystując kanały dystrybucji w przypadku innych zagrożeń, celem większości spamu rozsyłanego przez moduł spambotu jest zarażenie większej liczby systemów Emotetem, jeszcze bardziej rozszerzając zasięg złośliwego kanału dystrybucji.

Ponieważ Emotet kradnie zawartość skrzynek pocztowych ofiar, często potrafi tworzyć złośliwe (choć wyglądające realistycznie) wiadomości, które odbiorcy odbierają jako część prowadzonej konwersacji. Ponadto wiadomo, że Emotet kradnie dane logowanie SMTP, zarządzając serwerami poczty wychodzącej ofiary jako narzędzia do rozsyłania spamu.

Aby uzyskać więcej informacji na temat Emoteta, zapoznaj się z poprzednim raportem o zagrożeniach w serii raportów na temat cyberbezpieczeństwa, W obronie przed obecnie krytycznymi zagrożeniami.

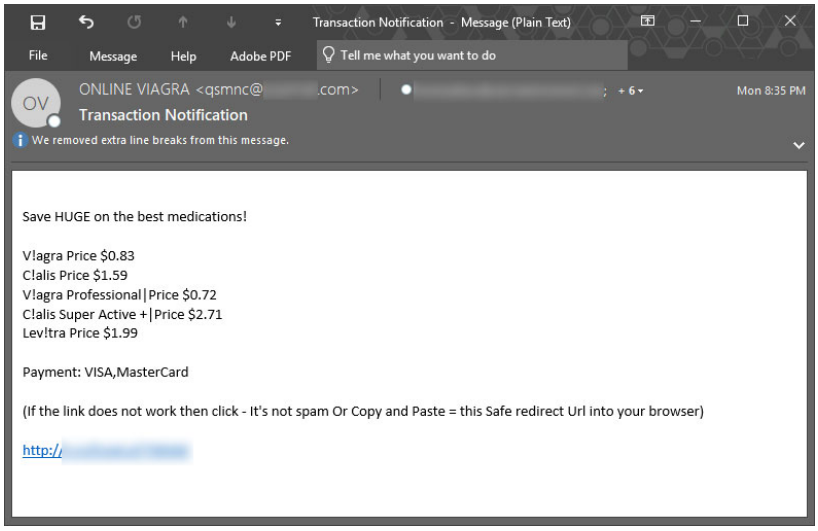
> **„Cisco Email Security zmniejszyło ilość czasu spędzanego na wykrywaniu zagrożeń oraz obniżyło ilość spamu o ok. 80%”.**
>
> **Jacquelyn Hemmerich, Dyrektor ds. bezpieczeństwa, Sarasota w stanie Floryda**

Gamut

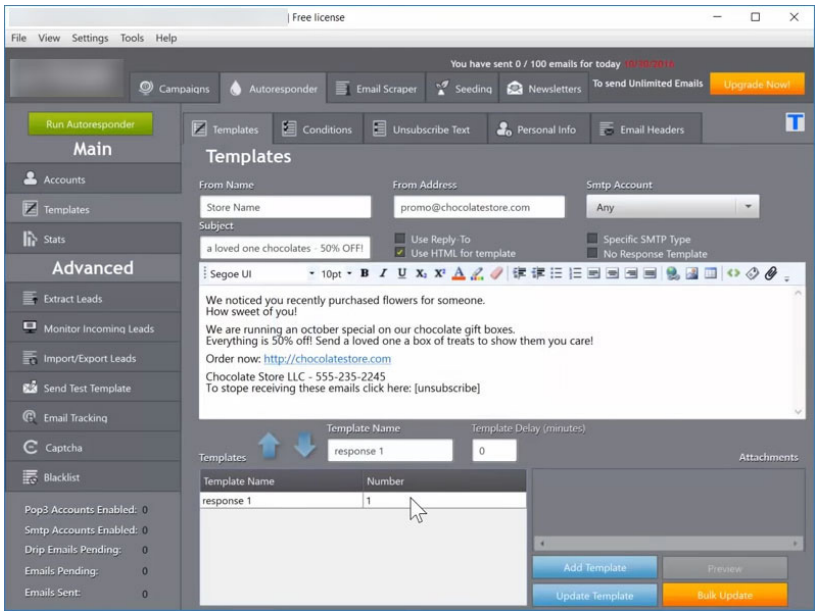
Botnet Gamut zajmuje się rozsyłaniem spamu związanego z randkowaniem i związkami, przede wszystkim w oparciu o założenie, że spotykasz się z ludźmi z Twojej okolicy. W innych kampaniach osoby odpowiedzialne za botnet wysyłają wiadomości reklamujące leki lub oferty pracy (zob. rys. 10).

Zarejestrowano różne domeny, chociaż sama ich infrastruktura wydaje się dość prosta, bo składa się z jednej domeny i wielu subdomen, często wskazujących na jeden adres IP. Mimo że Cisco nie potwierdzilo, czy ofertowane usługi są niezgodne z prawem, proces rejestracji wydaje się próbą wyłudzenia danych osobowych.

Rysunek 10 Wiadomość spam wysłana przez botnet Gamut.



Rysunek 11 Przykład zestawu narzędzi do rozsyłania spamu.



Zestawy narzędzi do masowego wysyłania wiadomości e-mail

Alternatywnym podejściem wielu spamerów jest zakup narzędzi do wysyłania dużej liczby wiadomości e-mail. Korzystanie z wielu z tych narzędzi bywa uzasadnione, to znaczy w przypadku sprzedawania ręcznie wykonanych i szytych na zamówienie zasłon prysznicowych, można by teoretycznie z nich korzystać, aby zwiększać świadomość marki poprzez masowe rozsyłanie wiadomości do osób z własnej listy mailingowej. Jednak korzystanie z niektórych funkcji zawartych w takich zestawach narzędzi, jak na przykład tych pozwalających na rotację wysyłanych adresów IP i niestandardowe przebudowywanie załączników w celu wygenerowania unikatowych wartości hashów, jest w tym przypadku dużo mniej prawdopodobne.

Ostatnio inżynierowie z grupy Talos Cisco odkryli na Facebooku grupy, w których cyberprzestępcy sprzedawali narzędzia do rozsyłania poczty masowej wraz z obszernymi listami adresów e-mail, które prawdopodobnie zostały zdobyte poprzez kradzież danych. W takich przypadkach nabywcy tych narzędzi w sposób oczywisty korzystali z nich w nikczemnych celach.

Oszustwo jako metoda

Jeśli poczta e-mail jest najczęstszym wektorem ataku, najczęstszą metodą jest oszustwo – zwłaszcza w przypadku przestępczości zorganizowanej.

Jeśli poczta e-mail jest najczęstszym wektorem ataku, najczęstszą metodą jest oszustwo – zwłaszcza w przypadku przestępczości zorganizowanej. Cyberprzestępcy odpowiedzialni za oszustwa typu BEC próbują okradać firmy z tysięcy dolarów. Osoby dokonujące cyfrowych haraczy podstępem nakłaniają użytkowników do dokonywania wpłat w bitcoinach. A jeśli chodzi o oszustwa związane z wpłacaniem zaliczek – wskazówka znajduje się w samej nazwie.

Nic z tego nie jest nowością. Poczta e-mail to tylko jedno z narzędzi, które cyberprzestępcy wykorzystują do popełnienia oszustwa. Z historycznego punktu widzenia przestępcy dążą do wykorzystywania okazji, pojawiających się w każdej generacji technologii, aby zwiększyć dochód z działalności przestępczej.

Patrząc na straty odnotowane przez niemiecką policję federalną (Bundeskriminalamt BKA) i FBI, ponad 80% wszystkich odnotowanych strat związanych z cyberprzestępczością można przypisać oszustwom. Kładziemy nacisk na słowo „odnotowane", ponieważ mogą występować niewymierne straty, które trudno jest określić i dokładnie opisać. Oznacza to, że statystyki, które są rejestrowane, są dość wiarygodne.

Dlatego stwierdzenie, że oszustwo jest motorem napędzającym straty powodowane cyberprzestępczością, jest prawdziwe. W rzeczywistości, analizując dwie metody oszustwa wskazane przez statystyki FBI, a mianowicie naruszenie bezpieczeństwa poczty firmowej (BEC) i włamania na konta e-mail (EAC), możemy stwierdzić, że w 2018 roku straty wyniosły 1,3 mld USD. W porównaniu, podobne straty spowodowane oprogramowaniem typu ransomware, metodą często przytaczaną i analizowaną, wyniosły 3,5 mln USD. Faktem nadal pozostaje: straty związane z niewykrytymi oszustwami będą nadal rosnąć, ponieważ straty związane z incydentami naruszeń bezpieczeństwa firmowej poczty e-mail, jak i włamaniami na konta e-mail wzrosły o 78% w okresie od 2016 do 2017 roku.

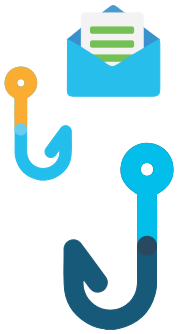
„Rozwiązanie Cisco Email Security spowodowało, że bezpieczeństwa poczty e-mail dosłownie przestało być zmartwieniem kierownictwa i pozwoliło nam się skupić na innych obszarach. Wyłapuje wszystko! Wiedza, że podjęliśmy doskonałą decyzję w zakresie bezpieczeństwa poczty e-mail, daje spokój ducha!"

Steven Wujek, starszy architekt ds. IT, Technology Concepts & Design, Inc.

Aby uzyskać więcej informacji na temat oszustw i strat spowodowanych cyberprzestępczością, zapoznaj się z serią na naszym blogu Cyberprzestępczość i oszustwa.

„Zastosowanie holistycznego podejścia do bezpieczeństwa nie jest tylko kwestią produktu zabezpieczającego lub koniecznością biznesową. **Chodzi o analizę osób, procesów i technologii w całej organizacji.** W Cisco zaczynamy od podejścia, w którego centrum znajdują się ludzie, praca, którą wykonują i przyczynianie się do tego, aby mogli ją wykonywać bezpiecznie. Jednym ze sposobów jest zapewnienie pracownikom praktycznych wskazówek dotyczących rozpoznawania i zgłaszania podejrzanych wiadomości e-mail zanim w nie klikną."

Steve Martino, Wiceprezes i Dyrektor ds. cyberbezpieczeństwa, Cisco



Jak chronić się przed atakami za pośrednictwem poczty e-mail

Charakterystyczne cechy wiadomości e-mail zawierającej phishing

Nadzieję daje fakt, że zagrożenia dostarczane przez wiadomość e-mail można zidentyfikować, jeśli wie się, czego szukać. Poniżej przedstawiono kilka przykładów. Szczegółowe informacje na temat każdego z nich można znaleźć na następnej stronie.

Do: ty@twojmail.com

1 Od: Amazon Shipping <amz@123fnord.com>

Temat: Twoja ostatnie zamówienie

Szanowni Państwo,

2 Dziękujemy Ci za zamówienie. Poniżej znajdują się szczegóły:

Zakup: miesięczny abonament na dostawę jedzenia dla zwierząt marki Puppy Food™

Koszt miesięczny: 121 dolarów USD

Data i godzina: 3 maia 2019, 10:21

Adres IP: 254.189.234.159.01

Kraj zakupu: Gwatemala

3 Jeśli chcesz zrezygnować z subskrypcji, anuluj ją natychmiastowo postępując zgodnie z załączoną instrukcją lub wprowadzając poniżej szczegóły Twojej karty kredytowej:

4

5 http://badphishingsite.com/dontgothere.html

Z poważaniem

Dział przesyłek Amazon

6 **nieotwierajtegoto.zle**

Rysunek 12 Ostrzeżenie Microsoft Office o makrach w otwartym dokumencie.

1. **Pole „Od”: adres.** Czy nazwa w polu „Od”: adres jest niezgodna z adresem e-mail?
2. **Liczne błędy ortograficzne i gramatyczne lub rozmazane logo.** Jeśli wiadomość e-mail wygląda na napisaną w sposób niechlujny, może nie być prawdziwa.
3. **Zmuszanie do szybkich działań.** Jeśli wiadomość e-mail zawiera prośbę o podjęcie natychmiastowych działań, jeśli zmusza do pilnego działania lub wzbudza ciekawość – zachowaj ostrożność.
4. **Prośba o podanie danych osobowych lub poufnych.** Nigdy nie odpowiadaj na niechciane wiadomości e-mail z prośbą o podanie danych osobowych, finansowych lub poufnych.
5. **Nieprawidłowy wygląd adresu URL.** Wiele phishingowych URL po głębszej analizie wygląda nietypowo i nie należy ich klikać. Jeśli adres URL jest ukryty w obrębie łącza tekstowego, umieść nad nim kursor myszy i spójrz na dół przeglądarki, aby je sprawdzić. Jeśli masz wątpliwości, nie klikaj go.
6. **Nierozpoznany typ pliku.** W większości profesjonalnych okoliczności powinno się przesyłać tylko kilka rodzajów plików. Jeśli rodzaj pliku wygląda dziwnie, nie otwieraj go.

W dodatku:

- **Zwolnij.** Przeciętny człowiek spędza 8-10 sekund na skanowaniu wiadomości e-mail, zanim podejmie działanie. Zwolnij i poszukaj wskazówek, które mogą wskazywać na próbę wyłudzenia informacji.
- **Jeśli coś brzmi zbyt dobrze, aby mogło być prawdziwe, prawdopodobnie jest oszustwem.** Czy w wiadomości e-mail oferują Ci miliony dolarów? Grożą, że Cię skompromitują lub skrzywdzą? Całkiem prawdopodobne jest, że wszystko to jest całkowicie zmyślone.
- **Zwracaj szczególną uwagę na znaki ostrzegawcze.** Jeśli rozpoznajesz nadawcę i otwierasz załącznik, zwróć szczególną uwagę na ostrzeżenia dotyczące rozszerzeń lub makr, które należy włączyć (Rysunek 12). Rzadko, jeśli w ogóle, jest to konieczne.

Strategie zapobiegania atakom

Istnieje kilka metod, które można stosować w celu zmniejszenia ryzyka stwarzanego przez zagrożenia w ramach poczty e-mail.

Przeprowadzaj regularne ćwiczenia phishingowe. Twoi pracownicy są Twoją największą ochroną przed phishingiem, szczególnie przed najbardziej dopasowanymi próbami phishingu. Pracownicy, którzy potrafią nauczyć się rozpoznawać próbę phishingu, mogą powstrzymać największe źródło zagrożeń punktów końcowych.

Aby zwiększyć świadomość, należy regularnie przeprowadzać phishingowe ćwiczenia w celu sprawdzenia i edukowania użytkowników. Naśladuj najnowsze techniki używane w świecie rzeczywistym, aby pracownicy byli na bieżąco z tym, z czym mogą się spotkać. Cisco zaleca przeprowadzanie tego rodzaju ćwiczeń co miesiąc, zaczynając od łatwych do wykrycia kampanii phishingowych i stopniowo zwiększając ich stopień złożoności. Użytkowników, którzy nabiorą się na symulowane ataki phishingowe, należy natychmiast przeszkolić (np. przesłać testowe „złośliwe" łącze URL, które przeniesie do informacji o phishingu). W przypadku użytkowników wysokiego ryzyka w organizacji, których błąd mógłby skutkować poważnymi szkodami, należy przeprowadzać ćwiczenia kampanii phishingowych dostosowane do indywidualnych potrzeb.

Uwierzytelnianie wieloskładnikowe. W przypadku faktycznej kradzieży poświadczeń firmowego konta e-mail, uwierzytelnianie wieloskładnikowe może uniemożliwić cyberprzestępcom uzyskanie dostępu do konta i spowodowanie strat.

Piękno wieloskładnikowego uwierzytelniania tkwi w jego prostocie. Powiedzmy, że komuś faktycznie udaje się zdobyć dostęp do Twoich lub czyichś danych logowania i próbuje się zalogować. Dzięki wieloskładnikowemu uwierzytelnianiu, wiadomość sprawdzająca zostaje przesłana automatycznie do właściciela danych logowania z informacją, czy faktycznie się logował. W tym przypadku użytkownik zdając sobie sprawę, że nie próbował się logować, od razu temu zaprzecza. To z powodzeniem udaremnia atak.

Dbaj o aktualny stan oprogramowania. W niektórych przypadkach wiadomości e-mail zawierające złośliwe łącza URL mogą przekierowywać użytkowników na strony wykorzystujące luki w zabezpieczeniach. Aktualizowanie przeglądarek i oprogramowania oraz wszystkich wtyczek pomaga w łagodzeniu zagrożeń stwarzanych przez takie ataki.

Nigdy nie przelewaj pieniędzy nieznajomemu. Dotyczy to oszustw związanych z zaliczkami i oszustw typu BEC. Jeśli w jakikolwiek sposób prośba wydaje Ci się podejrzana, nie reaguj. Szczególnie w przypadku prób oszustwa biznesowego należy ustanowić surowe zasady, które wymagają potwierdzenia przelewów przez osoby na wysokich stanowiskach w firmie oraz mieć wyznaczonego drugiego sygnatariusza.

Bądź ostrożny wobec próśb o zalogowanie się. Cyberprzestępcy, którzy usiłują ukraść dane logowania bardzo się starają aby ich strony wyglądały tak samo, jak strony logowania które znamy. Jeśli pojawi się okno logowania, należy sprawdzić łącze URL i upewnić się, że pochodzi z prawdziwej strony właściciela. Jeśli okno logowania jest wyskakującym oknem, rozszerz je, aby upewnić się, że pełen adres URL lub przynajmniej cała domena, są widoczne.

Sprawdź, czy wiadomość e-mail brzmi wiarygodnie. W przypadku oszustw, takich jak cyfrowe haracze i próby nakłonienia do wpłacenia zaliczki, nadawcy często opracowują skomplikowane historie, aby przekonać Cię, że wiadomość e-mail jest wiarygodna. Czy przedstawiona historia ma sens? Czy w historii są jakieś luki z punktu widzenia technicznego, procesu finansowego lub innego? Jeśli tak, traktuj ją sceptycznie.

Niezbędne jest przygotowanie

Istnieje wiele różnych sposobów, w jakie zagrożenia związane z pocztą e-mail oszukują lub starają się nakłonić użytkownika do udzielenia odpowiedzi, kliknięcia adresu URL lub otwarcia załączników. Uzasadnia to korzystanie z oprogramowania zabezpieczającego pocztę e-mail, które może przechwytywać i poddawać kwarantannie złośliwe wiadomości e-mail i filtrować spam.

Niestety, odkryliśmy martwiący trend: odsetek organizacji korzystających z zabezpieczeń poczty e-mail maleje. Zgodnie z naszymi najnowszymi analizami porównawczymi bezpieczeństwa cybernetycznego, tylko 41% respondentów korzysta obecnie z zabezpieczeń poczty e-mail w ramach ochrony przed zagrożeniami, nawet jeśli twierdzą, że poczta e-mail jest najczęstszym wektorem ataków narażających organizację na ryzyko. To spadek w porównaniu do roku 2014, kiedy 56% organizacji korzystało z zabezpieczeń poczty e-mail.

Istnieje kilka możliwych przyczyn tego spadku. Jedną z nich może być przejście do chmury. W niedawnym badaniu przeprowadzonym przez firmę ESG w imieniu firmy Cisco ponad 80% respondentów powiedziało, że ich organizacja korzysta z usług poczty e-mail opartych na chmurze. Ponieważ coraz więcej organizacji wybiera usługi poczty e-mail hostowane w chmurze, narzędzia poczty e-mail w siedzibie klienta są mniej potrzebne, a niektóre zespoły IT zakładają, że mogą się bez nich obejść.

Jednakże, podczas gdy wiele usług poczty e-mail w chmurze zapewnia podstawowe funkcje zabezpieczeń, należy podkreślić potrzebę ochrony warstwowej. W rzeczywistości, w ramach tego samego sondażu przeprowadzonego przez firmę ESG, 43% respondentów odkryło, że wymaga dodatkowego zabezpieczenia w celu ochrony poczty e-mail po przeniesieniu na chmurę. W końcu ważne potrzeby zespołów IT w zakresie ustalania zasad, uzyskiwania wglądu w informacje i kontroli, korzystania z systemów testowych i wykorzystywania zewnętrznych funkcji blokowania, nie zniknęły.

Kolejnym zagadnieniem, z jakim obecnie zmagają się zespoły ds. bezpieczeństwa, jest zwiększona powierzchnia ataku, co naturalnie prowadzi do powstania większej liczby obszarów, które potrzebują ochrony. Jeśli budżety bezpieczeństwa nie nadążają za tym wzrostem, zespoły mogą musieć rozplanowywać istniejące zasoby tak, aby ochronić za ich pomocą większy obszar zagrożenia.

Biorąc pod uwagę, że poczta e-mail jest najczęstszym wektorem ataków, jej ochrona nie może zostać zignorowana. Podczas przeprowadzania jakiejkolwiek oceny ryzyka cybernetycznego ważne jest ustalenie priorytetów najbardziej krytycznych punktów wejścia dzięki dokładnej ochronie oraz systemom zarządzania ryzykiem, a także poprzez obniżenie prawdopodobieństwa ataku, stanowiącego dla organizacji ryzyko. Następnie należy przydzielić zasoby, które są współmierne do krytycznego znaczenia potencjalnych strat.

Ponadto firma Gartner sugeruje, aby managerowie ds. bezpieczeństwa i zarządzania ryzykiem (SRM) podjęli trzy kroki w celu poprawy ochrony przed atakami typu phishing:

1. Przeprowadzenie aktualizacji bramy poczty e-mail i innych narzędzi kontrolujących, aby poprawić ochronę przed phishingiem.
2. Zapoznanie pracowników z rozwiązaniem i stworzenie funkcji do wykrywania i reagowania w przypadku podejrzenia ataku.
3. Współpraca z managerami biznesowymi w celu opracowania standardowych procedur operacyjnych w zakresie obsługi danych wrażliwych i transakcji finansowych.

Jak chronić pocztę e-mail

Przyjrzeliśmy się charakterystycznym cechom wiadomości phishingowej i strategiom zapobiegania atakom. Teraz przeanalizujemy oczekiwania względem technologii zabezpieczeń w 2019 roku.

Podobnie jak w przeszłości, wielowarstwowe podejście do bezpieczeństwa ma kluczowe znaczenie w ochronie organizacji przed atakami wykorzystującymi wiadomości e-mail. Istnieje kilka wypróbowanych i przetestowanych funkcji zabezpieczeń poczty e-mail, które mają znaczenie także dzisiaj.

Na przykład:

- Ochrona przed spamem wciąż musi być stosowana, aby zapobiegać otrzymywaniu niechcianych wiadomości e-mail i złośliwego spamu.
- Zabezpieczenia przed zagrożeniami, takie jak funkcje blokowania adresów URL oraz złośliwego oprogramowania i informacje na temat łączy URL mają kluczowe znaczenie w blokowaniu złośliwego oprogramowania, phishingu, oprogramowania typu ransomware i kryptokopalni w załącznikach oraz zwalczania złośliwych łączy w wiadomościach.
- Zintegrowane sprawdzanie pliku w środowisku testowym powinno dziać się automatycznie w tle dla nowo przychodzących plików, aby szybko stwierdzić, czy nie są złośliwe.

Należy jednak mocno podkreślić, że krajobraz zagrożeń ulega ciągłym zmianom, a cyberprzestępcy zawsze będą szukać nowych sposobów, by zaatkować.

Następujące technologie zabezpieczeń, oprócz wypróbowanych i przetestowanych, mogą przyczynić się do zwalczania tego nieustannie zmieniającego się środowiska:

- Bardziej zaawansowane zabezpieczenia przed phishingiem pojawiły się dzięki wykorzystaniu uczenia maszynowego, które pomogło zrozumieć i potwierdzić tożsamość wiadomości e-mail oraz relacje behawioralne w celu blokowania zaawansowanych ataków phishingowych.
- Obecnie można aktywować zabezpieczenia domeny DMARC, aby chronić markę firmy, uniemożliwiając cyberprzestępcom korzystanie z legalnej domeny firmowej w kampaniach phishingowych.
- Funkcja kwarantanny wiadomości jest przydatna do przechowania wiadomości w czasie, gdy załącznik pliku jest analizowany przed dostarczeniem wiadomości do adresata, usuwania złośliwego załącznika lub całkowitego usunięcia wiadomości.
- Naprawa wiadomości e-mail pomaga w przypadku, gdy złośliwy plik zostanie wykryty po dostarczeniu go do odbiorcy, pozwalając na objęcie danej wiadomości z złośliwym załącznikiem kwarantanną już z poziomu skrzynki.
- Zewnętrzne informacje o zagrożeniach związanych z pocztą e-mail w STIX są obecnie powszechnie wykorzystywane przez produkty zabezpieczające pocztę e-mail, co pomaga w przypadku gdy organizacja chciałaby korzystać raczej z informacji o wertykalnych źródłach zagrożeń niż oryginalnych informacji zawartych w produkcie.
- Integracja zabezpieczeń poczty e-mail z szerszą ofertą bezpieczeństwa staje się również powszechna w celu sprawdzenia czy zaawansowane złośliwe oprogramowanie lub wiadomości w środowisku mogły zostać dostarczone do poszczególnych użytkowników lub skrzynek pocztowych.

„Cisco zostało wybrane liderem w dziedzinie bezpieczeństwa firmowej poczty e-mail w raporcie Forrester Wave z roku 2019, otrzymując najwyższe oceny w kategoriach: opcje wdrożenia, ochrona przed atakiem i uwierzytelnianie poczty e-mail, działania i operacje (w tym skalowalność i niezawodność) oraz przywództwo technologiczne."

Forrester Wave™: Bezpieczeństwo firmowej poczty e-mail, II kwartał 2019

O serii o cyberbezpieczeństwie Cisco

W ciągu ostatniej dekady Cisco opublikowało wiele informacji na temat bezpieczeństwa i zagrożeń dla specjalistów zainteresowanych stanem globalnego cyberbezpieczeństwa. Te kompleksowe badania dostarczają szczegółowych danych na temat zagrożeń i ich następstw dla firm, a także wielu dobrych praktyk, mających na celu ochronę przed niepożądanymi skutkami wycieków danych.

W ramach nowego podejścia kierownictwo Cisco Security publikuje serię publikacji opartych na badaniach i danych pod nazwą Seria o cyberbezpieczeństwie Cisco. Rozszerzyliśmy liczbę tytułów, aby zawrzeć różne raporty dla specjalistów do spraw bezpieczeństwa o różnych zainteresowaniach. Wcześniejsza seria raportów z 2019 roku skupia się na dogłębnej ekspertyzie badań dotyczących zagrożeń i innowacji w branży bezpieczeństwa i zawiera Analizę porównawczą ochrony danych, Raport na temat zagrożenia i Analizę porównawczą Cisco, a także inne, które ukażą się w ciągu roku.

Aby uzyskać więcej informacji i dostęp do raportów oraz zarchiwizowanych wersji, odwiedź www.cisco.com/go/securityreports.

Centrala dla krajów Ameryki Północnej i Południowej
Cisco Systems, Inc.
San Jose, CA

Centrala dla krajów Azji i Pacyfiku
Cisco Systems (USA) Pte. Ltd.
Singapur

Centrala europejska
Cisco Systems International BV Amsterdam,
Holandia

Firma Cisco ma ponad 200 biur na całym świecie. Pełną listę adresów, numerów telefonów oraz faksów można znaleźć na stronie internetowej firmy Cisco pod adresem: www.cisco.com/go/offices.

Opublikowano w czerwcu 2019 roku THRT_02_0519_r1