**Cisco wskazuje na najważniejsze trendy w zakresie cyberzagrożeń**

Jeśli chodzi o bezpieczeństwo, decyzja o tym, na co przeznaczyć zasoby, ma kluczowe znaczenie. Aby zrobić to optymalnie, firmy muszą wiedzieć, jakie zagrożenia na tym polu mają największą szansę pojawić się w ich organizacjach w niedalekiej przyszłości i jaki mogą mieć na nie wpływ. Wyzwanie polega na tym, że peleton najbardziej aktywnych niebezpieczeństw zmienia się niezwykle dynamicznie, a częstotliwość poszczególnych ataków jest bardzo zróżnicowana. Dlatego tak pomocna staje się wiedza na temat kluczowych trendów w krajobrazie zagrożeń. Może ona dostarczyć amunicji do skutecznej obrony i informacji co do tego, gdzie najlepiej alokować zasoby.

Eksperci Cisco, analizując ruch z platformy Umbrella przyglądają się aktywnościom, które występują w środowisku zagrożeń, analizując jednocześnie ruch na zainfekowanych stronach i protokoły DNS. Robią to, patrząc na organizację jako całość, a dopiero na kolejnym etapie analizują liczby punktów końcowych, które mogą potencjalnie łączyć się ze złośliwymi witrynami oraz liczby zapytań, które te strony otrzymują. Działania te pozwalają uzyskać wgląd w to, jak wielu użytkowników klika w zainfekowane linki w poczcie e-mail, jak bardzo aktywne są wirusy typu RAT (remote acces trojan) lub czy cryptomining nadal rośnie w siłę. Zebrane dane mogą być źródłem wiedzy o tym, gdzie należy zainwestować większe zasoby, czy np. na szkolenia z zakresu bezpieczeństwa czy obszary, w których należy zbudować poradniki dotyczące tego, jak polować na cyberzagrożenia.

Analizując zapytania DNS wysyłane do podejrzanych domen oraz tych zainfekowanych konkretnymi wirusami w okresie od stycznia do grudnia 2020 roku, eksperci Cisco przejrzeli szereg trendów związanych z cyberzagrożeniami. Na tej podstawie wyróżnili te, z którymi organizacje mogą zetknąć się najczęściej.

**Organizacje i złośliwa aktywność DNS**

Według danych Cisco Umbrella, w 86 procent organizacji przynajmniej jeden użytkownik próbował połączyć się z witryną phishingową, prawdopodobnie poprzez kliknięcie w link znajdujący się w wiadomości.

Co ciekawe, podobne scenariusze pojawiają się w innych kategoriach:

* W 70 procent organizacji znaleźli się użytkownicy, którym prezentowano złośliwe reklamy w przeglądarce.
* 51 procent firm spotkało się z aktywnością związaną z ransomware.
* 48 procent organizacji wykryło złośliwe oprogramowanie wykradające informacje.

**Cryptomining**

Nie jest zaskoczeniem, że ten typ ataków generował najwięcej ruchu DNS spośród wszystkich kategorii. Podczas, gdy ta forma ataków jest często preferowana przez cyberprzestępców w celu generowania niewielkich dochodów, jest on stosunkowo łatwy do odnotowania po stronie DNS, ponieważ regularnie pinguje serwery, prosząc o więcej mocy obliczeniowej.

Ich częstotliwość w dużej mierze pokrywa się z wahaniami wartości popularnych kryptowalut.

**Phishing**

Ilość aktywności DNS związanych z phishingiem utrzymywała się na dość stabilnym poziomie przez cały rok, z wyjątkiem grudnia, w którym odnotowano 52-procentowy wzrost w okresie świątecznym. Jeśli chodzi o liczbę punktów końcowych odwiedzających strony phishingowe, znaczący wzrost nastąpił w sierpniu i wrześniu. Ma to związek m.in. z bardzo dużą kampanią phishingową pomiędzy lipcem a wrześniem.

**Trojany**

Podobnie jak w przypadku cryptominingu, trojany rozpoczęły rok bardzo mocno. Niezwykle wysoka liczba punktów końcowych łączących się z witrynami trojanów była w dużej mierze spowodowana przez Ursnif/Gozi oraz IcedID – dwa groźne wirusy znane z tego, że współpracują ze sobą w celu rozprzestrzeniania ransomware. Tylko te dwa złośliwe programy stanowiły 82% trojanów zaobserwowanych na punktach końcowych w styczniu. Ponadprzeciętne wyniki ze stycznia były prawdopodobnie związane z kampanią świąteczną prowadzoną przez atakujących, a następnie wraz z upływem roku spadły i ustabilizowały się.

W drugiej połowie roku, pod koniec lipca przebudził się natomiast Emotet, jeden z groźniejszych trojanów ostatnich lat, generując ogromny ruch, który narastał przez cały wrzesień. Tylko to zagrożenie jest odpowiedzialne za duży wzrost aktywności DNS w okresie od sierpnia do września. W sumie zatknęło się z nim 45% organizacji.

**Ransomware**

Przez większą część roku dominowały dwa kluczowe zagrożenia typu ransomware - jedno pod względem zasięgu, drugie pod względem głębokości działania. Począwszy od kwietnia, liczba komputerów zaatakowanych przez Sodinokibi (znany jako REvil) znacznie wzrosła i rosła aż do jesieni. Wzrost ten był na tyle znaczący, że 46 procent organizacji zetknęło się z tym zagrożeniem. We wrześniu ogólna liczba zapytań dotyczących tej konkretnej grupy ransomware wzrosła pięciokrotnie w porównaniu z sierpniem, co prawdopodobnie wskazało na to, że ładunek ransomware był aktywowany na wielu zaatakowanych systemach.

To jednak nadal kropla w morzu w porównaniu z aktywnością wirusa Ryuk, który jest w dużej mierze odpowiedzialny za listopadowo-grudniowy skok aktywności. Był on tak wysoka, że wpłynęła na ogólną aktywność w pozostałej części roku. Jednak liczba punktów końcowych łączących się z domenami powiązanymi z Ryukiem pozostawała stosunkowo niewielka i stała przez cały rok, wykazując jedynie niewielki wzrost przed gwałtownym wzrostem aktywności zapytań. Podsumowując Sodinokibi atakuje dużą liczbę punktów końcowych, żądając mniejszego okupu. Ryuk atakuje znacznie mniej systemów, żądając znacznie większego okupu.

**Skuteczne zapobieganie atakom**

„Dane wykorzystane do zilustrowania tych trendów pochodzą z Cisco Umbrella, usługi bezpieczeństwa dostarczanej w chmurze, która obejmuje zabezpieczenia DNS, bezpieczną bramę internetową, zaporę sieciową i funkcje brokera bezpieczeństwa dostępu do chmury (CASB) oraz informacje o zagrożeniach” – mówi Łukasz Bromirski, Engineering Product Manager, Cisco Security Business Group..

„W każdym z tych przypadków złośliwe działanie zostało zatrzymane przez Umbrella. Użytkownik, który kliknął w phishingową wiadomość e-mail, nie był w stanie połączyć się ze złośliwą witryną” – dodaje Artur Czerwiński, Dyrektor ds. Technologii, Cisco Polska.

Umbrella łączy wiele funkcji bezpieczeństwa w jednym rozwiązaniu, dzięki czemu można rozszerzyć ochronę na urządzenia, użytkowników zdalnych i rozproszone lokalizacje w dowolnym miejscu. Umbrella to najprostszy sposób na skuteczną ochronę użytkowników w dowolnym miejscu w ciągu kilku minut.

Dodatkowo, narzędzie Umbrella Investigate zapewnia najbardziej kompletny obraz zależności i ewolucji domen internetowych, adresów IP i plików, pomagając w identyfikowaniu infrastruktury napastników i przewidywaniu przyszłych zagrożeń. Żaden inny dostawca nie oferuje takiego samego poziomu interaktywnej informacji o zagrożeniach.

**Trendy dotyczące bezpieczeństwa cyfrowego związane z poszczególnymi branżami**

Oczywiście znajomość dominujących trendów w krajobrazie zagrożeń pozwala być lepiej przygotowanym do lokowania zasobów bezpieczeństwa tam, gdzie są one najbardziej potrzebne, jednak istotne jest także to, że różne branże są w różnym stopniu narażone na pewne typy zagrożeń. Na przykład, w branży usług finansowych można zaobserwować większą aktywność złodziei informacji, podczas gdy sektor produkcji może być bardziej narażony na oprogramowanie ransomware.

**Sektor IT**

Zdecydowana większość złośliwego ruchu DNS w sektorze technologicznym – branżą związaną z rozwojem i/lub dystrybucją produktów i usług IT – może być przypisana do dwóch kategorii: cryptomining i phishing. Tylko te dwie kategorie odpowiadały za 70 procent złośliwego ruchu w organizacjach z tego sektora. Nic dziwnego, że w IT zaobserwowano znacznie więcej ruchu związanego z cryptominingiem niż w jakiejkolwiek innej branży. Chociaż znaczną część tej aktywności można przypisać cyberprzestępcom, możliwe jest również, że większa wiedza na temat kryptowalut może skłonić pracowników tej branży do prób zainstalowania koparek kryptowalut na swoich komputerach firmowych, powodując blokady DNS w ramach Cisco Umbrella z powodu naruszenia polityki firmy.

Co ciekawe, sektor technologii odnotował drugi najwyższy poziom ruchu związanego z ransomware, głównie za sprawą ataków z wykorzystaniem Sodinobiki i Ryuk. Jednak niezwykle wysoki udział cryptominingu obniżył ogólny odsetek, który wyniósł sześć procent. Aktywność trojanów była również wysoka, biorąc pod uwagę, że Emotet i Trickbot zostały wykorzystane do dystrybucji Ryuka.

**Sektor usług finansowych**

W sektorze usług finansowych, to ataki phishingowe spowodowały najwyższy poziom złośliwego ruchu DNS. Eksperci Cisco analizujący krajobraz zagrożeń zaobserwowali o 60% więcej przypadków ataków tego typu niż np. w szkolnictwie wyższym. Możliwe, że sektor ten jest celem ataków phishingowych częściej niż inne, po prostu ze względu na bliskość celu końcowego wielu cyberprzestępców, jakim są pieniądze. Potwierdzeniem tej tezy jest fakt, że w sektorze usług finansowych zaobserwowano więcej zagrożeń polegających na kradzieży informacji niż w jakiejkolwiek innej branży.

**Opieka zdrowotna**

W branży ochrony zdrowia zaobserwowano więcej trojanów niż w jakimkolwiek innym sektorze, ale także większą niż gdzie indziej liczbę wirusów typu dropper, czyli tych służących do instalowania złośliwego kodu na komputerach ofiar. Większość aktywności opartych na trojanach można przypisać Emotetowi, ponieważ organizacje opieki zdrowotnej zostały mocno dotknięte przez to zagrożenie w 2020 roku. Prawie siedem na dziesięć trojanów zaobserwowanych w sektorze opieki zdrowotnej to Emotet. Dodając do tego bliskiego kuzyna Emoteta - Trickbota, otrzymujemy 83% całego ruchu związanego z trojanami.

Nie będzie zapewne zaskoczeniem, że ataki ransomware również zaznaczyły swoją obecność w sektorze opieki zdrowotnej. Szczególnie aktywny był Ryuk, bez wątpienia w związku z dużą aktywnością Emoteta. Sektor ten znalazł się na drugim miejscu pod względem ruchu związanego z ransomware.

**Sektor produkcji**

Podobnie jak w branży IT, aktywność w zakresie cryptominingu była również wysoka w sektorze produkcyjnym. Odnotowano mniej więcej połowę aktywności zaobserwowanej w sektorze technologicznym, ale co ciekawe, w produkcji było prawie trzy razy więcej punktów końcowych zaangażowanych w cryptomining. Krótko mówiąc, większa liczba maszyn skutkująca mniejszą aktywnością DNS prowadzi do wniosku, że te punkty końcowe miały mniejsze moce obliczeniowe w porównaniu do tych z sektora technologicznego. Możliwe, że zaatakowane maszyny były zaangażowane w sam proces produkcji, nawet związany z obszarem Internetu rzeczy. W takich przypadkach, cryptomining byłby prawdopodobnie wolniejszy, ale nadal mógłby wpływać na szybkość produkcji.

Okazuje się, że sektor produkcyjny jest również najbardziej narażony na ransomware. W branży tej odnotowano prawie tyle samo ataków związanych z ransomware, co w dwóch najbliższych branżach łącznie (technologie i ochrona zdrowia). Wydaje się to być wyraźnym sygnałem, że branża ta jest regularnie obierana za cel cyberprzestępców, prawdopodobnie ze względu na polowanie na dużych graczy i potencjalną zapłatę, jaką mogą otrzymać atakujący.

**Szkolnictwo wyższe**

Pandemia COVID-19 spowodowała zamknięcie kampusów na całym świecie, przejście na tryb zdalny i hybrydowy. Ponieważ zajęcia odbywały się online, wiele szkodliwych działań, które zostałyby zablokowane w uczelnianej infrastrukturze IT, pojawiło się w sieciach domowych studentów. Spowodowało to spadek aktywności cyberprzestępców w tym sektorze w wielu kategoriach począwszy od marca, a także znacznie niższe ogólne liczby w 2020 roku niż w latach poprzednich.

Nie oznacza to, że ich aktywność spadła gwałtownie, ponieważ niektóre działania wymagające dostępu do zasobów kampusu odnotowały swój udział w aktywności DNS. Na przykład, działania phishingowe zdołały uplasować szkolnictwo wyższe na drugim miejscu w zestawieniu branżowym. Firmy zajmujące się wydobywaniem kryptowalut również często celują w sektor szkolnictwa wyższego, próbując wyłudzić zasoby komputerowe lub okazyjny dostęp do przetwarzania w chmurze studentów, aby uruchomić swoje koparki.

**Administracja rządowa**

Spośród wszystkich analizowanych przez Cisco branż, sektor rządowy wydaje się być najbardziej równomiernie obłożony pod względem głównych kategorii ataków – phishingu, cryptominingu, ransomware i trojanów. W obszarze administracji publicznej, zaobserwowano także dość równomierny rozkład dla każdej z tych kategorii, patrząc z miesiąca na miesiąc.

Jedynym wyjątkiem od tego trendu był cryptomining, który odnotował niskie liczby w pierwszych trzech kwartałach roku, by w październiku skoczyć w górę, gdy wartości kryptowalut osiągnęły najwyższy poziom w 2020 roku i kontynuowały wzrost. Jednak liczby miesiąc do miesiąca nie ulegały wahaniom w ostatnim kwartale roku, pozostając w większości na tym samym wysokim poziomie w każdym miesiącu.

**Zapobieganie udanym atakom**

Nie ma wątpliwości, że analizowanie trendów w krajobrazie zagrożeń może przynieść korzyści. Wiedząc, gdzie pojawiają się ataki, łatwiej jest podjąć decyzję, gdzie należy alokować zasoby, aby się przed nimi bronić. Cryptomining i phishing są obecnie powszechnie spotykane, podobnie jak trojany takie jak Emotet i Trickbot, wykorzystywane do wdrażania oprogramowania ransomware, takiego jak Ryuk.

Oczywiście, różne sektory są narażone na różne zagrożenia w odmienny sposób, więc pomocne jest zrozumienie specyficznych trendów otaczających sektor, w którym działamy. Na przykład, ekspert z sektora usług finansowych powinien uważnie śledzić trendy związane z phishingiem, podczas gdy osoba odpowiedzialna za bezpieczeństwo w firmie produkcyjnej może chcieć przyjrzeć się bliżej oprogramowaniu ransomware.

 .:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) to światowy lider technologiczny zapewniający działanie Internetu od 1984 r. Pracownicy, partnerzy i produkty Cisco pomagają społeczeństwom łączyć się w bezpieczny sposób i już dziś korzystać z cyfrowych możliwości jutra. Dowiedz się więcej na www.newsroom.cisco.com. Cisco i logo Cisco to zastrzeżone znaki towarowe należące do Cisco i/lub jego podmiotów zależnych w U.S. i innych krajach. Pełna lista znaków towarowych Cisco dostępna jest pod adresem: www.cisco.com/go/trademarks. Znaki towarowe firm trzecich są ich własnością. Użycie słowa partner nie oznacza stosunku partnerstwa pomiędzy Cisco i inną firmą.