ŚWIĘTY MIKOŁAJ, ROZPOZNANIE MOWY, MENEDŻER SZPITALA I 200 MILIONÓW PUNKTÓW, CZYLI WNIOSKI Z MNIEJ ZNANYCH PRZYPADKÓW RANSOMWARE

30.10.2017

Schyłek października 2017 r. w branży cyberbezpieczeństwa był przepełniony doniesieniami o najnowszym ransomware Bad Rabbit, natomiast cały mijający rok z dużym prawdopodobieństwem będzie zapamiętany pod kątem pojawienia się dwóch głośnych kampanii – WannaCry i NotPetya. Nie będzie przesadą stwierdzenie, że kampanie te należały do największych w ostatnich latach. Stąd, działały na wyobraźnię nie tylko specjalistów bezpieczeństwa teleinformatycznego ale i obywateli, czyli przeciętnych użytkowników systemów teleinformatycznych. Międzynarodowy zasięg oddziaływania, konsekwencje ataków w świecie fizycznym oraz towarzysząca im warstwa socjotechniczna sprawiły, że media i opinia publiczna przez długi czas były zainteresowane nowym rodzajem złośliwego oprogramowania. O ile jednak sposób działania robaka, który szyfruje dane użytkownika żądając okupu od użytkownika w celu ich przywrócenia jest nowatorski dla laików, o tyle dla osób w branży jest znanym mechanizmem.

A zatem tak jak w większości przypadków, również i w odniesieniu do ransomware, głośne przykłady medialne jak WannaCry czy NotPetya stanowią tylko wierzchołek góry lodowej. Warto chociażby zwrócić uwagę na dane statystyczne. Zgodnie z raportem firmy Symantec „Internet Security Threats" w 2016 r. wykryto o 36 proc. więcej przypadków ataku typu ransomware niż w 2015. Tylko w ubiegłym roku znaleziono ponad 100 nowych „rodzin" złośliwego oprogramowania tego typu. Według Symanteca od 2014 r. łącznie pojawiło się ponad 650 tys. unikalnych egzemplarzy tego zagrożenia. Ubiegły rok był też przełomowy, jeśli chodzi o wysokość okupu, którego żądali cyberprzestępcy od swoich ofiar. Średnio wynosił on ok. 1000 USD. Z kolei badacze z Cybersecurity Ventures przewidują, że koszty wynikające z destrukcyjnej działalności ransomware w skali globalnej będą większe niż 5 mld USD. Istotna z punktu widzenia atakowanego urządzenia wydaje się również częstotliwość infekowania. Kaspersky Lab zbadał, że w 2016 r. ransomware atakował użytkowników i przedsiębiorstwa odpowiednio co 10 i 40 sekund. W tym samym raporcie znalazła się także informacja o tym, że co piąta ofiara oprogramowania nie otrzymała danych po zapłacie okupu.
Zważywszy zatem na rosnącą popularność i ewolucję ransomware, warto dokonać analizy mniej znanych, ale charakterystycznych przypadków, które mogą być jednocześnie dowodem na różnorodność zjawiska i nierzadko wynikają z nich osobne wnioski dla dobrych praktyk ochrony przed ransomware i bezpieczeństwa w ogóle. Poniżej przedstawione są te przypadki opierając się na kluczu kalendarzowym.

Marry X-Mass

Choć pojawił się na samym początku 2017 r. to jego warstwa socjotechniczna była inspirowana mijającymi świętami Bożego Narodzenia. W jednej ze swych odsłon ransomware rozprzestrzeniał się pod postacią zainfekowanych plików .doc, przesyłanych w wiadomości phishingowej spreparowanej jako zawiadomienie o stawieniu się na rozprawie sądowej. Przy włączonej opcji uruchamiania makr dokument Microsoft Word pobierał i uruchamiał na komputerze ofiary plik .hta informujący o zaszyfrowaniu wszystkich plików na komputerze. Warto zwrócić uwagę na fakt, że atakujący w tym przypadku nie informowali od razu o konkretnej sumie, którą należy zapłacić w Bitcoinach. Kwotę tę ofiary mogły otrzymać poprzez przesłanie wiadomości do przestępców. W drugim etapie tej kampanii, atakowane urządzenie mogło również zostać zainfekowane dodatkowym oprogramowaniem szpiegującym i zbierającym m.in. dane uwierzytelniające czy dane z kart kredytowych. W związku z dwutygodniowym opóźnieniem w stosunku do świąt katolickich, analitycy podejrzewają, że za kampanią stoją cyberprzestępcy obchodzący Boże Narodzenie zgodnie z kalendarzem świąt prawosławnych. Taki wniosek sugeruje również kontakt mailowy w popularnej rosyjskiej domenie „yandex.com" oraz możliwość kontaktu poprzez aplikację Telegram, szeroko wykorzystywaną w Rosji czy na Ukrainie. W marcu 2017 r. firma Check Point zaprezentowała narzędzie umożliwiające deszyfrację zainfekowanych plików.

> RANSOMWARE ATAKUJE WSZYSTKICH, ZARÓWNO UŻYTKOWNIKÓW INDYWIDUALNYCH, JAK I BIZNES CZY STRUKTURY ADMINISTRACJI PAŃSTWOWEJ

Android.Lockdroid.E

Lutową edycję ransomware'a Android.Lockdroid atakującego urządzenia mobilne oparte na popularnym systemie operacyjnym należy zaklasyfikować do innowacyjnych typów oprogramowania, chociażby ze względu na metodę pozwalającą odszyfrować pliki. Standardowo dla tego typu zagrożeń, zainfekowany telefon krok po kroku instruuje w jaki sposób ofiara powinna zdobyć hasło deszyfrujące. Domyślnie, w przypadku gdy zablokowane urządzenie nie pozwala na wykonanie żadnej akcji, użytkownik powinien zaczerpnąć tę informację z drugiego systemu. W teorii jednak wcale nie jest to wymagane, gdyż wystarczy, że użytkownik przypadkiem odgadnie hasło wypowiadając je do telefonu. Android.Lockdroid.E jest bowiem wyposażony w interfejs rozpoznania mowy i właśnie na ten sposób uwierzytelniania postawili cyberprzestępcy projektując robaka. W następstwie wypowiedzenia prawidłowego hasła, ekran blokujący zostaje usunięty. Jak wynika z analizy Symantec, hasła te są krótkie i nieskomplikowane, a oprogramowanie dopasowuje wypowiadane słowa metodą heurystyczną. Wcześniejsza wersja Lockdroida wymagała od użytkownika zeskanowania kodu QR, gdzie znajdowała się instrukcja przywrócenia systemu.

Sanctions

W marcu 2017 r. światło dzienne ujrzała nowa wersja ransomware'a, której interfejs graficzny dawał jasno do zrozumienia, co cyberprzestepcy myślą o amerykańskich sankcjach nałożonych na Federację Rosyjską. Komunikat, oprócz satyrycznej grafiki zawiera odnośnik do „satoshibox.com", usługi hostingowej, umożliwiającej pobranie plików w zamian za przelew odpowiedniej sumy bitcoinów lub innej kryptowaluty. W przypadku Sanctions, cenę klucza deszyfrującego przestępcy ustanowili na poziomie 6 BTC (wcześniej były to 3 bitcoiny).

Rensenwere

Programistom złośliwego oprogramowania Rensenwere z całą pewnością bardziej zależało na trwałym zablokowaniu systemów niż uzyskaniu korzyści finansowych. Autorzy nie przyjęli jednak strategii polegającej na żądaniu wysokiej kwoty. Ofiara by odzyskać dane musiała osiągnąć wysoki wynik (0,2 mld punktów) na jednym z poziomów gry komputerowej „Undefined Fantastic Object". Ransomware szyfruje większość plików o popularnych rozszerzeniach, m.in. .mp3, .doc, .xls czy .rar nadając im rozszerzenie .rensenwere. Interesujący jest mechanizm w jaki sposób oprogramowanie sprawdza, czy gracz uzyskał żądany wynik. W trakcie gry Rensenwere odczytuje proces uruchomionej aplikacji i w momencie uzyskania wyniku rozpoczyna deszyfrację. Na szczęście doniesienia z Twittera wskazują na to, że pomysł z niestandardowym żądaniem był wyłącznie żartem autora. Niezależnie od tego faktu, studium przypadku pokazuje możliwości jakie daje ten rodzaj zagrożenia, gdzie ograniczeniem jest tylko wyobraźnia i kreatywność cyberprzestępcy. W serwisie YouTube można odnaleźć filmy prezentujące przebieg gry i osiągnięcie wyniku, który określił w swoim żarcie autor Rensenwere'a. Bardzo doświadczonej osobie zdobycie 0,2 mld punktów zajęło około 20 minut.

Reyptson

Odpowiednio w maju i czerwcu 2017 r. pojawiły się doniesienia o zagrożeniach WannaCry i NotPetya. Zdobyły one duży rozgłos i zostały szeroko opisane w mediach informacyjnych i branżowych. Jednakże już w połowie lipca dał o sobie znać inny interesujący przypadek ransomware'a – hiszpański Reyptson, który rozprzestrzenia się m.in. poprzez zainfekowane załączniki. Ciekawa jest metoda propagacji trojana, który po uruchomieniu w systemie operacyjnym odczytuje listę kontaktów klienta poczty Thunderbird i w imieniu właściciela poczty wysyła do adresatów spam z załączonym zagrożeniem pod przykrywką niezapłaconej faktury. Transakcja zapłaty okupu odbywałą się w sieci TOR, a cyberprzestępcy żądali kwoty od 200 do 500 EUR. Kampania była ukierunkowana na użytkowników systemów Windows.

Defray

Odkryta w sierpniu 2017 r. kolejna inkarnacja złośliwego oprogramowania Defray jest interesująca z tego względu, iż dowodzi skuteczności kampanii o niewielkiej skali ale precyzyjnie określonych celach. Defray w dwóch etapach ataku mierzył odpowiednio w sektor zdrowia i edukacji, a następnie w przemysł wytwórczy i nowych technologii. Atak był ograniczony do podmiotów prowadzących swoją działalność w Stanach Zjednoczonych i Wielkiej Brytanii, przy czym każda z kampanii liczyła zaledwie kilka precyzyjnie spreparowanych wiadomości pocztowych adresowanych do selektywnego grona odbiorców. Socjotechniczna warstwa kampanii była dobrze przemyślana i zaplanowana, o czym świadczy fakt, że wśród adresatów znaleźli się m.in. wymieni z imienia i nazwiska dyrektorzy

departamentów, a w przypadku sektora zdrowia, wiadomości phishingowe naśladowały raporty o pacjentach przesyłane przez „szpitalnego menedżera IT". Załącznikami w tych listach były zainfekowane dokumenty Microsoft Word. W tym przypadku przestępcy żądali wysokiej, jak na tego rodzaju atak, kwoty na poziomie 5 tys. USD w bitcoinach. Dopuszczali jednak możliwość negocjacji informując o tym w dokumencie tekstowym, który pojawiał się wraz z procesem zaszyfrowania plików.

SynAck

We wrześniu 2017 r. eksperci zaobserwowali wzmożoną aktywność wirusa SynAck. Podobnie jak w przypadku Defraya, warto zwrócić uwagę na wysoki okup, którego żądają przestępcy. Ofiary by odblokować swoje systemy muszą uiścić sumę 2,1 tys. USD liczoną w BTC. Zgodnie z informacjami opublikowanymi przez portal destroyadware.com wartość portfela przestępców pod koniec września ukształtowała się na poziomie ok. 420 tys. USD. Do infekcji SynAckiem mogło dojść poprzez skompromitowanie niezabezpieczonego protokołu RDP obsługującego usługę zdalnego pulpitu w większości systemów Windows. Atak jest prosty i odbywa się w oparciu o metodę bruteforce. W tym przypadku, wiadomość od atakujących nie pojawia się na ekranie ofiary od razu po procesie szyfrowania a można ją przeczytać z poziomu pulpitu w formie dokumentu tekstowego. Jak sprawę komentują analitycy i specjaliści bezpieczeństwa teleinformatycznego, SynAck być może działa na zasadzie komercyjnej usługi (ransomware as a service). Ocenia się, iż głównym celem przestępców były sieci i urządzenia korporacyjne.

Bad Rabbit

Eksperci bezpieczeństwa teleinformatycznego bili na alarm z powodu nowego wirusa, który w dość krótkim czasie zdążył sparaliżować niektóre podmioty sektora transportu i mediów, głównie w Rosji, na Ukrainie i w Bułgarii. Pierwsze doniesienia w dużym stopniu wskazywały na to, iż zagrożenie jest bardzo podobne do malware'a Petya/NotPetya, ale okazało się, że podobieństwo ogranicza się wyłącznie do metody szyfrowania plików. W sumie zaatakowanych zostało ponad 200 organizacji. Na celowniku przestępców znalazły się sieci korporacyjne, głośnymi ofiarami były metro w Kijowie, lotnisko w Odessie i rosyjska agencja prasowa Interfax. Aby ransomware zainfekował systemy komputerowe, ofiara musi pobrać złośliwe oprogramowanie poprzez fałszywą aktualizację popularnego programu Adobe Flash Player. Większość zarażonych źródeł obejmuje strony w domenie .ru (pełna lista dostępna pod linkiem: https://exchange.xforce.ibmcloud.com/collection/XFTAS-SI-2017-00001-Bad-Rabbit-51701e9c25aaaf7e02b19fa6d63ccc80). Przestępcy za odszyfrowanie plików oczekują okupu w wysokości 0,05 BTC, czyli obecnie mniej więcej 280 USD. W momencie publikacji niniejszego artykułu sprawa nieco ucichła, głównie z powodu opracowania tzw. kill switcha, który zapobiega uruchomieniu aplikacji na komputerze. Pozostaje jednak pytanie - czy „zły królik" jest operacją, za którą stoją cyberprzestępcy odpowiedzialni za kampanię NotPetya i czy jak wówczas motywem działania były względy finansowe czy też zamierzone działania destrukcyjne? Być może uda się rozwiać te wątpliwości, jeśli nastąpi kolejny etap ataku Bad Rabbita.

Z omówienia niektórych przypadków ransomware z ostatnich tygodni płynie kilka refleksji odnośnie ewolucji tego zjawiska. Warto zwrócić uwagę na kreatywność i przygotowanie cyberprzestępców, zarówno pod względem warstwy socjotechnicznej (celowane kampanie phishingowe, komunikaty wzbudzające uczucie niepokoju i presji), czy technicznej (szerokie spektrum wektorów ataku ukierunkowanych na różne rodzaje urządzeń, wykorzystywanie znanych podatności, sposoby szyfrowania plików). Z pewnością zjawisku sprzyja popularność

kryptowalut, które z jednej strony umacniają ich anonimowość, a z drugiej pozwalają na szybkie wzbogacenie się dzięki stale rosnącemu kursowi BTC. Ransomware atakuje wszystkich, zarówno użytkowników indywidualnych, jak i biznes czy struktury administracji państwowej. W wielu przypadkach nieznane są metody obrony przed tymi atakami, dopiero dłuższa analiza techniczna pozwala na wypracowanie takich mechanizmów, które i tak bywają zawodne. Bazując na doświadczeniu oraz mając świadomość w jaki sposób działa ransomware, można opracować kilka potencjalnych scenariuszy dużego paraliżu infrastruktury krytycznej, kampanii negatywnego oddziaływania psychologicznego na społeczeństwo czy zręcznie przygotowanego modelu biznesowego (jak w przypadku ransomware-as-a-service). Póki co najlepszą rekomendacją, obok stale zaktualizowanych zasobów, weryfikowania poczty przychodzącej czy silnych haseł dostępowych, jest posiadanie aktualnej kopii zapasowej.

Autor: Kamil Gapiński

Kierownik Projektu
Fundacja Bezpieczna Cyberprzestrzeń

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**