Cyberdefence 24

aut. Andrzej Kozłowski 27.11.2017

RANSOMWARE JAKO PRZYKRYWKA DO DESTRUKCJI SYSTEMÓW [WYWIAD]

O zmieniającym się krajobrazie zagrożeń, ostatnich kampaniach ransomware oraz bezpieczeństwie współczesnej infrastruktury Internetu mówi w wywiadzie dla Cyberdefence24.pl Raj Samani CTO w McAfee.

Dr Andrzej Kozłowski: Wygłosił Pan prelekcję na konferencji Secure 2017 zatytułowaną „Appetite for Destruction. Addressing emerging threats today". Jakie są dzisiaj nowe zagrożenia?

Raj Samani: Jedną z najważniejszych rzeczy, na którą chciałem zwrócić uwagę, jest fakt, że zagrożenia nie są problemem czysto technicznym. Niedawno walczyliśmy z ransomware BadRabbit. Początkowo atak dotknął systemy komputerowe w Rosji i na Ukrainie, teraz wiemy, że ofiarą padły również Polska czy Niemcy, a także USA. BadRabbit wpłynął na pracę lotniska i metra. Wcześniejszy ransomware WannaCry sparaliżował służbę zdrowia. Dlatego podkreślam, że tego, co robimy, nie można ograniczać tylko i wyłącznie do kwestii informatycznych, ponieważ efekt tych ataków jest bardzo realny. Gdy przykładowo 8 tysięcy osób nie może dostać się do lekarza albo ich wizyty zostają przesunięte, koszt, jaki ponosi społeczeństwo, jest ogromny.

Warto też spojrzeć na ten problem z perspektyw mikro. Jeżeli jakaś operacja lub wykonanie zadania przesunie się przez atak o 12 tygodni, to również będzie miało to spory wpływ na nasze życie zawodowe. Tak samo w domu – możemy wszystko skrupulatnie zaplanować, wynająć niańkę, kupić frak na imprezę, a przez kawałek kodu wszystko może ulec zmianie. Jeśli chcemy lepiej zrozumieć zagrożenie, to podstawą jest to, żebyśmy się skupili na tym, jaki ma ono potencjalny wpływ na społeczeństwo.

Często prasa prześciga się w nagłówkach, informując, który kraj był odpowiedzialny za jakiś atak. Mówiąc szczerze, to jest problem dla organów ścigania, dla rządu. My musimy się skupić na identyfikacji potencjalnych skutków ataku oraz na tym, w jaki sposób możemy je przezwyciężyć.

Wracając do ostatniej kampanii ransomware. Czy BadRabbit w jakikolwiek sposób jest

podobny do poprzedników: WannaCry i NotPetya?

Są pewne podobieństwa - BadRabbit i NotPetya żądają okupu. Z analizy, której dokonaliśmy, wynika jednak, że nie są one jednakowe. Wydaje się, że wstępną ścieżką infekcji była fałszywa aktualizacja komputerów oraz kradzież danych do logowania. Nie mogę jednak powiedzieć, że kod jest taki sam czy że program został napisany w taki sam sposób.

Ostatnio w przeciągu kilku miesięcy mieliśmy trzy duże kampanie ransomware. Dlaczego akurat teraz, a nie np. 5 lat temu?

To jest bardzo dobre pytanie. Krajobraz zagrożeń zmienia się i ewoluuje wraz z czasem. Użyłeś słowa ransomware, ale moim zdaniem nie mówimy już o ransomware. Definiujemy go jako próbę zarobienia pieniędzy poprzez przechowywanie danych jako tzw. zakładników. Czy tym był właśnie WannaCry? Podczas mojej prezentacji podałem przykłady, w których pieniądze nie były głównym celem. Jaki był cel NotPetya? Zniszczyć dane. To dowód na to, że żyjemy obecnie w świecie, w którym okup (ransom) nie jest motywatorem. Celem cyberprzestępców może być np. wpłynięcie na ceny ropy naftowej na świecie, chęć udowodnienia czegoś albo zniszczenie systemów komputerowych. Osiągają go, udając, że mamy do czynienia z ransomware. Nie trzeba daleko szukać – proszę spojrzeć na ostatni atak na bank na Tajwanie. Zaszyfrowano tam dane z użyciem ransomware w celu odwrócenia uwagi zespołu IT. W tym czasie hakerzy manipulowali systemami bankowymi, tak aby wykraść jak największą ilość pieniędzy. Oczywiście była to wieloetapowa i zaawansowana operacja, której jednym z elementów było wykorzystanie ransomware, ale głównym celem było zupełnie coś innego. To nowość, jeżeli mówimy o aktualnym krajobrazie zagrożeń.

Wracając do kampanii BadRabbit. W przypadku NotPetya mechanizm płacenia był mało skomplikowany i łatwy do zablokowania.

Podobnie było z WannaCry. W tym przypadku trzeba było ręcznie skontaktować się z żądającymi okupu. Nie było żadnego mechanizmu automatyzacji. Podobnie sytuacja wyglądała w przypadku NotPetya. Wciąż pracujemy nad stwierdzeniem, jak jest z BadRabbitem. Mamy informację od naszego zespołu, że część osób zapłaciła okup, ale nie wiemy, czy otrzymali oni dane z powrotem. Jest jednak zbyt wcześnie, żeby jednoznacznie ocenić tę kwestię.

W przypadku WannaCry minęły miesiące, zanim dowiedzieliśmy się, czy ktoś zapłacił okup na palcach jednej ręki możemy też policzyć udokumentowane przykłady odszyfrowania danych. Co zatem było rzeczywistym celem atakujących? Naszym zdaniem nie chodziło o okup. Wierzymy, że ani WannaCry, ani NotPetya nie były ransomware'ami.

Większość ataków z ostatnich 20 lat była motywowana chęcią zysku. Jeżeli obecnie nie chodzi o pieniądze, to o co?

Ataki wciąż mogą być motywowane chęcią zdobycia pieniędzy. Pamiętajmy też, że za jednym atakiem może stać kilka osób, a każda z nich może mieć inny cel. Jednej może zależeć np. na destabilizacji jakiegoś systemu, a drugiej, która dostarcza infrastrukturę do przeprowadzenia ataku, na zysku. Były szef Europejskiego Centrum Cyberbezpieczeństwa (*European Cybercrime Center)* powiedział, *że*

dzisiaj cyberprzestępcy chcący dokonać konkretnych ataków nie muszą posiadać żadnej wiedzy technicznej, wystarczy im karta kredytowa, którą zapłacą komuś, kto odpowiada za techniczną stronę przedsięwzięcia. Dodał też, że aktualnie istnieje ponad 100 organizacji cyberprzestępczych. Jego zdaniem posiadają więcej i bardziej zaawansowanych zdolności ofensywnych niż większość państw. To jest naprawdę szokujące stwierdzenie.

Ciężko jest często również jednoznacznie stwierdzić, czy mamy do czynienia z haktywistami, czy z cyberprzestępcami. Mogą przecież pracować wspólnie. Ponadto jest wiele osób do wynajęcia, które mogą pracować dla grup przestępczych albo dla państw w celu zdestabilizowania sytuacji w innym kraju.

Czyli możemy wyobrazić sobie sytuację, że państwo/państwa stoją za tymi kampaniami ransomware?

Nie wiem. Słyszałem różnego rodzaju spekulacje.

Spekuluje się, że grupa Lazarus miała stać za WannaCry, a Rosja za kampanią NotPetya.

Ja i mój zespół nie zajmujemy się atrybucją ataków. Współpracujemy z Eurpolem czy Narodową Agencją ds. Przestępczości (*National Crime Agency*). Kiedy wykonujemy naszą pracę, analizując główną kampanię, dzielimy się naszą techniczną wiedzą z instytucjami odpowiedzialnym za egzekwowanie prawa i szeroko rozumianym sektorem publicznym. Dlaczego? No przecież nigdy nie prowadzisz dochodzenia sam, szukając złodzieja, który obrabował Twój dom. Tak samo jest w przypadku ścigania cyberprzestępców, dlatego ściśle współpracujemy i koordynujemy nasze działania z organami śledczymi. Wspieramy ich pracę oraz pomagamy przy śledztwach. Staramy się zrozumieć złośliwe oprogramowanie, jego kod itp., wszystkie inne rzeczy związane przykładowo z międzynarodowymi nakazami aresztowania są zadaniem policji.

Ostatnio dotarły do nas informacje o słabościach w podstawowych elementach architektury Internetu, jak np. bezpieczeństwo sieci WiFi czy osłabienia kluczy RSA. Wydaje się, że architektura nie jest bezpieczna.

W naszym biznesie nigdy nie możemy mówić o całkowitym bezpieczeństwie. Często posługuję się anegdotką, która brzmi, że na każde pytanie w tej branży odpowiedź brzmi: może. Czy jestem bezpieczny? Może. Czy zostanę zhakowany? Może. Czy będziemy świadkiem narodzin botnetu złożonego z drukarek 3D? Może. Tworzymy systemy, które są skomplikowane i interoperacyjne. Windows XP miał około 44 milionów linii kodu. Mówimy tu o systemie, który powstał około 20 lat temu. Nawet nie chcę zgadywać, ile linijek kodu ma Windows 10. Taka jest natura świata, w którym żyjemy. Mamy systemy z bardzo dużą liczbą opcji, więc zawsze pojawi się jakaś podatność. Dlatego lepiej

zamiast mówić, że Internet jest niezabezpieczony, powinniśmy zmienić podejście i zaakceptować fakt, że podatności istnieją. O części z nich wiemy, inne wciąż są dla nas nieodkryte, ale wiedzą o nich inne osoby, są też takie, o których nie wie nadal nikt.

Według mnie kluczowe jest, aby przestać straszyć wszystkich ludzi na kuli ziemskiej skutkami zagrożeń, zamiast tego powinniśmy zadbać o skuteczną politykę informacyjną – zamiast upubliczniać informację o podatności, lepiej zacząć od poinformowania producenta oprogramowania. Chodzi o to, abyśmy zagrożenia potraktowali nie jako powód do zrobienia szumu medialnego, ale jako punkt wyjścia do zbudowania bezpiecznego i świadomego społeczeństwa. To bardzo istotne, biorąc pod uwagę fakt, że za kilka lat każdy z nas może wraz z rodziną jeździć autonomicznym samochodem uzależnionym całkowicie od technologii.

Mówiąc o jednym z problemów dla współczesnego cyberbezpieczeństwa nie możemy zapomnieć o Internecie rzeczy. Co należy zrobić w tym obszarze?

Musimy odejść od założenia, że informowanie o podatnościach jest czymś złym. Wręcz przeciwnie, rozsądna polityka ujawniania luk jest fantastycznym narzędziem wzmacniania cyberbezpieczeństwa.

Powinniśmy zawrzeć porozumienie z każdą fabryką, która chce, żebyśmy kontrolowali i informowali ją o znalezionych podatnościach w ich produktach. Tworzenie atmosfery strachu i niepewności nic nie da – musimy walczyć o bezpieczne społeczeństwo. Chodzi przecież o to, żebyśmy nie musieli się obawiać o swoje bezpieczeństwo, na przykład wioząc dzieci samochodem do szkoły. To w naszym interesie jest, żeby wszystkie urządzenia, które trzymamy w rękach i z których korzystamy, przechodziły przez najważniejsze testy bezpieczeństwa.