ROBERT ŻELAZO DLA CYBERDEFENCE24.PL: POŚPIECH JEST JEDNĄ Z GŁÓWNYCH PRZYCZYN, DLA KTÓRYCH LUDZIE POPEŁNIAJĄ BŁĘDY

O roli firmy FireEye na światowym rynku cyberbezpieczeństwa, przyszłości atrybucji ataków w cyberprzestrzeni – mówi w wywiadzie dla CyberDefence24 Robert Żelazo, dyrektor regionalny FireEye.

Cyberdefence24: Czym zajmuję się FireEye?

Robert Żelazo: FireEye jest obecne na rynku bezpieczeństwa informatycznego od kilkunastu lat. Byliśmy pierwszą firmą, która adresowała zagadnienia ataków typu zero-day. Problem z tymi atakami jest taki, że nikt on nich nie wiedział wcześniej, nie posiadają odpowiednich sygnatur (nazwa zero-day pochodzi od ilości dni, jakie pozostają na ich załatanie, dokładnie zero – przyp. red.). Zagadnieniem, którym oprócz tego zajmujemy się jako FireEye, są też ataki Advanced Persistent Threats (APT) oraz advanced malware, wszystko to analizujemy i blokujemy bez używania sygnatur.

Na naszych systemach analizujemy kopię całego ruchu sieciowego, przechodzącego przez sieć naszego klienta i uruchamiamy na urządzeniach FireEye zawarte w ruchu sieciowym ataki. Są to zwykle pliki wykonywalne, czasami pliki PDF, dokumenty programów biurowych. Przy takim ataku monitorujemy kilka wektorów sieciowych: Web, e-mail, ale również ruch mobilny. Oferujemy też usługi odpowiadające na zagrożenie (incident response). Jednak ostatnio korzystamy także z możliwości jakie daję nam przejęta przez FireEye, firma iSight Partners. Pracownicy firmy iSight, korzystając ze swojej wiedzy, umiejętności oraz odpowiednich narzędzi, zdobywają w sieciach hakerów informacje na temat planowanych przez nich ataków. Jedyne co się zmieniło, po przejęciu to skupienie się na firmach korzystających z rozwiązań FireEye. Dzięki temu nasi klienci, wiedzą wcześniej, że atak na ich infrastrukturę jest planowany, w dodatku klient FireEye wie, za pomocą jakich narzędzi zostanie zaatakowany i kiedy można się ataku spodziewać.

Cyberdefence24: Aaron Cherrington podczas swojego wystąpienia na panelu, opisał całą sytuację jeżeli chodzi o udział rosyjskich hakerów w ostatnich słynnych atakach. Czy Polski oddział współpracował w ramach odkrywania kolejnych informacji na temat tych ataków?

R. Ż.: Firma FireEye, działa jako jedna firma w skali globalnej i nie ma podziału na osobne jednostki krajowe. W firmie pracuje wielu reasercherów, którzy prowadzą swoje działania rozsiani niemal po całym świecie. Mamy osoby pracujące w Rosji, Chinach czy na Ukrainie. Ich zadaniem jest zbieranie informacji o lokalnych atakach, zebrane informacje analizują, na bazie takich analiz powstają raporty Mandianta – opisujący szczegółowo cyberataki dokonane przez jednostki wojskowe chińskich hakerów (opis jednego z raportów pojawił się na łamach Cyberdefence24 – przyp. red.).

Przykładem tych dokumentów są takie raporty jak ten dotyczący APT1 (Mandiant), skupiał się głównie na atakach z Chin. Inne raporty poświęciliśmy także na hakerów z Rosji, chodzi o te dotyczące APT28

czy APT29. Przyznam, że Rosjanie są dość aktywni jeżeli chodzi o działania w cyberprzestrzeni. Posiadamy jeden z oddziałów w Rosji, który obsługuje klientów na tamtym terenie. Oni podobnie jak niemal wszyscy na świecie sami padają często ofiarą rosyjskich hakerów. To nie jest tak czarno-biało, że Rosjanie są źli i są tylko źli i atakują w sieci wszystkich, tylko nie swoje firmy.

Ataki w głównej mierze obecnie są napędzane przez chęć zysku, już parę lat temu dochody z cyberprzestępczości przekroczyły te wynikające z handlu narkotykami. Jak widać, jest to ogromna skala. Unia Europejska dodała ataki cybernetyczne do listy zagrożeń, obok takich elementów jak klęski żywiołowe. Nie tylko Rosjanie atakują w sieci, jednak nie zmienia to faktu, że istotnie w Rosji obecnie zauważmy wzmożoną aktywność hakerów.

Jedna z grup, którą się zajmowaliśmy w swoich badaniach, APT29, ewidentnie działa w strefie czasowej Sankt Petersburga i Moskwy, ich aktywność jest niemal zerowa podczas rosyjskich świąt narodowych. Moim zdaniem, musieli by być naprawdę bardzo wyrachowani, aby swoją aktywność ukrywać podczas takich świąt czy w nocy.

Co ciekawe, w ostatnim czasie przeprowadzaliśmy testy w jednym z komercyjnych banków w Moskwie. Trwały one niecały miesiąc i na gorącym uczynku złapaliśmy rosyjskiego hakera, który próbował wykraść dane i pieniądze z tego banku. Później okazało się, że to nie pierwsze jego włamanie. Kilka miesięcy wcześniej z tego samego banku wykradziono około 7 mln dolarów.

Po tym zdarzeniu rozpoczęliśmy dochodzenie w sprawie tego włamania, udało nam się zdobyć skan paszportu tego człowieka, okazało się, że jest to Rosjanin ukrywający się w Odessie (południowa Ukraina – przyp. red.) i jest on obecnie poza zasięgiem rosyjskich organów ścigania.

Cyberdefence24: Wspomniał pan o raporcie Mandiant i atrybucji. Jakich technik używa FireEye, przypisując atak do danej grupy?

R. Ż.: Po pierwsze analizujemy kod ataków, które badamy. Jednocześnie sprawdzamy strefy czasowe, patrzymy kiedy aktywność hakerów jest największa. Oprócz tego staramy się sprawdzić, co było motywem ataku hakerów na sieci czy komputery. Dzięki współpracy z iSight Partners, naszych ponad 200 agentów rozsianych po świecie, udając hakerów, wykrada informacje z forów hakerskich. Chodzi m.in. o informacje na temat planowanych ataków, nasi agenci wiedzą, którzy ludzie odpowiedzialni są za ataki, w jakim języku się porozumiewają.

Moim zdaniem działalność iSight Partners jest unikalna na światową skalę. Jest to pierwsza znana mi firma, działająca na rynku bezpieczeństwa informatycznego, która aktywnie wykrada informacje z forów i sieci hakerskich. Fora te nie tylko znajdują się w znanym wszystkim dark webie. Znane są przypadki komunikacji hakerów na forum My Little Pony czy forum Pingu.

Cyberdefence24: Wspomniał pan o ponad 200 agentach, którzy monitorują tego typu fora. Czy każdy z tych agentów działa w regionie, w którym się znajduję i w ramach języka, którym się posługuję?

R. Ż.: Nasi pracownicy są to ludzie rozsiani po całym świecie, ci agenci nie mają biur, pracują po prostu w domach. Nie publikujemy żadnych danych na ich temat, szczególnie danych osobowych. Dla przykładu, jeden z pracowników w Chinach nie monitoruje rynku chińskiego, tylko to co dzieje się dookoła. Z kolei agent w Singapurze jest skupiony na rynku chińskim.

Cyberdefence24: Brzmi to trochę jak prywatna agencja wywiadowcza w cyberprzestrzeni.

R. Ż.: Tak, to faktycznie tak trochę wygląda. Proszę jednak wziąć pod uwagę jakie z tym wiążą się korzyści dla klientów firmy FireEye. Jeżeli korzystają oni z pełnego pakietu zabezpieczeń, który chroni

ich przed atakami hakerów, czy atakami typu zero-day, dla których nie ma sygnatur. Teraz dla takiego klienta nieocenioną korzyścią jest, móc się w pełni przygotować, ustawić odpowiednie priorytety przed samym atakiem.

Jeżeli byłbym klientem firmy używającej naszych rozwiązań, która dowiaduję się dzięki iSight Partners, że grupa rosyjska APT29, będzie w najbliższym ataku wykorzystywać takie podatności systemu Windows, to jestem w stanie odpowiednio przygotować się na atak. Odpowiednio wcześnie załatać lukę w systemie.

Ale nawet w przypadku ataku, który skończy się sukcesem dla hakerów, firma iSight Partners jest w stanie poinformować klientów, o tym, że na czarnym rynku pojawiły się np. numery kart kredytowych firmy.

Cyberdefence24: Czy gdyby wiedzieli Państwo wcześniej o powiedzmy takich atakach, jakie ostatnio miały miejsce w Stanach. To czy poinformowalibyście państwo stronę rządową o takim zdarzeniu?

R. Ż.: Nie mogę podać tutaj żadnych nazw organizacji rządowych. Nasz poprzedni szef firmy, David DeWalt jest wieloletnim doradcą prezydenta Baracka Obamy w sprawach cyberbezpieczeństwa. Tak więc jesteśmy w bliskiej współpracy z administracją. Również w Polsce jesteśmy zaangażowani we współpracę z administracją i organizacjami państwowymi. Oczywiście, nasz klient, który jest na celowniku hakerów, jest informowany o tym fakcie natychmiast jak uzyskamy potwierdzenie tej informacji. Później działamy jedynie z lokalnymi CERT-ami.

Cyberdefence24: Jak to miejsce w przypadku, kiedy to nie jest państwa klient?

R. Ż.: Jeżeli nie jest to nasz klient, to pierwszą rzeczą jaką robimy, po uzyskaniu informacji o planowanym ataku jest przekazanie tej wiedzy lokalnemu CERT-owi.

Cyberdefence24: Czy zdarzały się takie przypadki, w których firma poinformowana o ataku zdecydowała się na wybór Państwa rozwiązań?

R. Ż.: Mamy w Polsce kilka takich przypadków, gdzie wykryliśmy planowane ataki na firmy. I faktycznie był to takim elementem, który przekonał firmę do zostania naszym klientem. Oczywiście zdarzają się takie przypadki, gdzie firmy ignorują takie znalezione przez nas informacje. Potem jedynie mogą mieć pretensje do samych siebie.

Cyberdefence24: Czy uważa Pan, że przez działalność Pana firmy będziemy mogli coraz częściej przewidywać ataki w cyberprzestrzeni? Nie mówię może o wszystkich, ale może chociaż te w najważniejszych instytucjach.

R. Ż.: To jest cel do którego dążymy. Chcemy, żeby było bezpieczniej. Jednocześnie, pragniemy aby tych ataków było coraz mniej i mogli je przewidywać.

Jednak nie oszukujmy się, nie ma 100 proc. zabezpieczenia, nigdy nie będzie tak, że będziemy zawsze bezpieczni. Nawet jeżeli użyjemy wszystkich najlepszych zabezpieczeń jakie na świecie są. 4 lata temu, kiedy zaczynaliśmy naszą przygodę na rynku polskim, docieraliśmy do klientów, którzy mieli najlepsze wtedy zabezpieczenia na rynku. Mieli najlepsze zapory sieciowe, IPSy, antywirusy, Web Gatewaye, E-mail Gatewaye. Przychodziliśmy do tych klientów, z naszymi urządzeniami, mówiliśmy im istotnie, że ich zabezpieczenia są w tej dziedzinie jednymi z najlepszych. Prosiliśmy wtedy o szansę, o możliwość przeanalizowania czystego ruchu, przefiltrowanego przez wszystkie zabezpieczenia. Robiliśmy to w ramach testów Proof of Value. Takie darmowe testy trwają około miesiąca. Przez 4 lata obecności na rynku przeprowadziliśmy takich testów ponad 100 i w prawie

każdym przypadku, wykryliśmy złośliwe oprogramowanie, które istniało w sieci klienta.

Nawet najlepsze zabezpieczenia sygnaturowe nie pozwolą uniknąć ataków typu zero-day. Ponieważ na nie nie ma sygnatur, tak samo jeżeli chodzi o ataki, które są odporne na metody heurystyczne. FireEye jest taką ostatnią linią ochrony, swoistą wisienką na torcie.

Oczywiście nie było nam łatwo przekonać klientów do tego, żeby dali nam szansę. Ci którzy jednak skorzystali z naszych usług, znacznie wzmocnili w ten sposób bezpieczeństwo swoich systemów.

Cyberdefence24: Ciągle mówimy o znaczeniu edukacji dla zapewnienia cyberbezpieczeństwa. Czy nie ma sposobu na rozprawienie się tym z problemem?

R. Ż.: Myślę, że ciągle największą bolączką każdego systemu jest człowiek. W tym miejscu nic się nie zmieniło. Edukacja oczywiście jest kluczowa. Natomiast, musimy spojrzeć na profil typowego użytkownika, pracownika firmy. Nie mówię tu o osobach starszych, które jednak są często na bakier z technologią, czy dzieciach, które potrafią być naiwne i popełniać błędy.

Chodzi o typowego pracownika korporacji. To jest człowiek, który ma dużo zadań, nie jest wstanie po prostu nadążyć i wszystko zweryfikować. Podejmuje decyzje w szybkim tempie, inaczej się po prostu nie da. Jeżeli działamy szybko, bez chwili zatrzymania, to zdarzy nam się kliknąć na załącznik w poczcie elektronicznej, czy otworzymy fakturę przesłaną na nasz adres e-mail. Potem okazuje się, że faktura była jednak zarażona złośliwym kodem i jest za późno na jakiekolwiek działania.

Komputer został zainfekowany, raczej nie uda się go odzyskać bez reinstalacji systemu, co jest bardzo bolesne.

Myślę, że pośpiech jest jedną z głównych przyczyn, dla których ludzie popełniają błędy. Jednak tego nie jesteśmy wstanie zmienić. Dlatego musimy edukować pracowników, użytkowników. Ale oprócz tego musimy stosować takie rozwiązania, aby nie wszystko zależało od ich błędnych decyzji.

Czytaj też: Android - zagrożenie, którego nie widać