Cyberdefence 24

aut. Szymon Palczewski 09.12.2020

„SŁODKA ZEMSTA" ROSYJSKIEGO FSB NA AMERYKANACH? ZHAKOWANO GIGANTA CYBERBEZPIECZEŃSTWA

Hakerzy powiązani z państwem przeprowadzili skuteczny cyberatak na amerykańskiego giganta cyberbezpieczeństwa „FireEye". W wyniku incydentu skradziono specjalistyczne narzędzia hakerskie znajdujące się w arsenale koncernu. W dochodzenie zaangażowano FBI oraz liderów branży technologicznej, w tym Microsoft. Ślady operacji wskazują na celowe działanie hakerów rosyjskiego wywiadu FSB. Cyberatak to „słodka zemsta" Kremla?

FireEye, jedna z największych firm specjalizujących się w cybebezpieczeństwie, poinformowała, że padła ofiarą cyberataku, który został przeprowadzony przez grupę hakerów powiązanych z państwem. Na taki stan rzeczy wskazuje wysoka dyscyplina, bezpieczeństwo operacyjne oraz wykorzystanie zaawansowanych technik podczas operacji. Szczegóły na temat incydentu przedstawił CEO FireEye – Kevin Mandia.

Dyrektor generalny firmy jednoznacznie stwierdził, że „jesteśmy świadkami ataku ze strony państwa o najwyższych zdolnościach ofensywnych". Operacja przeprowadzona przez wrogich hakerów różniła się od dziesiątków tysięcy incydentów, którymi zajmowało się FireEye przez lata. Cechą charakterystyczną kampanii był wysoki poziom zaawansowania, co przełożyło się na jej skuteczność.

> *Hakerzy dostosowali swoje światowej klasy zdolności specjalnie do namierzania i atakowania FireEye. Są dobrze wyszkoleni w zakresie bezpieczeństwa operacyjnego i wykonują działania z dyscypliną oraz skupieniem*
>
> *Kevin Mandia, CEO FireEye*

Hakerzy działali potajemnie, używając metod, które skutecznie „obchodzą" narzędzia bezpieczeństwa oraz inne specjalistyczne rozwiązania. Ponadto, podczas operacji zastosowali nowatorską kombinację technik, których nigdy wcześniej ani specjaliści FireEye ani partnerzy firmy nie widzieli.

Kevin Mandia wskazał, że obecnie prowadzone jest dochodzenie w tej sprawie. W cały proces zostało zaangażowane FBI oraz giganci branży technologicznej, w tym Microsoft. Co warto podkreślić, wstępne ustalenia zewnętrznych podmiotów potwierdzają, że był to cyberatak przeprowadzony przez wysoce zaawansowaną grupę powiązaną z państwem, która wykorzystała nowatorskie technik.

Zaawansowane cyberszpiegostwo i przejęcie narzędzi

Analiza incydentu wykazała, że celem operacji były konkretne narzędzia Red Team (wewnętrzna komórka FireEye), używane do testowania zabezpieczeń klientów firmy (np. poprzez symulowanie cyberataków). W wyniku przeprowadzonych działań hakerom udało się uzyskać do nich dostęp.

> *Nie jesteśmy pewni, czy atakujący zamierza użyć naszych narzędzi Red Team, czy też publicznie je ujawnić. Niemniej jednak, zachowując szczególną ostrożność, opracowaliśmy ponad 300 środków zaradczych (...) w celu zminimalizowania potencjalnego ryzyka związanego z kradzieżą naszych narzędzi*
>
> *Kevin Mandia, CEO FireEye*

Obecnie nie znaleziono żadnych dowodów na to, jakoby hakerzy użyli skradzionych narzędzi. Specjaliści zapewniają, że nadal będą monitorować i śledzić działania wrogich podmiotów, aby zapewnić bezpieczeństwo w cyberprzestrzeni.

Posiadanie cudzej "cyberbroni" to ogromna zaleta dla wrogiego podmiotu, ponieważ w ten sposób może on przeprowadzać operacje hakerskie, pozostawiając swoje narzędzia w arsenale. Dzięki temu nawet po ujawnieniu incydentu, specjaliści oraz służby staną przed wyzwaniem zlokalizowania źródła, które posługiwało się nie swoimi narzędziami. To znacząco utrudnia dochodzenie, a czasami wręcz prowadzi do nierozwiązania sprawy.

Kradzież narzędzi zespołu FireEye to jednak nie jedyny aspekt kampanii. Hakerzy w ramach operacji poszukiwali przede wszystkim informacji dotyczących klientów rządowych firmy. Pomimo, że uzyskali oni dostęp do wewnętrznych systemów, na obecnym etapie dochodzenia nie znaleziono dowodów, które wskazywałyby, że wykradli z nich dane. „Jeśli odkryjemy, że pobrano dane klientów, skontaktujemy się z nimi bezpośrednio” – zadeklarował CEO FireEye Kevin Mandia.

> With the Fireeye breach news coming out, it's important to remember that no one is immune to this. Many security companies have been successfully compromised over the years, including Symantec, Trend, Kaspersky, RSA and Bit9 1/
>
> — Dmitri Alperovitch (@DAlperovitch) December 8, 2020

Cyberatak na amerykańskiego giganta cyberbezpieczeństwa nie jest zaskoczeniem, ponieważ firmy tego typu z reguły są przedmiotem zainteresowania hakerów. Wynika to z faktu, że są to podmioty posiadające specjalistyczne narzędzia, w tym często imitujące lub wręcz zaliczane do kategorii cyberbroni, oraz umożliwiające dostęp do konkretnych urządzeń ich klientów („po nitce do kłębka”).

Jednak zdaniem Amerykanów cyberatak i kradzież narzędzi FireEye to największa tego typu wroga operacja, jaka miała miejsce od słynnej już obecnie kampanii wymierzonej w Agencję Bezpieczeństwa Narodowego (ang. National Security Agency – NSA). Adam Schiff, przewodniczący Komisji Wywiadu Izby Reprezentantów, wskazał w specjalnym oświadczeniu dotyczącym sprawy FireEye, że od 2016

roku amerykańska infrastruktura krytyczna regularnie jest przedmiotem operacji prowadzonych przez przeciwników.

Ślady prowadzą do…

FireEye poinformowało, że cyberatak został przeprowadzony przez państwo, lecz nie podało konkretnego źródła incydentu. Warto jednak zwrócić uwagę, że przedstawiony opis operacji oraz fakt, że funkcjonariusze FBI przekazali sprawę wewnętrznej komórce specjalizującej się rosyjskich operacjach wskazuje, iż głównym podejrzanym jest Moskwa – informuje o śledztwie New York Times.

We wtorek FBI oficjalnie potwierdziło, że kampania została przeprowadzona przez aktora państwowego, lecz nie wskazało na konkretny kraj, który miał być odpowiedzialny za incydent.

> *FBI bada incydent, a wstępne wskazówki wskazują na aktora o wysokim poziomie wyrafinowania, powiązanym z państwem narodowym*
>
> *Matt Gorham, zastępca dyrektora FBI Cyber Division*

O śladach prowadzących do Rosji donosi także Joseph Marks, dziennikarz The Washington Post zajmujący się cyberbezpieczeństwe. Jak podkreślił, wszystko wskazuje na to, że cyberatak na FireEye został przeprowadzony przez hakerów Kremla. Taką informacją podzielił się amerykański urzędnik zaznajomiony ze sprawą, który ze względów bezpieczeństwa pragnie pozostać anonimowym.

> New to this story: The FireEye hack appears to be linked to Russia, according to a U.S. official familiar with the matter, who spoke on condition of anonymity to discuss a sensitive matter. https://t.co/d3HmTYFqQy
>
> — Joseph Marks (@Joseph_Marks_) December 8, 2020

New York Times sugeruje, że rosyjscy hakerzy wykorzystali skupienie amerykańskich służb i firmy FireEye na zabezpieczeniu wyborów prezydenckich i kontroli sytuacji po ich zakończeniu. To miało pozwolić Moskwie na przeprowadzenie skutecznego ataku i pozyskaniu zaawansowanych narzędzi hakerskich oraz danych na temat klientów rządowych poszkodowanej firmy.

Czy cyberatak to odwet Kremla za liczne oskarżenia stawiane przez FireEye pod adresem GRU, FSB, SVR i innych jednostek? Firma wielokrotnie ujawniała operacje prowadzone przez rosyjskich hakerów, w tym na przykład kampanię wymierzoną w ukraiński sektor energetyczny w 2015 roku.

Ellen Nakashima, reporterka The Washington Post, poinformowała, powołując się na swoich informatorów, że kampanię przeprowadzili hakerzy rosyjskiego FSB, którzy znani są w środowisku pod nazwą APT29 lub Cozy Bear. Jest to ta sama grupa, która włamała się na serwery Demokratów w 2015 roku, a także do systemów Białego Domu, Pentagonu oraz próbowała ukraść badania nad szczepionką przeciwko COVID-19.

> Sources tell the WaPo that the Russian SVR intelligence service --APT 29 -- appears to be behind the hack of FireEye. That's the same group that hacked Democratic servers in 2015. But the investigation continues. @Joseph_Marks_ https://t.co/bhg8gBaUNN
>
> — Ellen Nakashima (@nakashimae) December 8, 2020

W ostatnim czasie infrastruktura Stanów Zjednoczonych musi zmagać się ze wzmożoną aktywnością ze strony rosyjskich hakerów. Dotyczy to nie tylko cyberataków wymierzonych w sektor medyczny, w tym przede wszystkim ośrodki zajmujące się koronawirusem, ale także podmioty z sektora obronnego.

Na początku grudnia br. NSA wydała ostrzeżenie, w którym opisała kampanię prowadzoną przez hakerów sponsorowanych przez Rosję. Zagrożenie jest realne i trwa nadal, dlatego Agencja zarekomendowała wprowadzenie szczególnych środków ostrożności przez podmioty powiązane z Pentagonem.

Podczas operacji wrogi podmiot wykorzystuje lukę w produktach firmy VMware (firma tworząca oprogramowanie do wirtualizacji), aby uzyskać dostęp do chronionych danych z sektora obronnego USA.

Komunikat NSA został skierowany przede wszystkim do administratorów Departamentu Obrony Stanów Zjednoczonych, Narodowego Systemu Bezpieczeństwa (National Security System – NSS) oraz bazy przemysłu obronnego (Defense Industrial Base – DIB), ponieważ – jak wskazuje Agencja – to właśnie ich dotyczy „problem”.

Skąd wynika nasilenie rosyjskiej aktywności w sieci, której celem są amerykańskie podmioty? Na to pytanie trudno jest znaleźć jednoznaczną odpowiedź. Możliwe, że jest to próba wykorzystania skupienia służb USA oraz firm zajmujących się bezpieczeństwem na ochronie wyborów oraz kontrolowaniu sytuacji po ich zakończeniu. To także okres „przejściowy” między zakończeniem prezydentury Donalda Trumpa oraz objęciem władzy przez Joe Bidena, co stwarza zamieszanie i chaos, który Rosja może próbować wykorzystać na rzecz realizacji własnych zadań.

Niemniej jednak odkryte w ostatnim czasie incydenty z udziałem hakerów Kremla pokazują, że Moskwa obrała na cel podmioty, które mają duże znaczenie z perspektywy interesów Stanów Zjednoczonych. Czy wskazane wydarzenia doprowadzą do zaognienia wzajemnych relacji między Rosją a USA? Odpowiedź wydaje się być twierdząca.

Czytaj też: Cybernajemnicy w globalnej operacji. Ślady wskazują na… GRU?