Komentarz KBN

Nr 1 (73) / 2021 12 stycznia 2021 r.

Znaczenie cyberataku na SolarWinds

Błażej Sajduk

O powadze ataku na SolarWinds świadczą co najmniej dwa fakty. Po pierwsze, kroki jakie podjęła amerykańska administracja federalna, w tym zwłaszcza wdrożenie dyrektywy prezydenckiej nr 41 ((PPD)-41). Skutkiem tego było powołanie przez Radę Bezpieczeństwa Narodowego, na polecenie Donalda Trumpa, The Cyber Unified Coordination Group (UCG), organu unifikującego działania śledcze administracji (Federalnego Biura Śledczego, FBI; Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury, CISA oraz Biura Dyrektora Wywiadu Narodowego, ODNI). Ponadto wydana 13 grudnia 2020 roku przez CISA, zaraz po wykryciu ataku, dyrektywa nr 21-01 nakazuje natychmiastowe wyłączenie urządzeń wykorzystujących oprogramowanie Orion, w których wykryto złośliwe oprogramowanie.

Aby lepiej zrozumieć sytuację związaną z atakiem na SolarWinds należy na wstępie przywołać w kolejności chronologicznej kilka cyberincydentów z nieodległej przeszłości. Rosja jest już od dłuższego czasu oskarżana przez Waszyngton o wrogie działania w cyberprzestrzeni. W 2016 roku najprawdopodobniej to rosyjskim służbom udało się zinfiltrować serwery pocztowe polityków Partii Demokratycznej i przekazać zdobyte informacje serwisowi WikiLeaks. Wykradzionymi informacjami były m.in. treści wewnątrzpartyjnej korespondencji. Eksperci zgodnie ocenili ten atak jako próbę ingerencji w amerykański proces wyborczy ze strony zewnętrznego podmiotu (najprawdopodobniej grup APT 29 – Cosy Bear i APT – Fancy Bear, działających w ramach Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, GRU).

Przeprowadzenie ataków wykorzystujących łańcuchy dostaw wymaga zaangażowania dużych zasobów ludzkich i materialnych, są też niezwykle trudne do wykrycia. Do tej pory nie były częstym zjawiskiem (choć tą metodą w 2017 roku zaatakowana została aplikacja CCleaner oraz w 2019 roku ASUS), jednak wiele wskazuje, że ten sposób ataku będzie coraz częściej wybierany przez crackerów wspieranych przez aparat państwowy. Ponadto mechanizm ataku na SolarWinds przypomina ten wykorzystywany w ataku NotPetya z 2017 roku – wektorem ataku także była aktualizacja oprogramowania, w tamtym przypadku księgowego MEDoc, w której znajdował się złośliwy kod infekujący komputery. NotPetya był atakiem wymierzonym głównie w Ukrainę. Efektem zainfekowania było zaszyfrowanie danych na przejętym komputerze oraz żądanie okupu za ich odszyfrowanie. Analiza kodu źródłowego pokazała jednak, że rzeczywistym celem działania złośliwego programu było nie tyle wyłudzenie okupu, co permanentne zablokowanie zainfekowanych maszyn. Amerykańska administracja atak ten przypisała rosyjskiemu GRU.

W odpowiedzi na przywołaną powyżej, domniemaną rosyjską kampanię dezinformacyjną podczas wyborów prezydenckich w USA w 2016 roku, US Cyber Command w 2018 roku przeprowadziło działania odwetowe wymierzone w rosyjską Agencję Badań Internetowych (ABI), potocznie określaną mianem fabryki rosyjskich trolli. Wielu ekspertów potwierdza, iż atak miał miejsce i doprowadził przez kilka dni w okresie śródwyborów do poważnych problemów w funkcjonowaniu ABI (sformatowanie twardych dysków poprzez przejęcie kontroli nad sterownikami RAID). W lipcu 2020 roku Donald Trump publicznie przypisał sobie podjęcie decyzji o tym ataku. Tak więc atak na SolarWinds mógł stanowić kolejną odsłonę amerykańsko-rosyjskiej rywalizacji w cyberprzestrzeni.

Czym jest SolarWinds oraz oprogramowanie Orion

Ponad 300 tysięcy podmiotów jest klientami firmy SolarWinds. Trzonem jej działalności biznesowej jest dostarczanie narzędzi służących do szeroko pojmowanego zarządzania sieciami informatycznymi (Network Management System, NMS), w tym tworzenia kopii zapasowych systemu. Sztandarowym produktem jest rodzina programów Orion. Oprogramowanie służące do zarządzania sieciami jest doskonałym celem ataku, ponieważ monitoruje wszystkie podłączone do sieci urządzenia i, w zależności od konfiguracji, często ma przyznane uprawnienia na poziomie administratora do dokonywania modyfikacji zarówno ustawień sieci, jak i parametrów jej funkcjonowania. Tym samym atakujący, któremu uda się przejąć kontrolę nad oprogramowaniem zarządzającym siecią uzyskuje te same uprawnienia. Oprogramowanie Orion jest wykorzystywane przez największe amerykańskie przedsiębiorstwa (425 na 500 z listy Fortune US), a w skali świata przez ponad 30 tysięcy podmiotów z czego 18 tysięcy pobrało aktualizację zawierającą złośliwe oprogramowanie.

Możliwy przebieg ataku

8 grudnia 2020 roku prywatna firma zajmująca się cyberbezpieczeństwem FireEye poinformowała o wykradzeniu firmowych narzędzi służących do testowania sieci klientów za pomocą kontrolowanych cyberataków. Żadne z tych narzędzi nie korzystało z zero-day exploitów. Odkryciu temu towarzyszyło wykrycie znacznie poważniejszego naruszenia bezpieczeństwa w narzę-

dziach Orion. Opinia publiczna została o tym fakcie poinformowana 13 grudnia przy okazji ujawnienia ataku na Departamenty Skarbu oraz Handlu. Atak został przeprowadzony za pomocą strategii naruszania integralności łańcucha dostaw za pomocą backdoora nazwanego przez FireEye SUNBURST (przez Microsoft Solorigate). Ze względu na dużą ilość nowatorskich rozwiązań zastosowanych podczas ataku, specjaliści z firmy FireEye nazywają ten atak UNC2452 (nie wiążąc go automatycznie z którąkolwiek rosyjską grupą crackerską, tym samym pozostawiając otwartym kwestię przypisania tego ataku konkretnemu państwu).

Szkodliwe oprogramowanie było umieszczane od marca do czerwca 2020 roku w autoryzowanej przez producenta i certyfikowanej (podpisanej) przez Symantec bibliotece (SolarWinds.Orion.Core.BusinessLayer.dll), która stanowiła element aktualizacji środowiska programu Orion. Złośliwe oprogramowanie zainfekowało co najmniej 18 tysięcy użytkowników. Celem ataku padły również serwery chmurowe Microsoft wykorzystywane przez pakiet Office 365, co najprawdopodobniej umożliwiło wejście do systemów innych podmiotów, a następnie wykorzystanie złośliwego oprogramowania zamieszczonego w kodzie aktualizacji przesyłanej przez SolarWinds. Microsoft przyznał również, że atakujący uzyskali dostęp do kodu źródłowego jego oprogramowania, firma zapewnia jednak, że projektuje swoje narzędzia kierując się zasadą bezpieczeństwa jako priorytetu (*security by design*) domniemając, iż crackerzy również mogą dysponować dostępem do kodu źródłowego.

Docelowo SUNBURST umożliwiał nieautoryzowane połączenie z zewnętrznym serwerem http, jednak absolutnym priorytetem atakujących było pozostanie w ukryciu, a nie możliwie szybki transfer danych z zainfekowanych sieci. Po wgraniu do systemu użytkownika złośliwe oprogramowanie pozostawało w ukryciu przez 12-14 dni, co zabezpieczało je przed mechanizmami wykrywania stosowanymi przez programy antywirusowe. Następnie złośliwe oprogramowanie podejmowało próby nawiązania kontaktu z serwerami strony trzeciej (C2), z którego otrzymywało polecenia dotyczące m.in. kopiowania plików. Szczególnego podkreślenia wymaga fakt zarządzania działaniami złośliwego oprogramowania już po zainfekowaniu systemów ofiar, np. po uzyskaniu dostępu do sieci ofiary wykorzystane backdoory były usuwane. Co więcej, atakujący używali lub emulowali adres IP pochodzący z państwa ofiary ataku. Wszystkie te aktywności odbywały się pod ukryciem, przez co dla użytkowników były widoczne jako działania mające na celu usprawnienie funkcjonowania programu Orion, mieszając się z procesami faktycznie przewidzianymi przez producenta – firmę SolarWinds. Ponadto kroki wiodące do nawiązania kontaktu z siecią wykonywane były przez SUNBURST sekwencyjnie, następowały po restarcie macierzystego procesu lub całego systemu. Dodatkowej pikanterii całej sprawie dodaje fakt, iż SolarWinds zalecał swoim klientom wyłączenie oprogramowania antywirusowego w celu niezakłóconej pracy Oriona. Wszystko to dodatkowo utrudniło wykrycie włamania przez system antywirusowy Einstein wykorzystywany przez US CERT.

Prawdopodobne jest, że atak ten był częścią bardziej rozbudowanej kampanii cybernetycznej, która najprawdopodobniej składała się z fazy infiltracji dostawcy rozwiązań dla SolarWinds, opracowania szkodliwego oprogramowania oraz fazy obejmującej działania już po przejęciu kontroli, w której backdoor był wykorzystywany do pozyskiwania informacji.

Długotrwały proces przygotowywania całego przedsięwzięcia sugeruje fakt, iż domenę główną, z którą komunikowało się złośliwe oprogramowanie utworzono już w lipcu 2018 roku (modyfikując w znaczący sposób pod koniec 2019 roku). Należy też podkreślić, iż co najmniej 30% zainfekowanych podmiotów nie zostało zaatakowanych, co wskazywać może na dużą dyscyplinę atakujących oraz bardzo świadomy cel całej operacji cybernetycznej. Innymi słowy, w przeciwieństwie do klasycznych ataków, celem nie było zmaksymalizowanie okupu poprzez infekowanie możliwie dużej ilości urządzeń, co stanowi poszlakę pozwalającą uznać, że cała akcja była centralnie dowodzona i koordynowana.

Microsoftowi (i innym podmiotom współpracującym w celu przeciwdziałania skutkom ataku, w tym FireEye i GoDaddy) bardzo szybko (już 15 grudnia 2020 r.) udało się przejąć (w toku tzw. sinkholingu) główną domenę (avsvmcloud[.]com), z którą SUNBURST próbował nawiązać kontakt. Tym samym udało się również odciąć komunikację szkodliwego oprogramowania z siecią sterującą (C2). To nie pierwszy raz, gdy Microsoft (po uzyskaniu zgody sądu) przejmuje domeny odpowiedzialne za kierowanie botnetami. Podobne przypadki nastąpiły w trakcie zwalczania ataków Necurs i TrickBot w 2020 roku. Choć nie ma pewności, że to odetnie całkowicie kontrolę atakujących od zainfekowanych sieci, na pewno poważnie utrudni im dalsze działanie.

Znaczenie ataku

Ponieważ atak nastąpił z poziomu producenta samego źródła oprogramowania, o pełnej skali działań crackerów opinia publiczna przekona się w większym zakresie dopiero za jakiś czas. Wciąż nie jest jasne, jak głęboko atakującym udało się przeniknąć do sieci użytkowników oprogramowania Orion i czy uzyskali możliwość sprawowania pełnej kontroli poziomu administratora sieci, w tym uprawnień do edytowania zawartości informacji przesyłanej w sieciach. Uwagę zwraca fakt, iż atakującym udało się pozyskać certyfikaty poświadczające autentyczność aktualizacji przesyłanej z serwerów SolarWinds. Wskazuje to na fakt, iż crackerzy najmując się jako podwykonawcy mogli mieć dostęp do kodu źródłowego na poziomie deweloperskim, co umożliwiło im uniknięcie wykrycia podczas skanowania oprogramowania przez producenta, zanim zostanie ono udostępnione klientom.

Interpretacja prawna tego, czym był atak SUNBURST i jakie można wyciągnąć konsekwencje wobec jego sprawców nie jest jednoznaczna. Z jednej strony skala ataku przewyższa dotychczasowe działania cyberszpiegowskie, z drugiej strony celem ataku nie było zniszczenie infrastruktury krytycznej, a w jego wyniku nie ucierpiał żaden człowiek. Innymi słowy, jego skala i efekty nie są porównywalne z atakiem kinetycznym, tym samym zdają się nie wypełniać znamion zasady nr 69 sformułowanej w „Podręczniku tallińskim 2.0". Tym niemniej sposób ataku każe postawić pytanie, czy trwałe podważenie zaufania do własnych sieci nie ociera się o cyberatak. Już teraz pojawiają się głosy ekspertów, iż dla przywrócenia zaufania niezbędne jest odtworzenie systemów od podstaw. W tym kontekście otwarte pozostaje pytanie, czy atak SUNBURST, choć bezpośrednio nie wyrządził szkody infrastrukturze krytycznej (jak w przypadku Stuxnet), pośrednio spowoduje konieczność wymiany znacznej części infrastruktury informatycznej.

Choć celem ataku było zdobycie informacji na temat rządowych klientów SolarWinds, to jego znaczenie wynika nie tyle z jego technicznej złożoności, ale z faktu, iż będzie on miał skutki na-

tury psychologicznej. Podkopał bowiem amerykańskie zaufanie do własnych instytucji na co najmniej dwóch poziomach. Po pierwsze, pojawiły się wątpliwości co do skuteczności działań amerykańskich agencji federalnych odpowiedzialnych za cyberbezpieczeństwo. Nie były one w stanie uchronić państwa przed tak poważnym zagrożeniem i gdyby nie atak na prywatną firmę Fire Eye, aktywność crackerów wciąż pozostawałaby w ukryciu. Po drugie, podkopane zostało zaufanie do bezpieczeństwa własnych sieci, co jest największym strategicznym sukcesem atakujących. Nie ma bowiem gwarancji, że wykorzystywane aktualnie oprogramowanie będzie zdolne do wykrycia szkodliwego kodu, który wciąż może z powodzeniem kamuflować swoją obecność, „oślepiając" dotychczasowe zabezpieczenia.

Atak SUNBURST wymusi na nowej administracji USA doprecyzowanie oraz rewizję dotychczasowych zasad postępowania USA w cyberprzestrzeni, w tym ustalenie granicy, po przekroczeniu której nastąpi odpowiedź oraz jej formy. Ponadto USA stanie przed wyzwaniem efektywnej praktycznej realizacji założeń wysuniętej obrony, tzn. aktywnego ograniczania możliwości cybernetycznych wrogich podmiotów.