Найбільш нищівна кібератака в історії США

Ніколи такого не було, і от знову: росіяни проникли у комп'ютерні мережі уряду США.

Відомий виробник рішень у галузі кібербезпеки ***FireEye*** 13 грудня оголосив про викриття глобальної кампанії комп'ютерного шпигунства. Поширення зловмисного коду відбувалось через популярного постачальника програмного забезпечення, з чим українці добре знайомі після NotPetya. У даному разі хакери використовували програму Orion від компанії ***SolarWinds*** — виробника ПЗ для моніторингу роботи мереж і баз даних, віддаленого адміністрування тощо.

Як пише The Guardian, клієнтами SolarWinds є сотні тисяч організацій по всьому світу, у тому числі зі списку Fortune 500, а також урядові організації з Північної Америки, Європи, Азії і Близького Сходу. Повідомлялося, що до клієнтів SolarWinds входять 10 найбільших американських телеком-операторів. За даними самої SolarWinds, програмне оновлення, що уможливлює доступ хакерів, могли встановити до 18 тис. її клієнтів, тож справа дійсно серйозна.

Десятки постраждалих

Встановлено, що атака почалась у березні-травні (саме тоді було додано зловмисний код у оновлення Orion). Хакери отримали можливість віддаленого доступу до мереж жертв, завдяки чому могли красти звідти інформацію, відстежувати електронну пошту та інші канали внутрішніх комунікацій. Сама FireEye також зазнала атаки. Власне, ще 9 грудня компанія повідомила про злам своїх серверів і викрадення інструментів,

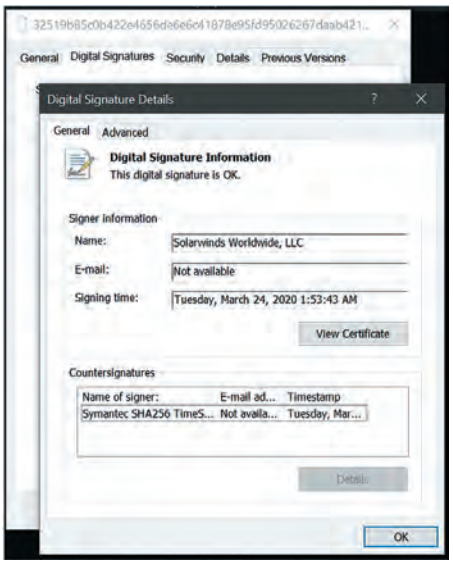

Рис. Цифровий підпис SolarWinds на троянізованому програмному компоненті (джерело: FireEye)

які вона використовувала у тестах на проникнення. Розслідування того інциденту і привело до виявлення кампанії шпигування.

Злочинці перетворили на троян один з компонентів Orion, який міститься у стандартному файлі завантаження, теж троянізованому, з підробленим підписом (**рис.**). Як ідеться у блозі компанії, після встановлення ця зловмисна програма (якій FireEye дала назву SUNBURST) вичікує два тижні і потім намагається налагодити зв'язок з доменом управління. Далі вона може виконувати команди, які забезпечують передавання і запуск файлів, збирання даних про оточення і вимкнення системних служб. Троян маскує свій трафік під справжній протокол SolarWinds — Orion Improvement Program (OIP), а результати розвідки ховає у файлах конфігурації. Також троян має засоби уникнення антивірусів та інструментів розслідування інцидентів.

Згодом американська агенція з кібербезпеки й захисту інфраструктури (CISA) повідомила, що група, яка стояла за даною кібератакою, використовувала не лише вектор проникнення через SolarWinds. Наразі агенція розслідує інциденти, де використовувались схожі тактики, техніки і процедури.

Що саме шукали хакери, достеменно не відомо, проте експерти вважають, що це могли бути якісь секрети ядерної галузі, документація щодо передової зброї, результати досліджень, що стосуються вакцин від COVID-19, та досьє на лідерів країни і керівників промислових гігантів.

Наразі відомо, що злочинці «хакнули» принаймні шість федеральних відомств США, у тому числі департаменти з питань енергетики і торгівлі, а також державне казначейство і сам Держдеп. Повідомлялося, що було зламано мережу Національної адміністрації з питань ядерної безпеки, яка відповідає, зокрема, за збереження американського ядерного арсеналу. Підозрілу активність виявлено в мережах Федеральної комісії з регулювання енергетики, лабораторій Сандія і Лос-Аламос, інших стратегічних установ і об'єктів.

За даними ***Microsoft***, постраждали загалом десятки технологічних компаній і фірм, що працюють у галузі безпеки, а також неурядових організацій. Хоча більшість атак припали на США, жертви були також виявлені в Канаді, Мексиці, Бельгії, Іспанії, Великобританії, Ізраїлі та ОАЕ, і очікується, що цей перелік лише зростатиме. Атака є «винятковою за своїми обширом, складністю і ударом», — зазначає Microsoft.

«Злам був такий масштабний, що навіть наші фахівці з кібербезпеки погано уявляють собі обсяг і глибину самого вторгнення», — так, за повідомленням The Guardian, сказав сенатор Стівен Лінч, глава комітету з нагляду і реформ Палати представників Конгресу США після закритого засідання, присвяченого цьому питанню. Агенція Associated Press наводить слова ще одного американського чиновника, який на умовах анонімності назвав атаку вкрай нищівною. «Схоже, це найгірша хакерська атака в історії Америки, — сказав чиновник. — Вони проникли усюди».

Про найбільш руйнівне і масштабне вторгнення у американські військові і розвідувальні системи говорив і сенатор-демократ Кріс Кунс, порівнявши кібератаку з нападом, який можна «класифікувати як оголошення війни». SolarWinds у своїй заяві, яку наводить Washington Post, теж вказала, що її продукти були перетворені на зброю у ході «складної і спрямованої... атаки, за якою стояла іноземна держава».

Що ж це за держава? За твердженням Washington Post, атаку вчинили російські хакери з групи APT29, відомої також як Cozy Bear, яка є частиною Служби зовнішньої розвідки РФ. 18 грудня про російський слід

публічно заявив держсекретар США Майк Помпео, який сказав, що це видно «дуже чітко», проте ще раніше про подібне говорили американські фахівці з кіберзебпеки і різні офіційні особи. Як повідомляє AP, конгресмени-демократи після ознайомлення з закритим звітом також підтвердили, що це зробили росіяни.

М'яч на полі Америки

Проте Дональд Трамп наступного дня після заяви Помпео написав у Твіттері, що «фейкові медіа» роздули кібератаку до розмірів, набагато більших, ніж насправді. «Мене повністю увели в курс справи, і все під контролем. «Росія, Росія, Росія», — ось про що всі починають торочити, тільки-но щось стається», — написав Трамп, додавши, що за атакою міг стояти і Китай.

Associated Press з посиланням на джерело в уряді США повідомила, що чиновники Білого дому готували заяву, в якій Росія прямо називалася «головним діячем», що сто яв за кібератаками, проте в останній момент дістали наказ відставити це (як тут не згадати інцидент у Керченській протоці 2018 року, після якого Держдеп також готував жорстку антиросійську заяву, але її заблокував тодішній радник Трампа з питань безпеки Джон Болтон; так пише сам Болтон у своїй книжці «Кімната, де це відбувалося»).

З іншого боку, Reuters повідомляє з посиланням на власні джерела, що команда новообраного президента Байдена розглядає варіанти покарання Росії — від санкцій до власних кібератак на російську інфраструктуру. Відповідь має бути достатньо потужною, щоб завдати винним великих економічних, фінансових або технологічних збитків, проте такою, щоб уникнути ескалації конфлікту між двома ядерними державами. У будь-якому разі головною метою цієї відповіді має стати ефективне стримування і зменшення потенціалу для майбутніх російських кібератак. Сам Байден в інтерв'ю CBS пообіцяв, що винних буде притягнуто до відповідальності, згадавши про «фінансові наслідки» як для індивідуальних осіб, так і для організацій.

Тут можна пригадати звіт сенатського комітету з розвідки, у якому йшлося, що у 2016 році адміністрація Барака Обами виявилася не готовою до російського втручання у вибори і не змогла сформулювати адекватної відповіді. Тоді американський уряд виявився паралізованим і скутим обмеженнями — як реальними, так і уявними, — і лише обговорював можливі кроки, не зважуючись на жодний. У грудні того року, вже програвши вибори, Обама наказав вислати з країни 35 російських дипломатів і закрити два консульства, а також ухвалив символічні фінансові санкції. Ще було здійснено обмежену кібероперацію у відповідь: у важливі російські комп'ютерні системи були імплантовані «закладки», спроектовані таким чином, щоб їх знайшли. Їхнім призначенням було нагадати Москві про можливості США.

Проте, за даними Washington Post, Обама також таємно дав дозвіл на закладання в російську критичну інфраструктуру справжньої кіберзброї — цифрових «бомб», які можна було б «підірвати» дистанційно у разі нової кібератаки з Москви. Але Обама вже залишав свою посаду, а проект все ще перебував на стадії планування, тож невідомо, якою була його доля за президентства Трампа. З іншого боку, посилаючись на власні джерела, Washington Post зазначала, що операція не потребувала подальшого схвалення з боку Трампа, хоча він міг її зупинити іншим розпорядженням. Станом на середину 2017 року він цього не зробив (звісно, якщо не вважати це все просто ще одним натяком Кремлю, зробленим через медіа).

Чи є в розпорядженні Байдена «зброя помсти», ми не знаємо. Але цим разом уряд демократів явно панькатися не збирається, тож буде цікаво.

Між тим на подолання наслідків атаки можуть знадобитися місяці, попереджає AP. Навіть у такій країні, як США, просто бракує досвідчених фахівців, щоб виявити усі урядові і приватні системи, куди проникли хакери. І якщо останні дійсно працюють на російську СЗР, то чинитимуть впертий опір екзорцизму. «Єдиний спосіб впевнитися, що мережа чиста, — це спалити її дощенту і відбудувати заново», — наводить Associated Press думку експерта з кібербезпеки з Гарвардського університету Брюса Шнаєра.

А поки що коаліція компаній перебрала домен, який хакери використовували як центр управління, і передала його у володіння Microsoft. Завдяки цьому оператори SUNBURST не зможуть завантажувати додаткові хакерські програми у ті мережі, які ще не оновили ПЗ Orion після викриття кібератаки. Понад те, стало відомо, що FireEye переконфігурувала домен таким чином, щоб він діяв як «вимикач», за певних обставин зупиняючи дію зловмисного ПЗ.

Василь ТКАЧЕНКО, СиБ