УДК 007:351.778.542

Я.В. Невойт

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПЕРІОД 2015-2016 РОКІВ

В статті проведено аналіз сучасних загроз інформаційної безпеки в період 2015-2016 років. Наведено статистику інцидентів інформаційної безпеки за сферами компаній та розглянуто основні атаки, що зазвичай використовуються зловмисниками. Сформовані тренди комп'ютерних атак, що спостерігалися в останні роки. Сформовані ключові елементи інформаційної безпеки сучасного підприємства.

Ключові слова: інформаційна безпека, атака, соціальна інженерія, інциденти.

Вступ

Ми часто чуємо в новинах про те, що постійно трапляються якісь інциденти інформаційної безпеки. І хоча здається, ніби інциденти трапляються десь далеко, вони цілком можуть торкнутися кожного. У 2017 році нас чекає на 30% більше інцидентів з інформаційної безпеки у фінансовій сфері і більш переконливі сценарії соціальної інженерії.

Немає жодної сфери суспільної діяльності, яка не була б цікава хакерам. На одні компанії нападають в пошуках конфіденційної інформації, на інші - з метою наживи, а хтось і зовсім стає випадковою жертвою масової атаки. Досвід роботи з моніторингу та реагування на інциденти дозволяє простежити певні тренди і зробити висновки про те, які галузі атакують найбільш часто і як це відбувається. Знання про переваги зловмисників при реалізації атак допоможуть бути напоготові і вчасно вжити превентивних заходів щодо захисту інформаційної інфраструктури, уникнувши неприємних наслідків або хоча б знизивши можливі збитки.

Основна частина

Отже, перш за все, порівняємо компанії, постраждалі від комп'ютерних атак в 2016 і 2015 роках (рис.1.).

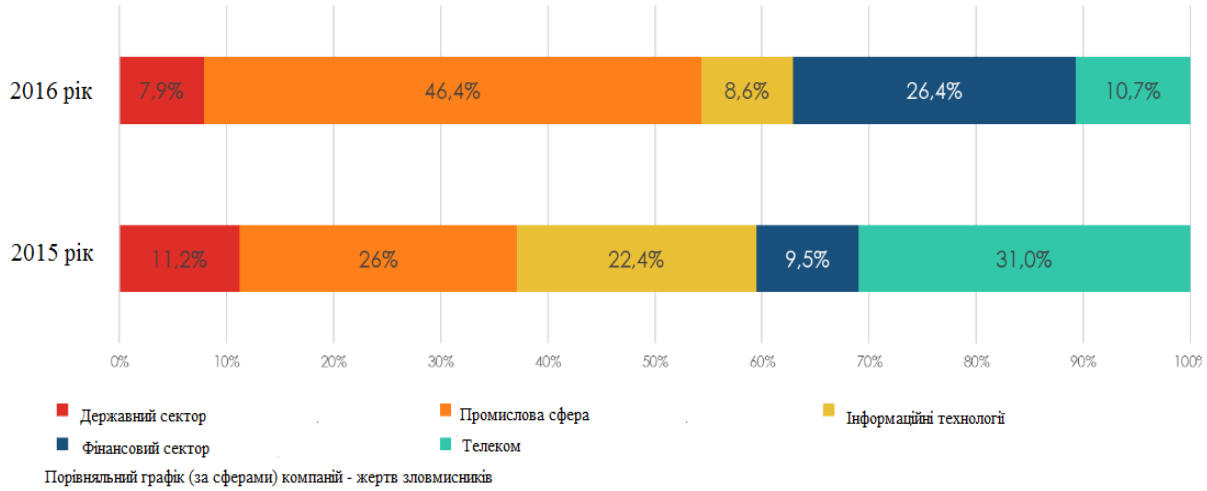

Рис.1 Статистика інцидентів інформаційної безпеки за сферами компаній

В 2016 році зафіксовано майже в три рази більше промислових компаній, що зіткнулися з інцидентами інформаційної безпеки, ніж було за рік до цього. Причому комп'ютерні атаки на промислові об'єкти склали близько 37% від загального числа розслідуваних інцидентів за останні два роки.

Зловмисники атакували об'єкти критичної інфраструктури цілеспрямовано, причому атаки відрізнялися ретельністю підготовки. Вони використовували передові технології та складні шкідливі програми, а інструменти розроблялися з урахуванням специфіки конкретної цільової системи. Такі атаки вимагають значних фінансових і тимчасових витрат.

© Я.В. Невойт, 2017

Цільові атаки на об'єкти критичної інфраструктури можуть призводити до серйозних наслідків і навіть потенційно до людських жертв, але найбільш частим наслідком є витік конфіденційної інформації.

Один з таких інцидентів стався в грудні 2015 року та призвів до компрометації ключових активів інфраструктури однієї великої промислової компанії. Тобто зловмисникам стала доступна конфіденційна інформація, що зберігалася та оброблялася в компанії. В ході розслідування з'ясувалося, що шпигунство було реалізовано шляхом довгострокової присутності в скомпрометованої системі різних шпигунських програм (Enfal, PlugX), які належать кільком групам, що спеціалізуються на реалізації цілеспрямованих атак на інфраструктури по всьому світу.

В 2016 році зазначено новий сплеск комп'ютерних атак, спрямованих на організації фінансової сфери. Такі інциденти зайняли більше 26% від загального числа інцидентів, розслідуваних у 2016 році. Більш того, в 2017 році прогнозується 30-відсоткове зростання числа повідомлень про інциденти в банках, процесингових компаніях, брокерських компаніях, компаніях, що займаються грошовими переказами, і фінтехстартапах. Основною причиною є те, що з погіршенням економічної ситуації в фінансовому секторі багато фінансових організацій проводять оптимізацію витрат і скорочують вкладення в забезпечення інформаційної безпеки.

Якщо при атаках на промислові організації зловмисникам, як правило, потрібна була цінна інформація, то атаки на компанії фінансової сфери - банки і біржі - відбувалися з метою наживи.

При цьому в гонитві за максимальною вигодою злочинці почали замість клієнтських рахунків атакувати самі банки.

Навесні 2016 року фахівці розслідувався інцидент, який, незважаючи на швидке реагування, встиг завдати значної шкоди одному українському банку. Атака була реалізована з використанням шкідливого Green Dispenser, встановленого на банкомати. Ця троянська програма дозволяла по команді здійснювати видачу готівки з диспенсера. Примітно те, що для захисту від випадкового запуску у шкідливій програмі використовувалася двухфакторна аутентифікація з двома пін-кодами - статичним і динамічним (унікальним для кожного запуску).

Зловмисник підходив до банкомату з попередньо завантаженим шкідливим програмним забезпеченням, вводив статичний пін-код, після чого на екрані банкомату з'являвся QR-код (рис.2). За допомогою мобільного додатка злочинець сканував QR-код, отримував другий (динамічний) пін-код, що відкриває доступ до диспенсеру готівки, забирав гроші і йшов.

Рис.2. QR-код, який використовується кібершахраями

У жовтні 2016 року було зафіксовано діяльність угруповання Cobalt, про існування якої стало відомо зовсім недавно. В результаті інциденту за одну ніч з декількох банкоматів одного з банків Східної Європи була вкрадена сума, еквівалентна 2 213 056 грн в місцевій валюті.

На підготовчі роботи зловмисники витратили два місяці: за цей час за допомогою поштових розсилок, що містять шкідливе програмне забезпечення, вони скомпрометували

© Я.В. Невойт, 2017

внутрішню мережу банку, отримали доступ до комп'ютерів співробітників, відповідальних за роботу банкоматів, віддалено завантажили шкідливі програми на банкомати і отримали можливість управління ними. Дії цього угруповання відрізняло використання легітимної комерційної програми Cobalt Strike, призначеної для автоматизації робіт з тестування на проникнення. Крім того, зловмисники застосовували утиліти для роботи з обліковими даними і програмне забезпечення для віддаленого управління комп'ютерами, які будь-хто може завантажити з сайтів виробників. Щоб не привертати уваги до своїх дій, для завантаження на сервери і робочі станції необхідних утиліт злочинці використовували легітимні ресурси, обрані на основі результатів пошуку в поширених пошукових системах (зокрема, github.com), а для завантаження шкідливих програм - популярний файлообмінник. Для віддаленого підключення та управління банкоматами використовувалася RAdmin - програма, яку активно використовували адміністратори цього банку, а тому її запуск не викликав підозр у відділу безпеки.

Для безпосереднього отримання готівки зловмисники використовували підставних осіб, так званих дропів (money mules), яких знаходили по оголошеннях в інтернеті. Підставна особа в призначений час (переважно вночі) підходила до банкомату і забирала гроші, які видавав банкомат з віддаленої команди зловмисника.

Практично в половині (45%) випадків при реалізації атак зловмисники використовували шкідливі програми. При цьому в 27% всіх атак мало місце впливу на користувачів методами соціальної інженерії.

Слабким місцем в системі захисту будь-якої організації, як і раніше залишається недостатня поінформованість співробітників в питаннях інформаційної безпеки. Зловмисникам це відомо, і тому вони активно використовують соціальну інженерію як при реалізації масових атак, так і в якості початкового етапу цільової атаки. Серед відмінностей цільових атак від масових можна виділити дії атакуючого в разі невдачі: якщо масові атаки в разі відсутності реакції з боку жертви припиняються, то цільові тривають, але вже з використанням інших методів або векторів.

Рис.3. Розподіл типів атак, які застосовуються зловмисниками

© Я.В. Невойт, 2017

Восени 2016 року було проведено аналіз скомпрометованих вузлів великої промислової компанії. В ході розслідування з'ясувалося, що компрометація сталася в результаті запуску шкідливого коду, отриманого співробітниками компанії з масових спам-розсилок.

В останні два роки в основному фахівці стикалися з використанням соціальної інженерії при цільових атаках на організації різних галузей. Засобом для впровадження в цільову систему програмного забезпечення, необхідного для подальшого розвитку атаки, як правило, виявлялася електронна пошта. Зловмисники імітували листи від партнерів, з якими жертви регулярно взаємодіяли в рамках роботи. І це не викликало підозр, так як відправнику повністю довіряли. Такі атаки можливі лише після ретельної підготовки і вивчення внутрішніх процесів компаній, а також після атак на партнерські організації.

Наприклад, навесні 2016 року розслідувався інцидент, коли нібито від імені генерального директора італійської промислової компанії була проведена масова спам-розсилка на контрагентів компанії. Всі листи містили персональні звернення по імені та прізвища одержувача, а шаблон листа відповідав оригінальним листам, що розсилаються компанією. Однак в листах були посилання на фішингові ресурси, які містили шкідливе програмне забезпечення і виглядала ідентично як офіційний сайт компанії.

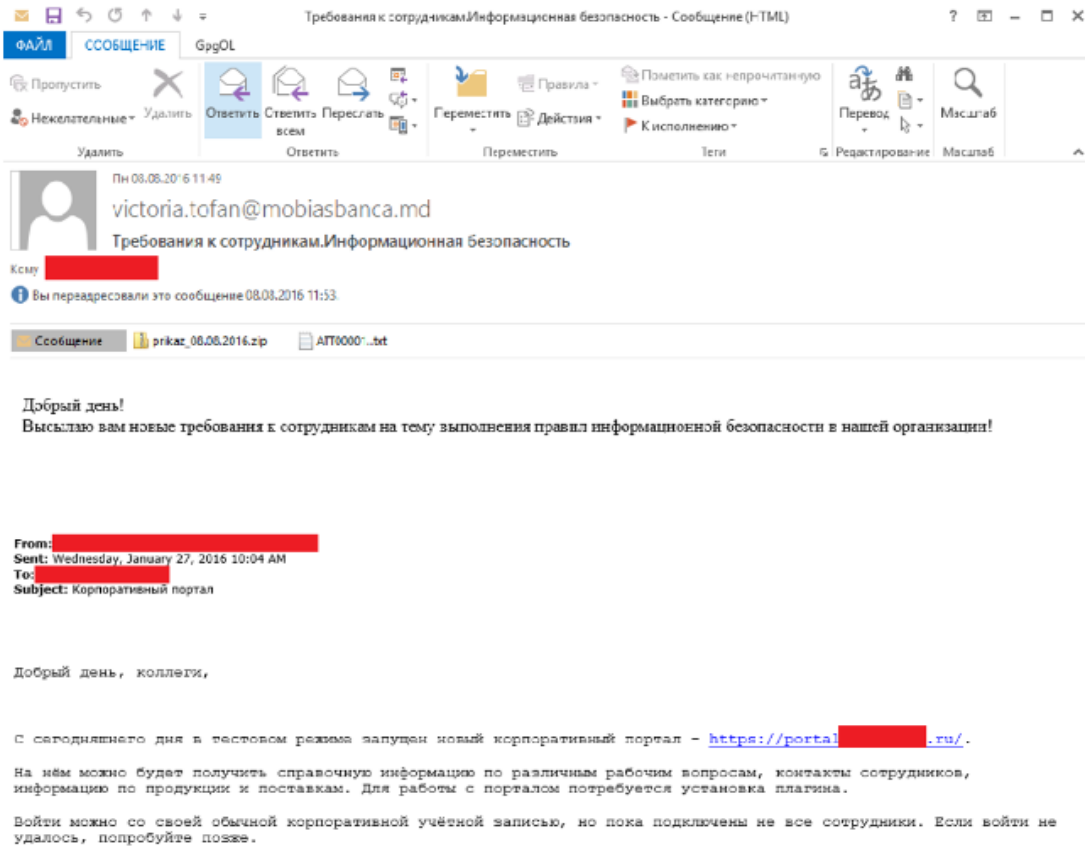

Рис.4. Листи від зловмисників не викликають підозр у одержувачів

Наслідки такого роду атак оцінити вкрай складно, оскільки не можна точно сказати, хто з контрагентів «купився» на фішингову розсилку і які саме ресурси в результаті атаки були скомпрометовані.

Можна говорити про те, що методи соціальної інженерії вже не перший рік популярні у зловмисників, і вони не стануть від них відмовлятися в найближчий рік, подбавши про створення нових, ще більш переконливих сценаріїв.

Три чверті комп'ютерних атак, в 2015-2016 роках, виявилися цільовими. Однак зустрічалися і такі ситуації, коли до порушень роботи інфраструктури хакери не мали ніякого відношення.

© Я.В. Невойт, 2017

Рис.5. Типи подій ІБ, зафіксованих у 2015-2016 роках

Так, в наприкінці 2015 року, експерти проводили аналіз інциденту, що стався на одному підприємстві і викликав аварійну зупинку промислового обладнання. Курйоз у тому, що причиною спрацювання аварійного режиму на програмно-апаратному комплексі виявилися проблеми в проводці і сильна вібрація будівлі при роботі обладнання. І хоча подія не була інцидентом інформаційної безпеки, це послужило поштовхом до проведення оцінки захищеності автоматизованих систем підприємства, в результаті якої були виявлені і усунені суттєві недоліки в захисті.

Згадані в статті інциденти - лише деякі приклади того, що дійсно відбувається щодня, щогодини і навіть щохвилини.

Підводячи підсумки, можна сформулювати тренди комп'ютерних атак, які спостерігали в останні роки:

- В гонитві за максимальною вигодою зловмисники атакують фінансові організації: під прицілом виявляються банки і біржі. Злочинці мислять глобально. Вкрасти кошти цілого банку вигідніше, ніж спустошити рахунок одного клієнта або касети одного банкомату;
- В разі атаки на промислові підприємства під загрозою розголошення виявляється конфіденційна інформація, а іноді і державна таємниця. Такі атаки вимагають гарної підготовки і фінансування, оскільки застосовуються передові технології і програмне забезпечення, розроблене з урахуванням специфіки конкретної цільової системи;
- Соціальна інженерія стала для зловмисників «відмичкою до всіх дверей». Галузева приналежність постраждалих компаній не має значення, оскільки вихідним вектором атак є вплив на працівників: їх переконують відкрити поштові вкладення, відповісти на пару питань по телефону, ввести облікові дані на підробленому сайті і т. д. Даний метод проникнення в локальну мережу виявився настільки дієвим, що зловмисники в новому році подбають про створення ще більш переконливих сценаріїв.
- На промислових підприємствах часто застосовують принцип «працює - не чіпай», а установка оновлень вважається «небезпечною» для технологічних процесів і тому не проводиться. Процес управління оновленнями програмного забезпечення в компаніях дуже тривалий і може затягнутися на роки. У зв'язку з цим можна сказати, що в атаках переважало використання відомих уразливостей і готових, перевірених не на одній жертві експлойтів.

© Я.В. Невойт, 2017

Висновки

- Будь-яка успішна компанія може стати жертвою комп'ютерної атаки. Щоб 2017-2018 рік не приніс несподіванок, компаніям слід звернути пильну увагу на ряд ключових елементів інформаційної безпеки:
- навчання співробітників правилам інформаційної безпеки, проведення спеціалізованих тренінгів для персоналу.
- забезпечення захисту від шкідливих вкладень, переданих по електронній пошті, за допомогою засобів антивірусного захисту і систем виявлення шкідливого контенту.
- моніторинг подій інформаційної безпеки: несвоєчасне виявлення інцидентів значно знижує успіх проведеного розслідування. Тут на допомогу фахівцям приходять SIEM-системи.
- виключення надмірності привілеїв в інформаційних системах.
- впровадження суворої пральний політики.
- своєчасне оновлення програмного забезпечення - як тільки розробники випустили патч.
- перевірка захищеності веб-додатків і регулярне тестування на проникнення.

Список використаної літератури

1. [Електронний ресурс] – Режим доступу: http://cert.gov.ua
2. [Електронний ресурс] – Режим доступу: https://www.anti-malware.ua

Надійшла 12.01.2017 р. Рецензент: д.т.н., проф. Бурячок В.Л.

© Я.В. Невойт, 2017