всьому світу незалежно від мотивів і цілей онлайн-атак. Компанії не сприятимуть урядам у нанесенні кібератак і вживатимуть заходів щодо захисту своїх продуктів і сервісів від зламу або некоректного використання на всіх етапах технологічної розробки та дистрибуції.

Підприємства будуть докладати додаткових зусиль для підтримки розробників, компаній і приватних користувачів своїх технологій, допомагаючи їм розширювати свою здатність до самозахисту. Такі зусилля можуть включати спільну розробку нових практичних стандартів забезпечення безпеки та нових функцій, які компанії зможуть впроваджувати у свої продукти і сервіси.

Компанії будуть розвивати існуючі зв'язки і спільно створювати нові формальні й неформальні партнерства з іншими представниками галузі, громадянського суспільства і дослідницьких кіл з метою нарощування масштабів технічного співробітництва, виявлення чинників вразливості, спільного аналізу ризиків і зведення до мінімуму потенційну можливість появи шкідливих кодів у кіберпросторі.

Звичайно, цього недостатньо, щоб зупинити бурхливе зростання кіберзлочинів у світі, але це може стати першим кроком до об'єднання всього небайдужого до проблем кібербезпеки суспільства задля протидії злочинцям у кіберпросторі.

Одержано 02.11.2018

УДК 004.056.5

Антон Вікторович ВОЛКОВ,
курсант 1 курсу групи Ф4-102 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

НАЙБІЛЬШ РОЗПОВСЮДЖЕНІ ЗЛОЧИНИ У КІБЕРПРОСТОРІ

Вступ і постановка проблеми.

Широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Через збільшення ролі комп'ютеризації в житті громадянина і держави, збільшується і можлива шкода завдана зловмисниками шляхом злочинів в кіберпросторі. Інтернет став ефективною зброєю в руках злочинців. За оцінками експертів Міжнародної торгової палати, число злочинів, які вчиняються за допомогою глобальної комп'ютерної мережі Інтернет, зростає, причому пропорційно числу користувачів. За даними Інтерполу, Інтернет став тією сферою, де рівень злочинності зростає найшвидшими темпами.

Наразі жодна країна не здатна протистояти цим загрозам самостійно, в повній мірі. Саме тому провідні країни і організації співпрацюють для боротьби з кіберзагрозами. За останні роки вже не

раз поставало питання про вдосконалення міждержавного співробітництва у сфері боротьби зі злочинами з використанням нових інформаційних технологій. Для ефективного запобігання транснаціональним комп'ютерним злочинам необхідний узгоджений міжнародний підхід на різних рівнях. Як один з найвагоміших кроків для взаємодії на міжнародному прийняття «Конвенції про кіберзлочинність» Ради Європи від 23.11.2001. Наразі конвенцію підписано 29-тьма країнами і ратифіковано 14-тьма.

До найбільш популярних за останній період злочинів, скоєних в кіберпросторі, ввійшли: таргетована атаки, атаки через «IoT», атаки вірусів-вимагачів, таємний майнінг, скіммінг.

Таргетована атака (targeted attaks) – атаки проведені на інфраструктуру компаній та державних служб. Перед атакою, кіберзлочинці ретельно вивчають засоби захисту організації що атакується. При цьому атаці можуть бути піддані не тільки звичні інформаційні системи компанії, але і автоматизовані засоби управління технологічним процесом. Антивірусні продукти не в силах запобігти таргетованій атаці, так як шкідливі програми розробляються з урахуванням використовуваного антивірусного програмного забезпечення з розрахунком, що вони не будуть виявлятися. Атаки спрямовані на конкретну організацію, і підготовка до них займає багато часу. Злочинці ретельно вивчають використовувані у потенційної жертви засоби захисту і знаходять потрібні уразливості, які і використовуються для проведення атаки. Спочатку метою націлених атак були об'єкти військового і державного призначення, з часом нападам піддаються комерційні організації.

Етапи націлених атак: на підготовчому етапі вивчається об'єкт, що атакується, збирається інформація, проводяться розвідувальні заходи, визначаються слабкі місця. Для моніторингу використовуються: розсилки, офіційні сайти та акаунти в соціальних мережах, профільні форуми. За допомогою програм аналізаторів проводиться вивчення мережевої інфраструктури та програмного забезпечення що на комп'ютерах організації. Для отримання даних можуть використовуватися автоматизовані методи або індивідуальні, такі як телефонні дзвінки. Після завершення підготовки виробляється стратегія, підбираються інструменти атаки. Шкідливі програми пишуться під конкретну атаку і жертву, це необхідно для подолання штатних засобів захисту. Сьогодні відомо про більше ніж сто провідних угрупованнях що проводять таргетовані атаки. Від їх дій страждають державні та комерційні структури в 85 країнах.

Атаки через «інтернет речей» (Internet of Things, або IoT). Інтернет речей – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудоване програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі

пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. Така система допомагає полегшити керування великими системами пристроїв, проте наразі більшість з них не захищена від кібератак, зловмисники заражають інтелектуальний інтерфейс і через нього отримують доступ для несанкціонованого входу в системи керування цими пристроями.

Віруси-вимагачі – це тип шкідливої програми, який злочинці встановлюють на Ваших комп'ютерах. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати Ваш комп'ютер. Після цього програма відображає спливаюче вікно з повідомленням, що Ваш комп'ютер заблокований і що Ви не зможете отримати до нього доступ, якщо не заплатите. Проте гарантії що після того як користувач заплатить роботу комп’ютеру буде відновлено не має.

Таємний майнінг. В останні роки були виявлені заражені комп’ютери, потужності яких зловмисник використовує для майнінгу криптовалют за допомогою технології блокчейн таємно від власника. Наразі від таємного майнінгу страждають незахищені сервери так як злочинці виявили що заражати їх значно ефективніше.

Скімінг – вид шахрайства з банківськими картками, при якому шахрай використовує спеціальний пристрый для зчитування магнітної доріжки платіжної картки. Скімер являє собою пристрій, що встановлюється в картоприймач, і кардрідер на вхідних дверях в зону обслуговування клієнтів в приміщенні банку. Являє собою пристрій з зчитує магнітною головкою, підсилювачем – перетворювачем, пам'яттю і адаптером для підключення до комп'ютера. Скиммери можуть бути портативними, мініатюрними (шиммери).

Основна ідея і завдання скіммінгу – вважати необхідні дані (вміст доріжки / трека) магнітної смуги карти для подальшого відтворення її на підробленої. Таким чином, при оформленні операції з підробленою карткою авторизаційний запит і списання грошових коштів за шахрайською транзакції будуть здійснені з рахунку оригінальною, «скіммірованной» карти.

Найчастіше разом зі скімером використовують й інші пристрої:

Мініатюрна відеокамера, яка встановлюється на банкомат і спрямовується на клавіатуру введення у вигляді козирка банкомату або сторонніх накладок, наприклад, рекламних матеріалів – використовується вкупі зі скімерів для отримання ПІН власника, що дозволяє отримувати готівку в банкоматах з підробленою карткою. Дані пристрої живляться від автономних джерел енергії – мініатюрних батарей електроживлення, і, для утруднення виявлення, як правило, виготовляються і маскуються під колір і форму банкомату.

Скиммери можуть накопичувати вкрадену інформацію про пластикові картки або дистанційно передавати її по радіоканалу зловмисникам, які знаходяться поблизу. Після копіювання інформації з карти шахраї виготовляють дублікат карти і, знаючи ПІН, знімають всі гроші в межах ліміту видачі, як в Росії, так і за кордоном. Також шахраї можуть використовувати отриману інформацію про банківську карту для здійснення покупок в торгових точках.

Більшість кібератак проводиться віддалено, дуже часто з території інших країн. Для підвищення ефективності боротьби з такими злочинами доцільною буде міжнародна співпраця у сфері кібербезпеки. Наприклад, Інтерпол відкрив у Сінгапурі центр інновацій з пошуку злочинців в Інтернеті та захисту інформаційного простору. У цьому центрі будуть працювати понад 100 експертів з більш ніж 50 країн. Крім того, для підвищення ефективності протидії кіберзлочинності, Інтерпол планує активно залучати і представників приватного сектору, які працюють у сфері цифрових технологій. Щодо нашої держави то значним проривом у цій області стала заява між Україною і Сінгапуром підписана 29 жовтня 2018 р. міністрами внутрішніх справ цих країн.

Висновок. Для ефективної протидії кіберзлочинності окремих відомчих ініціатив вже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів. Також потрібно визначити основні пріоритети розвитку державних структур по боротьбі з кіберзлочинністю такі як: реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору в загальній та організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами; запровадження сучасних новітніх інформаційних технологій в органи державної влади, технічна підготовка, перепідготовка та підвищення кваліфікації фахівців по боротьбі з кіберзлочинністю.

Одержано 01.11.2018

УДК 343.346.8:004.056.53

Олександр Ігорович ГОНЧАРЕНКО,
слухач магістратури факультету № 1
Донецького юридичного інституту внутрішніх справ;
ORCID: https://orcid.org/0000-0003-1971-4057

ПРАВООХОРОННА ДІЯЛЬНІСТЬ ЩОДО ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИНІВ

Останнім часом майже усі політичні та суспільні процеси тісно пов’язані з інформаційним простором та інформаційними технологіями, на ряду з цим, кількість кіберзлочинів та спроб їх вчинення зростає.