притягнуті до кримінальної відповідальності в Нью-Джерсі і Нью-Йорку. П'ятеро із них зізналися в злочинах.

Також жертвами криптовалютних аферистів стають досить відомі в світі бізнесу люди. За інформацією BBC у жовтні 2018 р. хакери зламали кілька верифікованих облікових записів в Twitter і виманили у користувачів під виглядом глави SpaceX Ілона Маска криптовалюти на суму понад $ 150 тис. Відзначається, що після того, як зловмисники зламували перевірені акаунти, вони змінювали імена та фотографії так, щоб вони були схожі на сторінку Маска. Після цього хакери розміщували оголошення про роздачу криптовалюти, для участі користувачам треба було перевести невелику суму у біткоінах.

В Україні також поширюється хвиля шахрайств, пов'язаних з криптовалютами. Так за інформацією Кіберполіції України у 2017 році шахраї викрали у власників bitcoin- гаманців на blockchain.info близько 700 BTC.

Користувачі сервісу стали жертвами фішингу: замість сайту blockchain.info вони прямували на підробні сайти зі схожими назвами. В результаті шахраї отримували дані для доступу до справжніх гаманців. Уперше про проблему повідомили представники Cisco, які виявили фішингову мережу у кінці 2017 року. Імовірно, більшість користувачів переходили на заражені сайти через Google Adwords – рекламну мережу Google, яка дозволяє показувати рекламу вище за результати пошуку. У 2018 році корпорація прийняла нові правила перевірки оголошень, після чого масштаб атак помітно знизився.

Криптовалюта, як анонімний платіжний засіб, буде завжди привабливим інструментом для самих різних злочинних схем, як то відмивання брудних коштів від наркоторгівлі, шантажу, торгівлі зброєю, дитячою порнографією тощо. Тому ефективна протидія відмиванню злочинних доходів і зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, які можуть бути пов'язані з відмиванням доходів, отриманих в сфері кіберзлочинності, та ефективному міжнародному співробітництву, а також співпраці між державним і приватним сектором.

Одержано 06.11.2018

УДК 004.056.53

Гліб Вікторович УШАКОВ,
магістр факультету № 6
Харківського національного університету внутрішніх справ

ГЛОБАЛЬНІ РИЗИКИ КІБЕРПРОСТОРУ

Інформаційний простір став місцем і, в той же час, безпосередньо інструментом злочину, відтепер злочин не вимагає попередньої «обробки клієнта» і особистого контакту з потенційною жертвою. Головним інструментом злочинця стає лише комп'ютер і доступ до

інформаційно-комунікаційних систем, де він за допомогою комп'ютерних вірусів і інших протизаконних технічних засобів отримує доступ до баз даних, банківських рахунків, автоматизованих систем управління.

Europol назвав вісім основних небезпечних тенденцій кіберзлочинів:

1) злочин в якості послуги: «підпільні цифрові послуги» підкріплюються моделлю «злочин-в-якості-послуги», яка стає все більш популярною і затребуваною. Вона об'єднує між собою спеціалізованих постачальників хакерських утиліт і організовані злочинні угруповання. Терористи мають очевидний потенціал для отримання доступу до цього сектору в недалекому майбутньому;

2) програми-вимагачі: вимагання та банківські «трояни» залишаються головними загрозами серед шкідливого програмного забезпечення. І ця тенденція навряд чи зміниться в найближчому майбутньому;

3) злочинне використання даних: дані залишаються ключовим товаром для кіберзлочинців. У багатьох випадках вони використовуються для отримання негайної фінансової вигоди, але все частіше застосовуються для реалізації більш складних схем шахрайства, зашифровуються з метою отримання викупу, або використовується безпосередньо для вимагання;

4) платіжне шахрайство: EMV (чіп і PIN-код), гео-блокування і інші промислові заходи безпеки продовжують допомагати в ефективній боротьбі з картковим шахрайством, але, тим не менш, зростає і число атак, спрямованих проти банкоматів. Організовані злочинні групи починають компрометувати платежі, пов'язані з використанням безконтактних карт (NFC);

5) он-лайн сексуальне насильство над дітьми: використання платформ з наскрізним шифруванням для обміну медіа файлами, а також застосування анонімних платіжних систем сприяє ескалації он-лайн трансляції жорстокого поводження з дітьми;

6) зловживання «темною стороною мережі»: «темна частина всесвітньої інтернет-павутини» продовжує сприяти злочинцям, які беруть участь в ряді незаконних видів діяльності, таких як, обмін файлами з записом сексуального насильства над дітьми. Ступінь, в якій екстремістські групи використовують кібертехнології для здійснення атак, в даний час обмежені, але пропозиція в «темної мережі» хакерських утиліт і послуг, а також незаконних товарів, може швидко змінити ситуацію, що склалася;

7) соціальна інженерія: правоохоронними органами було зареєстровано зростання числа фішинг-атак, спрямованих на цілі, які мають високу значимість. Головною загрозою стали атаки проти генеральних директорів підприємств та організацій.

8) віртуальні валюти: Bitcoin залишається тією валютою, яку шахраї вважають за краще для оплати за придбання незаконних

товарів і послуг в даркнеті. Bitcoin також став стандартним платіжним рішенням при вимаганні викупу та інших форм вимагання.

Як і раніше спостерігається зростання обсягу, масштабу і вартості кіберзлочинів. За останній час ці показники досягли небувалого рівня. Деякі держави, що входять в ЄС, говорять про те, що випадки злочинів в сфері кібербезпеки, можливо, вже перевершують чисельність традиційних злочинів.

Кількість і якість інструментів кібернападу значно випереджає ці показники у інструментів захисту. Зростання чисельності шахраїв спільно зі збільшенням кількості можливостей для участі в високоприбуткової незаконної діяльності частково підживлює подібну тенденцію, так само як і поява нових інструментів для здійснення кіберзлочинів в таких сферах, як мобільне шкідливе ПЗ і шахрайство, спрямоване проти банкоматів. Значна частина кіберзлочинців, як і раніше, використовує старі технології, методи захисту від яких доступні, але не користуються широким розповсюдженням. Проте, головна частина проблеми полягає в недостатньому дотриманні стандартів цифрового безпеки юридичними і фізичними особами.

Наприклад, в останньому своєму докладі голова Пентагону скаржиться на відсутність інструментів розробки програмного забезпечення, менеджменту даних і виробництва, яким можна було б довіряти. Ситуація ускладнюється «неадекватними практиками в питаннях кібербезпеки, які властиві багатьом ключовим постачальникам програмного забезпечення».

Кіберпростір став не тільки місцем скоєння злочину і отримання незаконного доходу, але і місцем легалізації такого доходу. При цьому різноманіття видів кіберзлочинів в сукупності з різноманіттям способів відмивання доходів, отриманих від здійснення даних видів злочинів, призводять до складності їх виявлення і розслідування.

Виявлені схеми і механізми відмивання доходів, отриманих від кіберзлочинності, дозволяють стверджувати, що переміщення коштів здійснюється як традиційними способами перекладу, так і з використанням сучасних систем термінових переказів, електронних платіжних систем і електронних грошей.

При цьому кошти використовуються в одних випадках для придбання передплачених карт, товарів або послуг в мережі Інтернет, а в інших переводяться в ігрові фішки казино або електронні гроші, перераховуються між електронними гаманцями з подальшою конвертацією та переведенням у готівку.

У свою чергу, використання готівки залишається одним з найбільш поширених способів приховування подальшого руху незаконного доходу і напрямків його вкладення, а також джерел походження таких коштів під час введення грошей в банківську систему. Це дозволяє злочинцям підтримувати анонімність, придбану на етапі отримання незаконного доходу, і під час відмивання доходів.

Ще однією загрозою для кіберпростору є міждержавні кібервійни.

У червні 2018 року стало відомо про наділення кіберкомандування збройних сил США правом проводити хакерські атаки з метою запобігання готуються кібернападів. Про це дізналася газета The New York Times (NYT) з нової стратегії підрозділу. За даними видання, Пентагон наділив кіберкомандування повноваженнями здійснювати щоденні хакерські рейди на іноземні мережі для попередження кібератак. До недавнього часу відомство дотримувалося більш оборонної позиції, борючись з уже розгорнутими кібератаками на американські мережі. Відзначається, що до більш агресивної стратегії США прийшли після більш ніж 10 років боротьби з тероризмом, коли Пентагон зрозумів, що краще протистояти терористам всередині їх простору. При цьому підрозділ кібербезпеки Пентагона отримав новий статус незалежної «командної одиниці» і таким чином вперше постав на одну дошку з дев'ятьма іншими бойовими підрозділами США. Ця зміна свідчить, що «кібератаки визнані повноцінними бойовими діями».

В результаті транскордонних кібератак Інтернет може розпастися на окремі національні і регіональні ділянки. Про це повідомляється в доповіді «Глобальні ризики – 2018», представленому на Всесвітньому економічному форумі (ВЕФ) в Женеві.

Фрагментація Глобальної мережі може призвести до припинення її функцій і уповільнення технічного прогресу. Запобігти поділ Інтернету на частини допоможе розвиток сфери кібербезпеки. На думку авторів доповіді, велике значення в цьому відіграє діалог між урядами та технологічними компаніями.

Згідно з доповіддю, в даний час більше уваги приділяється розвитку наступальних, а не оборонних можливостей в кіберпросторі. Через це виникає «туман невизначеності, при якому потенціал неправильних розрахунків може викликати спіраль каральних заходів». У свою чергу, прийняття відповідних заходів може викликати ланцюгову реакцію, відзначають автори.

Існує ймовірність того, що справжнє джерело кібератаки буде визначений невірно і удару у відповідь буде завдано по невинній цілі. Тоді ця невинна ціль також може завдати удару у відповідь, і коло залучених в конфлікт сторін розшириться. В результаті атак на невірні цілі в хід навіть може піти фізична, а не кіберзброя.

В даний час застосування звичайного озброєння регулюється з правової точки зору, і необхідно розробити подібні норми по відношенню до ведення кібервійни, впевнені автори доповіді. За допомогою таких норм можна було б заборонити цілі класи кіберзброї, як це зроблено з хімічною та біологічною зброєю.

Протидія кіберзлочинності поєднує в собі комплекс правових, технічних, організаційних та інформаційних заходів. При цьому роль кожного з цих заходів не може бути визначена пріоритетною або другорядною.

Одержано 06.11.2018