Карандась Ян Володимирович,
головний судовий експерт сектору комп'ютерно технічних видів досліджень відділу досліджень у сфері інформаційних технологій Запорізького НДЕКЦ МВС України

КІБЕРЗЛОЧИННІСТЬ: ВСТУП, МОТИВАЦІЯ, КАТЕГОРІЇ

«Кіберзлочинність» або «злочинність в області цифрових технологій» є давно встановленим явищем. Зростання глобального зв'язку, нерозривно пов'язаний з розвитком сучасної кіберзлочинності. Будь-яка злочинна діяльність, яка включає в себе комп'ютер як інструмент, метою чи засобом для зберігання інформації, входить в сферу кіберзлочинності.

Поширення цифрових технологій і конвергенція обчислювальних і комунікаційних пристроїв змінили спосіб спілкування і ведення бізнесу, в переважній більшості своїй позитивно, проте є і негативна сторона цих подій.

Злочин випливає за можливостями; практично кожен прогрес супроводжувався відповідною нішею, яка використовується в злочинних цілях. «Кіберзлочинність» використовувалася для опису широкого спектра правопорушень, включаючи злочини проти комп'ютерних даних і систем (наприклад, «хакинг»), підробку і шахрайство за допомогою комп'ютера (наприклад, «фішинг»), порушення контенту (наприклад, дитячою порнографією), і порушення авторського права (наприклад, поширення піратського контенту) [1, с. 17].

Електронний банкінг та онлайн-продаж створили сприятливий підставу для шахрайства. Електронні засоби зв'язку, такі як електронна пошта і меседжер можуть бути використані для вистежування і переслідування. Легкість, з якою цифрові носії інформації можуть бути скопійовані, призвели до великих проблем в порушенні авторських прав. Наша зростаюча залежність від комп'ютерів і цифрових мереж робить саму технологію привабливою мішенню – для отримання інформації або в якості засобів заподіяння руйнування і збитків. Ідея окремої категорії комп'ютерних злочинів виникла приблизно в той же час, коли комп'ютери стали більш доступними.

Комп'ютерні мережі зробили для злочинців те ж саме, що і для звичайних користувачів, вони спростили роботу і стали більш

зручними. Деякі кіберзлочинці використовують Інтернет, щоб знайти своїх жертв, сюди входять шахраї, серійні вбивці та інші. Поліція може часто перешкоджати цим видам злочинів і ловити злочинців, створюючи операції, в яких вони маскуються під жертву, яка звернеться до злочинця.

В інших випадках злочинці використовують мережі для зберігання записів, пов'язаних з їх злочинами (таких як продавець наркотиків або список повій), вони використовують цю технологію для спілкування з потенційними клієнтами або їх колегами по злочинності. Вражає те, що значне число злочинців використовують свої власні ноутбуки або облікові записи електронної пошти для цього. Це ситуація, коли ІТ-фахівці можуть випадково наштовхнутися на докази злочину, в тому числі на злочини, які самі по собі не пов'язані з комп'ютерами та мережами.

Кіберзлочинці складаються з різних груп і категорій. Кримінальне профілювання – це мистецтво і наука про розробку опису характеристик злочинця (фізичних, інтелектуальних і емоційних) на основі інформації, зібраної на місці злочину. Профіль складається з набору певних характеристик, які можуть бути передані злочинцеві, які здійснюють певний тип злочинів. Його можна використовувати для звуження поля підозрюваних або оцінки ймовірності того, що конкретний підозрюваний скоїв злочин.

Критичне профілювання, хоча і не зовсім просте або реальне в реальному житті, є цінним інструментом, який може дати розслідування багатьох відомостей про людину, яка вчинила певний злочин або серію злочинів. Тим не менш, важливо розуміти, що профіль, побудований на місці злочину, забезпечить тільки уявлення про загальний тип особи злочинця, яка вчинила злочин; профіль не буде вказувати на конкретну людину в якості підозрюваного. Хоча хороші профілі можуть бути напрочуд точними щодо професії правопорушника, освітнього фону, дитячих переживань, матеріального становища і навіть загального фізичного вигляду, завжди буде багато людей, які відповідають даним профілем. У сценарії кіберзлочинності [2, с. 103] кіберзлочинці класифікуються за такими основними категоріями.

1. Діти і підлітки у віці від 6 до 18 років. Проста причина такого типу поведінки у дітей проявляється в основному через допитливості. Інший близький випадок може полягати в тому, щоб проявити себе серед інших дітей в їх групі.

2. Організовані хакери. Ці хакери в основному працюють групами осіб, для досягнення певної мети. Причиною може бути їхня політична упередженість, фундаменталізм і т.п.

3. Професійні хакери / зломщики. Їх робота мотивована грошима. Ці хакери в основному працюють над зломом сайтів або крадіжці достовірної, надійної і цінної інформації. Крім того, вони навіть працюють над зломом систем роботодавців в основному в якості заходів, щоб зробити її безпечнішою, виявивши лазівки.

4. Незадоволені співробітники. У цю групу входять ті люди, які були або звільнені, або незадоволені своїм роботодавцем. Щоб помститися, вони зазвичай зламують систему свого роботодавця.

Мережа абсолютно необхідний інструмент для хакерів. Якщо у хакера немає фізичного доступу до комп'ютера з мережею, для нього неможливо вчинити злочин.

Хакери можуть здійснювати кілька злочинів, такі як несанкціонований доступ, крадіжка даних, пошкодження сайту, випуск вірусів і DoS, а також інші атаки, які призводять до втрати інформації серверів або збою мережі в цілому.

Хакери вивчають своє «ремесло» шляхом проб і помилок, вивчаючи мережеві операційні системи і протоколи з метою вивчення їх вразливостей. Є безліч сайтів для задоволення потреб хакерів, які надають інструменти, які можуть бути використані для злому сайтів. Веб-сайти, такі як Ethical Hacker Network, Cult of the Dead Cow, Hacktivismo, Security Hacks і Darknet, надають інформацію та програмне забезпечення для виявлення вразливостей і систем доступу. Звичайно, для цих цілей можна використовувати практично будь-який інструмент мережевої безпеки, який використовується для тестування системними адміністраторами.

На додаток до цього є групи новин, списки і розсилки, онлайн-документи і відеоролики, які містять керівництво та детальну інформацію та створення програм для злому. Хакерські конференції такі як DEFCON і Black Hat Briefings, надають реальні напрацювання для хакерів.

Список використаних джерел

1. Chawki M. Cybercrime, Digital Forensics and Jurisdiction / M. Chawki, A. Darwish, M. A. Khan, S. Tyagi // Switzerland: Springer, 2015. 145 p.

2. Shinder, D. L. Scene of the Cybercrime 2nd Edition / D. L. Shinder, M. Cross // Syngress, 2008. 744 p.