І все ж прогрес в боротьбі з кіберзагрозами є. Існує такий напрямок досліджень, як генеративні змагальні мережі, - коли одночасно працюють дві моделі машинного навчання з протилежними цілями. Наприклад, одна намагається щось знайти, а інша - приховати те ж саме від виявлення. Цим принципом можна користуватися при створенні команд умовного противника, щоб з'ясовувати, якими можуть бути нові загрози.

Список використаних джерел

1. Ситуационные центры в решении проблем информационной безопасности [Електронний ресурс] – Режим доступу до ресурсу: http://www.itsec.ru/articles2/Inf_security/sit_cents [Назва з екрану].
2. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница : УНИВЕРСУМ – Винница, 1999. – 320 с.
3. Рябинин И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб.: Политехника, 2000. – 248 с. 9.
4. https://www.cio.ru/news/121117-Kak-iskusstvennyy-intellekt-mozhet-protivostoyat-kiberugrozam

---

УДК 004.056: 004.738.5

ВІДОМОСТІ ПРО ХАКЕРІВ ТА ХАКЕРСТВО

Реус О.А., студ. гр. АГ-181
Науковий керівник: **Гур'єв В.І.,** к.т.н., доцент
Чернігівський національний технологічний університет

Останніх 5-7 років в засобах масової інформації, а особливо в інтернет- виданнях ми чуємо інформацію про діяльність певної групи людей, які діяли разом або по одинці, яких називають "хакерами". На сьогоднішній день при дослідженні кримінального закону щодо злочинів у сфері використання ЕОМ, необхідно з'ясувати питання: хто ці люди? Чому вони вчиняють кримінально карані діяння? Повертаючись до історії, варто згадати про походження слова "хакер". В англійській мові дієслово "to hack" перекладається як "рубати, різати". Зародження хакерства знаменується не рядом зломів комп'ютерних систем чи баз даних, а дослідженням існуючої на початку 60-х років минулого століття при Масачусетському технологічному інституті комп'ютерної техніки та невтомних спроб молодих комп'ютерних геніїв створити машини на зразок тих, які знаходилися в стінах МТІ . Для того, щоб робота стала "хаком", вона повинна були мати технологічну новизну та новизну стилю. А якщо хтось говорив, що "хакерив" систему, то малося на увазі визнання майстерності в його діях. З часом найуспішніші члени клубу почали називати себе "хакерами". Що було особливою гордістю для них . Однак, програми, які писали хакери того часу не носили ознак правопорушень і застосовувались лише для вдосконалення своїх знань, вмінь та навичок. Досліджуючи можливості перших комп'ютерів, хакери дали поштовх для створення нової культури. Їхня етика говорила: "Доступ до комп'ютерів і до всього, що може дати нам знання про влаштування світу, повинен бути повним і необмеженим. Завжди дотримуйтесь Практичного Імперативу! ". В своїй діяльності хакери притримувалися думки, що необхідно розібрати досліджувану систему на частини, поспостерігати, як ці частини працюють, а потім використати ці знання, щоб створити нові, цікавіші речі. Хакери відкидали будь-які фізичні бар'єри, людей чи закони, які намагалися завадити у задоволенні жаги знань. Їхнім бажанням було покращити все те, що на їх думку працювало не досконало. Крім того, на переконання хакерів, для розвитку творчих здібностей повинен бути реалізований принцип вільного обміну інформацією, особливо комп'ютерними програмами.

Саме цей принцип став основою для вдосконалення програмного забезпечення та самовдосконалення самих хакерів і основою для створення хакерської етики. Для них було цінним мистецтво створення невеликих та функціональних програм. Проявом здібностей хакерів зламувати паролі стала система "Compatible Time-sharing System" (Сумісна система з розподілом часу), яка для роботи з собою вимагала авторизації – введення відповідного паролю. Оскільки хакери у своїй діяльності не визнавали, згідно з хакерською етикою, будь-яких обмежень, а інформація повинна бути доступною, ця система була об'єктом злому. Іншим таким же об'єктом діяльності хакерів стала система Miltics, система захисту якої була значно потужнішою. Виробники цієї системи вважали, що за користування останньою користувач повинен вносити плату, що суперечило етиці хакерів. Тому хакери "виснажували" цю систему різними хакерськими трюками.

В кінці 60-хроків хакерство почало поширюватися. Причиною цього було те, що ветерани МТІ залишали лабораторію і несли культуру в нові місця. Люди почали хотіти займатися хакерством, оскільки комп'ютери ставали доступнішими.

Крім МТІ осередком розвитку хакерства став Стенфордський університет, де молоді хакери творили історію розвитку хакерської етики. В цей час ARPA створила комунікаційну мережу комп'ютерів, на яку великий вплив мала хакерська етика. Вивчаючи розвиток хакерства та сучасний його стан, хакерство умовно можна поділити на "біле" хакерство та "чорне" хакерство. Такий умовний поділ не означає, що вони не вчиняють діянь, які становлять склад злочину, а визначається їх наслідками та такою складовою складу злочину як об'єкт. По своїй суті, "біле" хакерство передбачає дотримання хакерської етики, яка

розвивалася ще в 60-х роках і передбачає вдосконалення існуючих систем без завдання будь-якої шкоди об'єкту. Цих людей не цікавить особистий зиск. Їх діяльність хоч і носить злочинний характер, але спрямована на досягнення певних благ. На сучасному етапі розвитку технологій та наявності знань у осіб, діяльність яких пов'язана із незаконним заволодінням інформацією та контролем над комп'ютерними системами, з'являється необхідність залучення хакерів для захисту комп'ютерних систем. Таким чином, відбувається легалізація праці хакерів. Саме "білі" хакери працюють на великі компанії та державні структури. Для прикладу, Британська секретна служба проводить набір на роботу молодих хакерів-самоучок, влаштувавши, як повідомляє інтернет-видання "Die Welt", інтернет-конкурс, переможець якого має шанс отримати посаду в секретній службі . Діяльність таких осіб, котрі отримали роботу, полягає у санкціонованих державою діяннях, які хоч і мають склад злочину, але суб'єкти, які їх вчиняють, не підлягатимуть кримінальному переслідуванню та покаранню. Однак, залишається абсолютна більшість молодих людей, які не залучаються до подібної легальної праці і намагаються заробити на незаконній діяльності. Ціллю їх діяльності є незаконне заволодіння інформацією та контролем над комп'ютерними системами. Діяльність таких осіб має характер кримінально-караних діянь і становить суть так званого "чорного" хакерства. Саме таких хакерів називають кракерами, які отримують особисту вигоду шляхом зламування кодів, саме вони вчиняють так звані кіберзлочини .

Крім того, для встановлення суб'єкта злочинів в сфері використання ЕОМ, слід встановити кримінологічний портрет хакера. Для хакера, який знайомий з комп'ютером з дитинства, останній є таємницею. Він готовий досліджувати його і присвячує цьому максимум можливого часу. Як правило, вік хакера становить 15-45 років. Для аналізу становлення особи хакера, на думку автора, необхідно в першу чергу проаналізувати особливості підліткового віку, з якого все починається. В психології підлітковий вік характеризується як кризовий вік. Діти в такому віці стають самостійнішими, однак за відсутності досвіду не можуть повністю справитися з проблемами, які намагаються вирішити самостійно. Цей він багатий на емоції та переживання, що зумовлюється фізіологічними змінами та змінами в психіці. В цей період підліток намагається самовиразитися і при цьому потребує допомоги старшого, однак через бажання стати самостійним він не звертається за допомогою до старших. Крім того, активізуються процеси пізнання, з'являються нові інтереси та уподобання. Сприйняття стає більш обдуманим та залежить від вибраної мети. Досить цікавим аспектом є також інше – ставлення сучасних хакерів до своєї діяльності. Таке ставлення виражається в різних заявах та маніфестах хакерів. Так, в своєму маніфесті хакери ідентифікують себе як осіб, які є відчуженими від суспільства, дивними та дещо замкнутими. Ці люди повністю пов'язують своє життя з комп'ютерами і працюють з ними практично весь час, крім сну, харчування та спілкування з собі подібними, а тому в них мало друзів. Дуже часто вони спілкуються в мережі. В спілкуванні з іншими людьми, хакери стикаються з нерозумінням зі сторони суспільства. Деякі хакери люблять славу і їх об'єднує одне – вони хакери, вони вільнодумці.

Науково-технічний прогрес сьогодні не стоїть на місці. З кожним днем з'являються нові технології та форми захисту інформації, нові технічні засоби та способи їх злому. А тому сучасні умови науково-технічного прогресу вимагають від кракерів покращення своїх знань, умінь та навичок, вимагають винайдення все новіших способів "обманути" систему захисту. Як і тепер, так і в майбутньому кракер, як і хакер – це не учень в школі, в табелі якого низькі оцінки з точних наук, це висококваліфікований спеціаліст в галузі фізики, математики, інформаційних наук, з величезним досвідом діяльності. Як зазначають представники компанії "Лабораторія Касперського" атаки кракерів в майбутньому стануть більше цілеспрямованими, об'єктами атак стануть не окремі користувачі, а великі світові корпорації і державні підрозділи. Згідно з прогнозами спеціалістів об'єктами атак кракерів стануть компанії, які займаються нафтою та газом, енергетикою, важким машинобудуванням тощо. Також спеціалісти стверджують, що російські користувачі почали мігрувати в зарубіжні соціальні мережі. Така міграція користувачів може стати причиною міграції атак хакерів. Отже, питання хакерства сьогодні є дуже актуальним. Хакерський рух сформувався ще в 60-х роках минулого століття. На особистісні риси молодих хакерів тих часів мали значний вплив жага знань та бажання самовдосконалення та вдосконалення їхнього світу комп'ютерної техніки. З часом серед хакерів з'явилися особи, які почали застосовувати свої знання для власного збагачення, таких осіб називали кракерами. На сьогоднішній день істинних хакерів, які дотримуються хакерської етики практично не залишилося. Досить часто хакери, які дотримуються хакерської етики влаштовуються працювати адміністраторами мережі або надають консультації для користувачів комп'ютерів. Однак, кракери, діяльність яких практично завжди має протизаконний характер все частіше і частіше здійснюють протизаконні дії. Формування особи хакера відбувається з підліткового віку, коли формується психіка дитини. На формування особи хакера значний вплив мають батьки. Саме батьки повинні спрямувати пізнавальну діяльність підлітка в галузі хакерської діяльності в русло дотримання закону. Саме вплив батьків на особу підлітка дасть можливість здійснити корекцію формування особистості хакера. Що ж стосується осіб, які декілька років займаються кракерством та осіб, які вперше цим зайнялися, для регуляції їх діяльності потрібно застосовувати заходи на рівні закону.

Список використаних джерел

1. Хакерська етика. Матеріал з Вікіпедії — вільної енциклопедії. [Електронний ресурс] // Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Хакерська_етика.

2. Кто такие Хакеры и Кракеры? Категория: Компьютерная безопасность. [Електронний ресурс] // Режим доступу до ресурсу: https://www.infoconnector.ru/kto-takie-khakery-i-krakery.

3. Трофимов, В. В. Інформатика: підручник для бакалаврів / Трофимов В. В.; під ред. В. В. Трофімова - 2-е вид., Випр. і доп. - М.: Видавнитство Юрайт, 2015. - 917 с. - (Серія: Бакалавр. Академічний курс)

4. Безпека в інтернеті [Електронний ресурс] // Режим доступу до ресурсу: http://www.rl.kiev.ua/ua/poleznaya-informatsiya/bezopasnost-v-internete/.

УДК 004.056.53:351.746:007](477)

КІБЕРАТАКИ В УКРАЇНІ 2014-2019 РР.

Марченко В.С., студ. гр. КБ-161,
Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доц.
Чернігівський національний технологічний університет

Кожен день у світі з'являються нові віруси та виникають загрози як безпеці окремого громадянина так і країні в цілому. Одні зловмисники використовують старі алгоритми, коди та схеми, інші створюють нові, однак у них завжди є дещо спільне (наприклад, шляхи проникнення на чужий комп'ютер, принципи роботи тощо). Таким чином, потрібно вивчати особливості функціонування шкідливого програмного забезпечення, для того, щоб в майбутньому мати можливість уникнути загрози.

Атака на систему «Вибори» ЦИК (травень-листопад 2014 р.). Угруповання хакерів "КіберБеркут" опублікувала в Інтернеті структуру інформаційних систем Центральної виборчої комісії. Також злочинці запевняли, що у їх розпорядженні є закрите поштове листування членів ЦВК України, технічна документація системних адміністраторів ЦВК і окружних виборчих комісії. До сьогодні достеменно не відомо чи був це злом або вірус. Але фактом залишається те, що схеми, які з'явились в інтернеті є справжніми.

Атака на енергетичний сектор BlackEnergy (грудень 2015 р.-січень 2016 р.).Про дану атаку повідомила компанія «Прикарпаттяобленерго» Авторство даного віруса приписують російській хакерської групи Sandworm. Через цю атаку залишилась велика частина західної України (Івано-Франківська область) без електрики. Даний вірус мав змогу відключати ряд процесів і пошкоджувати файли запуску.

Атаки Red Petya, Green Petya і GoldenEye (жовтень-грудень 2016). Перші віруси-шифрувальники сімейства Petya. Ці віруси шифровали дані зараженого комп'ютера і вимагали 0,9 біткоїна для розшифрування a GoldenEye навіть 1,3 біткоїна. Було заражено тисячі компютерів і нанесені мільоні збитки. Хакери заробили 3,99 біткоїна.

Атака GreyEnergy на транспортну компанію (жовтень- грудень 2016). Зараження відбувалось через взлом сервера або по електронній пошті (зараженим файлом). Даний вірус збирав інформацію (логіни і паролі) він був націлений на промислові мережі критичної важливості

Атака WannaCry (травень- червень 2017). Вірус-шифрувальник, який передавався через протоколи обміну файлами. Його ціль була - інфікувати великі компанії і державні установи (через локальні мережі). Злочинці вимагали від 300- до 600 доларів за ключ, який повинен був дешифрувати файли. Майже всі випадки зараження припадають на комп'ютери під управлінням Windows 7. Його головна особливість в том, що заразитися можна було нічого не робивши через вразливість Microsoft. Збитки понесли більше 100 компаній по всій України.

Атака банківського сектору TeleBots (січень-березень 2017). Вірус розповсюджувався завдяки програмі M.E.Doc. Разом із підробленим оновленням щахраї розіслали так званий бекдор, а потім по всій локальній мережі. Користувачами програми є близько півмільйона компаній та фізичних осіб-підприємців, вона встановлена на близько мільйон комп'ютерів по всій країні. Отже можна зробити висновок, що збитки були великі.

Атака Globelnposter Ransomware (вересень- жовтень 2017) Вірус-шифрувальник. Злочинці вимагали 2500 грн, для дешифрування. Особливістю його була націленість на Україну тому, що повідомлення про дешифрування було українською мовою, але у файлах була також і англійська мова. При цьому шахраї вимагали заплатити через айбокс (він знаходиться лише на території України). Даний вірус зупинив роботу багатьох великих компаній.

Атака бізнес сектора DanaBot (жовтень-грудень 2018). Це банківський троян, який навчений розсилати себе для подальшого зараження. Зараження комп'ютерів відбувалось після того, коли людина відкривала файли, що був прикріплений до електронного листа. А сам вірус викрадав логіни і паролі до всіх програм (почта, банківські рахунки і т.д.). Було дві особливості даного ПЗ: перший збирає поштові адреси з існуючих ящиків жертв, а другий, якщо поштовий сервіс працює на базі Open-Xchange, троян впроваджує скрипт, який таємно розсилав спам від імені жертви.