

НАЙВІДОМІШІ СПРОБИ ХАКЕРСЬКИХ ЗЛАМІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет.

Анотація

Проаналізовано наймасштабніші хакерські атаки в світі. Досліджено методи запобігання зламу програмного забезпечення та систематичне інструктування користувачів щодо необхідних заходів кібербезпеки.

Ключові слова: Злами, хакерство, кібервійна, захист.

Abstract

This thesis reveals the topic of the most vulnerable hacker attacks in the history of mankind of the world. Methods of software hacking prevention and systematic instructing of users on the necessary cybersecurity measures have been studied.

Keywords: *Hacking, cyber warfare, protection..*

Вступ

Хакерство народилося і розвивалося протягом десятиліть як форма соціального протесту і відходу від реального світу в світ кіберпростору. Однак в останні роки з'явилася тенденція відходу в бік кібертероризму. Кібератаки будь-якого типу наступального маневру використовуються окремими особами або цілими організаціями. Цільові комп'ютерні інформаційні системи, інфраструктури, комп'ютерні мережі, або персональні ЕОМ на різних засобах злочинних дій, як правило, відбуваються з анонімного джерела, що краде, змінює або знищує вказану ціль шляхом злому у вразливій системі [1].

Сьогодні явище хакерства в першу чергу пов'язується та розгорається все сильніше з кібервійною - війною, в якій немає ні правил ні законів, а цілі виправдовують будь-які засоби і методи. Хакерство, як явище, офіційно вважається поза законом, але фактично це одна з рушійних сил нашого суспільства на шляху науково-технічного прогресу. Різного роду хакерські атаки відбуваються постійно. Кібератаки можуть спричинити неминучі втрати та лиха.

Результати дослідження

Свобода та можливості, які надає Інтернет, постійно використовуються злочинцями, бандитами та терористами, які діють на темній стороні мереж, в зв'язку із цим кіберзлочинність є однією з найбільших соціальних проблем відколи існує доступ до мереж Інтернету. Знаменитим хакерам знадобилися десятиліття роботи над виявленням критичних вразливих місць та розкриттям стратегій, що заклали основи Інтернету та його вільного для всіх лібертаріанства.

Найвідомішими хакерськими зломами є такі:

1. Роберт Таппан Морріс і Морріс Ворм (1988 р.). Творець першого комп'ютерного черв'яка, переданого через Інтернет, Морріс, студент Корнельського університету в США, стверджував, що його розробка не мала на меті завдати шкоди, а мала безневинний намір визначити простори кіберпростору. Однак черв'як зіткнувся з критичною помилкою і перетворився на вірус, який швидко розмножувався і почав заражати інші комп'ютери, що призводило до відмови в обслуговуванні. Як повідомлялося, 6000 комп'ютерів спричинили збитки на ремонт на суму \$ 10 - 100 мільйонів доларів. Хоча ця подія може розглядатися як нещасний випадок, вона, без сумніву, відіграла роль у надиханні катастрофічних типів атак, які ми бачимо сьогодні [2].

2. MafiaBoy завдає збитків у розмірі 1 мільярда доларів (2000 р.). Ще 15-річним хлопцем, який викликав пустощі у кіберпросторі, був Майкл Кальче (MafiaBoy). У 2000 році Кальче був лише канадським студентом середньої школи, коли вирішив розв'язати DDoS-атаку на ряді високопоставлених комерційних веб-сайтів, включаючи Amazon, CNN, eBay і Yahoo. Завдав підприємцям \$ 1,2 млрд доларів шкоди та був затриманий. Оскільки він все ще був неповнолітнім, Кальче був засуджений у 2001 році до восьми місяців під вартою, а це означає, що його рухи та дії будуть обмежені. Його доступ до Інтернету також був обмежений судом.

3. Google China постраждав від кібератаки (2009 р.). Хакери отримали доступ до декількох корпоративних серверів Google, а інтелектуальна власність була викрадена. У своєму блозі Google заявив, що має «докази, які свідчать про те, що основною метою зловмисників був доступ до облікових записів Gmail правозахисників Китаю». Оскільки компанія глибше копала, вони знайшли численних користувачів з США, Китаю та Європи, які регулярно отримували доступ без дозволу. Ці листи належали захисникам прав людини в Китаї. Тому уряд Китаю був звинувачений в порушенні прав людини протягом багатьох років. Google вийшов на китайський ринок з www.google.cn в 2006 році і потрапив під жорсткий режим цензури Інтернету в Китаї. Кібернапади в грудні 2009 року призвели до переоцінки бізнесу компанії в країні. У березні 2010 року Google перемістив свої сервери для google.cn до Гонконгу, щоб уникнути політики фільтрації Інтернету в Китаї [3].

4. Підліткова атака на NASA та Міністерство оборони США (1999 р.). Джонатан Джеймс (15 років) зміг проникнути в комп'ютери департаменту Міністерства оборони США і встановити на своїх серверах «бекдор». Це дозволило йому перехопити тисячі внутрішніх листів від різних урядових організацій, включаючи ті, що містять імена користувачів і паролі для різних військових комп'ютерів. Використовуючи вкрадену інформацію, Джеймс зміг викрасти частину програмного забезпечення NASA, яке коштувало агентству космічних досліджень \$ 41,000, оскільки системи були закриті на три тижні. За даними NASA, «програмне забезпечення вартістю \$ 1,7 мільйона підтримували фізичне середовище Міжнародної космічної станції, в тому числі контроль температури і вологості всередині приміщення». Джеймс був спійманий, але отримав легке покарання з огляду на його молодий вік. Він вчинив самогубство в 2008 році після звинувачень у змові з іншими хакерами з метою викрадення інформації з кредитних карток.

5. Хакер Церкви Саентології (2008 р.). У січні 2008 року, Нью-Джерсі підліток разом з бандою хакерів почав атаку DDoS. Дмитру Гузнеру, якому виповнилося 19 років, було пред'явлено звинувачення і засуджено за DDoS-атаку. Максимальне покарання становило 10 років тюремного ув'язнення і штраф у розмірі 250 тисяч доларів, але він був остаточно засуджений до двох років випробування і йому було наказано заплатити Церкві Саентології \$ 37 500 [4].

6. Solar Sunrise (1998 р.). Коли в США почалася систематична кібератака, яка захопила контроль над більш ніж 500 урядовими та приватними комп'ютерними системами, спочатку вважалося, що це були кібератаки іракських оперативників, Хакери експлуатували комп'ютери, що працюють на операційній системі Sun Solaris, тому колективні атаки називалися "Solar Sunrise". Уряд США зібрав низку оборонних підрозділів, у тому числі ФБР і Агенцію оборонних інформаційних систем для розслідування цього питання. Несподіваним для всіх було те, що хакерами виявились троє підлітків з Каліфорнії. Атаки показали, як скоординовані зусилля можуть вплинути на IT-інфраструктуру всієї країни.

7. Вірус Меліси (1999 р.). Це був дуже простий вірус, який закінчився тим, що коштував 80 мільйонів доларів. Вірус Меліси заражав документи Microsoft Word і автоматично поширював себе як вкладення електронною поштою. Він поширювався на перші 50 імен, перелічених у вікні адреси електронної пошти Outlook. Творець Меліси, Девід Сміт, стверджував, що він не мав наміру заподіяти шкоду комп'ютерам, але був заарештований і засуджений до 20 місяців ув'язнення. Результатом розповсюдження даного вірусу стала розробка спеціалізованого антивірусного програмного забезпечення [5].

Висновки

Детально дослідивши питання щодо зламів систем, можна стверджувати, що в сучасних умовах проблема захисту від хакерських атак, інтернет-загроз та захисту від хакерів стає з кожним днем актуальнішою. Однак більшість користувачів ще не до кінця усвідомлюють наслідки таких атак на комп'ютерні мережі і персональні комп'ютери, часто не дотримуються елементарних правил безпечної поведінки в Інтернеті. В результаті, хакери з легкістю обходять прості ешелони захисту, отримуючи нові можливості для здійснення різних злочинів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хакерська атака [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D0%B0_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0.
2. Первый компьютерный вирус в Интернете - Червь Морриса [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: <https://cameralabs.org/4417-pervyj-kompyuternyj-virus-v-internete-cherv-morrisa>.
3. Найвідоміші хакерські атаки в історії [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://techtoday.in.ua/news/najvidomishi-hakerski-ataki-v-istoriyi-50493.html>.
4. Top 10 most notorious cyber attacks in history [Електронний ресурс] – Режим доступу до ресурсу: <https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/>.
5. Cyber attacks: Today's reality.: Cyber Security Solutions [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nec.com/en/global/solutions/cybersecurity/about/index.html>.

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.

Антонюк Ганна Олександрівна – студент групи КІТС-186, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: antoniukanna78@gmail.com.

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.

Antoniuk Anna Oleksandrovna – Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.