УДК 65.012.8 + 004

Тетяна Петрівна КОЛІСНИК,
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ОСОБЛИВІ ПИТАННЯ ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ

На теперішній час мало хто із користувачів знає, що тільки 15-20 % Інтернету доступні. Інша частина таємна і називається глибинним Інтернетом.

Тому якщо розглянути видиму частину, то можна зробити простий висновок, що кожна підключена до Інтернет система ненавмисно просочує внутрішню інформацію про свою організацію, яка може бути використана для розробки цільової атаки. Залежно від джерела цього витоку, інформація може відноситися до компонентів, які використовуються у фізичній інфраструктурі, активів організації, процесів управління тощо.

Велика частина цієї інформації у більшості випадків, відноситься до топології мережі організації та видів сервісів у ній. Це дозволяє зловмисникові намітити цілі для подальших атак.

Збір інформації, що стосується конкретних осіб може бути активно використаний в атаках соціальної інженерії – можливо, через оману, підкуп або шантаж. Також важливим аспектом цього витоку інформації є її відкритий доступ через Інтернет, і, ймовірно, те, що вона може міститись у системах, не пов'язаних з організацією. Тому, доступ до інформації стає незалежним від ресурсів організації і, отже, до неї може «анонімно» звернутися будь-хто.

Як правило процеси виявлення цього витоку інформації дуже прості і існує безліч легко доступних інструментів та сервісів, які дозволяють зробити їх ще простішими. Але, багато з інструментів або вже вбудовані в найпопулярніші операційні системи, або знаходяться у вільному доступі на різних Інтернет ресурсах.

Методи, що використовуються для виявлення витоку інформації, як правило, називають «пасивним або активним збором інформації» – і вони грають життєво важливу роль (яка часто упускається з виду) в будь-якому тесті на проникнення (пентест) або оцінці безпеки інформаційних ресурсів.

Фахівці стверджують, що пасивна розвідка може включати переглядання цільових веб-сайтів, щоб переглянути та завантажити публічно доступний контент, в той час як інші стверджують, що пасивна розвідка не припускає відправку будь-яких пакетів взагалі на цільовий сайт.

Багато важливої інформації може бути зібрано пасивно, а потім використано в прямій атаці або для зміцнення інших від нападів. Залежно від джерела, легко може бути отримана така інформація, як - поточний рівень встановлених оновлень та патчів, топологія внутрішньої мережі або дані щодо облікових записів.

Виходячи з вищевказаного основні процеси пошуку та обробки інформації передбачають використання таких Інтернет-ресурсів та джерел як:

1. Бази даних Інтернет – інформація щодо IP-адрес.
2. Доменна система імен – інформація щодо вузлів.
3. Пошукові системи – інформація, що стосуються організації або її співробітників.
4. Системи електронної пошти – інформація, що міститься в кожному процесі доставки пошти.
5. Угоди про присвоєння імен – спосіб, у який організація кодує або класифікує сервісі, які працюють на її вузлах.
6. Аналіз сайту – публічно доступна інформація, що може становити ризик для безпеки.

Слід важливо зрозуміти де отримують цю інформацію і рівень деталізації інформації, бо тоді організація зможе припинити цей витік інформації просто і швидко.

Якщо розглядати основний сегмент збору інформації, то слід виділити більш увагу питанням отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел використовуючи такі, а іноді вони стають нажаль основними, можливими методами як:

- оголошення про пошук роботи, каталоги пропозицій, прохідні сторінки та інші підказки, інший вміст сайту;
- пошук документів та визначення цікавого контенту;
- веб-портали, веб-пошта та адміністративні консолі;
- тестові сторінки, лог-файли та сторінки статусу сервера;

- резервні копії, застарілі файли, і на код стороні сервера;
- файли конфігурації та дамп бази даних файлів;
- спеціалізовані форуми;
- файли користувачів і паролів;
- клієнтський код;
- виявлення вразливостей;
- дослідження програмного забезпечення відомих вразливостей на основі виявлених технологій;
- перевірка URL та пасивне сканування через перехоплюючий проксі;
- інші документи, що представляють інтерес.

Одержано 30.10.2017

УДК 004.89

Олексій Феліксович ЛАНОВИЙ,
кандидат технічних наук, доцент, доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖІ DARKNET ДЛЯ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Серед основних тенденцій розвитку інформатизації суспільства, що стосується практично всіх сфер життєдіяльності слід відзначити стрімкий розвиток інформаційної мережі Інтернет. Розвиток інформаційних технологій сприяв виникненню нового виду злочинності – комп'ютерної, а перехід на цифрові технології, методи електронного управління технологічними процесами, конвергенція і глобалізація комп'ютерних мереж стали передумовою появи кіберзлочинності. Фахівці зазначають, що загроза поширення кіберзлочинності та кібертероризму за рівнем негативного впливу може бути порівняна з реальними бойовими діями. Водночас, розвиток інтернету призводить до виникнення низки проблем: соціальних, організаційних, юридичних тощо, але найгострішою є активне використання мережі злочинним світом. Міжнародним суспільством кіберзлочинність визнано загрозою не тільки національній безпеці окремих держав, а й людству та міжнародному порядку в цілому [1].

Тіньовий або глибинний Інтернет («Deep Web») – величезна частина Інтернету, яка знаходиться за межами стандартних методів пошуку. Значна частина тіньового Інтернету – це сай-