Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: аналіз проблеми захисту від ddos-атак на основі ботнетів
назви записувати нижнім регістром (як у реченні)

Назва (англ.): analysis of security problem caused by botnet-based ddos-attack
переклад англійською

Освітній ступінь : ***магістр***

Шифр та назва спеціальності: **125 Кібербезпека**

напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: **Екзаменаційна комісія № 32**
напр.: Екзаменаційна комісія №1

Установа захисту: **Тернопільський національний технічний університет імені Івана Пулюя**

напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 23.12.2019 **Місто:** Тернопіль

Сторінки:
Кількість сторінок дипломної роботи: 133 Кількість сторінок реферату: 6

УДК: 004.056

Автор дипломної роботи
Прізвище, ім'я, по батькові (укр.): Амбок Володимир Іванович
розкривати ініціали

Прізвище, ім'я (англ.): Ambok Volodymyr
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ, ФІС, Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Александер Марек Богуслав
повністю

Прізвище, ім'я (англ.): Aleksander Marek
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ, КБ, Тернопіль, Україна

Вчене звання, науковий ступінь, посада: д.т.н., проф., професор кафедри КБ

Рецензент
Прізвище, ім'я, по батькові (укр.): Михайлишин Михайло Стахович
повністю

Прізвище, ім'я (англ.): Mykhailyshyn Mykhailo
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ, кафедра ММ, Тернопіль, Україна

Вчене звання, науковий ступінь, посада: к.т.н., доц., доц. кафедри ММ

Ключові слова

українською: БОТНЕТ, ЗАГРОЗА, ІДЕНТИФІКАЦІЯ БОТНЕТІВ, , ПРОТОКОЛ

до 10 слів

англійською: BOTNET, THREAT, BOTNET IDENTIFICATION,, PROTOCOL

до 10 слів

Анотація

українською: Ботнет — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів. За допомогою ботнетів часто надсилається спам, встановлюються шпигунські програми або здійснюється викрадення облікових даних користувачів. Масштабний ботнет може використовуватися для атак типу DDoS (Distributed Denial of Service) для спрямування додаткового трафіку на сайт та сповільнення роботи або збоїв підключення.

Шкідливі програми виду ботнет розповсюджуються за допомогою вкладень електронної пошти та через завантаження файлів і підроблених програм. Зловмисники також націлюються на такі уразливі місця, як неоновлене програмне забезпечення та відсутність захисту в мережі Інтернет. Все частіше під приціл зловмисників потрапляють камери, смарт-телевізори та навіть автомобілі. Виявлення, а, відповідно, і захист від ботнетів є важливою і актуальною задачею. Обчислювальна потужність одного ботнету дозволяє здійснювати декілька зловмисних дій швидко та часто без виявлення.

англійською: Botnet is a network of computers infected with malware. Cybercriminals use botnets that consist of a large number of computers for various malicious activities without the knowledge of users. Botnets often send spam, install spyware, or steal user credentials. A large-scale botnet can be used for DDoS (Distributed Denial of Service) attacks to direct additional traffic to the site and slow down work or connection failures.

Botnet-type malware is spread through email attachments and through file downloads and fake applications. Attackers also target vulnerabilities such as uninstalled software and a lack of Internet security. Increasingly, the target of intruders is cameras, smart TVs and even cars.

Detecting and, accordingly, protecting against botnets is an important and urgent task. The computing power of a single botnet allows several malicious actions to be performed quickly and often without detection