УДК 621.396

Андрій Дівіцький, Антон Сторчак, Василь Некоз
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Україна

АТАКИ НА ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Представлено атаки на державні інформаційні ресурси, що обробляються засобами інформаційно-телекомунікаційних систем. Представлено загальну структуру реалізації атаки. Проведено аналіз атак на системи обробки державних інформаційних ресурсів. Представлено класифікацію атак та параметри цих атак. Описані стратегії здійснення атак. Висунуто перелік вимог до методів виявлення атак. Визначено, що реалізація загроз відбувається за допомогою множини різнонаправлених атак.

Ключові слова: державні інформаційні ресурси, інформаційно-телекомунікаціні системи, атаки на державні інформаційні ресурси, фази атак, класифікація атак, вразливості систем.

Andriy Divicky, Anton Storchak, Vasyl Nekoz

APPLICATIONS APPLICABLE FOR TERRORIST, PRIVACY OR ACCURACY IN PUBLIC INFORMATION RESOURCES

Attacks on state information resources processed by means of information and telecommunication systems are presented. The overall structure of the attack implementation is presented. The analysis of attacks on state information resources processing systems was carried out. The classification of attacks and parameters of these attacks is presented. The strategies for attacking are described. The list of requirements for methods of detection of attacks is issued. It is determined that the realization of threats occurs through a set of multi-directional attacks.

Keywords: state information resources, information and telecommunication systems, attacks on state information resources, phases of attacks, classification of attacks, vulnerability of systems.

Державні інформаційні ресурси (ДІР) являють собою систематизовану інформацію, що є доступною за допомогою інформаційних процесів, що використовують засоби обчислювальної техніки та забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. Під обробкою ДІР розуміємо виконання однієї або кількох операцій, а саме: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. Від надійного виконання зазначених операцій та функціонування інформаційно-телекомунікаційних систем (ІТС) в значній мірі залежить рівень захищенності ДІР та ефективна робота державних установ, організацій. На стан ІТС впливають атаки, тобто дії зловмисників або шкідливих програм, які спрямовані на захоплення ДІР, отримання повного контролю над системами управління ДІР або на втручання в нормальне функціонування ІТС.

Атаки реалізуються для порушення конфіденційності, цілісності або доступності ДІР, що зберігається, обробляється та циркулює в ІТС. З цією метою, як

правило, використовують вразливості ІТС, які являють собою певні апаратні способи втручання або нездатність системи протистояти реалізації певних загроз.

Атаки на ДІР в ІТС класифікуються за: характером впливу (пасивні, активні); метою впливу (порушення конфіденційності, порушення цілісності, порушення доступності); умовою початку здійснення впливу (атака на запит від об'єкта, що атакується; атака по настанню події, що очікується на об'єкті; безумовна атака); наявністю зворотного зв'язку з об'єктом, який атакується (зі зворотним зв'язком, односпрямована атака); розташуванню атакуючого щодо атакуємого об'єкта (внутрішньо сегментна, між сегментна); кількістю атакуючих (розподілена, нерозподілена).

Аналіз останніх публікацій свідчить про те, що існуючі атаки, які застосовуються для проведення вторгнень в ІТС поділяються на 5 категорій. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. В свою чергу кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на мережу . До вказаних атак відносять:

Side-channel атаки (атаки сторонніми каналами) – атаки, спрямовані на вразливості в практичній реалізації криптосистеми. На відміну від теоретичного криптоанализа, атаки по стороннім каналах використовуть інформацію про фізичні процеси в пристрої, які не розглядаються в теоретичному описі криптографічного алгоритму. До найчастіше застосованих Side-channel атак належать: probing attack, timing attack, fault–induction attack, power analysis attack, electromagnetic analysis attacks та інші атаки;

DoS атаки – це мережеві атаки, спрямовані на створення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні. Вказані атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та блокування сервера. До найчастіше застосованих DoS атак належать: back, land, neptune, pod, smurf, teardrop attacks та інші атаки;

U2R атаки – пропонують отримання зареєстрованим користувачам привілеїв адміністратора. До U2R атак відносять наступні атаки: buffer_overflow, loadmodule, perl, rootkit;

R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster та інші атаки;

Probe-атаки – сканування мережевих портів з метою отримання конфіденційної інформації. Probe-атаки поділяються на наступні типи: ipsweep, nmap, portsweep, satan та інші.

Зазвичай атака надходить до ІТС у вигляді повідомлення, яке містить в собі мову, відео, аудію інформацією або дані. Вказані атаки за своєю функцією можуть впливати на: управління ІТС, розмежування доступу, обмін пакетами, енергетичні характеристики, доступ до кодування, управління інформацією та інше.

Опис стратегій здійснення атак, що використовуються при проведення атак на інформаційні системи представлено в проекті корпорації The MITRE Adversarial Tactics, Techniques and Common Knowledge [5]. В свою чергу база даних (атак) та модель для оцінки поведінки зловмисників (при здійсненні вторгнень) являє собою матрицю ATT@CK, яка описує найбільш небезпечні фази атаки на ІТС, а саме:

– отримання початкового доступу (Initial Access) – представляє вектори, які використовують зловмисники для отримання доступу до мережі;

– виконання (Execution) – застосування методів, що призводять до виконання коду зловмисника в локальній або віддаленій системі;

– закріплення в атакуємій системі (Persistence) – будь-які зміни доступу або конфігурації системи, які забезпечують постійну присутність зловмисника в цій системі;

– підвищення привілеїв (Privilege Escalation) – зловмисник має скористатись слабкими місцями системи для отримання прав локального адміністратора або рівня system/root;

– обхід захисту (Defense Evasion) – набір атрибутів, які застосовує зловмисник для ухилення від виявлення;

– отримання облікових даних (Credential Access) – методи отримання доступу або контролю обліковими даними системи, домена або служби, що використовуються в системі;

– огляд (Discovery) – методи отримання зловмисником відомостей про систему і внутрішню мережу;

– горизонтальне просування (Lateral Movement) – методи збору інформації із системи без використання додаткових інфструментів;

– збір даних (Collection) – методи збору інформації;

– витік (Exfiltration) – матоди та атрибути видалення файлів і інформації з цільовою системи;

– управління і контроль (Command and Control) – взаємодія зловмисника з підконтрольними системами.

Тобто для виявлення широкого спектру різнонаправлених за своїм фізичним змістом атак сучасні системи виявлення атак та методи виявлення атак повинні враховувати вищезазначені особливості атак та мати наступні можливості, а саме: інтелектуалізація процесу встановлення вразливостей та виявлення атак; високу точність виявлення атак; високу швидкість виявлення атак; можливість виявлення нових типів атак; робота в умовах непередбачуваності; можливість самонавчання, саморганізації та ін.

Висновки. Проведений аналіз класифікацій, категорій, стратегій, та здійснення фаз атак на ДІР, показав їх різноманітність. На основі цих даних виникає завдання щодо удосконалення існуючих та розробку нових методів виявлення атак, що підвищить єфективність функціонування системи забезпечення безпеки ДІР, на що і буде направлена подальша наукова робота.

Література

1. Основи формування державної системи кібернетичної безпеки: монографія / В.Л. Бурячок. – К.: НАУ, 2013. - 432 с.

2. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач.

3. В. Базилевич, В. Гур'єв, Я. Усов // Захист інформації. - 2018. - №20(1). - с.61-66. DOI: 10.18372/2410-7840.20.12453

4. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних / Я.В. Корпань // Реєстрація, зберігання і обробка даних. - 2015. - №17(2). – С. 39-46.

5. Офіціальний сайт KDD Cup 1999 Data. Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99

6. Офіціальний сайт The MITRE Corporation. Режим доступу: http://attack.mitre.org