УДК 621.391 **doi: 10.26906/SUNZ.2021.2.132**

Д. В. Дорошенко

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

МЕТОДИКА ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Анотація. У статті запропоновано методику виявлення несанкціонованих обчислювальних процесів інформаційно-телекомунікаційних систем. Існуючі технології виявлення APT атак засновані на процедурах багаторівневого аналізу великого масиву даних про різноманітні поточні події в ІТС. Ці дані збираються в електронних журналах подій. Очевидно, що модель APT атаки повинна дозволяти пов'язувати події за часом і в просторі. Комплекси програм, які наповнюють інформацією журнали і реалізують автоматизовані технології їх аналізу, відомі як системи SIEM. У свою чергу, технології автоматизованого аналізу подій засновані на моделях атак. Шаблон APT атаки – це набір взаємопов'язаних подій. Порівняння такого шаблону і поточних подій становить суть процесу оцінки в рамках SIEM. Основним завданням методики є автоматизація процесу виявлення несанкціонованих дій, прийняття рішення про наявність APT атаки, та реалізацію методів захисту від неї. Основу APT атаки становить комплекс дій, що реалізуються в різних компонентах ІТС на тривалому відрізку часу. З позицій політики безпеки такі події окремо можуть нести легальний характер. Розглянуто програмні та апаратні засоби, призначені для прихованого спостереження за діяльністю користувачів інформаційно-телекомунікаційних систем. Санкціоновані моніторингові програмні продукти використовуються адміністраторами безпеки інформаційно-телекомунікаційних систем для забезпечення моніторингу. Детально розглянуто застосування для прихованого моніторингу активних процесів інформаційно-телекомунікаційних систем. Запропоновано використати в якості прикладу несанкціонованого обчислювального процесу програмні та апаратні кейлоггери. Детально описано методи захисту від них. Отримані результати доцільно направити на удосконалення методів виявлення несанкціонованих обчислювальних процесів інформаційно-телекомунікаційних систем.

Ключові слова: APT атака; SIEM; кейлоггер; інформаційно-телекомунікаційна система.

Вступ

При стрімкому розвитку мережевих технологій та глобальній інформатизації суспільства на перший план висуваються проблеми забезпечення високого рівня захищеності інформаційно-телекомунікаційних систем. Зі збільшенням числа комп'ютерних інцидентів, пов'язаних із безпекою, світ переконався, що навіть найнадійніші системи захисту не здатні захистити від складних кібератак на ІТС державних і комерційних установ. Тому розробка систем виявлення та протидії атак є одним із найбільш актуальних напрямків наукових досліджень в області інформаційної безпеки. В процесі такої розробки необхідно постійно проводити наукові дослідження, що вивчають та детально аналізують можливі варіанти реалізації складних атак.

Постановка завдання. Застосування APT значно ускладнило ситуацію обробки даних SIEM. Основу APT атаки становить комплекс дій, що реалізуються в різних компонентах ІТС на тривалому відрізку часу. З позицій політики безпеки такі події окремо можуть нести легальний характер.

Програмні та апаратні засоби, призначені для прихованого спостереження за діяльністю користувачів інформаційно-комунікаційних систем та персональних комп'ютерів, отримали широке застосування останнім часом.

Санкціоновані моніторингові програмні продукти використовується адміністраторами безпеки інформаційно-комунікаційних систем для забезпечення її спостережливості – "властивості обчислювальної системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів та процесів з метою запобігання порушенню політик інформаційної безпеки і/або забезпечення відповідальності за певні дії" [1]. Саме ця властивість в залежності від якості її реалізації дозволяє в тій чи іншій мірі контролювати дотримання встановлених правил роботи на комп'ютерах та політики інформаційної безпеки.

Особливу небезпеку становлять моніторингові програмні продукти та апаратні засоби, які приховано, несанкціоновано (як правило, дистанційно) встановлені без відома адміністраторів безпеки автоматизованої системи або без відома користувачів. Вказана категорія моніторингових продуктів далі в статті іменуватиметься як "програми-шпигуни" або шпигунське програмне забезпечення. Очевидно, що модель APT атаки повинна дозволяти пов'язувати ці події за часом і в просторі. Основним завданням методики є автоматизація процесу виявлення несанкціонованих дій, прийняття рішення про наявність атаки, та реалізацію методів захисту від неї.

Аналіз останніх досліджень та публікацій. Існуючі технології виявлення APT атак засновані на процедурах багаторівневого аналізу великого масиву даних про різноманітні поточні події в ІТС. Ці дані збираються в електронних журналах подій. Комплекси програм, які наповнюють інформацією журнали і реалізують автоматизовані технології їх аналізу, відомі як системи SIEM.

В роботі [6] розглянуті моделі APT–атак та методів їх застосування. Моделі використовують різну математичну базу, але більшість з них засновані на кінцевих автоматах та представляють атаку як послідовність станів автомата. Жодна з моделей не дозволяє врахувати в комплексі вразливості, що активізуються атакою, методи її реалізації та можливі

наслідки. Тобто, питання розробки якісної моделі інформаційної атаки залишається невирішеним.

Мета статті – розроблення методики виявлення несанкціонованих обчислювальних процесів інформаційно-телекомунікаційних систем, яка дозволить автоматизувати процес виявлення несанкціонованих дій, прийняття рішення про атаку, та реалізацію методів захисту від неї.

Основна частина

APT атака (advanced persistent threat) (Розвинена стала загроза) – різновид складних кібератак з метою встановлення несанкціонованого доступу до інформаційних систем жертви для їх використання або контролю в майбутньому. Як правило, APT атака відбувається у декілька етапів, а саме:

1. Зовнішня розвідка. Здійснюється збір інформації про характеристики ІТС з різноманітних зовнішніх джерел.

2. Проникнення в ІТС. На основі інформації зовнішньої розвідки приймається рішення про засоби і способи запуску процесів на одному з вузлів ІТС. Зловмисник здійснює реалізацію прийнятого рішення шляхом направлення через Інтернет необхідних даних для запуску процесу встановлення прихованого каналу віддаленого управління вузлом ІТС.

3. Доставка засобів впливу. На цьому етапі зловмисник запускає процес доставки програмних засобів для здійснення внутрішньої розвідки в межах цільової ІТС.

4. Внутрішня розвідка. Зловмисник запускає штатні та нештатні процеси для збору даних про структуру ІТС. Після аналізу отриманих даних реалізується рішення про просування між вузлами ІТС до моменту виявлення цільового ресурсу ІТС.

5. Цільова акція. На основі отриманих даних про знаходження критичного ресурсу зловмисник приймає рішення про спосіб реалізації цільового впливу та засоби для цього. За допомогою прихованого каналу управління вузлом ІТС доставляються за запускаються необхідні процеси здійснення цільової атаки.

6. Приховування слідів. На цьому етапі стираються дані, які були пов'язані з кібератакою.

Після виявлення несанкціонованих дій SIEM вимагає від оператора прийняти рішення про наявність атаки, та запустити засоби протидії. Схема застосування SIEM з активним оператором зображена на рис. 1. У свою чергу, технології автоматизованого аналізу подій засновані на моделях атак. Шаблон APT атаки – це набір взаємопов'язаних подій. Порівняння такого шаблону і поточних подій становить суть процесу оцінки в рамках SIEM. Схему застосування SIEM з використанням шаблону APT атаки зображено на рис. 2.

Як приклад несанкціонованих обчислювальних процесів пропонується розглянути кейлогери.

Між продуктами для забезпечення моніторингу і "продуктами-шпигунами" дуже тонка грань – це грань між управлінням інформаційною безпекою та порушенням інформаційної безпеки. При цьому наявність в програмі таких функцій, як можливість початкової конфігурації модулю моніторингу та отримання виконуваного файлу, який при виконанні не виводить повідомлень на екрані, вбудованих засобів доставки та дистанційного встановлення скомпільованого модулю на комп'ютер користувача, сприяють процесу перетворення продукту для моніторингу в "продукт-шпигун". Навпаки, виконання програмою наступних функцій: можливість інсталяції та конфігурації модулю моніторингу тільки при безпосередньому фізичному доступі до комп'ютера користувача, обов'язкова наявність прав адміністратора для інсталяції та конфігурації програми – найчастіше робить продукт малопридатним для шпигунських цілей та несанкціонованого застосування.

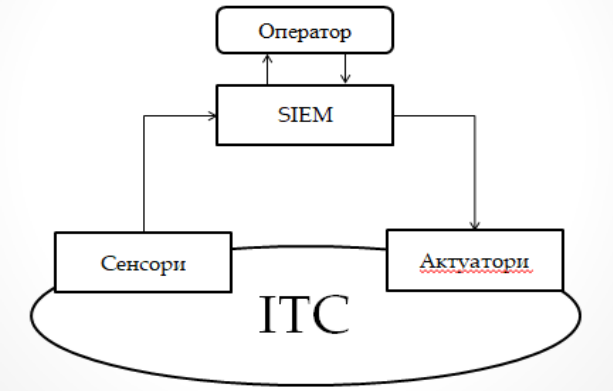

Рис. 1. Схема застосування SIEM з активним оператором

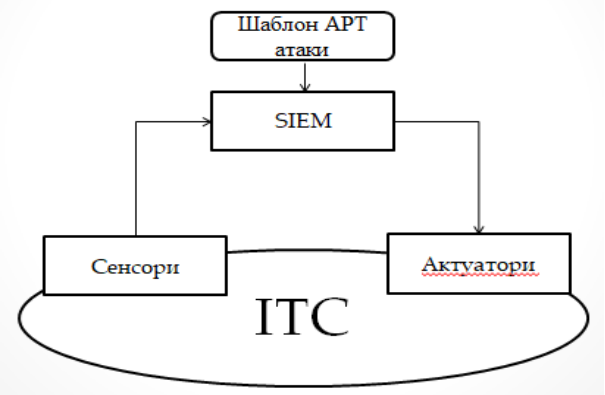

Рис. 2. Схема застосування SIEM з використанням шаблону APT атаки

Застосування програмного забезпечення для моніторингу дозволяє адміністратору безпеки:

- визначати (локалізувати) всі випадки спроб несанкціонованого доступу до конфіденційної інформації з точним зазначенням часу та місця, з якого така спроба здійснювалася;
- виявляти факти несанкціонованого встановлення програмного забезпечення;
- контролювати використання комп'ютерів в неробочий час та виявляти мету їх використання;
- визначати всі випадки несанкціонованого використання модемів в локальній мережі шляхом аналізу фактів запуску несанкціоновано встановлених додатків;
- отримувати достовірну інформацію, на підставі якої буде модифікуватися політика інформаційної безпеки;

- контролювати доступ до серверів та персональних комп'ютерів;
- проводити аудит інформаційної безпеки;
- досліджувати комп'ютерні інциденти.

Застосування "програм-шпигунів" дозволяє зловмисникові:

- перехоплювати інформацію;
- здійснювати шпигунство;
- отримувати доступ до систем криптографії – відкритих і закритих ключів, паролів.

"Продукти-шпигуни" являють собою серйозну загрозу захисту інформаційно-комунікаційних систем.

Одна з найбільш небезпечних особливостей всіх "програм-шпигунів" і апаратних пристроїв – кейлоггерів – реєстрація натискань клавіш користувачем з метою контролю його активності. Коли користувач набирає на клавіатурі пароль, кейлоггер записує кожне натискання клавіш. Крім цього, сучасні "програми-шпигуни" дозволяють захоплювати текст з вікон додатків і робити скріншоти екрану чи окремих вікон. Іншими словами, "програма-шпигун" може перехопити текст з документа, навіть якщо користувач його не набирав з клавіатури, а просто відкрив та переглянув файл.

Програмні кейлоггери (keyloggers) належать до тієї групи програмних продуктів, які здійснюють контроль за діяльністю користувача ПК.

Спочатку програмні продукти цього типу призначалися виключно для запису інформації про натискання клавіш клавіатури, в тому числі і системних, в спеціалізований журнал реєстрації (Log-файл), який згодом вивчався користувачем, що встановив цю програму. Log-файл може відправлятися по мережі на мережевий диск, ftp сервер, на Email тощо. Останнім часом програмні кейлоггери виконують багато додаткових функцій – перехоплення інформації з вікон, перехоплення кліків миші, "фотографування" знімків екрану, ведення обліку всіх отриманих та відправлених Email, моніторинг файлової активності, моніторинг системного реєстру, перехоплення звуку з мікрофона і відеозображення з веб-камери, тощо.

Кейлоггери можуть бути вбудовані в комерційні, безкоштовні і умовно-безкоштовні програми, троянські програми, віруси і хробаки. При цьому нерідко для поширення хробаків використовується широко відома вразливість IFrame браузера Microsoft Internet Explorer, яка дозволяє запускати довільний код на комп'ютері користувача при простому перегляді HTML документа в браузері або поштовому клієнті Outlook.

Апаратні кейлоггери (hardware keylogger) являють собою мініатюрні пристрої, що можуть бути прикріплені між клавіатурою і комп'ютером або вбудовані в саму клавіатуру. Вони реєструють всі натиснення клавіш на клавіатурі. Апаратні кейлоггери не вимагають установки будь-якої програми на комп'ютері об'єкта, щоб успішно перехоплювати всі натискання клавіш. Такий пристрій може бути таємно прикріплений до ПК об'єкта ким завгодно — колегою, прибиральницею, відвідувачем тощо. Коли апаратний кейлоггер прикріплюється, зовсім не має значення, в якому стані знаходиться комп'ютер — увімкненому або вимкненому.

Зловмисник може зняти пристрій в будь-який зручний момент, а його вміст скачати, коли йому буде зручно. Обсяги внутрішньої незалежної пам'яті даних пристроїв дозволяють записувати до 10 мільйонів натискань клавіш. Дані пристрої можуть бути виконані в будь-якому вигляді, так що навіть фахівець не в змозі іноді визначити їх наявність при проведенні аудиту.

Апаратні кейлоггери поділяються на зовнішні та внутрішні, їх відмінні риси описані нижче.

Зовнішні апаратні кейлоггери підключаються між звичайною клавіатурою ПК і комп'ютером і реєструють кожне натискання клавіш. Для роботи їм не потрібні батареї, встановлені програми, вони можуть працювати на будь-якому ПК. Зловмисник може підключити їх до одного комп'ютера, щоб записати інформацію, а потім, при необхідності, підключити до іншого, щоб відтворити її.

Найскладніше виявити (та знешкодити) внутрішній апаратний кейлоггер, у якого апаратний модуль перехоплення натискань клавіш вбудований в корпус клавіатури.

Для виявлення і видалення моніторингових програмних продуктів, які можуть бути встановлені без відома користувача ПК, в даний час використовуються програми різних типів, які забезпечують більш-менш ефективний захист виключно тільки проти відомих "програм-шпигунів" за допомогою сигнатурного аналізу. Для ефективної роботи програм даного типу необхідно отримати код "програми-шпигуна", виділити з неї сигнатуру і включити дану сигнатуру в свою базу. При оновленні сигнатурної бази користувачі отримують можливість боротися з даним варіантом "програми-шпигуна". За таким принципом працюють багато антивірусних програм.

Але є й інша група програм-шпигунів, яка найбільш небезпечна для будь-яких автоматизованих систем – це невідомі "програми-шпигуни". Вони підрозділяються на п'яти типів.

1. "Програми-шпигуни", що розробляються під егідою урядових організацій.

2. "Програми-шпигуни", які можуть створюватися розробниками різних операційних систем і включатися ними до складу ядра операційної системи.

3. "Програми-шпигуни", які розроблені для вирішення конкретного завдання, пов'язаного з викраденням критичної інформації з цільового комп'ютера.

4. Корпоративні програмні продукти, які дуже рідко вносяться в сигнатурні бази..

5. "Програми-шпигуни", що представляють собою keylogging модулі, що включаються до складу програм-вірусів. До внесення сигнатурних даних в вірусну базу дані модулі є невідомими.

Інформація про "програми-шпигуни" першого і третього типу, як правило ніде не опубліковується, і, відповідно, їх код не може бути внесений в сигнатурні бази, тому вони не можуть виявлятися ніякими програмними продуктами, які використовують сигнатурний аналіз.

Інформація про програми-шпигуни другого типу ніде не опубліковується, даний код працює на рівні ядра операційної системи і, відповідно, вони не можуть виявлятися ніякими додатками.

Інформація про "програми-шпигуни" четвертого типу вноситься в сигнатурні бази дуже рідко. Але навіть якщо додати такі програми в сигнатурні бази, то деактивувати, а, тим більше, видалити їх часто неможливо без руйнування операційної системи. Вони не мають своїх процесів, а маскуються у вигляді потоків у системні процеси, можуть працювати тільки з оперативною пам'яттю комп'ютера і не працювати з жорстким диском, вони мають режими контролю цілісності і самовідновлення після збоїв.

Інформація про "програми-шпигуни" п'ятого типу вноситься в сигнатурні бази через кілька годин або днів після початку відповідної вірусної атаки. За цей час конфіденційна інформація користувача персонального комп'ютера вже може бути вкрадена і відіслана в мережу Інтернет на заздалегідь підготовлену зловмисником адресу.

Ніякі програмні продукти не в змозі визначити наявність встановлених апаратних пристроїв, які забезпечують перехоплення натискань клавіатури користувачем ПК.

Сьогодні існує тільки два методи протидії апаратним кейлоггерам при роботі на ПК: фізичний пошук та усунення кейлоггера; використання віртуальних клавіатур для введення особливо важливої інформації (паролі, коди доступу, PIN коди, тощо).

Висновки

У статті запропоновано методику виявлення несанкціонованих обчислювальних процесів інформаційно-телекомунікаційних систем. В якості тестування методики використано програмні та апаратні кейлоггери. Проблема перехоплення інформації за допомогою кейлоггерів стоїть досить гостро. У світі існують сотні подібних програм, які можуть бути несанкціоновано встановлені без відома користувача чи адміністратора ПК. Отже, застосування комплексного підходу, який дозволить відрізнити санкціоновані засоби моніторингу від шкідливого ПЗ, дозволить захистити інформаційно-телекомунікаційні системи від використання кейлоггерів, що дозволить зменшити негативні наслідки від APT атак.

Подальші дослідження доцільно направити на удосконалення методів виявлення несанкціонованих обчислювальних процесів інформаційно-телекомунікаційних систем.

СПИСОК ЛІТЕРАТУРИ

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. // Департамент спеціальних телекомунікаційних системі захисту інформації Служби безпеки України. Київ, 1999/
2. "2001 AMA Survey: WorkplaceMonitoring & Surveillance: Summary of Key Findings" American Management Association. http://www.amanet.org/research/pdfs/ems_short2001.pdp
3. "Computer And Internet Surveillance in the Workplace:Rough Notes". Andrew Schulman, Chief Researcher, Privacy Foundation, US, 2001-2002http://www.sonic.net/~undoc/survtech.htm
4. "The Extent of Systematic Monitoring of Employee E-mail and InternetUse" AndrewSchulman, ChiefResearcher, PrivacyFoundation, US, 2001-2002. http://www.sonic.net/~undoc/extent.htm
5. Н.Д. Красноступ, Д.В. Кудин. Шпионские программы и новейшие методы защиты от них. http://bozza.ru/art-75/html.
6. Яковів І.Б., Дорошенко Д.В. Аналіз моделей APT-атак та методів їх застосування. Безпека інформації в інформаційно-телекомунікаційних системах: матеріали XX МНПК, 22-24 травня 2018 р. Київ, 2018. С. 74-75.
7. Яковів І.Б., "Кібернетична модель APT атаки", Information Technology and Security, vol. 6, iss. 1, pp. 46-58, 2018.
8. Дорошенко Д.В. Методика визначення та реєстрації актуальних обчислювальних процесів персонального комп'ютера на базі ОС Windows. Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання: матеріали НПК, 19-20 листопада 2019 р. : тези доповіді. Київ, 2019. С. 58-59
9. Яковів І.Б.. Базова модель інформаційних процесів та поведінки системи кіберзахисту. *Information Technology and Security*. 2019. Vol. 7, Iss. 2 (13). P. 183–196.

Received (Надійшла) 18.03.2021
Accepted for publication (Прийнята до друку) 19.05.2021

The methods of detection unauthorized computer processes of information and telecommunication systems

Denys Doroshenko

Abstract. The article proposes a method for detecting unauthorized computational processes of information and telecommunication systems. Existing APT attack detection technologies are based on multi-level analysis procedures for a large array of data on various current events in ITS. This data is collected in electronic event logs. Obviously, the APT attack model should be able to link events in time and space. Complexes of programs that fill journals with information and implement automated technologies for their analysis are known as SIEM systems. In turn, automated event analysis technologies are based on attack models. An APT attack pattern is a set of interrelated events. Comparison of such a template and current events is the essence of the evaluation process within SIEM. The main task of the methodology is to automate the process of detecting unauthorized actions, deciding on the presence of an APT attack, and implementing methods of protection against it. The basis of the APT attack is a set of actions that are implemented in various components of ITS over a long period of time. From the standpoint of security policy, such events may be legal in nature. Software and hardware designed for covert surveillance of users of information and telecommunications systems are considered. Authorized monitoring software products are used by security administrators of information and telecommunication systems to ensure monitoring. The application for covert monitoring of active processes of information and telecommunication systems is considered in detail. It is proposed to use software and hardware keyloggers as an example of an unauthorized computational process. Methods of protection against them are described in detail. The obtained results should be used to improve methods for detecting unauthorized computing processes of information and telecommunications systems.

Keywords: APT; SIEM; key logger; information and telecommunication system.