Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Смоляк
Дмитрий Сергеевич

Система мониторинга событий информационной безопасности корпоративной сети

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 "Методы и системы защиты информации, информационная безопасность”

_____

Научный руководитель
Пулко Татьяна Александровна
кандидат технических наук, доцент

_____

Минск 2016

ВВЕДЕНИЕ

Современные информационные системы включают большое число различных устройств и прикладных систем, таких, как маршрутизаторы, межсетевые экраны, операционные системы, системы управления базами данных, антивирусные программные средства, системы передачи сообщений и т.д (далее – источники событий). Источники событий порождают записи аудита (сообщения) в различных форматах. Некоторые источники событий ведут файлы журналов аудита, некоторые используют базы данных для хранения записей аудита. Число событий только на устройствах систем информационной безопасности (например, межсетевых экранах) может превышать несколько миллионов в сутки. Для получения реального представления об уровне информационной безопасности в информационной системе эта информация должна постоянно накапливаться и анализироваться. Анализ полученных данных вручную без применения автоматизированных систем представляет собой практически невыполнимую задачу. Сбор, сравнение и анализ всех данных от многочисленных независимых источников событий занимают значительное время и требуют специальных исследований. Для автоматизации решения даных задач используются системы мониторинга событий информационной безопасности.

Одной из важнейших задач мониторинга событий безопасности является обнаружение атак на рабочие станции пользователей с помощью вредоносного программного обеспечения. Своевременное обнаружение подобного рода атак позволяет сократить время реагирования на данные атаки и предотвратить возможный ущерб от их реализации. В качестве меры противодействия обнаружению злоумышленники зачастую тестируют разработанное ими вредоносное программное обеспечение на предмет обнаружения антивирусными средствами и дорабатывают его для повышения скрытности своего присутствия в системе. В результате этого вредоносное программное обеспечение остается незаметным для антивирусного программного

обеспечения и пытается замаскировать свою деятельность под видом легитимной работы операционной системы. Одним из распространенных способов маскирования является имитация ключевых процессов операционной системы, т.е. процессов которые выполняют основные функции операционной системы и запускается незадолго после ее загрузки.

В связи с этим возникает задача обнаружения аномалий запуска процессов операционных систем рабочих станций для обнаружения вредоносного программного обеспечения, которое использует механизмы маскирования собственного присутствия.

В данной магистерской диссертации рассмотрены способы обнаружения аномалий запуска процессов операционной системы Windows с помощью утилиты Microsoft Sysmon, позволяющей фиксировать в журнале аудита операционной системы Windows события запуска процессов на ранних этапах загрузки операционной системы, а также системы мониторинга событий информационной безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 5.2 «Системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и систем, их информационная безопасность» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 – 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в исследовании возможности применения систем мониторинга событий информационной безопасности для обнаружения аномалий запуска процессов операционной системы Windows.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать возможность применения системы мониторинга событий информационной безопасности для обнаружения аномалий запуска процессов операционной системы Wndows.

2. Определить эталонные характеристики и описание для перечня ключевых процессов операционной системы Windows.

3. Определить способы обнаружения аномалий запуска процессов операционной системы Windows с помощью системы мониторинга событий информационной безопасности.

4. Провести апробацию предложенных способов обнаружения.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XIII Белорусско-российской научно-технической конференции “Технические средства защиты информации” (Минск, 2015) и Международной научно-практической конференции "Проблемы удаленного мониторинга техногенных объектов" (Минск, 2015).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 1 статья в сборнике материалов конференций, 1 статья в научном журнале.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приводится оценка современного состояния задачи мониторинга событий информационной безопасности и использования их для обнаружения аномалий запуска процессов операционной системы Windows, формулируются решаемые в магистерской диссертации задачи.

В первой главе приводится описание систем мониторинга событий информационной безопасности и решаемых ими задач, приводится сравнение систем мониторинга событий информационной безопасности, приводится перечень систем мониторинга, присутствующих на рынке Республики Беларусь.

Во второй главе приводится обоснование выбора и обзор архитектуры системы мониторинга событий информационной безопасности HP ArcSight ESM, обзор утилиты Microsoft Sysmon, используемой для детального журналирования запуска процессов операционной системы Windows.

В третьей главе приводятся известные способы обнаружения аномалий работы операционных систем, формулируется задача обнаружения аномалий работы процессов с помощью системы мониторинга событий информационной безопасности, формулируется методика проведения исследования, приводится схема макета, используемого для проведения исследования. Приводятся конфигурационные параметры элементов макета, формулируются эталонные характеристики для перечня процессов операционной системы Windows.

В четвертой главе происходит апробация методики обнаружения аномалий работы процессов операционной системы Windows с помощью системы мониторинга событий информационной безопасности HP ArcSight ESM.

В заключении приводятся основные результаты, полученные в ходе выполненных исследований.

ЗАКЛЮЧЕНИЕ

Определены и описаны характеристики ключевых процессов операционной системы Microsoft Windows, позволяющие использовать их в качестве параметров для обнаружения аномалий. Были сформулированы методы обнаружения аномалий запуска процессов с помощью системы мониторинга событий информационной безопасности HP ArcSight ESM на основе событий утилиты Microsoft Sysmon. Был разработан метод синтаксического анализа событий Microsoft Sysmon с помощью модуля сбора событий ArcSight SmartConnector, созданы правила корреляции, позволяющие оперативно получать уведомления о происходящих нарушениях информационной безопасности.

Предложенные в данной магистерской диссертации способы интеграции системы мониторинга событий информационной безопасности с утилитой детализированного журналирования запуска процессов Microsoft Sysmon могут быть использованы для построения систем защиты информации любых предприятий, требованием для которых является обеспечение мониторинга и контроля аномалий работы операционных систем. Описанные характеристики запуска ключевых процессов операционной системы Windows и способы обнаружения аномалий в них могут быть использованы для реализации в средствах защиты информации рабочих станций пользователей.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Смоляк Д.С. Анализ необходимости внедрения систем централизованного хранения и анализа журналов аудита / Д.С. Смоляк, Т.А. Пулко // XIII Белорусско-российская научно-техническая конференция “Технические средства защиты информации”: Тезисы докладов – Минск, 2015 – С.45 – 46.

2-А. Смоляк Д.С. Мониторинг событий информационной безопасности техногенных объектов / Д.С. Смоляк, Т.А. Пулко // Доклады БГУИР – №7 – С.122 – 125.