

УДК 004.75

## МОНИТОРИНГ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕХНОГЕННЫХ ОБЪЕКТОВ

Д.С. СМОЛЯК, Т.А. ПУЛКО

*Белорусский государственный университет информатики и радиоэлектроники  
П. Бровка, 6, Минск, 220013, Беларусь*

*Поступила в редакцию 27 октября 2015*

Современные техногенные объекты являются одними из критически важных объектов информационной безопасности. Вторжения в информационные системы техногенных объектов могут привести к нарушению технологических процессов, которые могут повлечь за собой серьезные последствия. Мониторинг и корреляция событий информационной безопасности позволяет сократить время обнаружения и реагирования на инциденты информационной безопасности.

*Ключевые слова:* событие информационной безопасности, компьютерная сеть, корреляция событий информационной безопасности, процесс операционной системы.

### Введение

Современные техногенные объекты включают в себя множество устройств, используемых в корпоративных информационных системах, а также устройства и приложения, специфичные для технологических процессов. Использование систем централизованного мониторинга событий информационной безопасности информационных систем позволяет получить информацию о состоянии безопасности информационной системы в единой точке для оперативного обнаружения и реагирования на возможные инциденты информационной безопасности.

### Теоретический анализ

Информационные системы включают множество различных устройств и прикладных систем, таких, как маршрутизаторы, межсетевые экраны, операционные системы, системы управления базами данных, антивирусные программные средства, системы передачи сообщений, а также специфичные для каждой системы программные и аппаратные средства (далее – источники событий). Формат аудита каждого из видов устройств имеет различия, что в конечном счете порождает трудности для анализа состояния каждого из источников событий.

Количество событий, создаваемых устройствами в течение суток, может превышать миллионы. 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 решения этих задач используются системы централизованного мониторинга событий безопасности [1].

Благодаря использованию систем мониторинга событий информационной безопасности можно в единой точке собрать информацию от множества устройств информационной системы предприятия, проводить анализ этих событий и задавать правила оповещения в случае возникновения подозрительных ситуаций. Сопоставление событий от различных устройств, а также систематизация информационных потоков внутри информационных систем позволяет обнаруживать такие инциденты безопасности как наличие информационных потоков между

корпоративной и технологической сетями техногенных объектов, возникновение подключений к сети Интернет из сегментов сети, которые должны быть изолированы, возникновение аномалий в процессах операционных систем операторов технологических процессов. Использование журналов аудита систем разграничения доступа и сетевых устройств позволяет определять отклонения от шаблонного поведения в случае возникновения вторжений и распространения атаки по компьютерной сети техногенного объекта [2].

Задачу обнаружения аномалий в процессах операционной системы Windows, используемой в качестве операционной системы операторов технологических процессов можно реализовать с помощью использования программного обеспечения Sysmon [3]. Sysmon (System Monitor) – системная служба, которая после установки ведет непрерывный мониторинг и запись логов. Служба загружается вместе с операционной системой и позволяет тщательно изучить состояние операционной системы, найти следы вредоносной или подозрительной активности, а также понять, какие конкретно методы применяет злоумышленник или вредоносная программа.

### Методика

Для обнаружения аномалии в работе процессов операционной системы Microsoft Windows используется следующая методика (на примере процесса операционной системы explorer.exe):

- 1) определить эталонное состояние работы процесса операционной системы explorer.exe (в качестве эталонного состояния работы процесса explorer.exe считается такое, при котором данный процесс не осуществляет сетевых соединений);
- 2) установить и настроить программное обеспечение Microsoft Sysmon для регистрации событий запуска процессов и установления сетевых соединений;
- 3) установить и настроить модуль сбора событий информационной безопасности HP ArcSight FlexConnector;
- 4) настроить правило корреляции событий безопасности программного обеспечения HP ArcSight ESM с целью обнаружения аномалии работы процесса операционной системы Windows;
- 5) с помощью программного обеспечения Metasploit произвести эксплуатацию уязвимостей операционной системы, результатом которой будет являться аномалия работы процесса explorer.exe операционной системы Windows;
- 6) обнаружить аномалию в окне просмотра результатов срабатывания правил корреляции HP ArcSight ESM.

### Экспериментальная часть

Произведена эксплуатация уязвимости операционной системы Windows с помощью программного обеспечения Metasploit (рис. 1).

```
show op msf exploit(payload_inject) > show options
Module options (exploit/windows/local/payload_inject):
-----
Name      Current Setting  Required  Description
-----
NEWPROCESS false           no       New notepad.exe to inject to
PID       2632            no       Process Identifier to inject of process to inject payload.
SESSION   1               yes      The session to run this module on.

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC process         yes      Exit technique (accepted: seh, thread, process, none)
LHOST    192.168.1.104   yes      The listen address
LPORT    4444            yes      The listen port

Exploit target:
-----
Id  Name
--  ---
0   Windows

msf exploit(payload_inject) > exploit
[*] Running module against WIN7-CLIENT
[*] Preparing 'windows/x64/meterpreter/reverse_tcp' for PID 2632
[*] Sending stage (972208 bytes) to 192.168.11.21
[*] Meterpreter session 2 opened (192.168.1.104:4444 -> 192.168.11.21:49222) at 2014-08-09 21:31:13 -0400
msf exploit(payload_inject) >
```

Рис. 1. Работа программного обеспечения Metasploit

В результате изменения в работе процесса операционной системы Windows explorer.exe зафиксированы приложением Sysmon, о чем свидетельствует запись в журнале аудита (рис. 2).

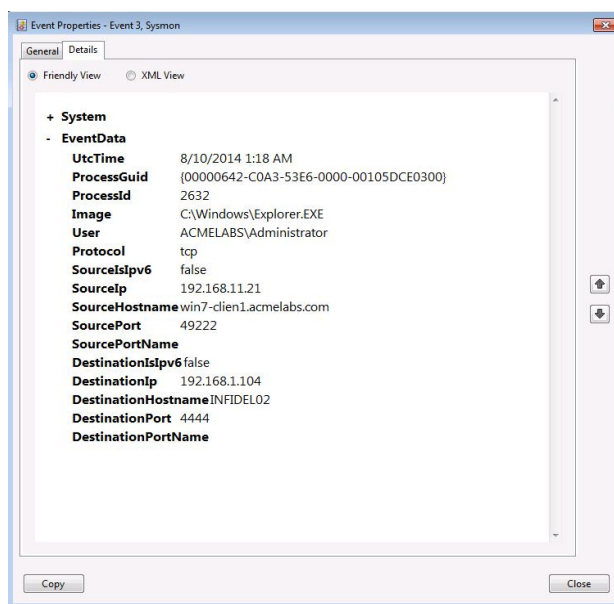


Рис. 2. Регистрация изменений процесса explorer.exe

Результат работы приложения Sysmon успешно отправлен в систему мониторинга HP ArcSight ESM, которая по заданному критерию (недопустимое состояние процесса explorer.exe) произвела срабатывание правила корреляции и оповещение на экране аналитика безопасности (рис. 3).

| Radar  |              |          |               |                |
|--|--------------|----------|---------------|----------------|
| Name   | File Name    | Priority | Device Vendor | Device Product |
| Недопустимое состояние процесса explorer.exe | explorer.exe | 8        | Microsoft     | Sysmon         |
| Недопустимое состояние процесса explorer.exe | explorer.exe | 8        | Microsoft     | Sysmon         |

Рис. 3. Срабатывание правил корреляции системы мониторинга

## Результаты

С помощью программного обеспечения Microsoft Sysmon и правила корреляции программного обеспечения HP ArcSight ESM удалось обнаружить аномалию в запуске процесса операционной системы Windows 7 (появление сетевого соединения для процесса, который не должен обладать такой возможностью).

## Заключение

На примере одного из ключевых процессов операционной системы Windows рассмотрен способ обнаружения аномалии операционной системы с использованием системы централизованного мониторинга и корреляции событий информационной безопасности.

Централизация мониторинга событий безопасности является важным процессом в управлении информационной безопасностью техногенного объекта. Возможность регистрации событий от множества устройств в единой точке и настроенные правила корреляции событий позволяют обнаружить инциденты и своевременно регистрировать на них.

# MONITORING OF INFORMATION SECURITY EVENTS IN TECHNOGENIC OBJECTS

D.S. SMOLIAK, T.A. PULKO

## Abstract

Modern technologic objects are among the critical objects of information security. Intrusions into technologic objects' information systems can lead to a violation of technological processes that can cause serious consequences. Monitoring and correlation of information security events allows to reduce time of detection and response to information security incidents.

## Список литературы

1. Guide to Computer Security Log Management [Электронный ресурс]. – Режим доступа: <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>. – Дата доступа: 25.10.2015.
2. Guide to Industrial Control Systems (ICS) Security [Электронный ресурс]. – Режим доступа: <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>. – Дата доступа: 25.10.2015.
3. Sysmon v3.1 [Электронный ресурс]. – Режим доступа: <https://technet.microsoft.com/en-us/sysinternals/dn798348>. – Дата доступа: 25.10.2015.