## Подготовка 1

Предоставить физический доступ к исследуемой системе компьютерным криминалистам.

Изучить детали функционирования сети и процессов в нормальных условиях. Заранее подготовить и держать в доступном месте информацию с деталями стандартного использования портов. Наличие этой информации позволит отследить характер и природу изменений на момент инцидента.

В случае необходимости, обратиться к эксперту по Windows ОС.

## Обнаружение 2

**Основные признаки присутствия вредоноса в системе**

- Регулярные предупреждения антивируса; невозможность актуализации сигнатур, невозможность запуска или внезапная остановка работы антивируса. .
- Аномальная активность жесткого диска: диск совершает ресурсозатратные операции в необычное время.
- Аномально медленная работа компьютера.
- Аномальная сетевая активность: Интернет связь стала медленной или очень медленной.
- Беспричинная перезагрузка компьютера.
- Неожиданный отказ в работе некоторых приложений.
- Появление сторонних поп-ап окошек браузера при просмотре веб-страниц.
- Появление вашего IP-адреса в черных email листах (например SORBS, Spamhaus, Barracuda, и т.п. ).
- Ваши адресаты жалуются на получения от вас нехарактерных имэйлов или мгновенных сообщений, похожих на спам.

Для выполнения действий, указанных далее рекомендуется использование инструментов, присутствующих в Windows по умолчанию. Авторизованные пользователи также могут использовать **Sysinternals** Troubleshooting Utilities.

## Обнаружение 2

**Нехарактерные учетные записи**

Проверить подозрительные учетные записи, в особенности в группе Administrators:
*C:\> lusrmgr.msc*

**Подозрительные файлы**

- Проверить наличие необычно крупных файлов (>10Мб).
- Проверить файлы, недавно добавленные в системные папки, особенно в C:\WINDOWS\system32.
- Проверить папки со скрытыми атрибутами:
*C:\> dir /S /A:H*

**Подозрительные записи в реестре**

Обратить особое внимание на необычные ключи, особенно в “загрузочных” разделах реестра:
*HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
*HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce*
*HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx*
*HKLM\Software\Microsoft\Windows NT\CurrentVersion \ Winlogon*
Аналогично для HKCU

**Подозрительные процессы и сервисы**

- Проверить наличие подозрительных запущенные процессов, в особенности “SYSTEM” и “ADMINISTRATOR”:
*C:\>taskmgr.exe или tlisk/tasklist(в зависимости от версии ОС)*
*Возможно использование psexplorer.*
- Проверить наличие запущенных нестандартных сетевых сервисов
*C:\> services.msc*
*C:\> net start*
Сравнить со стандартными сетевыми сервисами

**Подозрительная сетевая активность**

- Проверить общие каталоги и их причастность к стандартным сетевым процессам:
*C:\> net view \\127.0.0.0*
- Проверить открытые сессии:
*C:\> net session*
- Проверить сессии, открытые с другими системами:
*C:\> net use*
- Проверить подозрительные соединения NetBIOS:
*C:\> nbtstat –S*

## Обнаружение 2

- Проверить подозрительную активность на системных TCP/IP портах:
*C:\> netstat –na 5* (пятисекундная актуализация)

Использовать –о флажок в Windows XP/2003 для идентификации владельца процесса:
*C:\> netstat –nao 5*

- Использовать анализаторы сетевого траффика (Wireshark, tcpdump) для обнаружения подозрительный попыток соединений с удаленных систем. Для провоцирования вредоноса рекомендуется параллельное просматривание потенциально привлекательных для malware веб ресурсов, например авторизационных банковских порталов и корреляция с действий с изменением сетевого поведения процессов.
Сравнить со стандартной сетевой активностью системы.

**Подозрительные автоматизированные задания**

- Проверить подозрительные автоматизированные задания: *C:\> at;* в Windows 2003/XP : *C:\> schtasks*
- Проверить пользовательские папки autostart:
*C:\Documents and Settings\user\Start Menu\Programs\Startup*
*C:\WinNT\Profiles\user\Start Menu\Programs\Startup*

**Подозрительные записи системного журнала**

- Проверить в логах:
*C:\> eventvwr.msc*
- Проверить на наличие следующих событий:
*“Event log service was stopped”*
*“Windows File Protection is not active”*
*“The protected System file <name> was not restored to its original”*
*“Telnet Service has started successfully”*
- Проверить журналы файервола на наличие подозрительных записей.
- Для обнаружения malware также возможно использование актуализованного антивируса; данный способ, однако, может уничтожить улики.

Отсутствие найденных улик не означает безопасность системы. Так, присутствие руткита может модифицировать результаты вышеописанных команд. Рекомендуется продолжение расследования методами компьютерной криминалистики на базе сделанной побитовой копии исследуемой системы. Возможно использование специализированного ПО: EnCase, X-Ways, FTK и др.

## Сдерживание 3

Физически отключить и изолировать инфицированную систему от сети во избежание распространения вредоноса и усугубления последствий от его действий, таких как рассылка спама, использования в рамках ботсети для DDoS атак, использование инфицированной системы для хранения нелегальных данных и др.

Отправить идентифицированные вредоносные файлы в обслуживающий вас CERT. Запросить дополнительной помощи у CERTa в случае, если вы неуверенны по поводу обнаруженных файлов. Занимающиеся инцидентом специалисты должны изолировать вредоносный код и разослать его в обслуживающие вашу организацию антивирусные компании. Передачу вредоноса лучше осуществлять в виде защищенного паролем архива.

## Устранение 4

Загрузить инфицированную систему с Live CD и сохранить все важные данные на внешний жесткий диск. В случае необходимости, передать дать соответствующее задание технической команде поддержки.

**Удалить вредоносные файлы и соответствующие записи реестра.**

- В зависимости от типа обнаруженного вредоноса, применить соответствующие методы и ПО, присутствующие на сайтах основных антивирусных вендоров.
- Осуществить антивирусную онлайн проверку.
- Использовать антивирусные Live CD (скачать с сайтов антивирусных компаний), для дезинфекции системы.

## Восстановление 5

- **Удостовериться в отсутствии на системных дисках руткитов MBR типа.**
- Отформатирвать диски скомпрометированной системы.
- Переустановить ОС и ПО
- Восстановить пользовательские данные за счет резервных копий.

В случае невозможности переустановки с нуля (критические системы), **заменить все подверженные компрометации файлы в особенности системные на гарантированно безопасные.**

Перезагрузить систему после всех действий по дезинфекции и **проверить еще раз полным антивирусным сканом (жесткие диски + оперативную память)**.

## После инцидента 6

**Отчет**

Написать отчет об инциденте заражения; сделать отчет доступным причастным лицам. В рамках отчета необходимо раскрыть:

- Причины инфекции
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

**Капитализация опыта**

Формализовать и задокументировать опыт, накопленный в результате управления инцидентом с целью увеличения эффективности будущих действий.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

# Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #7

## Обнаружение вредоноса на Windows

Живой анализ зараженной системы

Автор IRM: CERT SG
Версия IRM: 1.3 (RU)

## Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

**В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.**

## Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

**IRM предоставляет детальную информацию по каждой из фаз.**