Подготовка 1

- Предоставить компьютерным криминалистам физический доступ к атакуемой системе. Физический доступ предпочтителен удаленному по причине меньшей вероятности обнаружения ваших ответных действий хакерами (например, посредством установки сетевого анализатора пакетов).
- Выполнить побитовую копию диска атакуемой системы; она может понадобиться для криминалистических и судопроизводственных нужд.
- Наличие физического доступа также может быть использовано для отсоединения атакуемой системы от внешних сетей.
- Изучить детали функционирования сети / системы в нормальных условиях. Заранее подготовить, задокументировать и держать данную информацию в надежном месте. Документация должна содержать детали стандартного использования портов для возможности отследить характер и природу изменений.
- Изучить детали стандартной работы типовых сервисов на производственных машинах и серверах. В случае необходимости, обратиться к эксперту по Windows ОС. Заранее подготовить и задокументировать эту информацию.

В случае использования унифицированных мастер образов для установки на корпоративные системы, подробно задокументируйте стандартные процессы, сервисы и ПО. При сверении, необходимо подвергнуть проверке все обнаруженные нестандартные компоненты.

Чем лучше знания о стандартной работе ваших ресурсов, тем больше шансов на обнаружение аномалий.

Обнаружение 2

Для обнаружения аномалий рекомендуется использование **Sysinternals** Troubleshooting Utilities.

- **Нестандартные учетные записи**

Проверить подозрительные учетные записи, в особенности в группе Administrators:
C:\> lusrmgr.msc
или
C:\> net localgroup administrators или *net localgroup administrateurs (сверьтесь с локализацией ОС)*

- **Необычные файлы**

- Нестандартно большие файлы (>5Мб). Их присутствие может быть индикатором компрометации инспектируемой системы;
- Файлы, недавно добавленные в системные папки, особенно в C:\WINDOWS\system32;
- Файлы со скрытыми (“hidden”) аттрибутами:
C:\> dir /S /A:H
“*windirstat*”.

- **Необычные записи в реестре Windows**

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
Возможно использование ***HiJackThis***. (Also have a look in your Startup folder)

- **Необычные процессы и сервисы**

Проверить запущенные процессы на предмет наличия необычных, в особенности процессов “SYSTEM” и “ADMINISTRATOR”:
C:\> taskmgr.exe
(или *tlisk*, *tasklist* в соответствии с версией ОС)
Возможно использование “*psexplorer*”.

- **Проверить папки autostart**

C:\Documents and Settings\user\Start Menu\Programs\Startup
C:\WinNT\Profiles\user\Start Menu\Programs\Startup

- **Проверить на наличие запущенных нестандартных сетевых сервисов**

C:\> services.msc
C:\> net start

- **Необычная сетевая активность**

- Проверить общие каталоги и их причастность к стандартному функционированию системы:
C:\> net view \\127.0.0.1

Возможно использование “*tcpview*”

Обнаружение 2

- проверить открытые сессии:
C:\> net session

- проверить сессии, открытые машиной с другими системами:
C:\> net use

- проверить подозрительные соединения NetBIOS:
C:\> nbtstat –S

- проверить подозрительную активность на системных портах:
C:\> netstat –na 5
(5 – актуализация каждые 5 секунд)
Для Windows XP/2003 использовать флаг –o для идентификации владельца процесса:
C:\> netstat –nao 5
Возможно использование *“fport”*.

- **Необычные автоматизированные задания**

Проверить автоматизированные задания на наличие подозрительных:
C:\> at
На Windows 2003/XP: *C:\> schtasks*

- **Необычные записи системного журнала**

Проверить системный журнал на наличие нестандартных записей:
C:\> *eventvwr.msc*
Возможно использование “*Event Log Viewer*”.

-Проверить события, затрагивающие работу файрвола, антивируса, защиты файлов, а также подозрительные вновь-созданные сервисы.

-Обратить особое внимание на большое количество неудачных попыток авторизации и заблокированные учетные записи.

-Проанализировать логи файрвола на предмет выявления фактов подозрительной активности.

- **Проверка на наличие Руткитов**

Возможно использование “*Rootkit Revealer*”, “*Rootkit Hooker*”, “*Ice Sword*”, “*Rk Detector*”, “*SysInspector*” или “*Rootkit Buster*”.
Предпочтительно использование нескольких програм.

- **Проверка на вредоносное ПО**

Провести полную проверку диска системы антивирусом с обновленной базой сигнатур. При возможности использовать несколько антивирусных решений.

Сдерживание 3

Если затронутая система критична для производственного процесса и не может быть отключена, создать резервную копию важных данных – на случай деструктивного поведения хакера и попыток удаления содержимого системы. Также рекомендуется создать копию системной памяти для дальнейшего анализа. Возможно использование DumpIt, Memoryze, Win32dd Win64dd, Volatility.

Если система не критична для производственного процесса, отключить подачу электрического питания. Если это лаптоп, притопить кнопку питания в течение нескольких секунд пока система не отключится.

Если “живой” анализ системы не дает результата, необходимо приступить к расследованию по горячим следам в офлайн режиме, считая систему по умолчанию скомпрометированной.

Необходимо осуществить **побитовуя копию** содержимого диска инспектируемой системы на внешний носитель. Возможно использования *dd, ddrescue, FTK Imager,* CloneZilla, Encase, X-Ways или иного специализированного криминалистического ПО или оборудования.

Найти доказательства действий хакера:

- **Найти файлы, использованные злоумышленником**, включая удаленные (с использованием специализированного ПО) и установить их функционал в рамках данного использования. Эти сведения необходимы для оценки уровня угрозы.
- **Проверить файлы с недавним обращением.**
- **Проверить общие сетевые ресурсы** на предмет распространения через них вредоносного ПО.
- **Установить каким образом злоумышленник получил доступ в систему**, рассмотрев все возможные варианты. Если не найдено доказательств вторжения извне, возможно был использован прямой физический доступ или помощь инсайдера.
- **Обновить ОС и ПО**: атакующая сторона могла воспользоваться уязвимостями.

Устранение 4

В случае компрометации системы:

- Временно заблокировать доступ ко всем учетным записям, причастным к инциденту.
- Удалить установленные злоумышленниками файлы .

Восстановление 5

Независимо от глубины проникновения хакеров и вашу осведомленность об инциденте, система остается потенциально уязвимой. **Наилучшее решение – тщательно проверив на наличие руткитов MBR, переустановить систему с нуля и применить все доступные обновления.**

В этом случае также необходимо **сменить пароли для всех учетных записей**: пароли пользователей должны состоять из 12 и более символов, включать цифры, прописные и заглавные буквы и специальные символы.

В случае невозможности переустановки с нуля (критические системы), **необходимо заменить все подверженные компрометации файлы на гарантировано безопасные** (Например: *svchost.exe*).

После инцидента 6

Отчет

Написать отчет об инциденте заражения; сделать отчет доступным членам Кризисной Группы. В рамках отчета необходимо раскрыть следующие темы:

- 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 #2

Вторжения в Windows Системы

Анализ атакуемых Windows систем

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.