Подготовка 1

- Назначить ответственных лиц из каждого вовлеченного департамента для участия в Кризисной Группе (КГ). Внести подробные координаты членов кризисной группы в контактный список и распространить между участниками.

- Убедиться в дееспособном, функциональном и актуализованном состоянии специализированного оборудования, как то антивирусы, IDS, анализаторы логов и т.п.

- Убедиться в наличии актуализованной версии картографии сети и инвентаря аппаратного оборудования.

- Выполнять регулярный мони-торинг безопасности и своевременно информировать ответственных лиц о направлениях угрозы.

- Убедиться в существовании формализованных и регулярно тестируемых процессов непрерывности производства в отношении критических объектов предприятия.

Обнаружение 2

Обнаружение заражения

Собрать, проанализировать и упорядочить информацию, поступающую из различных источников:

- Логи антивирусов
- Intrusion Detection Systems
- Подозрительные попытки подключений к серверам
- Аномально большое количество заблокированных учетных записей
- Подозрительный сетевой траффик
- Подозрительные попытки подключения к файерволам
- Увеличение количества звонков в центр поддержки
- Нехарактерная нагрузка или зависания
- Аномальное увеличение объемов исходящего почтового траффика

При обнаружении одного или нескольких из вышеперечисленных симптомов, лица, определенные на первой стадии (см. “Подготовка”) сконтактируются и, в случае необходимости, создадут Кризисную Группу.

Идентификация инфекции

Проанализировать симптомы для идентификации вредоноса, выявления векторов заражения и определения способов противодействия.

Полезная информация может быть найдена в:

- Бюллетенях CERT/CSIRT
- Сторонних службах поддержки (Microsoft, антивирусные вендоры, и т.д.)
- Тематических ресурсах (Secunia, и т.д.)

Оповестить начальника отдела информационной безопасности. Оповестить CERT/CSIRT/IRT.

Определить периметр распространения вредоноса и уровень его воздействия на производственные процессы.

Сдерживание 3

Кризисная Группа должна выполнить следующие действия:

- Изолировать инфицированный сегмент сети от Интернета и других сетей.
- В случае невозможности изоляции критического производственного траффика, разрешить его, предварительно убедившись в невозможности распространения инфекции через данный вектор или найти обходные пути для его обеспечения.
- Нейтрализовать векторы распространения заражения. Вектором распространения может быть что угодно - от сетевого траффика до уязвимостей в ПО. Меры безопасности могут включать в себя установки патчей ПО, блокировку сетевого траффика, отключение отдельных устройств, и т.д.

Возможно использование:

- Patch deployment tools (WSUS)
- Windows GPO
- Внедрение правил файерволов
- Специальные операционные процедуры

Повторить вышеуказанные действия для каждой подсети в зоне действия вредоноса до полного предотвращения распространения заражения.

Рекомендуется осуществлять параллельный мониторинг всех действий с помощью спецсредств (антивирусная консоль, серверные логи, звонки в центр поддержки).

Необходимо держать весь процесс распространения вредоноса под четким контролем.

Мобильные устройства

Убедитесь в невозможности использования переносных компьютеров и жестких дисков, планшетов и смартфонов для распространения компьютерного червя. Блокируйте соответствующие соединения и оповестите конечных пользователей.

Устранение 4

Предпринять необходимые меры для устранения последствий

- Связаться с провайдером и удостовериться, что тот осуществляет все необходимое для восстановления контроля над ситуацией. Вот некоторые из возможных мер:
  - Фильтрация (на уровне Tier 1 или 2)
  - Traffic-scrubbing/Sinkhole/Clean-pipe
  - Blackhole маршрутизация
- В случае идентификации лиц, причастных к атаке рассмотреть возможность вовлечение правоохранительных органов. Данные действия необходимо согласовать с руководством и юридическим департаментом.

Ответственность за принятие технических мер противодействия лежит на *вашем Интернет провайдере.*

Восстановление 5

Восстановить функциональность всех сервисов

Оценить сроки отказа в обслуживании
- Убедиться в доступности затронутых сервисов.
- Убедиться в возвращении производственных инфраструктур в базовое состояние.

Обратный откат контрмер
- Вернуть базовые настройки траффика.
- Перезапустить остановленные сервисы.

Убедиться, что восстановительные меры применяются совместно с другими командами поддержки оборудования и сетей. Эффект от возвращения в базовый режим может быть непредсказуемым.

После инцидента 6

Задокументировать детали инцидента, обсудить извлеченные уроки, оптимизировать планы и процессы защиты.

- Рассмотреть возможность принятия дополнительных мер на фазе подготовки для обеспечения более эффективной и оперативной работы по управлению инцидентом.
- Формализовать условия, повлиявшие на принятие решений в подготовительной фазе.
- Оценить эффективность ваших действий по управлению инцидентов во время атаки, включая действия сотрудников и процессы передачи информации.
- Рассмотреть и наладить связи внутри организации, которые могли бы благоприятно повлиять на управление будущими инцидентами DDoS.
- В случае текущих судопроизводственных процессов, наладить тесное сотрудничество с юридическими департаментами.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

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

IRM #4

Распределенные атаки на отказ в обслуживании

Управление DDoS инцидентами

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.