Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию для оптимизации временных затрат в момент инцидента.

- Создать инвентарь всех доменов и сайтов, принадлежащих компании. Отдельным списком, выделить все транзакционные сайты компании.
- Создать инвентарь всех торговых марок и брендов, принадлежащих компании.
- Приготовить специальную веб страницу для оповещение пользователей в момент мошеннической атаки. Согласовать детали публикации страницы с вовлеченными лицами, ответственными за хостинг и функционирование сайтов компании.
- Приготовить формуляры абуз-имэйлов для заполнения и рассылки заинтересованным сторонам (хостинг провайдеры, регистраторы, операторы DNS-сервисов, вебмэйл провайдеры и т.п.). Желательно подготовить формуляры на нескольких языках. Минимально: на языке страны основной операционной деятельности компании и на английском языке.

Внутренние контакты

- Составить контактный список сотрудников, ответственных за регистрацию официальных доменных имен компании.
- Составить список сотрудников, ответственных за принятие решений по киберпреступным инцидентам и конкретно по скаму.

Внешние контакты

- Создать внутреннюю команду, занимающуюся киберпреступными инцидентами и доступную в режиме 24/7:
  - Создать легко-запоминающийся электронный адрес для принятия оповещений о фишинге и других мошенничествах, например: security@yourdomain.tld;
  - Создать веб форму - не более чем в двух кликах от лицевой страницы - для оповещения мошеннических кампаниях;
  - Создать официальный и активный твиттер команды.
- Создать подробный список контактов для контрмер:
  - Хостинг провайдеры
  - Регистраторы доменов
  - Вебмэйл провайдеры (Gmail, Yahoo, Yandex и т.п.)
- Создать и поддерживать список контактов команд CERT/CSIRT; данные команды смогут помочь в наиболее серьезных ситуациях. Контакты доступны на First.org.

Пользовательская осведомленность

Не ждите случаев мошенничества для оповещения клиентов. Повышайте пользовательскую осведомленность о разнообразных мошеннических схемах (фиктивные лотереи, наследства, благотворительные акции, кредиты, вакансии о работе, интернет аукционы и т.п.). Уведомите клиентов, что вы никогда не станете обсуждать с ними подобные предложения.

Обнаружение 2

Обнаружить случай мошенничества, определить затрагиваемый периметр, привлечь к решению компетентные стороны, собрать доказательную базу.

Обнаружение случаев онлайн мошенничества

- Регулярно отслеживать все каналы входящей информации по электронному мошенничеству (e-mail, web forms).
- Развернуть сеть спам-ловушек; собирать поступающий спам от партнерских организаций и команд безопасности.
- Организовать мониторинг специализированных веб-ресурсов, таких как aa419, PhishTank и др.
- Организовать мониторинг специализированных мэйлинг листов, RSS и Twitter фидов, в которые поступают оповещения о случаях фишинга.
- Автоматизировать процесс мониторинга на базе этих и других ресурсов таким образом, чтобы каждое обнаружение по ключевому слову автоматически направляло оповещение вовлеченному аналитику с возможностью мгновенного реагирования.
- Осуществлять регулярный мониторинг веб-логов ваших сайтов. Проверяйте на наличие подозрительных рефереров. Очень часто, последним этапом мошеннической кампании является легитимный сайт атакуемой компании.

Привлечение компетентных сторон

Оповестить сотрудников вашей компании, принимающих решение по данному типу инцидентов. Решение о возбуждении контрмер по отношению к мошенническому сайту или адресу электронной почты должно приниматься в самые кратчайшие сроки.

Сбор доказательной базы

- Создать датированную копию мошеннического сайта. Возможно использование HTTrack. Собрать каждую страницу мошеннического ресурса (глубина копирования >1). При необходимости, сделать копии экранов каждой страницы.
- Собрать копии электронных сообщений, отосланных мошенником своим жертвам. Необходимо, чтобы сообщение содержало служебные заголовки. В идеале, сохранять сообщения мошенника в общедоступных .msg или .eml форматах.

Сдерживание 3

Минимизировать эффект от атаки

- Обнародовать адрес обнаруженного мошеннического веб ресурса.

Использовать встроенный функционал оповещения о вредоносных ресурсах в Internet Explorer, Firefox, Chrome, Safari, Opera. Использовать специализированные ресурсы: AntiPhishing.ru, Phishing-Initiative.com, и т.п.

Данная мера предотвратит посещение пользователем вредоносного ресурса до его нейтрализации вашей командой безопасности.

- Добавить адрес электронной почты мошенника в черные спам листы и специализированные ресурсы, например Signal Spam или Spamcop.
- Оповестить клиентов посредством публикации страницы о текущей мошеннической кампании (см. фазу «Подготовка»).
- В случае частых скам кампаний создать и опубликовать информативный раздел, посвященный мерам пользовательской безопасности. Раздел должен содержать описания наиболее типичных форм мошеннических акций с графическими примерами и пояснениями.
- Проанализировать исходный код мошеннического ресурса.
  - Проследить куда отправляется украденная у клиентов информация: на другой веб-ресурс посредством PHP скрипта или отсылается на имейл адрес злоумышленника.
  - Установить не подкачиваются ли графические ресурсы (изображения, баннеры) используемые мошенническим ресурсом непосредственно с легитимного сайта. В этом случае возможно изменить используемые мошенником графические ресурсы для оповещения пользователей. Например, заменить центральное лого на крупную надпись «МОШЕННИЧЕСКИЙ РЕСУРС – не использовать».

Устранение 4

Ликвидировать угрозу

- Оповестить хостинг провайдера, в зоне ответственности которого находится мошеннический ресурс. Посылать оповещения необходимо по адресам контактов, указанных в Whois и на сайте хостинг компании. Постараться дозвониться до провайдера по телефону. Также эффективно использование вебчатов и формуляров оповещения о вредоносном контенте, как правило доступных на сайте хостинг провайдеров. Очень часто электронные адреса команд, ответственных за борьбу с вредоносным контентом на серверах провайдера выглядят как abuse@hostingcompany.tld.
- Связаться с вебмейл провайдером, электронный адрес которого используется для общения с жертвами мошенничества. Попросить заблокировать учетную запись, не забыв отослать пример мошеннического - в идеале, **вместе со служебными заголовками** или в виде приложенного оригинального электронного сообщения мошенника (в формате .msg, .eml, и т.д.).
- Постараться идентифицировать дополнительные каналы общения мошенника со своими жертвами, например Skype, Facebook, Vkontakte. Хорошо работает поиск пользователя по email. По идентификации таковых, попросить заблокировать учетные записи у соответствующих сервисов.

Если вы не получили ответа на запросы, повторите (3х, 4х, 5х) сообщения и, в особенности, телефонные звонки. Возможна настройка отправки абуз сообщений через регулярные интервалы, например каждые 2 (4, 12, 24) часа.

- Если работа по блокировке фишинг ресурса происходит слишком медленно, послать запрос о помощи локальной CERT/CSIRT команде, в зоне ответственности которой происходит инцидент. Ее вовлечение должно ускорить процедуру ликвидации вредоносного ресурса.

Восстановление 5

Убедиться в нейтрализации угрозы

- Убедиться в недоступности мошеннического ресурса и нефункциональности учетной записи адреса электронной почты мошенника.
- Поставить вредоносные ресурсы, причастные к данной мошеннической схеме на мониторинг с автоматическим оповещением по изменению контента сайта: нередки случаи возвращения ресурса под контроль злоумышленников. Возможно использование Website Watcher или собственных скриптов мониторинга доступности веб-ресурсов.
- При возможности, организовать мониторинг доменных имен на базе ключевых слов, использованных для регистрации нейтрализации мошеннического доменного ресурса.
- После полной нейтрализации фишинг ресурсов убрать предупредительное сообщение о фишинг кампании с официального сайта (см. фазу “Подготовка”).

После инцидента 6

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

- Включение каких дополнительных шагов в подготовительную фазу позволит быстрее и эффективнее реагировать на будущие инциденты?
- Обновить список контактов, добавить примечания по оптимизации подхода к каждому контакту.
- Установление какие дополнительных внутренних и внешних контактов поможет увеличить эффективность работы по данному типу инцидентов.
- Взаимодействовать с юридическим отделом в случае подачи официальных жалоб.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

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

IRM #14

Скам

Реагирование на инциденты онлайн мошенничества

Автор IRM: CERT SG

Версия IRM: 1.1 (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.