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 фишинг 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, вебмейл 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 фишингу.

Внешние контакты

- Создать внутреннюю команду, занимающуюся инцидентами киберпреступности и доступную круглосуточно:
  - Создать легко запоминающийся электронный адрес для принятия оповещений о фишинге и других мошенничествах, например: security@yourcompany;
  - Создать веб форму – не более чем в двух кликах от лицевой страницы – для оповещения о фишинге;
  - 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 фишинга для оповещения клиентов. Повышайте пользовательскую осведомленность о фишинге; объясните, что такое фишинг и каким он бывает. Уведомите клиентов, что вы никогда не запросите их логины, пароли, значения токенов, номера банковских карточек и телефонов и т.п.

Подготовка 1

Осведомленность сотрудников

Ваши собственные сотрудники должны быть в курсе фишинга и иных проблем безопасности. Таким образом необходимо повысить и их уровень осведомленности и определить рамки общения с клиентами – предотвратить любую возможность отправки клиентам транзакционных ссылок или запроса у них логинов, паролей, номеров банковских карточек и телефонов и т.п.

Обнаружение 2

Обнаружить инцидент, определить затрагиваемый периметр, привлечь к решению компетентные стороны.

Обнаружение фишинга

- 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 веблогов ваших сайтов. Проверяйте на наличие подозрительных рефереров. Очень часто, последним этапом фишинг кампании является легитимный сайт атакуемой компании.

Вовлечение компетентных сторон

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

Сбор доказательной базы

Создать датированную копию фишинг сайта. Возможно использование HTTrack. Собрать каждую страницу фишинг сайта (глубина копирования >1). При необходимости, сделать копии экранов фишинг страниц. Собрать копии полученного фишинг спама.

Сдерживание 3

Минимизировать эффект от атаки

- Обнародовать URL обнаруженного фишинг 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 момента его нейтрализации вашей командой безопасности.

- Оповестить клиентов посредством публикации страницы о текущей фишинг кампании (см. фазу «Подготовка»).
- В случае частых фишинг кампаний создать и опубликовать информативный раздел, посвященный мерам пользовательской безопасности и доступный из авторизационного интерфейса. Раздел должен содержать описания наиболее типичных форм мошеннических акций с графическими примерами и пояснениями.
- Проанализировать исходный код фишинг 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 фишинг ресурсом непосредственно с легитимного сайта. В этом случае возможно изменить используемые фишером графические ресурсы для оповещения пользователей. Например, заменить лого на крупную надпись «ФИШИНГ РЕСУРС – не использовать».

Устранение 4

Ликвидировать угрозу

- Если фишинг ресурс располагается на взломанном легитимном сайта, постараться выйти на прямой контакт с владельцем сайта (предпочтительно по имейлу И телефону). Необходимо объяснить причину контакта и роль, выполняемую сайтом без ведома владельца. Необходимо дать четкие указания на то, какие именно действия должен произвести владелец скомпрометированного ресурса для нейтрализации фишинг и предотвращения дальнейших случаев компрометации (например: удаление вредоносных папок, удаление шеллов фишера, актуализация используемого CMS).
- Вне зависимости от реакции владельца скомпрометированного ресурса, необходимо оповестить хостинг провайдера, в зоне ответственности которого находится фишинг 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. Очень часто электронные адреса команд, ответственных за борьбу с вредоносным контентом на серверах провайдера выглядят как abuse@hostingcompany.tld.
- Связаться с вебмэйл провайдером, электронный адрес которого используется для приема украденных транзакционных клиентских данных. Запросить заблокировать учетную запись по причине использования во вредоносной фишинг-схеме.
- В случае использования ресурса-редиректа, приоритизировать работу по приостановлению деятельности этого ресурса.

Если вы не получили ответа на абуз-действия, продублируйте (3x, 4x, 5x) 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 фишинг ресурса или нефункциональности учетной записи адреса электронной почты мошенника.
- Поставить фишинг URL на мониторинг с автоматическим оповещением по изменению контента сайта: нередки случаи возвращения ресурса под контроль злоумышленников. В особенности в случае частичной нейтрализации (например, в случае активности сайта-редиректа). Возможно использование Website Watcher или собственных скриптов мониторинга доступности веб-ресурсов.
- 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 каких 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 #13

Фишинг

Реагирование на фишинг-ресурсы

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.