#CODEIB

Как проверить навыки кибербезопасности сотрудников

Другач Юрий

Автор блога о соц. инженерии icast.ru
Участник Bug Bounty Яндекс, Google, PayPal
Основатель проекта StopPhish

СОДЕРЖАНИЕ

Виды социальной инженерии

3 класса СИ:

✓Массовая (всем подряд)
✓Таргетированная (под конкретного сотрудника)
✓Смешанная (под компанию или подразделение)

Как реагировать:
✓При массовой - в спам
✓При таргетированной - оповещаем всю организацию
✓При смешанной - предупреждаем остальных сотрудников в подразделении

Как сделать массовую атаку

По списку email отправляем одинаковое письмо

Коллеги, добрый день.
Во время карантина у нас есть хорошие новости.

Наш обслуживающий банк предоставляет беспроцентную карту рассрочки на 60 000 р. сроком на 6 месяцев.
В случае тяжелой финансовой ситуации, с помощью заявления можно будет и вовсе списать эту сумму.

По ссылке http://sberbank.ru/registration-187@118.62.14.87/?rid=17263 заполните заявку на получение карты.
Она будет бесплатно доставлена курьером в течении 3-х дней.

С уважением, Миронов Андрей

Как сделать таргетированную атаку

Выясняем:

- С кем общается
- С чем связана деятельность

С кем общается сотрудник

	Бухгалтер	Продавец	IT-специалист	Топ-менеджер
Гос. органы	*			*
Клиенты	*	*		
Руководитель	*	*	*	
СМИ				*

Дальше думаем, с чем связана работа, например, продавца: продажи, выставление счета

Получаем пример письма

Андрей, приветствую.
Просьба просчитать смету для клиента.
Загрузил ТЗ на диск https://yadi.sk/RSj8v
Жду сегодня.

Михайлов С.Е.
Коммерческий директор
АО «ГазМяс»

Смешанная СИ

Исходная база: email, компания, адрес сайта.

Коллеги, добрый день.

В связи с коррекцией регламентов по удаленной работе АО «Газстрой», просьба сегодня ознакомиться с документом.
Логин и пароль для доступа такой же, как у вашего email.
Разместили на сайт http://www.gazstroy.ru/reglament-udalennaya-rabota@17.62.14.87/rid=12376

По окончании удаленной работы, в офисе за него нужно будет расписаться, но использовать уже сейчас.

С уважением, Иванов Андрей
ИТ-служба
АО «ГазСтрой»

Регулярность учебных атак

2-4 учебных атаки в неделю

Тестовая группа:
50 сотрудников прошедших обучение и 50 не обученных.

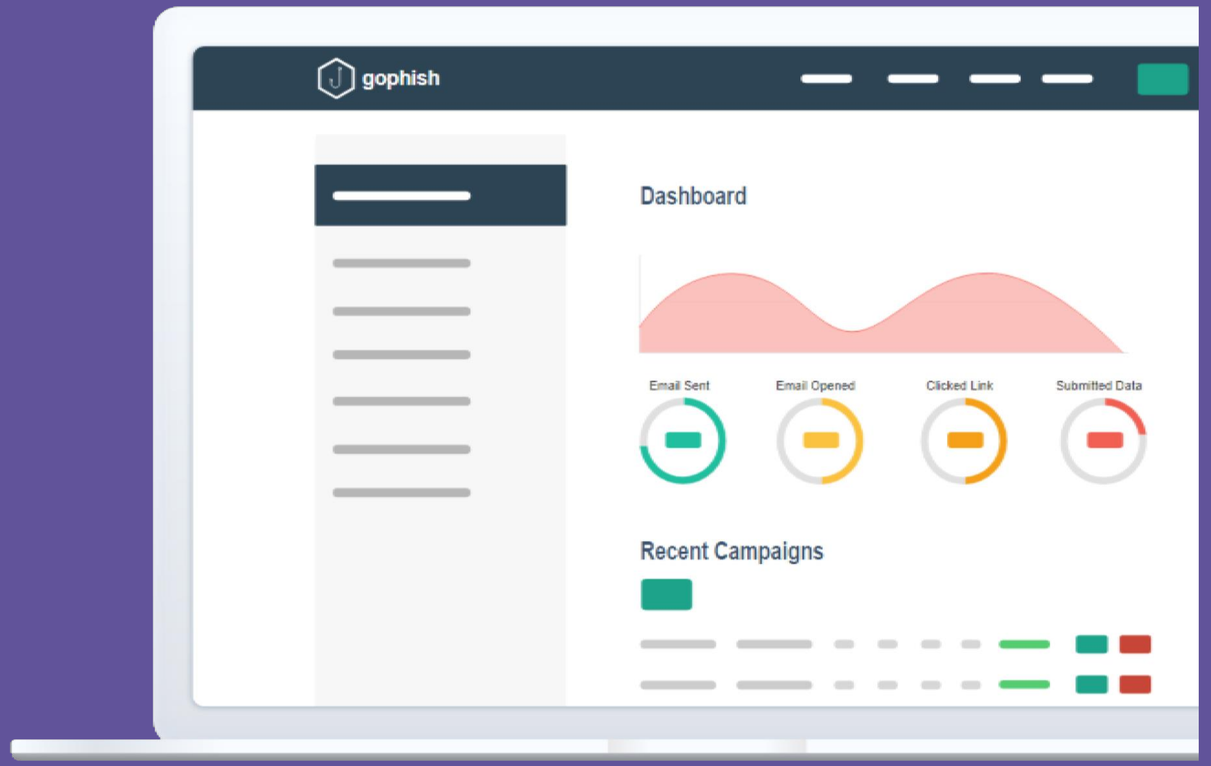
Технические особенности:
терминальный интернет.

Сценарий атаки:
Смешанная СИ

Результат:
«Не обученные» - 34 перехода и 30 скачиваний
«Обученные» - 30 переходов и 25 скачиваний

Платформа для атак Gophish

Getgophish.com



Пример письма: 45% инцидентов

Коллеги, добрый день.
В связи с продлением ограничений до конца майских праздников, было принято решение провести тестирование сотрудников на коронавирус на дому.

Составляется график тестирования по каждому подразделению.
Просьба сегодня выбрать даты для проведения сотрудникам тестов на нашем портале http://domain.ru

Из представленной таблицы выберите свободные ячейки.

С уважением,
Елена Симонова

Пример письма: 50% инцидентов

{Name}, добрый день.

Информацию о графике работы в майские праздники и системе начисления доплат за удаленную работу разместили на нашем портале https://my.corporat.local/news/grafik-may@kalinkaltd.online/rid=18827

Во избежание недоразумений, просьба ознакомиться сегодня.

С уважением, Андреева Ирина
АО «Газмяс»
Москва, 128096, ул. Ленина, д.1
+7 (495) 127-27-27

Пример письма: 60% инцидентов

Добрый день.

Как вы просили, выложила зарплатную ведомость за май с коррекциями + премии
https://gazmyas.ru/private/HR/

С уважением,
Ольга Тагунова
начальник Отдела
по работе с персоналом
АО «ГазМяс»

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

dys@icast.ru
fb.com/yuresd
Блог: icast.ru