

КОНТРОЛИРУЕМЫЙ ВЗЛОМ

3-е издание

БИБЛИЯ
СОЦИАЛЬНОЙ
ИНЖЕНЕРИИ



Юрий Другач



Оглавление

Предисловие.....	11
Об этом издании	11
От автора	12
Кому и как можно использовать эту книгу?	14
Для представителей служб ИБ, СБ и ИТ-служб	16
Для пентестеров.....	17
Для хакеров.....	17
Что такое социальная инженерия?	17
Опасность социальной инженерии.....	18
Цитаты.....	19
Ущерб от СИ.....	19
Глава 1. Онлайн-атаки	23
Подготовка	23
Пентестеру	24
OSINT для СИ	24
Разведка боем	25
Проверка антиспама	28
Переходим на личности	28
Какую фишинговую форму создавать?	29
Несуществующий адрес.....	29
Пробиваем MX-записи.....	30
Неведение.....	30
От чьего имени писать?.....	31
ВЕС-атака.....	32
Таблица персонализации	33
Пример email-MITM.....	34
Какой фишинговый домен купить?.....	35
Безопаснику	35
Готовим атаки	36
Атаки по email	36
Идеи по составлению темы письма.....	36
Какую подпись и оформление использовать?	37

Выбираем контекст.....	37
Векторы и сценарии.....	38
Контекст: событийные атаки (Event attacks)	38
Событийные атаки: чрезвычайная ситуация.....	38
Событийные атаки: праздники.....	39
Событийные атаки: политика.....	39
Контекст: причина	40
Якобы взлом.....	40
Внеплановая проверка от СРО	41
Неудачные попытки авторизации	42
Уведомление	42
Что вы делаете в Бразилии?.....	42
Контекст: запросы.....	43
Контекст: вопросы	43
Вопрос с вложением.....	43
А что это вы мне отправили?	43
Контекст: отправка	44
Контекст: изменения	44
Контекст: желание	45
Контекст: «непонятки».....	46
Переписка-ссылка.....	46
Одинокий файл	46
Усиление контекста	46
Усиление контекста: эмоции.....	47
Усиление контекста: давление	48
Адресаты в копии	48
Письма от госорганов.....	49
Срочно обновитесь	50
Усиление контекста: ложь	50
Фейковая переписка	51
Фейковая пересылка.....	51
Усиление контекста: совпадение	52
Источники фишинговых писем	52
Файлы	53
Некорректное отображение	53
Подарочный сертификат	53
Пустой файл	54
Документ с «мыльпой».....	56
Имитация Excel-таблицы в Word-документе	60
Небезопасный PDF-файл.....	60
Файл как прокладка перед нагрузкой	62
Отсутствующий сертификат	64
Разрешите и заполните	65
Файл ICS	66
Социальные сети	67
Подготовка	68
О поиске сотрудников в соцсетях	72
Клонирование аккаунтов.....	73

Медленно, но верно	73
Многоходовка в соцсети	73
Терпеливо ждем	74
Поддельный рекрутер	74
Мессенджеры	75
Telegram-каналы	76
Сотрудник — физлицо	76
Онлайн-консультанты	76
Веб-сайты	77
Поддельное окно для ввода логина и пароля	77
Скачайте на нашем сайте	78
Корпоративные порталы	78
Разрешите уточнить	79
Новостные ресурсы	79
Туда, да не туда	80
Фейковая капча и предупреждение о cookie	80
Всплывающее окно	81
Персонализированный сайт	83
Покажи себя	84
Реклама	85
Таргет по MAC-адресу	85
Таргет по геолокации	86
Адвёртинг	86
Фиктивный APK-файл	87
Лидеры мнений	87
Видео-deepfake	87
Видео без видео	88
Аудио-deepfake	88
Find trap сценарии	89
Find trap с помощью рекомендаций	90
Выдуманная компания	91
Find trap с помощью звонков	91
Продажа фиктивного сертификата	91
Комментарии	92
Легализованная СИ	92
Отправили к вам	93
Фишинг	94
Проверка на утечку	94
Data-phishing	94
Многоходовки	96
Фейковое интервью	97
Отложенная отправка	97
Цепочки писем	98
Цепочки писем: неправильная кодировка как повод	98
Цепочки писем: простите, не туда	98
Цепочки писем: нас взломали	98
Цепочки писем: использование для data-фишинга	99
Фейковые посетители	99

Глава 2. Технологические трюки введения в заблуждение.....	101
Маскировка ссылок	101
Символ @	101
Слеш в Unicode	102
Домены в Punycode	102
Зашумление юникодом	102
Обфускация ссылок	102
QR-коды	103
Некорректный протокол	104
Ссылки в виде картинок	104
Ссылка в документах	104
Очень длинная ссылка	105
Ссылка виде цифр	106
Невидимая при наведении мыши	106
Редиректы	107
Неактивные ссылки	108
Похожие на официальные	109
Ссылки в поддоменах	110
Сращивание с поддоменом	110
Сращивание с протоколом	110
Домен после слеша	110
В дополнение	110
Капча от ботов защитного ПО	110
Одноразовые ссылки	111
Подделка отправителя	111
Email с официального ресурса	112
Вложения и файлы	113
Файлы Microsoft Office	113
Рушим шаблоны поведения через печать	114
PDF-файлы	115
HTML-файлы	116
Маскировка расширения <i>html</i>	117
Архивы с паролем	117
Архивы без пароля	118
Редко используемые форматы архивов	119
Онлайн-документы	119
Excel-файл, размещенный онлайн	119
Глава 3. Атаки в офлайне.....	123
Проникновение на физические объекты	123
Предмет в руках	123
Подслушанная легенда	124
Проведение интервью	125
Давайте помогу	125
Корпоративная столовая	125
Небезопасные парковки	126
Паровозик	126
Мусорный дайвинг	127
Отделение банка	127

Отвлекающий маневр	128
Потенциальный клиент	128
Собеседование	128
Гостевой пропуск	128
Подделка карты-пропуска	129
Черный ход	129
Плечевая атака	129
Piggybacking	129
USB-устройства	130
Таргетированная флешка	131
Флешка с легендой	131
«За букет роз»	131
Juice jacking	132
Смишинг	132
Вишинг	133
Подделка номера	133
Многоходовый звонок	133
Вернитесь на работу	133
Забыл кодовое слово	134
Отсылка к отпускнику	134
Синхронный ввод	134
Телефон + find trap	135
Любой добавочный	135
Китовые атаки	135
Усиление звонком	136
Квид про кво	136
Callback phishing	137
Нас взломали, помогите восстановить	138
Бумага не во благо	138
Подбрасывание корпоративных документов	138
Визуальный пропуск	138
Реклама на бумаге	139
QR-коды на бумажных носителях	139
Справка	139
Общественный транспорт	141
Wi-Fi	141
Мероприятия	141
Двухдневное мероприятие	142
Организовал себе на голову	142
Конференции, выставки и форумы	142
Пришел к одним, пошел к другим	142
Корпоратив	142
Комбинирование	143
Истории для вдохновения	143
Обход системы	143
Пентест тюрьмы	145
Случай в отеле	146
Неприступная крепость	148

Глава 4. Проведение онлайн-атак по email.....	151
Какой софт использовать?	151
Список email-пользователей	152
Как создавать сообщения для атак?	152
Чек-лист применения электронной СИ.....	154
Как повысить киберграмотность сотрудников?	154
Технические аспекты обучения.....	156
Глава 5. Технические меры противодействия СИ	159
Софт	159
Корпоративный браузер	159
Сегментация сети и Zero Trust	160
Невозможность залогиниться в почте с недоверенных IP-адресов	160
Обнаружение повторного использования пароля	160
Фиды о фишинге	161
Антифишинговый шрифт	161
Настройка DKIM, SPF и DMARC	162
Предотвращение выполнения исходного кода	163
SSO	164
Sandbox.....	165
Технические аспекты защиты от СИ	165
Способы применения чек-листа	165
Выбирайте методы фильтрации вредоносного содержимого в зависимости от вашей тактики.....	165
Настройте защиту от фишинговых ссылок	166
Ссылки, похожие на официальные сайты	167
Настройте защиту от вредоносных вложений.....	167
Возможные к запрету расширения, используемые в фишинге	167
Настройте проверку заголовков email на подозрительные признаки	167
Настройте защиту по содержимому письма	168
Hardware	168
Межсетевые экраны	168
FIDO	169
Различия между UAF, U2F и FIDO2	169
Недостатки этого способа защиты	170
OTP-токены.....	170
Глава 6. Организационные меры противодействия СИ.....	173
Модель зрелости осведомленности о безопасности.....	173
Одобрение процесса повышения осведомленности у руководителей	175
Обучение: памятки, курсы, форматы обучения	176
Регламенты	177
Регламент обучения персонала	178
Некоторые аспекты для учета в регламентах	178
Контроль реквизитов	179
Дополнительная проверка перед оплатой	179
Как вести себя с гостями?.....	179
Общение с коллегами.....	180
72 минуты до начала конца	180
Сотни регламентов по информационной безопасности	181

Глава 7. Искусственный интеллект	183
Создание фишинговых форм с помощью ИИ	184
Вредоносный поисковик	188
Подделка голоса.....	191
Хакерские инструменты на основе ИИ.....	191
Создание фишингового письма с ИИ	192
Масштабирование применения ИИ.....	197
Послесловие	199
Приложение 1. Генератор онлайн-СИ	201
Приложение 2. Классификатор СИ.....	202
Электронная социальная инженерия v0.81.....	202
Офлайн социальная инженерия v0.2	208
Приложение 3. Таблица персонализации.....	210
Приложение 4. Бесплатное в помощь службе ИБ и ИТ.....	211
Приложение 5. Критерии выбора платформы по повышению осведомленности	212
Приложение 6. Словарь терминов.....	218