Целевые атаки на топ-менеджмент

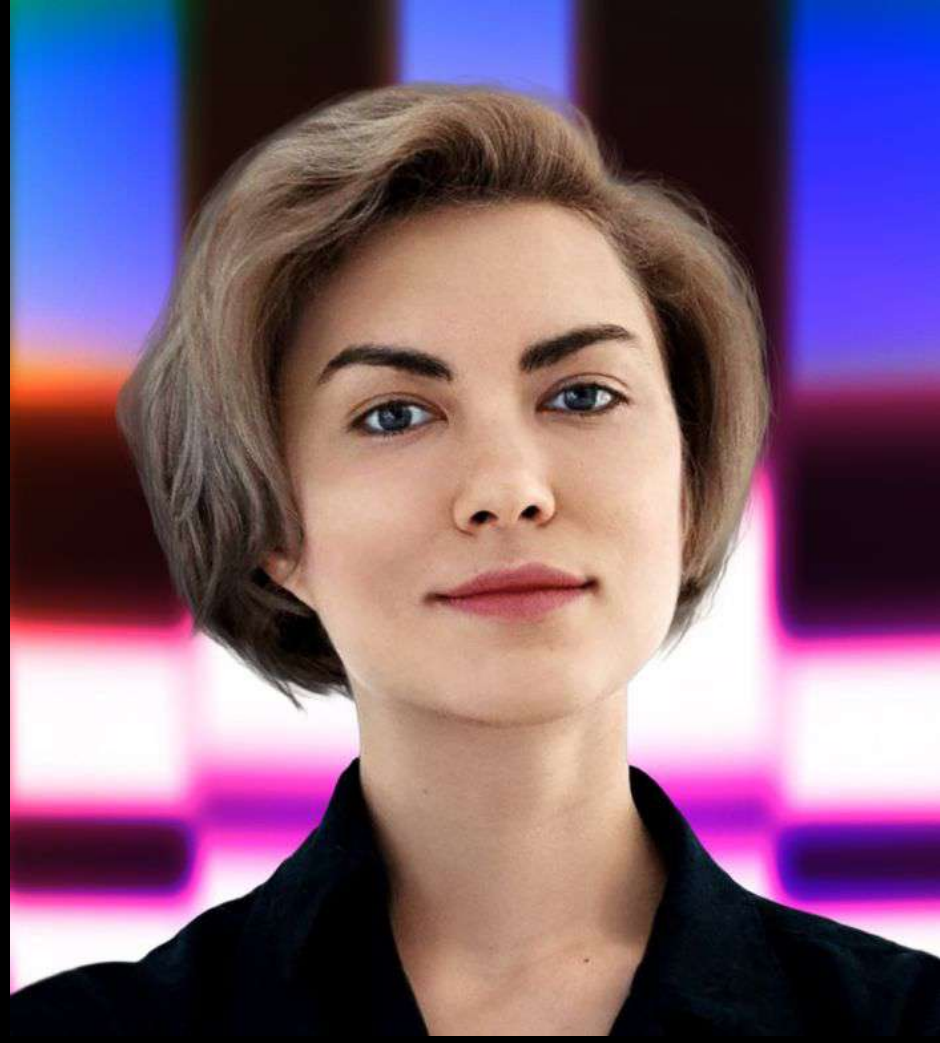
Екатерина Тьюринг

Кибердетектив в сфере экономической безопасности

искусство бизнеса

Екатерина Тьюринг

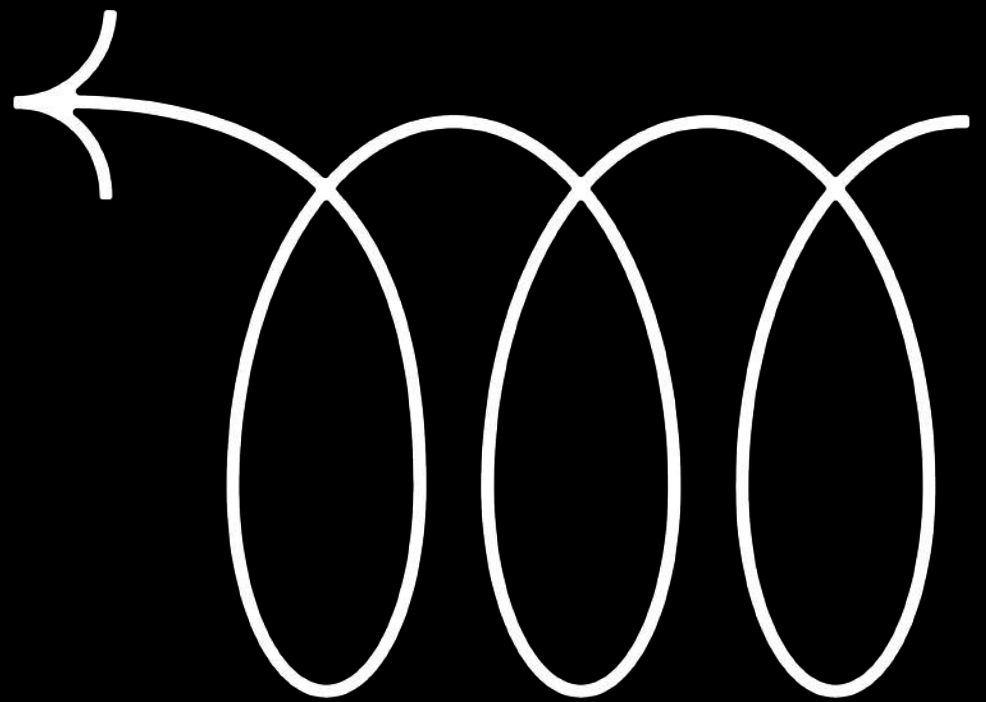
- Кибердетектив в сфере экономической безопасности
- Ex-VK, Ex-Avito antifraud lead
- Управляющий партнер СФЕРА intelligence — агентства глубокой проверки бизнеса в России и за рубежом



СФЕРА
intelligence

Все модели угроз похожи друг на друга — каждая отдельно взятая взломанная компания уникальна по-своему

Каждая компания уникальна, но модели угроз и методы взлома — одинаковые



CNews.ru

Взломан крупнейший мировой производитель военной и аэрокосмической техники. Сотрудники попались на простейшую уловку хакеров

Представители компании General Dynamics сообщили о том, что фишеры провели успешную кибератаку на ее сотрудников.

2 янв. 2025 г.

Хакер.ru

За один день группа TA558 разослала более 76 000 фишинговых писем

Аналитики компании FACCT обнаружили новую масштабную фишинговую атаку хак-группы TA558. Всего за один день злоумышленники разослали...

1 месяц назад

SecurityLab.ru

Хакеры атакуют вручную: 74% критичных инцидентов – дело рук людей

LotL, фишинг и повторные атаки – главные тренды киберинцидентов-2024 . image. Исследователи из «Лаборатории Касперского» представили...

3 недели назад

Веерная атака

Целевая атака

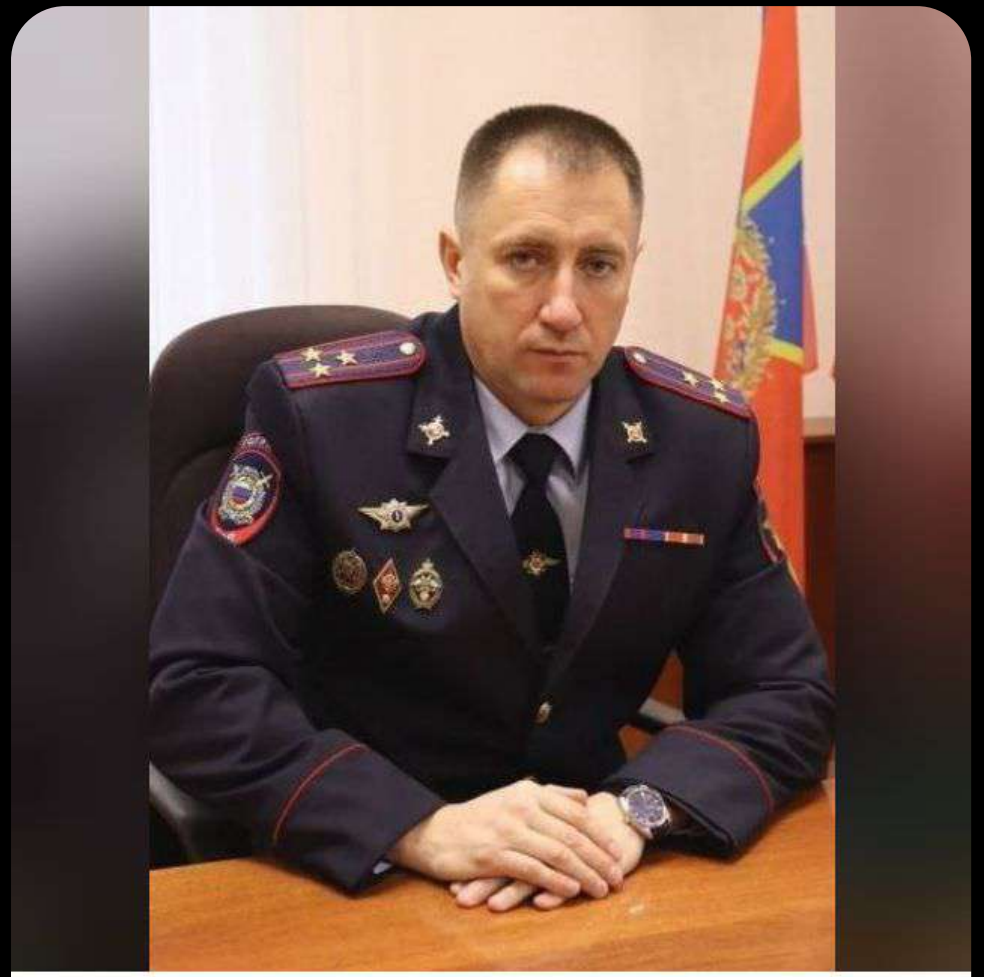
Веерная атака

Целевая атака

Привет, я менеджер проекта LINIO и в настоящее время ищу сотрудников на неполный рабочий день. Вы можете работать с использованием мобильного телефона. Работа займет 1-2 часа! Свяжитесь со мной, чтобы выполнить две первые простые задачи получить за это 500 рублей оплаты. Отправьте код: TM72634. Заработная плата составляет от 2000 до 30000 рублей в день。 Если вам интересно, пожалуйста, сделайте скриншот этого текстового

Веерная атака

Целевая атака



Мошенники развели бывшего замглавы информационного центра УМВД по Кировской области. Подполковника полиции обманули от имени замглавы управления.

Веерная атака

Целевая атака

Преподаватель МПГУ три месяца переводил деньги мошенникам, охотясь за коллекционными значками для частной коллекции университета.

Все перечисленные атаки — веерные

Все перечисленные атаки — веерные

Характерны:

1. Отсутствие избирательности
2. Масштабируемость

Задача:

зафиксировано
100 успешных атак
на топ-менеджеров

Предположите:

1. Какой вид атаки
встречается чаще —
веерная или целевая?

2. Распределение долей —
сколько из 100 атак
было целевых?

Ответ: веерная, доля — 90%

Задача:

зафиксировано
100 успешных атак
на топ-менеджеров

Предположите:

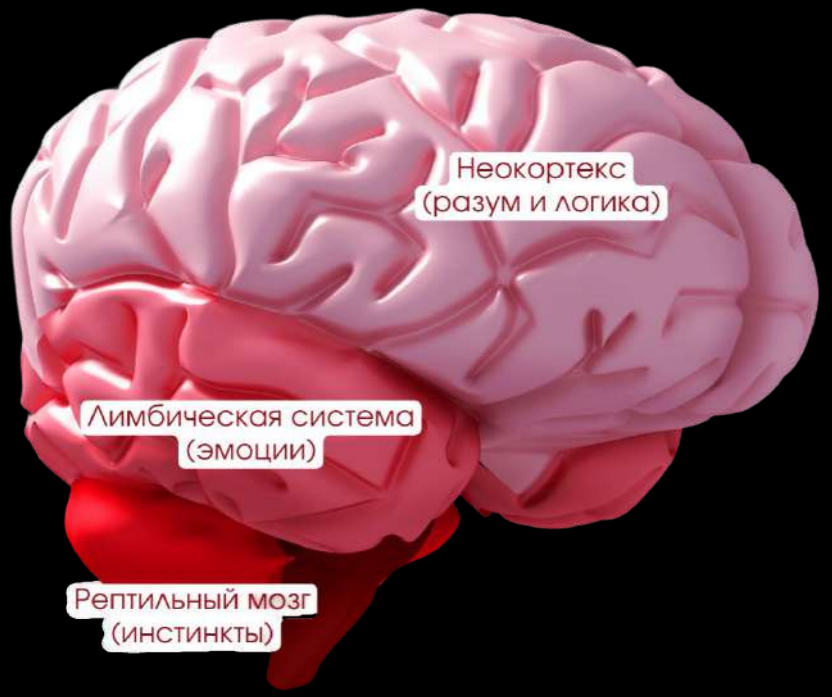
1. Какой вид атаки встречается чаще — веерная или целевая?

2. Распределение долей — сколько из 100 атак было целевых?

Почему социальная инженерия работает?

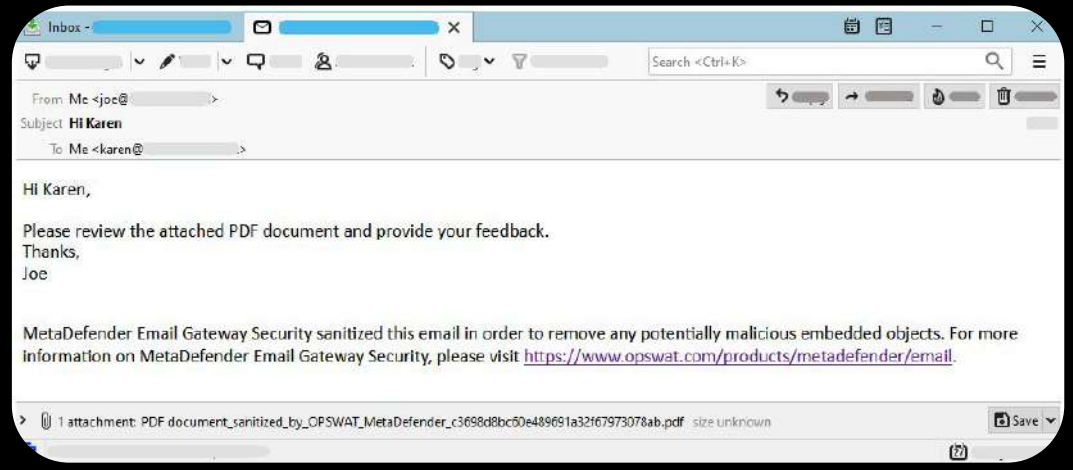
— Лимбическая система отвечает за эмоции
— Рептильный мозг отвечает за инстинкты
— Неокортекс отвечает за анализ информации

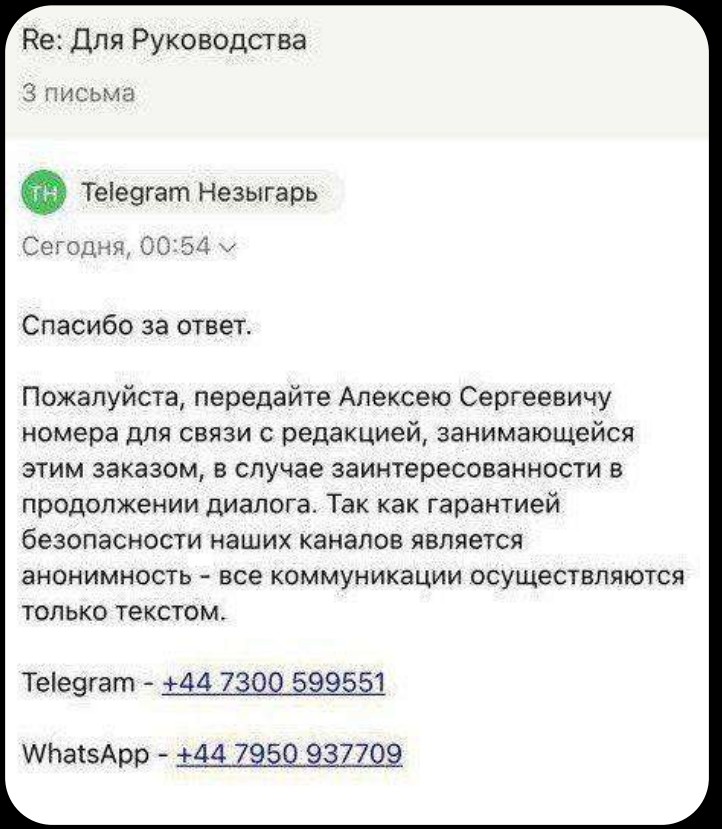
Рептильный мозг активирует стрессовое состояние, при котором мы принимаем эмоциональные решения под действием триггеров: страха, жадности, FOMO.



Виды целевых атак методами социальной инженерии

- Вымогательство и шантаж
- Мошеннические сделки
- Информационный вброс





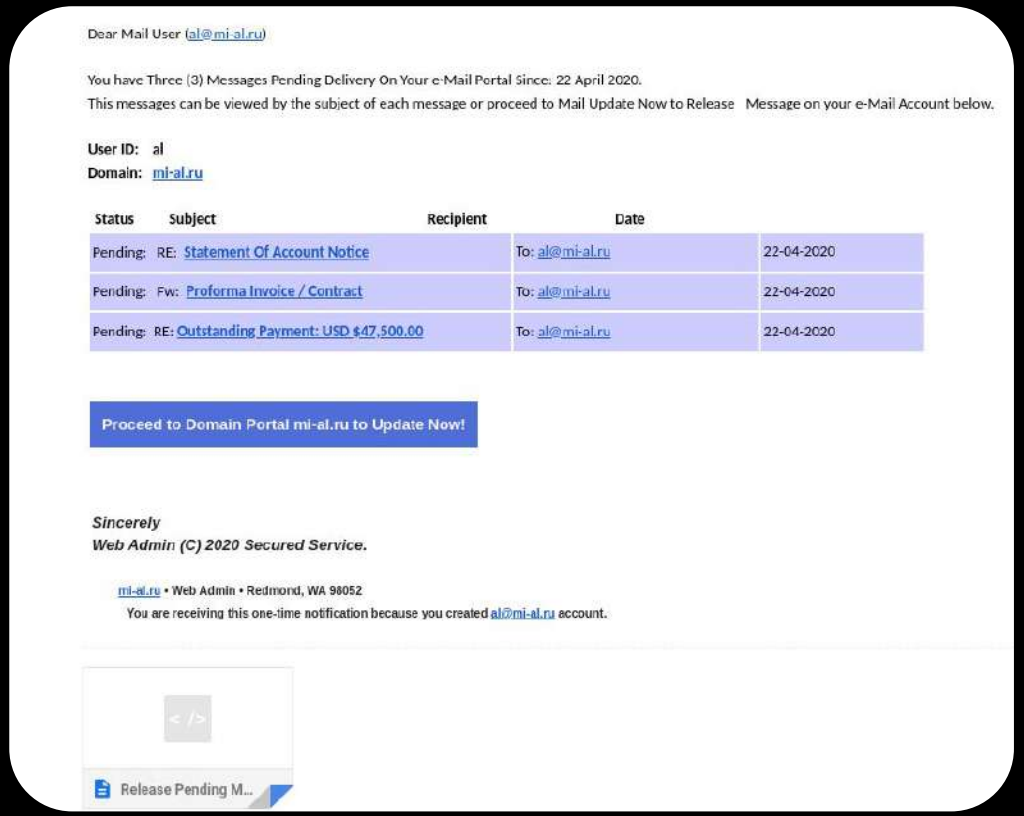
Вымогательство

Популярные легенды:

— Отмывание денег

— Спонсирование иностранных государств

— Коррупция и взятки



Dear Mail User (al@mi-al.ru)

You have Three (3) Messages Pending Delivery On Your e-Mail Portal Since: 22 April 2020.
This messages can be viewed by the subject of each message or proceed to Mail Update Now to Release Message on your e-Mail Account below.

User ID: al
Domain: mi-al.ru

Status	Subject	Recipient	Date
Pending:	RE: Statement Of Account Notice	To: al@mi-al.ru	22-04-2020
Pending:	Fw: Proforma Invoice / Contract	To: al@mi-al.ru	22-04-2020
Pending:	RE: Outstanding Payment: USD $47,500.00	To: al@mi-al.ru	22-04-2020

Proceed to Domain Portal mi-al.ru to Update Now!

Sincerely
Web Admin (C) 2020 Secured Service.

mi-al.ru • Web Admin • Redmond, WA 98052
You are receiving this one-time notification because you created al@mi-al.ru account.

Release Pending M...

Секрет успеха в:

— Глубокой подготовке — есть реальные нарушения

— Качественной реализации — используют подделки

— Физической коммуникации

Вымогательство: взлом в Telegram

Популярные легенды:

— Откаты и любовницы
— Доступ к чувствительным данным
— Доступ к конфиденциальным документам

Технология:

Шаг 1. Веерный взлом
Шаг 2. Анализ контента
Шаг 3. Связь с жертвой
Шаг 4. Шантаж

Вымогательство: взлом Telegram

1. Завершить лишние сессии
2. Обновить или установить облачный пароль
3. Определить уровень риска
4. Обратиться к команде реагирования
5. Действовать согласно разработанному плану

Вымогательство: взлом Telegram

Очистить кэш? Нет

Вымогательство: взлом Telegram

Откатиться к заводским настройкам? Нет

Вымогательство: взлом Telegram

Удалить чат, заблокировать мошенника? Нет

Вымогательство

Меры защиты:

— Квалифицированная служба безопасности

— Опытные корпоративные юристы и консультации с ними по чувствительным вопросам

— Конкретный плейбук действий

— Регулярные инструктажи

Мошеннические сделки: использование доверенности

Популярные легенды:

— Продажа прав на товарный знак от имени владельца
— Выход на сделку, организация закупок
— Перевод предоплаты

Секрет успеха в:

— Стандартных стимулах социальной инженерии
— Невнимательности жертвы при проверке документов

77 А А 6608008

ДОВЕРЕННОСТЬ

Город Москва, двадцать четвёртого апреля две тысячи двенадцатого года.

Я, гр. Владимир Иванович, 25 октября 1952 года рождения, место рождения: ст. Ново-Малороссийская Выселковского р-на Краснодарского края, гражданство: Российская Федерация, пол: мужской, паспорт 45 06 , выданный паспортно-визовым управлением Главного управления внутренних дел города Москвы 22 июля 2002 года, код подразделения 771-001, зарегистрированный по адресу: гор. Москва, ул. д. , корп. 2, кв. 66, настоящей доверенностью уполномочиваю

гр. , 05 марта 1984 года рождения, место рождения: гор. Москва, гражданство: Российская Федерация, пол: мужской, паспорт 45 , выданный ОВД района Марьино гор. Москвы мая года, код подразделения 772-079, зарегистрированного по адресу: гор. Москва, д. ; кв. , быть моим представителем во всех компетентных учреждениях и организациях Подольского района Московской области, в том числе в местной администрации, Комитете по управлению имуществом, Комитете по земельным ресурсам и землеустройству, филиале ФГУ "Земельная кадастровая палата, отделе Управления федерального агентства кадастра объектов недвижимости по Московской области, Подольский р-н, филиале ФГУП "МОБТИ", эксплуатационных организациях, ГУ ИС (ЕИРЦ), ЕГРП, налоговых органах, Ростехнадзоре, по Московской области, Роспотребнадзоре по Московской области Главархитектуре, СЭС, Водоканале, Пожнадзоре, Электросетях, Экологической экспертизе, архивах, Управления Федеральной службы государственной регистрации, кадастра и картографии по Московской области, нотариальной конторе, других компетентных органах, по вопросам оформления и собственность **ЗЕМЕЛЬНОГО УЧАСТКА И ЖИЛОГО ДОМА**, находящихся в ДСПК " ", расположенном по адресу: Московская обл., Подольский р-н, Кленовский с. о. вблизи с. , уч. , с правом проведения межевания земельного участка, регистрации ранее возникшего права на указанное имущество, подавать от моего имени заявления и прочие документы, получать кадастровый паспорт на земельный участок, технический паспорт на жилой дом, правоустанавливающие документы на оформленное в собственность имущество, другие необходимые документы, зарегистрировать все правоустанавливающие документы и право собственности в Управлении Федеральной службы государственной регистрации, кадастра и картографии по Московской области, с правом подачи заявления о приостановлении государственной регистрации, получения уведомления о приостановлении государственной регистрации, сообщения об отказе в государственной регистрации, внесения изменений в записи ЕГРП, внесения изменений в документы, с правом уплаты тарифов, сборов, пошлин, **с правом получения свидетельства о государственной регистрации права и всех необходимых зарегистрированных документов, без права продажи вышеуказанного имущества** делать от моего имени заявления, с правом подачи заявления об исправлении технических ошибок, расписываться за меня и совершать все действия, связанные с выполнением этого поручения.

Доверенность выдана сроком на три года, полномочия по настоящей доверенности не могут быть переуполномочены другим лицам.

Содержание ст. ст. 185-189 Гражданского кодекса Российской Федерации доверителю разъяснено.

Содержание настоящей доверенности доверителю зачитано вслух.

доверитель

Город Москва.

Двадцать четвёртого апреля две тысячи двенадцатого года.

Настоящая доверенность удостоверена мной, Малютиной Тамарой Васильевной, нотариусом города Москвы.

Доверенность подписана гр. Владимиром Ивановичем в моем присутствии. Личность его установлена, дееспособность проверена.

Зарегистрировано в реестре за № Д-1739.

Взыскано по тарифу: 1000 руб. 00 коп.
В том числе взыскано за услуги правового и технического характера: 800 руб. 00 коп.

Нотариус Малютина Т.В.

Мошеннические сделки: использование доверенности

Как не попадаться:

- Проверять документы
- Проверять физлиц, выходящих на сделку
- Проверять юрлиц
- Самостоятельно искать ЛПР

Контур Фокус

СФЕРА
intelligence

Мошеннические сделки: компрометация оценки перед сделкой M&A

Популярные легенды:

— Подмена документов

— Сокрытие компрометирующей информации

— Недоступность внутренней информации — пароли, сервера, кошельки

Секрет успеха в:

— Экономии компании на глубоком Due Diligence

— Некомпетентности сотрудников в проведении Due Diligence

Информационный вброс —

это специально распространенная ложная информация,
цель которой — навредить человеку или организации.

Анатомия атаки:

- → Поиск инфоповода
- → Разработка легенды
- → Запуск атаки
- → Распространение атаки
- → «Сбор сливок»

Информационный вброс: план реагирования

1

Мониторинг инфопространства

2

Фиксация и локализация фактов атаки

3

Разработка антикризисной стратегии

4

Правовое решение конфликта

5

Расследование инцидента

Ключевые рекомендации

Компетентная СБ

Важный навык — план реагирования на кризисные ситуации

Инструкции

Конкретные плейбуки для разных ролей вместо стандартного обучения

Насмотренность

Знание не схем, но сигналов, которые переиспользуют в разных схемах

Гибкие пентесты

ИБ, социальная инженерия, антифрод, устойчивость топ-менеджеров

«Тот, кто владеет информацией, — владеет ситуацией. Бизнес не прощает догадок».

Екатерина Тьюринг

@sferaintel
@katyaturing

искусство бизнеса

СФЕРА intelligence