Современные киберугрозы и методы социальной инженерии при совершении преступлений в сети интернет

VULNERABILIDAD - -

DEFECTOS O ERRORES EN EL SISTEMA QUE PUEDEN APROVECHARSE

delincuete

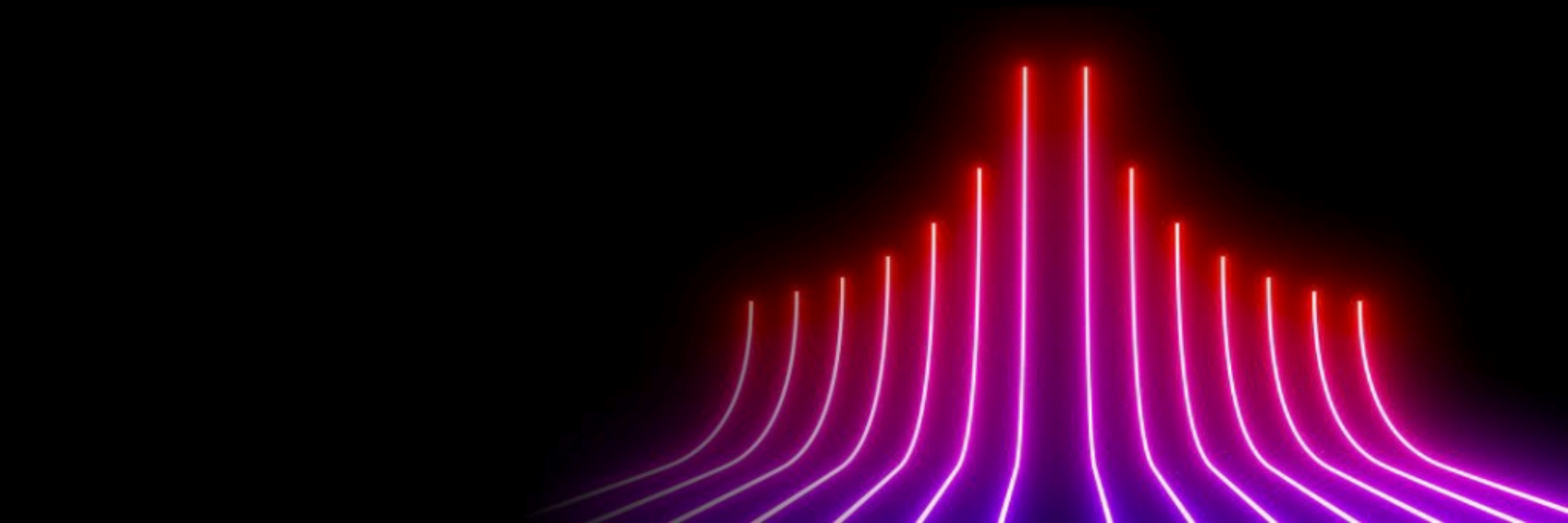
УЯЗВИМОСТЬ —

НЕДОСТАТКИ ИЛИ ОШИБКИ В СИСТЕМЕ, КОТОРЫМИ МОГУТ ВОСПОЛЬЗОВАТЬСЯ ЗЛОУМЫШЛЕННИКИ.

VECTOR DE ATAQUE -

ES UN CONJUNTO DE FORMAS Y MEDIOS, CON LA AYUDA) DE QUE LOS ATACANTES PENETRAN AL SISTEMA.

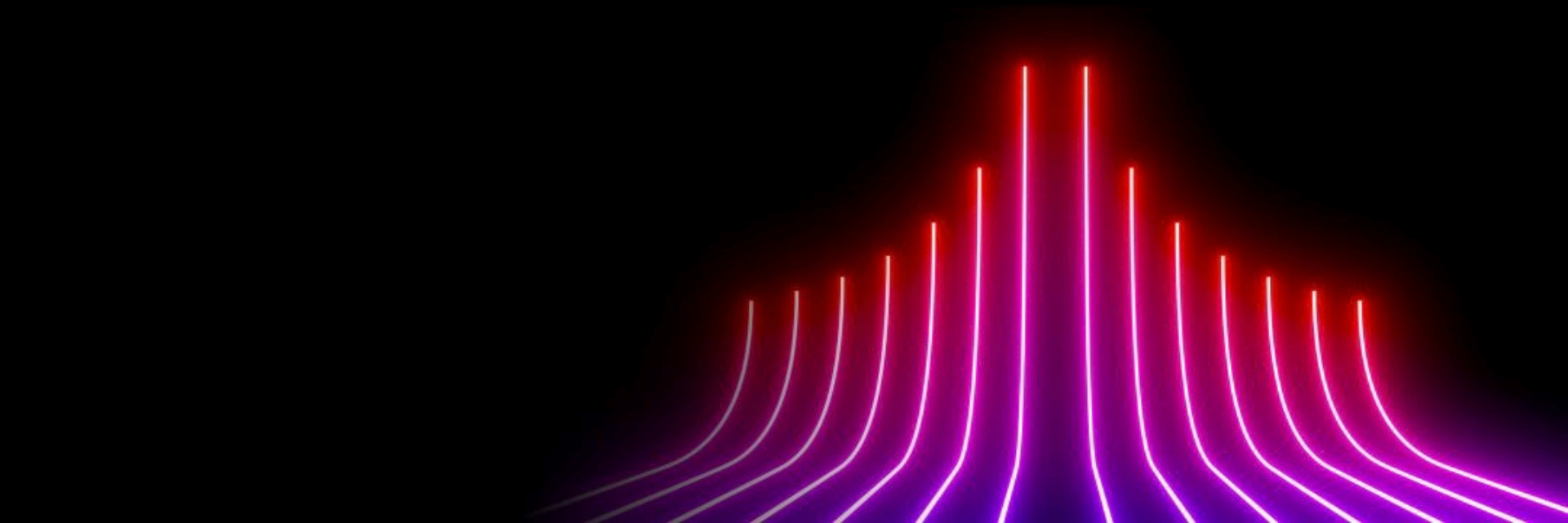
COMO VECTORES DE ATAQUE PUEDEN UTILIZAR, POR EJEMPLO, MÉTODOS INGENIERÍA SOCIAL, EXPLOTACIÓN VULNERABILIDADES.



ВЕКТОР АТАКИ —

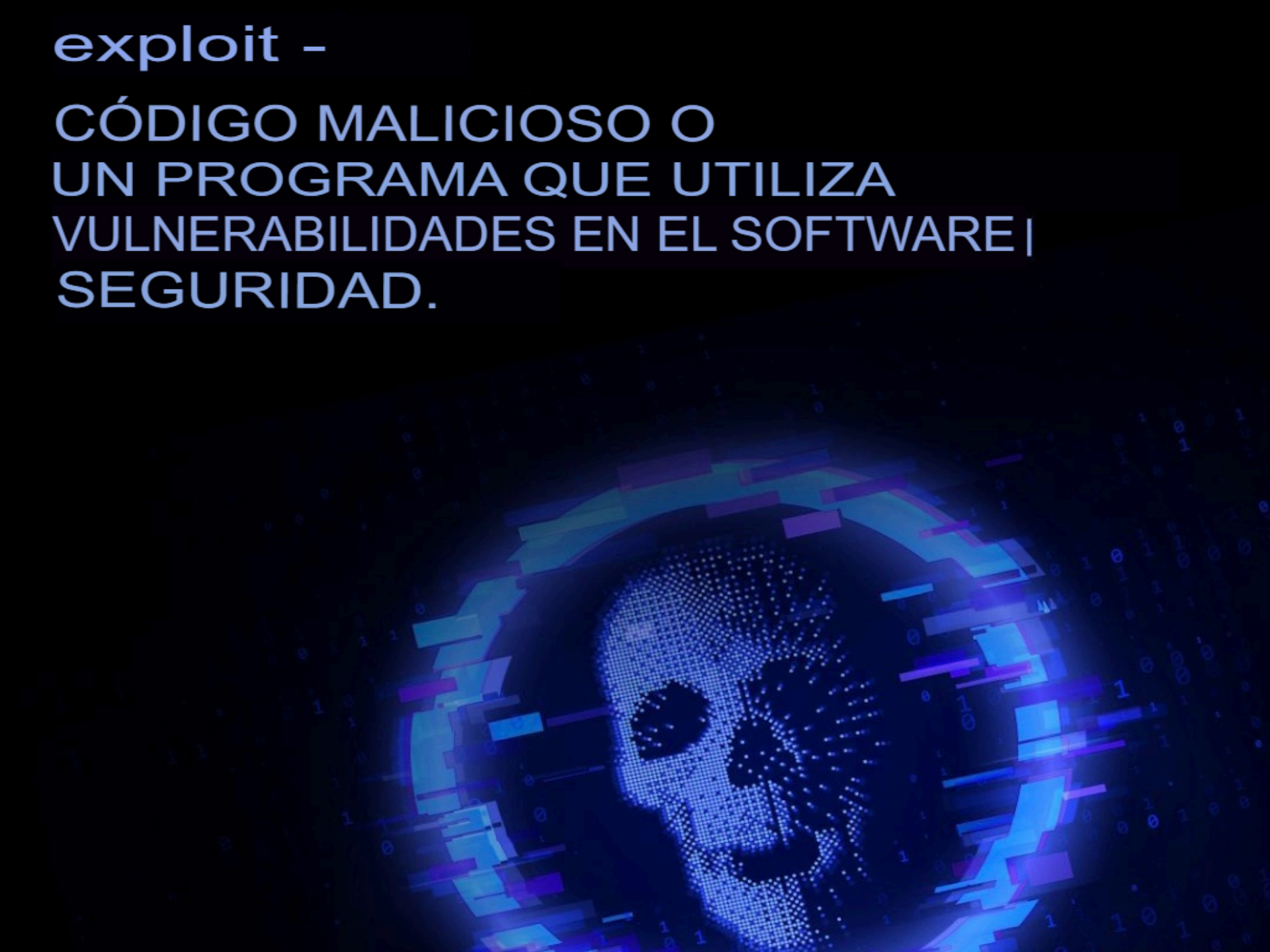
ЭТО СОВОКУПНОСТЬ СПОСОБОВ И СРЕДСТВ, С ПОМОЩЬЮ КОТОРЫХ АТАКУЮЩИЕ ПРОНИКАЮТ В СИСТЕМУ.

В КАЧЕСТВЕ ВЕКТОРОВ АТАКИ МОГУТ ИСПОЛЬЗОВАТЬСЯ, НАПРИМЕР, МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ.



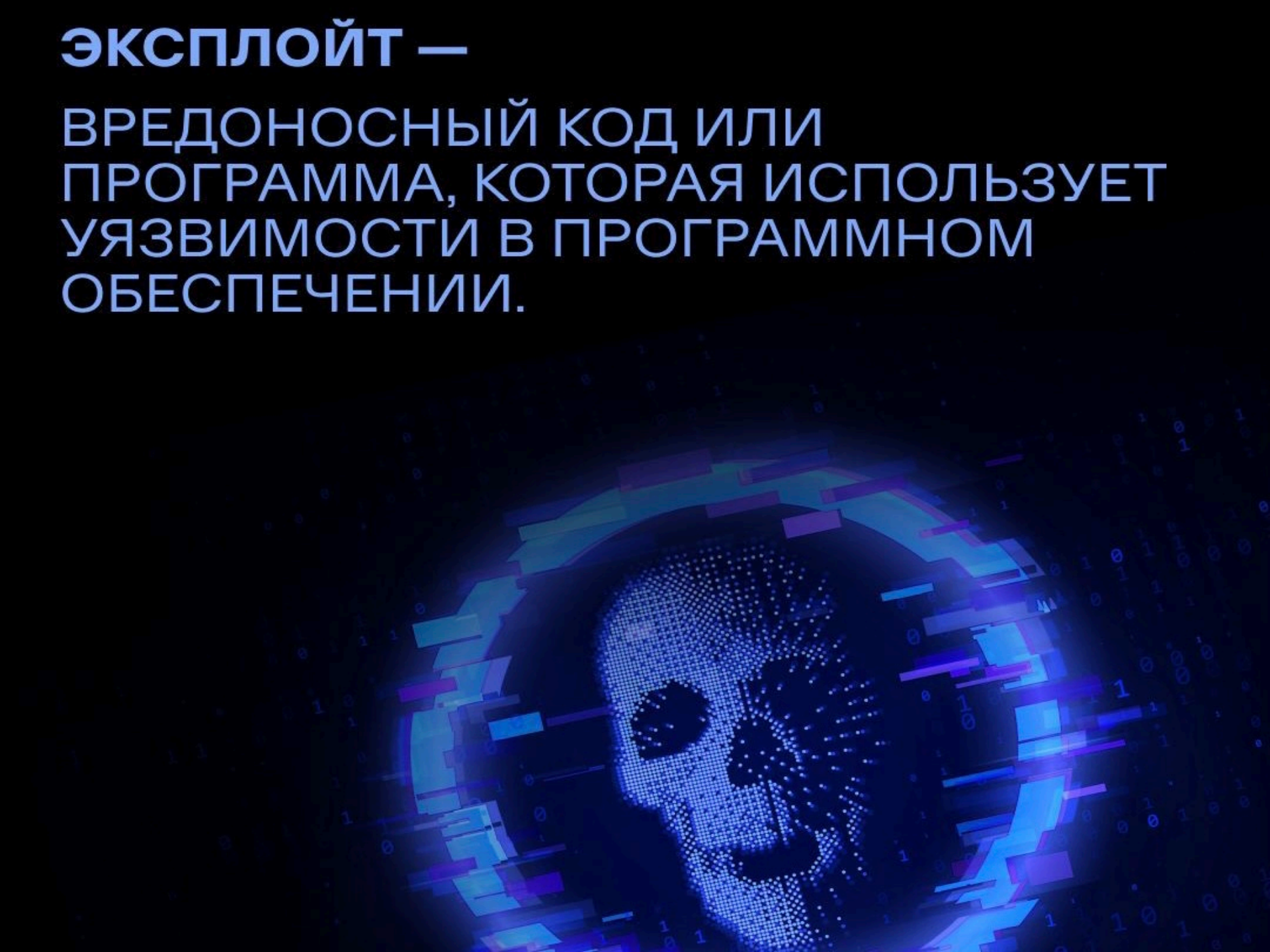
exploit –

CÓDIGO MALICIOSO O
UN PROGRAMA QUE UTILIZA
VULNERABILIDADES EN EL SOFTWARE |
SEGURIDAD.



ЭКСПЛОЙТ —

ВРЕДОНОСНЫЙ КОД ИЛИ ПРОГРАММА, КОТОРАЯ ИСПОЛЬЗУЕТ УЯЗВИМОСТИ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ.



SUPERFICIE DE ATAQUE -

NÚMERO TOTAL DE POSIBLES VULNERABILIDADES ESPECÍFICAS SISTEMA.

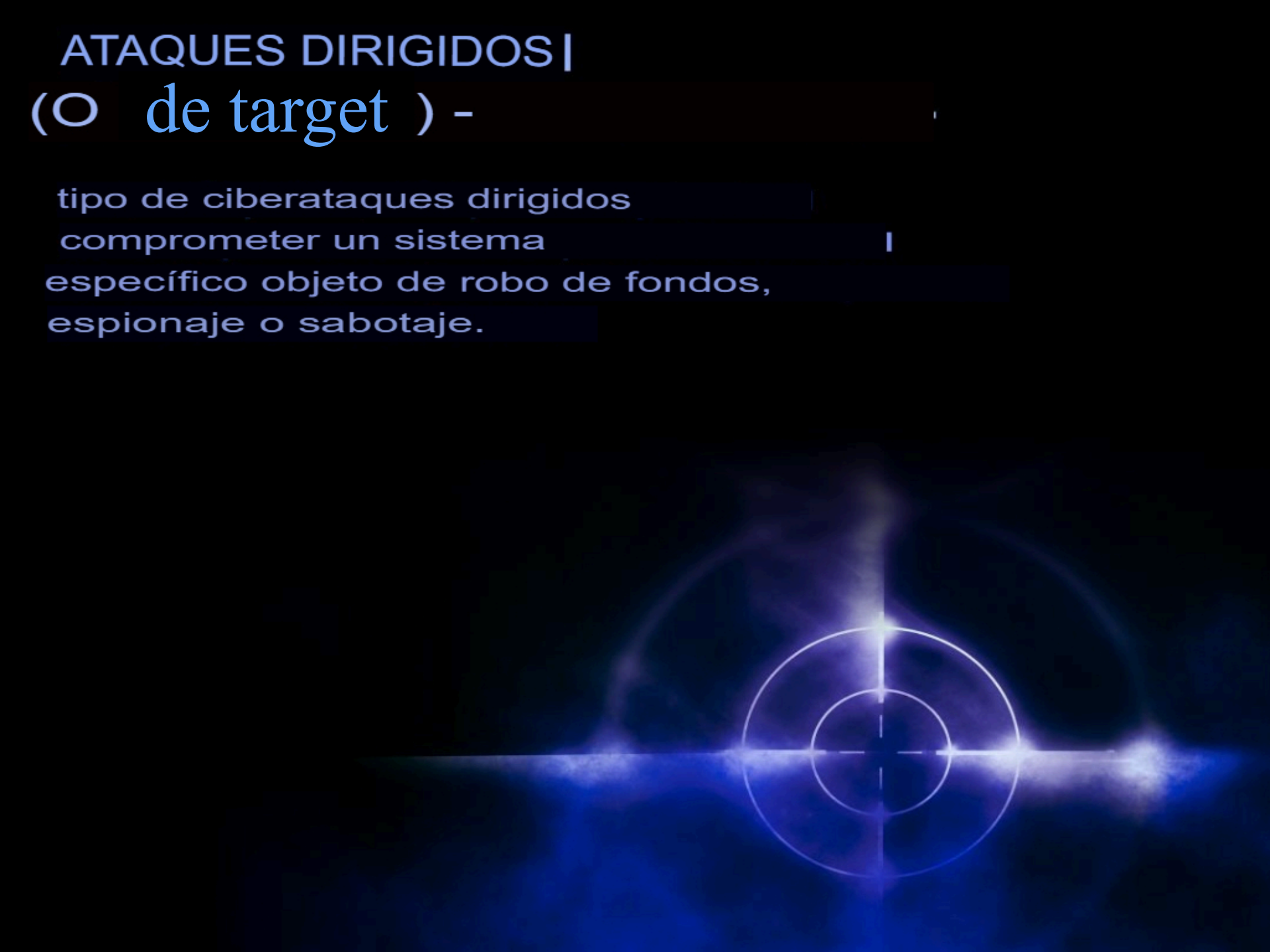
ПОВЕРХНОСТЬ АТАКИ —

ОБЩЕЕ КОЛИЧЕСТВО ВОЗМОЖНЫХ УЯЗВИМОСТЕЙ В КОНКРЕТНОЙ СИСТЕМЕ.

ATAQUES DIRIGIDOS

(O de target) -

tipo de ciberataques dirigidos
comprometer un sistema
específico objeto de robo de fondos,
espionaje o sabotaje.



ЦЕЛЕВЫЕ АТАКИ (ИЛИ ТАРГЕТИРОВАННЫЕ) —

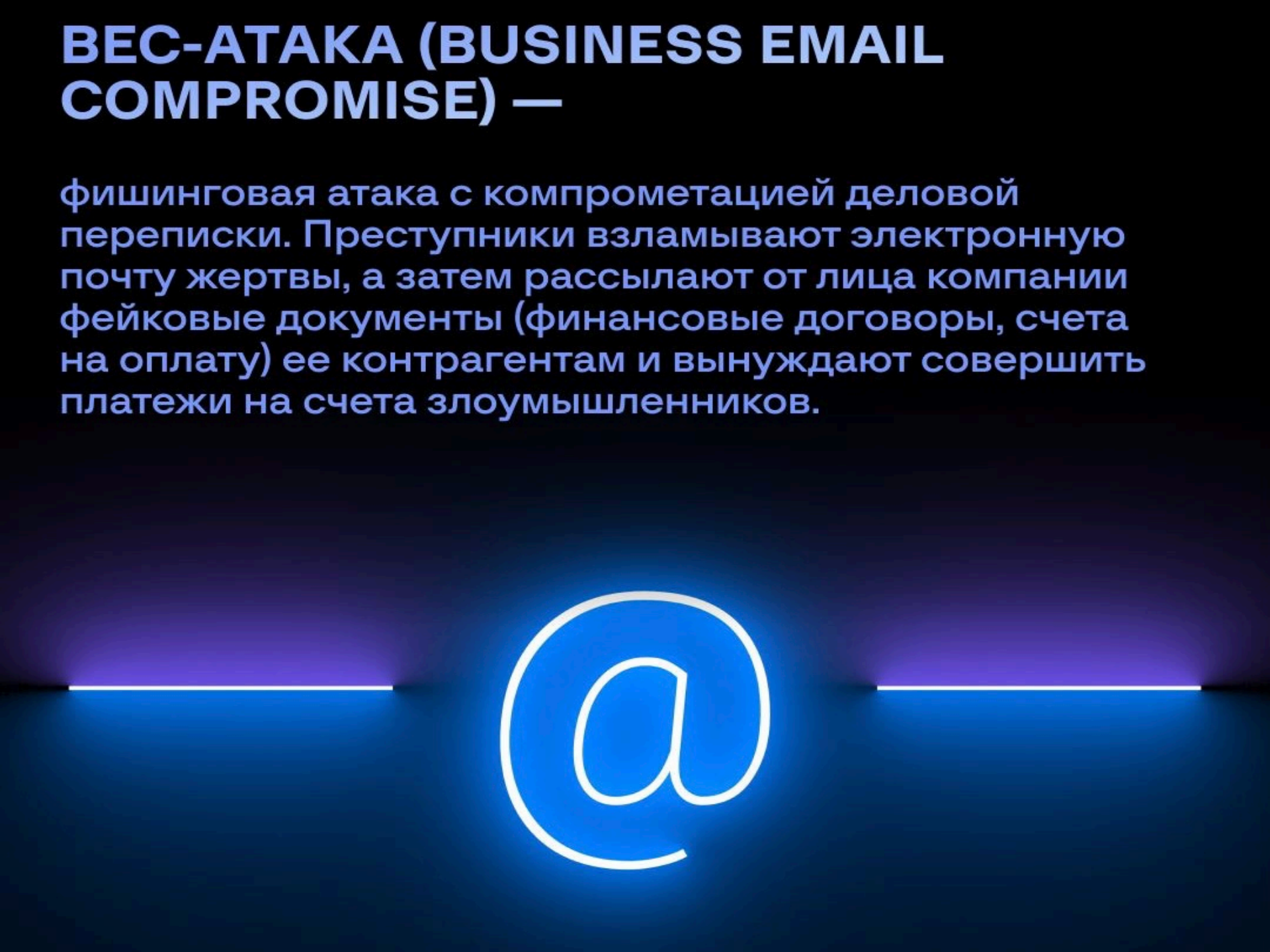
вид кибератак, которые направлены на компрометацию конкретной системы или объекта для хищения денежных средств, шпионажа или саботажа.

ATAQUE DE RECARGA (BUSINESS EMAIL COMPROMISE) --

ataque de phishing que compromete el negocio correspondencias. Delincuentes piratean electrónica el correo de la víctima y luego enviado en nombre de la empresa documentos falsos (contratos financieros, cuentas para pagar a sus contrapartes y obligarlos a realizar pagos a cuentas de intrusos.

BEC-АТАКА (BUSINESS EMAIL COMPROMISE) —

фишинговая атака с компрометацией деловой переписки. Преступники взламывают электронную почту жертвы, а затем рассылают от лица компании фейковые документы (финансовые договоры, счета на оплату) ее контрагентам и вынуждают совершить платежи на счета злоумышленников.



ATAQUE DOS (DENIAL OF SERVICE, DENEGACIÓN DE SERVICIO) --

ciberataque para dificultar acceso
de usuario inaccesible o
servicios relacionados al recurso atacado.

DOS-АТАКА (DENIAL OF SERVICE, ОТКАЗ В ОБСЛУЖИВАНИИ) —

кибератака с целью затруднить или сделать недоступным доступ пользователей или связанных сервисов к атакуемому ресурсу.

ATAQUE DDOS

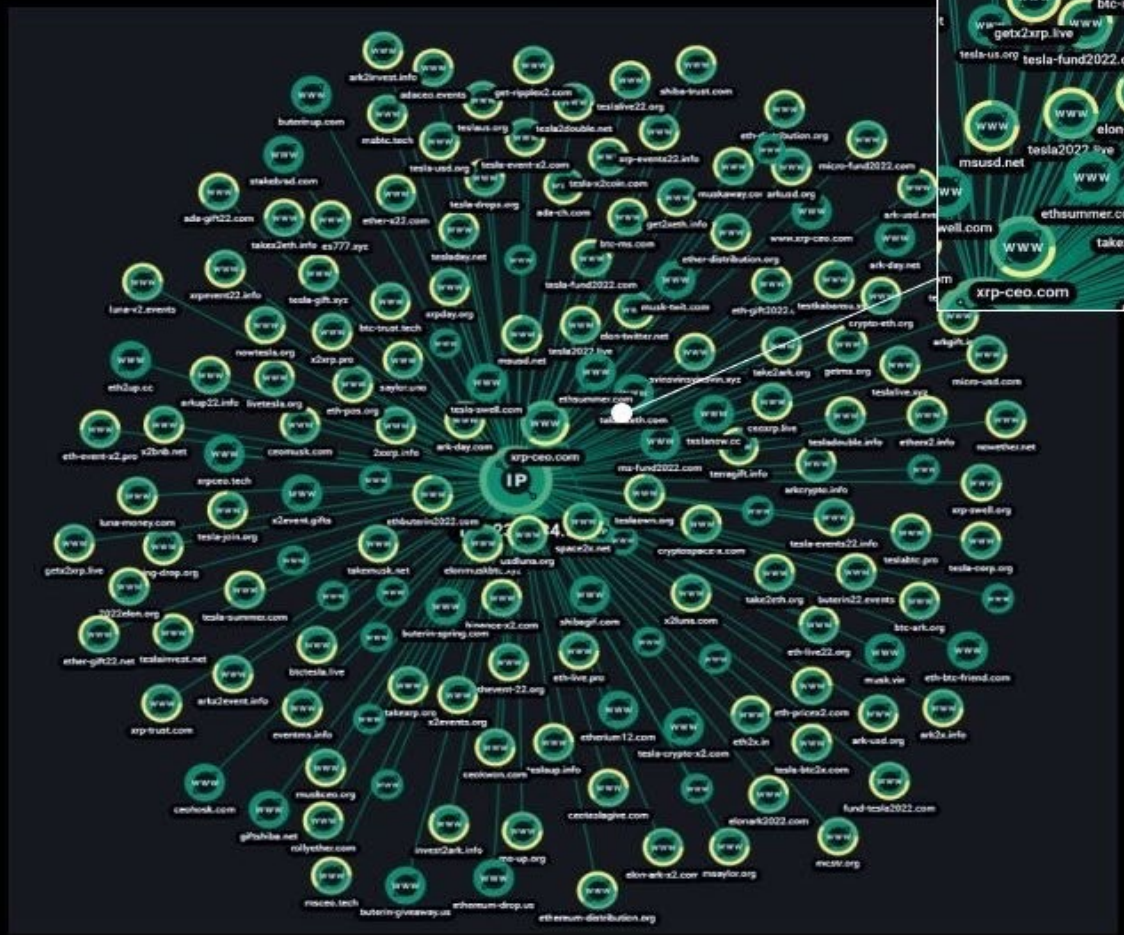
(DISTRIBUTED DENIAL OF SERVICE) -

ataque que carga el servido y se ejecuta simultáneamente con un gran número de ordenadores (a menudo se utiliza una red de "zombies infectados- computadoras") para crear un crecimiento en forma de avalancha solicitud de un recurso y, por lo tanto, incapacitarlo.

DDOS-АТАКА (DISTRIBUTED DENIAL OF SERVICE) —

атака, создающая нагрузку на сервер и выполняемая одновременно с большого числа компьютеров (зачастую используется сеть из зараженных «зомби-компьютеров»), чтобы создать лавинообразный рост запросов к ресурсу и тем самым вывести его из строя.

Esquema de una red de estafadores
construida utilizando un gráfico de infraestructura de red



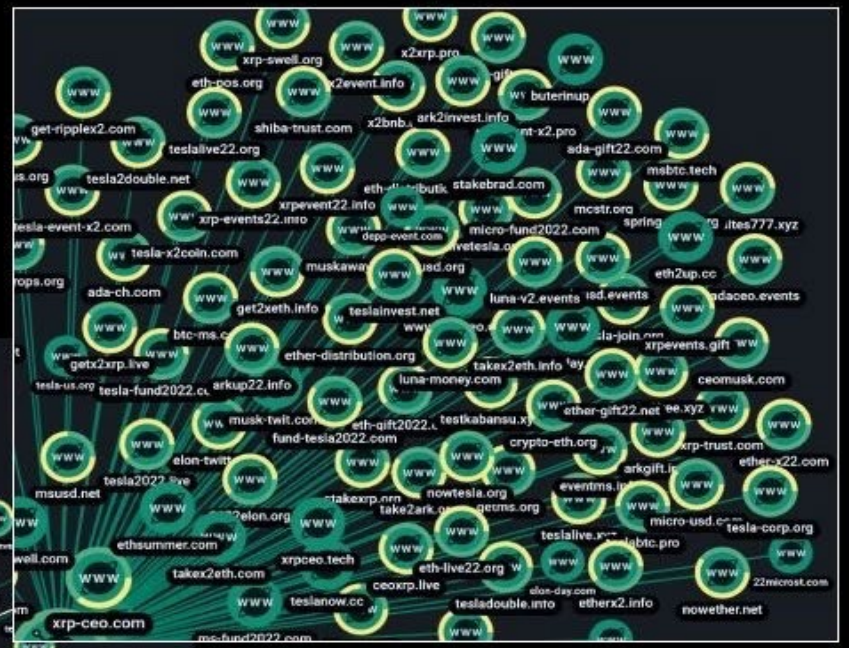
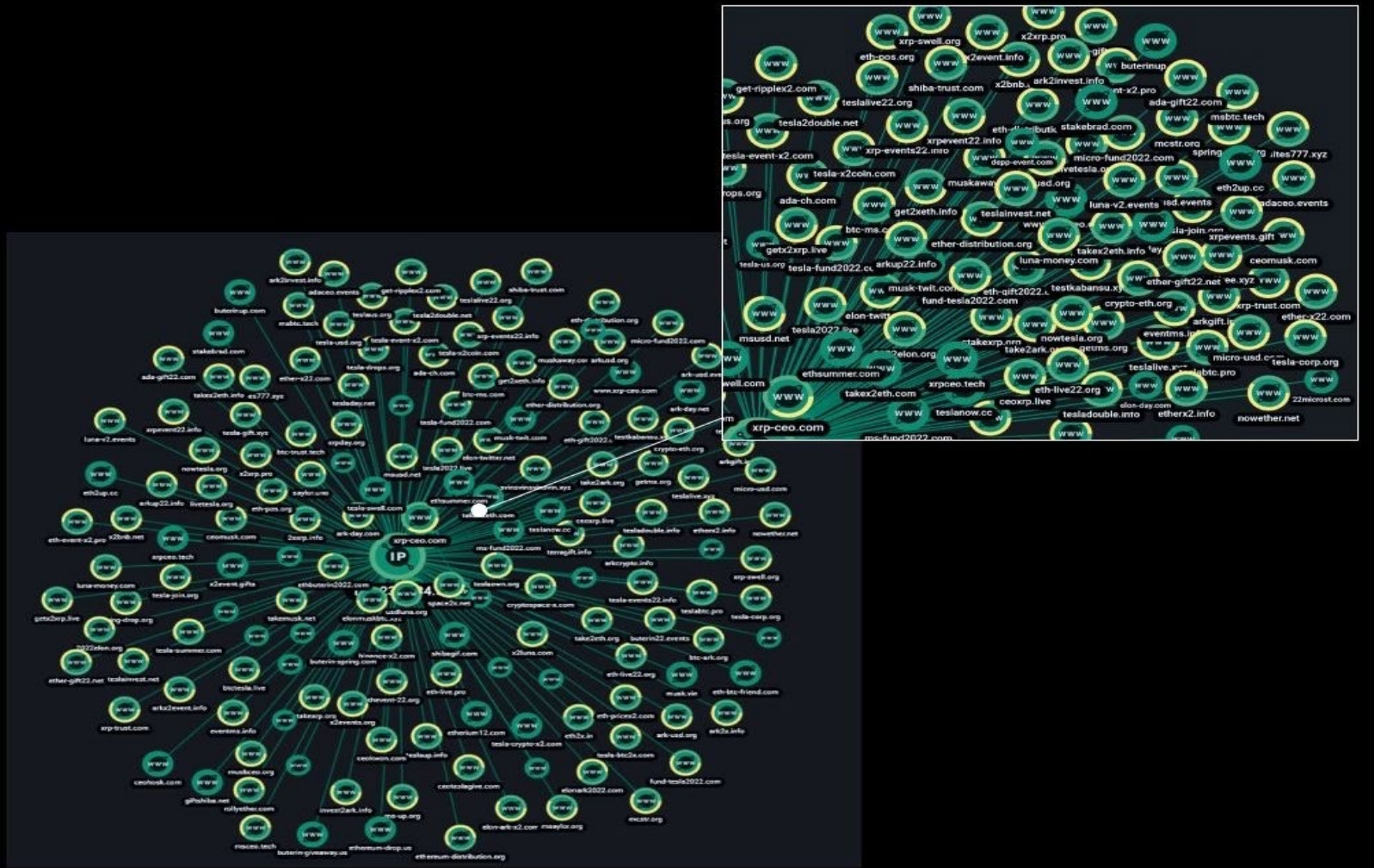


Схема мошеннической сети, построенная с помощью графа сетевой инфраструктуры

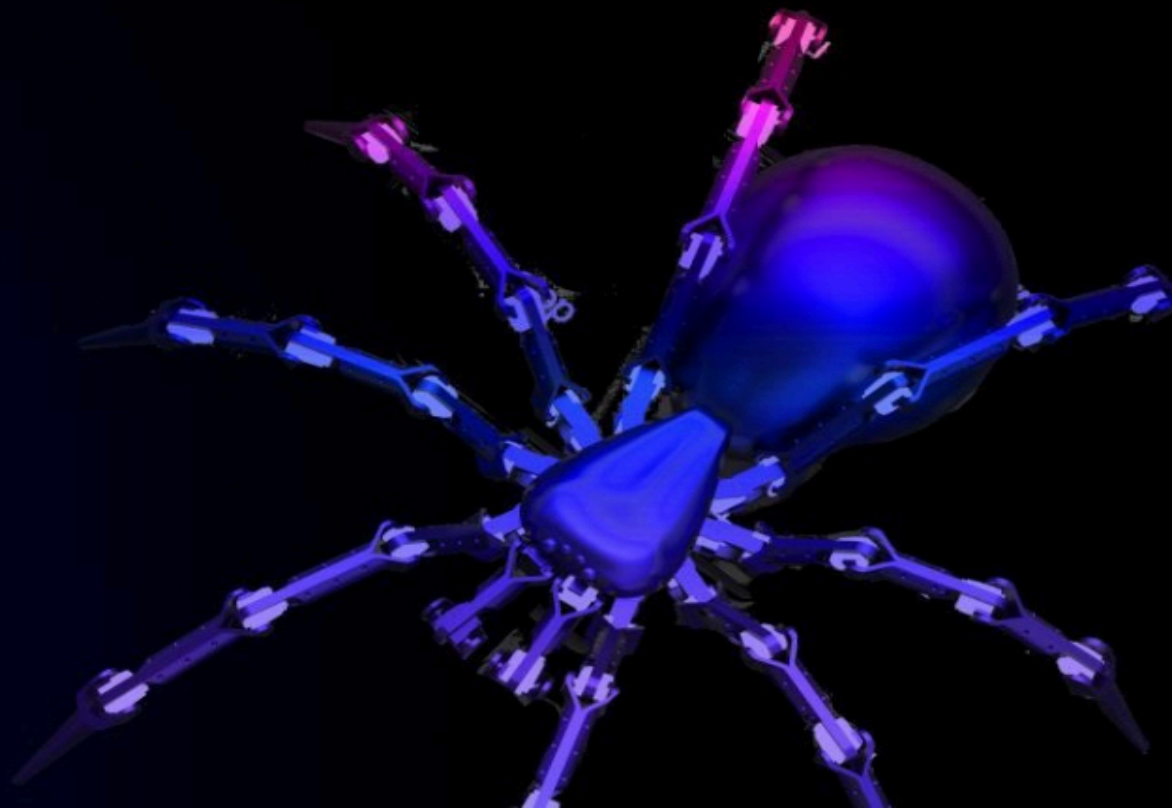


PROGRAMA DE CIFRADO -

TIPO DE MALWARE

PROGRAMAS.

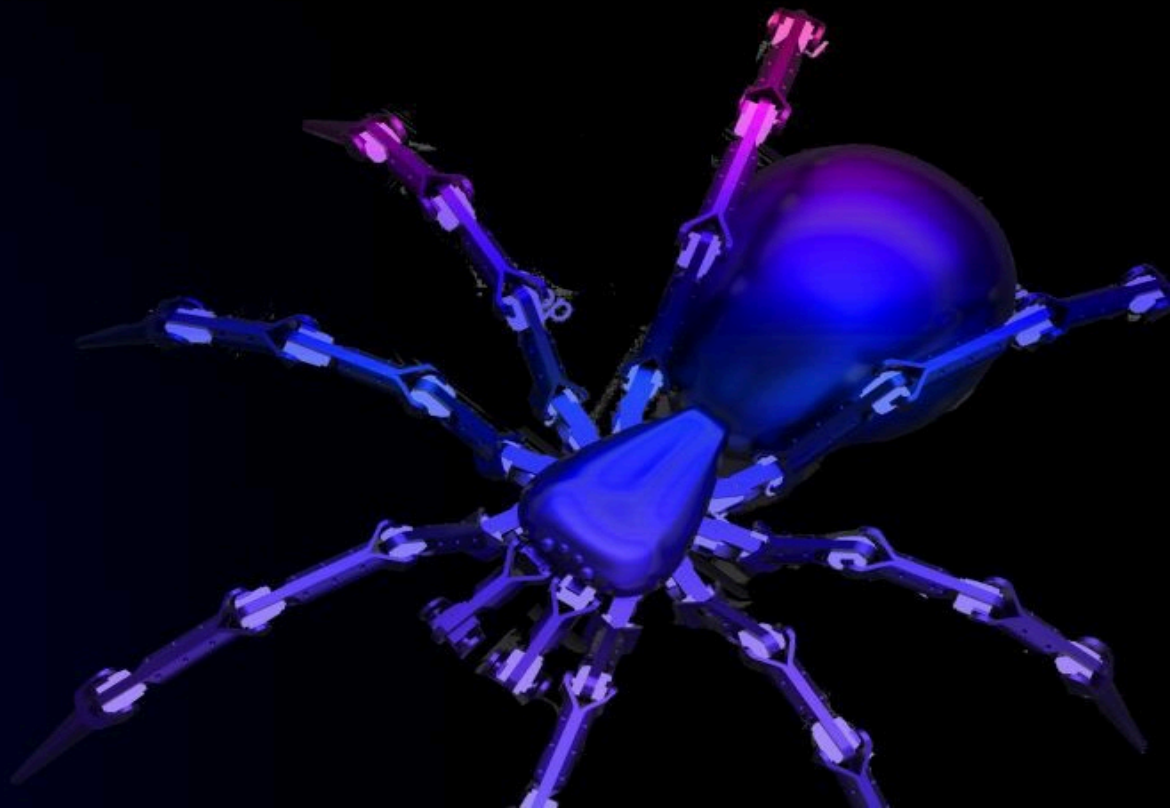
ENCRIPTA LOS DATOS Y LUEGO EXIGE A LA VÍCTIMA EXTROCIÓN PARA RECUPERAR EL ACCESO. PROMEDIO DE EJECUCIONES HIPOTECARIAS REQUERIDAS EN 2021, $247,000.



ПРОГРАММА-ШИФРОВАЛЬЩИК —

РАЗНОВИДНОСТЬ ВРЕДОНОСНОЙ ПРОГРАММЫ.

ШИФРУЕТ ДАННЫЕ И ЗАТЕМ ТРЕБУЕТ ОТ ЖЕРТВЫ ВЫКУП ДЛЯ ВОССТАНОВЛЕНИЯ ДОСТУПА. СРЕДНИЙ РАЗМЕР ТРЕБУЕМОГО ВЫКУПА В 2021 ГОДУ — $247 000.



TROYANO - -

el malware que más penetra en el sistema bajo la apariencia de una aplicación legítima o archivo (¿recuerdas el mito del caballo de Troya ?), y, a diferencia de los gusanos, no tiene un mecanismo auto-difusión.

Los troyanos combinan un gran número de funciones: pueden recopilar información sobre el dispositivo o propietario, robar credenciales de Inicio de sesión en la banca en línea, cargar otros programas, robar o destruir datos etc.

ТРОЯН —

вредоносная программа, чаще всего проникающая в систему под видом легитимного приложения или файла (помните миф про Троянского коня?), и, в отличие от червей, не имеющая механизма самораспространения.
Трояны сочетают большое количество функций: могут собирать информацию об устройстве или владельце, похищать учетные данные для входа в онлайн-банкинг, подгружать другие программы, воровать или уничтожать данные и т.д.

DROPPER -.

malware diseñado para instalación
no autorizado y oculto al usuario instalación
en el ordenador de la víctima de otro
malware.

ДРОППЕР —

вредоносная программа, предназначенная для несанкционированной и скрытой от пользователя установки на компьютер жертвы другого вредоносного ПО.

Puerta TRASERA - -

malware que permite el atacante
se conecta en cualquier momento
computadora de la víctima y realizar acciones de
forma remota con la computadora:
reiniciar, iniciar programas, copiar archivos,
descargar otros malware, etc.

БЭКДОР —

вредоносная программа, позволяющая злоумышленнику в любой момент подключаться к компьютеру жертвы и удаленно выполнять действия с компьютером: перезагружать, запускать программы, копировать файлы, загружать другие вредоносные программы и т.д.

KEYLOGGER --

Keylogger, software,
capaz de capturar y interceptar todas las acciones usuario
en el teclado, movimiento y pulsación teclas del
ratón, así como tomar capturas de pantalla.

КЕЙЛОГГЕР —

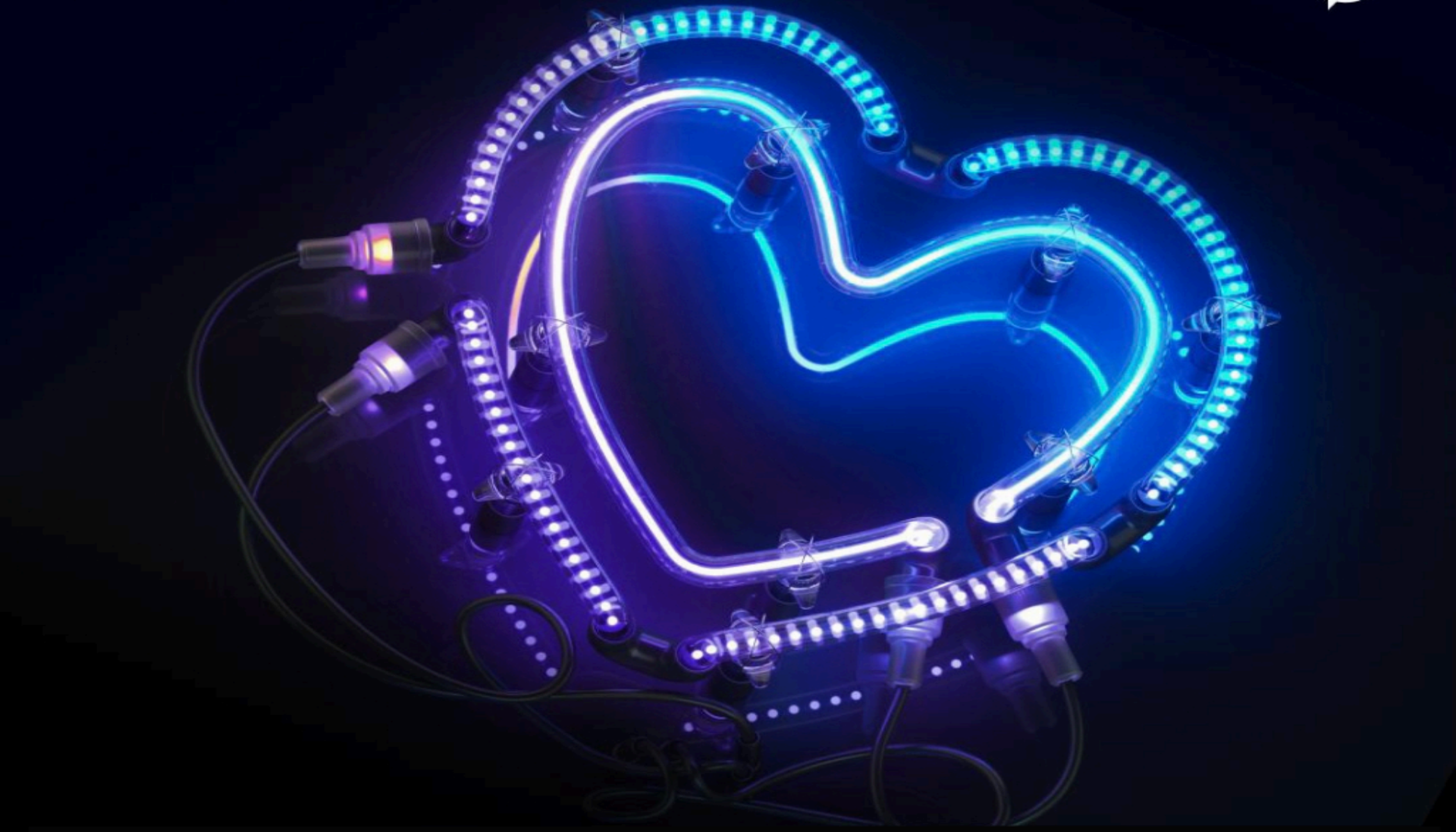
клавиатурный шпион, программное обеспечение, способное перехватывать и фиксировать все действия пользователя на клавиатуре, движение и нажатия клавиш мыши, а также делать снимки экрана.

STEELER - -

malware para robar a un infectado registros de computadora: contraseñas, cookies, historial navegador, pantallas de Escritorio, datos tarjetas bancarias.

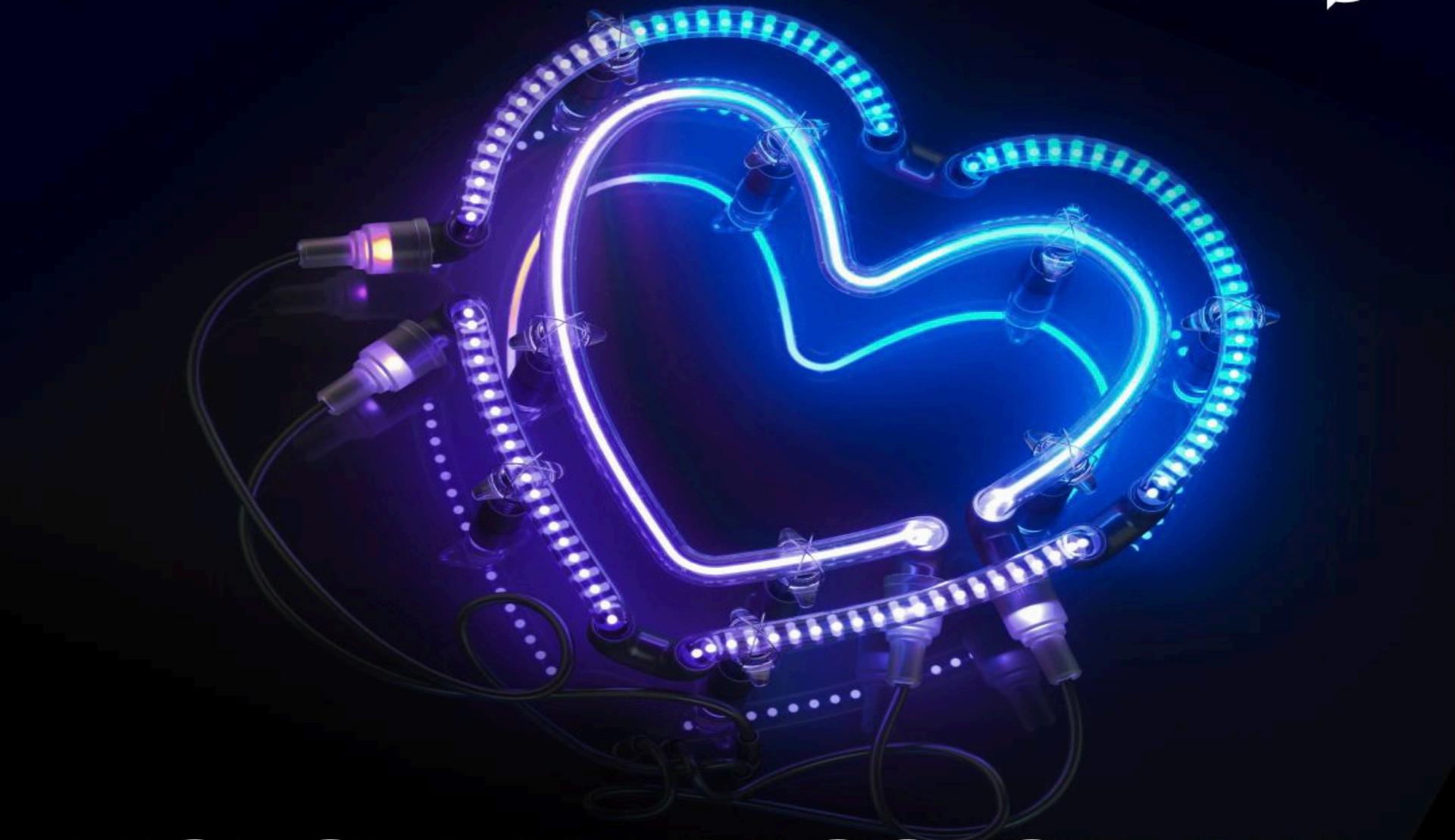
СТИЛЕР —

вредоносная программа для кражи с зараженного компьютера логов: паролей, куки-файлов, истории браузера, скринов рабочего стола, данных банковских карт.



AMOR A DISTANCIA:

Esquema fraudulento popular
Fake Date ha salido de Rusia



ЛЮБОВЬ НА РАССТОЯНИИ:

популярная мошенническая схема Fake Date вышла за пределы России

SEÑALES DE UN SITIO DE PHISHING:

* No hay conexión segura: dirección la página comienza con http\\, no https\\, falta el icono de candado;

- El dominio es nuevo y registrado recientemente (puede verificar la fecha de registro, por ejemplo, a través del Servicio whois7.ru);

- El sitio se ve extraño: logotipos turbios, imágenes de baja calidad, gramaticales y errores de sintaxis, irrelevante información;

* El nombre del dominio es diferente del nombre recursos originales, por ejemplo, en la dirección línea en lugar de google.com tal vez qoogle.com ;

- Área de dominio inusual: por ejemplo, en lugar de. ru или.com el sitio está registrado en.online.

ПРИЗНАКИ ФИШИНГОВОГО САЙТА:

- Отсутствует безопасное соединение: адрес страницы начинается с http\\, а не https\\, отсутствует значок замка 🔒;
- Домен свежий и зарегистрирован совсем недавно (проверить дату регистрации можно, например, с помощью сервиса whois7.ru);
- Сайт выглядит странно: мутные логотипы, некачественные картинки, грамматические и синтаксические ошибки, неактуальная информация;
- Название домена отличается от названия оригинального ресурса, например, в адресной строке вместо google.com может быть qoogle.com;
- Необычная доменная зона: например, вместо .ru или .com сайт зарегистрирован на .online.

SEÑALES DE UN CORREO ELECTRÓNICO DE PHISHING:

* Tono emocional: la carta promete grandes ganancias, recibir un regalo o un bono, o, por el contrario, causa miedo o ansiedad;

* El remitente pide prisa (Date prisa, más bien, abre, tienes una hora, tres horas, 24 horas en tomar una decisión, de lo contrario su bono se quemará, reenviar urgentemente...);

* Errores tipográficos, errores, gráficos de baja calidad;

* El atacante puede presentarse como su conocidos o actuar en nombre de un conocido marca: Mira cuidadosamente la dirección, de donde vino la carta.

ПРИЗНАКИ ФИШИНГОВОГО ПИСЬМА:

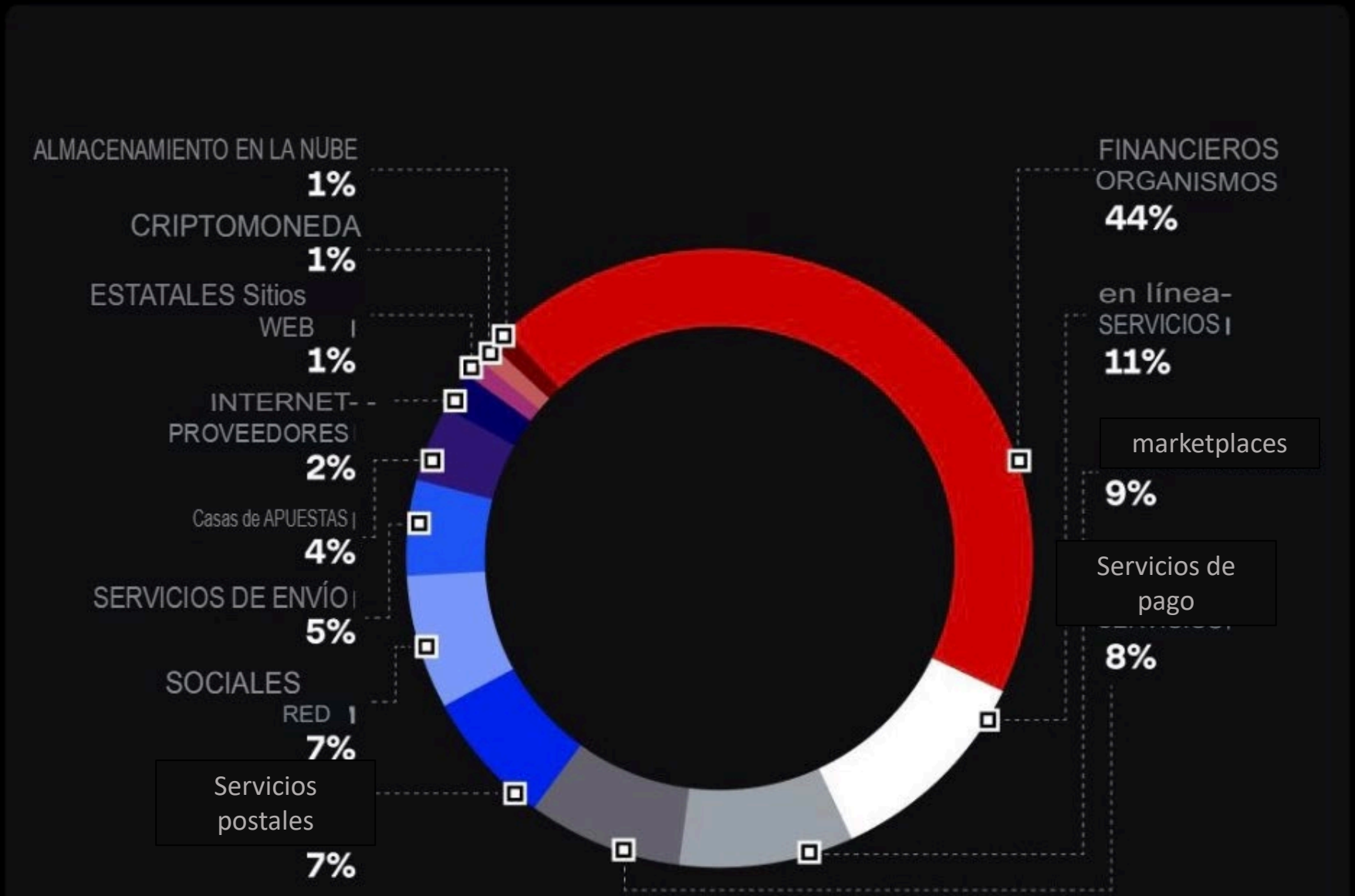
- Эмоциональный оттенок: письмо либо обещает крупный выигрыш, получение подарка или бонуса, либо, наоборот, вызывает страх или тревогу;

- Отправитель побуждает к спешке (торопитесь, скорее откройте, у вас час, три часа, 24 часа на принятие решение, иначе ваш бонус сгорит, срочно перешлите...);

- Опечатки, ошибки, некачественная графика;

- Злоумышленник может представиться вашим знакомым или действовать от имени известного бренда: внимательно смотрите на адрес, с которого пришло письмо.

Recursos de phishing en Runet en 2022



Фишинговые ресурсы в Рунете в 2022 году