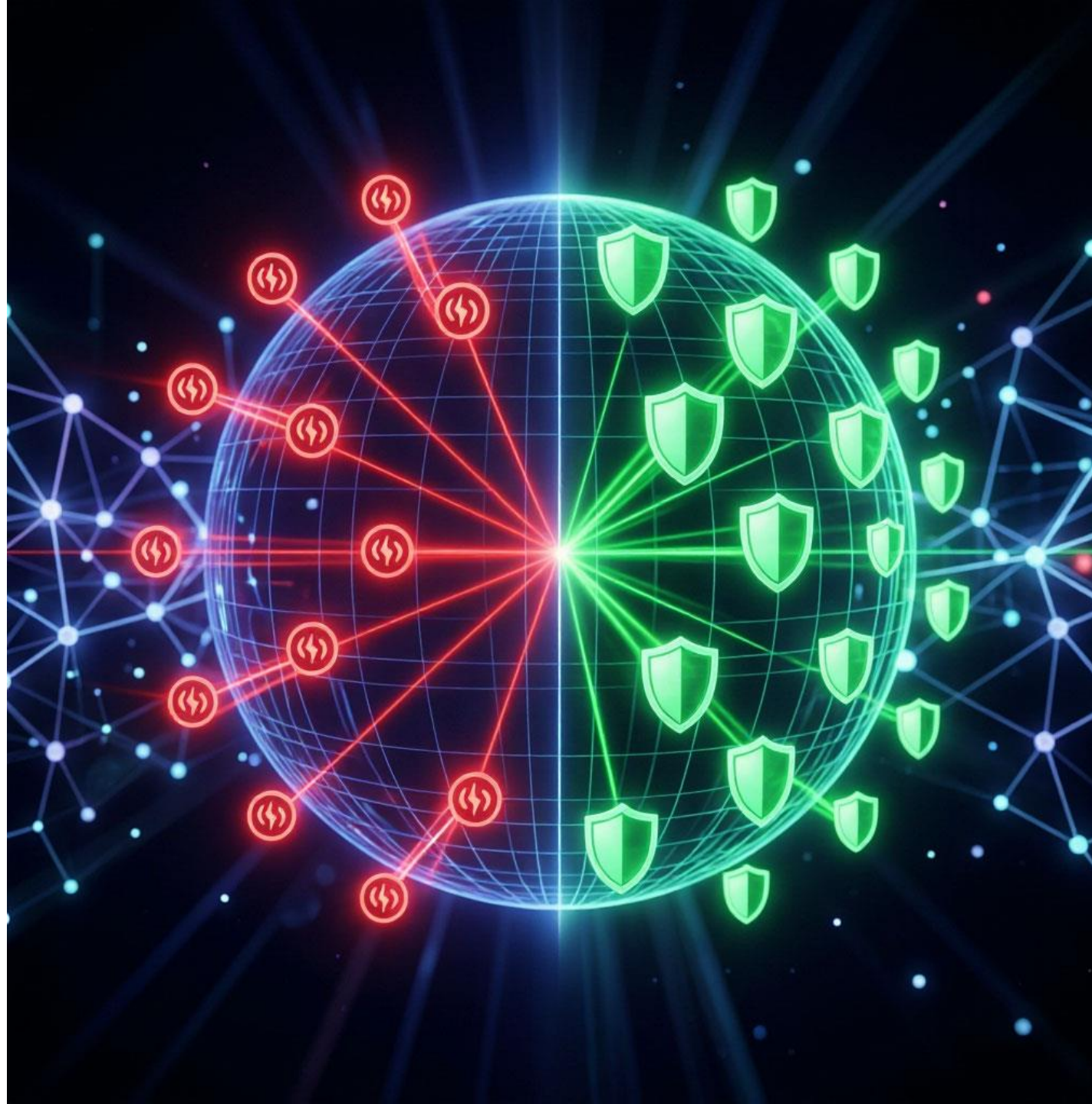


Две стороны DNS: аналитика угроз и моделирование защиты

TLDCON 2026

Ташкент, сентябрь 2026





Ольга Баскакова
Руководитель проектов



Станислав Гончаров
Руководитель
департамента защиты от
цифровых рисков

F6



Андрей Петров
Директор по
информационной
безопасности



Сергей Журило
Директор по
информационной
безопасности



Дмитрий Коваленко
Архитектор DNS-решений



TLDCON 2026

Ташкент, сентябрь 2026

ПРИКЛАДНОЙ КИБЕРБЕЗ



Maliciously Registered Domains

были зарегистрированы
непосредственно с вредоносной целью

Compromised Domains

изначально легитимные домены,
которые были взломаны



Для пользователя картина одна. Природа угрозы — разная

Домен зарегистрирован для атаки

Администратор действует осознанно. Домен создан как часть инфраструктуры атаки.

Легитимный домен взломан

Администратор — пострадавшая сторона.

Домен используется не по назначению.

Внешне результат идентичен: фишинг, распространение ВПО,
мошенничество

Отсюда и соблазн реагировать одинаково — блокировкой домена в обоих случаях

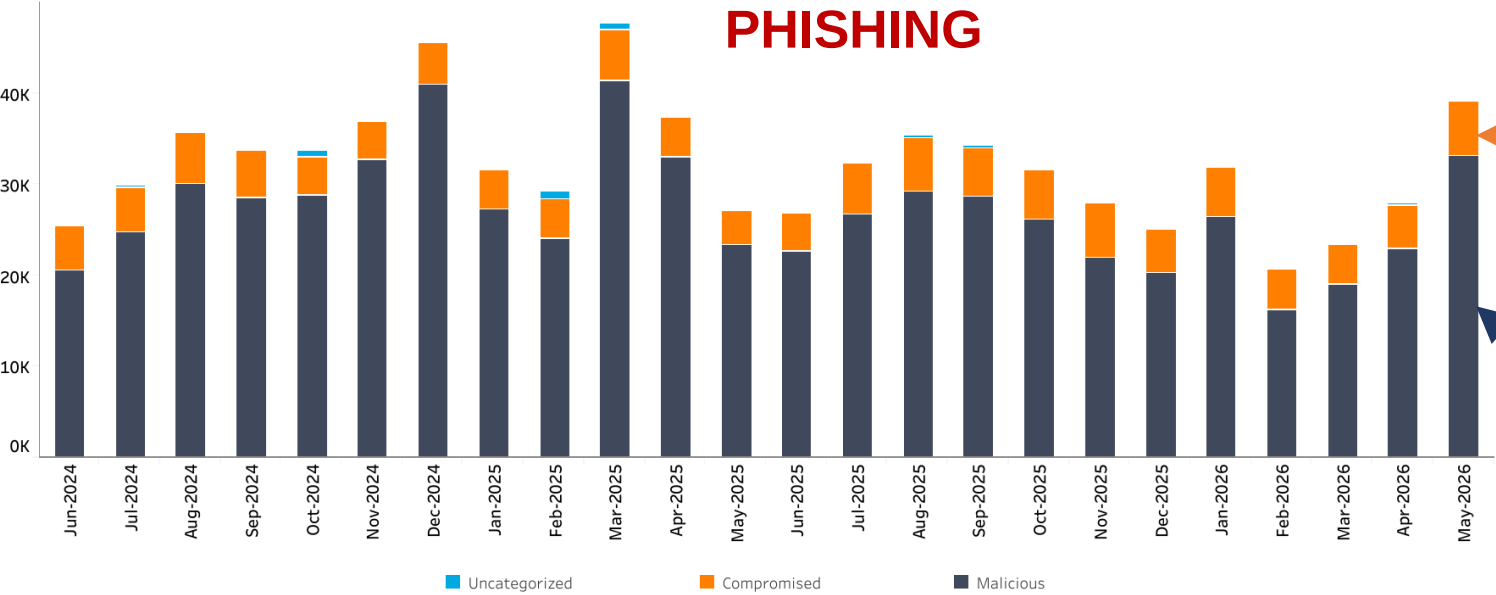
НЕМНОГО ЦИФР



Reporting Periods in View:
Last 24 Reporting Periods

Date Range: 2024-06 to 2026-05

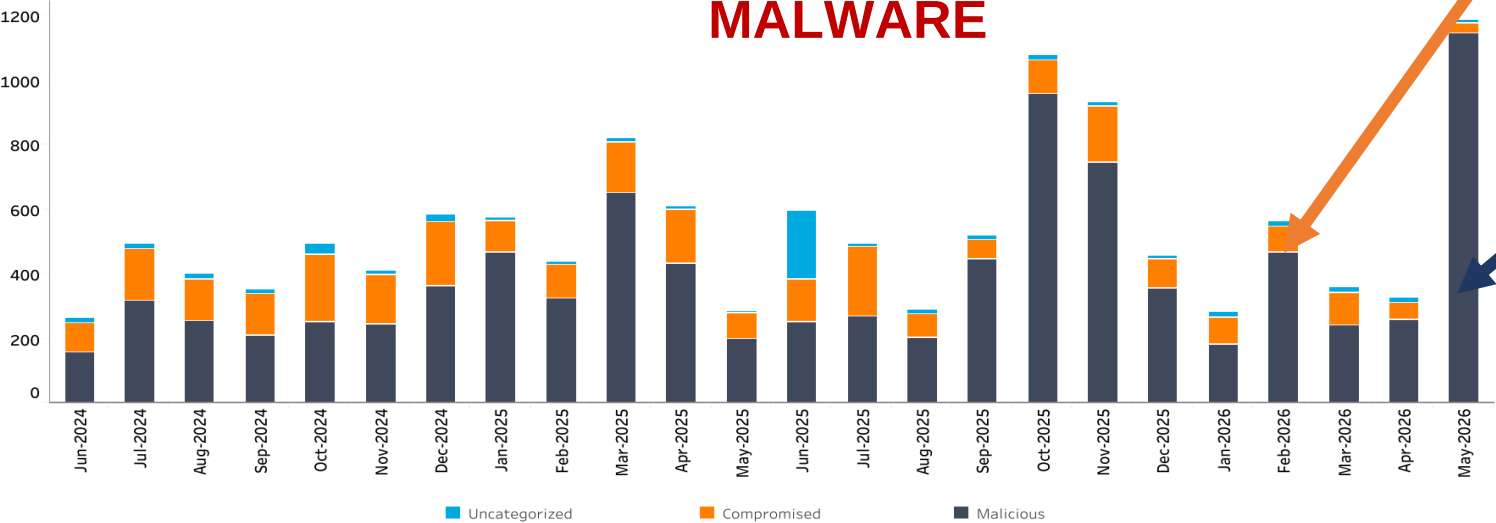
Abuse Type:
Phishing



Compromised

Maliciously
Registered

Last 24 Reporting Periods



Тенденция взломов

F6

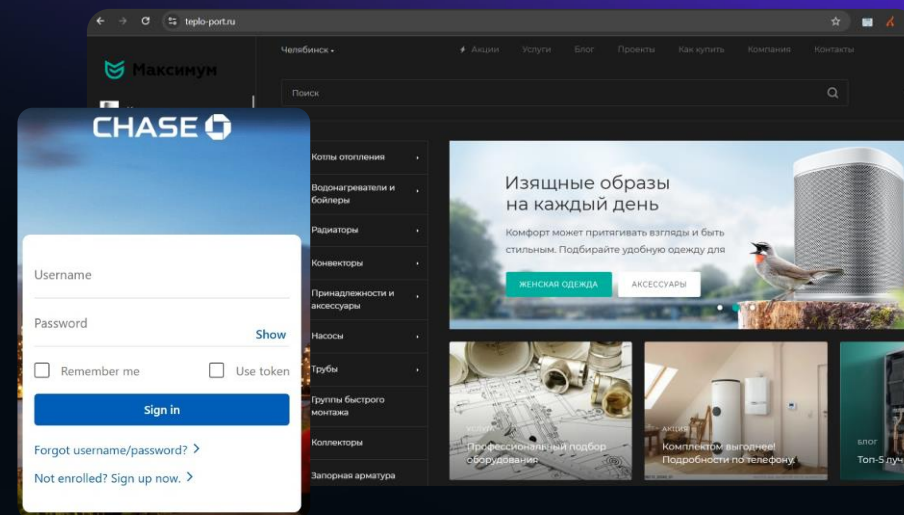
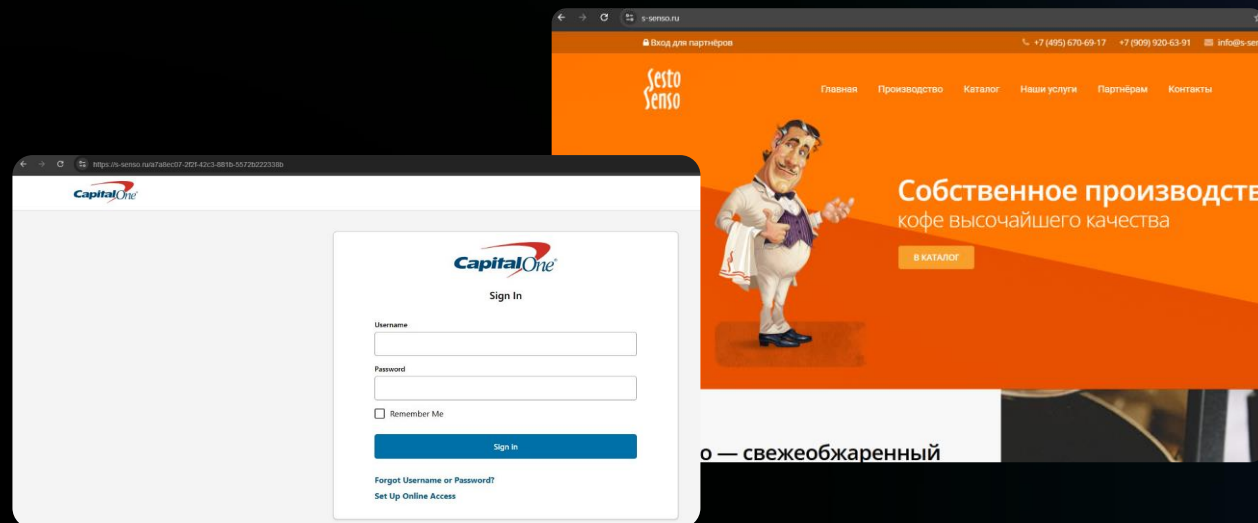
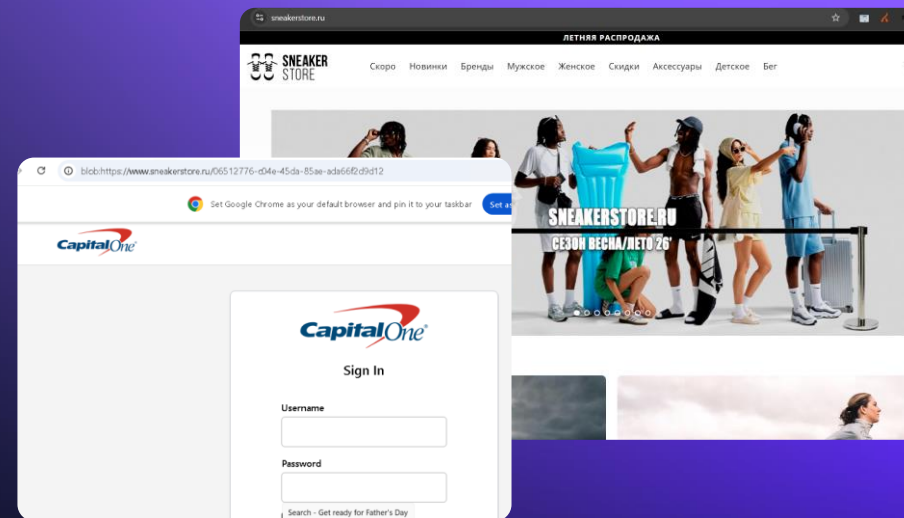
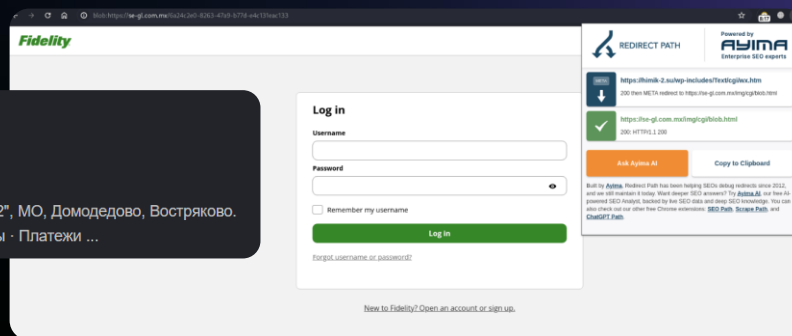
За последний год (с 23.06.2025 до 23.06.2026) CERT F6 было обработано 57 взломанных ресурсов, что в 3 раза больше, чем в прошлом году



himik-2.su
<https://himik-2.su/view/item>

СНТ "ХИМИК-2", Домодедово

СНТ "ХИМИК-2", Домодедово. Официальный сайт СНТ "Химик-2", МО, Домодедово, Востряково. Перейти к содержанию. Главная · Бланки · Документы · Контакты · Платежи ...



СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГРОЗ



ЦЕЛИ

ИНСТРУМЕНТЫ

ПРИЗНАКИ



Злонамеренная регистрация/взломы

F6

Методы реагирования

Этап	Коректные действия	Злонамеренная регистрация	Взломы
Проверка	✓	Признаки фишинга / скама / распространения ВПО	Открыть ресурс без маски Поисковая выдача WebArchive Whois
Реагирование	✓	КЦ РФ Хостинг-провайдер Регистратор Регулятор доменной зоны	Обращение к администратору ресурса КЦ РФ Хостинг-провайдер Регистратор Регулятор доменной зоны
	✗	Обращение к администратору ресурса	Реагирование без попытки связаться с владельцем ресурса

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГРОЗ



ЦЕЛИ

ИНСТРУМЕНТЫ

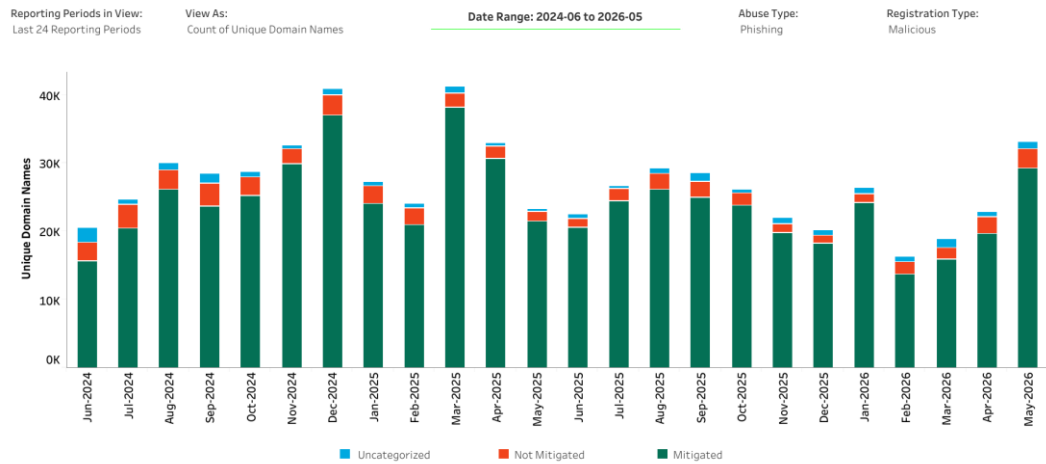
ПРИЗНАКИ



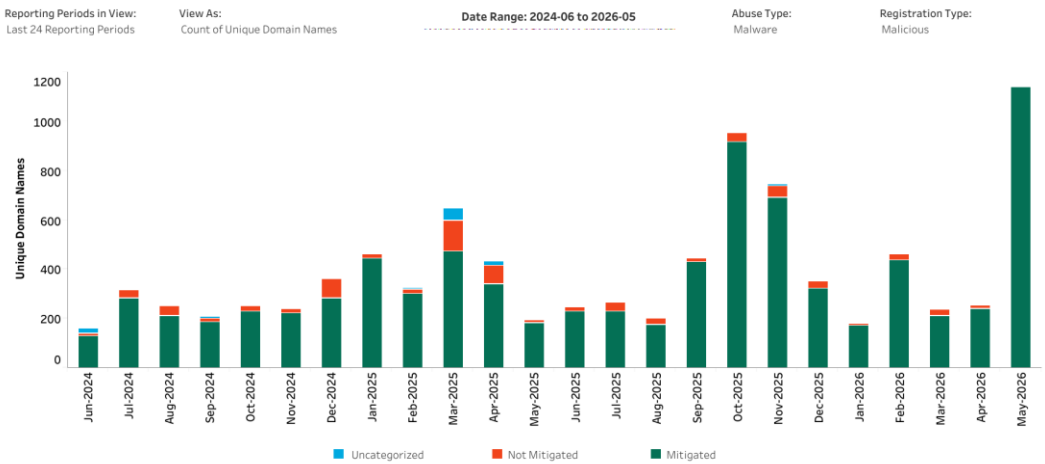
ЕЩЕ НЕМНОГО СТАТИСТИКИ



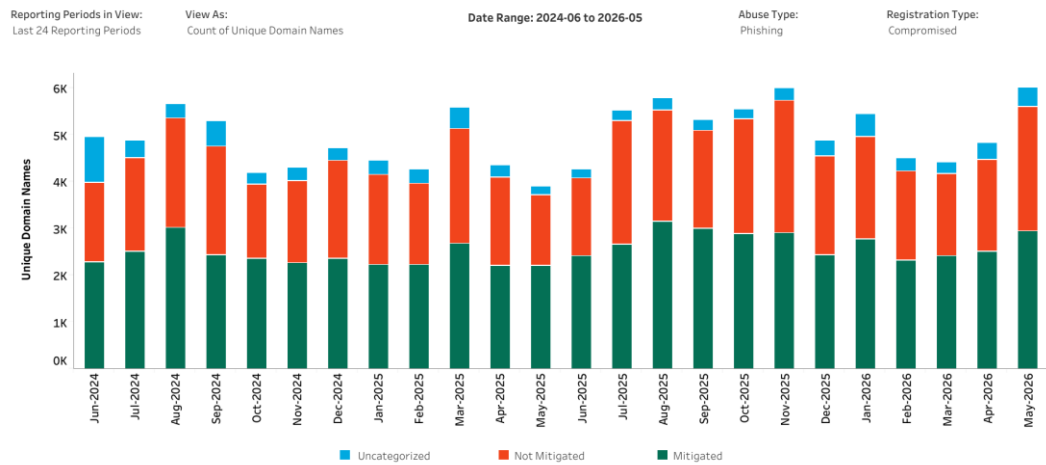
MALICIOUSLY (phishing)



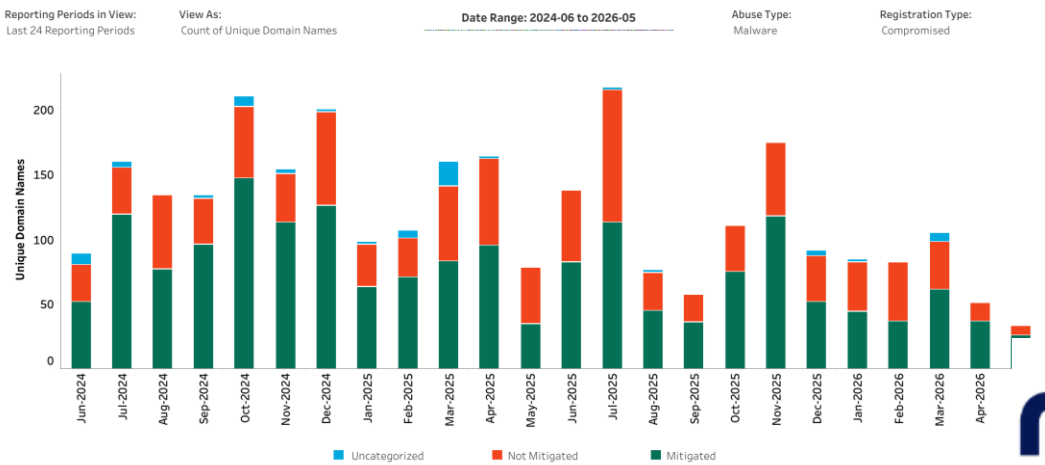
MALICIOUSLY (malware)



COMPROMISED (phishing)



COMPROMISED (malware)



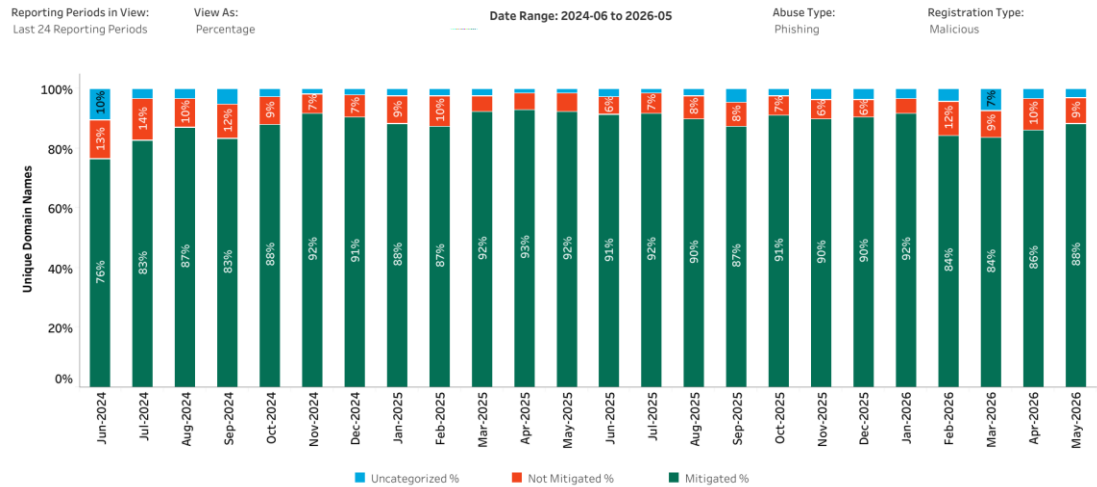
Mitigated

Not Mitigated

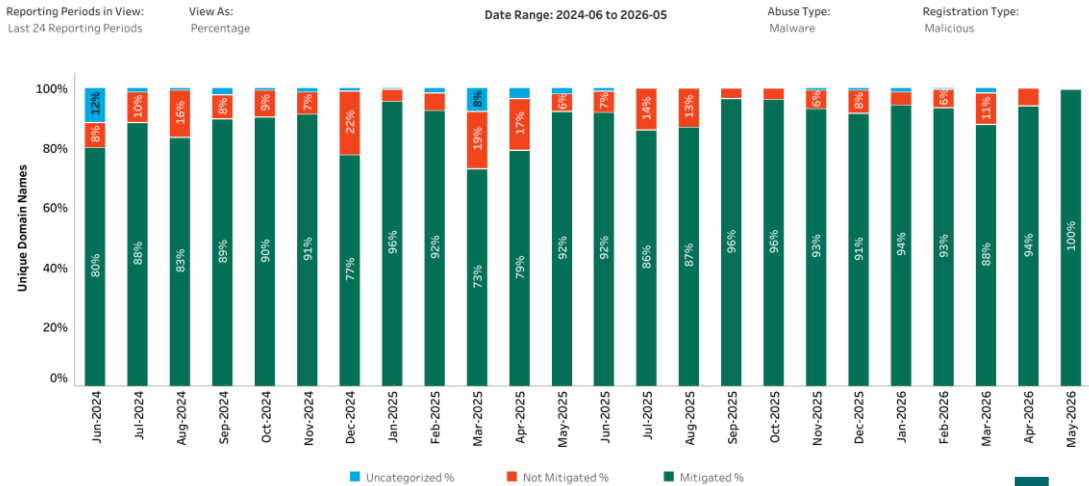
ЕЩЕ НЕМНОГО СТАТИСТИКИ



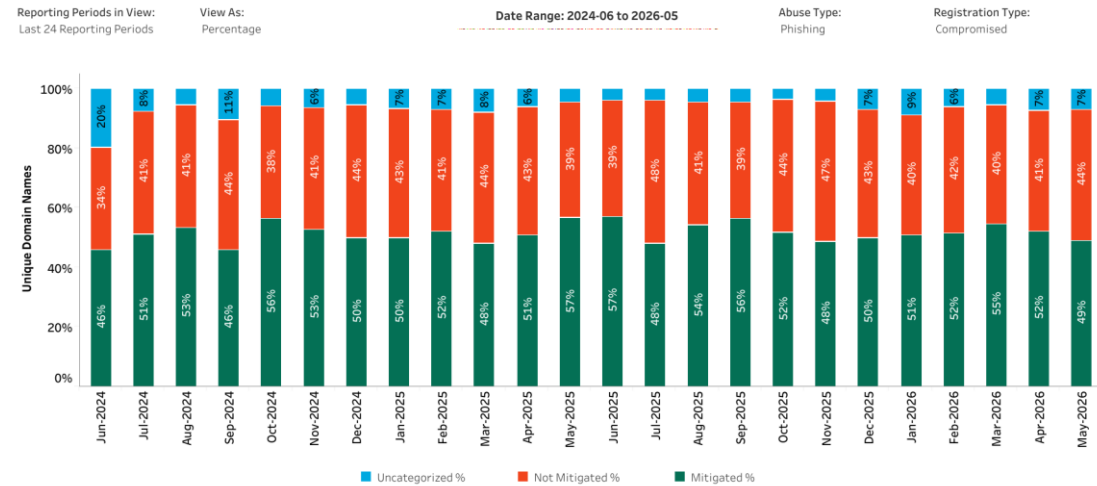
MALICIOUSLY (phishing)



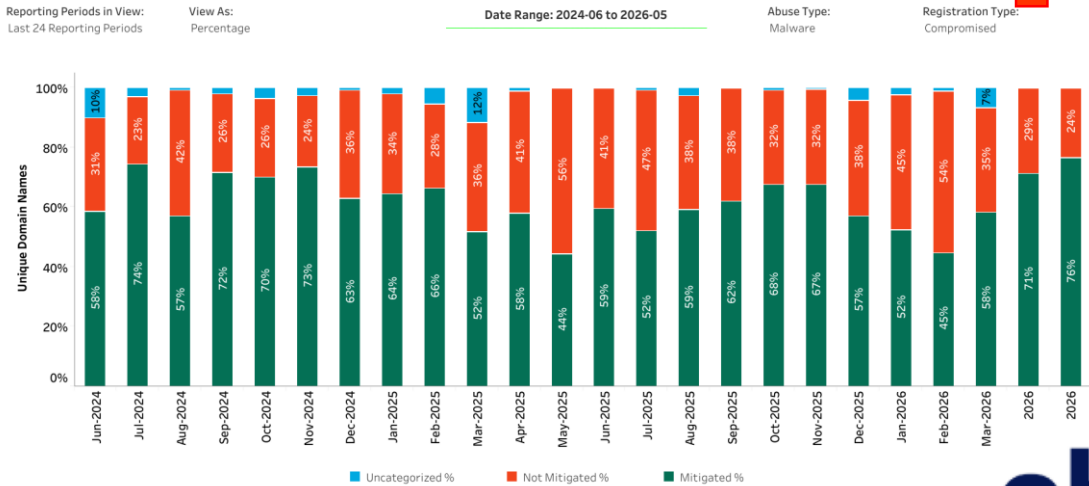
MALICIOUSLY (malware)



COMPROMISED (phishing)



COMPROMISED (malware)



Mitigated

Not Mitigated

СХОЖЕСТЬ И ОТЛИЧИЯ В МЕТОДАХ РЕАГИРОВАНИЯ



Кто должен реагировать в случае компрометации

Отличия в работе в gTLD и страновых доменах

Взлом сайта



Контент сайта



Затруднение
выявления
хостинг-
провайдера



Обращение
к регистратору



Обращение
к хостинг-
провайдеру



gTLD

Действуют единые правила в рамках договоров между ICANN и регистраторами, регистратурами. В соответствии с RAA первично обращение по факту выявленного DNS abuse должен рассматривать регистратор.



ccTLD

Порядок противодействия нарушениям определяется правилами конкретной национальной доменной зоны, национальным законодательством. Поэтому они разнятся от зоны к зоне. В зависимости от реализованного в правилах ccTLD механизма противодействия угрозам – это, как правило:

регистратор / компетентная организация / оператор доменной зоны

Кейсы долгого реагирования

F6

Мошеннический сайт с предложением установки стороннего приложения под предлогом получения работы. Для установки приложения требовалось войти в Apple ID, который принадлежал киберпреступнику. В следствие входа в аккаунт устройство жертвы блокировалось как украденное, телефон жертвы превращался в "Кирпич", на экране блокировки мошенник устанавливал сообщение с требованием выкупа для разблокировки устройства. Регистратор принимал решение об отказе в отключении данного домена по причине того, что они рассматривали его как классический фишинг, коим ресурс не был. В результате долгих переговоров ресурс был заблокирован. Устранение нарушения заняло 112 дней.



Блокировка домена при компрометации — чрезмерная мера

Отключается вместе с доменом:

- сайт и все поддомены
- корпоративная почта
- CRM, платежи, интеграции
- доступы сотрудников и SSO

**«Сжечь дом целиком, чтобы
убить паука в подвале»**



Выявление и реагирование: асимметрия информации и полномочий

Регистраторы видят угрозу на моменте регистрации

Но не имеют полномочий предпринимать меры.

Первым при компрометации реагирует провайдер

Потому что в данном случае скомпрометирован сайт или его сегмент, не домен. Вспоминаем про паука.

В .ru/.рф и gTLD/newgTLD отличаются возможности

В иностранных зонах регистратор имеет возможность самостоятельно блокировать заведомо злонамеренный домен. В .ru/.рф нужно обращаться в КО чтобы получить обратно запрос на блокировку уже от КО.

ЕСИА смещает угрозу, а не устраняет ее

**Чем сложнее
регистрировать
домены анонимно
и массово, тем больше
интерес к взлому
существующих
ресурсов.**

Типовые точки входа

- устаревшие CMS без обновлений
- переиспользуемые и слабые пароли
- забытые поддомены и тестовые стенды
- аккаунты администраторов в ЛК регистратора

Чем удобен взломанный ресурс

- история и возраст
- репутация в фильтрах и поиске
- доверие пользователей
- меньше подозрений на старте атаки

СХОЖЕСТЬ И ОТЛИЧИЯ В МЕТОДАХ РЕАГИРОВАНИЯ





СЛУЧАЙНЫЙ КЕЙС



TYPO-ДОМЕНЫ



ОДИНАКОВЫЕ ПЛАТЕЛЬЩИКИ



АВТОРЕГИСТРАЦИЯ ЧЕРЕЗ API

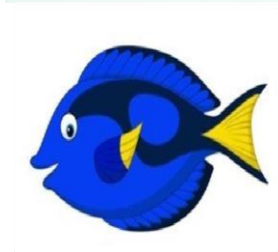
Описание: Замечена волна регистраций доменов с опечатками в названии бренда. Все оплачены одной картой. Заявки прошли через API реселлера



СЛУЧАЙНЫЙ КЕЙС



TLS АНОМАЛИЯ



C2 ТРАФИК



**ВСПЛЕСК ЗАПРОСОВ К РЕДКОМУ
ПОДДОМЕНУ**

Описание: Легитимный домен, но с одного из узлов идёт устойчивый C2 трафик. Аномальные TLS рукопожатия (нестандартные шифронаборы, частые переподключения). Отмечен резкий всплеск запросов на редкий поддомен



СЛУЧАЙНЫЙ КЕЙС



РЕГИСТРАЦИЯ ЧЕРЕЗ РЕСЕЛЛЕРА



БЫСТРОЕ ДЕЛЕГИРОВАНИЕ НА VPS



**ВСПЛЕСК DNS ЗАПРОСОВ К ВНЕШНИМ
IP**

Описание: Домен зарегистрирован формально легитимно через реселлера. Делегирован на VPS в течение 10 минут после регистрации. Отмечен всплеск DNS запросов к IP с плохой репутацией



СЛУЧАЙНЫЙ КЕЙС



НОВЫЙ ПАРТНЕР



МАССОВЫЕ РЕГИСТРАЦИИ



ЛЕГИТИМНЫЕ TLS-СЕРТИФИКАТЫ

*Описание: новый реселлер регистрирует много поддоменов.
Сертификаты — корректные.*



Ольга Баскакова
Руководитель проектов



Станислав Гончаров
Руководитель
департамента защиты от
цифровых рисков

F6



Андрей Петров
Директор по
информационной
безопасности



Сергей Журило
Директор по
информационной
безопасности



Дмитрий Коваленко
Архитектор DNS-решений



TLDCON 2026

Ташкент, сентябрь 2026

ПРИКЛАДНОЙ КИБЕРБЕЗ