

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Разузнаване на заплахите

Непрекъснато наблюдение на dark web, сайтове за споделяне на текст, бази с изтекли данни и нелегални общности за ваши идентификационни данни, данни и марка — с проверка от анализатор и подкрепа при сваляне, когато нещо се появи.

ПОДХОДЯЩО ЗА	Марки, изложени на фишинг и измами; екипи, които искат видимост отвъд периметъра
ПОЛУЧАВАТЕ	Непрекъснато наблюдение, приоритизирани сигнали, доклади от разследвания
ОБХВАЩА	Наблюдение на dark web и изтичания

Разузнаване оттам, където нападателите действително работят

Атаките започват извън вашия периметър — идентификационни данни за продажба, домейн с правописна подмяна, фишинг комплект, който се представя за вас, ваши данни в база с изтекла информация. Наблюдаваме тези източници непрекъснато и ви казваме кое е реално, кое е спешно и какво да направите по въпроса.

Нашите собствени инструменти за събиране достигат до dark web, сайтове за споделяне на текст, бази с изтекли данни, Telegram и нелегални общности; нашите анализатори превръщат шума в разузнавателна информация, по която можете да действате — включително пакети с доказателства за премахване на злонамерената инфраструктура, предназначени за регистратори, хостинг доставчици и CERT екипи, каквито сме подготвяли срещу действаща операция за фишинг като услуга.

Какво наблюдаваме

- Изтекли и откраднати идентификационни данни
- Изтичане на данни чрез пробиви и сайтове за споделяне на текст
- Домейни с правописна подмяна и представяне за вашата марка
- Фишинг и смишинг комплекти, насочени към вас
- Разговори в dark web и нелегални общности
- Изтичания на данни и изходен код

Как протича

- Обхват и активи — Договаряме марките, домейните, ключовите думи и данните за наблюдение.
- Събиране — Непрекъснато събиране в dark web, сайтове за споделяне, изтичания и канали.
- Анализ — Анализаторите проверяват и приоритизират — сигнал, а не суров поток.
- Сигнал и действие — Навременни сигнали, доклади от разследвания и подкрепа при сваляне.

Какво получавате

- Непрекъснато наблюдение — Постоянно събиране от източниците, които имат значение за вас.
- Приоритизирани сигнали — Проверени, подредени известия — а не шум.
- Доклади от разследвания — Анализи с контекст и препоръчани действия.
- Подкрепа при сваляне — Координирани сигнали за злоупотреба и пакети с доказателства за сваляне, когато нещо е действащо.

Методологии и стандарти, на които се опираме

MITRE ATT&CK; · Diamond Model of Intrusion Analysis · Cyber Kill Chain · STIX / TAXII · Рамки за събиране на OSINT · Обработка по Traffic Light Protocol (TLP)

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/threat-intelligence.