



ПРИМЕР ОТ ПРАКТИКАТА

Анализ на смишинг комплект, който заобикаляше SMS двуфакторното удостоверяване

Публичен сектор · Разследване на заплахата и обратно инженерство на фишинг комплект

Хеширани доказателства с документирана верига на съхранение и сигнали за премахване на инфраструктурата

Анонимизиран съгласно NDA. Клиентът и идентифициращите детайли са премахнати. PXLSecurity LTD. · София, България · pxlsec.com



ПРИМЕР ОТ ПРАКТИКАТА

Анализ на смишинг комплект, който заобикаляше SMS двуфакторното удостоверяване

Сектор	Публичен сектор
Ангажимент	Разследване на заплахата и обратно инженерство на фишинг комплект
Резултат	Хеширани доказателства с документирана верига на съхранение и сигнали за премахване на инфраструктурата

9	в реално време	0
вида чувствителни полета, събрани от комплекта	препращане на PIN и еднократни кодове, заобикалящо SMS 2FA	данни, подадени към инфраструктурата на нападателя

ПРЕДИЗВИКАТЕЛСТВОТО

Смишинг кампания се представяше за национален портал за електронни услуги и плащане на глоби, за да събира платежни данни и данни за самоличност. Целта беше да се установи произходът на кампанията и да се съберат доказателства за премахване на злонамерената инфраструктура, без контакт с пострадали и без подаване на данни към нападателя.

КАК СЕ РАЗВИ

1. Събрахме данни за инфраструктурата и копие на активния фишинг комплект. Изчислихме хешове на събраните материали и документирахме веригата им на съхранение.
2. Анализирахме комплекта чрез обратно инженерство. Той беше изграден като едностранично приложение; описахме стъпките, през които преминава жертвата, и всички полета, които събира.
3. Установихме извличане на данни в реално време през WebSocket към същия произход. Хостинг сървърът служеше и като сървър на оператора.
4. Препращането на PIN и еднократни кодове показваше участие на оператор в реално време и позволяваше заобикаляне на SMS 2FA и 3-D Secure. Комплектът имаше интерактивни възможности, които надхвърляха статичните фишинг страници.
5. Свързахме инфраструктурата с операция за фишинг като услуга, използвана в няколко държави с различни примамки.

ОСНОВНИ КОНСТАТАЦИИ

High	Препращане на PIN и еднократни кодове в реално време, заобикалящо SMS 2FA и 3-D Secure
High	Комплект за фишинг като услуга, използван повторно в няколко държави
Medium	Сървър за събиране на данни, хостван от оператора зад обратен прокси

ВЪЗДЕЙСТВИЕ

Кампанията крадеше масово данни за платежни карти и самоличност на граждани, като заобикаляше двуфакторното удостоверяване в реално време.

РЕЗУЛТАТ

Предадохме доказателства с изчислени хешове и документирана верига на съхранение, както и пакети със сигнали до регистратора, хостинг доставчика, националния CERT, операторите на браузърни списъци за блокиране и сертифициращия орган. Материалите бяха подготвени и за предаване на правоохранителните органи. Анализът се ограничи до събиране на доказателства; към инфраструктурата на нападателя не бяха подавани данни.

ТЕХНИКИ

Обратно инженерство на комплекта · Разузнаване на заплахите · Анализ на препредаването на еднократни кодове · Верига на съхранение · Атрибуция

УСЛУГИ

Изследване на уязвимости и разработка на експлойти · Red Teaming

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, изпълнявани от старши инженери, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331