Witaj w PDC News! Jesteśmy tutaj po to, żeby dostarczać Ci najważniejszych informacji ze świata cyberbezpieczeństwa. Co tydzień przygotowujemy kompleksowe zestawienie informacji, będące przewodnikiem po zagrożeniach, trendach i regulacjach z obszaru cyberbezpieczeństwa. Niezależnie od tego, czy interesuje Cię ochrona danych, ataki hakerskie czy innowacyjne rozwiązania, w PDC News znajdziesz wartościowe treści, które pomogą Ci być na bieżąco. Zapraszamy do lektury!

POLSKIE ŹRÓDŁA INFORMACYJNE

10 grudnia wchodzi w życie obowiązek stosowania e-Doręczeń przez podmioty publiczne wskazane w ustawie z 18 listopada 2020 r. o doręczeniach elektronicznych. Nowa, cyfrowa forma komunikacji pomiędzy podmiotami publicznymi, obywatelami i firmami ma usprawnić przepływ informacji i gwarantować bezpieczeństwo danych.
Więcej informacji TUTAJ.

MINISTERSTWO CYFRYZACJI | E-DORĘCZENIA | PODMIOTY PUBLICZNE

NASK opublikował na swojej stronie poradnik „Cyfrowa (nie)śmiertelność", z którego można dowiedzieć się czym jest ghosting scam i jak cyberoszuści mogą wykorzystywać dane zamieszczone w sieci po śmierci internauty.
Więcej informacji TUTAJ.

NASK | GHOSTING SCAM | PORADNIK

NASK, CSIRT KNF oraz CBZC wspólnie publikować będą poradniki dotyczące podstawowych aspektów bezpieczeństwa finansowego użytkowników internetu, zwłaszcza w obszarze płatności bezgotówkowych. Pierwszy można znaleźć już pod TYM LINKIEM. Kolejne pojawiać się będą w okołotygodniowych odstępach, a finał całej akcji nieprzypadkowo przewidziany jest na 24 listopada 2023 r., czyli tzw. Black Friday.
Więcej informacji TUTAJ.

NASK | CSIRT KNF | CBZC | ZAGROŻENIA | CYFROWE TRANSAKCJE FINANSOWE | PORADNIK

AV LAB Foundation opublikowała kolejny raport zawierający wnioski z badania „Advanced In The Wild Malware Test". Główne konkluzje to:

- **Najwięcej malware pochodziło z serwerów zlokalizowanych w USA, Holandii, Szwecji.**
- **Średni czas reakcji na zagrożenie przez wszystkich producentów łącznie, to: 133 sekundy.**
- **Najszybszy średni czas reakcji na testowane zagrożenia uzyskał Sophos z czasem 10 sekund.**

Więcej informacji TUTAJ.

RAPORT | MALWARE | TEST

Analitycy Check Point Software zaobserwowali 6-krotny wzrost ataków z wykorzystaniem kodów QR (ataków typu Quishing). Wśród ofiar miała być m.in. „duża amerykańska firma energetyczna".
Więcej informacji TUTAJ.

QUISHING | KOD QR | ATAKI

W ostatnim tygodniu pojawiły się doniesienia medialne dotyczące podsłuchiwania klientów i farmaceutów przez dużą sieć aptek. Rzecznik Praw Obywatelskich zwrócił się w tej sprawie z komunikatem do prezes Naczelnej Rady Aptekarskiej. RPO pyta o podjęte działania, w tym czy zawiadomiono Urząd Ochrony Danych Osobowych i Państwową Inspekcję Pracy.
Więcej informacji TUTAJ i TUTAJ.

RPO | APTEKI | DONIESIENIA MEDIALNE

INNE ŹRÓDŁA INFORMACYJNE

Biały Dom pracuje nad sfinalizowaniem nowej polityki określającej, w jaki sposób rządy powinny reagować na ataki oprogramowania ransomware, w tym udostępniać informacje o atakujących i kontach, na których gromadzone są środki z okupu.
Więcej informacji TUTAJ.

USA | RANSOMWARE | PRAWO

W dniach 1-2 listopada w Wielkiej Brytanii odbył się AI Safety Summit. Na zakończenie szczytu przyjęta została deklaracja z Bletchley, w którym Zjednoczone Królestwo, USA, Australia, Unia Europejska i Chiny podpisały wspólną deklarację, wskazując, że sztuczna inteligencja to „katastrofalne zagrożenie" ryzyko dla ludzkości. …
Więcej informacji TUTAJ.

AI | SZCZYT CYFROWY | DEKLARACJA

Europejska Rada Ochrony Danych nakazała irlandzkiemu organowi nadzorczemu - IE DPA - podjęcie w ciągu dwóch tygodni ostatecznych środków dotyczących Meta Ireland Limited (Meta IE) i nałożenie zakazu przetwarzania danych osobowych na potrzeby reklamy behawioralnej na podstawie umowy i uzasadnionego interesu na terenie całego Europejskiego Obszaru Gospodarczego. W grudniu ubr. EROD wyjaśniła, że umowa nie stanowi odpowiedniej podstawy prawnej przetwarzania danych osobowych na potrzeby reklamy behawioralnej.
Więcej informacji TUTAJ.

META | EROD | PRZETWARZANIE DANYCH OSOBOWYCH

Jak wynika z najnowszego raportu niemieckiego Federalnego Urzędu ds. Bezpieczeństwa Informacji, Niemcy odnotowują obecnie znaczny wzrost zagrożeń w cyberprzestrzeni, a ryzyko ataków typu ransomware uważa się za wyjątkowo wysokie. W okresie od czerwca 2022 r. do czerwca 2023 r. odnotowano średnio ponad 300 tysięcy nowych wariantów złośliwego oprogramowania dziennie.
Więcej informacji TUTAJ.

RANSOMWARE | MALWARE | NIEMCY | RAPORT

PdC NASK
Kontakt: pdc@nask.pl