STRONY RZĄDOWE NA CELOWNIKU HAKERÓW. ATAKI PHISHINGOWE NA INSTYTUCJE PAŃSTWOWE

Od 2020 roku trwa zorganizowana kampania phishingowa, której celem są rządowe strony w regionach Azji, Australii i Oceanii oraz Europy, Bliskiego Wschodu i Afryki – alarmuje firma Cyjax. Hakerzy starają się wykraść poufne dane z wielu instytucji państwowych, między innymi na Białorusi, Ukrainie i w Uzbekistanie.

Jak informuje zajmująca się cyberbezpieczeństwem firma Cyjax trwająca od wiosny 2020 roku zorganizowana kampania phishingowa stała się odpowiedzialna za ataki na rządy siedmiu państw w regionie Azji, Australii i Oceanii (APAC) oraz Europy, Bliskiego Wschodu i Afryki (EMEA).

Celem kampanii jest pozyskanie danych uwierzytelniających, najprawdopodobniej w celu gromadzenia informacji wywiadowczych.

Wiele państw na celowniku

Według badaczy bezpieczeństwa w kampanii wykorzystano wiele domen phishingowych. Domeny te hostowały złośliwe strony, których celem było pozyskanie danych uwierzytelniających.

Witryny podszywały się pod liczne ministerstwa rządów krajów docelowych, takie jak departamenty finansów, energii i spraw zagranicznych.

Eksperci Cyjax zaznaczają, że uzyskanie dostępu do Ministerstwa Spraw Zagranicznych jest głównym celem wielu hakerów z państw narodowych. Na podstawie stron phishingowych można stwierdzić, że kampania koncentruje się głównie na celach na Białorusi, Ukrainie i w Uzbekistanie.

Odkryto, że niektóre strony naśladują Marynarkę Wojenną Pakistanu, serwis poczty elektronicznej Mail.ru oraz Główny Zarząd Wywiadu Ukrainy. Cyjax nazwała ataki na Ukrainę operacją TrickyMouse.

Pięć groźnych domen

Zgodnie z informacjami Cyjax obecnie co najmniej 15 stron jest aktywnie ukierunkowanych na rządy Białorusi, Gruzji, Kirgistanu, Pakistanu, Turkmenistanu, Ukrainy i Uzbekistanu.

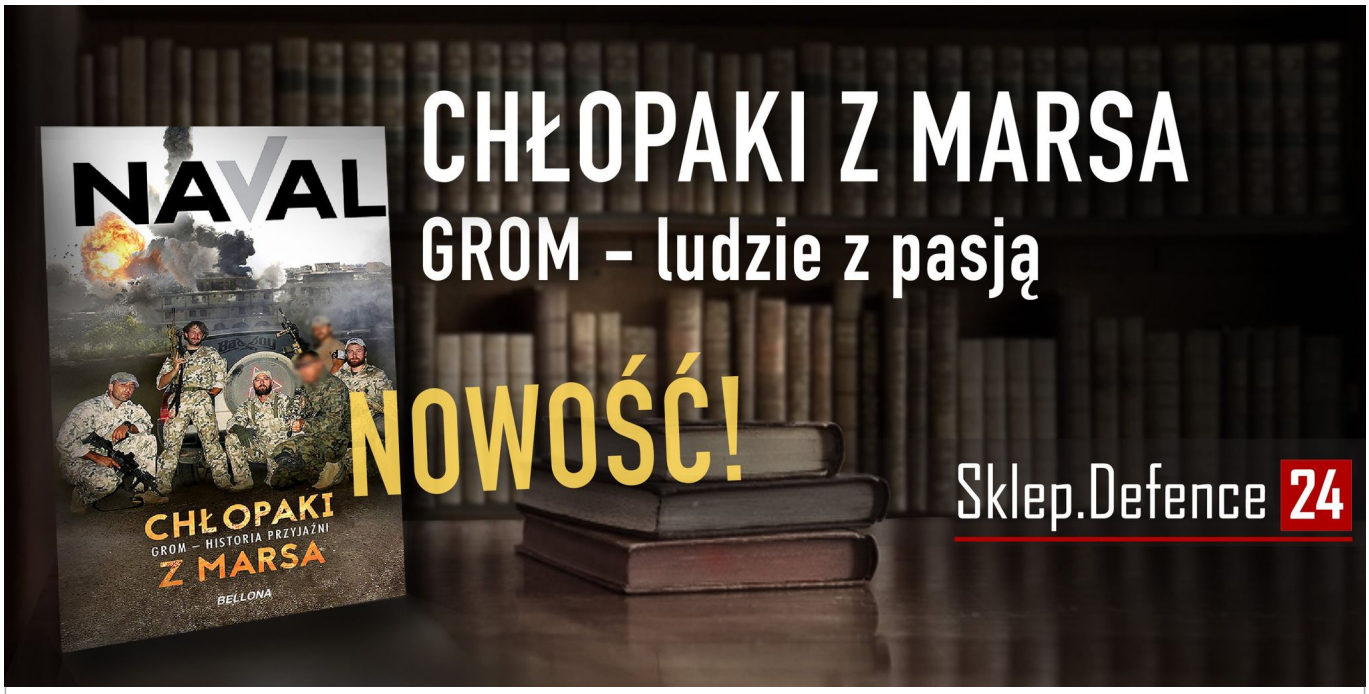
Napastnicy zarejestrowali pięć domen na potrzeby kampanii, korzystając z popularnych serwisów domenowych Tucows, PublicDomainRegistry, OVH SAS lub VDSINA.

Zidentyfikowane domeny rozpoczynały się od prefiksu „mail" i posiadały nazwę domeny oraz nazwę hosta docelowego departamentu rządowego. Jeden z adresów IP OVH był wykorzystywany do hostowania kilku domen.

Według analityków kampania skupia się na ograniczonej grupie ofiar i nie przynosi bezpośrednich

korzyści finansowych. Sugeruje to, że napastnicy stojący za tą kampanią to gangi cyberprzestępców sponsorowane przez konkretne państwo lub grupy, których celem jest kradzież poufnych informacji.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.



Fot. Reklama