

Hakerzy zaatakowali US Marshals Service

03.03.2023

Według raportu Departamentu Obrony hakerzy zaatakowali US Marshals Service (amerykańską agencję federalną odpowiadającą za egzekwowanie wyroków sądów federalnych) za pomocą oprogramowania ransomware i zdołali wykraść informacje o prowadzonych śledztwach.

Większość ataków ransomware uderza w komercyjne firmy, które w mniemaniu hakerów byłyby skłonne zapłacić okup. Przykład US Marshals Services pokazuje, że nie zawsze tak jest. Niekiedy celem cyberprzestępców stają się także amerykańskie agencje federalne, co może wzbudzać zdziwienie wśród opinii publicznej.

Hakerzy zaatakowali US Marshals Service – kulisy ataku

Cyberatak na infrastrukturę sieciową US Marshals Services miał miejsce 17 lutego br. To właśnie wtedy jeden z systemów tej agencji został naruszony w wyniku ataku ransomware. Podobnie jak w przypadku większości tego typu ataków hakerzy szukali danych przed zablokowaniem systemu i najwyraźniej udało im się zdobyć niektóre

poufne dokumenty.

„System, którego dotyczy problem, zawiera poufne informacje organów ścigania, w tym zwroty z procesu prawnego, informacje administracyjne i dane osobowe dotyczące podmiotów dochodzeń USMS, stron trzecich i niektórych pracowników USMS” – powiedział Reuterowi Drew Wade, szef biura spraw publicznych Marshals Service.

US Marshals Service natychmiast podjęło działania obronne

Zgodnie z raportem US Marshals Service agencja natychmiast poinformowała o cyberincydencie Departament Sprawiedliwości, który wszczął dochodzenie. Warto zauważyć, że hakerzy zdążyli złamać zabezpieczenia tylko jednego urządzenia, zanim agencja wykryła włamanie.

Raport CNN wskazał również, że wykradzione dane nie zawierały informacji o programie ochrony świadków, co niewątpliwie jest ulgą dla wielu osób, które są nim objęte.

Władze jeszcze nie upubliczniły żadnych informacji na temat typu użytego w ataku ransomware oraz grupy hakerskiej odpowiedzialnej za włamanie.

„Od kilku lat obserwujemy znaczący wzrost cyberataków skierowanych na instytucje rządowe. Przykład US Marshals Service tylko potwierdza ten trend. Jedynym sposobem na powstrzymanie ataków typu ransomware jest korzystanie ze skutecznego oprogramowania antywirusowego

wyposażonego w specjalny moduł antiransomware. Warto również zadbać o edukację swoich pracowników w zakresie niebezpieczeństw w sieci” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania antywirusowego Bitdefender.

Źródło: <https://bitdefender.pl/hakerzy-zaatakowali-us-marshals-service/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 03.03.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.