KAMSOFT
SPÓŁKA AKCYJNA

KAMSOFT S.A.
40-235 Katowice
ul. 1 Maja 133

KRS NR
0000345075
Sąd Rejonowy
Katowice-Wschód
Wydział VIII
Krajowego Rejestru
Sądowego

Kapitał zakładowy
52 600 000 zł
w całości opłacony

NIP
9542685559

REGON
241371988

KONTO BANKOWE
PEKAO S.A.
45 1240 4227
1111 0010
2861 3872

Telefon:
32 209 07 05

Fax:
32 209 07 15

Internet:
www.kamsoft.pl

E-poczta:
biuro@kamsoft.pl

Wydziały zamiejscowe:

KAMSOFT Północ
87-100 Toruń
ul. Żwirki i Wigury
81C/48A
Tel.: 56 655 24 19

KAMSOFT Zachód
64-100 Leszno
Strzyżewice
ul. Lotnicza 1
Tel.: 65 512 89 00

KAMSOFT Południe
25-317 Kielce
ul. Niska 5/2
Tel.: 41 362 92 02

Katowice 2024-05-08

Szanowni Państwo,

W ślad za wcześniej przesłanymi informacjami za pomocą bezpośrednich kanałów komunikacyjnych, dodatkowo poinformujemy Państwa o próbie ataku phishingowego z nieuprawnionym wykorzystaniem nazwy KAMSOFT i celowo zmodyfikowanej domeny internetowej. Atak najprawdopodobniej przeprowadzony jest w celu kradzieży danych i stanowi istotne zagrożenie dla bezpieczeństwa Państwa danych, w tym danych o Państwa pacjentach!

Atakujący stworzyli fałszywą stronę internetową, udającą oficjalną stronę KAMSOFT S.A., oraz przesłali link do strony za pośrednictwem SMS. Fałszywa strona zachęca do pobrania złośliwego oprogramowania (VIDAR), pod pozorem rzekomej aktualizacji oprogramowania. Ta strona została skonstruowana w taki sposób, aby wyglądała autentycznie i wiarygodnie, co może wprowadzić wiele osób w błąd.

Pobranie i uruchomienie wskazanego tam pliku, będzie skutkować uruchomieniem złośliwego oprogramowania a w konsekwencji kradzieżą danych – np. loginów i haseł zapisanych w przeglądarce, które następnie mogą zostać użyte do dalszej kradzieży danych, w tym danych Państwa pacjentów.

Chcielibyśmy podkreślić, że żadna z oficjalnych aktualizacji KAMSOFT nigdy nie była i nie jest dystrybuowana za pośrednictwem SMS, ani żądająca pobrania pliku z internetu. W celu aktualizacji oprogramowania zawsze zalecamy korzystanie wyłącznie z autoryzowanych serwisantów Krajowej Sieci Serwisu KAMSOFT. W przypadku wątpliwości zawsze należy sprawdzić autentyczność wiadomości kontaktując się z serwisem lub bezpośrednim opiekunem serwisowym.

Jeżeli otrzymali Państwo taką informację, prosimy o nie otwieranie jej, nie klikanie w linka, nie pobieranie i nie otwieranie jej zawartości!

Jeżeli ktoś z państwa padł ofiarą ataku (otworzył zawartość umieszczoną na fałszywej stronie) zalecamy natychmiastowe wyłączenie komputera i kontakt z Państwa działem IT lub Państwa opiekunem serwisowym, celem przeprowadzenia weryfikacji i zminimalizowania skutków potencjalnego ataku. Zalecana jest również zmiana wszystkich haseł, z których Państwo korzystają.

Aby chronić się przed tego rodzaju atakami, również w przyszłości, zalecamy podjęcie następujących kroków:

Proszę nie klikać w podejrzane linki ani nie pobierać załączników z wiadomości e-mail, które wydają się podejrzane.

Proszę sprawdzać zawsze autentyczność strony internetowej, zanim wykonacie państwo jakiekolwiek działania, zwłaszcza gdy jest to związane z pobieraniem plików lub udostępnianiem danych osobowych. Czasem adres strony może do złudzenia przypominać stronę oryginalną i różnić się jednym lub kilkoma znakami.

Proszę regularnie aktualizować oprogramowanie antywirusowe i firewall oraz korzystać z najnowszych wersji systemów operacyjnych i aplikacji.

Informujemy również, że KAMSOFT S.A. nie ma wpływu na podejmowane tego rodzaju ataki, niemniej jednak dokładamy wszelkich starań i podejmujemy działania, aby je w jak największym stopniu ograniczyć jak również ograniczyć skutki ich działania.

Zweryfikowaliśmy, że strona jest już umieszczona na Liście ostrzeżeń przed niebezpiecznymi stronami, prowadzoną przez CERT i w przypadku otworzenia jej na urządzeniu mobilnym otrzymają państwo ostrzeżenie o zagrożeniu. Otwarcie strony na zwykłym komputerze wymaga podjęcia pewnych działań aby ostrzeżenie było skuteczne. Więcej o liście ostrzeżeń przed niebezpiecznymi stronami można znaleźć tutaj: Lista Ostrzeżeń przed niebezpiecznymi stronami | CERT Polska

Podjęliśmy również kroki, aby wszystkimi możliwymi kanałami poinformować klientów KAMSOFT S.A. o sytuacji zagrażającej bezpieczeństwu ich danych.

Prosimy o wzmożoną czujność i nie otwieranie linków z wiadomości z podejrzaną treścią.

Jeżeli otrzymali Państwo taki fałszywy SMS, prosimy o przesłanie zgłoszenia do CERT Polska (CSIRT NASK), który jest jednym z trzech Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego na poziomie krajowym.

W jaki sposób można przekazać zgłoszenie?

na stronie: https://incydent.cert.pl

e-mailem: cert@cert.pl

SMS-em: 799 448 084 (należy przekazać całą wiadomość w oryginalnej formie – nie należy wycinać linku czy fragmentów treści) https://www.nask.pl/pl/aktualnosci/4183,Teraz-jeszcze-latwiej-zglosic-incydent-bezpieczenstwa-przez-SMS.html

Z poważaniem,

Zespół KAMSOFT S.A.