K O M U N I K A T

Incydent cyberbezpieczeństwa oraz prawdopodobny wyciek danych po ataku hakerskim typu RANSOMWARE na infrastrukturę informatyczną firmy e-Impet Jarząbek Group Sp. z o.o. oraz Fundacji "Życie Cudem Jest".

OPIS INCYDENTU CYBERBEZPIECZEŃSTWA

W dniu 27 stycznia 2025 r. (po godz. 8:15), Krzysztof Jarząbek, jako prezes oraz Administrator Danych Osobowych gromadzonych w szczególności w systemach, programach oraz na nośnikach zapisu danych, w ramach infrastruktur informatycznych firmy e-Impet Jarząbek Group Sp. z o.o. oraz Fundacji "Życie Cudem Jest", powziął informację o możliwym naruszeniu ochrony danych osobowych. Potencjalne naruszenie trwało mogło trwać od 26 do 27 stycznia 2025 roku.

W związku z powyższym podjęto natychmiastowe działania zapobiegające dalszym nadużyciom, które polegały na zablokowaniu - odcięciu zainfekowanych komputerów w postaci stacji roboczych (system WINDOWS 10 PRO) oraz serwera głównego (system WINDOWS 2016) od sieci wewnętrznej oraz pozbawiono całkowicie dostępu do internetu zewnętrznego. Odizolowano także routery (w tym główny CISCO) oraz inne urządzenia sieciowe mające potencjalny wpływ na przedmiotowy atak hakerski, w wyniku czego mogło dojść do nieuprawniony dostępu do system wraz z danymi.

Incydent został stwierdzony 27 stycznia 2025 roku i polegał na ataku szyfrującego pliki (Ransomware)[1]. Zgodnie z posiadanymi informacjami na temat "technik typowych dla tego typu ataku" istnieje duże prawdopodobieństwo, że dane przetwarzane w systemach objętych incydentem są lub mogą być, w posiadaniu osób trzecich.

O ZDARZENIU POINFORMOWANO

1. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK (https://cert.pl)
2. Centralne Biuro Zwalczania Cyberprzestępczości (https://cbzc.policja.gov.pl)
3. Prezesa Urzędu Ochrony Danych Osobowych *(pisemny wniosek jest w trakcie procedowania i zostanie przesłany do UODO, do dnia 29.01.2025 roku)* (https://uodo.gov.pl)
4. Urzędy Skarbowe *(zawiadomienia złożone w dniu. 27.01.2025 rok),*
5. ZUS'y *(prace w toku ze względu na konieczność zawiadomienia w formie papierowej*),
6. i/lub inne instytucja państwowe *(prace w toku)*,

[1] Ransomware, to rodzaj złośliwego oprogramowania, które infekuje komputer lub system, szyfruje dane ofiary i żąda okupu za ich odblokowanie. Głównym celem takiego ataku jest zmuszenie ofiary do zapłaty okupu, często w postaci kryptowaluty (np. Bitcoin), w zamian za klucz umożliwiający odszyfrowanie danych.

7. złożono zawiadomienie o popełnieniu przestępstwa przyjęte osobiście w dniu 28.01.2025 przez funkcjonariuszy CBZC o/Poznań.

AKTUALNE PRACE W ZWIĄZKU ZE ZDARZENIEM

Aktualnie trwają działania mające na celu ustalenie pozostałych okoliczności zdarzenia oraz trwa analiza „wektoru wejścia-wyjścia" incydentu, która jest prowadzona przez CSIRT NAS *(sprawa posiada nr zgłoszenia)*.

Prace analityczno-operacyjne prowadzone są także przez Centralne Biuro Zwalczania Cyberprzestępczości w Poznaniu *(w oczekiwaniu na sygnaturę sprawy)*, gdzie dodatkowo w toku czynności operacyjnych będą przejęte zeznania na okoliczność i pozyskane niezbędne informacje od "informatyka" (SB) odpowiedzialnego za stworzenie i zabezpieczenie infrastruktury informatycznej, który ze względów osobistych nie mógł być przy zgłoszeniu i pracami zabezpieczającymi podjętymi przez CBZC, jak i innych osób mogących mieć wpływ na przedmiotowy incydent.

Nadmieniamy, że zaatakowane komputery/serwery nie podsiadały zainstalowanego i działającego jakiegokolwiek programu pocztowego (klienta poczty e-mail), a w zaleceniach obu podmiotów, których potencjalni użytkownicy zainfekowanych komputerów nie maja prawa otwierania prywatnej poczty, a szczególnie otwierania jakichkolwiek załączników ze skrzynek pocztowych (e-mail) oraz mediów społecznościowych typu facebook, twitter, istagram, itp. Kategorycznie zakazane i od wielu lat przestrzegane, jest używanie prywatnych pendrive, laptopów, dysków przenośnych, płyt CD/DVD.

Firma e-Impet Jarząbek Group Sp. z o.o. oraz Fundacja "Życie Cudem Jest", realizuje ponadto czynności mające na celu niezwłoczne przywrócenie funkcjonowania systemów IT, systemów księgowych, jak i odtworzenie niezbędnych danych w celu realizacji podjętych zobowiązań wobec osób trzecich (prawnych, jak i fizycznych) oraz zapewnia, że podejmie wszelkie niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości, włącznie z skierowaniem spraw na drogę karno-sądową w stosunku do osób związanych z konfiguracją i zabezpieczeniem sieci IT.

W ramach aktualnie przeprowadzonych prac można przypuszczać, że na podstawie zaszyfrowanych i pozostawionych danych na dyskach komputerów i serwera głównego, że potencjalnie wykradzione dane mogą obejmować:

- dane osobowe [2] *(dokumenty kadrowo-płacowe i ewidencyjne, PESEL i/lub NIP)*
- dane księgowe [3] *(faktury, dowody księgowe, itp.)*
- zawarte umowy *(własne i obce)*
- informacje o realizowanych przedsięwzięciach własnych i/lub obcych *(o ile takowe były przechowywane)*

[2] Dostęp do programów kadrowo-płacowych, księgowych był zabezpieczony hasłami 10 znakowymi - alfanumerycznymi, gdzie musiała występować co najmniej: jedna mała litera, jedna wielka litera oraz cyfra, hals było okresowo zmieniane.

[3] Dostęp do programów kadrowo-płacowych, księgowych był zabezpieczony hasłami 10 znakowymi - alfanumerycznymi, gdzie musiała występować co najmniej: jedna mała litera, jedna wielka litera oraz cyfra, hals było okresowo zmieniane.

- dane dostępowe i/lub inne wrażliwe informacje *(takie jak m.in.: imię i nazwisko; adres firmy, którą Państwo reprezentujecie, kwoty transakcji pomiędzy kontrahentami, numer telefonu; adres e-mail)*

DODATKOWE INFORMACJE I OBJAŚNIENIA

Rozumiemy, że ta sytuacja może budzić Państwa zaniepokojenie, dlatego przygotowaliśmy odpowiedzi na pytania. W ten sposób przekażemy Państwu dodatkową wiedzę i narzędzia potrzebne do zwiększenia Państwa poziomu bezpieczeństwa.

Bardzo prosimy przekazać przedmiotowy komunikat osobom zainteresowanym lub których zdarzenie może dotyczyć, w szczególności zarządom spółek, udziałowcom *(aktualnym lub byłym),* pracownikom bez względu na formę zatrudnienia/umowy *(aktualnym lub byłym).*

1. Jakie skutki naruszenie może nieść dla Państwa?

Stale monitorujemy sytuację i aktualnie trwają prace na określeniem celu i zakresu ataku. Na chwilę obecną nie stwierdziliśmy, na podstawie losowo wybranej próbki danych, aby wykorzystano Państwa dane w niepożądany sposób.
Jednak ze względu możliwy na zakres ujawnionych danych uważamy, że powinni Państwo wziąć pod uwagę powstałe na skutek przedmiotowego incydentu ryzyko, bo ktoś może próbować *(podajemy przykładowe możliwości, choć nie wszystkie dotyczą przedmiotowego incydentu)*:

- uzyskać kredyt w instytucjach pozabankowych z wykorzystaniem Państwa danych, ponieważ niektóre instytucje mogą zapewniać łatwy i szybki proces kredytowy, a czasami nawet nie wymagają, aby klient okazał dokument tożsamości;
- uzyskać dostęp do świadczeń opieki zdrowotnej, które Państwu przysługują, lub do danych o stanie Państwa zdrowia. Może się tak stać, ponieważ często do telefonicznej rejestracji lub weryfikacji pacjenta wystarczy podanie numeru PESEL;
- używając Państwa danych, zawrzeć umowę o świadczenie usług, na przykład telewizji kablowej, telefonu czy Internetu, a potem przestać opłacać rachunki;
- wykorzystując Państwa dane, utworzyć konto w serwisie internetowym, np. społecznościowym;
- wysyłać Państwu niechcianą pocztę (spam);
- wykonywać do Państwa niechciane telefony, na przykład o charakterze marketingowym;
- przekazać osobom postronnym informacje, które Państwa dotyczą, w wyniku czego mogą odczuwać Państwo dyskomfort;
- próbować wyłudzić od Państwa dodatkowe informacje, potrzebne na przykład do zaciągnięcia kredytu w Państwa imieniu;
- opublikować Państwa dane w Internecie;

W związku z zaistniałą sytuacją, zależy nam, aby możliwie jak najpełniej znali Państwo potencjalne ryzyka.
Oczywiście ryzyka te nie muszą wystąpić w przypadku tego incydent, ale mogą.
Mimo to chcemy, aby byli Państwo ich świadomi i wiedzieli, jak się przed nimi bronić.

2. Co państwo mogą zrobić w tej sprawie?

Profilaktycznie prosimy o rozważenie i podjęcie któregoś (lub nawet kilku) z poniższych działań. Mogą one znacząco zredukować ryzyko nieuprawnionego wykorzystania Państwa danych osobowych o ile takie nastąpią.

Z uwagi na zakres danych, które mogły zostać ujawnione, dodatkowo zachęcamy Państwa do:

- zweryfikowania, czy przestępcy opublikowali Państwa dane. Można to zrobić na rządowej stronie: https://bezpiecznedane.gov.pl/
- zgłaszania podejrzanych wiadomości SMS na numer 8080. Jest on obsługiwany przez zespół CERT Polska, którego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo w Internecie *(wskazówka: Eksperci z CERT radzą, by podejrzane SMS-y przesyłać im poleceniem "Przekaż" lub "Prześlij dalej", a jeśli nie ma takiej możliwości, wystarczy skopiować treść wiadomości i wysłać ją na wspomniany numer. Dotyczy to wiadomości z linkami, ale też tych, które ich nie zawierają.)*
- zgłaszania prób oszustw (takich jak: złośliwe domeny, podejrzane wiadomości e-mail, fałszywe sklepy internetowe, złośliwe oprogramowanie, nielegalne treści) na stronie: https://incydent.cert.pl/#!/lang=pl,entityType=notObligatedEntity. Jest ona obsługiwana przez zespół CERT Polska, którego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo w Internecie;
- założenia konta w systemie informacji kredytowej i gospodarczej. Dzięki temu będą mogli Państwo monitorować przypisaną Państwu aktywność kredytową *(wskazówka: w niektórych systemach informacji kredytowej mogą Państwo włączyć alerty SMS i e-mail. Otrzymają je Państwo, gdy pojawią się zapytania od podmiotów finansowych o Państwa historię kredytową)*
- zgłoszenia właściwym instytucjom publicznym nieuprawnionego wykorzystania Państwa danych osobowych. Można to zrobić na stronie: https://www.gov.pl/web/gov/zglos-nieuprawnione-wykorzystanie-swoich-danych-osobowych-kradziez-tozsamosci--uniewaznij-dowod
- w przypadku upublicznienia Państwa danych – zwrócenia się do administratora strony, na której pojawiły się Państwa dane, z żądaniem ich usunięcia. Instrukcja, jak to zrobić, znajduje się na stronie firmy konsultingowej: https://odo24.pl/blog-post.jak-reagowac-na-kradziez-tozsamosci;
- w przypadku kradzieży tożsamości bądź próby szantażu przez cyberprzestępców – zgłoszenia tych przestępstw na policję. W takim przypadku warto rozważyć kontakt z najbliższym Wydziałem Terenowym Centralnego Biura Zwalczania Cyberprzestępczości: https://cbzc.policja.gov.pl
- sprawdzenia, czy dane które wyciekły, nie były przez Państwa wykorzystywane jako dane do logowania, w celu ich zmiany we wszystkich serwisach, w których były wykorzystywane;
- zachowania ostrożności, gdy podają Państwo swoje dane osobowe innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- zachowania szczególnej ostrożności w razie otrzymania wiadomości od nieznanych odbiorców;
- weryfikowania numerów rachunków bankowych w wiadomościach i powstrzymania się z zapłatą, jeśli numer rachunku różni się od tego, na który dotychczas wpłacali Państwo należności;
- niewykonywania płatności, których zażądano SMS-owo, telefonicznie, e-mailowo lub w inny sposób, którego;

- skontaktowania się z nami, jeśli będą mieć Państwo wątpliwości, czy to na pewno my wysłaliśmy do Państwa ewentualne wezwanie do zapłaty lub gdy będą chcieli Państwo ponownie wprowadzić utracone dane.

Jeśli zauważą Państwo jakiekolwiek oznaki nieuprawnionego wykorzystania Państwa danych, prosimy o jak najszybsze przekazanie nam tych informacji.

DLA BEZPIECZEŃSTWA SUGERUJEMY

Sugerowane zalecenia są również przydatne w przypadku podobnych incydentów w innych podmiotach lub dla osób, z którymi współpracujemy, a nie doświadczyły takiego problemu, jaki jest atak hakerski RANSOMWARE.

1. zmianę haseł dostępowych do swoich zasobów, w szczególności kont internetowych, kont bankowych, kont pocztowych, social-mediów, itp., aczkolwiek wysyłana do Państwa korespondencja e-mail, pochodziła z niezainfekowanego komputera, który jako jedyny w naszej infrastrukturze informatycznej podsiada klienta poczty e-mail. Komputer też dodatkowo posiada i „opiera się" na wielostopniowym uwierzytelnianiu oraz weryfikacji przy użyciu biometrii i/lub kluczy sprzętowych YUBIKEY. Poza tym nie posiadaliśmy i nie posiadamy wyżej wymienionych danych;
2. niepowiązywanie haseł np. do bankowości elektronicznej z własnymi danymi osobowymi (typu data urodzenia czy adres);
3. stosować dwuskładnikowe uwierzytelnianie, szczególnie dla kont serwisowych;
4. regularnie aktualizować oprogramowanie, zwłaszcza w systemach związanych z dostępem do Internetu;
5. zastrzeżenia numeru PESEL[4], który możemy dokonać na trzy sposoby:
   - w aplikacji mObywatel,
   - na stronie gov.pl, https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie
     w urzędzie.
6. bieżące i/lub okresowe monitorowanie wykorzystania swoich danych osobowych w systemach takich jak: Biuro Informacji Kredytowej, Biuro Informacji Gospodarczej, Krajowy Rejestr Długów, serwis Chroń PESEL;
7. działania te są zalecane, ale całkowicie dobrowolne.

3. Z kim się kontaktować w razie dodatkowych pytań?

Jesteśmy do Państwa pełnej dyspozycji.
Zapewniamy, że każde z pytań i obaw zostanie potraktowane należytą powagą i uwagą. Jesteśmy gotowi udzielić pomocy i wsparcia w zakresie posiadanej wiedzy i kompetencji i/lub skierować do określonych osób, funkcjonariuszy lub instytucji państwowych, i/lub podmiotów o podobnych charakterze.
Poniżej przedstawiamy pełne dane teleadresowe.

[4] wykorzystanie możliwości wprowadzonych ustawą z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz. U. z 2023 r. poz. 1394)[3] – to jest zastrzeżenie swojego numeru PESEL; więcej informacji na stronie https://antyweb.pl/zastrzezenie-numeru-pesel-czy-to-dziala

PEŁNE DANE TELEADRESOWE

OSOBA KONTAKTOWA

Krzysztof Jarząbek tel. 507.120.540 (e-mail: biuro@fzcj.pl lub biuro@e-impet.pl

POZOSTALE DANE KONTAKTOWE

e-IMPET Jarząbek Group Sp. z o.o.

biuro@e-impet.pl | www.e-impet.pl

Adres Siedziby

e-IMPET Jarząbek Group Sp. z o.o.

ul. Litewska 35, 64-100 Lesznie

KRS 0000314651

REGON 300700490

NIP 6972225356

Adres do korespondencji

e-IMPET Jarząbek Group Sp. z o.o.

ul. Grochowiaka 6; 64-100 Leszno

NIP: 6972225356

Fundacja Życie Cudem Jest

www.FZCJ.pl | biuro@FZCJ.pl

Adres Siedziby

Fundacja "Zycie Cudem Jest"

Piaski 2, 63-910 Miejska Góka,

KRS 0000362313

REGON 301515719

NIP 6991947381

Adres do korespondencji

Fundacja "Życie Cudem Jest"

ul. St. Grochowiaka 6; 64-100 Leszno

NIP: 6991947381

Z wyrazami szacunku

w imieniu Zarządu

e-IMPET Jarząbek Group Sp. z o.o. *Fundacja Życie Cudem Jest*

Krzysztof Jarząbek

Tel. 507.120.540