Specyfikacja API v1.2

Lista ostrzeżeń o stronach internetowych wyłudzających dane oraz doprowadzających użytkowników Internetu do niekorzystnego rozporządzenia ich środkami finansowymi

CERT Polska/NASK PIB

NASK
CERT.PL

Spis treści

Historia zmian dokumentu

Wersja	Data zmiany	Opis zmian
1.0	2020-03-23	Pierwsza wersja dokumentu
1.1	2020-03-24	Doprecyzowanie dok. interfejsów
1.2	2020-03-26	Sekcja o „landing page”

1 Wprowadzenie

Począwszy od dnia 23 marca 2020 r. CERT Polska - NASK PIB udostępnia *Listę ostrzeżeń o stronach internetowych wyłudzających dane, w tym dane osobowe oraz doprowadzających użytkowników Internetu do niekorzystnego rozporządzenia ich środkami finansowymi* dalej zwaną **Listą Ostrzeżeń**.

Pojawiające się w treści tego dokumentu hasło „złośliwa domena" odwołuje się do domen które zostały wpisane na Listę Ostrzeżeń.

Treść Listy Ostrzeżeń jest publicznie dostępna, a zawarte w niej informacje mogą być bez ograniczeń przetwarzane przez wszystkie podmioty zarówno w sposób manualny, jak i zautomatyzowany.

1.1 Cel dokumentu

Celem dokumentu jest opisanie technicznych aspektów funkcjonowania Listy Ostrzeżeń, których zrozumienie jest niezbędne do poprawnego przeprowadzenia integracji między Listą Ostrzeżeń, a systemem odbiorcy, który chce uzyskać dostęp do informacji o wykrytych przez CERT Polska - NASK PIB domenach wyłudzających dane oraz doprowadzających użytkowników Internetu do niekorzystnego rozporządzenia ich środkami finansowymi.

1.2 Odbiorcy

Dokument został przygotowany dla osób technicznych - programistów, administratorów IT oraz innych osób zajmujących się opracowywaniem oraz integrowaniem oprogramowania służącego do pozyskiwania informacji z Listą Ostrzeżeń prowadzoną przez CERT Polska - NASK PIB.

2 Interfejs programistyczny

2.1 Metody komunikacji

Obecnie, uzyskanie informacji o złośliwych domenach możliwe jest za pośrednictwem jednej metody komunikacji:

- **Pobranie listy złośliwych domen na żądanie** – odbiorca wywołuje usługę udostępnianą przez CERT Polska - NASK PIB i opisaną w niniejszym dokumencie. Odbiorca otrzymuje w ten sposób pełen spis złośliwych domen.

3 Specyfikacja interfejsu do pobierania listy złośliwych domen na żądanie

Opisywany interfejs umożliwia pobranie informacji znajdujących się na Liście Ostrzeżeń przez odwołanie się do publicznie dostępnego REST API, dostępnego za pośrednictwem protokołu HTTPS.

3.1 Obsługiwane formaty danych

Zawartość Listy Ostrzeżeń może zostać pobrana w formacie TXT, XML lub JSON, w zależności od indywidualnych preferencji odbiorcy danych.

3.2 Opis interfejsu TXT

- Adres usługi: `https://hole.cert.pl/domains/domains.txt`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o MIME-type `text/plain`;

Zwracany z usługi plik TXT zawiera listę wszystkich blokowanych domen wpisanych na Listę Ostrzeżeń. Poszczególne złośliwe domeny znajdują się w kolejnych liniach pliku, po jednej domenie na linię. Separatorem linii jest znak `\n`. Wszystkie domeny znajdujace się w odpowiedzi powinny zostać zablokowane przez odbiorcę. Jeżeli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Dokument zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie są w nim zawarte.

3.3 Opis interfejsu XML

- Adres usługi: `https://hole.cert.pl/domains/domains.xml`
- Oczekiwane żądanie: połączenie za pomocą protokołu HTTPS, zapytanie GET pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana wartość: kod odpowiedzi `200 OK`; dokument o MIME-type `application/xml` zgodny ze specyfikacją wspomnianą w punkcie „Schemat dokumentu XML”;

Zwracany z usługi plik XML zawiera informacje o wszystkich blokowanych domenach na Liście Ostrzeżeń oraz dacie ich wpisania na listę. Wszystkie domeny znajdujące się w odpowiedzi powinny zostać zablokowane przez odbiorcę. Jeśli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Dokument zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie będą w nim zawarte.

3.3.1 Schemat dokumentu XML

Aktualny dokument XSD[1] zawierający opis formalny formatu zwracanych danych jest możliwy do pobrania pod adresem:

`https://hole.cert.pl/schema/schema-domains.xsd`

Format danych został opracowany w sposób maksymalnie zbliżony do tego, który jest już wykorzystywany przez *Rejestr Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą* prowadzony przez Ministerstwo Finansów, co ma na celu zapewnienie kompatybilności z istniejącą infrastrukturą służącą do blokowania domen.

3.3.2 Przykładowe żądanie i odpowiedź XML

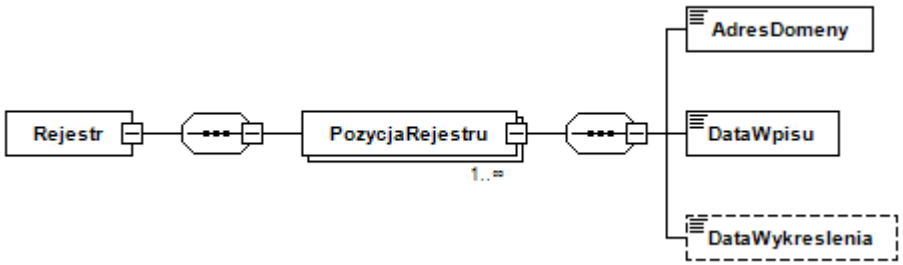
```
GET https://hole.cert.pl/domains/domains.xml HTTP/1.1
```

Listing 1: Żądanie pobrania listy złośliwych domen w formacie XML

```
<Rejestr>
  <PozycjaRejestru Lp="1">
    <AdresDomeny>domena1.example.invalid</AdresDomeny>
    <DataWpisu>2020-03-10T10:00:01</DataWpisu>
  </PozycjaRejestru>
  <PozycjaRejestru Lp="2">
    <AdresDomeny>domena2.example.invalid</AdresDomeny>
    <DataWpisu>2020-03-13T10:20:01</DataWpisu>
   </PozycjaRejestru>
  <PozycjaRejestru Lp="5">
    <AdresDomeny>domena10.example.invalid</AdresDomeny>
    <DataWpisu>2020-03-14T20:01:01</DataWpisu>
   </PozycjaRejestru>
</Rejestr>
```

Listing 2: XML zwracany w odpowiedzi na przesłane żądanie

[1] Dokumentacja formatu XSD - https://www.w3.org/XML/Schema



Rysunek 1: Graficzna reprezentacja schematu XML

3.4 Opis interfejsu JSON

- Adres usługi: `https://hole.cert.pl/domains/domains.json`
- Oczekiwane żądanie: połączenie za pomocą protokołu HTTPS, zapytanie GET pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana wartość: kod odpowiedzi `200 OK`; dokument o MIME-type `application/json`;

UWAGA! Zwracany z usługi plik JSON zawiera informacje o wszystkich domenach zawartych na Liście Ostrzeżeń, **również tych które zostały z niej wykreślone**!

Odbiorca powinien zablokować tylko te domeny, które znajdują się w zwróconym pliku oraz posiadają pole `DeleteDate` ustawione na wartość `null`. Wpisy w których uzupełnione jest pole `DeleteDate` oznaczają domeny wykreślone z Listy Ostrzeżeń, tj. takie, które nie powinny być już dłużej blokowane. Jeżeli implementacja tej logiki po stronie odbiorcy z jakiegoś powodu jest skomplikowana, zalecamy wykorzystanie prostszych interfejsów XML lub TXT.

3.4.1 Schemat dokumentu JSON

Aktualny opis formalny przesyłanych danych w formacie JSON schema[2] jest możliwy do pobrania pod adresem:

`https://hole.cert.pl/schema/schema-domains.json`

Dane zwracane przez Listę Ostrzeżeń są zgodne ze wspomnianym opisem.

[2]Specyfikacja JSON Schema - https://json-schema.org/

3.4.2 Przykładowe żądanie i odpowiedź JSON

```
GET https://hole.cert.pl/domains/domains.json HTTP/1.1
```

Listing 3: Żądanie pobrania listy złośliwych domen w formacie JSON

```
[
  {
    "RegisterPositionId": 1,
    "DomainAddress": "domena1.example.invalid",
    "InsertDate": "2017-04-26T09:44:27"
    "DeleteDate": null
  },
  {
    "RegisterPositionId": 2,
    "DomainAddress": "domena2.example.invalid",
    "InsertDate": "2017-04-30T12:30:27"
    "DeleteDate": "2017-05-01T15:50:01"
  }
]
```

Listing 4: JSON zwracany w odpowiedzi na przesłane żądanie

4 Landing page dla zablokowanych domen

Podczas blokowania domen rekomendujemy przekierowanie ich wpisem `A` w DNS na adres naszego landing page, który zawiera informacje o możliwych powodach zablokowania strony internetowej oraz garść wskazówek w zakresie bezpieczeństwa dla użytkowników końcowych.

Adresy IP z których serwowany jest landing page dostępne są w pliku:

`http://hole.cert.pl/schema/hole.txt`

Adresy mogą ulec zmianie w przyszłości. Treść powyższego pliku zostanie wtedy zaktualizowana. Wygląd serwowanego przez nas landing page można sprawdzić pod adresem: `http://hole.cert.pl/`

Rekomendujemy kierowanie użytkowników zablokowanych domen do landing page. Pozwoli to zwiększyć świadomość użytkowników i jednocześnie umożliwi CERT Polska lepsze szacowanie skali incydentów tego typu.

5 Kontakt techniczny w zakresie integracji

W przypadku pytań lub problemów technicznych dotyczących integracji z Listą Ostrzeżeń prowadzoną przez CERT Polska - NASK PIB prosimy o kontakt pod adresem e-mail **info@cert.pl** dołączając słowa `[lista ostrzeżeń]` do tematu wiadomości.

Ten kanał komunikacji w kontekście Listy Ostrzeżeń może być wykorzystywany do następujących celów:

- Zadawanie pytań technicznych związanych z niniejszym dokumentem oraz funkcjonowaniem Listy Ostrzeżeń;
- Zgłaszanie propozycji usprawnień w zakresie sposobu funkcjonowania Listy Ostrzeżeń od strony technicznej oraz integracyjnej;
- Zgłaszanie awarii i problemów z użytkowaniem Listy Ostrzeżeń zgodnie z niniejszym dokumentem;
- Zgłaszanie uwag do niniejszego dokumentu;