Specyfikacja API v2.0 - szkic

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

CERT Polska/NASK PIB

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”
2.0	2023-08-03	Specyfikacja API v2.0

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**.

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. Podkreślamy jednak, że poza obsługą blokowania domen bardzo ważne jest również usuwanie blokad stron, które już nie widnieją na Liście Ostrzeżeń. Poprawna obsługa obu akcji pozwoli nam na szybsze reagowanie na reklamacje dotyczące zablokowanych stron, a tym samym lepsze administrowanie Listą Ostrzeżeń.

Wraz z wejściem w życie ustawy z dnia 28 lipca o zwalczaniu nadużyć w komunikacji elektronicznej Lista Ostrzeżeń zyskała rangę ustawową. Jednym z wprowadzanych zapisów jest to, ze zgodnie z art. 21 ust. 1, podmiot posiadający tytuł prawny do domeny internetowej wpisanej na Listę Ostrzeżeń może wnieść do Prezesa UKE sprzeciw i domagać się wypisania domeny z listy.

W oryginalnym porozumieniu brało udział czterech przedsiębiorców telekomunikacyjnych. Od tego czasu wiele innych organizacji i firm różnej wielkości zaczęło korzystać z Listy Ostrzeżeń, aby chronić swoich pracowników i klientów. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej jeszcze bardziej ułatwia integrację z listą – art. 20 ust. 8 pozwala przedsiębiorcom telekomunikacyjnym biorącym udział w porozumieniu na uniemożliwianie użytkownikom na dostęp do stron wpisanych na Listę Ostrzeżeń.

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 Listy Ostrzeżeń prowadzonej przez CERT Polska - NASK PIB.

2 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.

2.1 Termin ważności blokowanych domen

Wszystkie udostępniane listy domen zawierają **wyłącznie** wpisy, które zostały zablokowane w ciągu 6 ostatnich miesięcy. W przeciwieństwie do wersji pierwszej, domeny zablokowane poza tym przedziałem czasu nie będą uwzględnione. W przypadku powtórnego pojawienia się na stronie zagrożenia, domena zostanie ponownie wpisana na Listę Ostrzeżeń.

2.2 Obsługiwane formaty danych

Zawartość Listy Ostrzeżeń może zostać pobrana w różnych formatach, w zależności od indywidualnych wymagań odbiorcy danych.

W aktualnej wersji dostępne są następujące formaty listy:

- TXT
- XML
- JSON
- CSV
- AdBlock
- Hosts
- MikroTik
- RPZ

2.3 Opis formatu TXT

- Adres usługi: `https://hole.cert.pl/domains/v2/domains.txt`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o typie MIME `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` (bajt ASCII: 0x0A). Wszystkie domeny znajdujące się w odpowiedzi oraz ich subdomeny 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.

2.4 Opis formatu XML

- Adres usługi: `https://hole.cert.pl/domains/v2/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 typie MIME `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.

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

Odbiorca powinien zablokować tylko te domeny oraz ich subdomeny, które znajdują się w zwróconym pliku oraz nie posiadają pola `DataWykreslenia`. Wpisy w których uzupełnione jest pole `DataWykreslenia` 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.

2.4.1 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.

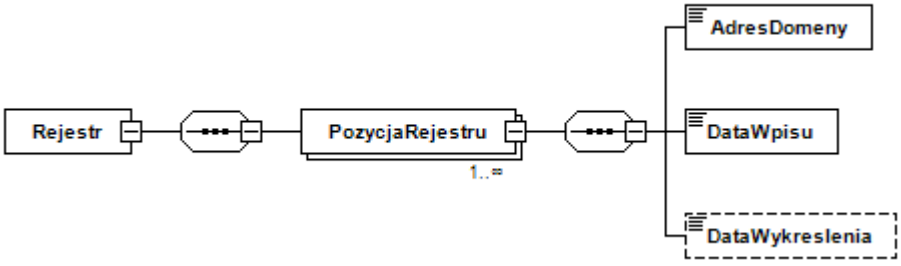
2.4.2 Przykładowe żądanie i odpowiedź XML

```
GET https://hole.cert.pl/domains/v2/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



Rysunek 1: Graficzna reprezentacja schematu XML

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

2.5 Opis formatu JSON

- Adres usługi: `https://hole.cert.pl/domains/v2/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 typie MIME `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 oraz ich subdomeny, 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.

2.5.1 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.

2.5.2 Przykładowe żądanie i odpowiedź JSON

```
GET https://hole.cert.pl/domains/v2/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

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

2.6 Opis formatu AdBlock

- Adres usługi: `https://hole.cert.pl/domains/v2/domains_adblock.txt`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o typie MIME `text/plain`;

Zwracany z usługi plik zawiera listę wszystkich blokowanych domen wpisanych na Listę Ostrzeżeń w formacie zgodnym z programami AdBlock Plus, uBlock Origin, AdGuard. Wszystkie domeny znajdujące się w odpowiedzi powinny zostać zablokowane przez odbiorcę. Jeżeli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Plik zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie są w nim zawarte.

2.6.1 Przykładowa treść pliku w formacie dla AdBlock

```
[Adblock Plus 2.0]
! Version: 202009111243
! Title: CERT.PL's Warning List
! Expires: 1 hours (update frequency)
! Homepage: https://www.cert.pl/news/single/ostrzezenia_phishing/
||zlosliwa-domena1.invalid^$all
||inna-zla-domena.example.com^$all
```

2.7 Opis formatu Hosts

- Adres usługi: `https://hole.cert.pl/domains/v2/domains_hosts.txt`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o typie MIME `text/plain`;

Zwracany z usługi plik w formacie hosts zawiera listę wszystkich blokowanych domen wpisanych na Listę Ostrzeżeń.

Złośliwe domeny kierowane są na adresy IP serwerów będących w dyspozycji CERT Polska - NASK PIB. Po wejściu na złośliwą domenę, użytkownikowi wyświetlony zostaje "landing page" zawierający informacje o tym, że strona stanowi zagrożenie, a także, że przedmiotowa domena została zablokowana na podstawie Listy Ostrzeżeń.

Wszystkie domeny znajdujące się w odpowiedzi oraz ich subdomeny powinny zostać zablokowane przez odbiorcę. Jeżeli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Plik zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie są w nim zawarte.

2.7.1 Przykładowa treść pliku w formacie Hosts

```
# CERT.PL's Warning List
# Homepage: https://www.cert.pl/news/single/ostrzezenia_phishing/
# Source: https://hole.cert.pl/domains/
# Version: 202009111248
# START HOSTS LIST
195.187.6.35 zlosliwa-domena.invalid
195.187.6.34 inna-zla-domena.example.com
```

2.8 Opis formatu MikroTik

- Adres usługi: `https://hole.cert.pl/domains/v2/domains_mikrotik.rsc`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o typie MIME `text/plain`;

Zwracany z usługi plik przeznaczony dla routerów MikroTik zawiera listę wszystkich blokowanych domen wpisanych na Listę Ostrzeżeń. Wszystkie domeny znajdujące się w odpowiedzi powinny zostać zablokowane przez odbiorcę. Jeżeli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Plik zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie są w nim zawarte.

Złośliwe domeny kierowane są na adresy IP serwerów będących w dyspozycji CERT Polska - NASK PIB. Po wejściu na złośliwą domenę, użytkownikowi wyświetlony zostaje "landing page" zawierający informacje o tym, że strona stanowi zagrożenie, a także, że przedmiotowa domena została zablokowana w oparciu o Listę Ostrzeżeń.

UWAGA: Ze względu na ograniczenia techniczne routerów MikroTik, plik z listą blokowanych domen nie może być większy niż 4 kB. W związku z tym, plik `domains_mikrotik.rsc` zawiera wyłącznie kilkadziesiąt/kilkaset najświeższych pozycji Listy Ostrzeżeń, tj. tyle najnowszych rekordów ile maksymalnie można zmieścić bez przekroczenia limitu rozmiaru pliku wynoszącego 4 kB.

2.8.1 Przykładowa treść pliku w formacie MikroTik

```
# Homepage: https://www.cert.pl/news/single/ostrzezenia_phishing/
add name="zlosliwa-domena.invalid" address="195.187.6.35"
add name="inna-zla-domena.example.com" address="195.187.6.34"
```

2.9 Opis formatu RPZ

- Adres usługi: `https://hole.cert.pl/domains/v2/domains_rpz.db`
- Użycie: zapytanie GET za pomocą protokołu HTTPS pod wymieniony adres, bez dodatkowych parametrów;
- Zwracana odpowiedź: kod odpowiedzi `200 OK`; dokument o typie MIME `text/plain`;

Zwracany z usługi plik przeznaczony dla serwerów DNS wspierających mechanizm DNS RPZ (`Domain Name Service Response Policy Zones`) zawiera listę wszystkich blokowanych domen wpisanych na Listę Ostrzeżeń. Wszystkie domeny znajdujące się w odpowiedzi powinny zostać zablokowane przez odbiorcę. Jeżeli domena nie znajduje się w odpowiedzi to oznacza, że nie powinna być blokowana. Plik zawiera wyłącznie aktywne pozycje, tj. pozycje wykreślone z Listy Ostrzeżeń nie są w nim zawarte.

Złośliwe domeny kierowane są na adresy IP serwerów będących w dyspozycji CERT Polska - NASK PIB. Po wejściu na złośliwą domenę, użytkownikowi wyświetlony zostaje "landing page" zawierający informacje o tym, że strona stanowi zagrożenie, a także, że przedmiotowa domena została zablokowana w oparciu o Listę Ostrzeżeń.

2.9.1 Przykładowa treść pliku w formacie RPZ

```
; RPZ file from hole.cert.pl
$TTL 300 ; default TTL
$ORIGIN hole.cert.pl.
@  IN SOA  localhost. root.localhost. (
        1663590735 ; serial
```

```
        300      ; refresh [5m]
        60       ; retry [1m]
        86400    ; expire [1d]
        300      ; minimum TTL [5m]
        )
@  IN NS   localhost.

zlosliwa-domena.invalid CNAME hole.cert.pl.
inna-zla-domena.example.com CNAME hole.cert.pl.
*.inna-zla-domena.example.com CNAME hole.cert.pl.
```

3 Specyfikacja interfejsu do pobierania historycznych informacji o zablokowanych domenach

Opisywany interfejs umożliwia pobranie informacji o historycznych blokadach oraz odblokowaniach domen na Liście Ostrzeżeń przez odwołanie się do publicznie dostępnego REST API, dostępnego za pośrednictwem protokołu HTTPS.

3.1 Opis formatu Actions

- Adres usługi: `https://hole.cert.pl/domains/v2/actions_<rok>.log`
- Oczekiwane żądanie: połączenie za pomocą protokołu HTTPS, zapytanie GET pod wymieniony adres uzupełniony o rok, bez dodatkowych parametrów;
- Zwracana wartość: kod odpowiedzi `200 OK`; dokument o typie MIME `application/x-ndjson`;

Zwracany z usługi plik NDJSON zawiera dane o wszystkich blokadach i odblokowaniach domen na Liście Ostrzeżeń w danym roku. Każda akcja jest zwracana jako pojedyncza linia zawierająca słownik w formacie JSON opisujący daną akcję.

3.1.1 Przykładowa treść pliku w formacie Actions

```
{"RegisterPositionId": 1, "DomainAddress": "zlosliwa-domena.invalid", "ActionTime": "2022-
09-19T08:09:59", "ActionType": "block"}
{"RegisterPositionId": 2, "DomainAddress": "inna-zla-domena.example.com", "ActionTime": "2022-
09-19T08:09:59", "ActionType": "block"}
{"RegisterPositionId": 1, "DomainAddress": "zlosliwa-domena.invalid", "ActionTime": "2022-
09-19T08:09:59", "ActionType": "unblock"}
```

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:

`https://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: `https://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;