Rozwój technik ataku grupy UNC1151/Ghostwriter

cert.pl/posts/2022/07/techniki-unc1151/

Grupa UNC1151/Ghostwriter od ponad roku atakuje skrzynki pocztowe polskich obywateli. Firmy Mandiant i Google, w swoich publikacjach wskazały, że grupa ta z dużym prawdopodobieństwem jest powiązana z rządem Białorusi. Jak wynika z naszych obserwacji, mimo upływu czasu, aktywność tej grupy nie zmniejszyła się, a stosowane przez nią techniki podlegają ciągłym zmianom. W ostatnim czasie obserwujemy wykorzystanie przez nią techniki Browser in the Browser. Technika ta może być wyjątkowo niebezpieczna i łatwa do przeoczenia.

Jedną z najczęściej stosowanych metod ataku przez grupę UNC1151 jest wysyłanie maili phishingowych, które mają na celu wyłudzenie danych do logowania do skrzynek pocztowych. Przejęte skrzynki są następnie przeszukiwane z zamiarem uzyskania dostępu do wrażliwych dokumentów oraz wykorzystywane do przejmowania powiązanych kont w mediach społecznościowych i rozpowszechniania dezinformacji.

Mimo, że początkowo nazwą "Ghostwriter" określono operację prowadzoną przez grupę UNC1151, której celem jest destabilizacja sytuacji politycznej w krajach Europy Środkowej, to obecnie obie te nazwy są używane wymiennie. W tym tekście będziemy posługiwali się głównie nazwą UNC1151.

Nadawca i treść maili

Maile phishingowe są najczęściej wysyłane ze skrzynek pocztowych utworzonych na portalach, z których korzystają potencjalne ofiary ataków. Poniżej przedstawiamy przykładowe adresy wykorzystywane do wysyłki wiadomości.

Cel Ataku	Skrzynka użyta do wysyłki
Konta użytkowników WP	
Konta użytkowników Interia	
Konta użytkowników Onet	
Konta użytkowników o2	
Konta użytkowników Gmail	

W większości przypadków ataki były wymierzone w użytkowników korzystających z dostawców polskich skrzynek pocztowych, ale zaobserwowaliśmy także próbę ataków na konta na Gmailu. W jednym z przypadków ataku na skrzynki poselskie zauważyliśmy, że

atakujący do wysyłki maili wykorzystali błędnie skonfigurowaną politykę SPF, DKIM i DMARC domeny o nazwie zbliżonej do "sejm.pl". Więcej można przeczytać w naszym artykule poświęconym poprawnej konfiguracji mechanizmów weryfikacji nadawcy wiadomości.

Przesyłane wiadomości podszywają się pod administratorów danego serwisu. Ich treść nakłania użytkownika do podjęcia natychmiastowego działania, którego brak może rzekomo doprowadzić do utraty dostępu do skrzynki, a nawet jej skasowania. Co ciekawe, wiadomości początkowo zawierały liczne błędy językowe, ale z biegiem czasu były one coraz lepiej przygotowane. Poniżej prezentujemy najczęstsze motywy oraz przykłady faktycznych maili wysyłanych przez grupę UNC1151. Na czerwono zaznaczono linki, których kliknięcie przenosi użytkownika na stronę wyłudzającą dane logowania.

Temat	**Rzekomy nadawca**	**Motyw**
Blokowanie konta e-mail	Obsługa poczty	Konieczność potwierdzenia danych
Zawieszenie konta	Kontrola Bezpieczeństwa	Złamanie warunków serwisu i konieczność weryfikacji tożsamości
Naruszenia konta	Biuro Obsługi Klienta	Konieczność potwierdzenia własności skrzynki
Skargi	Departament Bezpieczeństwa	Wykrycie podejrzanej aktywności na koncie i konieczność weryfikacji tożsamości
Uwaga	Zespół Poczty	Wykrycie wysyłki spamu z konta i konieczność weryfikacji tożsamości
Krytyczny alert	Walidacja Konta Poczty	Złamanie warunków serwisu i konieczność weryfikacji tożsamości

➤ Przykładowa wiadomość wycelowana w użytkowników poczty WP:

Drogi Użytkowniku / Użytkowniczko,

30 marca w życie wchodzi nowy regulamin. Każdy użytkownik ma obowiązek zaakceptować nowy regulamin jeśli dalej chce korzystać z naszych usług. Pomimo wiadomości z informacjami z zmianie regulaminu, które do Ciebie wysłaliśmy, nowy regulamin nie został jeszcze zaakceptowany.

Jeśli nie zaakceptujesz nowego regulaminu, będziemy zmuszeni zawiesić działanie Twojego konta, a następnie bezpowrotnie je usunąć.

Zaakceptuj nowy regulamin, aby Twoje konto nie zostało usunięte

Jesteśmy z Tobą już od dawna. Mamy nadzieję, że pozwolisz nam dalej dostarczać Twoją pocztę elektroniczną. Nie pozwól, żeby wszystkie wiadomości, zdjęcia, dokumenty w załącznikach i kontakty zostały bezpowrotnie usunięte. Zaakceptuj nowy regulamin i ciesz się najwyższą jakością poczty elektronicznej.

➤ Przykładowa wiadomość wycelowana w użytkowników poczty Interia:

Ta wiadomość pochodzi od Bezpiecznego Nadawcy - Dowiedz się więcej

➤Przykładowa wiadomość wycelowana w użytkowników poczty Onet:

onet POCZTA

Naruszenie zasad korzystania z konta

Dzień dobry,

chcielibyśmy Cię poinformować że nieraz systematycznie naruszałeś warunki specjalne tyczące się odrębnych serwisów.

Konto zostanie skasowane bez ostrzeżenia.

Po usunięciu konta stracisz możliwość korzystania z usług O!Konto i z danych powiązanych nierozerwalnie z kontem.

Jeżeli posiadasz:

konto Onet: wszystkie wiadomości konta zostaną usunięte, a skrzynka pocztowa przestanie być aktywna.
usługi płatne: jeżeli posiadasz subskrypcje, stracisz do nich dostęp. Twoja historia zamówień również zostanie usunięta.
pozostałe usługi: twoje dane osobowe zapisane w bazie profili zostaną skasowane.

Usunięcie skrzynki pocztowej jest nieodwracalne. Jeśli uważasz, że Twoje konto nie zostało użyte z naruszeniem zasad użycia, jesteś uprawniony złożyć odwołanie i zweryfikować konto.

Sposób tworzenia linków

W większości obserwowanych przypadków link zawarty w mailu kierował bezpośrednio na stronę phishingową utrzymywaną przez atakujących. W ciągu ostatniego roku założono prawie 100 domen dedykowanych pod ataki na osoby polskojęzyczne, które można bezpośrednio powiązać z grupą UNC1151. Początkowo były wykorzystywane głównie domeny o rozszerzeniach .site, .website i .online, potem obserwowaliśmy wzrost domen z rozszerzeniem .space, a obecnie najczęściej wykorzystywanym TLD jest .top. Domeny są tworzone w taki sposób, aby pasowały do treści wiadomości. Często w ramach jednej domeny jest kilka subdomen z phishingami na różnych dostawców poczty.

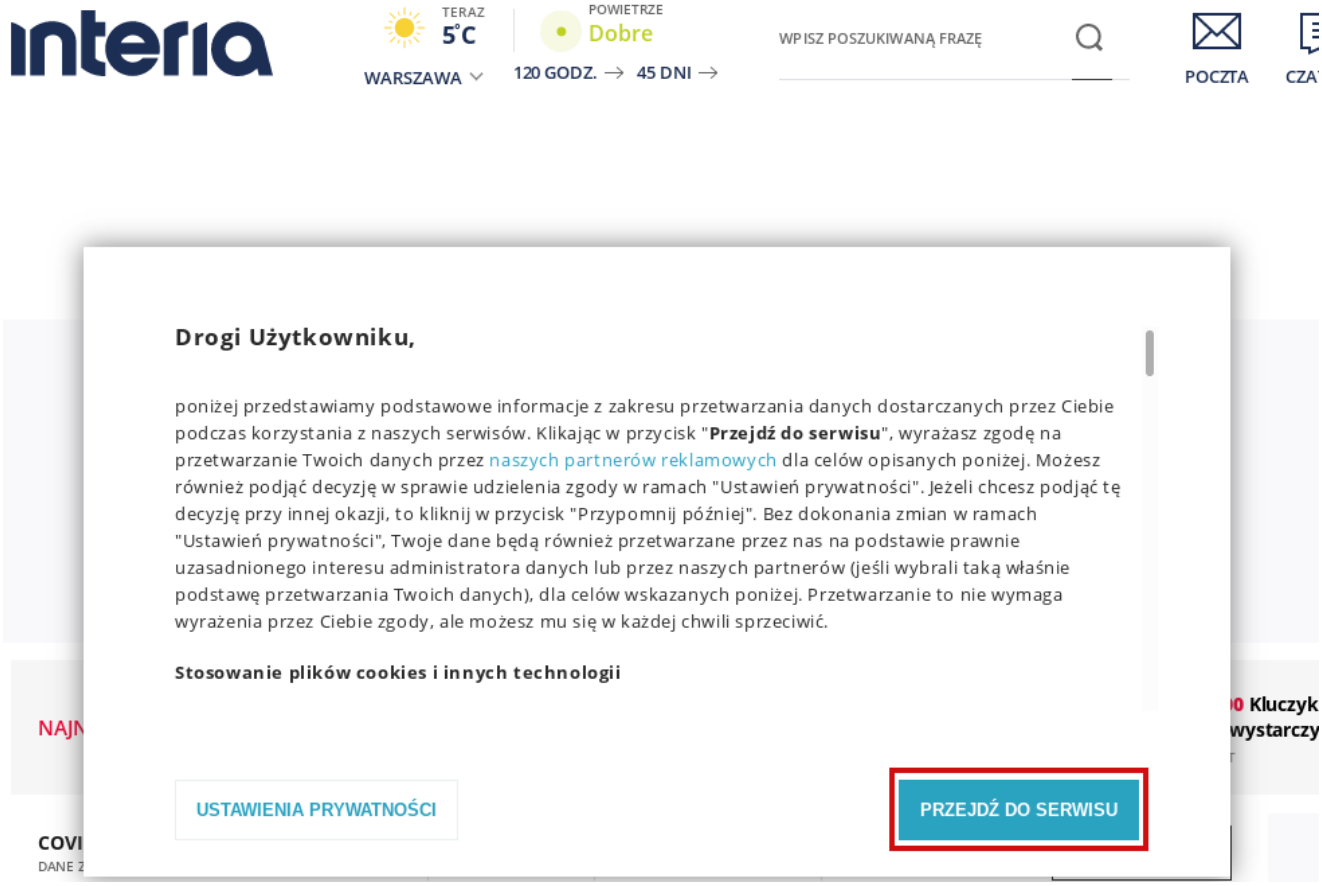
Przykładowe domeny używane w atakach w różnych okresach:

Domena	Data wykorzystania
autoryzacja-poczty.interia.site	2021-06-07
interia.weryfikacja-uzytkownika.site	2021-10-25
konto.safe-onet.online	2021-11-09
poczta.walidacja-konta.space	2021-12-28
poczta.walidacja-uzytkownika.space	2022-01-26
usluga.kontrola-poczty.top	2022-04-12
konto.weryfikacja-uzytkownika.top	2022-07-15

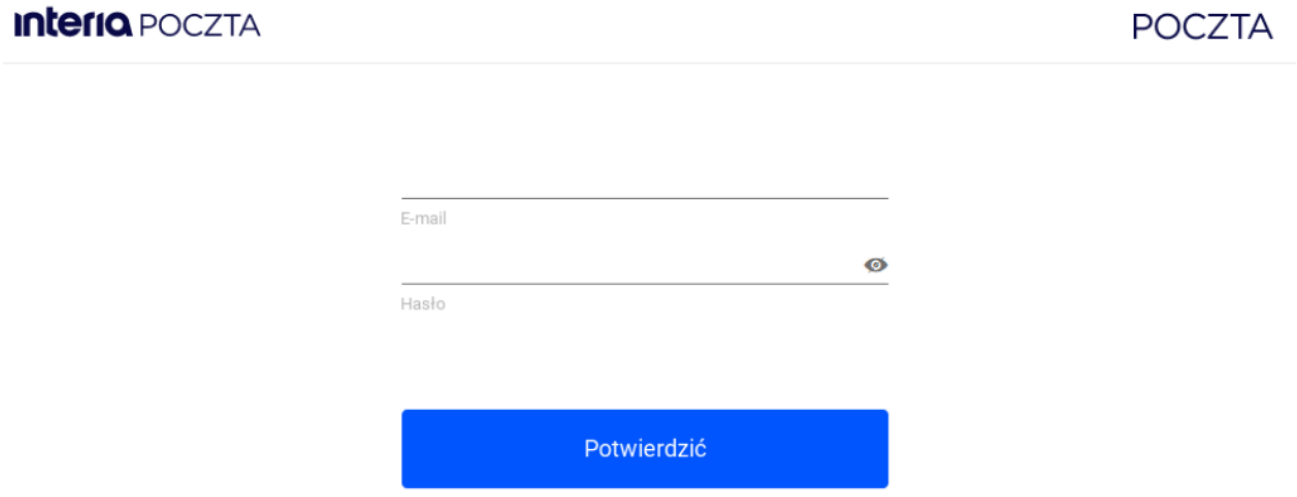
Każdy rozesłany link zawiera unikalny parametr, dzięki któremu atakujący są w stanie śledzić skuteczność kampanii dla każdej z ofiar pojedynczo – od otwarcia maila poprzez osadzone obrazki, przez kliknięcie w link, do podania danych.

Wykorzystanie przejętych stron

W okresie od czerwca 2021 do stycznia 2022, atakujący wykorzystywali przejęte polskie strony internetowe, na których pod dedykowanymi ścieżkami umieszczali przekierowania do phishingu. W mailach był podawany adres przejętej strony, często z długoletnią reputacją, zamiast nowo założonej domeny przez atakujących. Mogło to pomóc w ominięciu filtrów antyspamowych. Przykład strony z takim przekierowaniem pokazano poniżej:



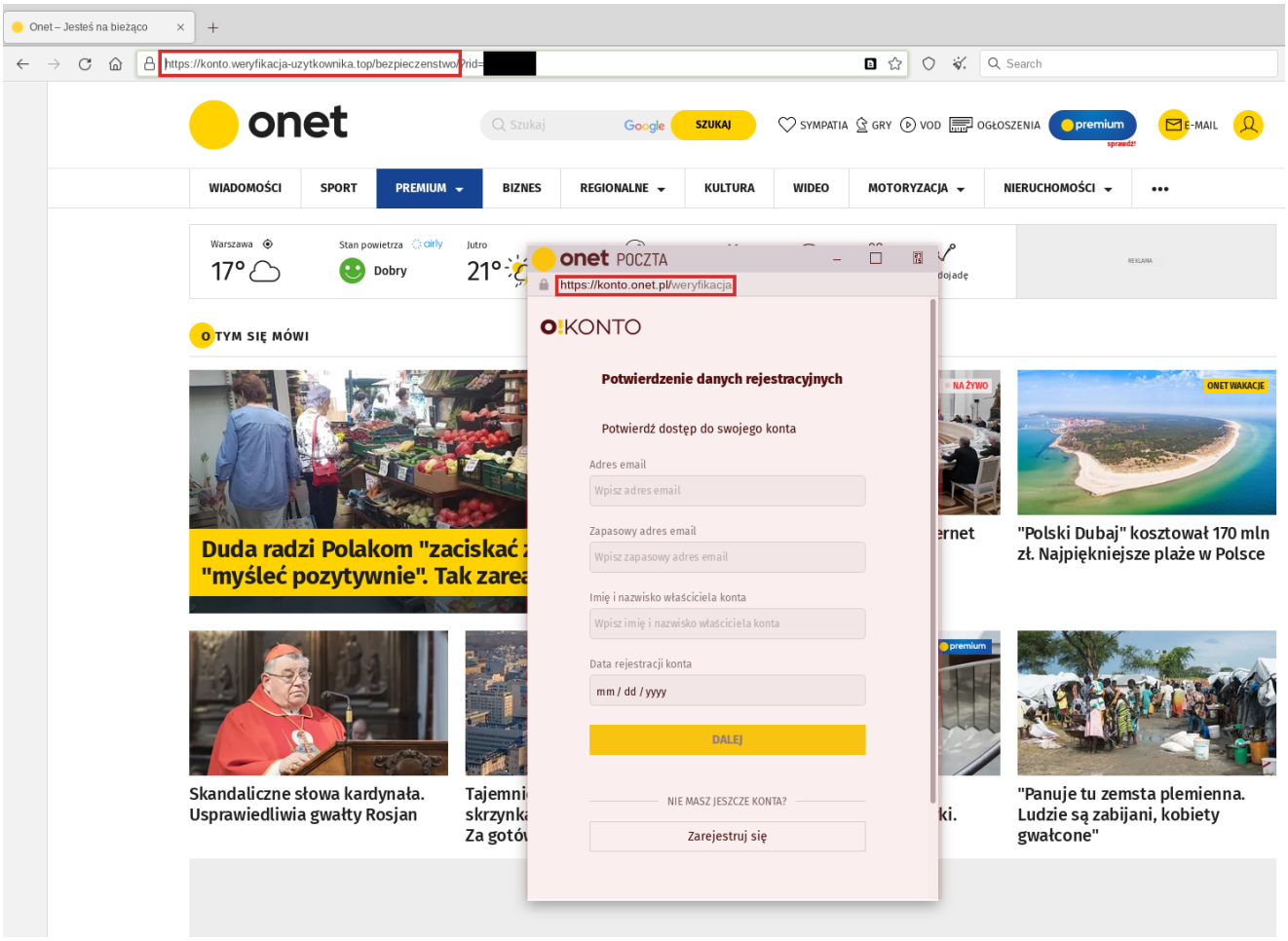
Komunikat udaje informację o stosowaniu plików cookie. Dopiero po kliknięciu "Przejdź do serwisu" ofiara była kierowana na docelową stronę wyłudzającą dane logowania, jak pokazano poniżej:



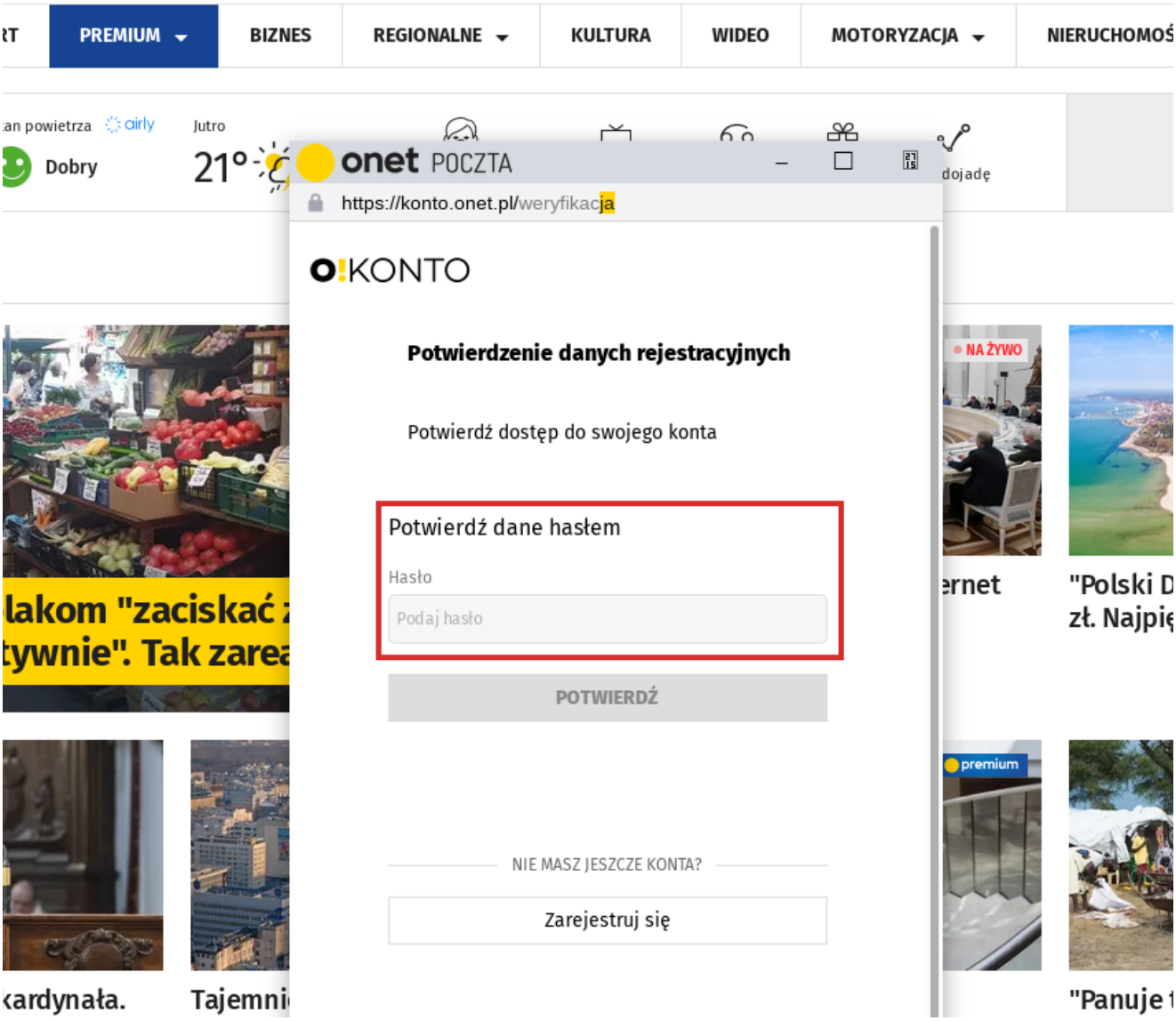
Technika Browser in the Browser

Od marca 2022 roku grupa UNC1151 zaczęła stosować technikę Browser in the Browser, o której ostrzegaliśmy w naszym artykule. Początkowo była ona wykorzystywana głównie w atakach ukierunkowanych na obywateli Ukrainy, ale obecnie obserwujemy ją także w Polsce. Technika ta może być wyjątkowo niebezpieczna i łatwa do przeoczenia. Polega ona na wyświetleniu w ramach odwiedzanej strony pozornie nowego okna przeglądarki, zawierającego fałszywy panel logowania. Okno to, będąc elementem strony, jest na tyle dobrze wykonane, że ofiara może mieć trudność z odróżnieniem spreparowanego okna od faktycznego nowego okna aplikacji.

Poniżej prezentujemy jedną z ostatnich kampanii tego typu skierowaną do użytkowników skrzynek na Onecie:



W kolejnym kroku po kliknięciu "Dalej" ofiara była proszona o podanie hasła. Podzielenie procesu na dwa etapy jest celowym działaniem mającym uśpić czujność i zwiększyć zaangażowanie ofiary:



Podsumowanie

Grupa UNC1151, która, jak wynika z analiz przeprowadzonych przez firmy Google i Mandiant, z dużym prawdopodobieństwem powiązana jest z białoruskim rządem, od ponad roku atakuje skrzynki pocztowe polskich obywateli. Wykorzystywane techniki z biegiem czasu ulegają zmianie, ale motyw przewodni używanych wiadomości, jak i cel pozostaje ten sam.

W obliczu działań grupy UNC1151 mocno zachęcamy do zapoznania się z naszym poradnikiem bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych oraz podzielenia się tą publikacją z bliskimi. Bez działań uświadamiających tego typu ataki nie skończą się i dalej będą ulegały modyfikacjom – nie da się ich całkowicie wyeliminować wyłącznie środkami technicznymi.

Zachęcamy również do zgłaszania wszelkich podejrzanych stron przez formularz na stronie https://incydent.cert.pl/. Jak wynika z naszych danych, w 2021 roku dzięki Waszym zgłoszeniom uchroniliśmy innych użytkowników przed blisko 4 milionami prób wejść na złośliwe strony.