enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Kradzież tożsamości

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

Kradzież tożsamości lub oszustwo dotyczące identyfikacji stanowi nielegalne wykorzystanie danych osobowych ofiary przez oszusta w celu podszycia się pod tę osobę i uzyskania korzyści finansowych oraz innych.

Zgodnie z dorocznym raportem dotyczącym bezpieczeństwa co roku wykrywa się co najmniej 900 przypadków kradzieży tożsamości lub przestępstw związanych z tożsamością[1]. Wśród najbardziej istotnych incydentów można wymienić:

- narażenie danych osobowych prawie 106 milionów klientów amerykańskich i kanadyjskich banków w związku z incydentem naruszenia danych spółki Capital One w marcu 2019 r.[2];
- narażenie 170 mln nazw użytkownika i haseł wykorzystywanych przez twórcę gier cyfrowych Zynga we wrześniu 2019 r.;
- przejęcie 20 mln kont brytyjskiej usługi przesyłania strumieniowego audio Mixcloud[3];
- naruszenie bezpieczeństwa danych osobowych 600 000 kierowców i 57 milionów pasażerów usługi Uber wskutek incydentu w listopadzie 2019 r.[3];
- oraz kradzież 9 mln rekordów danych osobowych klientów spółki EasyJet, w tym dotyczących dokumentów tożsamości i kart kredytowych.

Trend kradzieży tożsamości w dużym stopniu znajduje odzwierciedlenie w naruszeniach danych, które w porównaniu z 2018 r. odnotowały rekordową liczbę 3800 publicznie ujawnionych przypadków, 4,1 mld narażonych zapisów oraz wzrost liczby zgłoszonych naruszeń o 54%[4].

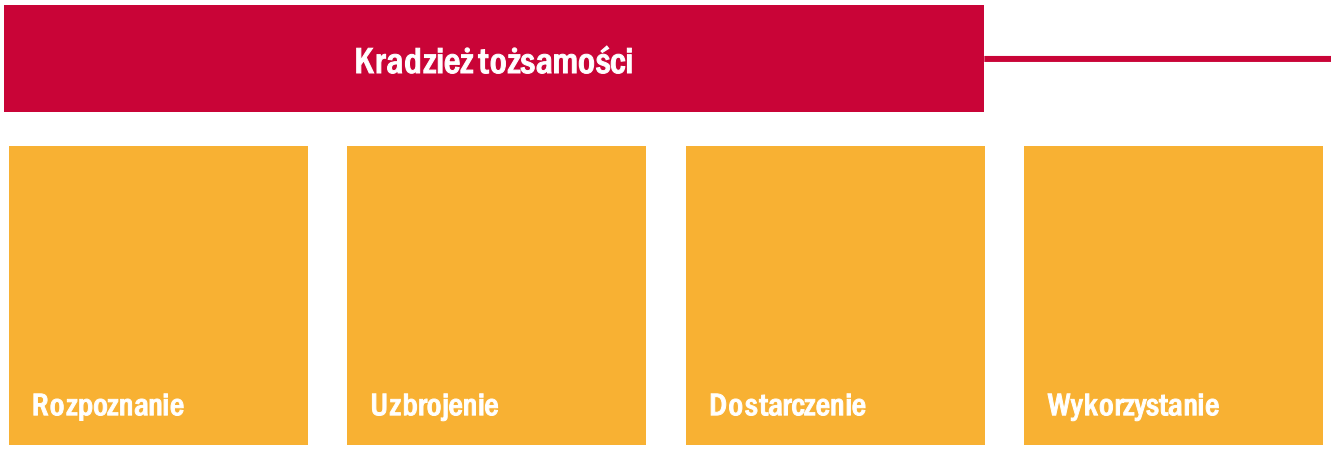
Wnioski

Rysunek 1: Źródło: Z badania koncernu IBM na temat bezpieczeństwa, dotyczącego kosztów zagrożeń wewnętrznych: Raport globalny[13]

Zagrożenie kradzieżą tożsamości

W roku 2019 niektórzy sprawcy szkodliwych działań kryjący się za poważnymi incydentami zostali postawieni przed sądem. W czerwcu nowojorska policja we współpracy z FBI postawiła przed sądem członków grupy „Fraud Ring", działającej w Stanach Zjednoczonych i innych krajach, której w 2012 r. udało się wykraść dane uwierzytelniające z iPhone'ów o wartości 1 mln USD (ok. 846 tys. EUR) w ramach zakrojonej na szeroką skalę operacji kradzieży tożsamości. Zanim udało się powstrzymać grupę, skradziona kwota osiągnęła wartość 19 mln USD (ok. 16 mln EUR)[4]. Miesiąc później poinformowano publicznie o „ugodzie Equifax"5. Spółka Equifax została zmuszona do wyrażenia zgody na wypłatę odszkodowania na rzecz Federalnej Komisji Handlu Stanów Zjednoczonych, Biura Ochrony Finansowej Konsumentów, 48 stanów, Dystryktu Kolumbia i Portoryko za naruszenie danych w 2017 r., o wartości co najmniej 575 mln USD (ok. 487 mln EUR). Z powodu tego naruszenia danych, które sklasyfikowano jako „całkowicie możliwe do uniknięcia", wyciekło prawie 148 milionów amerykańskich adresów i numerów ubezpieczenia społecznego. Pod koniec roku Brazylia nałożyła na serwis Facebook karę o wartości 1,6 mln USD (ok. 1,35 mln EUR) w imieniu obywateli tego kraju, w związku z wyciekiem danych dotyczącym spółki Cambridge Analytica[3].

Kill chain



Proces etapów ataku

Zakres działania

Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury, z jakich skorzystał atakujący.

WIĘCEJ INFORMACJI

Ataki z podszywaniem się pod markę

Zgodnie z trendami dla roku 2018, niektóre marki częściej padały ofiarą ataków z podszywaniem się, z powodu ich dobrej reputacji. Chociaż marki te – takie jak Microsoft (44%) i Amazon (17%) – nadal są liderami w rankingach ataków z podszywaniem się pod markę z 2019 r., należy zwrócić uwagę na nowe ofiary, takie jak amerykański urząd podatkowy (Internal Revenue Service – IRS)[7]. Szczególnie poufne informacje zawarte w deklaracji Wage and Tax Statement (W-2) były zawsze pokusą dla oszustów, którzy wykorzystywali podszywanie się pod IRS w 10% e-maili opartych na oszustwach dotyczących tożsamości w tym roku objętym raportem. Dlatego też prawidłowe formularze W-2 i standardowe amerykańskie formularze zwrotu podatku dla osób fizycznych (1040) są dostępne w „ciemnej sieci" w cenie 1–52 USD.

Materiały te, w połączeniu z numerami ubezpieczenia społecznego (Social Security Number – SSN) i datami urodzenia, które są również dostępne, umożliwiają każdemu niedoświadczonemu hakerowi, który chce zainwestować kwotę 1000 USD (około 846 EUR), legalny dostęp do rachunku bankowego w Stanach Zjednoczonych, złożenie fałszywego zeznania podatkowego, ubieganie się o zwrot podatku i wypłatę podwojonej lub potrojonej zainwestowanej kwoty. Zdaniem komórki ds. dochodzeń kryminalnych ponad 10 000 indywidualnych zeznań podatkowych z wnioskami o zwrot ponad 83 mln USD (około 70 mln EUR) stanowiło prawdopodobnie próbę wyłudzenia[9].

Cykl etapów wyłudzenia podatkowego „Parszywa dwunastka”

Rysunek 2 – źródło: BDO[19]

Trendy

_Podmiana tożsamości karty SIM

Technika ta jest stosowana od roku 2016 i wymierzona jest głównie w posiadaczy kryptowalut. W 2019 r. tę samą technikę wykorzystano jednak w stosunku do znanych osobistości lub ich kont z zamiarem kradzieży tożsamości ofiary. Ofiarami podmiany tożsamości kart SIM padły takie osoby, jak Jack Dorsey (dyrektor zarządzający Twittera), Jessica Alba (aktorka), Shane Dawson (aktor), Amanda Cerny (aktorka, dwukrotnie), Matthew Smith (aktor, czterokrotnie) i King Bach (artysta)[10]. Podmiana tożsamości kart SIM została również zastosowana na dużą skalę w dwóch przypadkach: w największym banku Mozambiku, gdzie skradziono aż 50 000 USD (ok. 42 300 EUR) z kont biznesowych znanych osób, oraz w Brazylii, gdzie urządzenia 5000 osób, głównie polityków, ministrów i gubernatorów, padły ofiarą ataku hakerów należących do zorganizowanego gangu[11].

_Karty podarunkowe jako koń trojański używany w celu włamania do poczty służbowej (BEC)

W roku 2019 ataki z naruszeniem na szwank wiadomości e-mail spowodowały straty o wartości miliardów euro. W takich przypadkach przestępcy podszywają się pod zaufaną osobę, zwykle w firmie, i nakłaniają podstępem ofiarę do dokonania transakcji finansowej lub ujawnienia poufnych informacji, osobistych lub firmowych. W przypadku ponad połowy ataków BEC ofiarę nakłoniono do zakupu karty podarunkowej. Podczas procesu sprzedaży doszło do przejęcia informacji poufnych, jak dane uwierzytelnienia rachunku bankowego. Ofiarę zmuszono także do przesłania przestępcy karty podarunkowej w postaci anonimowej, nieodwracalnej i bezpośredniej opcji zamiany na gotówkę. Średnia wartość kwoty skradzionej z użyciem karty podarunkowej to 1500 USD (ok. 1269 EUR)[12].

Wnioski

20%_ ataków z przejęciem tożsamości korzystało z kont, w przypadku których doszło do naruszenia zasad bezpieczeństwa[7]

30%_ ataków wzięło na cel konta kadry kierowniczej najwyższego szczebla, które przejęto z użyciem wyświetlania fałszywej nazwy[7]

65%_ ataków BEC nakłoniło ofiary do zakupu kart podarunkowych[12]

3,32_ mln USD to średni koszt naruszenia bezpieczeństwa danych

95%_ uczestników ankiety Eurobarometr uważało kradzież tożsamości za poważne przestępstwo

Trendy

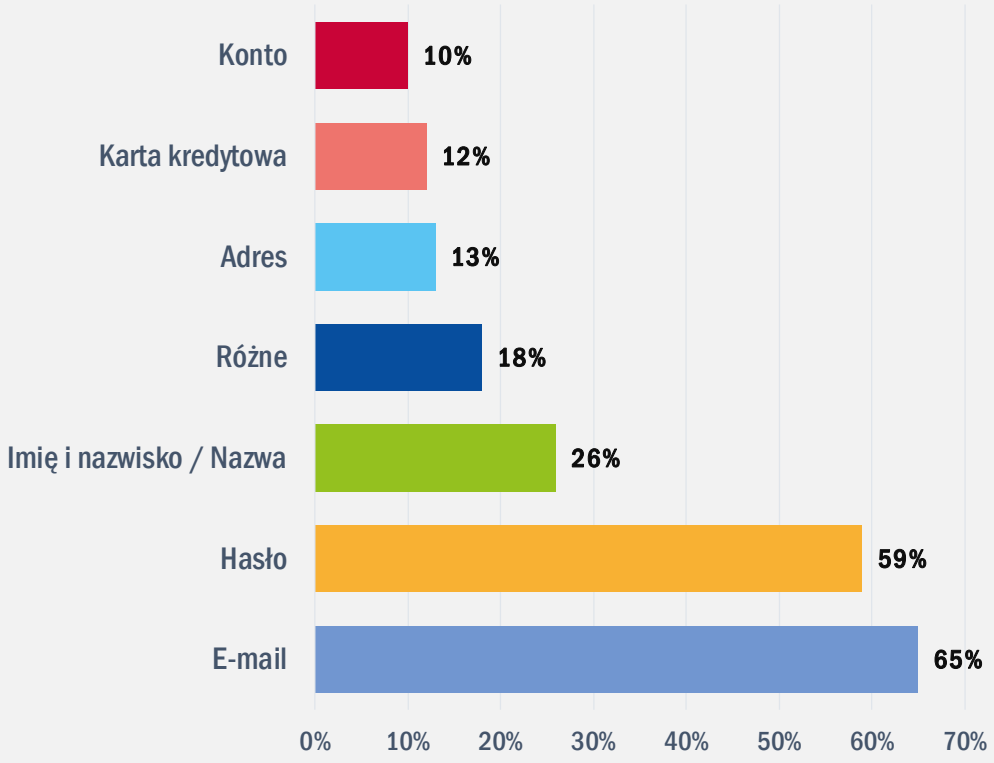
_Cyfrowe sobowtóry

Technika zwalczania nadużyć o nazwie „cyfrowe maski" została ujawniona, gdy ponad 60 000 skradzionych tożsamości cyfrowych pojawiło się jako produkt handlowy w sklepie Genesis w „ciemnej sieci" w kwietniu 2019 r. Sobowtóry te można było łatwo kupić w cenie 5–200 USD. Właściciel sobowtóra może łatwo imitować rzeczywistego użytkownika w sklepie internetowym lub usłudze płatniczej, zwłaszcza w połączeniu ze skradzionymi loginami i hasłami. Poza możliwością zakupu cyfrowych sobowtórów pojawiły się nowe narzędzia wspomagające potencjalnych podszywających się, jak przeglądarka Tenebris, która zawiera generator umożliwiający tworzenie unikatowych „odcisków palców" i masek cyfrowych[11].

W ostatnich latach za główne grupy odpowiedzialne za ataki z kradzieżą tożsamości uznano oszustów kopiujących dane kart kredytowych, przeszukujących śmietniki, hakerów, podszywających się pod administratorów i osoby stosujące phishing. W 2019 r. lista ta powiększyła się o takie pojęcia, jak „visher" i „smisher". „Visher" to osoba stosująca techniki phishingu przez telefon. W przeciwieństwie do osób podszywających się pod innych, „visherzy" udają, że reprezentują znaną organizację i oferują ofierze pomoc przy korzystaniu z usługi, na przykład zarządzaniu oprogramowaniem komputerowym, finansach czy zwrocie podatku. „Smisherzy" wysyłają fałszywe SMS-y, a gdy odbiorca odpowie, jego urządzenie zostanie przejęte bezpośrednio lub przekierowane do witryny wyłudzającej dane.

Na poniższej ilustracji przedstawiono najczęściej utracone rodzaje danych w 2019 r., zaś dane kont e-mail stanowią największy odsetek utraconych lub skradzionych rekordów. Liczby te ujawniają powagę sytuacji, gdy uwzględnić, że wiadomości e-mail mogą zawierać poufne informacje osobiste, firmowe i rządowe.

Najczęściej tracone rodzaje danych w 2019 r.



Rysunek 3 – źródło: RiskBased SECURITY[8]

Wektory ataku

Jak

- **CHMURA STANOWI INTERFEJS ATAKU DLA DANYCH KLIENTÓW**. W roku objętym raportem ucierpiała sieć dostarczająca treści (Content Delivery Network – CDN) Amazon CloudFront[14]. Witryny hostowane lub połączone z bibliotekami w infrastrukturze Amazona zostały narażone na szwank, gdyż wyciekły treści przesyłane zewnętrznie, w tym dane kart kredytowych.
- **ADRESY URL SŁUŻĄCE DO WYŁUDZANIA INFORMACJI**. W roku 2019 znów stosowane były powszechne techniki złośliwego oprogramowania dotyczące adresów URL[16], jak cybersquatting (złośliwe rejestrowanie domen z nazwą firmy czy instytucji), rejestrowanie podobnych domen czy narzędzia do skracania adresów URL.W ostatnim kwartale 2019 r. zauważono, że 26% złośliwych domen wykorzystywało bezpieczny certyfikat, a jeden certyfikat na trzy był certyfikatem SSL. Sztuczka ta zaburzała u użytkowników zdolność oceny, gdyż byli oni przyzwyczajeni do tego, że ikona kłódki w przeglądarce oznacza bezpieczeństwo[15].
- **Oszustwo W2**. Kolejnym atakiem wymierzonym przeciwko rekordom firm i organizacji i mającym na celu uzyskanie dostępu do informacji poufnych jest oszustwo W2. Oszuści zaczynają od podszywania się pod pracowników wyższego szczebla działu finansowego lub działu zasobów ludzkich do uzyskania rekordów pracowników. Rekordy te są następnie używane do kradzieży tożsamości. Nazwa oszustwa pochodzi od amerykańskiego formularza W2 używanego do zgłaszania wynagrodzeń pracowników. Uważa się, że liczba tego rodzaju oszustw opartych na zasadach inżynierii społecznej wzrosła w ciągu kilku ostatnich lat o 10% rocznie, choć nie jest ono nowe (po raz pierwszy zgłoszono je w 2016 r.)[9,17].
- **NIMCY**. W 2019 r. pojawiło się narzędzie wykorzystujące technikę „spear-phishingu", NIMCY, wprowadzone przez grupę odpowiedzialną za rodzinę złośliwego oprogramowania Zebrocy. Napisano je z użyciem języka Nim (dawniej Nimrod), stworzonego przez tę samą grupę hakerów. Ten nowy program do pobierania i uzyskiwania nieuprawnionego dostępu był używany do wykradania poświadczeń, naciśnięć klawiszy, przesyłanych wiadomości i plików od dyplomatów, urzędników sektora obronnego i pracowników ministerstw spraw zagranicznych. Atakujący najwyraźniej koncentrowali się na instytucjach rządowych ze środkowej Azji, szczególnie Pakistanie i Indiach[14].

- **ZAGROŻENIA DLA URZĄDZEŃ MOBILNYCH.** W roku 2019 zauważono rosnącą liczbę zagrożeń dla urządzeń mobilnych i trend ten utrzymywał się w 2020 r. Nawet szeroko wykorzystywane i zaufane platformy, jak Google Play, hostowały aplikacje używane do wykradania poświadczeń np. (np. Acesse SantaMobile, Modulo ID). Liczba pobrań była jednak bardzo niska, co świadczy, że potencjalnych ofiar nie udało się zwieść[20].

- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** Ósmy pod względem popularności koń trojański dla urządzeń mobilnych i najpopularniejszy bankowy koń trojański dla urządzeń mobilnych odpowiedzialny odpowiednio za 1,75% i 16,85% unikatowych ataków, w większości przypadków mający za cel poświadczenia bankowe ofiar i kody autoryzacyjne do uwierzytelniania dwuskładnikowego. Większość ofiar tego konia trojańskiego mieszka w Rosji, co sprawia, że należy ona do krajów z największym odsetkiem użytkowników atakowanych przez bankowe konie trojańskie dla urządzeń mobilnych[21].

- **FORMJACKING.** Technika o nazwie „formjacking" była wyjątkowo popularna w 2018 r., lecz wygląda na to, że liczba ataków znacząco spadła w pierwszym kwartale 2019 r. Jednak począwszy od majowego ataku na instytucje amerykańskiej ochrony zdrowia i kradzieży danych do logowania, liczba ataków nadal rosła w pozostałych miesiącach roku. W tym miesiącu odnotowano rekordowo wysoką liczbę 1,1 mln wykrytych przypadków. Pięć krajów, w których w 2019 r. wykryto najwięcej przypadków użycia techniki formjacking, to Stany Zjednoczone (51,8%), Australia (8,1%), Indie (5,7%), Wielka Brytania (4,1%) i Brazylia (3,5%). Grupa hakerska Megacart jest silnie powiązana z większością tworzonych narzędzi do formjackingu i atakami na takie organizacje, jak British Airways, Newegg, Feedify i Ticketmaster[22].

Ograniczenie ryzyka

Proponowane działania

- Unikanie korzystania z menedżera haseł w przeglądarce. W razie potrzeby można użyć zabezpieczonego menedżera haseł offline[23].
- Uwierzytelnianie każdego nadawcy zlecającego przelew pieniężny telefonicznie lub osobiście[19].
- Nie wolno udostępniać danych poufnych, jak rekordy dotyczące pacjentów, w postaci ręcznie zapisywanych notatek, by zapobiec ich utracie lub zagubieniu. Pliki cyfrowe to lepsza metoda danych wykorzystywanych przez krótki czas – następnie powinny one być niszczone.
- Używanie „wyszukiwania zagrożeń" w firmie, by wzmocnić plany zabezpieczeń. Wyszukiwanie zagrożeń prowadzą wykwalifikowani członkowie centrum operacyjnego bezpieczeństwa, których celem jest proaktywna identyfikacja luk w zabezpieczeniach i uniemożliwienie zagrożeniom ich wykorzystywania.
- Używanie zbiorów zasad, takich jak zasady oparte na prędkości, w celu ograniczenia liczby oszustw związanych z tożsamością, zwłaszcza w przypadku transakcji z użyciem kart płatniczych. Dane urządzeń prawidłowych transakcji mogą zapewnić wystarczającą ilość informacji do optymalnego stworzenia zasad.
- Używanie metody uwierzytelnienia z logowaniem jednokrotnym, jeśli jest dostępne, co umożliwia użytkownikowi uzyskanie dostępu do kilku aplikacji przy użyciu tego samego zbioru poświadczeń cyfrowych. Zaleca się usilnie stosowanie tego rozwiązania w celu zminimalizowania liczby kont użytkowników i zapisanych poświadczeń.
- Instalowanie ochrony punktów końcowych z użyciem oprogramowania antywirusowego, lecz również odpowiednie blokowanie plików wykonywalnych (np. blokowanie wykonywania w folderze tymczasowym).
- Uwierzytelnianie wieloskładnikowe to metoda zabezpieczeń pozwalająca na radzenie sobie z przejmowaniem czy utratą haseł i zapewnienie skuteczności procesu uwierzytelniania dzięki wielu kluczom. Wprowadzenie adaptacyjnego uwierzytelniania wieloskładnikowego pozwala zoptymalizować proces uwierzytelniania w oparciu o zachowania użytkowników i powiązane treści.

- Sprawdzanie adresów URL przesłanych we wiadomości e-mail lub odwiedzanych losowo w oparciu o ich adres IP, numer AS powiązany z IP, właściciela domeny czy relacje między tą domeną a innymi, przed podjęciem jakichkolwiek dalszych działań.
- Organizacje korzystające z usług w chmurze powinny prowadzić szeroko zakrojone działania w zakresie bezpieczeństwa w chmurze i najlepiej korzystać równocześnie z architektury przechowywania danych na miejscu, przechowywania w chmurze prywatnej i publicznej w celu chronienia danych osobowych klientów.
- Wymuszanie korzystania z silnych i aktualizowanych metod szyfrowania, jak TLS 1.3 (z użyciem krótkotrwałych kluczy sesji) w przypadku danych szczególnie chronionych, co utrudnia zadanie hakerom.
- Odpowiednie zabezpieczanie wszystkich dokumentów tożsamości oraz ich kopii (fizycznych lub cyfrowych) przed nieuprawnionym dostępem.
- Nieujawnianie danych osobowych przypadkowym odbiorcom i niereagowanie na prośby telefonicznie, w wiadomości e-mail lub osobiste.
- Wymuszanie używania urządzeń chronionych hasłem, zapewnianie dobrej jakości poświadczeń i bezpiecznych metod ich przechowywania.
- Zapewnianie dobrej jakości poświadczeń i bezpiecznych metod ich przechowywania we wszystkich wykorzystywanych mediach.
- Zachowanie szczególnej ostrożności podczas korzystania z publicznych sieci Wi-Fi, gdyż oszuści włamują się do nich lub imitują je. Podczas korzystania z takich sieci należy unikać dostępu do poufnych aplikacji i danych. Korzystanie z zaufanej usługi VPN przy łączeniu się z publicznymi sieciami Wi-Fi.
- Regularne sprawdzanie transakcji w wyciągach bankowych lub otrzymanych paragonach pod kątem nietypowych pozycji.
- Zainstalowanie oprogramowania do filtrowania treści w celu filtrowania niechcianych załączników, wiadomości ze złośliwymi treściami, spamu i niechcianego ruchu w sieci.
- Wymuszanie rozwiązań zapobiegających utracie danych.

Bibliografia

1. „2019 identity theft report released", 31 lipca 2019 r. ITIJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. „Capital One data breach: What you can do now following bank hack" , 12 sierpnia 2019 r. C | Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. „Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks". 8 stycznia 2020 r. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4. „$19 million worth of iPhones stolen in massive identity theft scam", 15 czerwca 2019 r. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. „Equifax to pay at least $575 million as part of FTC settlement" 22 lipca 2019 r. C | Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6. „2019 data breaches: 4 billion records breached so far" Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. „Q1 2019: Email Fraud and Identity Deception Trends" Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. „Data Breach QuickView Report, 2019 Q3 trends". Listopad 2019 r. RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. „IRS issues 2019 annual report; highlights program areas across the agency" 6 stycznia 2020 r. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. „Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too" 5 września 2019 r. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. „IT threat evolution Q2 2019", 19 sierpnia 2019 r. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. „Phishing Activity Trends Report", 12 września 2019 r. Anti-phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. „The Cost of Insider Threats" IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. „APT trends report Q2 2019", 1 sierpnia 2019 r. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. „Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more" Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. Raport ENISA o krajobrazie zagrożeń 2018 r. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. „Q2 2019 Cryptocurrency Anti-Money Laundering Report" CipherTrace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

18. „Latest Quarterly Threat Report – Q1 2019" Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

19. „BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare", październik 2019 r. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

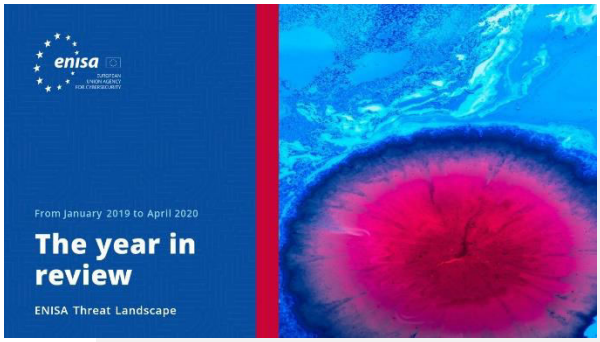
20. „IT threat evolution Q1 2019. Statistics", 23 maja 2019 r. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. „IT threat evolution Q3 2019. Statistics", 29 listopada 2019 r. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. „FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month", sierpień 2019 r. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. „Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web" VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

Powiązany



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Przegląd roku

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

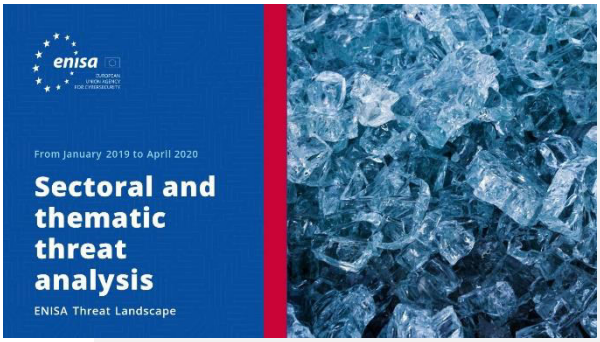
Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie cyberbezpieczeństwa i rozpoznawania zagrożeń cybernetycznych.



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Omówienie kwestii rozpoznawania cyberzagrożeń

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

Informacje o agencji

_ Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

Marco Barros Lourenço (ENISA) i Louis Marinos (ENISA).

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecja
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu