enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Wyłudzanie informacji (phishing)

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

Informacje ogólne

Wyłudzanie informacji, czyli phishing, to oszukańcza próba kradzieży przy użyciu technik inżynierii społecznej danych użytkownika, takich jak dane logowania, informacje o karcie kredytowej, a nawet pieniądze. **Ten rodzaj ataku jest zazwyczaj przeprowadzany za pomocą wiadomości e-mail, które wyglądają na wysłane z zaufanego źródła, z zamiarem nakłonienia użytkownika do otwarcia złośliwego załącznika lub podążania za fałszywym adresem URL**. Profilowane wyłudzanie informacji, zwane „spear phishing" opiera się na wstępnym wyszukiwaniu informacji o ofiarach, by próba oszustwa wyglądała bardziej autentycznie, dlatego też jest to jeden z najskuteczniejszych typów ataków na sieci przedsiębiorstw[1].

Emocjonalna reakcja skłania ludzi do nieostrożnych działań, które skutkują wyłudzeniem – do tego właśnie dążą hakerzy.Podczas symulacji wyłudzenia danych w ramach szkolenia należy kłaść na to nacisk. Szkolenie użytkowników poczty elektronicznej jest jednym z często stosowanych środków zapobiegania wyłudzeniu informacji, ale rezultaty nie są przekonujące, gdyż sprawcy zagrożeń stale zmieniają *sposób działania*. Standard uwierzytelniania wiadomości, sprawozdawczości i zgodności oparty na domenie (DMARC) zapewnia, że wiadomości e-mail z oszukańczych domen zostaną zablokowane, co zmniejszy odsetek skutecznych ataków z wyłudzaniem informacji, fałszowaniem adresu e-mail danych i wysyłaniem niechcianych wiadomości (spamu).

W przyszłości poczta e-mail pozostanie najczęściej stosowanym mechanizmem wyłudzania danych, lecz stan ten nie utrzyma się zbyt długo. Już dostrzegamy coraz częstsze wykorzystywanie komunikatorów serwisów społecznościowych, WhatsApp i innych, do przeprowadzania ataków. Najistotniejsza zmiana nastąpi w przypadku metod stosowanych do wysyłania wiadomości, które staną się bardziej wyrafinowane wraz z zastosowaniem wrogiej sztucznej inteligencji (AI) do przygotowania i wysyłania wiadomości. Wyłudzanie informacji i profilowane wyłudzanie informacji („spear phishing") to główne wektory ataku dla innych zagrożeń, jak nieumyślne zagrożenia wewnętrzne.

Wnioski

26,2_ **mld strat w 2019 r. z powodu ataków z włamaniem do poczty służbowej (Business E-mail Compromise, BEC)[20]**

42,8%_ **wszystkich złośliwych załączników stanowiły dokumenty Microsoft Office[25]**

667%_ **więcej przypadków oszustw z użyciem wyłudzania informacji zaledwie w ciągu 1 miesiąca podczas pandemii COVID-19[6]**

30%_ **wiadomości mających na celu wyłudzenie informacji jest dostarczanych w poniedziałki[29]**

32,5%_ **wszystkich wiadomości e-mail wykorzystuje słowo „płatność" w tytule[28]**

Kill chain

Wyłudzanie informacji (phishing)

Rozpoznanie	Uzbrojenie	Dostarczenie	Wykorzystanie

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

Trendy

_Najczęściej atakowane rodzaje usług to poczta internetowa i oprogramowanie jako usługa

Zgodnie z niektórymi prognozami w pierwszym kwartale 2019 r. liczba ataków typu wyłudzanie informacji ukierunkowane na oprogramowanie jako usługa (SaaS) i pocztę internetową po raz pierwszy przewyższyła liczbę ataków skierowanych przeciwko usługom płatniczym, co czyni z nich najbardziej profilowany sektor – 36% wszystkich ataków typu wyłudzanie informacji[2]. Ten nowy rekord jest zgodny z trendem w 2018 r., kiedy to takie usługi, jak SaaS i poczta internetowa wyprzedziły sektor finansowy[3]. Choć liczba ta spadła do 30,8% do końca 2019 r., powyżej wymienione usługi nadal plasują się na szczycie listy[2,3], zaś **usługi Microsoft 365 są najczęstszym celem wyłudzających informacje**[4].

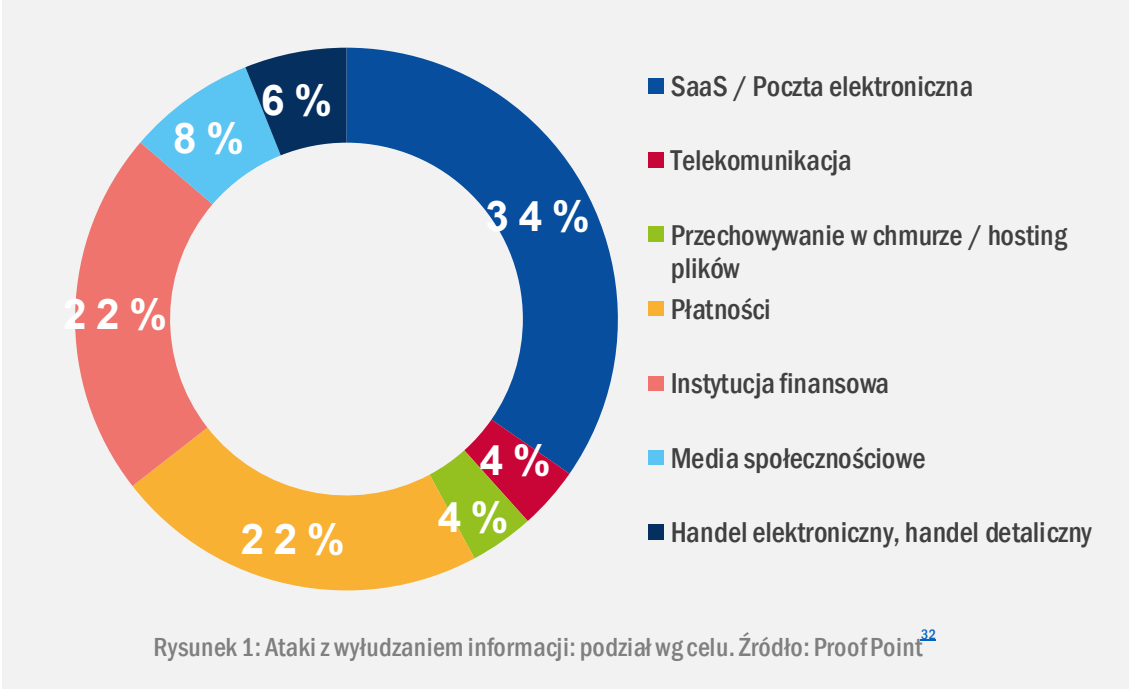
_Ataki z włamaniem do poczty służbowej (BEC) nadal stanowią problem

W przeprowadzonym niedawno badaniu ustalono, że 88% organizacji z całego świata doświadczyło profilowanego wyłudzania informacji, a 86% z nich doznało ataków z narażeniem na szwank firmowych wiadomości e-mail (BEC)[16]. W 2019 r. do najbardziej zagrożonych atakami należały usługi Microsoft 365, a ich głównym celem było pozyskanie poświadczeń[17]. Po uzyskaniu tych poświadczeń atakujący mógł zebrać więcej danych dotyczących organizacji, co mogło trwać tygodniami lub miesiącami18, a następnie mogło prowadzić do ataków z profilowanym wyłudzaniem informacji. Atakujący podszywał się pod pracownika, dyrektora wykonawczego (CEO), czy nawet zaufanego dostawcę, by przenieść środki lub przekierować płatności na rachunki podmiotów zewnętrznych[14] W pierwszym kwartale 2019 r. firmy były narażone na wzrost ataków BEC o 120% w stosunku do poprzedniego roku[19], skutkujących stratami w wysokości 26,2 mld USD (ok. 22,2 mld EUR)[20].

Ponad dwie trzecie witryn wykorzystujących wyłudzanie informacji wprowadziło protokół HTTPS

W ciągu kilku ostatnich lat zaobserwowano wyraźny wzrost[13] liczby witryn wyłudzających informacje, które wprowadziły protokół HTTPS. W ostatnim kwartale 2019 r. 74% witryn wyłudzających informacje wykorzystywało protokół HTTPS[32], co stanowi istotny wzrost w porównaniu z zaledwie 32% dwa lata wcześniej. Chociaż takie technologie, jak HTTPS i SSL są przeznaczone do zabezpieczania komunikacji między klientem a serwerem, obecność ikony kłódki na pasku adresu przeglądarki może stwarzać złudzenie, że strona jest godna zaufania.

Sprawcy zagrożeń mogą także wykorzystywać legalne witryny, które przejmują, by umieścić na nich treści służące do wyłudzania informacji, więc użytkownikowi końcowemu trudniej jest zidentyfikować witrynę jako niebezpieczną[14]. Inne elementy przyczyniające się nagłego wzrostu wykorzystania protokołu HTTPS to różnorodne bezpłatne usługi oferujące certyfikaty, jak Let's Encrypt[15] i fakt, że nowoczesne przeglądarki oznaczają każdą witrynę wykorzystującą protokół HTTPS jako bezpieczną i nie przeprowadzają dalszych kontroli.



Rysunek 1: Ataki z wyłudzaniem informacji: podział wg celu. Źródło: Proof Point[32]

Trendy

_Wzrost liczby przypadków ataku Phishing-as-a-Service (PhaaS)

Usługi tego rodzaju są zazwyczaj oparte na abonamencie lub mają postać zestawu, dostępnego do pobrania za opłatą, i usuwają bariery techniczne utrudniające dostęp, ponieważ umożliwiają one przeprowadzenie ukierunkowanego ataku przez osobę o mniejszych umiejętnościach technicznych. Raport analityka bezpieczeństwa [21] wymieniał 5334 unikatowe zestawy do wyłudzania informacji dostępnych do czerwca 2019 r. Stosunkowo niski koszt tych rozwiązań, około 50–80 dolarów za miesięczny abonament, był jeszcze bardziej niepokojący. W tym samym raporcie znalazła się informacja, że 87% zestawów zawierało mechanizmy unikania wykrycia, jak kodowanie znaków HTML i szyfrowanie treści. Co ciekawe, niektóre z tych usług hostowano w ramach legalnych usług w chmurze z odpowiednimi nazwami i certyfikatami systemu nazw domen (DNS). Dane statystyczne zaledwie jednego sklepu w Darknecie to dowód na skuteczność tych ataków: umożliwiły one atakującemu lub grupie przejęcie około 65 000 kont miesięcznie [22].

_Trendy dotyczące incydentów

- Zauważono zmianę w skuteczności ataków z wyłudzaniem informacji wykorzystującym miejsce w chmurze, DocuSign i usługi chmurowe Microsoft.
- Ataki z podszywaniem się obejmują takie schematy, jak włamania do poczty służbowej (BEC) oraz techniki oszukiwania w sferze tożsamości, oparte na inżynierii społecznej, które sprawiają, że kampanie wyłudzania informacji stają się bardziej skuteczne.
- Wyłudzanie informacji z użyciem usług Microsoft 365 było najczęściej stosowane, lecz nadal obserwuje się nacisk na pozyskiwanie poświadczeń.
- Ponad 99% wiadomości e-mail rozpowszechniających złośliwe oprogramowanie wymagało interwencji człowieka – użycia łącza, otwarcia dokumentu, zaakceptowania ostrzeżenia o bezpieczeństwie, czy innych zachowań – aby jego działanie było skuteczne [44].

Najczęściej spotykane motywy związane z wyłudzaniem informacji w 2019 r.

- Ogólne pozyskiwanie poświadczeń z użyciem wiadomości e-mail
- Wyłudzanie informacji z użyciem kont Office 365
- Wyłudzanie informacji od instytucji finansowych
- Wyłudzanie informacji z użyciem aplikacji Microsoft OWA
- Wyłudzanie informacji z użyciem OneDrive
- Wyłudzanie informacji od użytkowników kart American Express
- Ogólne wyłudzanie informacji z użyciem zestawu ChalBhai
- Wyłudzanie informacji z użyciem konta Adobe
- Wyłudzanie informacji z użyciem Docusign
- Wyłudzanie informacji z użyciem serwisu Netflix
- Wyłudzanie informacji z użyciem konta Dropbox
- Wyłudzanie informacji z użyciem konta LinkedIn
- Wyłudzanie informacji z użyciem konta Apple
- Wyłudzanie informacji za pośrednictwem instytucji pocztowej/firmy kurierskiej
- Wyłudzanie informacji z użyciem dokumentów Microsoft online (Excel i Word)
- Wyłudzanie informacji z użyciem ustawień Windows
- Wyłudzanie informacji z użyciem usługi Google Drive
- Wyłudzanie informacji z użyciem serwisu PayPal

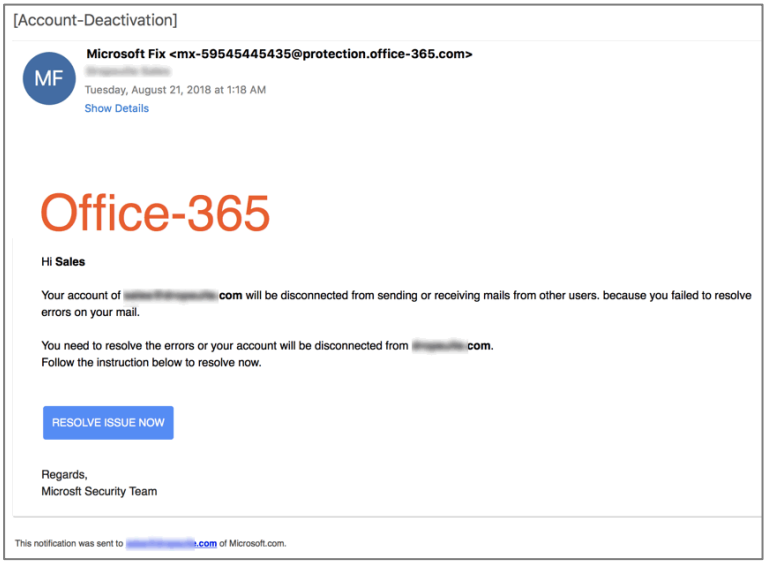
Źródło: Proof Point[32]

Trendy

COVID-19 używany jako przynęta przez wyłudzających informacje

Cyberprzestępcy wykorzystują strach społeczeństwa przed pandemią COVID-19, która po raz pierwszy pojawiła się pod koniec 2019 r. Doniesiono, że zaledwie w ciągu jednego miesiąca liczba ataków mających na celu wyłudzanie informacji, wykorzystujących istnienie wirusa, wzrosła o 667% (od końca lutego 2020 r. do końca marca 2020 r.), a schematy tylko tego rodzaju stanowiły aż 2% wszystkich oszustw z użyciem wyłudzania informacji[5].

Nowe oszustwa wykorzystujące e-maile mające na celu wyłudzanie informacji zaprojektowano tak, by wyglądały, jakby wysłano je z amerykańskiego Centrum Kontroli Chorób (CDC)[6], Światowej Organizacji Zdrowia[7] lub uniwersyteckich zespołów zajmujących się zagadnieniami zdrowotnymi[8]. Znajdowały się w nich nieprawdziwe stwierdzenia o wykrytych przypadkach zakażeń w miejscu zamieszkania ofiary lub opinie ekspertów medycznych, podane by nakłonić ofiarę do kliknięcia złośliwego łącza. Dlatego też FBI i WHO opublikowały ostrzeżenia[8,9]. Ponieważ podczas kwarantanny wiele osób pracowało zdalnie, często używając przestarzałych systemów zabezpieczeń[11], cyberprzestępcy próbowali wykorzystywać powstałe w ten sposób możliwości i luki w zabezpieczeniach[12].



Rysunek 2: Wiadomość e-mail z próbą wyłudzenia informacji z użyciem Office 365, źródło: Dropsuite[45]

Agencja ENISA w obliczu pandemii COVID-19

Wybuch pandemii COVID-19 wywołał ogromne zmiany w naszym stylu życia. W świecie, w którym coraz większa liczba osób łączy się przez sieć, na szczęście możemy nadal prowadzić życie zawodowe i prywatne w wirtualnej przestrzeni. W tym wyjątkowym okresie agencja ENISA udostępniła swoje zalecenia dotyczące bezpieczeństwa cybernetycznego[46] w różnych aspektach, w tym pracy zdalnej, zakupów online i e-zdrowia, a także udzielała poszkodowanym sektorom wartościowych i aktualnych porad na temat bezpieczeństwa. ENISA ocenia krajobraz zagrożeń w czasie pandemii i publikuje porady na temat zmniejszenia ryzyka związanego z najbardziej istotnymi zagrożeniami. Wiele uwagi poświęcamy wyłudzaniu informacji, gdyż liczba tego rodzaju ataków rośnie.

Rysunek 3: Zamieszczony w serwisie YouTube film agencji ENISA na temat COVID-19. Źródło: ENISA

Incydenty

Atakowane sektory

W 2019 r. celem licznych ataków mających na celu wyłudzenie informacji (lub profilowane wyłudzanie informacji) stał się sektor opieki zdrowotnej. Analityk bezpieczeństwa[42] uznał wyłudzanie informacji za główny wektor ataku w tym roku, z powodu wykorzystania taktyki opartej na inżynierii społecznej, polegającej na wysyłaniu wiadomości e-mail zarażonych złośliwym oprogramowaniem lub z łączami odsyłającymi do zarażonych witryn. Inne sektory, jak administracja rządowa i inne podmioty administracji publicznej, także stały się celem ataków mających na celu wyłudzanie informacji. Na przykład w listopadzie i grudniu 2019 r. kilku dyplomatów i dygnitarzy rządu ukraińskiego otrzymało wiadomości e-mail mające na celu profilowane wyłudzanie informacji, odsyłające do niebezpiecznych witryn[43].

Wektory ataku

Profilowane wyłudzanie informacji nadal pozostaje wyjątkowo popularną techniką uzyskiwania dostępu wstępnego wykorzystywaną przez sprawców szkodliwych działań. Stosują oni różnorodne taktyki inżynierii społecznej, by nakłaniać odbiorców do otwarcia załącznika lub odwiedzenia zarażonej witryny. Wiadomości mające na celu profilowane wyłudzanie informacji zawierają zwykle dokumenty Microsoft Office z obsługą makr lub łącze do takich dokumentów. Gdy użytkownik wybierze opcję „Włącz zawartość", osadzone makro zwykle rozpoczyna wykonywanie ciągu ukrytych skryptów, które ostatecznie prowadzą do pobrania złośliwego oprogramowania typu stage one lub dropper. JavaScript i PowerShell prawdopodobnie nadal pozostają najpopularniejszymi językami skryptowymi używanymi w tym celu.

Przykłady

_Atak mający na celu wyłudzanie informacji od studentów Uniwersytetu Lancaster doprowadził do wycieku danych osobowych[37]

_Hakerzy wyłudzili poświadczenia logowania od 2500 użytkowników aplikacji Discord[38]

_Dostawca internetowej usługi fitness padł ofiarą ataku mającego na celu wyłudzanie informacji[39]

_Pacjenci ucierpieli wskutek ataku z wyłudzaniem informacji od organizacji UConn Health[41]

_Filia producenta samochodów straciła 37 mln USD (ok. 31 mln EUR) z powodu oszustwa opartego na włamaniu do poczty służbowej (BEC)[33]

Ograniczenie ryzyka

Proponowane działania

- Szkolenie pracowników, by byli w stanie rozpoznawać fałszywe i złośliwe wiadomości i zachować czujność. Organizowanie symulowanych kampanii wyłudzania informacji, by przeprowadzić test infrastruktury organizacji, jak również reakcji pracowników.
- Rozważenie zastosowania zabezpieczającej bramki pocztowej z regularną (ewentualnie zautomatyzowaną) aktualizacją filtrów (antyspamowych, antywirusowych, filtrowania opartego na zasadach).
- Rozważenie zastosowania rozwiązań z dziedziny bezpieczeństwa wykorzystujących techniki uczenia maszynowego do identyfikacji w czasie rzeczywistym witryn wyłudzających dane.
- Wyłączenie automatycznego wykonywania kodu, makr, renderowania grafiki i automatycznego pobierania przesyłanych łączy na klientach poczty e-mail i ich regularna aktualizacja.
- Wprowadzenie jednego ze standardów zmniejszenia ilości spamu: SPF (Sender Policy Framework)[34], DMARC (Domain-based Message Authentication, Reporting & Conformance)[35] i DKIM (Domain Keys Identified Mail)[36].
- W idealnych warunkach – wykorzystywanie bezpiecznej poczty e-mail z użyciem sygnatur cyfrowych lub szyfrowania w przypadku transakcji finansowych lub wymieniania danych szczególnie chronionych.
- Wdrożenie wykrywania oszustw i anomalii na poziomie sieci, zarówno w przypadku poczty wychodzącej, jak i przychodzącej.
- Unikanie klikania przypadkowych łączy, szczególnie łączy skróconych stosowanych w serwisach społecznościowych.
- Unikanie klikania łączy lub pobierania załączników, jeśli użytkownik nie jest absolutnie pewien źródła wiadomości e-mail.

- Unikanie nadmiernego dzielenia się informacjami w mediach społecznościowych, np. o czasie pobytu poza biurem czy domem, informacjami o lotach itp., gdyż są one aktywnie wykorzystywane przez sprawców zagrożeń do gromadzenia informacji o celach.
- Sprawdzanie nazw domen odwiedzanych witryn pod kątem literówek, szczególnie witryn wrażliwych, jak witryny banków. Sprawcy zagrożeń zwykle rejestrują fałszywe domeny podobne do istniejących i używają ich do wyłudzania danych od ofiar. Samo sprawdzenie, czy mamy do czynienia z połączeniem HTTPS, nie wystarczy.
- Włączanie uwierzytelniania dwuskładnikowego zawsze, gdy jest to możliwe, co pozwoli zapobiec przejęciu konta.
- Używanie silnego i unikatowego hasła w każdej usłudze internetowej. Ponowne używanie tego samego hasła w różnych usługach to poważne naruszenie zasad bezpieczeństwa i należy go zawsze unikać. Używanie silnych i unikatowych poświadczeń w każdej usłudze internetowej ogranicza ryzyko potencjalnego przejęcia konta wyłącznie do tej jednej usługi. Używanie takiego oprogramowania, jak menedżer haseł, ułatwia zarządzanie całym zbiorem haseł.
- Podczas wykonywania przelewu należy zawsze dokładnie sprawdzić informacje o banku odbiorcy z użyciem innego medium. Nie należy ufać niezaszyfrowanym i niepodpisanym wiadomościom e-mail, zwłaszcza w przypadkach zastosowań szczególnie wrażliwych.
- Sprawdzanie, jak działają w naszej witrynie formularze do kontaktu, rejestracji, subskrypcji i przesyłania opinii i dodawanie w razie potrzeby reguł weryfikacji, by nie mogły zostać wykorzystane przez atakujących.

Bibliografia

1. „What Is Phishing?". Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. „Phishing Activity Trends Report Q1". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. „2018 Phishing Trends & Intelligence Report" 2018 r. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. „Microsoft remains phishers' #1 target for the fifth straight quarter", 22 sierpnia 2019 r. Vade Secure.
https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. „Threat Spotlight: Coronavirus-Related Phishing". 26 marca 2020 r. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6. „Coronavirus phishing emails: How to protect against COVID-19 scams", 2020 r. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. „Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer". 2020. IBM.
https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. „Abnormal Attack Stories #6: Coronavirus Credential Theft", 13 marca 2020 r.
https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. „FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic". 20 marca 2020 r. FBI.
https://www.ic3.gov/media/2020/200320.aspx

10. „Beware of criminals pretending to be WHO". 2020. WHO. https://www.who.int/about/communications/cyber-security

11. „Global police agencies issue alerts on Covid-related cyber-crime". 6 kwietnia 2020 r. SC Magazine.
https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. „Catching the virus cybercrime, disinformation and the COVID-19 pandemic". 3 kwietnia 2020 r. EUROPOL
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. „New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks". c 2019 r. FireEye.
https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. „HTTPS Protocol Now Used in 58% of Phishing Websites". 24 czerwca 2019 r. Trend Micro.
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. Let's Encrypt. https://letsencrypt.org/

16. „2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike".
23 stycznia 2020 r. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. „Human factor report". 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. „Phishing Activity Trends Report Q3". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. „Business Email Compromise Results in $26B in Losses Over the Last Three Years". 12 września 2019 r. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. „Business Email Compromise The $26 Billion Scam", 10 września 2019 r. FBI. https://www.ic3.gov/media/2019/190910.aspx

21. „Evasive Phishing Driven by Phishing-as-a-Service". 1 lipca 2019 r. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. „Phishing made easy: Time to rethink your prevention strategy?". 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. „Q3 2019: Email Fraud and Identity Deception Trends". 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. „FBI: BEC Losses Soared to $1.8 Billion in 2019". 12 lutego 2020 r. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. „Email: Click with Caution". Czerwiec 2019 r. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. „Experts report a rampant growth in the number of malicious, lookalike domains". 18 listopada 2019 r. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. „Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more". 7 listopada 2019 r. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. „Human Factor Report." 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. „2019 Phishing and fraud report", 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. „Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019", 8 maja 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. „Spam and phishing in Q3 2019". 26 listopada 2019 r. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. „Phishing Activity Trends Report". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. „Toyota Subsidiary Loses $37 Million Due to BEC Scam", 20 września 2019 r. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. „Domain-based Message Authentication, Reporting & Conformance". DMARC. https://dmarc.org/

Bibliografia

36. „DomainKeys Identified Mail (DKIM)". DKIM. http://www.dkim.org/

37. „Cyber incident". 22 lipca 2019 r. Uniwersytet Lancaster. https://www.lancaster.ac.uk/news/phishing-attack

38. „Hackers publish login credentials of 2500 Discord users" 22 lipca 2019 r. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. „Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People", 24 kwietnia 2019 r. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. „Phishing Attack Exposes 600k Health Records", 19 czerwca 2019 r. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. „326,000 Patients Impacted in UConn Health Phishing Attack". 25 lutego 2019 r. Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

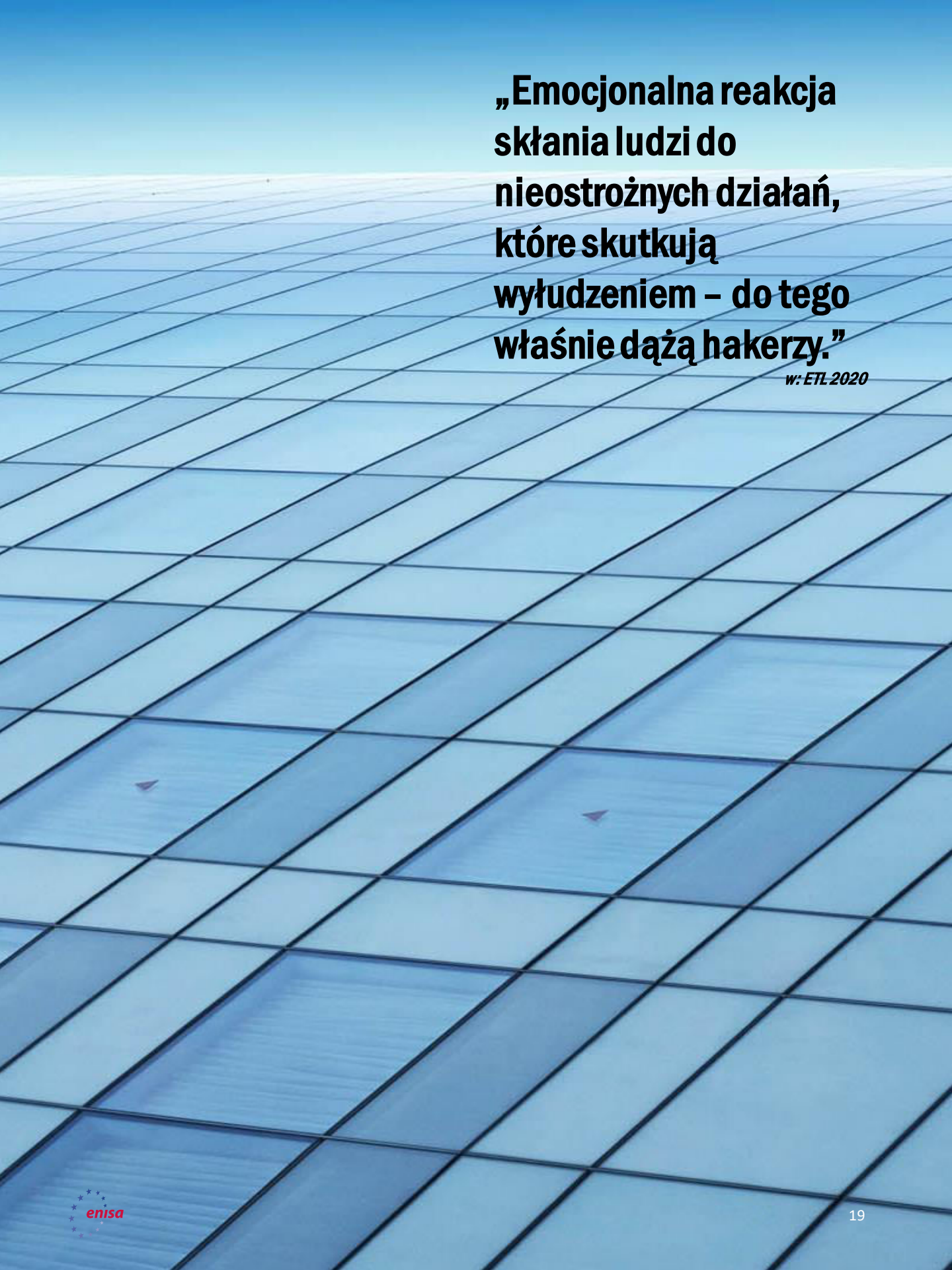
42. „Cybercrime Tactics and Techniques: the 2019 state of healthcare". 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. „Significant Cyber Incidents". 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. „More Than 99% of Cyberattacks Need Victims' Help". 9 września 2019 r. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

45. „office-365-phishing-attacks-deconstructed" https://dropsuite.com/office-365-phishing-attacks-deconstructed/

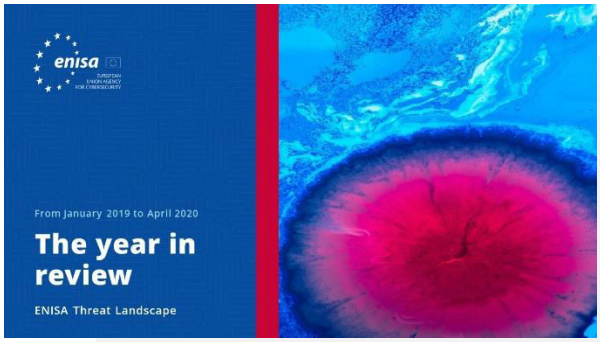
46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19



„Emocjonalna reakcja skłania ludzi do nieostrożnych działań, które skutkują wyłudzeniem – do tego właśnie dążą hakerzy."

w: ETL 2020

Powiązany



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

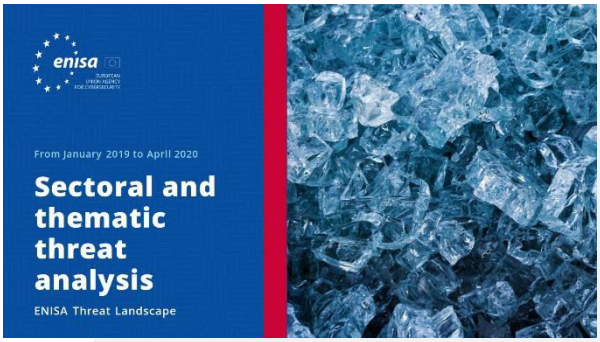
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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



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