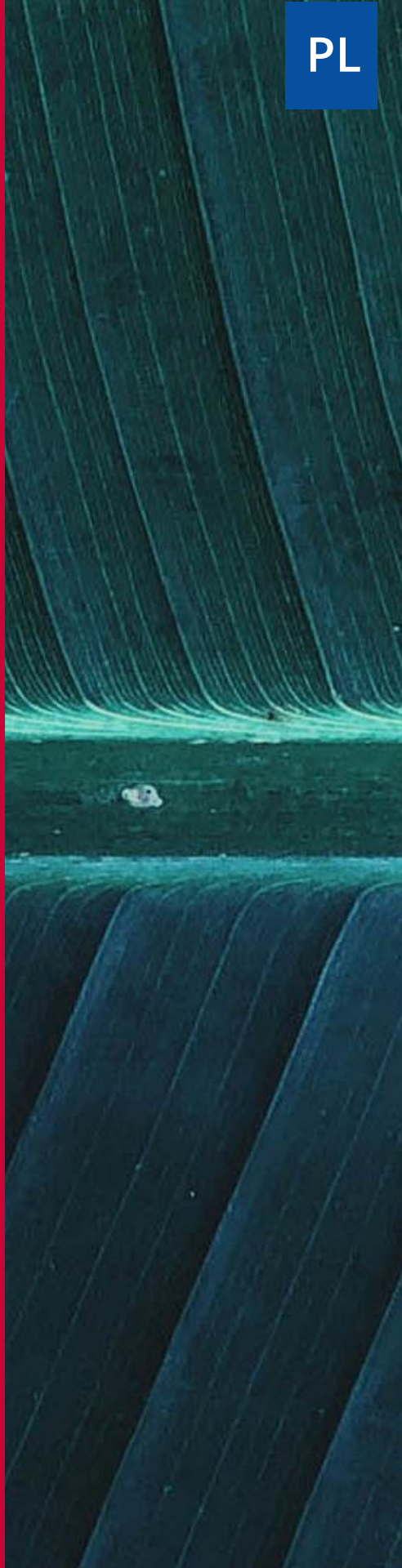
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL



Od stycznia 2019 r. do kwietnia 2020 r.

Spam

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

Informacje ogólne

Pierwsza wiadomość o charakterze spamu została wysłana w 1978 roku przez menedżera ds. marketingu do 393 osób za pośrednictwem sieci ARPANET. Była to kampania reklamowa nowego produktu firmy, dla której pracował, Digital Equipment Corporation. Mimo nowości pomysłu, dla owych pierwszych 393 spamowanych osób było to tak samo denerwujące, jak byłoby dzisiaj[1]. Otrzymywanie spamu jest niedogodnością, ale może też stwarzać sprawcy szkodliwych działań możliwość kradzieży danych osobowych lub zainstalowania złośliwego oprogramowania[2]. Spam polega na masowym wysyłaniu niechcianych wiadomości. Jest uważany za zagrożenie dla bezpieczeństwa cybernetycznego, gdy jest używany jako wektor ataku do dystrybucji lub umożliwiania innych zagrożeń.

Innym godnym uwagi aspektem jest to, że spam może być czasami mylony lub błędnie klasyfikowany jako kampania phishingowa. Główna różnica między nimi polega na tym, że phishing to wykorzystujące taktyki socjotechniczne ukierunkowane działanie, którego celem jest kradzież danych użytkowników. Spam natomiast to taktyka wysyłania niechcianych wiadomości e-mail na adresy ze zbiorczej listy. Kampanie phishingowe mogą wykorzystywać taktyki spamowe do dystrybucji wiadomości, podczas gdy spam może łączyć użytkownika z zaatakowaną witryną w celu zainstalowania złośliwego oprogramowania i kradzieży danych osobowych.

Kampanie spamowe w ciągu ostatnich 41 lat wykorzystywały wiele popularnych światowych wydarzeń społecznych i sportowych, takich jak między innymi finał Ligi Europy UEFA czy US Open. To jednak nic w porównaniu z aktywnością spamową obserwowaną w tym roku podczas pandemii COVID-19[8].

_Wnioski

85%_ **wszystkich wiadomości e-mail przesłanych w kwietniu 2019 r. było spamem, najwięcej od 15 miesięcy[1]**

14_ **milionów wiadomości spam związanych z wymuszeniami o charakterze seksualnym wykryto w 2019 roku[23]**

58,3%_ **kont e-mail w branży wydobywczej było adresatami spamu[17]**

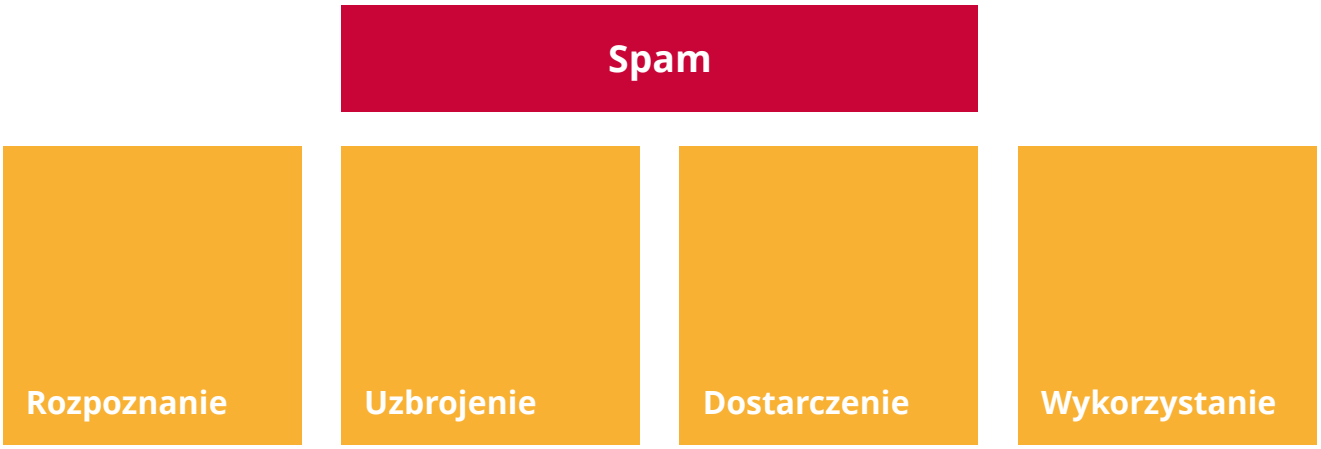
10%_ **wszystkich wykrytych przypadków spamu dotyczyło niemieckich kont e-mail[23]**

13%_ **przypadków naruszenia bezpieczeństwa danych było spowodowanych przez złośliwy spam[16]**

83%_ **firm nie było chronionych przed podszywaniem się pod markę za pośrednictwem poczty e-mail[20]**

42%_ **dyrektorów ds. bezpieczeństwa informacji (CISO) miało do czynienia z co najmniej jednym incydentem związanym ze spamem[1]**

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

Opis

Nowa odsłona starej taktyki

Po 41 latach istnienia spam pozostaje znaczącym zagrożeniem dla bezpieczeństwa, mimo istnienia innych, znacznie groźniejszych. Jednak po raz kolejny w omawianym okresie w kampaniach spamerskich pojawiły się nowe grupy docelowe, nowe sposoby i nowe łupy. Na przykład w sierpniu 2019 r. wiadomości e-mail będące spamem zachęcały właścicieli wielu kont do udostępnienia nie tylko skanu dowodu tożsamości, ale także selfie, kusząc możliwością „wygrania" darmowego smartfona. W innej kampanii spamowej użytkownicy zostali poproszeni o przesłanie własnego zdjęcia. Grupa docelowa spamerów została następnie rozszerzona o adres e-mail użytkownika do aktywacji płatnej telewizji lub usług transmisji na żywo. Na te konta wysyłano spam z fałszywymi wiadomościami o wygaśnięciu lub odnowieniu licencji. Użytkownicy zostali poproszeni o podanie w odpowiedzi danych swojego rachunku bankowego oraz danych osobowych w celu odnowienia rejestracji[2].

Spamowanie w celu dystrybucji złośliwego oprogramowania, oprogramowania typu ransomware i trojanów zdalnego dostępu

W sierpniu 2019 r. spam zawierający złośliwe pliki obrazów ISO wykorzystano do dystrybucji złośliwego oprogramowania LokiBot oraz trojana zdalnego dostępu (RAT) FlawedAmmyy. Spam był również wykorzystywany do dystrybucji trojana TrickBot, szpiegowskiego trojana Negasteal (znanego też jako Agent Tesla), RAT Ave Maria (znanego też jako Warzone) i słynnego od 2018 roku złośliwego makra Pawload. Również różne rodziny oprogramowania typu ransomware były dystrybuowane przez spam, np. wysoce aktywne w opisywanym roku Dharma, Crysis czy Ryuk[15,21].

Spam SMS

W tym roku przeprowadzona została operacja spamu SMS, w wyniku której ujawnione zostały dane osobowe ponad 80 milionów użytkowników. Na wiele numerów telefonów trafiły wiadomości zawierające określone wyrażenia, takie jak „zgarnij pieniądze” lub „serio, serio!”, oraz linki do fałszywych witryn. Każdy, kto skorzystał z hiperłącza, był proszony o zarejestrowanie się, ujawniając dane wrażliwe.Dowiedziono, że baza danych wykorzystywana przez spamerów była własnością firmy ApexSMS, której legalność jest wciąż nieznana. Choć analitycy bezpieczeństwa uzyskali dostęp do bazy danych i próbowali wydobyć jak najwięcej informacji, obawiając się, że operacja zostanie nieoczekiwanie przerwana, nadal nie wiadomo, kto i w jakim celu może mieć dostęp do tych danych i z nich korzystać, a są one wciąż dostępne[4].

Wszystko przez formularze

Spamerzy manipulowali formularzami opinii zwrotnej w witrynach internetowych dużych firm używanych do zadawania pytań, wyrażania życzeń lub subskrybowania biuletynów. Jednak w opisywanym roku zamiast spamować powiązane skrzynki pocztowe firmy, spamerzy wykorzystali niski poziom bezpieczeństwa witryn, obeszli wszelkie testy reCAPTCHA i zarejestrowali wiele kont z prawidłowymi informacjami e-mail. W rezultacie ofiary otrzymały wiarygodną odpowiedź od firmy, zawierającą wiadomość od spamera[2]. W ten sposób zmanipulowane zostały nawet Formularze Google, aby pobierać dane użytkownika i wysyłać komercyjny spam. Bardziej agresywnym przypadkiem był wymierzony w konta firmowe atak spamowy z żądaniem przesłania pieniędzy atakującemu. Aby przekonać ofiarę, spamerzy twierdzili, że są w stanie wysyłać obraźliwe wiadomości z adresu ofiary na ponad 9 milionów adresów e-mail, powodując umieszczenie adresu e-mail firmy na czarnej liście[3].

Opis

_Spam-kameleon

Różne kampanie w 2019 roku wykorzystywały do dystrybucji spamu ten sam system botnetów, choć do formatowania treści używały losowych nagłówków i szablonów. Dlatego analitycy bezpieczeństwa zaczęli badać te kampanie jako jedną grupę pod nazwą „spam-kameleon”[5].

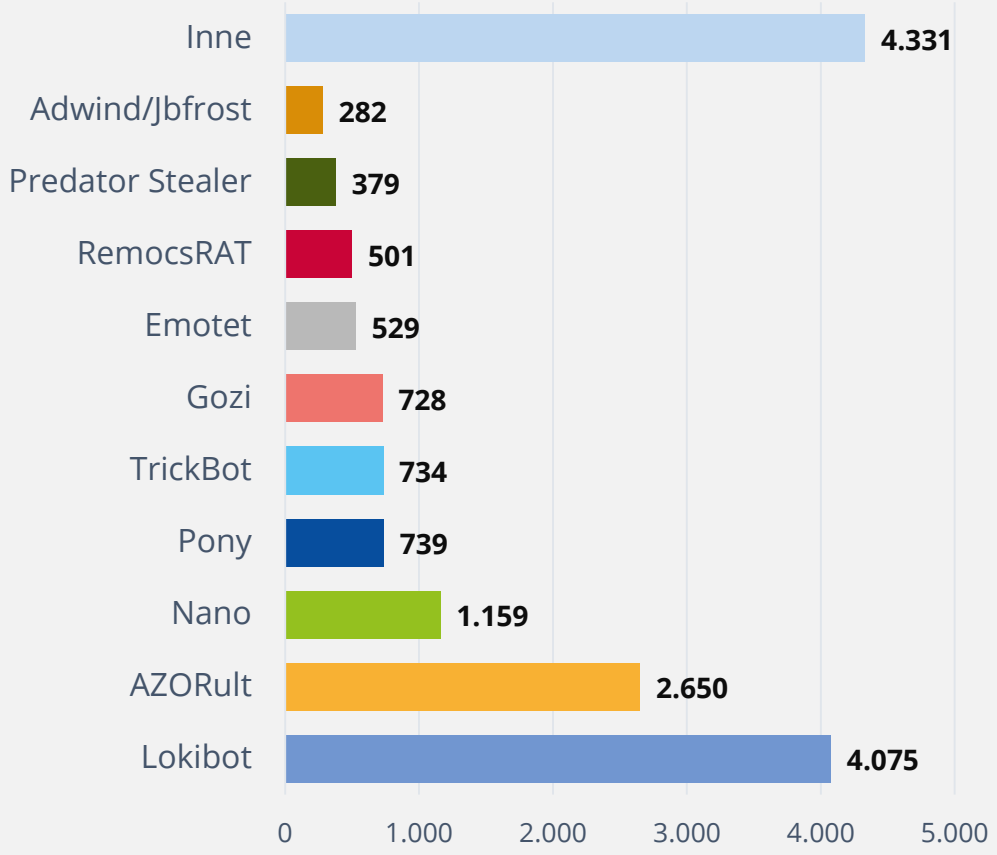
Wiadomości spamu-kameleona pochodziły z różnych krajów i zawierały fałszywe hiperłącza do fałszywych ofert pracy, serwisów rezerwacji biletów lotniczych, specjalnych ofert zakupu produktów, a nawet prostych, dobrze znanych usług. Wiadomości te wykorzystywały szablon podobny do używanego przez prawdziwe firmy, takie jak Google, Qatar Airways, FedEx, LinkedIn czy Microsoft, aby odbiorca nie zauważył różnicy[2].

_Stare boty górą

W październiku 2019 r. pocztę e-mail zalały wiadomości wykorzystujące szablony w językach angielskim, niemieckim, włoskim i polskim o wspólnym temacie „Informacja dotycząca płatności”. W załączniku do tych wiadomości znajdował się dokument zawierający makro, a odbiorcy byli proszeni o włączenie go podczas otwierania dokumentu. Po włączeniu makro mogło rozpocząć proces infekcji, próbując pobrać trojana Emotet[13].

Botnet spamowy Necurs[7] był w tym okresie bardzo aktywny po długim czasie niemal całkowitego uśpienia. Trzecim pod względem aktywności w 2019 roku botnetem spamowym był Gamut. Wiadomości rozsyłane przez Gamut dotyczą głównie propozycji randek lub zawierania znajomości, ofert produktów leczniczych i ofert pracy[1].

Liczba botnetów C2 powiązanych z rodzinami złośliwego oprogramowania

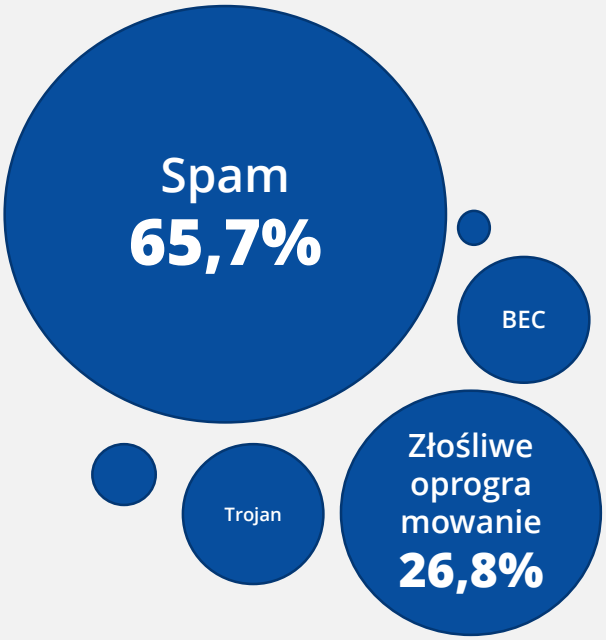


Rysunek 1 – źródło: Spamhaus [14]

Opis

_ COVID-19 otworzył nowe drzwi

Wkrótce po rozpoczęciu epidemii COVID-19 pojawiły się witryny phishingowe i złośliwe pliki dostarczane pocztą elektroniczną, posługujące się terminami koronawirus lub COVID-19. Wykryto, że kampania spamerska COVID-19 rozpowszechnia ukryty keylogger Eeskiri-COVID.chm19. Nazwa pliku może sugerować, że kampania pochodzi z Estonii (eeskiri w języku estońskim oznacza „rządzić")[11]. W połowie lutego 2020 r. odnotowano dziennie tylko kilkaset ataków związanych z COVID-19, ale do marca 2020 r. każdego dnia miało miejsce ponad 2500 ataków, co pod względem spamu zapowiadało trudny rok[12].



Rysunek 2: Zagrożenia związane z COVID-19. Źródło: Trend Micro[11]

_ Przykłady

01_ Operacja spamowa ApexSMS

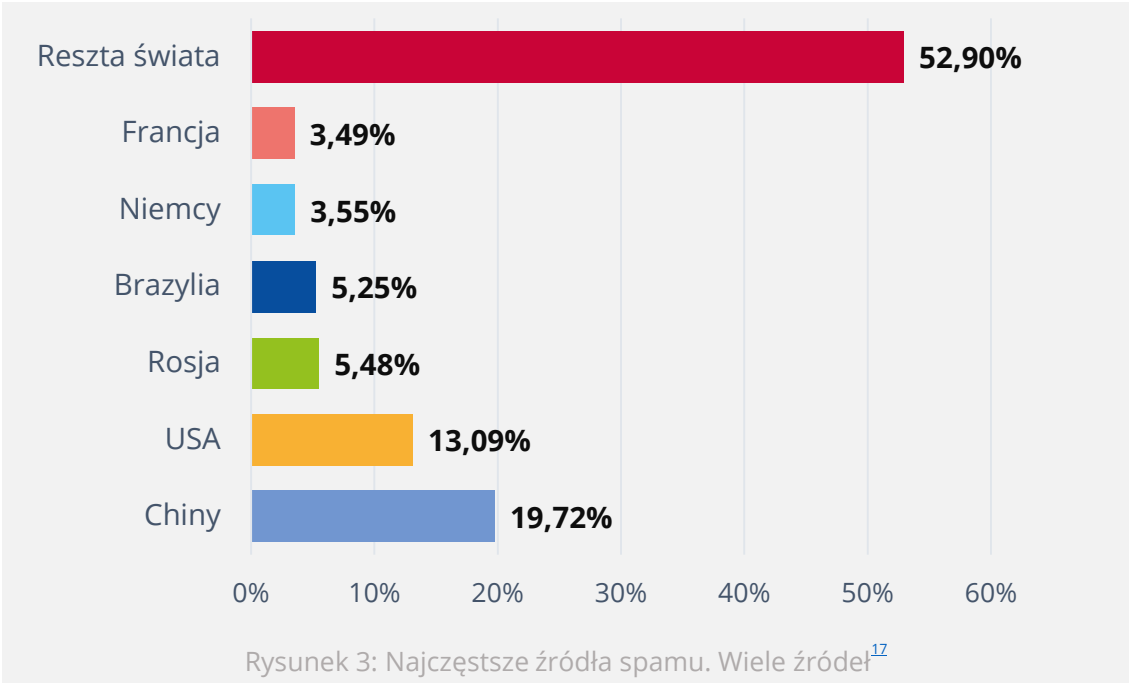
ApexSMS, firma zajmująca się marketingiem SMS-owym, doznała naruszenia bezpieczeństwa danych, przez co ujawnieniu uległy dane kontaktowe ponad 80 milionów osób.

02_ Kampania spamu-kameleona

Długotrwała, masowa kampania spamu pochodzącego z systemu botnetów wysyłającego wiadomości o losowych nagłówkach i często zmienianym szablonie.

03_ Kampania dystrybucji Emotet za pomocą spamu

Kampania spamowa wspierająca dystrybucję szkodliwego złośliwego oprogramowania Emotet.

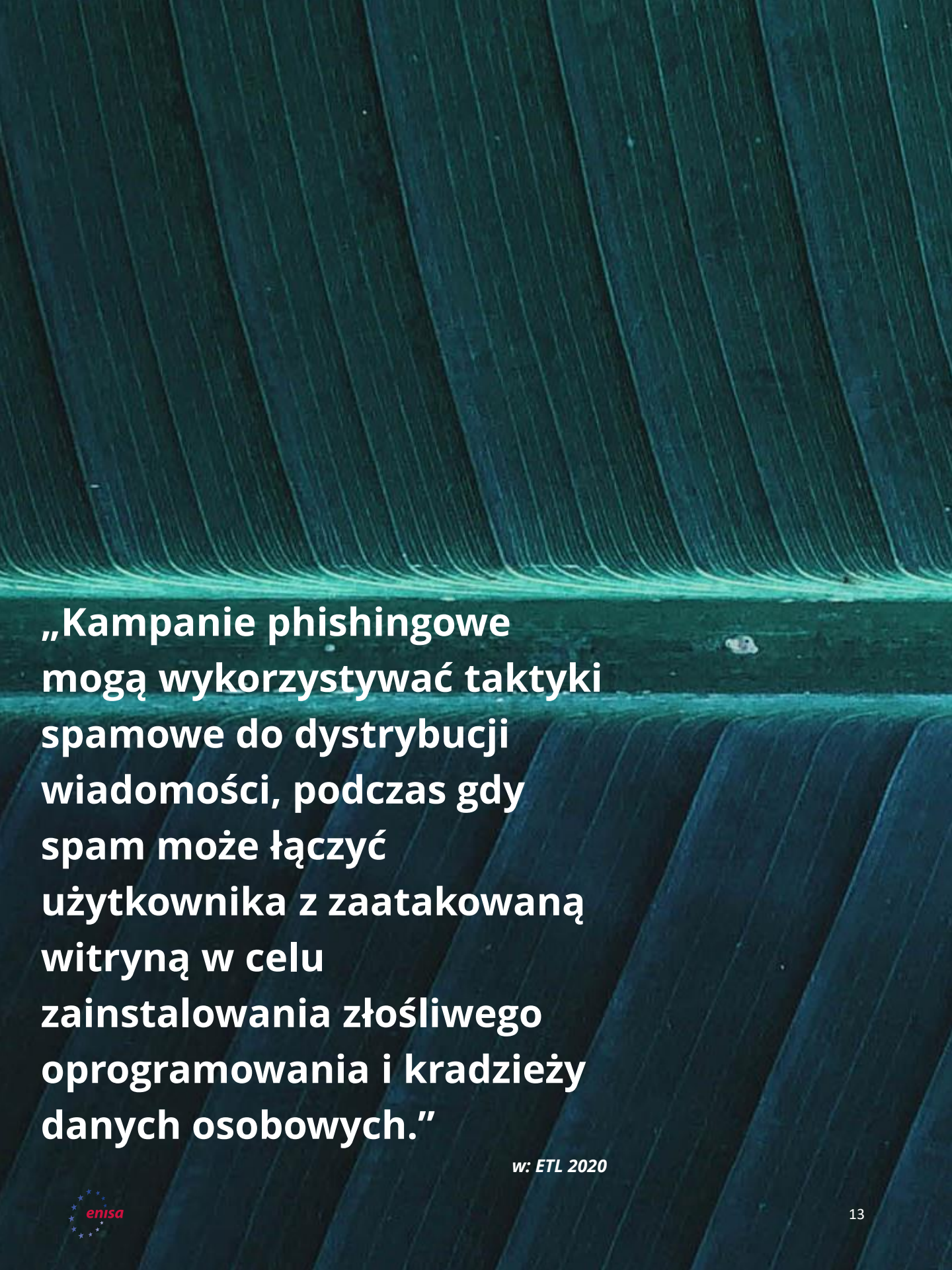


Rysunek 3: Najczęstsze źródła spamu. Wiele źródeł[17]

Ograniczenie ryzyka

Proponowane działania

- Wdrożenie filtrowania treści, by zlokalizować niechciane załączniki, wiadomości e-mail ze złośliwą zawartością, spam i niechciany ruch sieciowy.
- Regularna aktualizacja sprzętu, oprogramowania układowego, systemu operacyjnego oraz sterowników i oprogramowania.
- Używanie uwierzytelniania wieloskładnikowego przy dostępie do kont e-mail.
- Unikanie przelewów na niezweryfikowane rachunki bankowe.
- Unikanie logowania się do nowych serwisów o adresach otrzymywanych w wiadomościach e-mail lub SMS.
- Opracowanie standardowych procedur operacyjnych (SOP) i zasad postępowania z danymi wrażliwymi.
- Używanie bezpiecznej bramy poczty e-mail, jeśli to możliwe, z regularną i zautomatyzowaną aktualizacją filtrów (antyspamowe, chroniące przed złośliwym oprogramowaniem, filtrowanie oparte na zasadach).
- Wyłączenie automatycznego wykonywania kodu, włączania makr i wstępnego wczytywania grafiki i hiperłączy zawartych w poczcie.
- Wdrożenie technik bezpieczeństwa takich jak SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting & Conformance) oraz DKIM (Domain Keys Identified Mail).
- Regularna aktualizacja białych list, filtrów reputacji i RBL (Real-time Blackhole List).
- Używanie mechanizmów sztucznej inteligencji i uczenia maszynowego do wykrywania anomalii.



„Kampanie phishingowe mogą wykorzystywać taktyki spamowe do dystrybucji wiadomości, podczas gdy spam może łączyć użytkownika z zaatakowaną witryną w celu zainstalowania złośliwego oprogramowania i kradzieży danych osobowych.”

w: ETL 2020

Bibliografia

1. „Email: Click with Caution - How to protect against phishing, fraud, and other scams", Czerwiec 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

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

3. „Spam and phishing in Q2 2019", 28 sierpnia 2019 r. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. „SMS Spammers Doxxed", 9 maja 2019 r. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. „Tracking the Chameleon Spam Campaign", 25 września 2019 r. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. „5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned", 7 czerwca 2019 r. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. „The world worst spammers". 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. „Naming the coronavirus disease (COVID-19) and the virus that causes it". 2020. WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. „WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus", 6 lutego 2020 r. WHO. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. „COVID-19 situation update worldwide, as of 11 June 2020", 2020 r. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. „Developing Story: COVID-19 Used in Malicious Campaigns", 24 kwietnia 2020 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. „2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape", 6 kwietnia 2020 r. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. „Emotet is back: botnet springs back to life with new spam campaign", 16 września 2019 r. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. „Spamhaus Botnet Threat Report 2019", 28 stycznia 2020 r. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. „Evasive Threats, Pervasive Effects", 27 sierpnia 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

16. „Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study", 28 lutego 2019 r. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. „Internet Security Threat Report" Volume 24, luty 2019 r. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. „Spam and phishing in Q1 2019", 5 maja 2019 r. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. „Total Global Email & Spam Volume for May 2020", maj 2019 r. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

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

21. „The World's Most Abused TLDs" Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. „Trend Micro Cloud App Security Report 2019", 10 marca 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. „The Sprawling Reach of Complex Threats". 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. „SONIC WALL Security Center Metrics". SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

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

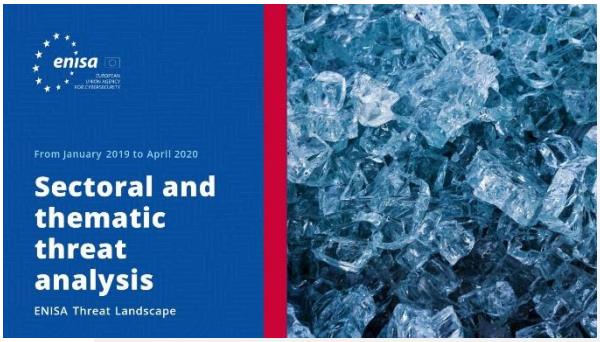
Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

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.



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.

PRZECZYTAJ RAPORT

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

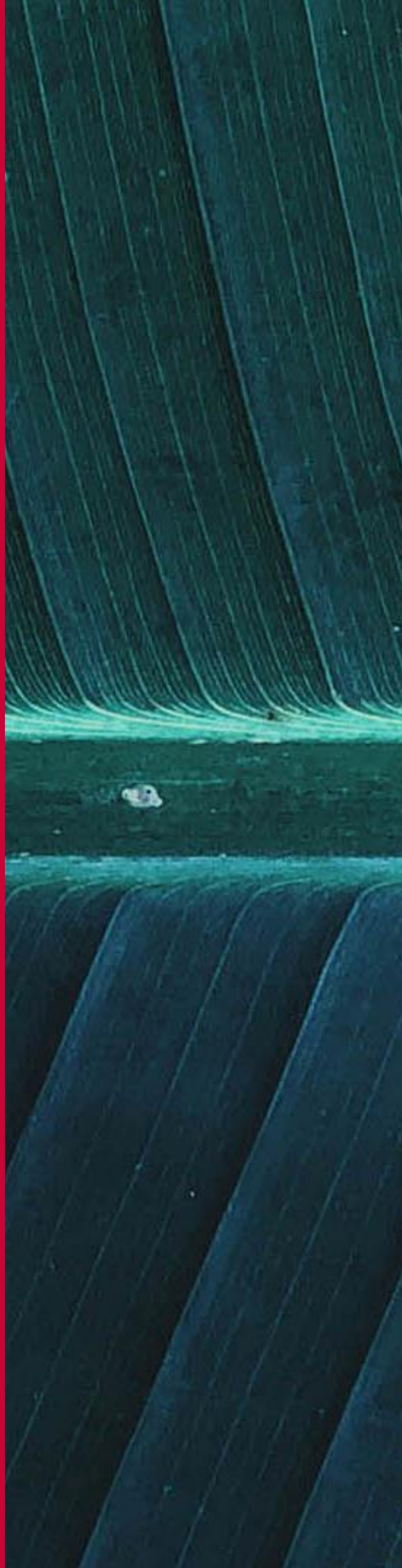
Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja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