enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

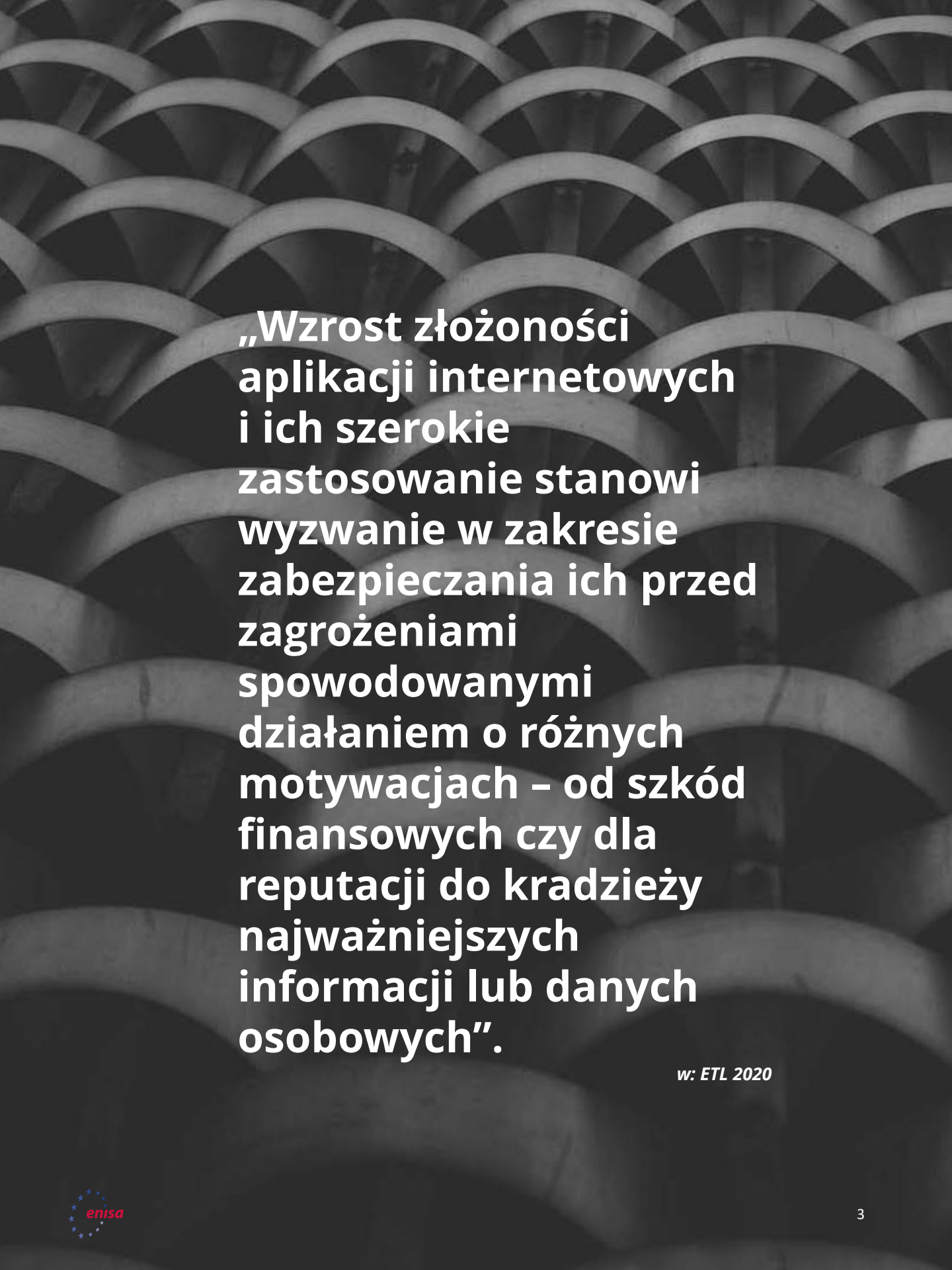
Ataki przez strony internetowe

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

Informacje ogólne

Ataki przez strony internetowe to dla sprawców szkodliwych działań atrakcyjna metoda, za pomocą której mogą oni zwodzić ofiary przy użyciu systemów i usług online jako wektora ataku. Obejmuje to ogromną powierzchnię ataku, na przykład tworzenie szkodliwych adresów URL lub złośliwych skryptów mających na celu przekierowanie użytkownika lub ofiary do pożądanej witryny internetowej lub pobranie przez niego złośliwej zawartości (tzw. ataki u wodopoju[1], ataki typu drive-by związane z pobraniem niechcianego pliku[2]) oraz wstrzykiwanie złośliwego kodu do prawdziwej, lecz mającej złamane zabezpieczenia witryny internetowej celem kradzieży danych (tj. formjacking[3]), aby osiągnąć zyski finansowe, wykraść informacje lub nawet wymusić okup poprzez oprogramowanie typu ransomware[4]. Oprócz wymienionych ważnymi wektorami wykorzystywanymi przez sprawców szkodliwych działań i odnotowanymi przez różne zespoły badawcze są exploity w przeglądarkach internetowych oraz złamane zabezpieczenia w systemach zarządzania zawartością (content management system, CMS).

Ataki siłowe typu brute force polegają na przeciążeniu aplikacji internetowej próbami logowania przy użyciu nazwy użytkownika i hasła. Ataki przez strony internetowe mogą wpłynąć na dostępność witryn, aplikacji i interfejsów programowania aplikacji (API) przy jednoczesnym naruszeniu poufności i integralności danych.



„Wzrost złożoności aplikacji internetowych i ich szerokie zastosowanie stanowi wyzwanie w zakresie zabezpieczania ich przed zagrożeniami spowodowanymi działaniem o różnych motywacjach – od szkód finansowych czy dla reputacji do kradzieży najważniejszych informacji lub danych osobowych”.

w: ETL 2020

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

Trendy

Powszechność

- **ZŁOŚLIWE OPROGRAMOWANIE Z FUNKCJĄ FORMJACKINGU KRADNIE DANE UŻYTKOWNIKÓW**. Wstrzykiwanie złośliwego kodu do witryn internetowych to dobrze znana technika wykorzystywana przez cyberprzestępców. Formjacking kiedyś notowano przede wszystkim w działalności związanej z wydobywaniem kryptowalut. Jednak, jak twierdzi analityk bezpieczeństwa[4], sprawcy szkodliwych działań przechodzą do stosowania tej techniki celem uzyskania danych użytkowników i szczegółów kont bankowych. Witryny będące celem ataku pozostawały zarażone średnio przez 45 dni. W maju 2019 r. analityk bezpieczeństwa odnotował zablokowanie niemal 63 milionów szkodliwych zapytań sieciowych związanych z formjackingiem.
- **„MAGECART" IDZIE DALEJ, ATAKUJĄC ŁAŃCUCH DOSTAW**. Według analityka bezpieczeństwa jedna z francuskich firm z branży mediów cyfrowych padła ofiarą szkodliwych działań tzw. Group12, zespołu, który zainfekował bazę danych reklam witryny internetowej, dostarczając kod do kopiowania danych i infekując tysiące stron, które wyświetlały dane ogłoszenie[5]. Odnotowano, że skuteczność działań tej grupy była jeszcze większa dzięki temu, że infrastrukturę do kopiowania danych przygotowano zaledwie na kilka miesięcy przed rozpoczęciem kampanii. Tym samym użytkownik końcowy mógł zostać zainfekowany tylko przez to, że wszedł na stronę, na której wyświetlana była taka reklama[6].
- **WSPÓŁPRACA OPARTA NA SIECI I KOMUNIKATORY INTERNETOWE**. Narzędzia te stają się pomostem pomiędzy sprawcami szkodliwych działań a ofiarami poprzez tak zwane tylne wejście SLUB. W marcu 2019 r. analityk bezpieczeństwa napotkał na kampanię, w której do infekowania ofiar techniką „u wodopoju" była wykorzystywana podatność CVE-2018-81747. Atak obejmował wieloetapowe schematy infekcji. Jednym z przykładów działania takich schematów jest pobranie pliku .dll, wykonanie go przy użyciu oprogramowania PowerShell, pobranie złośliwego oprogramowania oraz uruchomienie głównego „tylnego wejścia" (backdoor). Co ciekawe, złośliwe oprogramowanie łączyło się z wykorzystywanym do pracy komunikatorem Slack celem wysyłania wyników wykonania poleceń, które były dostarczane za pośrednictwem fragmentu kodu Gist na GitHub, w którym atakujący potencjalnie mógł dodawać polecenia[7,8].

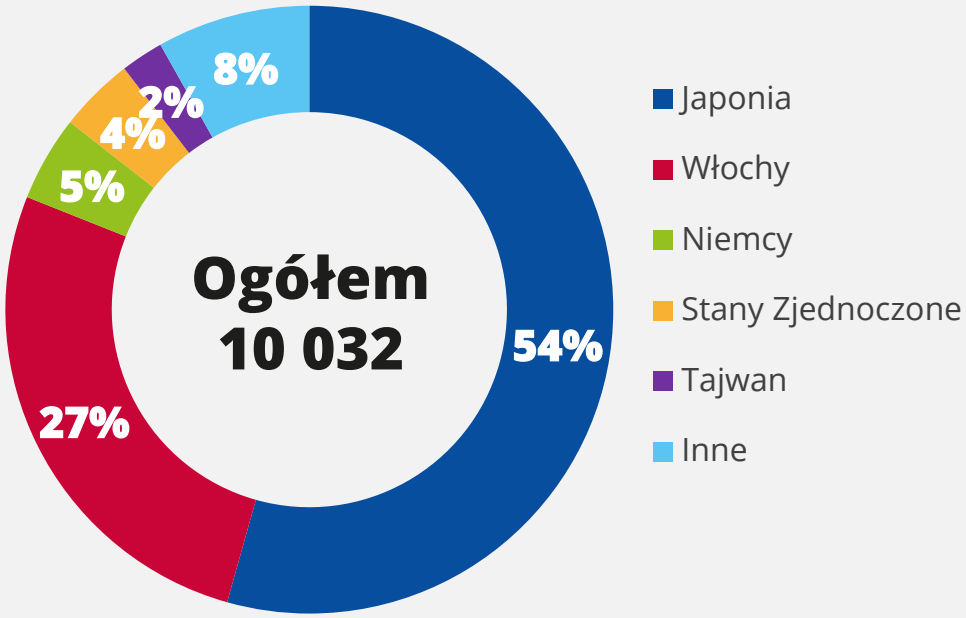
- **ROZSZERZENIA PRZEGLĄDAREK, OSZUSTWA I ZŁOŚLIWE REKLAMY**. Analityk bezpieczeństwa odkrył szeroko zakrojoną złośliwą kampanię reklamową wykorzystującą rozszerzenia do przeglądarki Google Chrome, która dotknęła około 1,7 mln użytkowników.Te rozszerzenia do Chrome maskowały przed użytkownikami końcowymi prawdziwą funkcję reklam polegającą na utrzymywaniu połączenia zainfekowanej przeglądarki z infrastrukturą C2. Analityk doszedł do wniosku, że aktywność kampanii wzrosła pomiędzy marcem a czerwcem 2019 r., aczkolwiek podejrzewa się, że kampania działała dużo wcześniej[9]. Inny analityk bezpieczeństwa odnotował pod koniec 2019 r. wzrost aktywności oprogramowania z reklamami NewTab, które ułatwia instalowanie rozszerzeń do przeglądarek[11].
- **WITRYNY GOOGLE WYKORZYSTANE DO HOSTOWANIA OPROGRAMOWANIA DO ATAKÓW TYPU DRIVE-BY**. Złośliwe oprogramowanie o nazwie „LoadPCBanker" (Win32.LoadPCBanker.Gen) odkryto w szablonie katalogów plików Witryn Google (wersja klasyczna – Classic Google Sites). Jak twierdzi analityk bezpieczeństwa, sprawca najpierw użył wersji klasycznej Witryn Google do stworzenia strony internetowej, a następnie wykorzystał szablon katalogów plików do hostowania złośliwego oprogramowania. Następnie jako kanału przesyłania i przechowywania danych ofiar użył usługi SQL[12,13].
- **ZŁOŚLIWE OPROGRAMOWANIE WYKORZYSTUJĄCE INTERNETOWY KONWERTER PLIKÓW WIDEO JAKO MECHANIZM POBIERANIA NIECHCIANYCH PLIKÓW W ATAKU TYPY DRIVE-BY**. Według analityka bezpieczeństwa od 2015 r. aktywne było oprogramowanie ShadowGate, czy też WordJScampaign, którego celem było oprogramowanie do wyświetlania reklam i reklamowe witryny internetowe. W roku 2016 stworzono pakiet exploitów Greenflash Sundown celem zintensyfikowania kampanii poprzez wstrzykiwanie pakietu do serwisów reklamowych o złamanych zabezpieczeniach i rozprzestrzenianie oprogramowania typu ransomware. W 2018 r. zaobserwowano, jak oprogramowanie ShadowGate przez krótki czas dostarczało programy wydobywające kryptowalutę na serwery w Azji Wschodniej. Dystrybucję ShadowGate w poszczególnych krajach przedstawiono na Rysunku 1.Inny analityk bezpieczeństwa także odnotował aktywność, której ślady prowadziły do onlinevideoconverter[.com], jednej z głównych witryn internetowych dostarczających zestaw exploitów[14,15,16,17,18].

Trendy

Powszechność

- **SYSTEMY ZARZĄDZANIA ZAWARTOŚCIĄ NADAL IDEALNYM CELEM ATAKU**. Popularność systemów zarządzania zawartością (CMS) wśród użytkowników internetu czyni te systemy atrakcyjnym celem dla sprawców szkodliwych działań. Analityk bezpieczeństwa wskazał wzrost liczby przypadków wykorzystania podatności znalezionej w 2018 r. (Drupalgeddon2) ukierunkowanej na platformę Drupal. Inny analityk bezpieczeństwa zaobserwował podobny trend wykorzystywania podatności w oprogramowaniu WordPress ukierunkowanego na luki bezpieczeństwa i przestarzałe wtyczki zewnętrzne[19,20].

- **EXPLOITY W PRZEGLĄDARKACH INTERNETOWYCH WYKORZYSTYWANE W ATAKACH „U WODOPOJU”**. Zaobserwowano sprawcę szkodliwych działań przeprowadzającego atak typu „u wodopoju” z wykorzystaniem portalu z wiadomościami w języku koreańskim. W tym ataku złośliwy skrypt (w języku JavaScript) został wstrzyknięty do strony głównej witryny w sposób automatyczny (z wykorzystaniem innego skryptu) poprzez sprawdzanie przeglądarki ofiary, a następnie wykorzystywana była podatność CVE-2019-13720 w przeglądarce Google Chrome. Ponadto w lipcu 2019 r. odkryto przypadki infekowania przeglądarki ofiary nową wersją złośliwego oprogramowania o charakterze tylnego wejścia SLUB (podatność CVE-2019-0752 w przeglądarce Internet Explorer) przy użyciu specjalnej witryny internetowej i techniki ataku „u wodopoju”. W innym śledztwie zespół ds. bezpieczeństwa w firmie produkującej oprogramowanie zidentyfikował zbiór zainfekowanych witryn internetowych używanych w atakach „u wodopoju” z wykorzystaniem podatności w telefonach iPhone[21,22].



Rysunek 1: Procentowy rozkład oprogramowania ShadowGate w różnych krajach

Wektory ataku

Jak

- **POBIERANIE NIECHCIANYCH PLIKÓW (ATAKI TYPU DRIVE-BY)**. Ten wektor ataku polega na tym, że szkodliwa zawartość jest pobierana na urządzenie ofiary. Przy tego rodzaju ataku użytkownik końcowy odwiedza legalną witrynę internetową, której zabezpieczenia zostały złamane. Można to osiągnąć poprzez wstrzykiwanie złośliwych skryptów do witryny, uruchomienie exploitów przeglądarkowych lub przekierowanie użytkownika do zainfekowanej strony bez jego wiedzy[25,26].
- **ATAKI „U WODOPOJU"**. Technikę tę wykorzystuje się do ataków celowanych przy użyciu zestawów exploitów z funkcjami ukrywania. Innymi słowy, jest to rodzaj ataku wykorzystywany, gdy sprawca szkodliwych działań jest zainteresowany zainfekowaniem konkretnej grupy użytkowników przy wykorzystaniu exploitów lub innej szkodliwej zawartości (np. skryptów lub reklam) wstrzykiwanych do witryny internetowej[27].
- **FORMJACKING**. Ta technika polega na wstrzykiwaniu złośliwego kodu do legalnych formularzy płatności w witrynie internetowej. Przy tego rodzaju ataku przechwytywane są w większości dane bankowe oraz inne dane osobowe umożliwiające identyfikację (personal identifiable information, PII). W takim scenariuszu użytkownik wprowadza dane logowania do banku lub dane karty w portalu płatności e-sklepu. Po wprowadzeniu i przesłaniu danych złośliwy skrypt przekazuje je jednocześnie do portalu i do sprawcy szkodliwych działań. Dane te są następnie wykorzystywane w różnego rodzaju działalności przestępczej: dla zysku finansowego, dla wymuszeń oraz celem sprzedaży na czarnym rynku[3,4].
- **ZŁOŚLIWE ADRESY URL**. Definiowane są jako łącza tworzone z zamiarem dystrybucji złośliwego oprogramowania lub umożliwienia dokonania oszustwa. Procedura obejmuje wydobycie danych ofiary metodą inżynierii społecznej, aby skłonić ją do kliknięcia na złośliwe łącze, z którego następnie na urządzenie użytkownika dostarczane jest złośliwe oprogramowanie lub zawartość[28].

Operacja WizardOpium

Wykryto podatność zero-day w przeglądarce Google Chrome wskutek pojawienia się ukierunkowanych ataków przez strony internetowe. Luka, zarejestrowana jako CVE-2019-13720, wpływa na wersje wcześniejsze niż 78.0.3904.87 na systemach Microsoft Windows, Mac i Linux. Błąd kryje się w komponencie audio przeglądarki internetowej, a jego skuteczne wykorzystanie może skutkować wykonaniem dowolnego kodu.

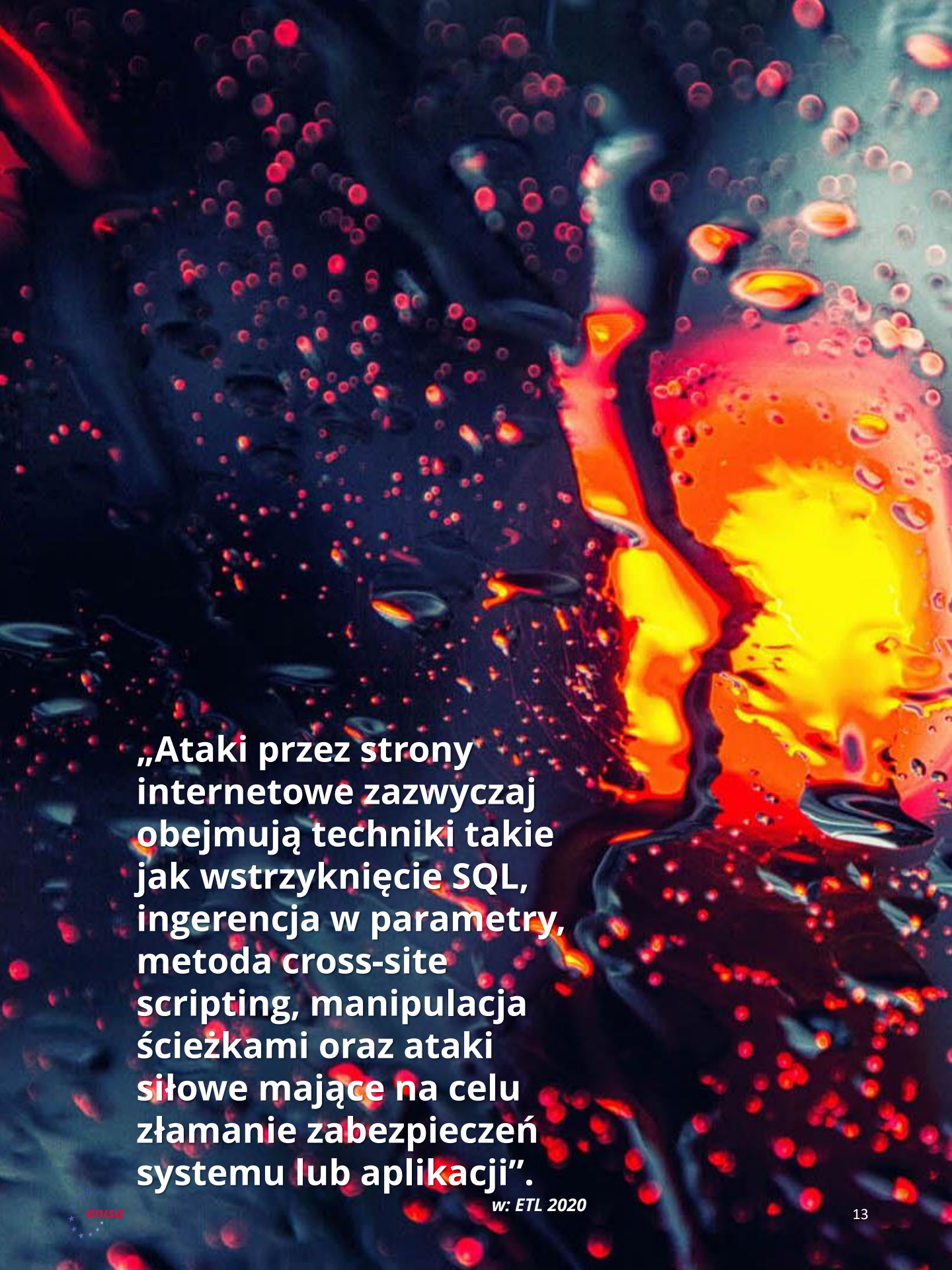
Ta podatność zero-day, odkryta przez analityka bezpieczeństwa i oznaczona numerem CVE-2019-13720, nie była powiązana z konkretnym sprawcą szkodliwych działań, lecz stanowiła część kampanii śledzonej jako Operacja WizardOpium. W międzyczasie firma Google wypuściła zaktualizowaną wersję Chrome 78.0.3904.87. Według analityka był to atak „u wodopoju" obejmujący wstrzyknięcie szkodliwego kodu na portal z wiadomościami w języku koreańskim. Złośliwy kod JavaScript umieszczony na stronie startowej umożliwia załadowanie z innej witryny skryptu profilującego[23,24].

Exploity przeglądarki to rodzaj wykorzystania podatności z użyciem złośliwego kodu ukierunkowanego na słabe punkty i luki w zabezpieczeniach oprogramowania (systemu operacyjnego i przeglądarki) lub związanych z nim wtyczek, aby na koniec uzyskać dostęp do urządzenia ofiary.

Ograniczenie ryzyka

_Proponowane działania

- Przestrzeganie dobrych praktyk w zakresie zarządzania poprawkami.
- Aktualizacja przeglądarki internetowej i związanych z nią wtyczek tak, by były nowe i zawierały poprawki uwzględniające znane podatności.
- Aktualizowanie oprogramowania stron opartych na systemie zarządzania zawartością (CMS) i portalu, aby uniknąć niezweryfikowanych wtyczek i dodatków.
- Dopilnowanie, aby punkty końcowe i zainstalowane oprogramowanie były aktualne, załatane i chronione.
- Izolacja aplikacji (biała lista aplikacji) i stworzenie środowiska piaskownicy celem zmniejszenia ryzyka ataków poprzez pobieranie niechcianych plików (drive-by). Na przykład technika izolacji przeglądarki może chronić punkty końcowe przed wykorzystaniem podatności w przeglądarce i infekcjami poprzez pobieranie niechcianych plików[29,30,31].
- W przypadku właścicieli witryn internetowych proaktywne podejście mające na celu ograniczenie skutków ataków przez strony internetowe polega na wzmocnieniu serwerów i usług. Obejmuje to kontrolę wersji skryptów w zawartości oraz skanowanie hostowanych lokalnie plików i skryptów serwera lub usługi sieciowej[32].
- Ograniczenia nakładane na zawartość w przeglądarce to kolejna technika ochrony przed atakami przez strony internetowe. Ułatwiające użytkowanie narzędzia, takie jak programy do blokowania reklam czy JavaScriptu, również ograniczają możliwość wykonania złośliwego kodu podczas odwiedzania pewnych witryn[29,30].
- Monitorowanie zawartości e-maili w przeglądarce i filtrowanie zawartości w celu wykrywania złośliwych adresów URL i plików/złośliwych programów oraz zapobiegania infekcji nimi.



„Ataki przez strony internetowe zazwyczaj obejmują techniki takie jak wstrzyknięcie SQL, ingerencja w parametry, metoda cross-site scripting, manipulacja ścieżkami oraz ataki siłowe mające na celu złamanie zabezpieczeń systemu lub aplikacji”.

w: ETL 2020

Bibliografia

1. „Watering Hole" Proofpoint. https://www.proofpoint.com/uk/threat-reference/watering-hole

2. „What Is a Drive-By Download?" Kaspersky. https://www.kaspersky.com/resource-center/definitions/drive-by-download

3. „Formjacking: Major Increase in Attacks on Online Retailers", Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers

4. „What is Formjacking and How Does it Work?", Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html

5. „Magecart's 7 Groups: Hackers Dropping Counter-Intelligence Code in JavaScript Skimmers". 14 listopada 2018 r. CBR. https://www.cbronline.com/in-depth/magecart-analysis-riskiq

6. „How Magecart's Web-Based Supply Chain Attacks are Taking Over the Web". 10 marca 2019 r. CBR. https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks

7. „CVE-2018-8174 Detail" 5 września 2019 r. NIST. https://nvd.nist.gov/vuln/detail/CVE-2018-8174

8. „Join a Slack workspace". Slack. https://slack.com/intl/en-gb/help/articles/212675257-Join-a-Slack-workspace

9. „New SLUB Backdoor Uses GitHub, Communicates via Slack" 7 marca 2019 r. Trend Micros. https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

10. „Security Researchers Partner With Chrome To Take Down Browser Extension Fraud Network Affecting Millions of Users" 13 lutego 2020 r. Cisco Duo Security. https://duo.com/labs/research/crxcavator-malvertising-2020

11. „Mac threat detections on the rise in 2019" 16 grudnia 2019 r. Malware Bytes. https://blog.malwarebytes.com/mac/2019/12/mac-threat-detections-on-the-rise-in-2019/

12. „File Cabinet", Google. https://sites.google.com/site/tiesitestutorial/create-a-page/file-cabinet

13. Google Sites. https://sites.google.com/site/

14. „Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted" 1 września 2016 r. https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html

15. „New Bizarro Sundown Exploit Kit Spreads Locky" Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

16. „Incoming! Multiple Popular Websites Attacked for Cryptocurrency Mining via GreenFlash Sundown Exploit Kit" 360 Blog. https://blog.360totalsecurity.com/en/incoming-multiple-popular-websites-attacked-cryptocurrency-mining-via-greenflash-sundown-exploit-kit/

17. „ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit" 27 czerwca 2019 r. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/

18. „GreenFlash Sundown exploit kit expands via large malvertising campaign" 26 czerwca 2019 r. Malware Bytes. https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/

19. „FAQ about SA-CORE-2018-002" 28 marca 2018 r. Drupal. https://groups.drupal.org/security/faq-2018-002

20. „Drupalgeddon2 still used in attack campaigns" 7 października 2019 r. Akamai. https://blogs.akamai.com/sitr/2019/10/drupalgeddon2-still-used-in-attack-campaigns.html

21. „Trustwave Global Security Report 2019", 2019. Trustwave.

22. „Stable Channel Update for Desktop" 31 października 2019 r. https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

23. „Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium". 1 listopada 2019 r. Kaspersky. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

24. „CVE-2019-13720 flaw in Chrome exploited in Operation WizardOpium attacks" 1 listopada 2019 r. Security Affairs. https://securityaffairs.co/wordpress/93278/hacking/cve-2019-13720-lazarus-attacks.html

25. „Web Browser-Based Attacks". Morphisec. https://www.morphisec.com/hubfs/1111/briefs/BrowserAttacksBrief-190327.pdf

26. „The 5 most common cyber attacks in 2019". 9 maja 2019 r. IT Governance. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

27. „Exploit Kits: Their Evolution, Trends and Impact". 7 listopada 2019 r. Cynet. https://www.cynet.com/blog/exploit-kits-their-evolution-trends-and-impact/

28. „Web-Based Threats: First Half 2019". 1 listopada 2019 r. Palo Alto. https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/

29. „Mitigating Drive-by Downloads" kwiecień 2020 r. ACSC. https://www.cyber.gov.au/publications/mitigating-drive-by-downloads

30. „MITRE ATT&CK: Drive-by compromise" 5 grudnia 2019 r. MITRE.

https://resources.infosecinstitute.com/mitre-attck-drive-by-compromise/#gref

31. „Protecting users from web-based attacks with browser isolation" 26 września 2019 r. Shi Blog – Security Solutions. https://blog.shi.com/solutions/protecting-users-from-web-based-attacks-with-browser-isolation/

32. "https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257". 11 kwietnia 2019 r. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257

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

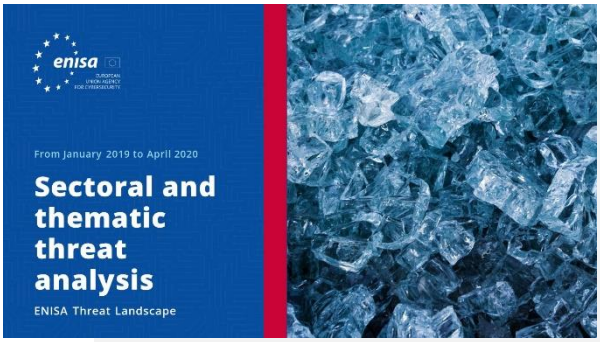
Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

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