



Ministerstwo
Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

01/2024





SPIS TREŚCI

<i>Wymiana cyber ciosów Rosji i Ukrainy.....</i>	<i>3</i>
<i>Półprzewodniki a suwerenność technologiczna</i>	<i>5</i>
<i>Podstawy cyberbezpieczeństwa danych medycznych.....</i>	<i>6</i>
<i>Szereg podatności w produktach firmy Ivanti – pytania dot. bezpieczeństwa rozwiązań VPN 7</i>	
<i>OSINT – znaczenie białego wywiadu i informacji dostępnych w sieci dla bezpieczeństwa użytkownika</i>	<i>9</i>
<i>Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta.....</i>	<i>12</i>
<i>INFORMACJA O SZKOLENIACH</i>	<i>14</i>
<i>Oznaczenia TLP.....</i>	<i>15</i>



Wymiana cyber ciosów Rosji i Ukrainy

Często zapominamy, że wojna Rosji z Ukrainą trwa od 2014 r., w tym w cyberprzestrzeni. Pełnoskalowa rosyjska inwazja w lutym 2022 r. poprzedzona była cyberatakami, bezpośrednio wspierała działania kinetyczne (np. cyberatak na Viasat), jak również towarzyszyła działaniom militarnym na późniejszych etap konfliktu. Jest to zgodne z rosyjską koncepcją wojny nowej generacji, niezależnie od skuteczności jej wdrożenia.

W ostatnich miesiącach nastąpiło nasilenie spektakularnych ukraińskich cyberataków wymierzonych w infrastrukturę krytyczną, w tym wojskową i przemysłu zbrojeniowego oraz systemy państwowe, obliczonych na zakłócenie działania, czy zdobycie kluczowych informacji dla prowadzenia działań zbrojnych. Poniższa grafika przedstawia wybrane najgłośniejsze upublicznione ukraińskie cyberataki.



Grafika przedstawiająca wybrane cyberataki pomiędzy Rosją i Ukrainą w ostatnich miesiącach. Źródło: opracowanie własne.

Również Rosja nie pozostaje dłużna. W ostatnie okresie najbardziej znaczący był cyberatak w grudniu 2023 r. na Kyivstar – największego ukraińskiego operatora komórkowego. Bywa określany największym cyberatakami od początku inwazji. Około 24,3 mln abonentów utraciło dostępu do usług telefonicznych i internetowych, sklepy w całym kraju nie były w stanie przetwarzać płatności mobilnych, a we Lwowie latarnie uliczne paliły się przez cały ranek, ponieważ zdalne sterowanie odbywało się przez sieć Kyivstar. Czasowo niedostępne były również aplikacje mobilne firmy. Co więcej, władze miasta Sumy poinformowały, że system ostrzegania przed nalotami "nie będzie działał tymczasowo". Jednak dane użytkowników miały nie zostać naruszone. Hakerzy naruszyli za to "część wewnętrznych



systemów operatora". Podobnych działań, o mniejszej skali, było znacznie więcej, jak np. cyberatak na ukraińskie Ministerstwo Edukacji i Nauki.

Zwiększona intensywność ofensywnych działań w cyberprzestrzeni wpisuje się w nowe ukraińskie podejście do prowadzenia wojny, wyłożone m.in. przez byłego już głównodowodzącego gen. W. Załużnego w „pożegnalnym” [eseju dla CNN](#). Nowa koncepcja obejmuje bowiem m.in. działania - tak w świecie wirtualnym jak i fizycznym - mające na celu zmniejszenie możliwości ekonomicznych Rosji, niszczenie jej potencjału przemysłowego oraz logistyki i całego systemu wsparcia maszyny wojennej. Wiąże się to z możliwym ograniczeniem wsparcia sprzętowego ze strony Zachodu oraz ograniczonymi własnymi zasobami ludzkimi i zbrojeniowymi, co zmusza Ukrainę do znajdowania nowych instrumentów pozwalających neutralizować rosyjski potencjał.

W tym kontekście warto jednak przytoczyć [słowa szefa amerykańskiego Biura Cyberprzestrzeni i Polityki Cyfrowej Nathaniela Ficka](#), najwyższego amerykańskiego "dyplomaty" ds. cyber. Stwierdził on, że Stany Zjednoczone zobowiązują się do dalszego wspierania wysiłków obronnych Ukrainy. Jego komentarze pojawiły się w czasie sporu między Demokratami i Republikanami w Senacie o zatwierdzenie ustawy mającej na celu m.in. zapewnienie pomocy dla Ukrainy o wartości 60 mld USD. Fick powiedział, że weto Senatu nie wpłynie na amerykańską cyberpomoc dla Ukrainy, ponieważ istnieją „inne mechanizmy i środki finansujące”, w tym uruchomiony w grudniu ub.r. Mechanizm Talliński ([w którym uczestniczy także Polska](#)). Wśród zasobów, które okazały się najbardziej skuteczne dla Ukrainy, Fick wspominał o migracji ukraińskich podmiotów rządowych do chmury, udostępnienie przez Polskę tysięcy terminali internetowych Starlink w celu zapewnienia odpornej łączności oraz koordynację między ukraińskimi i amerykańskimi rządami i firmami technologicznymi w celu przeciwdziałania rosyjskim cyberatakom. Przed inwazją Rosji, USA Cyber Command wysłało swoje siły na Ukrainę, aby współpracować z lokalnymi specjalistami i sprawdzić ukraińską sieć pod kątem złośliwego oprogramowania. Podczas tak zwanej operacji "hunt forward" ukraińscy i amerykańscy specjaliści odkryli co najmniej 90 próbek złośliwego oprogramowania infiltrujących krytyczne sieci Ukrainy. Ponadto, jak [poinformowało ukraińskie ministerstwo transformacji cyfrowej](#), dzięki wsparciu amerykańskiemu 16 agencji rządowych i kluczowych przedsiębiorstw będzie mogło w 2024 r. kontynuować wykorzystanie platformy Recorded Future - systemu rozpoznawania zagrożeń w cyberprzestrzeni (CTI). Wartość pomocy wynosi 23 mln USD. Biuro Ficka jest obecnie w trakcie opracowywania amerykańskiej międzynarodowej cyberstrategii, którą mają nadzieję opublikować na konferencji RSA Security w San Francisco w maju.

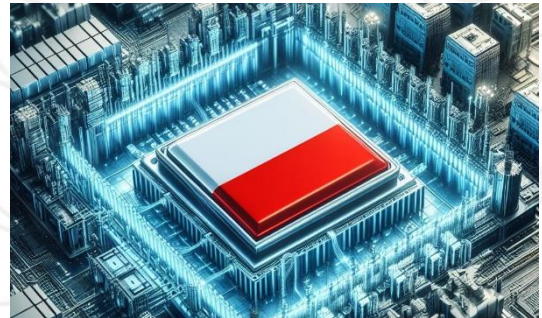
Źródła: Recorded Future, CyberDefence24.pl, KyivPost., gur.gov.ua, CNN, thedigital.gov.ua



Półprzewodniki a suwerenność technologiczna

[Ministerstwo Cyfryzacji wysłało do UOKiK prenotyfikację](#) dotyczącą pomocy publicznej dla Intelu, w związku z planowaną fabryką półprzewodników pod Wrocławiem. Zakład Integracji i Testowania ma kosztować 20 mld zł, a pomoc publiczna ma wynieść 6 mld zł. Jest to inwestycja mająca olbrzymie znaczenie dla polskiej gospodarki, włączająca nas w amerykańską część półprzewodnikowego łańcucha dostaw, tworząca wiele wysokokwalifikowanych miejsc pracy, nawet jeśli nie dotyczy najbardziej wyrafinowanego segmentu produkcji półprzewodników. Ma to też fundamentalne znaczenie dla bezpieczeństwa narodowego, wiążąc nas jeszcze bardziej ekonomicznie z najważniejszym sojusznikiem.

Pomimo korzyści gospodarczych, eksperci wskazują, że w ograniczony sposób przyczyni się to do wzrostu suwerenności technologicznej i włączenia rodzimych rozwiązań do światowego łańcucha dostaw. Do tego konieczna jest budowa krajowych kompetencji technologicznych i przemysłowych, a to wiązałoby się z koniecznością znacznych inwestycji w polski sektor półprzewodnikowy, który posiada już pewien bazowy potencjał.



Grafika wygenerowana przez AI mająca przedstawiać linię produkcyjną półprzewodników z elementem polskiej flagi.

Jak wskazuje prof. Piotr Grabiec z Instytutu Mikroelektroniki i Fotoniki "potrzebna jest mądra, oparta na merytorycznej wiedzy, rządowa strategia rozwoju technologii uwzględniająca potrzeby gospodarki i obronności kraju. Tego niestety od lat brakuje. [...] Przyciągnięcie do Polski inwestycji Intelu o wartości blisko 20 mld zł jest bardzo korzystne, ale nie załatwia problemu rozwoju mikroelektroniki w naszym kraju". Dr inż. Jarosław Tworóg wskazuje, iż "Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji stoi na stanowisku, że polska strategia powinna zawierać dwa elementy: wsparcie dla uruchomienia inwestycji zagranicznych w produkcję wielkoskalową oraz stworzenie długoterminowego programu rozwoju organicznego polskich firm".

Z kolei Alicja Musiał z firmy KP Labs podnosi, "że to nie jest do końca tak, że z tych zakładów wyjdą "Jobsy i Wozniaki". Bez zmiany nastawienia systemu edukacji, finansowania B+R [...] będziemy ostatecznie... tylko podwykonawcą. Tak jak w innych branżach, [...] tutaj także potrzebne jest wsparcie państwa, np. przez konkretne kształtowanie programów dofinansowania nauki, badania i rozwoju, czy wsparcie instytucji, które już istnieją". Argumentuje, że "te pieniądze [na wsparcie inwestycji Intelu] są znaczące w porównaniu do ogólnych nakładów na B+R oraz badania podstawowe, np. przez NCBiR, czy NCN", jak również że "powinny powstać programy, które ułatwią korzystanie z działającej już infrastruktury B+R półprzewodników w Polsce i rozwój dalszej. Tylko tak zwiększymy szansę rozwoju kadr i własnej produkcji bardziej złożonych mikroprocesorów w przyszłości".

Działania w tym zakresie realizuje już UE, nie tylko poprzez głośny European Chips Act, ale też inwestowanie mld euro w badania i innowacje półprzewodnikowe. Polska mogłaby nie tylko włączyć się w programy unijne, ale równolegle realizować własne ambitne przedsięwzięcia, aby łatwo nie oddać europejskiego i światowego kawałka chipowego tortu innym graczom.



Podstawy cyberbezpieczeństwa danych medycznych

Dynamiczny rozwój cyfryzacji usług opieki zdrowotnej sprawia masową digitalizację danych biomedycznych, a co za tym idzie konieczność zapewnienia możliwie najwyższego poziomu



Folder medyczny
Źródło: www.iconfinder.com

bezpieczeństwa na każdym z etapów ich przetwarzania. Ze względu na wysokie koszty i skomplikowanie ich pozyskania przez podmioty medyczne oraz potencjalnie wysoką wrażliwość (dotyczą stanu zdrowia nie tylko pojedynczych osób, ale całych społeczeństw), dane te stanowią atrakcyjny cel ataków dla m.in. grup przestępczych, rządów innych państw, firm ubezpieczeniowych, medycznych czy naukowych. Same dane natomiast mogą zostać wykorzystane do m.in. profilowania marketingowego klientów; uzyskania przewagi konkurencyjnej przedsiębiorstw z pominięciem przeznaczania ogromnych środków na badania i rozwój;

uczenia modeli AI; prowadzenia wojny informacyjnej i próby generowania wzrostów niepokoju społecznych w państwach uznanych za wrogie; indywidualnych prób szantażu osób pod groźbą publikacji informacji prywatnych; realizacja wrogich interesów poprzez wykorzystanie intymnych informacji jako metody nacisku na kluczowe osobistości społeczne (VIP) przez służby specjalne wrogich państw i zorganizowane grupy przestępcze.

Zgodnie z powyższym należy zaznaczyć, iż w obecnym scentralizowanym świecie cyfrowym, wysoka jakość usług medycznych to już nie tylko bezpośrednia jakość obsługi medycznej, ale również konieczność zachowania wysokich standardów bezpieczeństwa przetwarzania danych medycznych, osobowych, biologicznych i finansowych w zintegrowanych systemach placówek ochrony zdrowia służących do obsługi ubezpieczeniowo-zdrowotnej pacjentów.

Niestety, efektywne zabezpieczenie danych pacjentów w wielu przypadkach może skutkować spowolnieniem pewnych procesów lub zmniejszyć elastyczność świadczonych usług. Jednakże, w tym przypadku z zamiarem zachowania bezpieczeństwa danych pacjentów, należy najpierw zapewnić skuteczną ochronę baz danych, a następnie rozszerzać usługi cyfrowe związane z opieką zdrowotną.

Komentarz: Branża medyczna posiada jedno z najbardziej wrażliwych danych o swoich klientach. Odpowiednia ochrona danych przy jednoczesnym zapewnieniu szybkiego dostępu w celu szybkiego reagowania jest jednym z kluczowych filarów cyberbezpieczeństwa w jednostkach opieki medycznej. Wrażliwość sektora dobrze obrazuje atak ransomware na ALAB LABORATORIA w którym wyciekły dane ponad 200 tys. osób z lat 2017- 2023. W wyniku ataku, na forach hackerskich została upubliczniona lista nazwisk wraz z odpowiadającymi im numerami PESEL. Przypadek ten pokazuje to jak ważne jest odpowiednie zabezpieczenie danych w jednostkach sektora medycznego.



Logo firmy ALAB



Szereg podatności w produktach firmy Ivanti – pytania dot. bezpieczeństwa rozwiązań VPN

Użytkownicy chcący zapewnić sobie dostęp do sieci korporacyjnych korzystają z rozwiązań VPN udostępnianych do Internetu. Po uwierzytelnieniu użytkownika, taki dostęp jest przyznawany. Obecnie w wielu firmach, ciężko wyobrazić sobie pracę zdalną bez korzystania z takich rozwiązań. Problem zaczyna się w momencie, gdy VPN ma podatność, gdzie możliwe jest przejęcie pełnej kontroli nad nim, bez konieczności uwierzytelnienia – gdy istnieje możliwość jego ominięcia.

9 lutego 2024 r. Zespół CERT Polska na swoim koncie w serwisie 'X' poinformował o kolejnych krytycznych podatnościach w bramach VPN firm Fortinet (**CVE-2024-21762, CVE-2024-23113** – umożliwiające zdalne wykonanie kodu bez uwierzytelnienia) oraz Ivanti (**CVE-2024-22024** – ominięcie uwierzytelniania). W ostatnim czasie do producentów, którym aktywnie przyglądają się badacze bezpieczeństwa dołączyła firma Ivanti i jej VPN Connect Secure oraz Ivanti Policy Secure (NAC solution).

Miesiąc wcześniej, 10 stycznia, zidentyfikowano również inne podatności w produktach Ivanti, mianowicie firma ujawniła dwie luki w zabezpieczeniach, **CVE-2023-46805** (podatność na obejście uwierzytelniania z wynikiem CVSS 8.2) i **CVE-2024-21887** (podatność typu command-injection wykryta w wielu komponentach sieciowych z wynikiem CVSS 9.1), mające wpływ na urządzenia Ivanti Connect Secure VPN (dawniej Pulse Secure) i Ivanti Policy Secure. Udańe wykorzystanie może skutkować obejściem uwierzytelniania i wykonaniem polecenia, prowadząc do dalszej kompromitacji sieci ofiary. Mandiant zidentyfikował exploity zero-day dla tych luk wykorzystywanych od ok. grudnia 2023 r. przez podejrzanego o szpiegostwo aktora, obecnie śledzonego jako UNC5221. Ivanti ściśle współpracuje z Mandiant, zainteresowanymi klientami, partnerami rządowymi i firmą Volexity, aby rozwiązać te kwestie.

Co ciekawe na stronie amerykańskiej Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), 31 stycznia 2024 r. pojawiła się informacja:

“Agencies running affected products Ivanti Connect Secure or Ivanti Policy Secure solutions—are required to immediately perform the following tasks:

As soon as possible and no later than 11:59PM on Friday February 2, 2024, disconnect all instances of Ivanti Connect Secure and Ivanti Policy Secure solution products from agency networks. (...)”

Agencje użytkujące produkty Ivanti Connect Secure VPN oraz Ivanti Policy Secure zgodnie z powyższą informacją **obowiązane są do natychmiastowego odłączenia ww. rozwiązań od sieci do dnia 2 lutego 2024 r.** Powodem takiej rekomendacji może być z jednej strony zidentyfikowana szeroko zakrojona kampania infekowania systemów VPN Ivanti, jak również **podejrzenia, że aktywność związana z propagowaniem i wykorzystaniem podatności jest ściśle związana z chińską grupą APT – UTA0178.**

UTA0178 to chińska grupa hakerska z dużym prawdopodobieństwem sponsorowana przez państwo, która jest aktywna od co najmniej grudnia 2023 r. Wykorzystuje luki w zabezpieczeniach urządzeń Ivanti Connect Secure VPN, w szczególności wyżej opisane CVE-2023-46805 i CVE-2024-21887. Celem ataków grupy są różne sektory na całym świecie, w



tym rządowy, wojskowy, telekomunikacyjny, obronny, technologiczny. Grupa została powiązana także z ww. aliasem UNC5221. Grupa używa komponentu webshell – **GIFTEDVISITOR**. Rodzina złośliwego oprogramowania GIFTEDVISITOR była wykorzystywana w różnych kampaniach cyberszpiegowskich wymierzonych w infrastrukturę krytyczną, agencje rządowe i firmy technologiczne. Jest często używana w połączeniu z innymi narzędziami np. backdoor Zipline, Warpwire credential harvester itp. Obserwacje firmy Volexity ujawniły, że około 1700 urządzeń zostało naruszonych przy użyciu zmodyfikowanego webshella GIFTEDVISITOR.

Indicators of Compromise (IOCs)

Code Family	Filename	Description
LIGHTWIRE	compcheckresult.cgi	Web shell
THINSPPOOL	sessionserver.sh	Web shell dropper
WARPWIRE	lastauthserverused.js	Credential harvester
WIREFIRE	visits.py	Web shell
THINSPPOOL Utility	sessionserver.pl	Script
ZIPLINE	libsecure.so.1	Passive backdoor

Network-Based Indicators (NBIs)

symantke[.]com WARPWIRE C2

IOCs dot. podatności CVE-2023-46805 oraz CVE-2024-21887 identyfikowane przez Mandiant. Źródło: mandiant.com

Komentarz: W przypadku korzystania w organizacji z rozwiązań Ivanti, zaleca się natychmiastowe wdrożenie działań mitygujących dla ww. podatności na stronie Producenta. Dokładna analiza dostępna jest również na stronie Volexity.

Ponadto zgodnie z Ustawą o Krajowym Systemie Cyberbezpieczeństwa, art. 33. pkt.1, pkt.3, pkt.4, krajowe Zespoły CSIRT (MON, NASK i GOV) mogą przeprowadzić badanie w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. W przypadku identyfikacji podatności, składany jest wniosek w sprawie rekomendacji, a Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa po uzyskaniu opinii Kolegium do Spraw Cyberbezpieczeństwa wydaje, zmienia lub odwołuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Opisane działanie otwiera furtkę, celem wyeliminowania stosowania wadliwych systemów, które mogły zostać zainfekowane przez adversarza i/lub niosą poważne zagrożenie dla bezpieczeństwa systemów teleinformatycznych i zachowania poufności danych w podmiotach krajowych.

Źródła: https://twitter.com/CERT_Polska/status/1755860437810217253, cisa.gov, sekurak.pl, volexity.com, forums.ivanti.com, Recorded Future, Mandiant.com

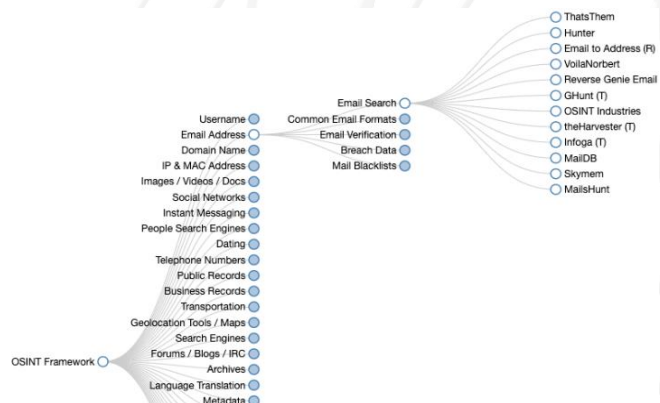


OSINT – znaczenie białego wywiadu i informacji dostępnych w sieci dla bezpieczeństwa użytkownika

Oczywistym jest, że im więcej informacji o danej osobie znajduje się w Internecie, tym dokładniejszy będzie jej profil. Mistrzostwo w profilowaniu, znajdowaniu informacji w oparciu o materiały dostępne w Internecie osiągnęła brytyjska organizacja dziennikarstwa śledczego, która specjalizuje się w sprawdzaniu faktów i białym wywiadzie – Bellingcat. O sobie mówią: „Ujawniamy prawdę w czasach postprawdy”. Postprawda w tym ujęciu to sytuacja, w której fakty są mniej istotne w kształtowaniu opinii publicznej niż odwołania do emocji i osobistych przekonań. Bellingcat został uznany w Rosji za agenta zagranicy w 2021 r. Organizacja znana jest z reportaży dot. wojny domowej w Syrii, wojny w Donbasie, czy działaniach rosyjskiej FSB (w tym otruciu Skripala i Nawalnego). Jednym z głośniejszych śledztw zespołu Bellingcata była sprawa libijskiego wojskowego Mahmouda Al-Werfalliego. Między innymi dzięki zespołowi, Międzynarodowy Trybunał Karny wystawił za ww. nakaz aresztowania za zbrodnię wojenną - zbiorowe zabójstwo. Dowody przeciwko Al-Werfalliemu to głównie filmy, które zamieszczał on i jego grupa w Internecie. Śledczy je analizowali, dzięki czemu byli w stanie wskazać, gdzie i kiedy dochodziło do zbrodni. Do analizy wykorzystywali m.in. zdjęcia z mediów społecznościowych, satelitarne, historyczne dane pogodowe, informacje o kącie padania światła itp.

Działania grupy dowodzą, że każda poszlaka wrzucona do sieci ma znaczenie, nawet najdrobniejsza i ma przełożenie na decyzje już nie w wirtualnym, a w realnym świecie. Żołnierze na froncie, czy to rosyjsko-ukraińskim, czy izraelsko-palestyńskim często dokumentują (świadomie bądź nie) działania wojenne i upubliczniają zdjęcia na mediach społecznościowych, co z jednej strony może prowadzić do osiągnięcia pewnego celu propagandowego/informacyjnego, a z drugiej poważnie zagrozić interesom jednej ze stron. Tak samo jest w życiu codziennym, jeśli czegoś nie robimy z premedytacją – w tym przypadku wrzucamy treści do mediów społecznościowych, chcąc osiągnąć zamierzony efekt, nie możemy mieć pewności do jakich celów zostaną wykorzystane nasze dane i to co umieszczamy w sieci. **Dlatego warto zadziałać wyprzedzająco i sprawdzić, co na nasz temat możemy znaleźć w Internecie i tym razem na zebrane informacje, spojrzeć z perspektywy potencjalnego cyberprzestępcy, profilującego swoją ofiarę.** Jak to zrobić? Oto kilka wskazówek.

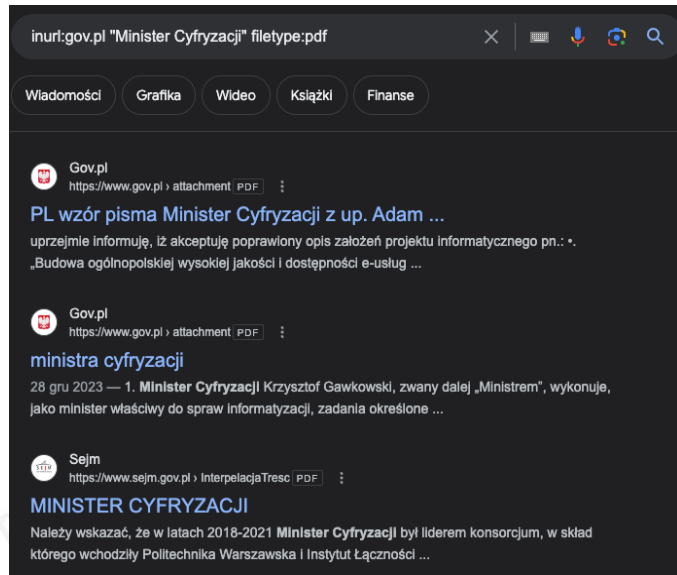
- Możemy wykorzystać **stronę** osintframework.com, która jest swoistym agregatorem narzędzi/stron internetowych wykorzystywanych do OSINT-u z podziałem na kategorie, zależnie od tego, jaki zakres danych nas interesuje – wybieramy właściwy.



OSINT Framework. Źródło: osintframework.com

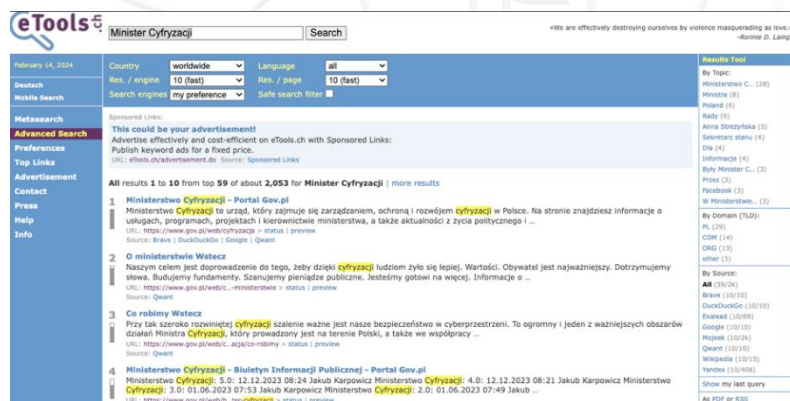


- Dodatkowo możemy skorzystać z **operatorów zaawansowanych w wyszukiwarce Google**. Przykładowo wpisując w wyszukiwarkę Google, operator: **inurl:gov.pl „Minister Cyfryzacji” filetype:pdf** – w wyniku dostaniemy kolejno wszystkie rekordy dotyczące plików .pdf, w których występowała fraza „Minister Cyfryzacji”, zamieszczonych na stronach w domenie gov.pl. Analogicznie możemy wpisać swoje dane np. dla strony swojej organizacji czy konta na mediach społecznościowych. Pomocne operatory dot. różnych elementów mogących nas zainteresować do wyszukania są opisane m.in. na stronie np. ahrefs.com.



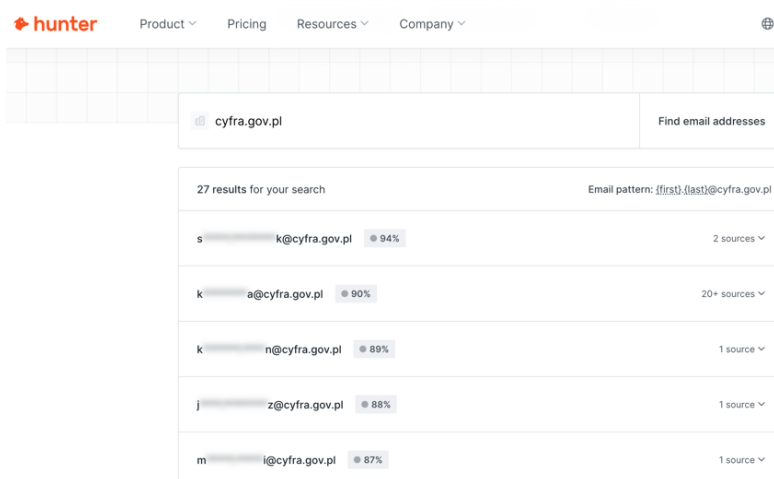
Zastosowanie operatorów zaawansowanych w wyszukiwarce Google. Źródło: google.com

- Oprócz wyszukiwarki Google, możemy skorzystać z innych alternatywnych np. etools.ch, które agregują dane z innych wyszukiwarek i podświetlają interesujące nas wyniki. Możemy wpisać swoje imię i nazwisko, adres e-mail.



Wyszukiwarka etools. Źródło: etools.ch

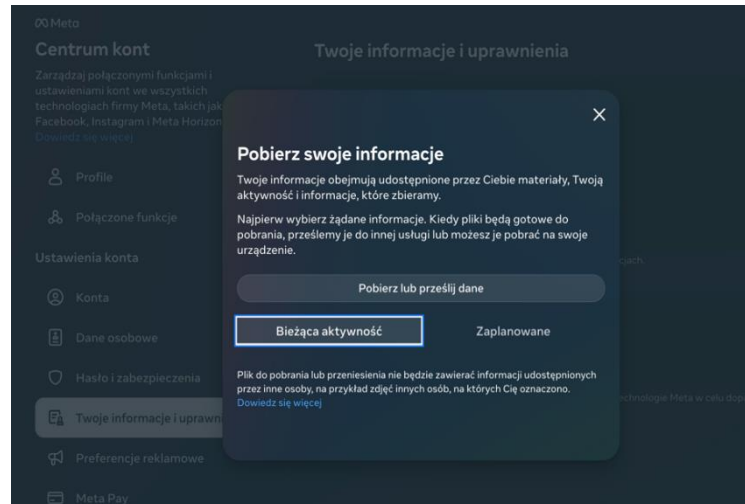
- Można zobaczyć również, czy nasz **firmowy adres mailowy jest dostępny z poziomu ogólnodostępnych wyszukiwarek typu Hunter**. Publiczna dostępność adresu może być wykorzystana do wysyłania maili phishingowych na dany adres.



Wyszukiwarka Hunter. Źródło: hunter.io



- Ponadto w zakładce 'ustawienia i prywatność' – 'ustawienia' – 'pobieranie informacji', można pobrać wszystkie zgromadzone o sobie informacje na koncie w serwisie Facebook w formie pliku. Warto to zrobić i całościowo spojrzeć na to co udostępniamy o sobie. Kopia danych, którą pobierzemy będzie zawierać wszystkie dane znajdujące się na Facebooku tj. zdjęcia, filmy, posty, informacje profilowe, lista znajomych i inne. Należy pamiętać, aby nie pobierać tych danych na niezabezpieczonym lub niezaufałym komputerze. To działanie pokazuje również, ile danych jest o nas zbierane przez właścicieli serwisów takich jak Facebook.



Konto w serwisie Facebook – pobieranie danych o sobie. Źródło: facebook.com

- Warto również pobrać jedno zdjęcie umieszczone przez nas w sieci i zobaczyć jakie metadane będziemy w stanie z niego odczytać.

Komentarz: Należy pamiętać, że wszystko, co umieszczamy w sieci może być wykorzystane przeciwko nam. Nasza aktywność w sieci może być analizowana nie tylko przez firmy zajmujące się profilowaniem użytkowników pod serwowane im treści marketingowe, ale również przez hakerów szukających nowych ofiar, czy to pozyskując informacje i nawiązując kontakt bezpośredni wykorzystując umieszczony w sieci numer telefonu, czy przeprowadzając spearphishing, atak ukierunkowany i celowany w konkretnego człowieka na podstawie profilu stworzonego w oparciu o dostępne informacje. Warto choć raz dokonać przeglądu naszej aktywności i ograniczyć dane, które udostępniamy bez potrzeby.



Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

Styczeń 2024 roku to kolejny miesiąc, w którym obserwowaliśmy, analizowaliśmy i zapobiegaliśmy licznym kampanią przestępczym. W pierwszym miesiącu nowego roku jako CSIRT KNF wykryliśmy i zgłosiliśmy do zablokowania 3 603 domeny, które wcześniej zakwalifikowaliśmy jako wyłudzające dane. Za ich pomocą przestępcy próbowali pozyskać loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe (imię, nazwisko, adres zamieszkania, e-mail, numer telefonu etc.).

Podobnie jak pisaliśmy w minionych miesiącach, również w styczniu 2024 trwał scenariusz znany pod nazwą „fraud inwestycyjny”. To ta metoda, w której przestępcy podszywają się pod znane osoby lub instytucje, celem nakłonienia potencjalnej ofiary do zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzą grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe. Nadal przestępcy wykorzystują technologie deepfake do tworzenia oszukańczych treści. Należy przyznać, że tworzone przez nich materiały są coraz bardziej dopracowane. Z czego to wynika? Technologia deepfake coraz bardziej się rozwija, ponosząc pewne koszty wystarczy, że przestępca powie pod kogo chce się podszyc i co sztuczny głos ma powiedzieć, resztę robi za niego narzędzie. Niestety, widok znanej osoby, która zachęca do inwestowania, mówi niezmiennym głosem i porusza się adekwatnie do tego co przedstawia sprawia, że ta socjotechnika staje się jeszcze bardziej skuteczna. To co jeszcze wydarzyło się w styczniu 2024, to wykorzystanie przez przestępców naszego wizerunku, czyli Komisji Nadzoru Finansowego. Jak to robili? Mając już zmanipulowaną osobę w omawianym wcześniej scenariuszu „fraud inwestycyjny”, zachęcają ją do coraz większych przelewów, jednak w pewnym momencie twierdzi, że chce wypłacić rzekomo zarobione środki. Atakujący informują o konieczności przejścia „weryfikacji AML”. Uzasadniają to potrzebą wypełnienia formalności sprawiających, że przychód nie będzie traktowany jako „pranie pieniędzy”. W tym celu wysyłają link, pod którym kryje się strona phishingowa podszywająca się pod wizerunek Komisji Nadzoru Finansowego. W rzeczywistości wykradane są dane uwierzytelniające do bankowości elektronicznej ofiary. Coraz częściej przestępcy wykorzystują również wariant oszustwa, w którym rzekomo oferowana jest pomoc w odzyskaniu środków osobom, które padły już wcześniej ofiarami fraudu inwestycyjnego. Wszystko po to, aby prowadzić dalszą grę psychologiczną i nakłaniać do przekazania im kolejnych oszczędności. Niestety jest to nadal rodzaj przestępstwa, w którym osoby poszkodowane tracą wysokie kwoty.

W styczniu 2024 przestępcy również w podszywali się polskie banki. Tym razem wykorzystywali wizerunek Banku Pocztowego, Banku Millennium, Santander Bank Polska oraz PKO BP. Tworząc strony przypominające prawdziwe strony banków, starali się wyłudzić informacje o kartach płatniczych oraz dane uwierzytelniające do bankowości elektronicznej. Kampanie przestępcze dystrybuowane poprzez wiadomości SMS oraz e-mail, dotyczyły m.in. następujących scenariuszy:

- podszywanie pod InPost i informacja o rzekomym braku adresu,
- podszywanie pod DHL i informacja o rzekomej konieczności dopłaty,



- podszycie pod UPS i informacja o rzekomej konieczności zaktualizowania danych,
- podszycie pod Allegro i informacja o rzekomym braku towarów i możliwości odebrania zwrotu pieniędzy,
- podszycie pod GLS i informacja o rzekomej konieczności uiszczenia opłaty,
- podszycie pod HBO MAX i informacja o rzekomym wygaśnięciu członkostwa.

Cyberprzestępcy do dystrybucji fałszywych stron wybrali również reklamy w mediach społecznościowych. Podszycując się pod markę Zalando, oferowali produkty w konkurencyjnych cenach. Po wejściu na stronę, ofiara musiała wypełnić formularz osobowy, a następnie zachęcana była do wpisania danych karty płatniczej. W ten sposób dane te trafiały w ręce przestępców.

Tak jak obiecywaliśmy w artykule z poprzedniego biuletynu, opublikowaliśmy kolejny artykuł dotyczący Sztucznej Inteligencji. Pokazujemy w nim jak różnorodne są źródła danych dla AI, od tekstów pochłanianych przez algorytmy przetwarzania języka naturalnego, przez obrazy i dźwięki, aż po dane finansowe i sensoryczne. Każdy klik, każde zapytanie, które wprowadzamy, staje się częścią gigantycznej układanki, z której AI uczy się, jak być naszym lepszym, szybszym pomocnikiem. Ale czy zastanawialiście się, jakie wyzwania i zagrożenia niesie za sobą ta niesamowita zdolność do uczenia się? W artykule nie unikamy trudnych tematów, takich jak bias (uprzedzenia) w danych czy kwestie związane z ochroną prywatności. To ważne, abyśmy jako użytkownicy i twórcy technologii byli świadomi nie tylko możliwości, ale i odpowiedzialności, jaką niesie za sobą korzystanie z AI. Zapraszamy do lektury: <https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/892-jak-sztuczna-inteligencja-przetwarza-dane>. Zachęcamy również do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook.



INFORMACJA O SZKOLENIACH

Zachęcamy również do udziału w bezpłatnych szkoleniach online dla podmiotów krajowego systemu cyberbezpieczeństwa, które organizuje Departament Cyberbezpieczeństwa MC.

Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej bazy wiedzy cyberbezpieczeństwa na portalu gov.pl – pod linkiem: <https://www.gov.pl/web/baza-wiedzy/szkolenia>

Zachęcamy również do zasubskrybowania biuletynu NASK – jest to przegląd najważniejszych informacji nt. cyberbezpieczeństwa, edukacji cyfrowej i nowych technologii.

Link do zapisów:

<https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html>



Źródło: <https://www.linkedin.com/newsletters/biuletyn-nask-https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html>



Oznaczenia TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i konsultantów) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie TLP:AMBER+STRICT , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacjami ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: cert.pl