EUROPEAN UNION AGENCY
FOR CYBERSECURITY

KRAJOBRAZ ZAGROŻEŃ 2021 WG AGENCJI UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA (ENISA)

Kwiecień 2020 r. do połowy lipca 2021 r.

PAŹDZIERNIK 2021 R.

INFORMACJE O ENISA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. ENISA – utworzona w 2004 r. i wzmocniona unijnym aktem o cyberbezpieczeństwie – 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. Przez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do połączonej gospodarki 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.

DANE KONTAKTOWE

Aby skontaktować się z autorami prosimy o skorzystanie z adresu etl@enisa.europa.eu.
Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

WYDAWCY

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

WSPÓŁAUTORZY

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

PODZIĘKOWANIA

Chcielibyśmy podziękować Członkom i Obserwatorom grupy roboczej ad hoc ENISA ds. krajobrazów zagrożeń cyberbezpieczeństwa za ich cenne opinie i komentarze podczas zatwierdzania niniejszego raportu. Chcielibyśmy również podziękować Grupie Doradczej ENISA i sieci Krajowych Urzędników Łącznikowych za ich cenne uwagi. Chcielibyśmy również podziękować zespołom ENISA ds. orientacji sytuacyjnej i powiadamiania o incydentach za ich aktywny wkład i wsparcie w procesie konsolidacji różnych informacji na potrzeby opracowania krajobrazu zagrożeń.

ZASTRZEŻENIA PRAWNE

PRAWO AUTORSKIE

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

SPIS TREŚCI

STRESZCZENIE

Jest to dziewiąte wydanie raportu Krajobraz zagrożeń wg ENISA (ETL), corocznego raportu na temat stanu krajobrazu zagrożeń dla cyberbezpieczeństwa, który identyfikuje główne zagrożenia, główne trendy zaobserwowane w odniesieniu do zagrożeń, twórców zagrożeń i techniki ataków, a także opisuje odpowiednie działania ograniczające ryzyko. W ramach ciągłego doskonalenia naszej metodologii tworzenia krajobrazów zagrożeń, w pracach nad tegorocznym raportem skorzystaliśmy z wsparcia nowoutworzonej grupy roboczej ad hoc ENISA ds. krajobrazów zagrożeń cyberbezpieczeństwa (CTL).

Raport ETL 2021 obejmuje okres od kwietnia 2020 r. do lipca 2021 r. określany w całym raporcie jako „okres objęty raportem". W okresie objętym reportem zidentyfikowano następujące główne zagrożenia:

- **Oprogramowanie szantażujące**
- **Złośliwe oprogramowanie**
- **Złośliwe wydobywanie kryptowalut**
- **Zagrożenia związane z pocztą elektroniczną**
- **Zagrożenia danych**
- **Zagrożenia dostępności i integralności**
- **Dezinformacja – informacja wprowadzająca w błąd**
- **Zagrożenia niezłośliwe**
- **Ataki na łańcuch dostaw**

W niniejszym raporcie omawiamy pierwszych 8 kategorii zagrożeń cyberbezpieczeństwa. Zagrożenia dla łańcucha dostaw, stanowiące dziewiątą kategorię, zostały ze względu na ich szczególne znaczenie szczegółowo omówione w specjalnym raporcie ENISA „Krajobraz zagrożeń dla ataków na łańcuch dostaw wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)" [1].

Dla każdego ze zidentyfikowanych zagrożeń omówiono techniki ataków oraz szczególnie istotne incydenty i trendy wraz z proponowanymi działaniami ograniczającymi ryzyko. Jeśli chodzi o trendy, w okresie objętym raportem zwracamy uwagę na następujące kwestie:

- **Za główne zagrożenie** w latach 2020-2021 uznano **oprogramowanie szantażujące.**
- **Instytucje rządowe zintensyfikowały działania** zarówno na poziomie krajowym, jak i międzynarodowym.
- **Coraz częstszą motywacją dla cyberprzestępców jest monetyzacja** ich działań, m.in. oprogramowanie szantażujące. Najczęstszą metodą wypłaty dla przestępców pozostaje **kryptowaluta**.
- **Spadek liczby przypadków użycia złośliwego oprogramowania**, który zaobserwowano w 2020 r., utrzymuje się w 2021 r. W 2021 r. zaobserwowaliśmy wzrost liczby cyberprzestępców, którzy uciekają się do stosunkowo nowych lub nietypowych języków programowania w celu portowania swoich kodów.
- Liczba **infekcji związanych ze złośliwym wydobywaniem kryptowalut** osiągnęła w pierwszym kwartale 2021 r. **rekordowo wysoki poziom** w porównaniu z ostatnimi latami. Motywację cyberprzestępców do dokonywania tych ataków stanowił **zysk finansowy** uzyskiwany ze złośliwego wydobywania kryptowalut.
- **Dominującą przynętą w kampaniach ataków e-mailowych nadal pozostaje COVID-19**.
- Zanotowano **gwałtowny wzrost liczby naruszeń danych w sektorze opieki zdrowotnej**.
- **Tradycyjnie stosowane kampanie DDoS (Distributed Denial of Service, rozproszony atak typu „odmowa usługi")** są w 2021 r. lepiej ukierunkowane, bardziej uporczywe i coraz bardziej wielowektorowe. Nową falę ataków DDoS przyciąga **IoT (Internet of Things, internet rzeczy)** w połączeniu z **sieciami mobilnymi**.

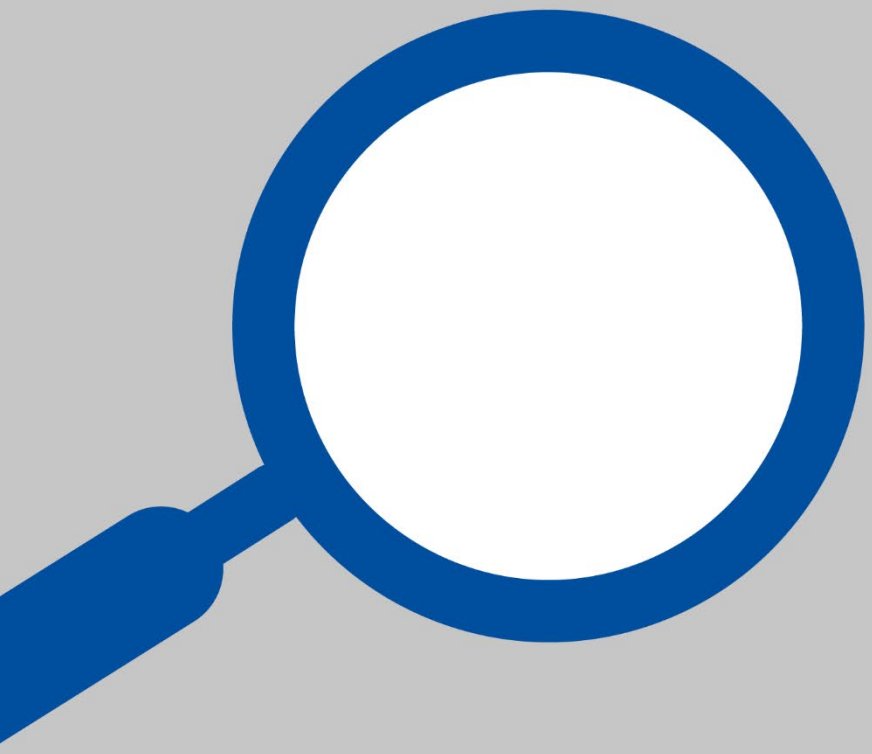
[1] Krajobraz zagrożeń dla ataków na łańcuch dostaw wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), lipiec 2021 r. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- W 2020 i 2021 r. obserwujemy **gwałtowny wzrost liczby incydentów niezłośliwych**, ponieważ pandemia COVID-19 przyczyniła się do występowania **błędów ludzkich** i **wadliwych konfiguracji systemu** do tego stopnia, że większość naruszeń w 2020 r. wynikała z błędów.

Zrozumienie trendów działań cyberprzestępców oraz ich motywacji i celów stanowi istotną pomoc w planowaniu bezpieczeństwa cybernetycznego i strategii ograniczania ryzyka. Jest to integralna część naszej ogólnej oceny zagrożeń, która umożliwia nadawanie priorytetów kontroli bezpieczeństwa oraz opracowanie specjalnej strategii z uwzględnieniem potencjalnego wpływu zagrożenia i prawdopodobieństwa jego materializacji. Z tego powodu na potrzeby raportu ETL 2021 wzięto pod uwagę następujące cztery kategorie podmiotów zagrażających cyberbezpieczeństwu:

- **Przestępcy sponsorowani przez państwo**
- **Cyberprzestępcy**
- **Hakerzy do wynajęcia**
- **Haktywiści**

W wyniku ciągłej analizy ENISA określiła trendy i punkty zainteresowania dla każdego z głównych zagrożeń przedstawionych w raporcie ETL 2021. Kluczowe ustalenia i osądy przedstawione w tej ocenie oparte są na wielu publicznie dostępnych zasobach, które wskazano w źródłach wykorzystanych przy opracowaniu tego dokumentu. Raport jest skierowany głównie do twórców polityki i decydentów, ale zainteresuje również środowiska zajmujące się cyberbezpieczeństwem od strony technicznej.



1. PRZEGLĄD KRAJOBRAZU ZAGROŻEŃ

Dziewiąta edycja raportu Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) zawiera ogólny przegląd krajobrazu zagrożeń dla cyberbezpieczeństwa. Raport ETL ma charakter częściowo strategiczny, a częściowo techniczny, i zawiera informacje interesujące zarówno dla czytelników zainteresowanych kwestiami technicznymi, jak i innych. W pracach nad tegorocznym raportem skorzystano z wsparcia nowoutworzonej grupy roboczej ad hoc ENISA ds. krajobrazów zagrożeń cyberbezpieczeństwa (CTL)[2].

W latach 2020 i 2021 odnotowano dalszą intensyfikację cyberataków, nie tylko pod względem ich wektorów i liczebności, lecz także pod względem ich oddziaływania. Jak można się spodziewać, pandemia COVID-19 miała również wpływ na krajobraz zagrożeń cyberbezpieczeństwa. Jednym z bardziej trwałych skutków pandemii COVID-19 jest utrzymująca się zmiana trybu pracy biurowej na tryb hybrydowy. Dlatego główny trend stanowią obecnie zagrożenia cyberbezpieczeństwa związane z pandemią i wykorzystywaniem tego „nowego stylu pracy". Tendencja ta oznacza zwiększenie powierzchni ataku, w wyniku czego zaobserwowaliśmy wzrost liczby cyberataków wymierzonych w instytucje i przedsiębiorstwa za pośrednictwem tzw. biur domowych[3].

Ogólnie rzecz biorąc, zagrożeń dla cyberbezpieczeństwa przybywa. Dzięki stale rosnącej obecności w internecie, przejściu z tradycyjnych infrastruktur na rozwiązania internetowe i oparte na chmurze, zaawansowanym połączeniom i wykorzystywaniu nowych funkcji pojawiających się technologii, takich jak sztuczna inteligencja (AI)[4][5], krajobraz cyberbezpieczeństwa uległ znacznej komplikacji pod kątem wyrafinowania ataków, ich złożoności i wpływu. Co ważne najwyższą pozycję wśród głównych zagrożeń zajęło zagrożenie dla łańcuchów dostaw oraz jego waga. Dlatego, ze względu na potencjalnie katastrofalne skutki kaskadowe, agencja ENISA postanowiła opracować odrębny krajobraz zagrożeń dla tej kategorii[6].

Warto zauważyć, że w tej edycji raportu ETL szczególny nacisk położono na wpływ cyberzagrożeń na różne sektory, w tym na te wymienione w dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NISD). Jeśli chodzi o krajobraz zagrożeń, potencjalne współzależności i istotne obszary, ciekawe wnioski można sformułować na podstawie specyfiki każdego sektora. Z tego powodu sektorowe krajobrazy zagrożeń wymagają szczegółowej analizy.

W tym roku działacze środowiska związanego z cybernetyką, a także decydenci polityczni, również wykonali kilka znaczących kroków. Globalna społeczność zaczęła zdawać sobie sprawę ze znaczenia komunikacji i współpracy w badaniu i śledzeniu cyberprzestępców, przy czym zwłaszcza oprogramowanie szantażujące (największe zagrożenie w okresie objętym raportem ETL 2021) stało się głównym punktem porządku dziennego spotkań światowych liderów w sprawie strategii.

Uważni czytelnicy poprzednich wydań ETL 2021 zauważą różnicę w ujęciu głównych zagrożeń. W tym roku ENISA zrobiła krok w tył i skonsolidowała kategorie zagrożeń z zamiarem integracji i lepszej reprezentacji zagrożeń o podobnym charakterze. Jest to element naszych starań, by wypracować zmodernizowaną taksonomię zagrożeń, która umożliwi metodologiczne ujęcie trendów w najbliższych kilku latach.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Raport pt. „Koszt naruszenia integralności danych" w 2020 r. - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Krajobraz zagrożeń związanych ze sztuczną inteligencją wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA): https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] Krajobraz zagrożeń dla ataków na łańcuch dostaw wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), lipiec 2021 r.https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Raport ETL 2021 korzysta z różnorodnych informacji ze źródeł otwartych i analiz cyberzagrożeń. Identyfikuje główne zagrożenia, trendy i ustalenia oraz wskazuje odpowiednie strategie wysokiego szczebla dotyczące ograniczania ryzyka. Obecnie agencja ENISA pracuje nad ujednoliceniem metodologii raportowania o krajobrazie zagrożeń, co ma na celu zwiększenie przejrzystości i spójności prac.

1.1. GŁÓWNE ZAGROŻENIA

W latach 2020 i 2021 pojawiła się i zmaterializowała cała seria cyberzagrożeń. Raport Krajobraz zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) identyfikuje, analizuje i omawia 8 głównych grup zagrożeń (zob. **Wykres1**).Te 8 grup zagrożeń wyróżniono ze względu na ich znaczenie w okresie objętym raportem, ich powszechność oraz wpływ, jaki wywiera materializacja tych zagrożeń.

- **Oprogramowanie szantażujące**
  Oprogramowanie szantażujące to rodzaj złośliwego ataku, w którym agresorzy szyfrują dane organizacji i żądają zapłaty za przywrócenie dostępu do nich. W okresie objętym raportem miało miejsce kilka znanych i szeroko nagłośnionych incydentów, co potwierdza tezę, że ataki z użyciem oprogramowania szantażującego stanowią główne zagrożenie. O znaczeniu i wpływie zagrożenia ze strony oprogramowania szantażującego świadczy również szereg powiązanych inicjatyw politycznych realizowanych w Unii Europejskiej (UE) i na całym świecie.

- **Złośliwe oprogramowanie**
  Złośliwe oprogramowanie to oprogramowanie komputerowe lub układowe przeznaczone do przeprowadzania nieautoryzowanych procesów, które będą miały negatywny wpływ na poufność, integralność lub dostępność systemu. Zagrożenie złośliwym oprogramowaniem od wielu lat niezmiennie zajmuje wysokie miejsce na liście zagrożeń, choć w okresie objętym raportem ETL 2021 jego znaczenie spadło. Zastosowanie nowych technik dołączania oraz kilka znaczących sukcesów organów ścigania wpłynęło na postępowanie cyberprzestępców.

- **Złośliwe wydobywanie kryptowalut**
  Złośliwe wydobywanie kryptowalut lub ukryte wydobywanie kryptowalut to rodzaj cyberprzestępstwa, w którym przestępca potajemnie wykorzystuje moc obliczeniową ofiary przestępstwa do generowania kryptowaluty. Wraz z rozprzestrzenianiem się kryptowalut i coraz większym zainteresowaniem nimi ze strony opinii publicznej zaobserwowano wzrost odpowiadających im incydentów cyberbezpieczeństwa.

- **Zagrożenia związane z pocztą elektroniczną**
  Ataki związane z pocztą elektroniczną to zestaw zagrożeń, które wykorzystują słabości ludzkiej psychiki i codziennych nawyków, a nie luki techniczne w systemach informatycznych. Co ciekawe zagrożenie to nadal utrzymuje się pomimo wielu kampanii uświadamiających i edukacyjnych ostrzegających przed tego typu atakami. W szczególności rośnie liczba oszustw z wykorzystaniem służbowych wiadomości mailowych oraz zaawansowanych i wyrafinowanych technik generowania zysków pieniężnych.

- **Zagrożenia danych**
  Ta kategoria obejmuje naruszenie bezpieczeństwa danych lub ich wyciek. Naruszenie bezpieczeństwa danych lub ich wyciek to wypływ wrażliwych, poufnych lub chronionych danych do niezaufanego środowiska. Naruszenia bezpieczeństwa danych mogą wystąpić w wyniku cyberataku, działań osób z wewnątrz, niezamierzonej utraty lub ujawnienia danych. Zagrożenie jest nadal wysokie, ponieważ zdobycie dostępu do danych bywa z wielu powodów głównym celem atakujących, np. w celu wymuszenia, uzyskania okupu, zniesławienia, rozpowszechniania dezinformacji itp.

- **Zagrożenia dostępności i integralności**
  Dostępność i integralność są celem wielu zagrożeń i ataków, wśród których szczególnie istotne są klasy ataków typu „odmowa usługi” (Denial of Service, DoS) i ataków na aplikację webową (Web Attack). Rozproszony atak typu „odmowa usługi” (DDoS), ściśle związany z atakami internetowymi, to jedno z najbardziej krytycznych zagrożeń dla systemów IT. Mierzy ono w ich dostępność poprzez wyczerpywanie zasobów, powodowanie spadku wydajności, utraty danych i awarie usług. To zagrożenie nieustannie zajmuje istotne miejsce w krajobrazie zagrożeń ENISA, zarówno ze względu na jego udział w zaistniałych incydentach, jak i na potencjalnie duże oddziaływanie.

- **Dezinformacja – informacja wprowadzająca w błąd**
  Wzrasta liczba kampanii dezinformacyjnych i wprowadzających w błąd, a wzrost ten jest wynikiem zwiększonego korzystania z platform mediów społecznościowych i mediów internetowych, a także częstszej obecności użytkowników w internecie spowodowanej pandemią COVID-19. Ta grupa zagrożeń pojawia się po raz pierwszy w raporcie ETL; jednak jej znaczenie w cyberświecie jest wysokie. Kampanie dezinformacyjne i wprowadzające w błąd są często stosowane w atakach hybrydowych w celu zmniejszenia ogólnego poziomu zaufania, głównego elementu cyberbezpieczeństwa.

- **Zagrożenia niezłośliwe**
  Zagrożenia te powszechnie rozumie się jako intencjonalne i złośliwe działania podejmowane przez przeciwników mających motywację do zaatakowania określonego celu. Kategoria ta obejmuje takie zagrożenia, w przypadku których złośliwe zamiary nie są widoczne. Zagrożenia wykorzystują głównie błąd ludzki i błędy konfiguracji systemu, ale mogą również obejmować fizyczne awarie dotyczące infrastruktury IT. Ze względu na swój charakter zagrożenia te są stałym elementem krajobrazu zagrożeń i stanowią istotną pozycję oceny ryzyka.

Wykres1: Krajobraz zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) - główne zagrożenia

Należy zauważyć, że powyższe zagrożenia obejmują kategorie i zbiór zagrożeń ujęte w ośmiu wymienionych powyżej obszarach. Każda z grup zagrożeń została poddana analizie w odrębnym rozdziale raportu, gdzie szczegółowo omawia się jej specyfikę i przedstawia bardziej szczegółowe informacje, ustalenia, trendy, techniki ataków i wektory ograniczania ryzyka.

1.2. NAJWAŻNIEJSZE TRENDY

Poniższa lista stanowi podsumowanie głównych trendów zaobserwowanych w krajobrazie cyberzagrożeń w okresie objętym raportem. Omówiono je szczegółowo w odpowiednich rozdziałach raportu Krajobraz zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

- **Odnotowano liczne wyrafinowane i istotne naruszenia łańcucha dostaw**, omówione w odpowiednim raporcie ENISA Krajobraz zagrożeń dotyczących łańcucha dostaw. Ważnym celem dla cyberprzestępców są **dostawcy usług zarządzanych**.
- **Epidemia COVID-19 sprzyja cyberszpiegostwu** i stwarza cyberprzestępcom **nowe możliwości działania**.
- **Instytucje rządowe intensyfikują działania** zarówno na poziomie krajowym, jak i międzynarodowym. Obserwuje się wzmożone wysiłki ze strony rządów mające na celu uniemożliwianie działań cyberprzestępców sponsorowanych przez państwa i podjęcie kroków prawnych przeciwko nim.
- **Coraz częstszą motywacją dla cyberprzestępców jest monetyzacja** ich działań, m.in. oprogramowanie szantażujące. Najczęstszą metodą wypłaty dla przestępców pozostaje **kryptowaluta**.
- Celem ataków cyberprzestępczych **coraz częściej jest infrastruktura krytyczna**.
- Najpowszechniejsze dwa **wektory infekcji oprogramowaniem szantażującym** to **e-maile phishingowe oraz atak brute-force usług pulpitu zdalnego (Remote Desktop Services, RDP)**.
- W ciągu 2021 r. wzrosło zainteresowanie modelami biznesowymi typu **oprogramowanie szantażujące jako usługa** (**Ransomware as a Service,** RaaS), a to utrudnia poprawne przypisanie ataków konkretnym cyberprzestępcom.
- W 2021 r. znacznie wzrosło wykorzystanie **oprogramowania szantażującego jako usługi z potrójnym wymuszeniem**.
- **Spadek przypadków użycia złośliwego oprogramowania**, który zaobserwowano w 2020 r., utrzymuje się w 2021 r. W 2021 r. zaobserwowaliśmy wzrost liczby cyberprzestępców, którzy uciekają się do stosunkowo nowych lub nietypowych języków programowania w celu portowania swoich kodów.
- **Złośliwe oprogramowanie atakujące środowiska kontenerowe** stało się znacznie bardziej powszechne i pojawiły się jego nowe warianty, takie jak bezplikowe złośliwe oprogramowanie uruchamiane z pamięci.
- Twórcy złośliwego oprogramowania wciąż wynajdują sposoby **utrudniania inżynierii wstecznej i analizy dynamicznej**.
- Liczba **infekcji związanych ze złośliwym wydobywaniem kryptowalut** osiągnęła w pierwszym kwartale 2021 r. **rekordowo wysoki poziom** w porównaniu z kilku ostatnimi latami. Motywacją do dokonywania tych ataków był dla cyberprzestępców **zysk finansowy** uzyskiwany ze złośliwego wydobywania kryptowalut.
- **W 2021 r. wielkość wydobycia kryptowalut i skala działań związanych ze złośliwym wydobywaniem kryptowalut są rekordowo wysokie.**
- Obserwuje się **przechodzenie od złośliwego wydobywania kryptowalut z użyciem przeglądarki do złośliwego wydobywania kryptowalut opartego na plikach**.
- **Dominującą przynętą stosowaną w masowych** atakach e-mailowych **pozostaje epidemia COVID-19**.
- **Oszukańcze służbowe wiadomości e-mail (Business E-mail Compromise, BEC) nasiliły się**, **stały się bardziej** wyrafinowane i lepiej **ukierunkowane**.
- Popularność zyskuje model biznesowy **phishing jako usługa**(Phishing-as-a-Service, PhaaS).
- Cyberprzestępcy coraz częściej zaczynają posługiwać się **informacjami o szczepionkach** w kontekście zagrożeń dla danych i informacji.
- Zanotowano **gwałtowny wzrost liczby naruszeń danych w sektorze opieki zdrowotnej**.
- Tradycyjne ataki DDoS (Distributed Denial of Service, rozproszone ataki typu „odmowa usługi") biorą sobie na cel **sieci mobilne i IoT (Internet of Things)**.
- **Atak typu odmowa usługi dla okupu (Ransom Denial of Service, RDoS)** to nowy poziom ataków typu „odmowa usługi".
- **Współdzielenie zasobów w środowiskach zwirtualizowanych zachęca cyberprzestępców do ataków DDoS.**
- W 2021 r. **kampanie DDoS** stały się lepiej ukierunkowane, bardziej uporczywe i coraz bardziej wielowektorowe.
- W przeprowadzaniu ataków przestępcy wspierają się **dezinformacją wykorzystującą sztuczną inteligencję (AI)**.
- **Podstawą ataków dezinformacyjnych jest phishing** wykorzystujący ludzkie zaufanie.
- **Poziom informacji wprowadzających w błąd i dezinformacji** leżących u podstaw działań cyberprzestępczych rośnie w niespotykanym dotąd tempie.

- **Model biznesowy dezinformacji jako usługi (Disinformation-as-a-Service, DaaS)** znacznie się rozwinął, głównie pod coraz większym wpływem pandemii COVID-19 i potrzeby posiadania większej ilości informacji.
- W 2020 i 2021 r. obserwujemy **gwałtowny wzrost liczby niezłośliwych incydentów**, ponieważ pandemia COVID-19 ułatwiła występowanie **błędów ludzkich** i **wadliwych konfiguracji systemu** do tego stopnia, że większość naruszeń w 2020 r. wynikała z błędów.
- Nastąpił **wzrost liczby niezłośliwych incydentów związanych z bezpieczeństwem chmury**.

1.3. UE A ODLEGŁOŚĆ GŁÓWNYCH ZAGROŻEŃ

Ważnym aspektem do rozważenia w kontekście krajobrazu zagrożeń wg ENISA jest bliskość cyberzagrożenia w odniesieniu do Unii Europejskiej (UE). Szczególnie istotna jest tu pomoc analitykom w ocenie znaczenia cyberzagrożeń, w ich skorelowaniu z potencjalnymi cyberprzestępcami i wektorami zagrożeń, a nawet w wyborze odpowiednio ukierunkowanych wektorów ograniczania ryzyka. Zgodnie z proponowaną klasyfikacją Wspólnej Polityki Bezpieczeństwa i Obrony UE (WPBiO)[7] dzielimy cyberzagrożenia na cztery kategorie przedstawione w **Tabeli 1**.

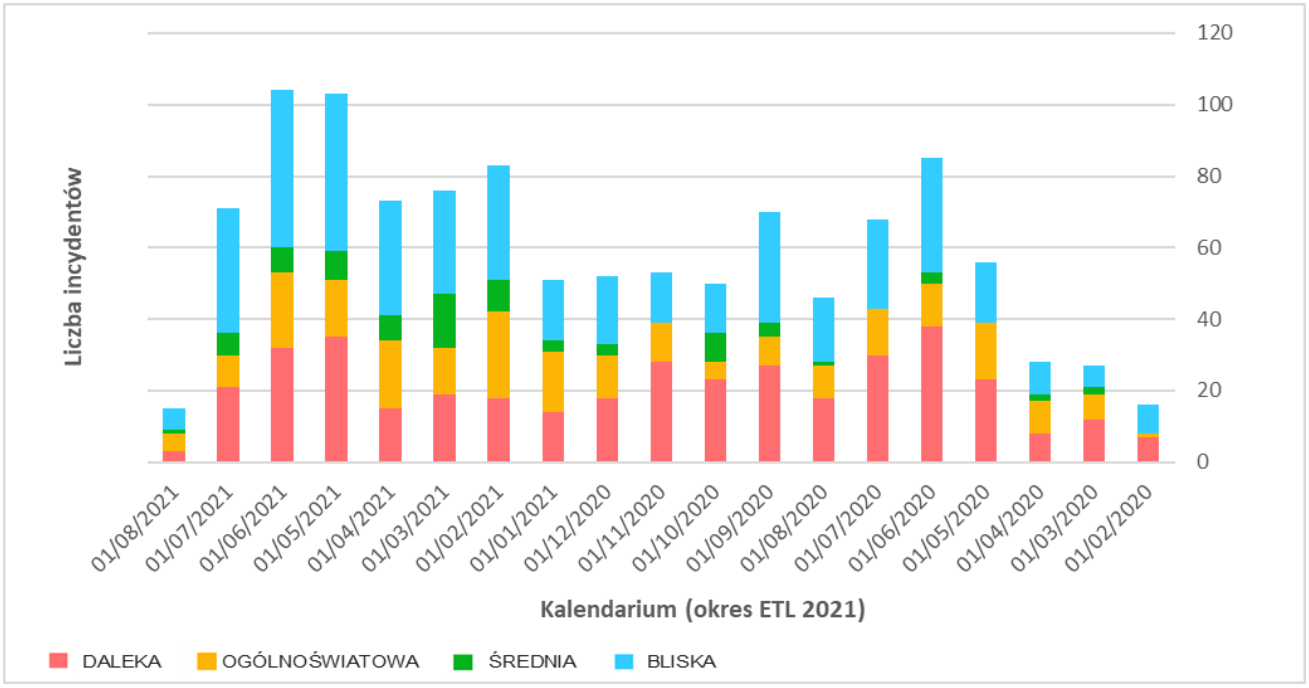
Tabeli 1: Klasyfikacja odległości cyberzagrożeń

ODLEGŁOŚĆ	Obawy
MAŁA	Narażone sieci, systemy, kontrolowane i zapewniane w granicach UE. Narażona populacja w granicach UE.
ŚREDNIA	Sieci i systemy uważane za kluczowe dla celów operacyjnych w zakresie jednolitego rynku cyfrowego UE i sektorów NISD, ale ich kontrola i zapewnienie opierają się na instytucjach publicznych lub prywatnych spoza UE lub państw członkowskich. Narażona populacja na obszarach geograficznych w pobliżu granic UE.
DALEKA	Sieci i systemy które w razie ataku będą miały krytyczny wpływ na cele operacyjne w zakresie jednolitego rynku cyfrowego UE i sektorów NISD. Kontrola i zapewnienie tych sieci i systemów wykraczają poza kompetencje instytucji publicznych lub prywatnych UE lub państw członkowskich (PC). Narażona populacja na obszarach geograficznych odległych od UE.
OGÓLNOŚWIATOWA	Wszystkie wyżej wymienione obszary

Wykres2 przedstawia kalendarium incydentów związanych z kategoriami głównych zagrożeń ujętych w raporcie ETL 2021.Należy zauważyć, że informacje przedstawione na wykresie oparte są na OSINT (Informacje ze źródeł otwartych) i są wynikiem prac ENISA w obszarze orientacji sytuacyjnej[8].

Wykres2: Kalendarium zaobserwowanych incydentów związanych z głównymi zagrożeniami ujętymi w raporcie ETL (orientacja sytuacyjna oparta na OSINT) według odległości.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Zgodnie z art. 7 ust. 6 aktu UE o cyberbezpieczeństwie https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN



Jak pokazuje powyższy wykres, w 2021 r. odnotowano większą liczbę incydentów w porównaniu z 2020 r. W szczególności w kategorii odległość BLISKA występuje rosnąca liczba obserwowanych incydentów związanych z głównymi zagrożeniami, co implikuje ich znaczenie w kontekście UE. Nic dziwnego, że miesięczne trendy (dla przejrzystości nie zaznaczono ich na wykresie) są dość podobne w różnych klasyfikacjach, ponieważ cyberbezpieczeństwo nie zna granic, a w większości przypadków zagrożenia materializują się na wszystkich poziomach odległości. Warto zauważyć, że w ostatnich miesiącach objętych raportem ETL 2021 obserwuje się wyższe wartości dla kategorii odległości BLISKA. Agencja ENISA będzie nadal monitorować ten trend, aby sprawdzić, jak ewoluuje i reaguje on na działania cyberprzestępców i bieżące wektory zagrożeń.

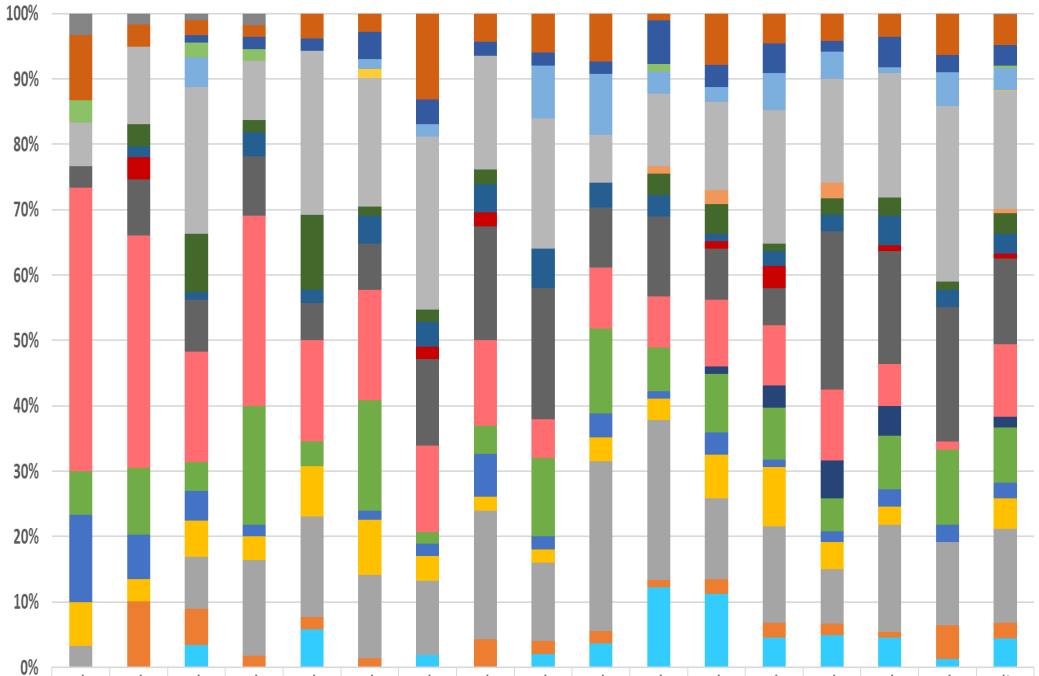
1.4. GŁÓWNE ZAGROŻENIA WEDŁUG SEKTORÓW

Cyberzagrożenia zwykle nie ograniczają się do jednego konkretnego sektora i w większości przypadków dotyczą więcej niż jednego z nich. Jest tak dlatego, że w wielu przypadkach do zagrożeń dochodzi na skutek wykorzystywania luk w podstawowych systemach teleinformatycznych, a te są stosowane w różnych sektorach. Należy jednak wziąć pod uwagę ataki ukierunkowane, a także ataki wykorzystujące różnice w poziomie dojrzałości cyberbezpieczeństwa w różnych sektorach oraz popularność/wyeksponowanie niektórych sektorów. Ze względu na te czynniki zagrożenia przejawiają się jako incydenty w określonych sektorach, dlatego ważne jest, aby dokładnie przyjrzeć się sektorowym aspektom zaobserwowanych incydentów i zagrożeń. Analiza trendów zaobserwowanych w poszczególnych sektorach oraz zależności międzysektorowych umożliwia wyciągnięcie wniosków.

Wykresy 3 i 4 przedstawiają sektory, w których wystąpiły incydenty zaobserwowane w oparciu o OSINT (Informacje ze źródeł otwartych) i są wynikiem prac ENISA w obszarze orientacji sytuacyjnej[9]. Dotyczą one incydentów związanych z głównymi zagrożeniami ujętymi w raporcie ETL 2021. Jest to pierwsza podjęta przez agencję ENISA próba ujęcia wpływu zagrożeń na określone sektory. W nadchodzących latach i w przyszłych wydaniach krajobrazu zagrożeń podjęte zostaną wysiłki w celu dostosowania omawianych sektorów do sektorów wymienionych w dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NISD) oraz propozycji jej zmiany (NISD 2.0).

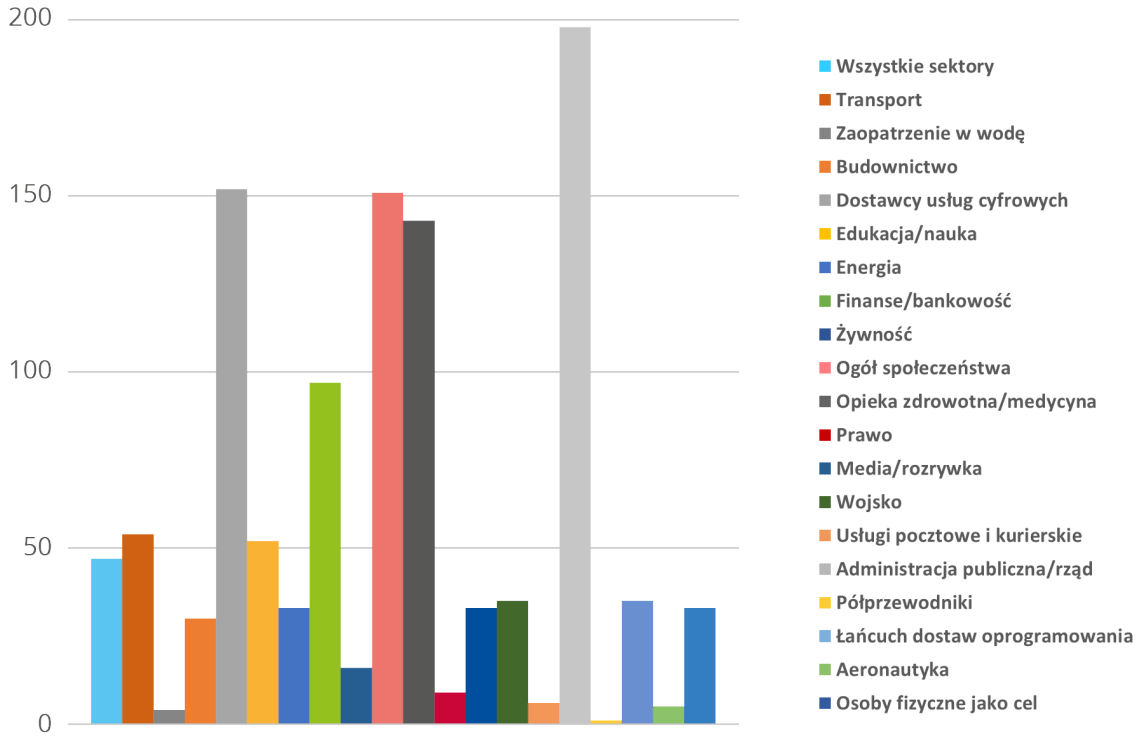
[9] Zgodnie z art. 7 ust. 6 aktu UE o cyberbezpieczeństwie (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Wykres3: Kalendarium zaobserwowanych incydentów związanych z głównymi zagrożeniami w raporcie ETL według sektorów.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Ogółem
Zaopatrzenie w wodę	1	1	1	1													2
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Osoby fizyczne jako cel			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Aeronautyka	1		2	1							1						4
Łańcuch dostaw oprogramowania			4			1	1		4	5	3	2	5	5	1	4	35
Półprzewodniki						1											1
Administracja publiczna/rząd	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Usługi pocztowe i kurierskie											1	2		3			6
Wojsko		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Media/rozrywka		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Prawo		2					1	1				1	3		1		7
Opieka zdrowotna/medycyna	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Ogół społeczeństwa	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Żywność												1	3	7	5		16
Finanse/bankowość	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energia	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Edukacja/nauka	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Dostawcy usług cyfrowych	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Budownictwo		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Wszystkie sektory			3		3		1		1	2	11	10	4	6	5	1	47

Wykres4: Narażone sektory wg liczby incydentów (kwiecień 2020 r. - lipiec 2021 r.)



W okresie objętym raportem duża liczba incydentów dotyczyła organów administracji publicznej i rządowych oraz dostawców usług cyfrowych. Tego ostatniego należy się spodziewać, biorąc pod uwagę horyzontalny charakter świadczenia usług dla tego sektora, a tym samym jego wpływ na wiele innych sektorów. Zaobserwowaliśmy również znaczną liczbę incydentów wymierzonych w użytkowników końcowych, niekoniecznie w konkretny sektor. Częstym celem był również sektor ochrony zdrowia, a aktywność tu odnotowana wykazuje oznaki wzrostu w ciągu ostatnich kilku miesięcy okresu objętego raportem (maj-lipiec 2021 r.). Co ciekawe, sektor finansowy mierzy się ze stałą liczbą incydentów w całym roku. Łańcuch dostaw oprogramowania również wykazuje zwiększoną liczbę incydentów w 2021 r., co zostało zauważone także w raporcie ENISA dotyczącym krajobrazu zagrożeń w łańcuchu dostaw.[10]

1.5. METODYKA

Postawą raportu Krajobraz zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) (ETL) są informacje dostępne ze źródeł otwartych, głównie o charakterze strategicznym, oraz materiały jednostki ENISA ds. analizy cyberzagrożeń (Cyber Threat Intelligence, CTI), zaś raport obejmuje więcej niż jeden sektor, technologię i kontekst. Przy tworzeniu raportu staraliśmy się zachować neutralność wobec branż i dostawców, odnosi się on więc do prac lub cytuje prace różnych badaczy z obszaru bezpieczeństwa, blogi na temat bezpieczeństwa i artykuły prasowe wskazane w tekście przy użyciu licznych przypisów końcowych. Raport ETL 2021 obejmuje okres od kwietnia 2020 r. do lipca 2021 r. określany w całym raporcie jako „okres objęty raportem".

Przy sporządzaniu raportu ETL 2021 zastosowano następujące podejście. ENISA metodą orientacji sytuacyjnej sporządziła wykaz głównych incydentów w danym okresie, o których informowano w otwartych źródłach. Wykaz ten był podstawą identyfikacji listy głównych zagrożeń, a także posłużył jako materiał źródłowy dla kilku trendów i statystyk wskazanych w raporcie.

Następnie ENISA oraz eksperci zewnętrzni przeprowadzili dogłębną analizę dostępnego piśmiennictwa z publicznie dostępnych źródeł, takich jak artykuły prasowe, ekspertyzy, raporty wywiadowcze, analizy incydentów i raporty z badań bezpieczeństwa. W drodze ciągłej analizy ENISA określiła trendy i punkty zainteresowania dla każdego z

[10] Krajobraz zagrożeń dla ataków na łańcuch dostaw wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), lipiec 2021 r. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

głównych zagrożeń przedstawionych w raporcie ETL 2021. Kluczowe ustalenia i osądy przedstawione w tej ocenie oparte są na wielu publicznie dostępnych zasobach, które wskazano w źródłach wykorzystanych przy opracowaniu tego dokumentu.

W raporcie staramy się odróżnić to, o czym informują nasze źródła, od naszej własnej oceny. (W tym celu posługujemy się zwrotem „w naszej ocenie"). Przeprowadzając ocenę, sygnalizujemy prawdopodobieństwo za pomocą zwrotów, które wyrażają oszacowanie prawdopodobieństwa (np. prawdopodobnie, bardzo prawdopodobnie, na pewno)[11].

W raporcie wykorzystano strukturę MITRE ATT&CK® [12], aby podkreślić taktyki i techniki ataku istotne dla danego zagrożenia (zob. Załącznik A).Dla każdej taktyki ATT&CK® przedstawione są techniki zastosowane przez przeciwnika. W wyniku może powstać lista możliwych do zastosowania działań łagodzących ATT&CK[13].MITER ATT&CK® to baza wiedzy, wspólny język taktyk i technik atakujących opartych na obserwacjach ze świata rzeczywistego. Baza wiedzy MITER ATT&CK® jest stosowana jako podstawa do opracowywania konkretnych modeli zagrożeń i metodologii w sektorze prywatnym, rządowym oraz w środowisku oferującym produkty i usługi związane z cyberbezpieczeństwem.

Raport został zatwierdzony przez powołaną w kwietniu 2021 r. grupę roboczą ad hoc ENISA ds. krajobrazów zagrożeń cyberbezpieczeństwa[14], w skład której wchodzą eksperci z europejskich i międzynarodowych podmiotów sektora publicznego i prywatnego.

Na potrzeby opracowywania raportów o krajobrazie zagrożeń ENISA jest w trakcie formalnego zatwierdzania metodyki mającej na celu zwiększenie przejrzystości i stworzenie podstaw dla ustrukturyzowanych i właściwie dostosowanych procesów. W ramach tego przedsięwzięcia w przyszłości zostanie upubliczniona metodyka opracowywania krajobrazów zagrożeń wraz ze zmienioną taksonomią.

1.6. STRUKTURA RAPORTU

W Krajobrazie zagrożeń 2021 ENISA (ETL) utrzymano strukturę poprzednich raportów ETL, wykorzystując podobną konstrukcję do podkreślenia głównych zagrożeń cybernetycznych w 2021 r. Czytelnicy poprzednich edycji zauważą, że kategorie zagrożeń zostały skonsolidowane zgodnie z działaniami zmierzającymi do zastosowania w przyszłości nowej taksonomii zagrożeń cyberbezpieczeństwa.

Raport ma następującą strukturę:

Rozdział 2 analizuje trendy związane z cyberprzestępcami (tj. przestępcy sponsorowani przez państwo, cyberprzestępcy, hakerzy do wynajęcia i haktywiści).
Rozdział 3 omawia główne ustalenia, incydenty i trendy dotyczące oprogramowania szantażującego.
Rozdział 4 przedstawia główne ustalenia, incydenty i trendy dotyczące złośliwego oprogramowania.
Rozdział 5 przedstawia główne ustalenia, incydenty i trendy dotyczące złośliwego wydobywania kryptowalut.
Rozdział 6 przedstawia główne ustalenia, incydenty i trendy dotyczące zagrożeń związanych z pocztą elektroniczną.
Rozdział 7 omawia główne ustalenia, incydenty i trendy dotyczące zagrożenia dla danych.
Rozdział 8 przedstawia główne ustalenia, incydenty i trendy dotyczące zagrożeń dla dostępności i integralności.
Rozdział 9 przedstawia główne ustalenia, incydenty i trendy dotyczące dezinformacji i informacji wprowadzającej w błąd.
Rozdział 10 koncentruje się na głównych ustaleniach, incydentach i trendach dotyczących zagrożeń niezłośliwych.
Załącznik A przedstawia techniki powszechnie stosowane w przypadku każdego zagrożenia, oparte na strukturze MITRE ATT&CK®.
Załącznik B ujmuje istotne incydenty według zagrożeń zaobserwowane w okresie objętym raportem.

[11] CIA - Words of Estimative Probability (Zwroty stosowane do szacowania prawdopodobieństwa) https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK®, https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes