Andrzej Skwarski

Akademia im. Jakuba z Paradyża
w Gorzowie Wielkopolskim

Studia Wschodnioeuropeiskie
Nr 15/2021

Cyberprzestępczość w dobie COVID-19. Nowe zagrożenia, metody przeciwdziałania.

Początek 2020 roku postawił przed światem poważne wyzwanie zatrzymania groźnego wirusa, który w ciągu kilku tygodni praktycznie dotarł do każdego zakątka świata. Paradoksalnie wirus, mimo niskiego poziomu śmiertelności zakażonych osób, wywołał wiele strachu, czasem wręcz paniki. Sparaliżował na wiele tygodni komunikację międzynarodową, wiele zakładów pracy, nauczanie bezpośrednie w szkole oraz wymusił na ludziach przestrzeganie zasad higieny oraz dystansu społecznego. Świat w swojej historii zmagał się z poważniejszymi chorobami takimi jak:

- Zaraza Antoninów - lata: 165 – 180; 5 mln zgonów
- Czarna Śmierć - lata: 1347 – 1351; 25 mln zgonów
- Ospa prawdziwa - lata: 1520 – 1979; 56 mln zgonów
- Wielka zaraza w Londynie - lata: 1665 – 1666; 100 000 zgonów
- Hiszpanka - lata: 1918 – 1920; 40 - 50 mln (wg niektórych źródeł nawet 100 mln) zgonów
- Grypa azjatycka - lata: 1957 – 1958; 1 - 2 mln zgonów
- Grypa Hong Kong - lata: 1968 – 1970; 1 - 4 mln zgonów
- Rosyjska grypa - lata: 1977 – 1978; 1 mln zgonów
- SARS - lata: 2002 – 2003; 800 zgonów
- Świńska grypa - lata: 2009 – 2010; 284 500 zgonów
- Ebola (ostatnia duża epidemia) - lata: 2014 – 2016; 11 300 zgonów
- Cholera (pandemie 1-7) - lata: 1817 - 2018 ostatnie ognisko epidemii; 1 mln zgonów

– HIV/AIDS - lata: 1981 – nieopanowana; 35 mln zgonów[782].

Mimo tak bogatych doświadczeń w zakresie walki z chorobami zakaźnymi, lawinowego rozwoju technologii wspomagających te działania oraz współpracy międzynarodowej pandemia Covid-19 stanowi poważny problem. Wspomniana już niska śmiertelność wirusa wywołała u wielu osób, a nawet całych grup społecznych, przekonanie o sztucznym budowaniu zagrożenia ze strony wirusa. Sytuacja ta stworzyła dodatkowe możliwości szerzenia dezinformacji na wszelkie tematy związane z pandemią. Brak rzetelnej wiedzy na temat zagrożeń, sposobów leczenia i przenoszenia choroby, wynikający głównie z krótkiego czasu od jej pojawienia, stanowi dodatkową przestrzeń do szerzenia nieprawdziwych informacji. Szybko okazało się, że dezinformacja w zakresie potencjalnych metod zwalczania wirusa jest groźna dla zdrowia, a nawet okazała sie przyczyną śmierci osób, które część z tych metod zastosowały.

Zorganizowana przestępcza działalność w okresie pandemii COVID – 19.

Przeniesienie naszych aktywności, głównie zawodowych, do sieci przyczyniło się do zwiększonej liczby cyberprzestępstw. Z drugiej strony lockdown, mniejsza aktywność w przestrzeni publicznej, ograniczenia w zakresie podróżowania wpłynęły na zmniejszenie poziomu przestępczości kryminalnej. Zgodnie ze statystykami Komendy Głównej Policji w marcu 2020 roku doszło do 4 126 kradzieży. W porównaniu z marcem 2019 kiedy odnotowano 9469 takich przestępstw, to ponad dwukrotnie mniej. Spadła również liczba kradzieży rozbójniczych z 99 do 66, a kradzieży z włamaniem z 3710 do 2697. Podobna sytuacja ma miejsce w innych krajach europejskich. We Włoszech, Francji czy Niemczech zanotowano spadki przestępczości kryminalnej od 35% do 45%. Podobne spadki zanotowano w Stanach Zjednoczonych a nawet Meksyku[783].

Przestępczość zorganizowana dostosowując się do powstałej sytuacji przeniosła swoją aktywność do innych dziedzin. Poza wspomnianą już cyberprzestępczością zgodnie z raportami Europolu i Interpolu przestępcy wykorzystali panujący strach stosując powszechne metody oszustw, między innymi telefonicznych. Ponadto wykorzystując braki w dostępie do środków dezynfekcyjnych, masek czy rękawiczek oszukali nie tylko pojedyncze osoby, ale nawet całe państwa. Ich ofiarą padły między innymi rządy Belgii, Holandii, Hiszpanii, Niemiec, Irlandii i

[782] I. Procyk-Lewandowska, *Historia pandemii na świecie, Coronawirus SARS COV-2 na tle innych pandemii,* https://www.medicover.pl/o-zdrowiu/historia-pandemii-na-swiecie-koronawirus-sars-cov-2-na-tle-innych-pandemii,6788,n,168 [dostęp 22.12.2020 r.].

[783] W. Kawa, *Przestępczość zorganizowana w dobie koronawirusa – próba bilansu,* https://fibis.pl/zagadnienia/przestepczosc-zorganizowana-w-dobie-koronawirusa-proba-bilansu/ [dostęp 27.12.2020 r.].

Polski. W zakresie niedoborów w/w artykułów przestępcy rozwinęli na szeroką skalę proceder sprzedaży fałszywych czy podrabianych produktów zdrowotnych i sanitarnych oraz środków ochrony indywidualnej i środków farmaceutycznych. Równie powszechne stały się działania w obszarze przestępczości przeciwko własności przemysłowej[784]. Zagrożenia w tym zakresie są szczególnie groźne ponieważ dotykają największych pracodawców w Unii Europejskiej. EUIPO (Urząd Unii Europejskiej ds. Własności Intelektualnej) we współpracy z Europolem oszacował w 2019 roku, że przedsiębiorstwa korzystające z patentów, wzorów przemysłowych czy praw autorskich generują około 42% PKB Unii Europejskiej. Daje to kwotę ok. 5,7 bln euro. W latach 2015 – 2018 statystyki wskazywały, iż nawet 6,8% importu do UE mogą stanowić produkty pochodzące z działalności przestępczej przeciwko własności przemysłowej. Z dużym prawdopodobieństwem można zakładać, że sytuacja wywołana pandemią będzie przyczyną wzrostu tych statystyk. Zdecydowana większość tych produktów wytwarzana jest poza Unią Europejską. 73% zatrzymanych towarów w 2017 roku na granicach UE pochodziła z Chin. Zauważalny jest trend przenoszenia tego rodzaju produkcji na teren Wspólnoty Europejskiej, co ułatwia późniejszą dystrybucję. Dla przestępców wygodną i stosunkowo bezpieczną formą jest sprowadzanie elementów składowych i łączenie ich w Europie w produkt końcowy[785].

Na początku grudnia 2020 roku Interpol wydał ostrzeżenie o możliwości prób sprzedaży przez zorganizowane grupy przestępcze podrabianych szczepionek przeciwko COVID – 19. Według Międzynarodowej Organizacji Policji przestępcy przygotowują się by z jednej strony zakłócać łańcuchy dostaw prawdziwych leków, z drugiej poprzez fałszywe strony internetowe zaspokajać popyt osób poszukujących szczepionki[786]. Odnotowano już ataki hakerskie na strony laboratoriów i instytucji zajmujących się przygotowaniem i produkcją leków. Jeden z cyberataków skierowany został na Europejską Agencję Leków (EMA) zajmującą się dopuszczaniem leków na rynek państw Unii Europejskiej, w tym między innymi szczepionek na COVID-19[787].

---

784 Tamże.

785 B. Stefanowicz, *Przestępczość związana z naruszaniem dóbr własności intelektualnej.* https://www.filipiakbabicz.com/przestepstwa-w-biznesie/2019/08/09/przestepczosc-zwiazana-z-naruszaniem-dobr-wlasnosci-intelektualnej/ [dostęp 28.12.2020 r.].

786 Interpol ostrzega: Szczepionki przeciwko COVID – 19 mogą stać się celem zorganizowanej przestępczości, https://www.tokfm.pl/Tokfm/7,171710,26566860,interpol-ostrzega-szczepionki-przeciwko-covid-19-moga-stac.html [dostęp 28.12.2020 r.].

787 W. Szczęsny, *Interpol ostrzega. Zorganizowane grupy przestępcze w 2021 roku zajmą się handlem szczepionkami*, https://polskatimes.pl/interpol-ostrzega-zorganizowane-grupy-przestepcze-w-2021-roku-zajma-sie-handlem-szczepionkami/ar/c1-15356689 [dostęp 28.12.2021 r.].

Problemy finansowe firm szczególnie z branży gastronomicznej, eventowej czy hotelarskiej stają sie kolejną szansą dla zorganizowanych grup przestępczych, które posiadają duże ilości pieniędzy szczególnie tych wymagających „wyprania". Wiele legalnych interesów może zostać przejętych na zasadzie kupna po zaniżonej cenie lub po wsparciu finansowym z lichwiarskim oprocentowaniem. Sebastian Fiedler, szef związku Niemieckich Urzędników Policji Kryminalnej, dostrzega tu ogromne niebezpieczeństwo braku kontroli i realnej wiedzy o skali zjawiska prania nielegalnych dochodów i kierowania ich do biznesu działającego zgodnie z prawem[788]. Zagrożenie to potwierdził raport, który powstał w uniwersyteckim włoskim ośrodku badawczym TransCrime pt. „Wpływ koronawirusa na przenikanie przestępczości zorganizowanej do biznesu". Autorzy raportu wyszli od założeni, że około 10% firm związanych z branżą turystyczną zagrożonych jest upadkiem, jeżeli pandemia nie zakończy się w 2020 roku. Sytuację tę z pewnością wykorzystają grupy przestępczości zorganizowanej. Potwierdzeniem raportu są słowa szefa prokuratury w Palermo Francesco Lo Voi, który powiedział: *„Silniejsze organizacje mafijne potrafią wyszukać wszystkie okazje, w których można odnieść korzyści. I to jest coś, co może teraz dotyczyć nie tylko* Włoch, *ale także innych krajów europejskich pogrążonych w kryzysie, które potem będą musiały się z niego podnieść*"[789].

Jeden z autorów raportu, Andrea Carni, podkreślił, że w wyniku pandemii może pojawić się większe społeczne przyzwolenie dla mafii. Należy jednak podkreślić, iż jest to opinia dotycząca państwa włoskiego, gdzie społeczna akceptacja dla działalności zorganizowanych grup przestępczych w różnych okresach historycznych była wysoka. Obecnie pojawiają się informacje o rozdawnictwie paczek żywnościowych przez przedstawicieli mafii. Zdaniem Nicola Gratteriego, szefa prokuratury w Catanzaro w Calabrii, jest to zabieg stosowany dla oswojenia mieszkańców i pokazanie im, że mafia jest alternatywą dla nieskutecznego państwa[790]. Jednakże pogarszająca się koniunktura gospodarcza, a wraz z nią ubożenie części grup społecznych, może wpłynąć na większą akceptację przestępczości zorganizowanej w innych krajach. Dziś nie jest jeszcze znany faktyczny wpływ pandemii na gospodarki krajów Unii. Należy jednak zakładać, iż w krajach rozwijających się kryzys będzie poważniejszy, co

[788]M. Muller, *Bezrobotni włamywacze i bezrobotni*, https://www.dw.com/pl/bezrobotni-w%C5%82amywacze-i-kieszonkowcy/a-53121131 [dostep 28.12.2020 r.].

[789]*Koronawirus we Włoszech. Turystyka nowym biznesem mafii? [Raport],* https://podroze.dziennik.pl/swiat/artykuly/6476964,koronawirus-covid-19-epidemia-turystyka-biznes-mafia.html [dostęp 28.12.2020 r.].

[790]R. Bojanowicz, *Renesans włoskich mafii. Niespodziewany efekt pandemii COVID – 19*,https://forsal.pl/artykuly/1474582,koronawirus-silne-organizacje-przestepcze-slabe-panstwo.html [dostęp 28.12.2020 r.].

może wpłynąć na pojawienie się fali imigracji. To jest kolejna okazja do czerpania zysków ze strony przestępców organizujących nielegalny przemyt ludzi[791].

Przestępstwa w sieci związane z pandemią COVID-19.

„Jeżeli jest nowa okoliczność, na której można się wzbogacić, znajdą się ludzie, którzy to wykorzystają”[792]. Zgodnie z tą sentencją już na początku pandemii, w kwietniu 2020 roku w wyniku zuchwałego cyberoszustwa, próbowano sprzedać w Indiach 182 metrowy pomnik. Była to Statua Jedności, przedstawiającą Sardara Vallabhbhai'a Patela, jednego z ojców niepodległych Indii. Oszust wycenił go na 4 miliardy USD i zadeklarował przekazanie pieniędzy rządowi Indii na walkę z pandemią[793].

Aktywność cyberprzestępców po wybuchu pandemii uległa zmianom nie tylko ilościowym, ale też jakościowym. Wszelkie instytucje zajmujące się problemem sygnalizują lawinowy wzrost cyberataków. Podczas jednego ze spotkań Rady Bezpieczeństwa ONZ, w maju 2020 roku, zaznaczono, że cybeprzestępczość nabiera tempa, a podczas pandemii liczba złośliwych emaili wzrosła o ponad 600%[794]. Natomiast w odniesieniu do zmian jakościowych, to zwiększyła się liczba ataków kierowanych na duże przedsiębiorstwa, korporacje, instytucje rządowe i te odpowiedzialne za zarządzanie kryzysowe. Celem jest uzyskiwanie maksymalnych zysków oraz spowodowanie jak największych strat po stronie podmiotu zaatakowanego. Wcześniej wiele ataków kierowano w stronę małych firm lub podmiotów w stosunku do których efektem miało być wywołanie strachu lub udowodnienie własnej skuteczności.

Podstawową przyczyną zwiększonej ilości ataków jest między innymi przesunięcie wielu aktywności do internetu, miedzy innymi lawinowy wzrost ilości osób pracujących zdalnie. Firmy zaskoczone wiosną 2020 roku pierwszą fala pandemii nie zawsze były przygotowane do bezpiecznej organizacji pracy zdalnej. Naprędce wdrażane systemy, sieci i aplikacje nie spełniały najwyższych standardów cyberzabezpieczeń co spowodowało

[791]M. Kowal, *Bankowość i finanse. Pandemia. Nowe zagrożenia dla bezpieczeństwa instytucji finasowych,* https://alebank.pl/bankowosc-i-finanse-pandemia-nowe-zagrozenia-dla-bezpieczenstwa-instytucji-finansowych/ [dostęp28.12.2020 r.].

[792] P. Borkowski, M. Bartosiewicz, *Jak COVID – 19 zmienia podejście do bezpieczeństwa w cyberprzestrzeni*, https://www.rp.pl/Dane-osobowe/305169991-Jak-COVID-19-zmienia-podejscie-do-bezpieczenstwa-w-cyberprzestrzeni.html [dostęp28.12.2020 r.]

[793]Tamże.

[794]K. Węgiel, *Zagrożenia w internecie. Mapa (anty)bezpieczeństwa*, https://domeny.pl/blog/zagrozenia-w-internecie-mapa-antybezpieczenstwa/#Phishing_+_COVID19 [dostęp29.12.2020 r.]

powstanie luk i podatności. Te oczywiście zauważyli przestępcy, wykorzystując je do realizacji przestępczych celów[795].

Jedną z najpopularniejszych metod stosowanych przez cyberprzestępców jest **phishing**. Jest to metoda polegająca na wyłudzeniu od potencjalnych ofiar wrażliwych danych takich, jak: hasła, loginy, numery kart kredytowych czy numery pesel. Dla wzbudzenia zaufania ofiar sprawcy podszywają się pod znane firmy i instytucje. Za pomocą specjalnie zmodyfikowanych informacji próbują nakłonić ofiarę do otwarcia linku prowadzącego do spreparowanej strony łudząco podobnej do prawdziwej. Za jej pośrednictwem następuje wyłudzenie podanych wyżej danych[796]. Stosowane przez przestępców oprogramowanie pozwala na przejęcie kontroli nad komputerem, rejestrowanie naciśnięć klawiszy, a w efekcie końcowym dotarcie do wrażliwych danych. W okresie pandemii przestępcy wykorzystując u ludzi lęk i niepewność oraz pragnienie uzyskania jak najbardziej wiarygodnych informacji na temat wirusa podszywają się pod organizacje rządowe, ministerstwa zdrowia, ośrodki zdrowia publicznego lub ważne osobistości w danym kraju, aby udawać wiarygodne źródła. Specjaliści zajmujący się badaniem ataków pishingowych w ramach projektu Barracuda wyodrębnili ich trzy podstawowe typy bazujące na wykorzystaniu motywu koronawirusa: oszustwo, podszywanie sie pod markę oraz włamanie do biznesowej poczty e-mail. Zespół obliczył, że do 23 marca 2020 roku 54% ataków to oszustwa, 34% - podszywanie się pod markę, 11% - wymuszenia[797]. Przykładem jednego z ataków wymuszających była próba, powtórzona 1008 razy w ciągu dwóch dni, uzyskania pieniędzy za rezygnację z zakażenia zaatakowanej wirusem osoby i jej rodziny. Atakujący powoływał się na znajomość miejsca zamieszkania ofiar. Inny rodzaj popularnego oszustwa wychwycony przez system Lentinel Barracuda, to powoływanie się na Światową Społeczność Zdrowia, która nie istnieje, ale nazwa jest zbliżona do Światowej Organizacji Zdrowia.

Najczęściej stosowane formy pishingu to:

- fałszywe polecenia rządowe oraz inicjatywy wsparcia finansowego,
- fałszywe wnioski o płatności i zwroty pieniędzy,
- oferty fałszywych szczepionek przeciwko COVID -19 lub materiałów medycznych,

[795]Sz. Palczewski, *Covid – 19 wzmacnia cyberprzestępczość. Globalna "pandemia cyberataków",* https://www.cyberdefence24.pl/covid-19-wzmacnia-cyberprzestepczosc-globalna-pandemia-cyberatkow [dostęp29.12.2020 r.].

[796]*Co to jest phishing i jak sie przed nim bronić*, https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/ [dostęp: 29.12.2020 r.].

[797]F. Shi, *Threat Spotlight: Coronawirus – Related Phishing*, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [dostęp: 29.12.2020 r.].

- złośliwe aplikacje śledzące COVID - 19 na telefony komórkowe,
- inwestycje i oferty giełdowe,
- prośby o darowizny na cele charytatywne związane z pandemią[798].

Pierwszym znanym złośliwym oprogramowaniem zgłoszonym przy wykorzystaniu tematu koronawirusa był Emotet. Pierwotnie występował jako popularny trojan bankowy. W 2019 roku stał się trojanem modułowym. Programy IBM sprawdziły, że Emotet rozpowszechniany jest w wiadomościach e-mail pochodzących z Japonii. Pozorował pochodzenie od instytucji zajmującej się opieką nad osobami niepełnosprawnymi. Pishingowe e-maile zawierały dokument, który pobierał i instalował Emotet, gdy włączano makra, co obecnie jest często wykorzystywane w dystrybucji złośliwego oprogramowania. Innym modułowym szkodliwym programem jest LokiBot, wykorzystywany do przechwytywania danych logowania. Rozpowszechniany był w dwóch kampaniach phishingowych powiązanych z koronawirusem. Jedna z nich wykorzystywała założenie załączonych faktur, które zawierały LokiBot, ale dodały przeprosiny za opóźnienie w wysłaniu faktur z powodu koronawirusa. Druga kampania podawała się za aktualizację wiadomości, która zawierała odsyłacz do złośliwego oprogramowania. Oprogramowanie Barracuda wykryło ponad 3700 wiadomości e-mail korzystających z przesyłania faktury[799].

Cyberprzestępcy coraz częściej wykorzystują złośliwe oprogramowanie przeciwko infrastrukturze krytycznej i instytucjom opieki zdrowotnej ze względu na potencjalny duży wpływ i korzyści finansowe. Ataki typu **ransomware i DDos** polegają na próbach wyłudzenia pieniędzy za pośrednictwem złośliwych stron od osób lub organizacji grożąc im rozproszonym atakiem typu odmowa usługi DDos. Wyłudzenie może mieć miejsce po przeprowadzonym ataku, jako rekompensata za jego wstrzymanie lub żądanie określonej kwoty pieniędzy może towarzyszyć groźbie przeprowadzenia ataku. W tym przypadku podmiot otrzymujący groźbę musi zdecydować czy jego systemy są w stanie przetrwać taki atak i odmówić przekazania pieniędzy lub liczyć, iż jest to groźba bez pokrycia. Ataki DDos polegają na wyczerpaniu zasobów aplikacji, witryny internetowej lub sieci, aby w ten sposób uniemożliwić korzystanie z usług przez uprawnione podmioty. Wyczerpanie zasobów następuje poprzez wysłanie do atakowanego celu lawinę śmieciowego ruchu sieciowego z różnych źródeł używając wielu

[798]S. C. Griffin, Covid – 19 increases Data Security Threats, Interpol Warns, https://www.lexology.com/library/detail.aspx?g=f5cfb491-c5f4-4644-9a48-b517f5e26dbe [dostęp:30.12.2020 r.].
[799]Tamże.

różnych protokołów sieciowych[800]. Oprogramowanie ransomware w okresie pandemii, która zmusiła sektor edukacji do przejścia na zdalny sposób kontaktu z uczniami i studentami, według dostępnych badań zostało wykorzystane o 25% razy więcej w 2020 roku w porównaniu z 2019 rokiem. Zgodnie z raportem FBI są cztery przyczyny z powodu których można spodziewać się wzrostu ataków ransomware i DDos w najbliższej przyszłości:

- łatwość dostępu dzięki misji edukacyjnej szkół w połączeniu z dodatkowym ruchem sieciowym i rozszerzoną skalą zagrożeń ze strony uczniów pobierających wiedzę w domach,
- potencjalnie duży zbiór cennych informacji do uzyskania z systemów działających w szkołach podstawowych, średnich oraz uniwersytetach,
- dostęp do dużej ilości oraz różnorodności urządzeń podłączonych do sieci, dających możliwość wykorzystania niezgodnego z prawem,
- łatwy sposób wejścia, który ułatwia przeprowadzenie ataku DDoS za pomocą narzędzi do samodzielnego ataku DDoS[801].

Atak ransomware różni się od DDos tym, że złośliwe oprogramowanie szyfruje systemy i bazy atakowanej osoby lub organizacji poprzez to stają się niemożliwe do użytkowania. Żądanie pieniędzy pojawia się po zakończeniu szyfrowania. Wprowadzenie złośliwego oprogramowania następuje najczęściej poprzez załączniki poczty e-mail. Zdaniem ekspertów firmy Kaspersky pandemia przyczyniła się do ogromnego wzrostu ilości ataków typu ransomware i DDos, co obrazuje wzrost o 217% liczby zatrzymanych ataków w drugim kwartale 2020 roku w zestawieniu do tego okresu 2019 roku. Eksperci twierdzą, że ilość ataków tego typu maleje na przełomie wiosny i lata, co związane jest z mniejszą aktywnością firm w tym okresie. Rok 2020 nie potwierdza takiej prawidłowości, ponieważ aktywność podmiotów gospodarczych tego roku w sieci była wysoka bez względu na sezon. Największą liczbę, aż 300 ataków zanotowano 9 kwietnia 2020 roku[802]. Specjaliści ostrzegają, że wraz z profesjonalizacją grupy wykorzystujące ransomware skrócą czas pomiędzy włamaniem do sieci, a pełnym jej

[800]*What is a Ransom DDos attack*, https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/ [dostęp: 29.12.2020 r.]

[801]M. Wetherbee, C. Hildenbrand, Threat Actors Target Remote Learning During Covid – 19, https://www.netscout.com/blog/threat-actors-target-remote-learning-during-covid-19 [dostęp: 30.12.2020 r.].

[802]P. Banerjee, *After ransomware, DDos attacks rose three times during coronawirus pandemic*, https://www.livemint.com/technology/tech-news/after-ransomware-ddos-attacks-rose-three-times-during-coronavirus-pandemic-11597319778730.html [dostęp: 30.12.2020 r.].

zaszyfrowaniem. Zmniejsza to szanse administratora systemu na podjęcie kroków obronnych. Zauważalne jest skracanie tego okresu z miesięcy na tygodnie, a nawet dni[803].

Specjalista ds. bezpieczeństwa z firmy Semantec uważa, że odnotowano wzrost liczby ataków DDos skierowanych na systemy Windows zainfekowane szkodliwym oprogramowaniem Chidos. Według opinii części specjalistów rosnąca ilość ataków związana jest z rosnącą liczbą serwerów Linux, które zainfekowano szkodliwym oprogramowaniem DDos. Semantec nie potrafi wskazać kto wykorzystywał Chidos do infekowania serwerów firmy oraz które z nich zostały przejęte. Większość z nich znajdowało się w Indiach, Chinach, Brazylii i Holandii. Dwa z zainfekowanych serwerów przeprowadziły analogiczne ataki na amerykańskiego dostawcę usług hostingowych oraz adres IP z siedzibą w Chinach[804].

Interpol informował o wzroście cyberataków wykorzystujących złośliwe oprogramowanie. Duży ruch w internecie związany z pandemią umożliwił włamania do sieci, **kradzieże danych**, przekierowania pieniędzy czy tworzenia **botnetów.** Jednym z najbardziej znanych takich ataków od 2016 roku jest Trickbot. Jest to sieć serwerów i zainfekowanych urządzeń na całym świecie, wykorzystywanych do przestępczej działalności. Może to być między innymi dystrybuowanie oprogramowania ransomware. Trickot jest jednym z najstarszych i największych na świecie. Microsoft wraz z innymi korporacjami prowadził w 2020 roku intensywne działania mające na celu wyłączenie go, ponieważ uznano, że może stanowić poważne zagrożenie dla wyborów prezydenckich w USA. Pomimo początkowych sukcesów, które doprowadziły do wyłączenia 62 z 69 zidentyfikowanych serwerów. Przestępcy do pozostałych siedmiu, które nie stanowiły serwerów w dosłownym tego słowa znaczeniu, a raczej rodzaj infrastruktury serwerowej, niemal natychmiast uruchomili kolejne 59. Te, poza jednym, ponownie zostały wyłączone. Z dużym prawdopodobieństwem można zakładać, iż walka z Trickbotem będzie trwała jeszcze bardzo długo[805].

Duży niepokój wśród specjalistów od cyberbezpieczeństwa wzbudza botnet InterPlanetary Storm. W maju 2019 roku wykryto jego pierwszy wariant atakujący system operacyjny Windows. Wkrótce kolejne wersje infekowały systemy Linux. Rozprzestrzeniał się w bardzo szybkim tempie. Był w stanie zainfekować ponad 13 tysięcy urządzeń w ciągu roku,

[803]D. Palmer, *Ransomware gangs are getting faster at encrypting networks. That will make them harder to stop,* https://www.zdnet.com/article/ransomware-gangs-are-getting-faster-at-encrypting-networks-that-will-make-them-harder-to-stop/ [dostęp: 30.12.2020 r.].

[804]M. J. Schwartz, *Malware Used to Launch DDos Attacks*, https://www.bankinfosecurity.com/malware-used-to-launch-ddos-attacks-a-8656 [dostęp: 30.12.2020 r.].

[805] S. Gliwa, *Największy botnet świata walczy o przetrwanie. Trickbot niczym feniks odrodzi sie z popiołów ?*, https://www.cyberdefence24.pl/najwiekszy-botnet-swiata-walczy-o-przetrwanie-trickbot-niczym-feniks-odradzi-sie-z-popiolow [dostęp: 2.01.2021 r.].

z czego 60% znajdowało się w Azji. Początkowo badacze mieli problem z ustaleniem do jakiego rodzaju przestępczej działalności jest wykorzystywany. Pracownicy firmy Bitdefender po dokonaniu analizy kodu ustalili, że botnet wykorzystywany jest jako anonimizujący serwer proxy i może być wynajmowany w systemie subskrypcyjnym. Tego rodzaju serwery wykorzystuje się do ukrywania IP użytkownika oraz usuwania wielu elementów identyfikujących między innymi cookies czy identyfikator przeglądarki. Interplanetary Storm opracowano w języku Golang, który jest coraz częściej wykorzystywany do pisania programów atakujących komputery z systemem Linux i używają SSH jako wektora ataku. Bogata baza kodu oraz tzw. przenośność powoduje ogromne zainteresowanie językiem Golang ze strony twórców złośliwego oprogramowania[806].

Agencja Unii Europejskiej (ENISA) zajmująca się bezpieczeństwem w zakresie cyberzagrożeń na terenie UE, w rocznym raporcie za 2020 rok od stycznia do kwietnia za najgroźniejsze w tym okresie uznała:

1) ataki z wykorzystaniem złośliwego kodu na stronach internetowych,
2) phishing, czyli bezpośrednie wyłudzanie poufnych informacji lub za pomocą złośliwego oprogramowania,
3) ataki na aplikacje internetowe,
4) SPAM – niechciana korespondencja,
5) ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu,
6) kradzież tożsamości
7) naruszenie poufności, integralności lub dostępności danych,
8) zagrożenia wewnętrzne powodowane przez pracowników,
9) botnety – sieci komputerów przejętych przez przestępców,
10) ingerencja fizyczna, uszkodzenia oraz kradzież,
11) wyciek danych,
12) ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych,
13) cyberszpiegostwo,

[806] *Botnet w roli anominizującego serwera do wynajęcia*, https://techno-senior.com/2020/10/21/botnet-w-roli-anonimizujacego-serwera-do-wynajecia/ [dostęp: 2.01.2021 r.].

14) kradzież kryptowalut (cryptojacking)[807].

Przeciwdziałanie zagrożeniom w cyberprzestrzeni w związku z pandemią COVID-19.

Koronawirus, który tak szybko zaatakował niemal cały świat postawił ogromne wyzwania przed lekarzami, firmami farmaceutycznymi oraz laboratoriami, aby jak najszybciej opracować sposoby leczenia, leki czy szczepionki, które pokonają wirusa. Również specjaliści w zakresie cyberbezpieczeństwa otrzymali zadanie znalezienia skutecznych narzędzi do walki z „wirusem" w sieci. Przeniesienie w czasie pandemii wielu aktywności do internetu dodatkowo zintensyfikowało działania, aby światowa sieć WWW nie została spenetrowana przez przestępców. Zagrożenie to nie tylko możliwość utraty pieniędzy, ale również fala dezinformacji i infodemii utrudniające podjęcie skutecznej walki z pandemią.

Amerykańskie Centrum Kontroli i Zapobiegania Chorób uruchomiło opracowanego przez Microsoft bota, który pomaga weryfikować COVID – 19. Rozwiązanie wykorzystuje sztuczną inteligencję w celu umożliwienia jak najbardziej spersonalizowanego dostępu pacjenta do informacji związanych ze zdrowiem poprzez naturalną konwersację. Bot jest wsparciem dla instytucji zajmujących się walką z pandemią, lekarzy, pielęgniarek, administratorów i innych pracowników służby zdrowia w zapewnieniu krytycznej opieki osobom zarażonym wirusem[808].

Wspomniana już Agencja Unii Europejskiej zajmująca się bezpieczeństwem w zakresie cyberzagrożeń na terenie UE opracowała 10 zasad jak chronić się przed atakami pishingowymi:

1. **Zastanów się nad prośbą o podanie danych osobowych i nad tym czy jest ona uprawniona.** Nie otwieraj niechcianych wiadomości e-mail od nieznanych Ci osób ani nie otwieraj podejrzanych załączników, których się nie spodziewałeś.
2. **Nigdy nie podawaj nikomu danych osobowych ani finansowych ani haseł za pośrednictwem poczty elektronicznej**.
3. **Unikaj e-maili, które nalegają, abyś działał szybko.**
   E-maile phishingowe często mają na celu wywołanie poczucia pilności lub wymagają natychmiastowego działania.

[807]15 głównych zagrożeń. Raport ENISA, https://www.gov.pl/web/baza-wiedzy/15-glownych-cyberzagrozen--raport-enisa [dostęp: 2.01. 2021r.].

[808]A. Klimczuk, *Bot pomagający w weryfikacji COVID – 19 uruchomiony w Centrum Kontroli i Zapobiegania Chorób CDC w Stanach Zjednoczonych,* https://news.microsoft.com/pl-pl/2020/03/24/bot-pomagajacy-w-weryfikacji-covid-19-uruchomiony-w-centrum-kontroli-i-zapobiegania-chorob-cdc-w-stanach-zjednoczonych/ [dostęp: 3.01.2021 r.].

4. **Poszukaj sformułowań i terminologii.**
   Oprócz phishingu cyberprzestępcy mogą również atakować określoną osobę za pomocą spear phishingu, używając pełnego imienia i nazwiska odbiorcy. Sprawdź terminy i język, które zwykle występują w typie otrzymywanej wiadomości e-mail.
5. **Sprawdź adres e-mail.**
   Sprawdź nazwę nadawcy, adres e-mail i czy domena e-mail jest zgodna z organizacją, z której pochodzi nadawca. Jeśli nie, prawdopodobnie jest to próba wyłudzenia informacji.
6. **Sprawdź łącze zanim klikniesz.**
   Zobacz swoje e-maile jako zwykły tekst, aby sprawdzić adres hiperłącza, oraz zobaczyć prawdziwe hiperłącze. Jeśli nie zgadza się z treścią wiadomości e-mail, prawdopodobnie jest to próba wyłudzenia informacji.
7. **Zwracaj uwagę na błędy ortograficzne i gramatyczne.**
   Jeśli wiadomość e-mail zawiera błędy ortograficzne, interpunkcyjne lub gramatyczne, może to być wiadomość phishingowa.
8. **Uważaj na zewnętrzne źródła rozpowszechniające informacje o COVID-19.**
   Odwiedź oficjalne strony internetowe, aby uzyskać aktualne informacje na temat COVID-19. Fałszywe wiadomości e-mail mogą wyglądać, jakby pochodziły od legalnej organizacji, ale te nigdy nie będą kontaktowały się bezpośrednio w celu uzyskania takich informacji.
9. **Chroń swoje urządzenia.**
   Zainstaluj oprogramowanie antyspamowe, antyspyware i antywirusowe i upewnij się, że są one zawsze aktualne.
10. **Odwiedź strony internetowe, wpisując samodzielnie nazwę domeny.**
    Większość firm korzysta z szyfrowania i protokołu Secure Socket Layer (SSL) / Transport Layer Security (TLS). Jeśli podczas przeglądania pojawi się błąd certyfikatu, potraktuj to jako znak ostrzegawczy[809].

Federalne Biuro Śledcze (FBI) oraz Agencja ds. Cyberbezpieczeństwa i Infrastruktury (CISA) zaproponowały rozwiązania w zakresie ograniczenia skutków ataków ransomware i DDos:

[809] Understanding and dealing with the pishing during the COVID – 19 pandemic, https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic [dostep: 3.01.2021 r.].

1) **ataki ransomware**

- FBI i CISA nie zalecają płacenia okupów,
- zgłaszaj incydenty ransomware do lokalnego biura terenowego FBI,
- regularnie twórz kopie zapasowe danych, przerwy powietrznej i zabezpieczaj hasłem kopie zapasowe offline,
- zastosuj plan odzyskiwania, aby utrzymywać i przechowywać wiele kopii wrażliwych lub zastrzeżonych danych i serwerów w fizycznie oddzielnej, bezpiecznej lokalizacji.

2) **ataki DDos**

- rozważ zarejestrowanie się w usłudze ograniczania ryzyka odmowy usługi, która wykrywa nietypowy ruch i przekierowuje go z dala od sieci,
- utwórz partnerstwo z lokalnym dostawcą usług internetowych przed zdarzeniem i współpracuj z nim w celu kontrolowania ruchu sieciowego atakującego twoją sieć,
- skonfiguruj zapory sieciowe, aby blokować nieautoryzowane adresy IP i wyłączać przekierowanie portów. Uwaga: NETSCOUT, a nawet dostawcy zapór ogniowych, ostrzegają przed używaniem zapór ogniowych do ochrony przed atakami DDoS i zamiast tego zalecają dedykowaną ochronę DDoS przed zaporami ogniowymi w celu zapewnienia właściwej ochrony[810].

Center for Internet Security (CIS) organizacja non profit zajmująca się opracowaniem i propagowaniem bezpiecznych praktyk w zakresie systemów informatycznych zaproponowała następujące rozwiązania w zakresie zabezpieczenia informatycznych urządzeń osobistych:

- stosowanie poprawek w zakresie usuwania luk w zabezpieczeniach,
- komputery domowe, wdrażanie zabezpieczeń w postaci programów antywirusowych, zapór i oprogramowania antyszpiegowskiego oraz stosowania ustawień zabezpieczeń w przeglądarkach internetowych,
- drukarki, sprawdzanie zabezpieczeń drukarki pod kątem marki i modelu aby zapewnić bezpieczeństwo urządzenia i połączenia sieciowego,
- urządzenia usb, korzystanie wyłącznie ze sprzętu certyfikowanego przechowywanego w bezpiecznych warunkach,

[810] M. Wetherbee, C. Hildebrand, *Threat Actors Target Remote Learning During COVID – 19*, https://www.netscout.com/blog/threat-actors-target-remote-learning-during-covid-19 [dostęp: 3.01.2021 r.].

- przechowywanie, informacje poufne należy umieszczać na szyfrowanych dyskach twardych komputerów lub dyskach zewnętrznych,
- fizyczne bezpieczeństwo urządzeń, w przypadku pozostawiania urządzeń bez kontroli stosować hasła blokujące. Nie udostępniać urządzeń służących do celów służbowych[811].

Podsumowanie

Pandemia COVID – 19 postawiła przed ludzkością poważne wyzwanie zwalczenia choroby, ale też rozwiązania wszelkich innych problemów, które towarzyszą nowej chorobie. Z pewnością wiele z nich pozostanie nierozwiązanych, co nie zwalnia ludzi z podejmowania prób ich złagodzenia. Do takich należą cyberzagrożenia. Zagrożenia w tym zakresie towarzyszą nam od momentu, gdy pojawiły sie komputery i zostały połączone w sieć.

Pandemia COVID -19 stworzyła nowe warunki dla przestępców wykorzystujących internet. Strach, brak rzetelnej wiedzy na temat wirusa oraz przeniesienie wielu aktywności do sieci stworzyło warunki dla przestępstw pishingowych czy ataków randsomware i DDos. Zanotowano wielokrotny wzrost tego rodzaju przestępstw z wykorzystaniem odwołań do tematów związanych z pandemią. Wiele podmiotów nieprzygotowanych do bezpiecznego funkcjonowania w sieci przy organizacji pracy zdalnej czy edukacji padło ofiarą przestępców. Organizacje międzynarodowe oraz krajowe zajmujące sie cyberbezpieczeństwem szybko dostrzegły zagrożenia wynikające z zaistniałej sytuacji. Podjęły kroki w postaci badań nad złośliwym oprogramowaniem oraz wydały zalecenia wspierające obronę przed atakami. Są to wskazówki opracowane jeszcze przed pojawieniem sie wirusa, uwzględniające jednak zmiany wprowadzone po jego pojawieniu się. Trudno oczekiwać, że stosując te zalecenia uda się w całości zwalczyć przestępczość w sieci. Przestępcy opracowują wciąż nowe sposoby atakowania celów i ważne jest, aby specjaliści w zakresie cyberbezpieczeństwa byli w stanie, jeżeli nie wyprzedzać ich ruchów, to przynajmniej reagować natychmiast po ich pojawieniu się.

Streszczenie:

Celem niniejszego opracowania jest próba przedstawienia zagrożeń w cyberprzestrzeni z jakimi mamy do czynienia od początku wybuchu epidemii oraz pandemii COVID-19.

[811]Resource Guide for Cybersecurity During the COVID – 19 Pandemic, https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/ [dostęp: 3.01.2021 r.].

Ogromne wyzwania, jakie stanęły przed ludzkością w związku z tym nieprzewidywalnym wirusem, dotyczą nie tylko sfery medycznej czy ekonomicznej, ale również bezpieczeństwa. Bardzo szybko okazało się, że są ludzie i organizacje, które wykorzystują ten trudny czas do dezinformowania, realizacji swoich partykularnych interesów bądź czerpania nienależnych zysków. Metoda analizy dostępnych źródeł oraz doświadczenie autora stanowią podstawę metodologiczną niniejszego artykułu.

Słowa kluczowe:

Cyberprzestępczość, bezpieczeństwo, pandemia COVID-19.

Key words:

Cybercrime, security, COVID-19 pandemic.

Bibliografia:

1. *15 głównych zagrożeń.* Raport ENISA, https://www.gov.pl/web/baza-wiedzy/15-glownych-cyberzagrozen--raport-enisa.
2. Banerjee P., After ransomware, DDos attacks rose three times during coronawirus pandemic, https://www.livemint.com/technology/tech-news/after-ransomware-ddos-attacks-rose-three-times-during-coronavirus-pandemic-11597319778730.html.
3. Borkowski P., Bartosiewicz M., Jak COVID – 19 zmienia podejście do bezpieczeństwa w cyberprzestrzeni, https://www.rp.pl/Dane-osobowe/305169991-Jak-COVID-19-zmienia-podejscie-do-bezpieczenstwa-w-cyberprzestrzeni.html
4. Botnet w roli anominizującego serwera do wynajęcia, https://techno-senior.com/2020/10/21/botnet-w-roli-anonimizujacego-serwera-do-wynajecia.
5. Co to jest phishing i jak sie przed nim bronić, https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/.
6. Gliwa S., Największy botnet świata walczy o przetrwanie. Trickbot niczym feniks odrodzi sie z popiołów ?, https://www.cyberdefence24.pl/najwiekszy-botnet-swiata-walczy-o-przetrwanie-trickbot-niczym-feniks-odradzi-sie-z-popiolow.
7. Griffin S. C., Covid – 19 increases Data Security Threats, Interpol Warns, https://www.lexology.com/library/detail.aspx?g=f5cfb491-c5f4-4644-9a48-b517f5e26dbe.
8. Interpol ostrzega: Szczepionki przeciwko COVID – 19 mogą stać się celem zorganizowanej przestępczości, https://www.tokfm.pl/Tokfm/7,171710,26566860,interpol-ostrzega-szczepionki-przeciwko-covid-19-moga-stac.html.
9. Kawa W., Przestępczość zorganizowana w dobie koronawirusa – próba bilansu, https://fibis.pl/zagadnienia/przestepczosc-zorganizowana-w-dobie-koronawirusa-proba-bilansu/.
10. Klimczuk A., Bot pomagający w weryfikacji COVID – 19 uruchomiony w Centrum Kontroli i Zapobiegania Chorób CDC w Stanach Zjednoczonych,

https://news.microsoft.com/pl-pl/2020/03/24/bot-pomagajacy-w-weryfikacji-covid-19-uruchomiony-w-centrum-kontroli-i-zapobiegania-chorob-cdc-w-stanach-zjednoczonych/.

11. Koronawirus we Włoszech. Turystyka nowym biznesem mafii? [Raport], https://podroze.dziennik.pl/swiat/artykuly/6476964,koronawirus-covid-19-epidemia-turystyka-biznes-mafia.html.
12. Kowal M., Bankowość i finanse. Pandemia. Nowe zagrożenia dla bezpieczeństwa instytucji finasowych, https://alebank.pl/bankowosc-i-finanse-pandemia-nowe-zagrozenia-dla-bezpieczenstwa-instytucji-finansowych/.
13. Kowal M., Bankowość i finanse. Pandemia. Nowe zagrożenia dla bezpieczeństwa instytucji finasowych, https://alebank.pl/bankowosc-i-finanse-pandemia-nowe-zagrozenia-dla-bezpieczenstwa-instytucji-finansowych/.
14. Muller M., Bezrobotni włamywacze i bezrobotni, https://www.dw.com/pl/bezrobotni-w%C5%82amywacze-i-kieszonkowcy/a-53121131.
15. Palczewski Sz., Covid – 19 wzmacnia cyberprzestępczość. Globalna "pandemia cyberataków", https://www.cyberdefence24.pl/covid-19-wzmacnia-cyberprzestepczosc-globalna-pandemia-cyberatkow.
16. Palmer D., Ransomware gangs are getting faster at encrypting networks. That will make them harder to stop, https://www.zdnet.com/article/ransomware-gangs-are-getting-faster-at-encrypting-networks-that-will-make-them-harder-to-stop/.
17. Procyk-Lewandowska, Historia pandemii na świecie, Coronawirus SARS COV-2 na tle innych pandemii, https://www.medicover.pl/o-zdrowiu/historia-pandemii-na-swiecie-koronawirus-sars-cov-2-na-tle-innych-pandemii,6788,n,168.
18. R. Bojanowicz, Renesans włoskich mafii. Niespodziewany efekt pandemii COVID – 19,https://forsal.pl/artykuly/1474582,koronawirus-silne-organizacje-przestepcze-slabe-panstwo.html
19. Resource Guide for Cybersecurity During the COVID – 19 Pandemic, https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/.
20. Schwartz M. J., Malware Used to Launch DDos Attacks, https://www.bankinfosecurity.com/malware-used-to-launch-ddos-attacks-a-8656.
21. Shi F., Threat Spotlight: Coronawirus – Related Phishing, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.
22. Stefanowicz B., Przestępczość związana z naruszaniem dóbr własności intelektualnej. https://www.filipiakbabicz.com/przestepstwa-w-biznesie/2019/08/09/przestepczosc-zwiazana-z-naruszaniem-dobr-wlasnosci-intelektualnej/.
23. Szczęsny W., Interpol ostrzega. Zorganizowane grupy przestępcze w 2021 roku zajmą się handlem szczepionkami, https://polskatimes.pl/interpol-ostrzega-zorganizowane-grupy-przestepcze-w-2021-roku-zajma-sie-handlem-szczepionkami/ar/c1-15356689.
24. Understanding and dealing with the pishing during the COVID – 19 pandemic, https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic.

25. Wetherbee M., Hildenbrand C., Threat Actors Target Remote Learning During Covid – 19, https://www.netscout.com/blog/threat-actors-target-remote-learning-during-covid-19.
26. Węgiel K., Zagrożenia w internecie. Mapa (anty)bezpieczeństwa, https://domeny.pl/blog/zagrozenia-w-internecie-mapa antybezpieczenstwa/#Phishing_+_COVID19.
27. What is a Ransom DDos attack, https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/.