Marek Piotr Stolarski*

Wpływ pandemii COVID-19 na cyberbezpieczeństwo

Streszczenie

Pojawienie się niebezpiecznego dla zdrowia i życia ludzi wirusa COVID-19 spowodowało niebezpieczny trend odstawienia na boczne tory obszarów, które w danej chwili mogły wydawać się mniej istotne w hierarchii występujących na co dzień zagrożeń, a uśpienie czujności spowodowane wybuchem globalnej pandemii okazało się być doskonałą okazją dla cyberprzestępców.

Wprowadzenie przez poszczególne państwa restrykcji dotyczących zakazu przemieszczania się czy możliwości przebywania na zamkniętych obszarach wymusiło podjęcie pracy zdalnej, żeby zachować zdolność operacyjną przedsiębiorstw do realizacji własnych celów biznesowych.

Specyfika takiej formy wykonywania obowiązków służbowych niesie za sobą ryzyko, które może być skutkiem nieświadomych decyzji pracownika pozbawionego pewnego rodzaju kontroli, jaką jest praca w bezpośrednim gronie współpracowników z użyciem firmowego sprzętu oraz firmowej infrastruktury sieciowej.

W przypadku pracy zdalnej istnieje ryzyko ataku na sieć domową pracownika, a sama specyfika pracy w miejscu zamieszkania zwiększa ryzyko korzystania ze sprzętu służbowego do celów prywatnych, tym samym zwiększa ryzyko infekcji powierzonego pracownikowi sprzętu.

Praca zdalna to również ryzyko, że pracownik padnie ofiarą przestępców podszywających się pod innych członków zespołu. Ponadto nieodpowiednie zabezpieczenie powierzonego sprzętu może przyczynić się do jego kradzieży i spowodować utratę danych lub ujawnienie ich osobom nieupoważnionym. Oprócz możliwej kradzieży poufnych informacji przestępcy mogą również dążyć do ich blokady lub zniszczenia.

W trakcie trwania pandemii nasiliła się liczba ataków ransomware, w których przestępcy szyfrują dane atakowanej organizacji i natępnie żądają określonej kwoty okupu w zamian za przekazanie kluczy deszyfrujących.

1 Dr inż. Marek Piotr Stolarski, MBA, e-mail: marek@stolarski.eu, ORCID: 0000-0002-3027-135X.

Artykuł porusza kwestie zmian organizacyjnych wprowadzonych na potrzebę walki z COVID-19, nowych okazji dla cyberprzestępców, a co za tym idzie nowych wyzwań w dziedzinie ochrony przed pojawiającymi się zagrożeniami, głównie wskazując na znaczenie świadomości użytkowników końcowych w bezpiecznym i higienicznym korzystaniu z narzędzi technologicznych.

Słowa kluczowe: COVID-19, cyberbezpieczeństwo, smishing, phishing, fałszywe strony, fałszywe wiadomości

Nagły przypadek

Zagrożenia dotykające społeczeństwa i gospodarki poszczególnych państw zazwyczaj przyjmują formę wydarzeń lokalnych charakteryzujących się różną intensywnością oraz zróżnicowanym czasem trwania. Pomimo wciąż postępującej globalizacji przeciętny obywatel danego państwa rzadko odczuwał na własnej skórze piętno kryzysu trwającego w danej chwili w innym miejscu na Ziemi. Pojawienie się w grudniu 2019 roku[1] pierwszych informacji o bardzo zaraźliwym wirusie szalejącym w chińskim mieście Wuhan nie wskazywało jeszcze na to, że kilka miesięcy później poziom aktywności życia ludzkiego na całym świecie spadnie niemal do zera. Zwrócenie praktycznie całej uwagi w stronę COVID-19 spowodowało niebezpieczny trend odstawienia na boczne tory obszarów, które w danej chwili mogły wydawać się mniej istotne w hierarchii zagrożeń. Uśpienie czujności spowodowane wybuchem globalnej pandemii stało się doskonałą okazją dla cyberprzestępców[2].

Wprowadzenie przez poszczególne państwa restrykcji dotyczących zakazu przemieszczania się czy możliwości przebywania na zamkniętych obszarach jedynie niewielkich, uprzednio określonych grup ludzi, wymusiło na kadrze kierowniczej podjęcie kroków mających na celu umożliwienie funkcjonowania działalności niezależnie od sytuacji panującej na ulicach. W związku z tym można było zaobserwować znaczny wzrost znaczenia wykonywania obowiązków zawodowych z miejsca zamieszkania z użyciem sprzętu komputerowego oraz rozmaitych narzędzi programowych. Również szkolnictwo przestawiło się na nauczanie online, umożliwiając uczniom i studentom realizację programu nauczania pomimo zamknięcia placówek oświatowych. W pierwszej połowie

1 *COVID-19 – China*, https://www.who.int/emergencies/disease-outbreak-news/item/2020-DON229 [dostęp: 17.08.2021].

2 C. Nabe, *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html [dostęp: 10.09.2021].

2020 roku także sektor e-handlu odczuł wyraźny wzrost zainteresowania zakupami online. Wzrost zainteresowania odczuły również wszelkiej maści firmy kurierskie dostarczające pod wskazany adres przedmioty zakupione w sieci[3].

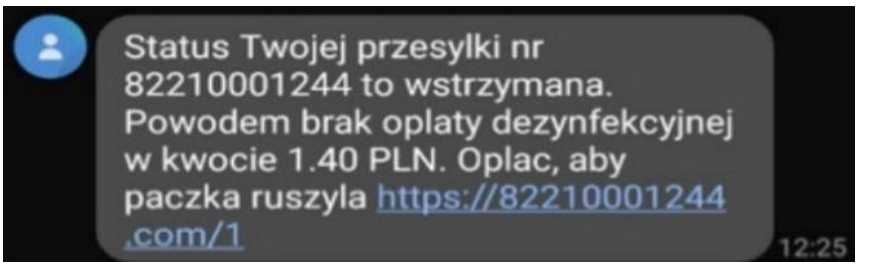
Znaczne nasilenie wykorzystania usług w domenie cyfrowej w codziennej pracy, nauce i innych dziedzinach życia spowodowało wzrost cybernetycznych działań przestępczych skupionych wokół tematu COVID-19. Metody przestępcze wraz z rozwojem ludzkości podlegają ciągłej ewolucji. W dzisiejszych czasach na całym świecie praktycznie nikt nie napada już na pociągi, a z pierwszych stron gazet zniknęły donosy o brutalnych działaniach grup przestępczych, które w latach 50. wieku XX wstrząsały ówczesną opinią publiczną. Przestępcze metody z biegiem lat uległy znacznej zmianie i z kręgów uzbrojonych osiłków przeniosły się w kręgi doskonale zorientowanych księgowych. Pokazuje to dobitnie, że zmiany społeczno-gospodarcze mają wpływ na zmianę kierunków działań przestępczych. Przestępcy działający zarówno w realnym świecie, jak i w cyberprzestrzenii z łatwością dostosowują się do panującej w danej chwili sytuacji i dostrzegają możliwości wykorzystania jej w przestępczych procederach. Na wzrost działań przestępczych w sieci mają również wpływ przeprowadzone szybko i niedokładnie procesy cyfryzacji wymuszone na podmiotach przez COVID-19.

Kliknij, bądź bezpieczny

Zarówno nagły skok w e-handlu, jak i wymuszone, szybkie przejście na zdalne wykonywanie obowiązków służbowych wywołały zainteresowanie ze strony cyberprzestępców. Już w pierwszej połowie 2020 roku pojawiły się pierwsze doniesienia o globalnych kampaniach phishingowych i smishingowych oscylujących wokół tematów panującej wówczas globalnej paniki spowodowanej błyskawicznym rozprzestrzenianiem się nowego koronawirusa. Kampanie te, które niemal w jednej chwili rozpoczęły się na całym świecie, zawierały podobnej treści wiadomości spersonalizowane pod dany rynek czy społeczeństwo. Cel tych wiadomości był jeden – skłonienie ofiar do podjęcia pewnych działań pod wpływem impulsu, który pojawiał się po przeczytaniu fałszywej wiadomości.

3 H. Gruenwald, *Parcel Delivery Services boom during Covid-19*, Norman, OK 2020.

Przestępcy dostosowali treść wiadomości tak, żeby wywołać strach, ciekawość lub przekonanie odbiorców, że należy podjąć niezwłoczne działania ze względu na ograniczenie dysponowanymi zasobami rzekomo przeznaczonymi do rozdania obywatelom przez instytucje rządowe.



Źródło: https://www.telepolis.pl/images/2021/05/cyberprzestepcy/smishing.jpg [dostęp: 9.09.2021].

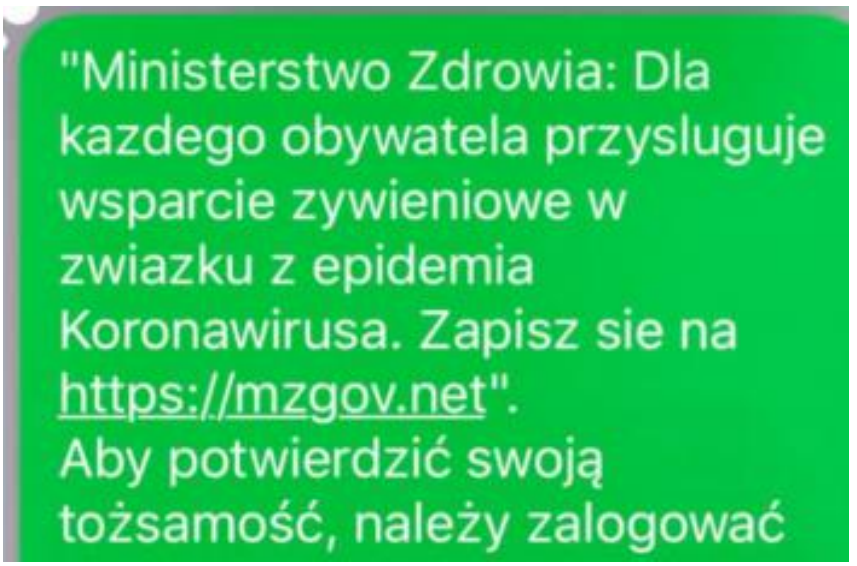
Rys. 1. Fałszywa wiadomość SMS skierowana do polskiego użytkownika

Powyższą wiadomość w pierwszej połowie 2020 roku otrzymało wielu użytkowników polskich operatorów sieci komórkowych. Wiadomości tego typu występowały w wielu różnych wariantach i zawierały różne kwoty oraz nadawców, którymi były rzekome firmy kurierskie, ale treść wiadomości dotycząca konieczności dezynfekcji paczki pozostawała niezmienna.

Źródło: https://niebezpiecznik.pl/wp-content/uploads/2020/03/smskor.png [dostęp: 9.09.2021].

Rys. 2. Fałszywa wiadomość dotycząca zaboru środków finansowych na podstawie specustawy

Wiadomość dotycząca zaboru znacznych środków finansowych z konta obywatela niewątpliwie mogła wywołać wśród potencjalnych ofiar wzburzenie oraz chęć natychmiastowej reakcji w celu zatrzymania transferu pieniędzy. W 2020 roku można było zaobserwować pewien chaos ustawowy dotyczący wytycznych podjętych w ramach walki z pandemią[4], co niewątpliwie mogło przyczynić się do nabrania przez potencjalne ofiary podejrzeń, że treść otrzymanej wiadomości może być prawdziwa.



Źródło: https://niebezpiecznik.pl/wp-content/uploads/2020/03/zapiszsie--350x232.png [dostęp: 9.09.2021].

Rys. 3. Fałszywa wiadomość informująca o rzekomych środkach pomocowych przysługujących każdemu obywatelowi

Informacja o możliwości otrzymania nieodpłatnie dodatkowych artykułów pierwszej potrzeby niewątpliwie mogła skłonić ofiarę do zapoznania się ze szczegółami „oferty". W treści powyższej wiadomości szczególną uwagę zwraca nazwa linka mająca sugerować, że prowadzi on do strony Ministerstwa Zdrowia.

4 https://bip.brpo.gov.pl/pl/raport_1/981 [dostęp: 10.08.2021].

W rzeczywistości link prowadził do podstawionej strony mającej na celu wyłudzenie danych dostępowych do konta bankowego ofiary, tym samym umożliwiał przestępcom wytransferowanie środków znajdujących się na przejętym rachunku bankowym.

Źródło: https://niebezpiecznik.pl/wp-content/uploads/2020/03/mzgovnet--768x638.png [dostęp: 9.09.2021].

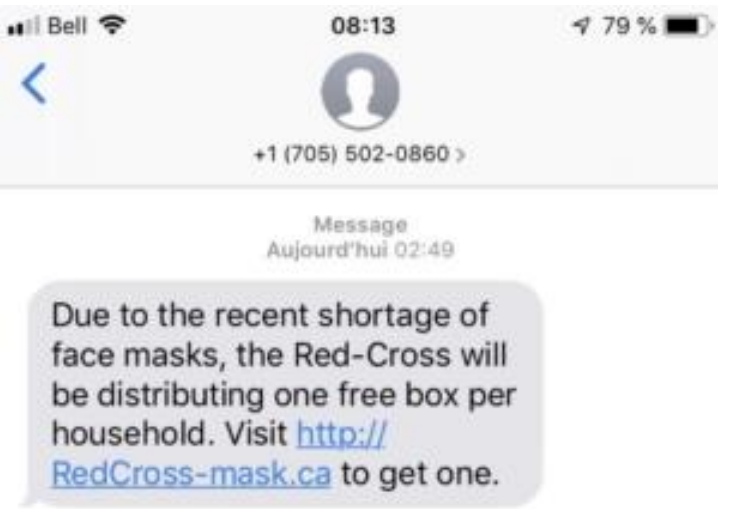
Rys. 4. Fałszywa strona mająca na celu skłonić ofiarę do udostępnienia danych pozwalających na zalogowanie się do banku

Podobnej treści wiadomości otrzymywali użytkownicy rozmieszczeni na całym globie. Pokazuje to, że kampanie mogą być prowadzone przez międzynarodowe grupy przestępcze lub wskazywać, że podobne treści sprawdzają się w większości przypadków, niezależnie od typu atakowanego społeczeństwa.

Źródło: https://www.itgovernance.co.uk/blog/wp-content/uploads/2020/04/coronavirusphishing2.jpg [dostęp: 9.09.2021].

Rys. 5. Fałszywa wiadomość wysyłana do osób korzystających z usług brytyjskich operatorów telekomunikacyjnych

Wiadomości o rzekomej wypłacie środków finansowych przeznaczonych do walki z epidemią otrzymywały również osoby zamieszkałe na Wyspach Brytyjskich i korzystające z usług tamtejszych operatorów GSM. Informacja o możliwości otrzymania rządowego wsparcia w wysokości 258 funtów szterlingów, niewątpliwie mogła skusić potencjalne ofiary do zapoznania się z „instrukcją otrzymania" pieniędzy.

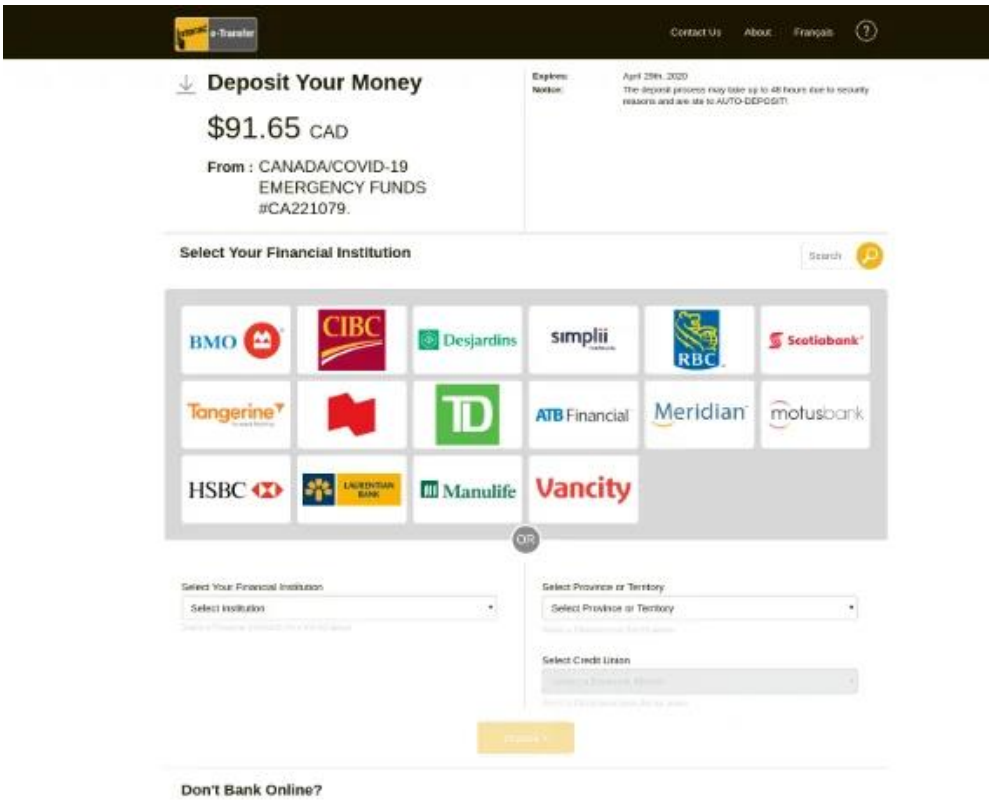


Źródło: https://www.redcross.ca/ [dostęp: 9.09.2021].

Rys. 6. Fałszywa wiadomość informująca o możliwości otrzymania za darmo pudełka zawierającego maseczki na twarz

Gwałtowny rozwój pandemii spowodował nagłe braki różnego rodzaju środków i sprzętu medycznego, w tym ochronnych rękawic jednorazowych, płynów odkażających czy zalecanych do stosowania maseczek ochronnych. W sytuacji, gdy ogromna większość jakichkolwiek zapasów takich środków została przeznaczona dla publicznych instytucji służby zdrowia[5], ceny takich produktów dla odbiorców indywidualnych urosły do niebotycznych rozmiarów, często wielokrotnie przewyższając ceny produktów obowiązujące zaledwie kilka tygodni wcześniej. Wiadomość o otrzymaniu tego typu środków za darmo z dużym prawdopodobieństwem mogła skusić ofiarę do reakcji i wykonania instrukcji zawartej w fałszywym linku.

5 M. Ważna, *W aptekach brak maseczek. „Służą przede wszystkim do ochrony osób zakażonych"*, https://www.medonet.pl/koronawirus/poradnik,w-aptekach-brak-maseczek--sluza-przede-wszystkim-do-ochrony-osob-zakazonych,artykul,67615337.html [dostęp: 15.09.2021].



Źródło: https://documents.trendmicro.com/images/TEx/articles/image002.png [dostęp: 9.09.2021].

Rys. 7. Fałszywa strona internetowa nakłaniająca ofiarę do zalogowania się na swoje konto bankowe poprzez podstawione panele logowania do popularnych banków działających w Kanadzie

Brytyjska policja informowała już w marcu 2020 roku, czyli na początku pandemii w Europie, że wykonanie przez ofiary instrukcji zawartych w fałszywych wiadomościach e-mail i SMS kosztowało je 800 tys. funtów w ciągu zaledwie jednego miesiąca[6]. Wykonywały one polecenia przestępców zawarte w wiadomościach nie tylko o treściach dotyczących konieczności wykonania dezynfekcji paczki, zaboru lub możliwości otrzymania środków finansowych lub produktów pierwszej potrzeby. Wraz z coraz większą liczbą doniesień o śmiertelnych ofiarach wirusa coraz więcej osób chciało dowiedzieć się bardziej szczegółowych informacji na temat objawów oraz przebiegu zakażenia.

6 https://www.westmercia.police.uk/news/west-mercia/news/2020/march/beware-fraud-and-scams-during-covid-19-pandemic-fraud/ [dostęp: 28.08.2021].

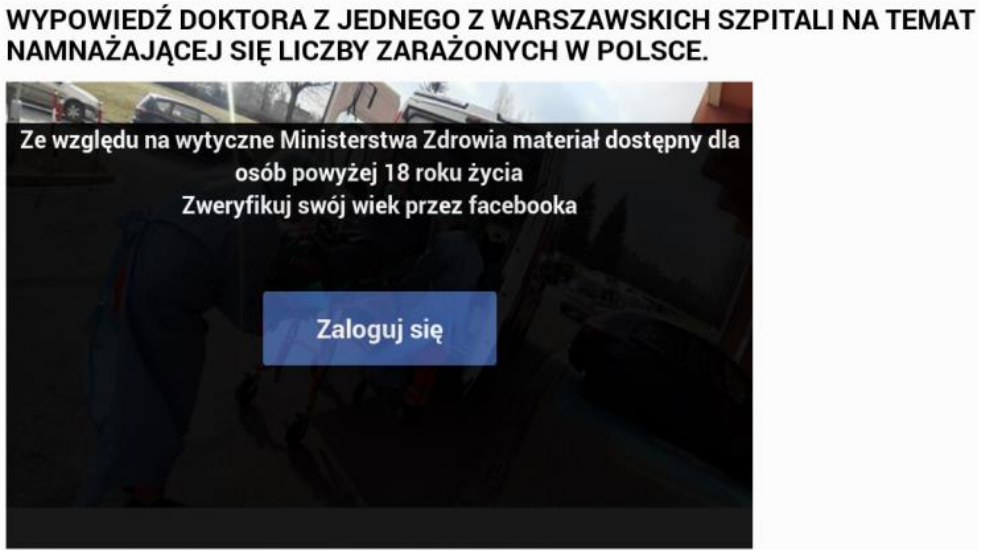
W związku z tym przestępcy na całym świecie uruchomili fałszywe strony internetowe zawierające rzekomy zbiór informacji na temat zagrożenia wirusem, a także rozpoczęli kampanie phishingowe za pośrednictwem poczty e-mail, podszywając się pod lekarzy, urzędników, a nawet przedstawicieli Światowej Organizacji Zdrowia.

Źródło: https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/ncov-email-5601.png [dostęp: 9.09.2021].

Rys. 8. Fałszywa wiadomość mająca skłonić ofiarę do pobrania załącznika zawierającego złośliwy kod

Oprócz rozsyłania fałszywych wiadomości zawierających pliki ze złośliwym kodem czy odnośniki do formularzy wyłudzających poufne dane przestępcy tworzyli również fałszywe artykuły lub całe serwisy informacyjne zawierające sensacyjne i pełne grozy doniesienia mające na celu skłonienie potencjalnej ofiary do przeczytania „artykułu". Podejmując próbę wejścia na fałszywy portal lub w fałszywy artykuł, ofiara otrzymywała powiadomienie

np. o konieczności weryfikacji wieku z wykorzystaniem panelu logowania zazwyczaj jednego z popularnych portali społecznościowych. W ten sposób przestępcy zdobywali dane dostępowe do konta ofiary.



Źródło: https://niebezpiecznik.pl/wp-content/uploads/2020/03/falsz-2-768x430.png [dostęp: 9.09.2021].

Rys. 9. Fałszywy artykuł mający na celu wyłudzenie dostępu do konta na portalu społecznościowym

Wykonanie jakiejkolwiek instrukcji zawartej w fałszywej wiadomości SMS czy w linku otrzymanym w wiadomości e-mail daje niemal 100-procentową pewność, że będzie ono miało dla ofiary poważne konsekwencje. Oprócz możliwej utraty wszystkich środków finansowych z konta bankowego zaatakowanej osoby przestępcy mogą również uzyskać dostęp do kont na portalach społecznościowych ofiary, a jeżeli osoba ta wykorzystuje sprzęt służbowy do celów prywatnych, to przestępcy mogą uzyskać dostęp do poufnych danych firmy.

Dom miejscem pracy

Wybuch pandemii miał niebagatelny wpływ na reorganizację metod pracy w wielu przedsiębiorstwach na całym świecie. Konieczność oddelegowania pracowników do pracy zdalnej, wykonywanej z ich miejsca zamieszkania, postawiła przed zespołami bezpieczeństwa dodatkowe wyzwania, których

marginalizowanie mogłoby doprowadzić do poważnej luki w systemie bezpieczeństwa danej organizacji. Według badań firmy rekrutacyjnej Devire, aż 67% firm działających na rodzimym rynku zdecydowało się na umożliwienie pracownikom pracy zdalnej[7].

Specyfika takiej formy wykonywania obowiązków służbowych niesie za sobą pewne ryzyko, które może być skutkiem nieświadomych decyzji pracownika pozbawionego pewnego rodzaju kontroli, jaką jest praca w bezpośrednim gronie współpracowników, z wykorzystaniem firmowych zasobów sprzętowych oraz firmowej infrastruktury sieciowej. W przypadku pracy zdalnej istnieje ryzyko ataku na sieć domową pracownika, a sama specyfika pracy w miejscu zamieszkania zwiększa ryzyko korzystania ze sprzętu służbowego do celów prywatnych i tym samym zwiększa ryzyko infekcji powierzonego pracownikowi sprzętu. Praca zdalna to również ryzyko, że pracownik padnie ofiarą przestępców podszywających się pod innych członków zespołu. Ponadto nieodpowiednie zabezpieczenie powierzonego sprzętu może przyczynić się do jego kradzieży i spowodować utratę danych lub ujawnienie ich osobom nieupoważnionym. Oprócz możliwej kradzieży poufnych informacji przestępcy mogą również dążyć do ich blokady lub zniszczenia. Służby całego świata wskazują na znaczne nasilenie, w trakcie trwania pandemii COVID-19, ataków ransomware, w których przestępcy szyfrują dane atakowanej organizacji i żądają określonej kwoty okupu w zamian za przekazanie kluczy deszyfrujących. W maju 2021 roku ofiarą ataku ransomware padła amerykańska firma Colonial Pipeline będąca operatorem rurociągów transportujących paliwa. W związku z atakiem działanie firmy zostało tak sparaliżowane, że musiała ona zawiesić swoją działalność. Przestępcy domagali się 4,4 mln USD okupu, który firma zdecydowała się w końcu zapłacić szantażystom. Miesiąc później Departament Sprawiedliwości Stanów Zjednoczonych poinformował, że tamtejszym służbom udało się odzyskać połowę kwoty zapłaconego okupu[8]. Raport Internet Organised Crime Threat Assessment[9] opublikowany przez

7 D. Dziwisz, *Wpływ COVID-19 na cyberbezpieczeństwo przedsiębiorstw prywatnych – konsekwencje i ryzyko nagłego przejścia na pracę zdalną*, http://www.zbn.inp.uj.edu.pl/documents/92718966/145706753/AnalizaCOVID-8-Dziwisz-1/d8729182-7b06-41a9-9329-5b67a6e537ed [dostęp: 10.09.2021].

8 *Colonial Pipeline forked over $4.4M to end cyberattack – but is paying a ransom ever the ethical thing to do?*, https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383 [dostęp: 10.09.2021].

9 https://www.europol.europa.eu/iocta-report [dostęp: 9.09.2021].

Europol w październiku 2020 roku wskazuje na zagrożenia związane z socjotechniką i inżynierią społeczną jako główną metodą wyłudzania poufnych informacji i danych dostępowych. Twórcy raportu zauważają również duże znaczenie ataków ransomware jako głównego źródła zagrożeń cybernetycznych firm i instytucji całego świata. Zaszyfrowanie infrastruktury, na której podstawie działa dana organizacja lub instytucja, może doprowadzić do sytuacji, że ich działanie zostanie uniemożliwione, a w konsekwencji zaprzestane w nieokreślonym czasie. Skuteczny atak ransomware np. na placówki medyczne w szczytowym punkcie pandemii może nieść za sobą katastrofalne w skutkach konsekwencje, tym samym przyczyniając się nawet do śmierci setek osób.

Nieubłagane statystyki

Naukowcy z WMG z University of Warwick, Abertay University, University of Kent, University of Oxford i University of Strathclyde współpracowali przy badaniu „Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemici". Ich wyniki zostały opublikowane w czasopiśmie „Computers & Security".

Wykorzystując Wielką Brytanię jako studium przypadku, dokument ujawnia wyraźny związek między ogłaszaniem przez rząd politycznych zmian i obostrzeń w związku z pandemią COVID-19 a kampaniami dotyczącymi cyberprzestępczości. Chociaż jest to wzorzec, który był podejrzewany od jakiegoś czasu, jest to pierwsza analiza z setek przypadków na całym świecie wyjaśniająca to powiązanie.

Analizując wykryte incydenty, naukowcy umiejscowili na osi czasu 43 cyberataki związane bezpośrednio z pandemią COVID-19. Ta oś czasu i jej późniejsza analiza miały pomóc w zrozumieniu tych ataków i sposobu ich funkcjonowania, a co za tym idzie, w lepszym przygotowaniu się do ich mitygacji, jeżeli kiedykolwiek wystąpią one ponownie.

Naukowcy zaangażowani w badanie odkryli, że od momentu ogłoszenia pierwszego przypadku w Chinach, co miało miejsce 8 grudnia 2019 roku, pierwszy zgłoszony cyberatak został zainicjowany dokładnie 14 dni później. Od tego momentu okresy między cyberatakami radykalnie się skróciły.

Ataki, które zaobserwowano, poddano kategoryzacji i po ich analizie stwierdzono, że:

- 86% wykorzystywało phishing i/lub smishing;
- 65% wykorzystywało złośliwe oprogramowanie;

- wynikiem 34% ataków były oszustwa finansowe;
- 15% koncentrowało się na wyłudzaniu informacji chronionych;
- 13% było zaangażowanych w pharming;
- 5% ataków to klasyczne hackerskie włamania;
- kolejne 5% dotyczyło unieruchomienia lub odmowy usługi (DoS/DDoS).

Zakończenie

Reasumując rozważania, należy stwierdzić, że przestępcy sprawnie dostosowują się do panującej w danej chwili sytuacji, potrafią tym samym dopasować swoje ataki globalnie, docierają do całych społeczeństw. Metody ich ataków to nie tylko rozsyłanie fałszywych wiadomości poprzez SMS czy e-mail, ale także zastawianie pułapek poprzez tworzenie fałszywych stron informacyjnych służących do wyłudzania danych dostępowych i innych poufnych informacji. Firmy i instytucje publiczne są obecnie narażone na ataki typu ransomware polegające na zaszyfrowaniu danych i zażądaniu przez przestępców okupu w zamian za przywrócenie stanu poprzedniego.

W obecnie panującej sytuacji i dynamicznej cyfryzacji rynku pracy polegającej na umożliwieniu pracownikom wykonywania obowiązków służbowych zdalnie z miejsca zamieszkania działy IT oraz bezpieczeństwa stanęły przed nowymi wyzwaniami, tj. zapewnieniem bezpieczeństwa organizacji przed atakami na poszczególnych pracowników, którzy nie działają w sieci firmowej oraz są rozproszeni na większym obszarze i korzystają z różnych dostawców usług sieciowych. Problemy stwarzane przez pracę zdalną nie powinny być bagatelizowane, a osoby odpowiedzialne za bezpieczeństwo teleinformatyczne organizacji powinny mieć świadomość zagrożeń mogących dotknąć ich organizację.

W przypadku użytkowników indywidualnych należy prowadzić kampanie informacyjne dotyczące różnego rodzaju prób wyłudzeń z wykorzystaniem sytuacji związanej z pandemią. Przestępcy stosują socjotechnikę i elementy inżynierii społecznej, żeby poprzez strach, ciekawość, złość czy chęć zysku skłonić ofiary do podjęcia impulsywnych i nieprzemyślanych działań mających na celu przekazanie atakującym poufnych informacji lub danych dostępowych. Rzetelne informowanie rządzących o planach i kierunkach działań w walce z pandemią może się przyczynić do poprawy cyberbezpieczeństwa obywateli, którzy odpowiednio poinformowani znacznie trudniej nabiorą się na informacje dotyczące rzekomych nakazów, zakazów lub zabieraniu czy rozdawaniu pieniędzy przez rząd.

Wybuch pandemii skierował uwagę światowej opinii publicznej na kwestie związane z ochroną zdrowia, ale należy pamiętać, że w cieniu zagrożeń biologicznych działają zagrożenia cybernetyczne mogące mieć duży wpływ na funkcjonowanie poszczególnych sektorów gospodarek świata już po zakończeniu pandemii.

Bibliografia

Colonial Pipeline forked over $4.4M to end cyberattack – but is paying a ransom ever the ethical thing to do?, https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383 [dostęp: 10.09.2021].

COVID-19 – China, https://www.who.int/emergencies/disease-outbreak-news/item/2020-DON229 [dostęp: 17.08.2021].

Dziwisz D., *Wpływ COVID-19 na cyberbezpieczeństwo przedsiębiorstw prywatnych – konsekwencje i ryzyko nagłego przejścia na pracę zdalną*, http://www.zbn.inp.uj.edu.pl/documents/92718966/145706753/AnalizaCOVID-8-Dziwisz-1/d8729182-7b06-41a9-9329-5b67a6e537ed [dostęp: 10.09.2021].

Gruenwald H., *Parcel Delivery Services boom during Covid-19*, Norman, OK 2020.

https://bip.brpo.gov.pl/pl/raport_1/981 [dostęp: 10.08.2021].

https://www.europol.europa.eu/iocta-report [dostęp: 9.09.2021].

https://www.westmercia.police.uk/news/west-mercia/news/2020/march/beware-fraud-and-scams-during-covid-19-pandemic-fraud/ [dostęp: 28.08.2021].

Nabe C., *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html [dostęp: 10.09.2021].

Ważna M., *W aptekach brak maseczek. „Służą przede wszystkim do ochrony osób zakażonych"*, https://www.medonet.pl/koronawirus/poradnik,w-aptekach-brak-maseczek--sluza-przede-wszystkim-do-ochrony-osob-zakazonych,artykul,67615337.html [dostęp: 15.09.2021].

Impact of COVID-19 pandemic on cybersecurity

Abstract

The existence of COVID-19, a virus that is dangerous to human health and life, resulted in a parlous trend of putting aside areas that at the moment might seem less important in the hierarchy of everyday threats, and the dormancy caused by the outbreak of the global pandemic turned out to be perfect opportunity for cyber criminals.

Enforcing restrictions on the prohibition of movement or the possibility of staying in closed areas by many countries, forced people to work remotely in order to maintain the operational capacity of enterprises to achieve their own business goals.

The specificity of this form of working carries a risk, which may be the result of unconscious decisions of an employee deprived of some kind of control, which is work in a direct group of colleagues, using the company's hardware resources and the company's network infrastructure.

In the case of remote work, there is also a risk of an malicious attack on the employee's home network, and the very specificity of working in the place of residence increases the risk of using work equipment for private purposes, thus increasing the risk of infection of the equipment entrusted to the employee.

Remote work also poses a risk that the employee will fall victim to criminals pretending to be other team members. In addition, inadequate protection of the entrusted equipment may contribute to its theft, thus causing data loss or disclosure to unauthorized persons. In addition to the possible theft of confidential information, criminals may also seek to block or destroy it.

The number of ransomware attacks in which criminals encrypt the data of an attacked organization and demand a certain amount of ransom in exchange for handing over decryption keys seriously increased during the pandemic.

The article addresses the issues of organizational changes introduced to fight COVID-19, new opportunities for cybercriminals, and thus new challenges cyber defenders, mainly pointing to the role of end-user awareness in the safe and hygienic use of technological tools.

Key words: COVID-19, cybersecurity, smishing, phishing, fake websites, false messages