RAFAŁ SKÓRA*

RANSOMWARE – JAKO ZAGROŻENIE DLA CYBERBEZPIECZEŃSTWA. ANALIZA PRZYPADKU ATAKU WANNACRY

Abstrakt

Artykuł ma za cel zdefiniowanie czym jest ransomware oraz jak wyglądała ewolucja tego rodzaju złośliwego oprogramowania. Kolejną kwestią poruszoną w niniejszym opracowaniu jest znalezienie odpowiedzi na pytanie – dlaczego cyberprzestępcy wybierają ransomware – jako metodę ataku? Czy należy spodziewać się wzrostu ataków tego typu w przyszłości? Analiza przypadku ataku WannaCry pozwoli ustalić: dlaczego tak szybko doszło do rozpropagowania robaka na całym świecie? Jak dużo ofiar zostało zainfekowanych? Jakie podmioty zostały ofiarami? Główną hipotezą pracy jest twierdzenie, że ransomware jest jednym z głównych cyberzagrożeń dla współczesnego państwa i przedsiębiorstwa.

Słowa kluczowe: cyberbezpieczeństwo, ransomware, WannaCry, zagrożenia cyberbezpieczeństwa, bezpieczeństwo informacji.

Informacja dla dzisiejszego państwa i biznesu staje się zasobem strategicznym, a jej właściwa ochrona i wykorzystanie mają przemożny wpływ na uzyskanie przewagi i powodzenia współczesnych narodów i przedsiębiorstw. Wraz z rozwojem technologii informacyjnych oraz Internetu systematycznie rośnie ilość przetwarzanych danych i informacji. Informacja jest podstawowym zasobem współczesnego świata, zasobem społeczeństwa informacyjnego, a w tego rodzaju społeczeństwie aktywność wszystkich podmiotów (państw, instytucji, organizacji, przedsiębiorstw) wiąże się nierozłącznie z szybkim i bezpiecznym przetwarzaniem ogromnych ilości informacji. Ich znaczenie wynika z faktu, iż autentyczna i dostępna w pożądanym czasie informacja może stanowić kluczowy czynnik sukcesu, zaś jej brak może być przyczyną klęski i niepowodzenia. Zagrożeń dla aktywów informacyjnych jest niezliczona ilość, nie sposób przygotować się do każdego z nich, nie tylko dlatego, że trudno je wszystkie zidentyfikować, ale dlatego, że będzie to

* mgr Rafał Skóra – absolwent Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, kierunek: Bezpieczeństwo wewnętrzne (2017). Kontakt e-mail: rafal.sakora@gmail.com

pochłaniało ogromne nakłady finansowe. Wobec tego ważne jest aby analizować środowisko oraz zabezpieczać te obszary które są najistotniejsze dla funkcjonowania państwa bądź firmy oraz w których istnieje najwyższe prawdopodobieństwo penetracji i wycieku informacji[1]. Jednym z dzisiejszych szybko ewoluujących zagrożeń dla państw i przedsiebiorstw w obszarze cyberbezpieczeństwa jest z ang. *Ransomware*. Wielu ekspertów, a także firm w Polsce[2] i na świecie[3] w swoich artykułach czy też raportach – zajmujących się bezpieczeństwem informacji – uznało 2016 rok jako rok ransmware'u. W branży cyberbezpieczeństwa jest on dziś jednym z głównych zagrożeń dla infrastruktury IT państw i przedsiębiorstw. Ransomware nie jest już tylko znany specjalistom zajmującym się podatnościami i zagrożeniami w cyberprzestrzeni, ale także przeszedł do mainstreamu i jest powszechnie znany z powodu dużej ilości doniesień prasowych w ogólnonarodowych mediach (w szczególności przez ostatnie ataki *ransomware* WannaCry[4] i Petya[5] w 2017 r.).

Warto zacząć od tego, czym tak naprawdę jest *ransomware*. Słowo *ransomware* wywodzi się z połączenia dwóch angielskich słów *ransom* oraz *software*. W wolnym tłumaczeniu z ang. *ransom* oznacza okup, zaś *software* oprogramowanie. Złączenie tych dwóch słów dało – Ransomware. Zatem najprostsze tłumaczenie tego słowa to „złośliwe oprogramowanie wymuszające okup czy też oprogramowanie szantażujące". Ransomware zalicza się do klasy złośliwego oprogramowania przeznaczonego specjalnie dla uzyskania zysku finansowego[6]. W przeciwieństwie do wirusów używanych podczas ataków typu z ang. *hacking* – kradzież danych – ransomwarenie nie jest przeznaczony do uzyskiwania dostępu do komputera lub systemu informatycznego aby pozyskać dane, ale w celu zablokowania części lub całości funkcjonalności systemu operacyjnego użytkownika albo zaszyfrowanie części lub całości danych znajdujących się na urządzeniu ofiary. Komputer lub urządzenie zainfekowane ransomwarem zmusza użytkownika do zapłacenia haraczu w zamian za przywrócenie kontroli nad systemem operacyjnym i dostępem do danych. Ransomware zakłóca działanie systemu komputerowego, czyniąc go niezdatnym do użytku. Sprawcy następnie wysyłają właścicielowi żądanie okupu, oczekując pieniędzy w zamian za cofnięcie dokonanych zmian czyli przywrócenie kontroli nad systemem czy uzyskanie dostępu do zaszyfrowanych danych. *Ransomware* można zatem podzielić na dwie grupy[7]:

---

1 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

2 W. Pawłowicz, *Ransomware to największe zagrożenie dla bezpieczeństwa IT*, źródło: https://www.computerworld.pl/news/Ransomware-to-najwieksze-zagrozenie-dla-bezpieczenstwa-IT,404822.html [dostęp: 20.09.2017].

3 McAfeeLabs, *Threats Report: December 2016*, https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf [dostęp: 20.09.2017].

4 R. Tomański, *Twórcy WannaCry mogli pochodzić z południowych Chin*, źródło: http://www.pap.pl/aktualnosci/news,952948,tworcy-wannacry-mogli-pochodzic-z-poludniowych-chin.html [dostęp: 20.09.2017].

5 J. Snoch, *Kolejny globalny atak ransomware. Petya zaatakował także Polskę!*, źródło: http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/kolejny-globalny-atak-ransomware-petya-zaatakowal-takze-polske.aspx [dostęp: 20.09.2017].

6 A. Liska, T. Gallo, *Ransomware. Defending Against Digital Extortion*, O'Reilly Media, USA 2016, s. 3.

7 B. Botezatu, *Czym jest ransomware?*, źródło: https://bitdefender.pl/czym-jest-ransomware-przewodnik-zapoznawczy-czesc-i [dostęp: 20.09.2017].

- blokujące część lub całość funkcji systemu. Niektóre wirusy ransomware blokują użytkownikowi dostęp do urządzenia, programów, zmniejszają moc obliczeniową urządzenia przez co staje się one często bezużyteczne;
- szyfrujące cześć lub całość danych. Tego typu ransomware szyfruje dyski i ich zawartość co uniemożliwia użytkownikowi otwieranie plików lub uruchamianie aplikacji.

Sposobów w jaki cyberprzestępcy infekują komputery złośliwym oprogramowaniem wymuszającym okup jest wiele, jednak najczęściej dochodzi do tego z wykorzystaniem[8]:

- spamu i socjotechniki. Ataki socjotechniczne są jedną z metod działania cyberprzestępców, polegają one na wywarciu wpływu lub manipulacji użytkownika danego systemu[9]. Obecnie zaobserwować można rosnącą liczbę incydentów wykorzystujących socjotechnikę, aby pozyskać informacje od osób wewnątrz danej organizacji, lub zainfekować ją złośliwym oprogramowaniem. Dobrze spreparowana wiadomość e-mail podszywająca się pod zaufany podmiot trafiająca na nieświadomego pracownika zapewnia wysokie prawdopodobieństwo skuteczności ataku;
- ataków typu z ang. *Drive by download*. Atak ten polega na tym, że do kodu strony internetowej wstrzykiwany jest złośliwy skrypt zawierający odnośnik do witryny zawierającej szkodliwe oprogramowanie. Po wejściu na zmodyfikowaną w ten sposób stronę następuje niewidoczne dla użytkownika przekierowanie do szkodliwego adresu, uruchomienie kodu zwanego *exploitem*[10], a następnie pobranie i instalacja niebezpiecznego oprogramowania na komputerze ofiary. Ataki *Drive-by download* są bardzo popularne przede wszystkim ze względu na prostotę działania i dużą skuteczność[11];
- stron internetowych. Nieświadomi użytkownicy Internetu wchodzą na strony internetowe których celem jest infekowanie komputerów czy też pobierają pliki z niezaufanych źródeł.

Zagrożenie jakim jest ransomware nie jest niczym nowym w bezpieczeństwie IT, pierwszym atakiem którego celem było zaszyfrowanie plików, a za ich odszyfrowanie żądano zapłaty okupu był atak tzw. *AIDS* znany również jako *PC-Cyborg* w 1989 r. Znaczny rozwój tego typu zagrożeń zaczął się w roku 2005 i 2006. Wraz z rozwojem kryptografii i Internetu, rozprzestrzenianie się wszelkiego rodzaju złośliwego oprogramowania stało się znacznie łatwiejsze dla cyberprzestępców, a kolejne lata umożliwiły hakerom opracowanie znacznie bardziej skutecznych metod szyfrowania niż te stosowane w ataku *PC-Cyborg*[12]. Jednak prawdziwa ewolucja i ekspansja złośliwego oprogramowania typu ransomware miała miejsce po 2013 r. a przyczyną tego są głównie trzy czynniki:

- sukces ataku *Cryptolocker* z 2013 r. który zaszyfrował dane zaskakująco dużej liczbie użytkowników i wymusił na nich okup o łącznej wartości 12 mln złotych[13]. Ransomware stał się metodą szybkiego i wysokiego zarobku;

---

8 A. Liska, T. Gallo, dz. cyt., s. 7.

9 T. Chandler, P. Wilson, *Social Engineering: The Art of Human Hacking*, Onepress, Warszawa 2013, s. 31.

10 Exploit – program mający na celu wykorzystanie błędów w oprogramowaniu.

11 N. Narine, *Ataki drive by download*, źródło: http://securelist.pl/threats/5891,ataki_drive_by_download_siec_w_oblezeniu.html [dostęp: 20.09.2017].

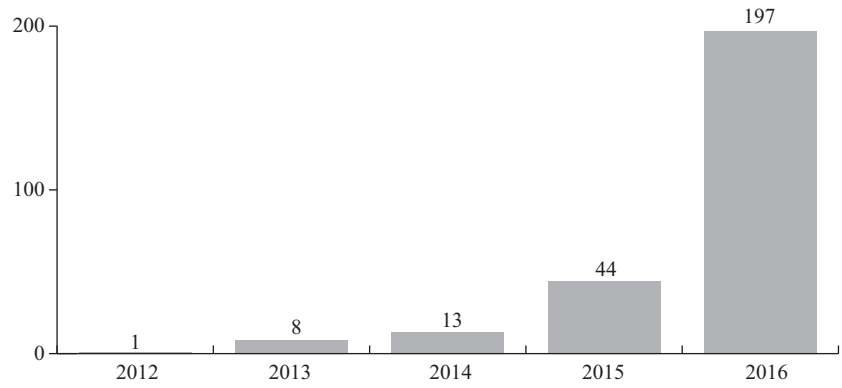
12 A. Liska, T. Gallo, *Ransomware*..., s. 5.

13 Symantec, *Ransomware and Businesses 2016*, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf [dostęp: 20.09.2017].

- rozwój kryptowalut. To nie przypadek, że ransomware upowszechnił się, kiedy w 2009 r. Bitcoin został wprowadzony jako kryptowaluta. Bitcoin pozwala cyberprzestępcom otrzymać zapłatę z zaszyfrowane pliki i pozostać anonimowym, ponieważ jest niemal niemożliwy do wyśledzenia przez organy ścigania, gdyż korzysta z sieci *peer-to-peer*[14];
- wzrastający zysk z tego typu ataków. Według badań IBM dochód cyberprzestępców w 2016 r. z tytułu oprogramowania szyfrującego wyniósł niemal 1 bilion dolarów[15]. Średni okup waha się w przedziale od 300 do 500 dolarów w BTC. Dla dużych przedsiębiorstw jest to stosunkowo niewiele w porównaniu z potencjalnymi stratami wynikającymi z utraty dostępności danych, dlatego też około 60% przedsiębiorstw płaci cyberprzestępcom okup w zamian za odzyskanie danych.

Cyberprzestępcy coraz częściej wybierają oprogramowanie szyfrujące jako metodę ataku, główną przyczyną jest zysk dużo większy niż w przypadku innego rodzaju cyberprzestępstw np. kradzieży danych osobowych klientów banku.

Wykres 1. Liczba nowych rodzin *ransomware*



Źródło: F-Secure, *State of cybersecurity 2017*, https://business.f-secure.com/the-state-of-cyber-security-2017 [dostęp: 20.09.2017].

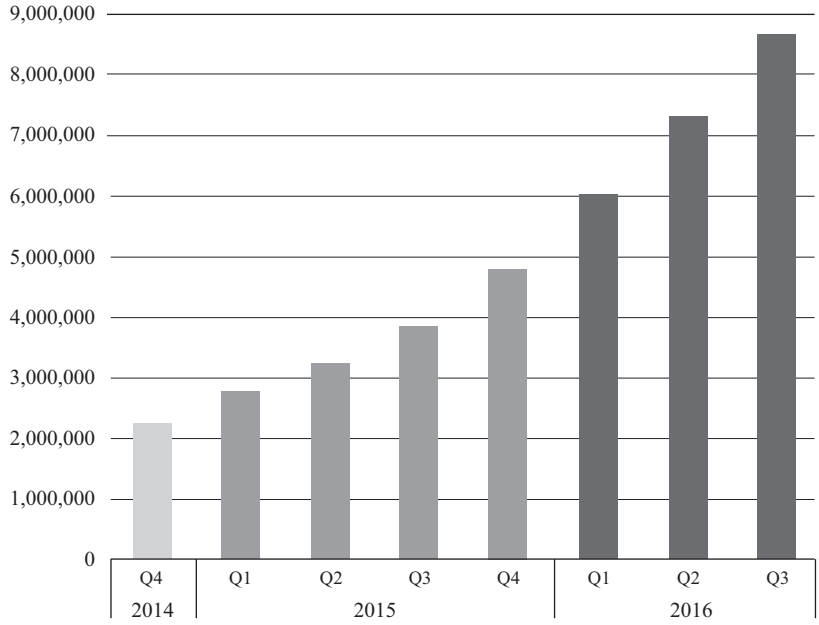
Wysokie prawdopodobieństwo pozostania anonimowym i uniknięcia wymiaru sprawiedliwości dzięki płatnościom dokonywanym w krypotowalutach oraz wysoki odsetek osób płacących okup przestępcom (relatywnie niska cena okupu wobec prawdopodobnych strat podmiotów zainfekowanych) jest przyczyną gwałtownego wzrostu nowych *rodzin ransomware* oraz liczby zainfekowanych użytkowników na przestrzeni 2013–2017 r. Na powyższym wykresie pochodzącym z raportu F-Secure widać szybki rozwój nowych wariantów ransomware'u, ich liczba podwoiła się w 2014 i 2015 roku, a w 2016 roku wzrosła niemal pięciokrotnie.

[14] M. Muszyński, *Hakerzy kochają bitcoiny. Bez wzajemności*, https://www.forbes.pl/finanse/bitcoin-podstawa-atakow-ransomware-hakerzy-go-uwielbiaja/g284n23 [dostęp: 20.09.2017].

[15] K. Torpey, *2016 Big Year for Ransomware – 70% Pays in This $1 BillionIndustry*, https://news.bitcoin.com/2016-big-year-for-ransomware-70-pays-in-this-1-billion-industry/ [dostęp: 20.09.2017].

Wzrasta nie tylko liczba wariantów złośliwego oprogramowania, ale także jego ilość w cyberprzestrzeni, wg Firmy McAfee w przeciągu dwóch lat ogólna liczba ransomware'u na świecie powiększyła się z 2 mln do aż 9 mln.

Wykres 2. Ogólna liczba *ransomware*na świecie



Źródło: McAfeeLabs, *Threats Report: December 2016*, https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf [dostęp: 20.09.2017].

Firma Google w jednym z raportów dotyczącym bezpieczeństwa Internetu z 2017 r. ostrzega, że tego typu ataki stały się *bardzo opłacalne i należy spodziewać się, że będzie do nich dochodzić w przyszłości*[16].

Pokłosiem sprzyjających warunków tego rodzaju złośliwego oprogramowania był atak z 12 maja 2017 r. Poniższy ekran pojawił się zastraszająco dużej liczbie użytkowników na niemal całym świecie w ciągu zaledwie kilku dni:

[16] PAP, *Google ostrzega przed dynamicznym rozwojem ransomware*, http://www.rp.pl/Telekomunikacja-i-IT-/170729310-Google-ostrzega-przed-dynamicznym-rozwojem-ransomware.html [dostęp: 20.09.2017].

Zdjęcie 1. Okienko informacyjne – ransmoware WannaCry

Źródło: https://zaufanatrzeciastrona.pl/post/jak-najprawdopodobniej-doszlo-do-globalnej-infekcji-ransomare-wannacry/ [dostęp: 20.09.2017].

Ransomware – WannaCry – swoim zasięgiem objął ponad 150 krajów infekując przy tym ponad 250 tys. użytkowników w ciągu tylko 2 dni. Zainfekowane komputery otrzymały nową tapetę oraz okno z informacją o ataku. Co ciekawe ransomware komunikował się z zainfekowanymi osobami w 28 różnych językach. Cyberprzestępcy najprawdopodobniej wiedzieli o tym, że znaleźli podatność, która pozwoli im osiągnąć międzynarodową skalę ataku. W okienku powyżej ofiara zostaje poinformowana o tym, że jej pliki zostały zaszyfrowane, a żeby odzyskać te dane musi zapłacić 300 dolarów (w bitcoinach). Jeżeli tego nie zrobi w przeciągu 3 dni, kwota haraczu wzrasta do 600 dolarów. Jeśli przestępcy nie otrzymają okupu w ciągu 7 dni, ofiara straci na zawsze możliwość odzyskania swoich danych (choć w przedstawionym komunikacie jest pewna sprzeczność, gdyż przestępcy zastrzegają, że jeśli ktoś jest tak *biedny*, że nie będzie w stanie zapłacić, to po 6 miesiącach przewidują uruchomienie możliwości darmowego odzyskania danych). Ofiarami ataku WannaCry zostały podmioty prywatne i publiczne; do najważniejszych z nich należą: National Health Service (służba zdrowia w Wielkiej Brytani)[17], Nissan i Renault, Telefonica[18], FedEx, VTB (Rosyjski bank), RZD (Rosyjskie koleje), Shaheen Airlines (Pakistańskie linie lotnicze) i wiele innych. Zainfekowane zostały nawet podmioty wchodzące w skład infrastruktury krytycznej państw, jak wspomniane wyżej NHS czy spółki energetyczne. Nissan i Renault wydały oficjalne oświadczenia o tym, że zostały zarażone WannaCry, a z powodu ataku

17 K. Rawlinson, *NHS leftreeling by cyber-attack: We areliterallyunable to do any x-rays*, https://www.theguardian.com/society/2017/may/13/nhs-cyber-attack-patients-ransomware [dostęp: 20.09.2017].

18 F. Palazuelos, *How the WannaCryransomwareattackaffectedbusinesses in Spain*, https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [dostęp: 20.09.2017].

linie produkcyjne stanęły, co spowodowało duże straty finansowe[19]. W przypadku National Health Service pacjenci czekający na ważną operację nie mogli skorzystać z rezonansu oraz rentgenów ponieważ urządzenia te są sterowane poprzez komputer z Windowsem XP podatnym na tego typu atak, które zostały zaszyfrowane. Jeden z pracowników brytyjskiej służby zdrowia w wywiadzie powiedział, że *część pacjentów prawdopodobnie umrze ze względu na to, że infrastruktura szpitalna nie działa poprawnie*[20]. Atak mógł być także fatalny w skutkach dla podróżujących rosyjskimi pociągami, gdyż centrum zarządzania infrastrukturą kolejową również zostało zainfekowane, a w przypadku przejęcia kontroli przez cyberprzestępców nad systemem zarzadzania ruchem lub wyłączeniem części funkcjonalnych tego systemu mogło dojść do wypadku.

Sposób działania WannaCry był następujący: kiedy ransom (*dropper exe*) zostanie osadzony na komputerze próbuje odwołać się do domeny (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) jeśli żądanie to powiedzie się, gdy taka domena istnieje – robak ten przestaje działać. Połączenie z tą domeną działa bowiem jak swoisty wyłącznik (tzw. killswitch). Kiedy analitycy badający kod źródłowy tego wirusa zauważyli, że w pierwszej kolejności próbuje on odwołać się do wspomnianej domeny od razu wykupili tą domenę, tym samym zaprzestając dalszego rozpropagowywania (Marcus Hutchins z KryptosLogic postanowił zarejestrować domenę na siebie, co zatrzymało infekowanie kolejnych komputerów). Jednak w momencie, kiedy nie było dostępu do domeny, ścieżka działania była następująca: robak skanuje sieć lokalną w poszukiwaniu komputerów, które mają wystawione usługi związane z protokołem SMB w wersji 1 i 2 są to porty 445 i 139. Następnie infekuje je poprzez dziurawy SMB i szyfruje pliki. WannaCry szyfruje pliki (179 rozszerzeń), dodając rozszerzenie WNCRY i wyświetla komunikat z żądaniem okupu. Przestępcy w komunikacie okupu na przemian pokazywali ofiarom tylko 3 adresy portfeli Bitcoin:

1. https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
2. https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
3. https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Jeden portfel zebrał 19 BTC, zaś wszystkie trzy portfele razem 52 BTC[21], a więc wpływy stanowiły łącznie około 140 tys. dolarów, co w przeliczeniu na polskie złote wynosi średnio pół miliona. Większość mediów opisywała ten atak jako *największy w historii*, jako *atak bez precedensu* jednak w rzeczywistości nie jest to do końca prawdą. W przeszłości miały miejsce podobne ataki, jednym z nich był Conficer, atak przez inną podatność, który swoim zasięgiem objął 15 mln ofiar czy wspomniany wcześniej Cryptolocker, który rozpoczął się w 2013 roku i zgromadził z okupu aż 12 mln złotych. Kampania WannaCry mimo ogromnego zasięgu nie odniosła sukcesu komercyjnego – zdecydowało się zapłacić ponad 200 osób, a całkowita suma wpłat wynosi około 140 tysięcy dolarów.

---

19 L. Frost, *Renault-Nissan isresuming production after a global Cyberattack caused stoppagesat 5 plants*, http://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5?IR=T [dostęp: 20.09.2017].

20 R. Daws, *State of the NHS' security makes you WannaCry*, https://www.telecomstechnews.com/news/2017/may/15/nhs-security-makes-you-wannacry/ [dostęp: 20.09.2017].

21 Stan na 24 lipca 2017 r.

Wobec tak szybko postępującego rozwoju złośliwego oprogramowania szyfrującego nasuwa się pytanie – jak się bronić przed ransomwarem? Przede wszystkim należy używać wspieranego aktualizacjami systemu operacyjnego, główną przyczyną tak szybkiego rozprzestrzenienia się robaka WannaCry była podatność starego systemu operacyjnego (Windowsa XP), komputery z oprogramowaniem nowszym nie zostały zainfekowane. Cyberprzestępcy nie próżnują i w miejsce jednego zablokowanego złośliwego oprogramowania tworzą kilka kolejnych wariantów. Chcąc się przed nimi zabezpieczyć, należy zawsze korzystać z aktualnego systemu operacyjnego oraz aktualizować urządzenia i oprogramowanie. Ponadto należy regularnie tworzyć kopie zapasowe, a najlepiej opracować plan kopii zapasowych i odzyskiwania. Przygotowane kopie powinno się przechowywać na osobnym, niepodłączonym do sieci urządzeniu oraz testować przywracanie systemu i plików ze zrobionych kopii zapasowych. Jeśli mimo stosowania powyższych rekomendacji użytkownik zostanie zainfekowany oprogramowaniem szyfrującym może skorzystać z inicjatywy *No More Ransom*, która została uruchomiona 25 lipca 2016 r. przez holenderską policję, Europol, Intel Security oraz Kaspersky Lab, zapoczątkowując nowy poziom współpracy między organami ścigania, a sektorem prywatnym w zakresie zwalczania oprogramowania ransomware. Celem projektu *No More Ransom* jest zapewnienie przydatnego zasobu dla ofiar oprogramowania ransomware. Użytkownicy mogą znaleźć tam informacje odnośnie tego, co to jest oprogramowanie ransomware, jak działa i co ważniejsze, jak się przed nim ochronić. W ciągu pierwszych dwóch miesięcy funkcjonowania portalu ponad 2500 osobom udało się odszyfrować swoje dane bez płacenia okupu przestępcom. Kolejnym celem inicjatywy jest uściślenie i rozwój współpracy między organami ścigania, a podmiotami sektora prywatnego w celu zwalczania tego zagrożenia[22].

Tytuł w języku angielskim:
RANSOMWARE – ONE OF THE BIGGEST THREATS IN CYBER SECURITY: CASE STUDY WANNACRY ATTACK

Bibliografia

Książki:

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.

Chandler T., Wilson P., *Social Engineering: The Art of Human Hacking*, Warszawa 2013.

Liska A., Gallo T., *Ransomware. Defending Against Digital Extortion*, USA 2016.

Raporty:

McAfee Labs, *Threats Report: December 2016*.

Symantec, *Ransomware and Businesses 2016*.

[22] Inicjatywa No More Ransom, https://www.nomoreransom.org/crypto-sheriff.php?lang=en [dostęp: 20.09.2017].

Źródła internetowe:

Botezatu B., *Czym jest ransomware?*, źródło: https://bitdefender.pl/czym-jest-ransomware-przewodnik-zapoznawczy-czesc-i [dostęp: 20.09.2017].

Daws R., *State of the NHS' security makes you WannaCry*, https://www.telecomstechnews.com/news/2017/may/15/nhs-security-makes-you-wannacry/ [dostęp: 20.09.2017].

Frost L., *Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plant*s, http://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5?IR=T [dostęp: 20.09.2017].

Inicjatywa *No More Ransom*, https://www.nomoreransom.org/crypto-sheriff.php?lang=en [dostęp: 20.09.2017].

Muszyński M., *Hakerzy kochają bitcoiny. Bez wzajemności*, https://www.forbes.pl/finanse/bitcoin-podstawa-atakow-ransomware-hakerzy-go-uwielbiaja/g284n23 [dostęp: 20.09.2017].

Narine N., *Ataki drive by download*, źródło: http://securelist.pl/threats/5891,ataki_drive_by_download_siec_w_oblezeniu.html [dostęp: 20.09.2017].

Palazuelos F., *How the WannaCry ransomware attack affected businesses in Spain*, https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [dostęp: 20.09.2017].

PAP, *Google ostrzega przed dynamicznym rozwojem ransomware*, http://www.rp.pl/Telekomunikacja-i-IT/170729310-Google-ostrzega-przed-dynamicznym-rozwojem-ransomware.html [dostęp: 20.09.2017].

Pawłowicz W., *Ransomware to największe zagrożenie dla bezpieczeństwa IT*, źródło: https://www.computerworld.pl/news/Ransomware-to-najwieksze-zagrozenie-dla-bezpieczenstwa-IT,404822.html [dostęp: 20.09.2017].

Rawlinson K., *NHS left reeling by cyber-attack: We are literally unable to do any x-rays*, https://www.theguardian.com/society/2017/may/13/nhs-cyber-attack-patients-ransomware [dostęp: 20.09.2017].

Snoch J., *Kolejny globalny atak ransomware. Petya zaatakował także Polskę!*, źródło: http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/kolejny-globalny-atak-ransomware-petya-zaatakowal-takze-polske.aspx [dostęp: 20.09.2017].

Tomański R., *Twórcy WannaCry mogli pochodzić z południowych Chin*, źródło: http://www.pap.pl/aktualnosci/news,952948,tworcy-wannacry-mogli-pochodzic-z-poludniowych-chin.html [dostęp: 20.09.2017].

Torpey K., *2016 Big Year for Ransomware – 70% Pays in This $1 Billion Industry*, https://news.bitcoin.com/2016-big-year-for-ransomware-70-pays-in-this-1-billion-industry/ [dostęp: 20.09.2017].