Anita Połowin*

Cyberzagrożenia w internecie – analiza przypadków

Streszczenie

W artykule opisano zagadnienia dotyczące ataków ransomware i specyficznych ataków phishingowych, które mają za zadanie doprowadzić do ataków ransomware. Analiza przypadku skupia się na opisie ataku ransomware oraz jego skutkach, przedstawia sposób postępowania cyberprzestępcy w celu nakłonienia użytkownika internetu do podjęcia takich działań, w których efekcie stanie się on ofiarą ataku ransomware. Celem opracowania jest zasugerowanie możliwych rozwiązań wyjścia z sytuacji, gdy użytkownik już stał się ofiarą ataku jednocześnie bez poddawania się szantażowi atakującego. Ponadto przedstawione przykłady ataków mają za zadanie nauczyć rozróżniać wiadomości phishingowe od autentycznych. W artykule wykorzystano autentyczne przykłady ataków, których omówienie pomoże zwiększyć czujność użytkowników internetu i zminimalizować skutki ewentualnego ataku cyberprzestępcy, a być może także ograniczyć liczbę ofiar ataków ransomware.

Słowa kluczowe: ransomware, phishing, smishing, cyberzagrożenia, cyberprzestępczość

* Anita Połowin, doktorantka, Akademia Sztuki Wojennej w Warszawie, e-mail: anita.144@proton.me, ORCID: 0009-0004-8429-5527.

Wstęp

Internet stał się już tak powszechny w naszym życiu, że trudno byłoby sobie wyobrazić obecnie funkcjonowania bez niego. Dużą część naszego życia spędzamy w cyberprzestrzeni, przeznaczamy czas na komunikowanie się między sobą za pomocą różnego rodzaju komunikatorów, mediów społecznościowych, kanałów i czatów, wymianę informacji, śledzenie reklam produktów, firm, usług, wyszukiwanie praktycznie wszystkiego przeniosło się do internetu, bankowość elektroniczna, zakupy w sieci, ale i bardziej wrażliwe elementy naszej tożsamości dotyczące np. elektronicznych dowodów tożsamości, elektronicznych rejestrów zdrowia, e-recept czy zwolnień lekarskich, w których zawarte są wrażliwe dane osobowe[1]. Pomimo dużego nacisku Unii Europejskiej na ochronę danych osobowych światowe firmy internetowe mają dostęp do ogromnej ilości danych obywateli, podczas gdy zwykły obywatel nie ma wiedzy o tym, kto dysponuje jego danymi, często bez udzielenia zgody na ich przetwarzanie. Przykładem jest przeglądarka internetowa, która gromadzi dane dotyczące systemu operacyjnego, adresu IP, ustawień komputera czy adresu mailowego. Z takich właśnie informacji często korzystają cyberprzestępcy. W XXI wieku cyberprzestrzeń stała się nieodzownym elementem codziennego funkcjonowania.

Wraz z przenoszeniem coraz większej ilości informacji do cyberprzestrzeni powstaje coraz więcej zagrożeń[2]. Większość zagrożeń przeniosła się do cyberprzestrzeni. Wynika to z tego, że coraz większa część ludzkiej egzystencji również przenosi się do tego środowiska. Przestępcy żyją wśród nas i także korzystają z dobrodziejstw internetu. Ponieważ płatności i zakupy przeniosły się do cyberprzestrzeni, a przestępcy dostosowali swoje działania do obecnych realiów, zatem oszustwa, wyłudzenia, kradzieże, zastraszanie i wiele innych zaczęły również funkcjonować w internecie[3].

Codziennością jest korzystanie z poczty elektronicznej, bankowości, przesyłanie informacji drogą elektroniczną. Z takiego sposobu przesyłania

1 Zob. K. Billewicz, *Ochrona danych osobowych – teoria i fikcja*, „Wiadomości Elektrotechniczne" 2014, nr 7, s. 1–2.

2 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, s. 15 i n.; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność. Wstęp do cyberbezpieczeństwa*, Toruń 2023, s. 289–391.

3 D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu" 2023, nr 53, s. 97–113.

informacji korzystają także cyberprzestępcy, i dostosowują techniki działania do obecnych technologii.

W tych korespondencjach są też przesyłane linki do stron internetowych. Chcemy komuś coś pokazać, pochwalić się czymś ciekawym, zdarza się też, że otrzymujemy korespondencję od urzędów, firm, faktury za usługi. Można zadań pytanie, czy w natłoku otrzymywanych informacji zawsze zwracamy uwagę na to, czy otrzymany e-mail jest faktycznie od tego nadawcy, od którego wydaje się, że powinien być? Wcale nie musi on pochodzić od zaufanego urzędu czy firmy, a może go jedynie łudząco przypominać.

W artykule omówiono jeden ze skutków phishingu, tj. atak ransomware. Wyjaśniono niebezpieczeństwo utraty danych spowodowane atakiem ransomware, a także utrata pieniędzy wyłudzonych przez oszustów stosujących ten atak.

Autorka podejmuje także próbę udzielenia odpowiedzi na pytanie, czy atak ransomware zawsze musi się kończyć utratą danych lub koniecznością zapłacenia okupu za odszyfrowanie danych. Dodatkowo wyjaśnia, że zapłacenie okupu atakującemu nie zawsze gwarantuje odzyskanie danych i pozbycie się problemu. Może być wręcz przeciwnie, dane mogą zostać przejęte przez atakującego i skopiowane przez niego, nie musi się on ograniczyć do zaszyfrowania dysku.

Rezultaty przeprowadzonych badań mają na celu pokazanie możliwości działań ofiary ataku, gdy komputer jest już zaszyfrowany. Okazuje się, że oprócz konieczności zapłacenia okupu są inne rozwiązania, które mogą być pomocne w odzyskaniu zaszyfrowanych danych.

Phishing i smishing

W ustawodawstwie polskim brak jest legalnej definicji phishingu. W literaturze przedmiotu wskazuje się, że phishing to metoda oszustwa polegająca na podszywaniu się pod inną osobę lub organizację[4]. Celem takiego działania jest nakłonienie ofiary do określonego działania.

Oszuści często podszywają się pod tego rodzaju instytucje, wysyłają fałszywe maile, które w treści często zawierają link do kliknięcia lub zachęcają do

4 J. Jancelewicz, *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Trzeci Sektor" 2022, nr 3–4, s. 59–60.

otworzenia załącznika, który miałby być fakturą, rachunkiem, pismem z banku czy urzędu. Tego rodzaju cyberzagrożenie nazywane jest phishingiem (od celowo błędnie napisanego słowa ang. fishing – łowić), łowienie swojej ofiary na haczyk jak wędkarz łowi rybę[5]. Phishing można podzielić na wiele rodzajów, np. ze względu na sposoby komunikacji atakującego z ofiarą. Jednym z rodzajów phishingu jest smishing[6]. To forma oszustwa polegającą na wysyłaniu fałszywych SMS-ów, najczęściej z informacją o konieczności dokonania dopłaty, zawierającą link do kliknięcia w celu uregulowania zaległości. Smishing to złożenie angielskich słów SMS i phishing. Artykuł nie koncentruje się szczegółowo na aspektach dotyczących samego zjawiska phishingu, ale na jednym z jego skutków, jako studium przypadku analizuje jeden z rodzajów ataków cyberprzestępców, do którego droga prowadzi przez zastosowanie phishingu.

Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane x

mBank przez s7.jupe.pl 14:15 (7 minut temu)
do mnie

Szanowny kliencie,

mBank

Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.

Pozdrawiamy,
Zespół mBanku

mBank S.A. z siedzibą w Warszawie przy ul. Senatorskiej 18, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość wg stanu na dzień 01.01.2013 r. wynosi 168.555.904 złotych.

Źródło: https://niebezpiecznik.pl/ [dostęp: 15.01.2024].

Rys. 1. Przykłady maili phishingowych i SMS-ów smishingowych

5 M. Podpora, *Największe zagrożenia w sieci: phishing*, https://instytutcyber.pl/publikacje/najwieksze-zagrozenia-w-sieci-phishing/ [dostęp: 4.03.2024].
6 G. Ułan, *Smishing – jak nie dać się oszukać oraz jak wspomagać i edukować innych*, https://antyweb.pl/smishing-jak-nie-dac-sie-oszukac [dostęp 13.03.2024].

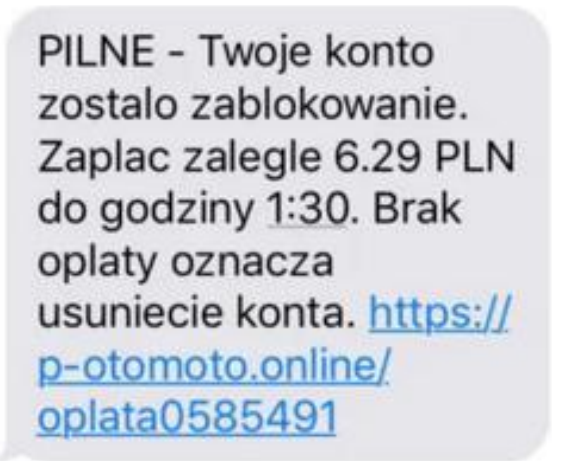
W analizowanym przypadku należy wrócić uwagę na adres nadawcy wiadomości umieszczony po nazwie mBank, tj. s7.jupe.pl, który nie jest adresem mailowym banku. Zanim klikniemy w link, kierując się obawą, czy z naszym kontem bankowym wszystko jest w porządku, warto spokojnie przyjrzeć się otrzymanej wiadomości.

Kolejnym przykładem fałszywej wiadomości zawierającej malware (rys. 2) jest podszywanie się pod znaną platformę filmową Netflix.

Źródło: https://bezpieczny.blog/ [dostęp: 16.01.2024].

Rys. 2. Przykładowe podszywanie się pod znaną platformę filmową Netflix

W analizowanym przypadku w czerwone ramki ujęto podejrzane treści, tj. nadawcę maila, adres: kontakt@twojelogo.co.pl, który nie jest adresem dostawy usługi, czyli zespołu Netflix. Ponadto na uwagę zasługuje informacja o konieczności kliknięcia w link do zalogowania się. Link jest odnośnikiem instalującym malware, najprawdopodobniej ransomware na komputerze ofiary. Dodatkowo należy też zwrócić uwagę na ostatni fragment zaznaczony na czerwono u dołu całej wiadomości. W tym przypadku pisownia jest niegramatyczna i nie ma składni polskiej. Błędy w pisowni są częste przy tego typu atakach. Należy pamiętać, że tak duża firma jak Netflix nie pozwoliłaby sobie na wysyłanie do swoich klientów informacji pisanych niepoprawnie.



Źródło: https://blog.home.pl [dostęp: 10.01.2024].

Rys. 3. Przykład ataku smishingowego

W powyższym przykładzie oszustwa smishingowego, czyli oszustwa z wykorzystaniem wiadomości SMS, ofiara jest namawiana do kliknięcia w spreparowany link, który udaje korespondencję od znanego portalu motoryzacyjny otomoto.pl. W tym przypadku należy zwrócić uwagę, że nie jest to adres tego znanego portalu, ale zupełnie inny – p-otomoto.online. W przypadku oszustów smishingowych linki łudząco podobne do oryginalnych często różnią się tylko jednym znakiem, np. tylko kropką, żeby było to trudniejsze do zauważenia i po to, żeby atak się udał. Dodatkowo w treści tej korespondencji brak jest polskich znaków, co również jest częste w tych atakach. Podobnie jak w phishingu, oszustwa smishingowe polegają na wywieraniu presji czasowej – konieczności zapłacenia określonej kwoty do podanej godziny. Żaden portal nie ustawia licznika czasu, po którego upływie nasze konto zostaje usunięte. Co do zasady

atakujący liczą w takich przypadkach na wywołanie stresu i stosowanie presji czasu po to, żeby ofiara od wpływem pośpiechu nie analizowała otrzymanej wiadomości. Jeżeli otrzymujemy prawdziwy SMS z powiadomieniami o konieczności zapłaty, to nie jest podawana godzina, do której należy uregulować należność, nawet z urzędu skarbowego, a tym bardziej portalu motoryzacyjnego. Niekiedy przy smishingu ofiara jest nakłaniana do wykonania połączenia telefonicznego, podczas którego jest automatycznie instruowana, jaki przelew pieniędzy wykonać[7].

Definiowanie sytuacji, w której ważną rolę gra czas i pośpiech, jest prawie zawsze nieodzowne w tego typu atakach. W pośpiechu ludzie często popełniają błędy, a o to właśnie chodzi cyberprzestępcom. Jest to tzw. zjawisko ataków socjotechnicznych, które są wpisane w działania cyberprzestępców wykorzystujących wyrafinowane techniki, także psychologiczne, żeby nakłonić swoją ofiarę do konkretnego zachowania[8].

Ransomware

Ransomware jest obecnie popularną metodą oszustwa stosowaną przez cyberprzestępców mającą na celu przekonanie ofiary do kliknięcia w nadesłany link udający korespondencję od zaufanej instytucji, np. urzędu, firmy. W przykładach podanych powyżej widać, że w treści takiego maila czy SMS-a często jest zawarta informacja o konieczności dopłaty za rachunek, przesyłkę, informacja o niedopłacie w urzędzie skarbowym. Co do zasady ludzie wolą mieć uregulowane rachunki i czują niepokój, gdy otrzymują takie informacje. To właśnie na takich uczuciach bazują atakujący. Należy wówczas zachować zdrowy rozsądek i powstrzymać się od klikania w nadesłany link, gdyż skutki mogą być opłakane. Warto zweryfikować otrzymaną informację i zadzwonić do instytucji czy urzędu, który jest jej nadawcą. Należy przy tym pamiętać, żeby samemu wyszukać dane do kontaktu do takiej instytucji, np. numer telefonu na stronie internetowej urzędu, żeby mieć pewność, że dzwonimy pod prawdziwy numer, a nie ten podany w korespondencji, której prawdziwość chcemy zweryfikować. Często wystarczy zapytać podczas takiej rozmowy telefonicznej, czy mamy jakąś niedopłatę lub rachunek do uregulowania. Zweryfikujemy wówczas

7 Zob. *Uwaga Smishing*, https://www.gov.pl/web/cyfryzacja/smishing [dostęp:13.03.2024].
8 Ch. Hadnagy, *Social Engineering: The Art of Human Hacking*, New Jersey 2010, s. 106–108, 131–169.

autentyczność otrzymanego maila. W ten sposób można uniknąć wielu kłopotów, np. ransomware.

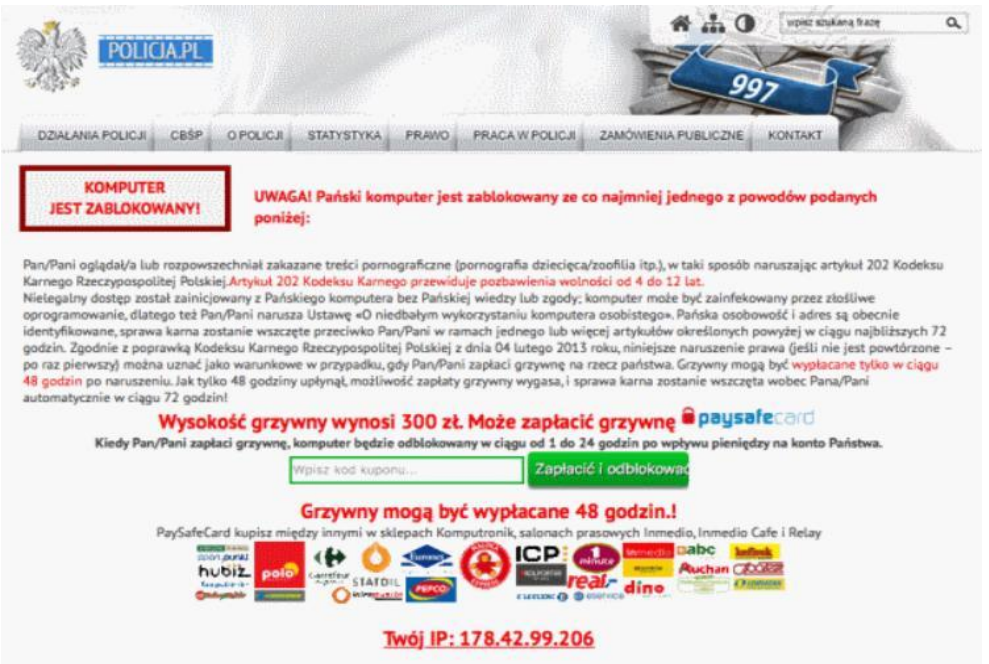
Ransomware jest jednym z ataków stosowanych przez cyberprzestępców. Jego nazwa została utworzona z angielskich wyrazów *ransom* – okup, s*oftware* – oprogramowanie[9]. Jest to oprogramowanie wymuszające na ofierze zapłacenie okupu. Pod takim nadesłanym w mailu linkiem może kryć się szkodliwe oprogramowanie określane ogólnie jako malware (***mal****icious* – złośliwe, *soft****ware*** – oprogramowanie)[10]. Ransomware jest jednym z rodzajów malware.

Co dzieje się po kliknięciu w link, pod który zaimplementowano złośliwe oprogramowanie typu ransomware? Jeżeli osoba otrzymuje maila z linkiem, pod którym kryje się złośliwe oprogramowanie typu ransomware, a wiadomość jej zdaniem jest przekonująca, to klika w taki link. Tym samym akceptuje instalację na swoim komputerze oprogramowania kryjącego się pod nadesłanym linkiem, ale, niestety tego nie widzi. Po kliknięciu otwiera się grafika danego urzędu lub spreparowana strona przekonująca, że mail jest prawdziwy. Może też nie być żadnej reakcji, jeżeli atakującemu na tym nie zależy, a chodziło jedynie o kliknięcie w link i uruchomienie ransomware na komputerze ofiary. Po instalacji pliki na dysku zostają zaszyfrowane i użytkownik traci do nich dostęp. Program szyfruje dysk komputera i blokuje do niego dostęp. Poniżej przedstawiono przykład wiadomości na ekranie komputera po uruchomieniu ransomware.

Przedmiotowa wiadomość pokazuje przykład podszywania się pod Policję. Po pierwsze należy zwróci uwagę, że w treści informacji występują liczne błędy gramatyczne. Po drugie, zawiera zapis o konieczności zapłacenia kary grzywny i czas, w jakim należy tej opłaty dokonać. Dla uwiarygodnienia programowanie zostało wyposażone także w funkcję sczytywania adresu IP komputera, na którym się znajduje. Powyższe wynika z umieszczenia na dole ekranu faktycznego adresu IP ofiary.

9 Zob. *Poradnik ransomware*, https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf [dostęp: 13.03.2024].

10 Zob. P. Alto, *Malware. What is Malware & How to Stay Protected from Malware Attacks*, https://www.paloaltonetworks.com/cyberpedia/what-is-malware [dostęp: 13.03.2024].



Źródło: https://www.ransomware.center [dostęp: 28.12.2023].

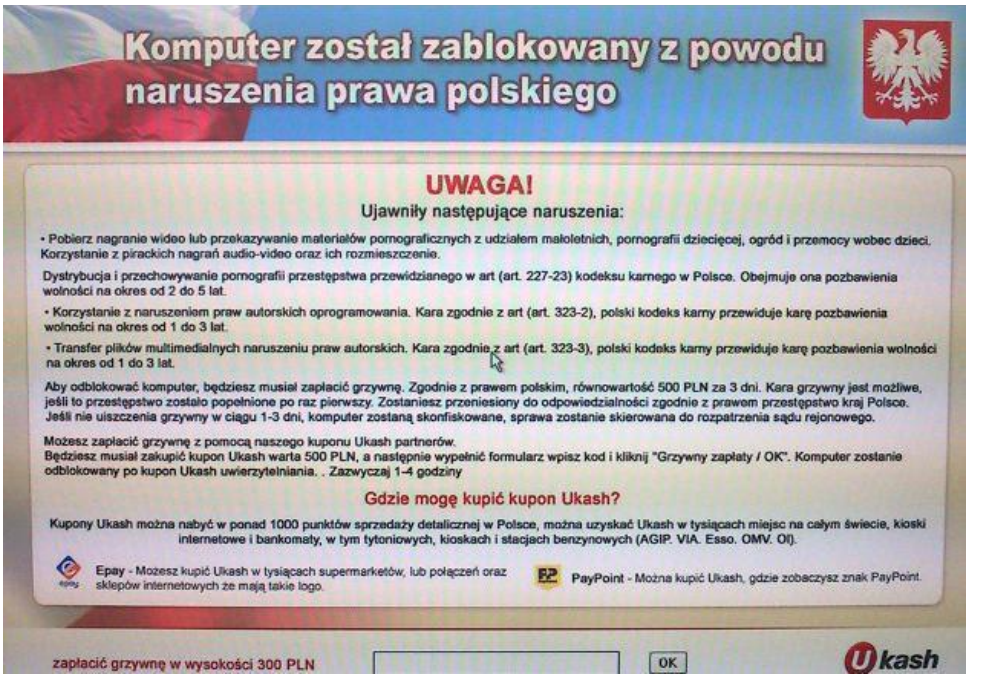
Rys. 4. Przykład wiadomości na ekranie komputera po uruchomieniu ransomware

Należy także pamiętać o tym, że żaden urząd, nawet skarbowy, ani organy ścigania nie przysyłają nam informacji z „tykającym licznikiem czasu". Jeżeli nawet nadawcą wiadomości jest urząd skarbowy i dotyczy ponaglenia w zaległej płatności, to nie będzie miało znaczenia, czy uregulujemy tę płatność zaraz czy za 2 godziny, gdy uda nam się skontaktować z urzędem i zweryfikować tę informację, albo nawet na drugi dzień. Nic nie zastąpi zdrowego rozsądku.

W przedstawionym przypadku opłata ma być uiszczona za pomocą systemu płatności Ukash. W wiadomości zawarto informację, w jaki sposób można dokonać płatności.

Ransomware blokuje użytkownikowi dostęp do komputera i uniemożliwia odczyt danych z dysku. Komputer zostaje zablokowany. Jedynym sposobem jego odblokowania – według atakującego – jest zapłacenie okupu. Jeżeli tego nie zrobi, to użytkownik straci dane bezpowrotnie. Tak brzmi najczęściej komunikat wyświetlony na ekranie. Ponadto na ekranie widnieją możliwości

zapłaty, najczęściej w kryptowalutach[11]. Atakujący podaje wówczas adres portfela kryptowalutowego do zapłaty oraz instrukcję zapłaty. Innym komunikatem jest też oskarżenie użytkownika (ofiary), że robił coś nielegalnego na komputerze i dlatego Policja zablokowała jego komputer. Należy podkreślić, że organy ścigania nie działają w ten sposób, a tego typu komunikaty są zwyczajnym oszustwem i podszywaniem się pod instytucję Policji.



Źródło: https://www.benchmark.pl [dostęp: 12.03.2024].

Rys. 5. Przykład zablokowanego przez ransomware komputera

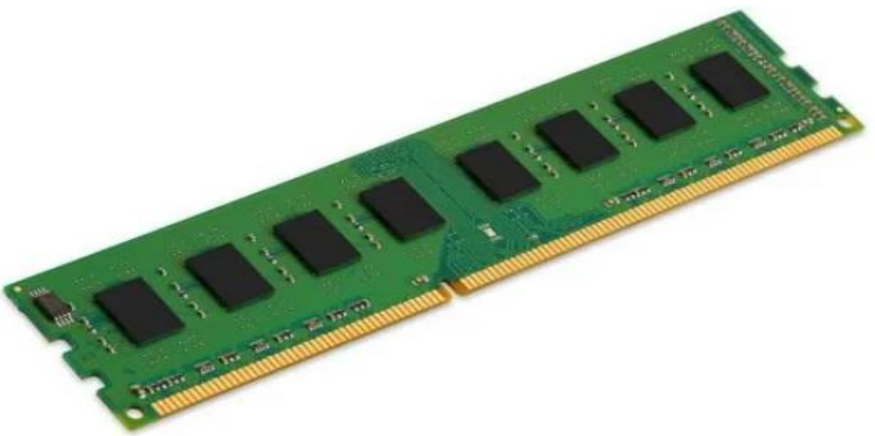
Zapłacenie żądanego okupu nie gwarantuje odszyfrowania komputera, nie zapewnia także tego, że ponownie nie zostanie on zaszyfrowany. W informacji ransomware cyberoszuści często umieszczają informację o tym, że nie tylko zaszyfrowali komputer, ale i wykradli dane znajdujące się na nim w celu szantażowania ofiary. Nie zawsze dane zostają wykradzione, ale zwykły użytkownik nie wie, co tak naprawdę w wyświetlanym komunikacie jest prawdą, a co jedynie szantażem. Dobrym rozwiązaniem jest robienie kopii zapasowych naszych danych, dlatego że możemy przywrócić z kopii zapasowej system operacyjny i dane.

11 Zob. K. Ashford, B. Curry, *What is cryptocurrency?*, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/ [dostęp: 13.03.2024].

Należy pamiętać, że zapłacenie okupu nie usuwa ransomwere z komputera nawet wtedy, kiedy atakujący odblokuje do niego dostęp, dlatego w dowolnym momencie komputer może być ponownie zaszyfrowany. Chodzi natomiast o to, żeby odzyskać dostęp do danych i usunąć ransomware, a następnie nie klikać już na podejrzane linki. Jest kilka instytucji, które na swoich stronach internetowych zamieściły wskazówki krok po kroku jak to zrobić.

Żeby zmotywować ofiarę do dokonana zapłaty, atakujący odgórnie ogranicza czas wykupu swoich plików. Zwykle po upływie tego czasu nie będzie możliwości ich odszyfrowania. Jeżeli ofiara zdecyduje się zapłacić przy użyciu karty płatniczej, to zaraz po otrzymaniu klucza deszyfrującego i odblokowaniu plików powinna zgłosić wymuszenie w swoim banku i zażądać uruchomienia procedury tzw. chargeback. Klient banku ma zawsze prawo do tej procedury, jeżeli uważa, że został poszkodowany wskutek nielegalnej transakcji. Bank uruchomi wówczas proces zwrotu środków finansowych.

Jeżeli żaden z deszyfratowów nie pomógł lub użytkownik komputera nie chce z niego korzystać ze względu na to, że nie ma pewności, czy nie pogorszy sytuacji, a zapłata nie wchodzi w grę, to pozostaje jeszcze jedna możliwość. Istnieje szansa, że klucz deszyfrujący użytego ransomware został zapisany w pamięci komputera, dlatego nie należy wyłączać komputera. Niektóre ransomware zanim zaszyfrują dysk komputera, zapisują klucz deszyfrujący w pamięci RAM komputera (ang. *random access memory* – pamięć o swobodnym dostępie*)* i jest tam dopóty, dopóki komputer jest włączony. Jest to tzw. pamięć ulotna.



Źródło: https://m.indiamart.com [dostęp: 28.12.2023].

Rys. 6. Wygląd pamięci RAM

Informacje zapisane w takiej pamięci są usuwane po odłączeniu zasilania lub po restarcie komputera. W tej pamięci przechowywane są dane niezbędne do pracy komputera, np. informacje o uruchomionych procesach systemowych i programach. Pamięć RAM służy do przechowywania tych informacji przez krótki czas. Jest ona opróżniana po wyłączeniu zasilania.

Wśród pamięci ulotnych wyróżniamy takie jej rodzaje, jak:

– SRAM (ang. *static random access memory)* – statyczna pamięć o dostępie swobodnym,

– DRAM (ang. *dynamic random access memory*++-) – dynamiczna pamięć o dostępie swobodnym[12].

Wyżej wymienione pamięci różnią się budową wewnętrzną i sposobem zapisu danych. Pamięć statyczna przechowuje dane tak długo, jak długo jest włączone zasilanie. Pamięć dynamiczna wymaga okresowego odświeżania zawartości ze względu na rozładowywanie się kondensatorów wewnątrz układu scalonego, które wykorzystywane są do zapisu informacji. Dostęp swobodny oznacza, że odczyt danych z takiej pamięci może być w dowolnej kolejności, a nie w ściśle określonej kolejce zapisu danych, jak to ma miejsce w innych rodzajach pamięci.

Dlaczego właśnie pamięć RAM jest tak istotna w przypadku ataku ransomware? W tej pamięci często jest zapisywany klucz deszyfrujący do odszyfrowania danych, do których ofiara nie ma dostępu po ataku ransomware. Jeżeli uda się go odczytać z tej pamięci, to będzie możliwe odszyfrowanie danych bez płacenia okupu, pod warunkiem, że nie zostało odłączone zasilania i zawartość pamięci nie została wykasowana.

Istnieją programy komputerowe, dzięki którym można próbować odszyfrować dysk, zwłaszcza w przypadku starszych programów do ransomware. Wszystkie one w celu usunięcia oprogramowania, które zaszyfrowało dane czy dysk, wymagają restartu komputera, żeby mogły działać. Jeżeli zastosowany program do usuwania ransomware będzie skuteczny, to zostanie odzyskany dostęp do danych, jeśli jednak nie, to podczas ponownego uruchomienia zostaje wykasowana pamięć RAM i klucz deszyfrujący oprogramowania, które zaszyfrowało zaatakowany dysk. Tym samym szansa wydobycia z pamięci klucza deszyfrującego jest stracona.

Po ataku ransomware ofiara powinna przede wszystkim upewnić się, że komputer jest podłączony do zasilania. Kolejnym krokiem jest skontaktowanie

12 Zob. *Pamięć RAM*, https://ckziumragowo.pl/kontakt [dostęp: 13.03.2024].

się z organami ścigania w celu zgłoszenia zaistniałej sytuacji. Specjaliści z Centralnego Biura Zwalczania Przestępczości Policji dysponują oprogramowaniem, które jest w stanie odczytać z pamięci RAM klucz deszyfrujący i odszyfrować nasze dane. Należy pamiętać, żeby nie wyłączać komputera, a zaraz po jego przyniesieniu na komisariat poprosić o podłączenie go do zasilania.

Należy zauważyć, że nie zawsze możliwe jest odczytanie klucza deszyfrującego. Jeżeli jednak utrata plików byłaby poważnym kłopotem, to warto jest podjąć takie próby. Pomoże to po pierwsze uniknąć płacenia okupu za odszyfrowanie (o ile ono w ogóle miałoby miejsce nawet po dokonaniu takiej opłaty), po drugie, odzyskać dostęp do komputera. W razie zabezpieczenia komputera przez uprawnione organy istniej możliwość zablokowania złośliwej strony internetowej nadawcy maila lub nawet ustalenia sprawcy tego incydentu. Tego typu działania są możliwe jedynie wtedy, kiedy ofiara zgłosi się ze sprzętem do organów ścigania.

Zakończenie

Przeprowadzone rozważania pozwalają stwierdzić, że uważne i ostrożne podchodzenie do maili nieznanego pochodzenia, sprawdzanie informacji w nich zawartych i weryfikowanie wiadomości pozwalają na ograniczenie potencjalnego ataku ransomware. Warto podkreślić, że ransomware nie dotyczy każdego użytkownika sieci i zawsze. Ważne jest, żeby przed podjęciem jakiegokolwiek działania, np. klikania w link, weryfikować adresy stron internetowych, oraz czytać komunikaty, jakie się wyświetlają zanim. Podczas poruszania się w internecie, jak wszędzie, należy zachować środki ostrożności, a wiele ataków będzie do uniknięcia. Należy pamiętać, że nic nie zastąpi zdrowego rozsądku, dlatego po otrzymaniu maili czy SMS-ów z informacją o zapłacie, dopłacie, linkiem do kliknięcia warto być podejrzliwym i bez niepożądanych emocji przyjrzeć się otrzymanej informacji zanim zrobimy następny krok. W ocenie autorki najczęstszymi powodami, przez które ludzie stają się ofiarami ataków ransomware, jest zdenerwowanie, pośpiech, niedokładne czytanie otrzymanej wiadomości, niezwracanie szczególnej uwagi na błędy w treści korespondencji.

Bibliografia

Alto P., *Malware. What is Malware & How to Stay Protected from Malware Attacks.* https://www.paloaltonetworks.com/cyberpedia/what-is-malware [dostęp: 13.03.2024].
Ashford K., Curry B., *What is cryptocurrency?*, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/ [dostęp: 13.03.2024].
Billewicz K., *Ochrona danych osobowych – teoria i fikcja*, „Wiadomości Elektrotechniczne" 2014, nr 7.
Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność. Wstęp do cyberbezpieczeństwa*, Toruń 2023.
Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Hadnagy Ch., Social Engineering: The Art of Human Hacking, New Jersey 2010.
Jancelewicz J., *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Trzeci Sektor" 2022, nr 3–4.
Pamięć RAM, https://ckziumragowo.pl/kontakt [dostęp: 13.03.2024].
Podpora M., *Największe zagrożenia w sieci: phishing*, https://instytutcyber.pl/publikacje/najwieksze-zagrozenia-w-sieci-phishing/ [dostęp: 4.03.2024].
Poradnik ransomware, https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf [dostęp: 13.03.2024].
Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu" 2023, nr 53.
Ułan G., *Smishing – jak nie dać się oszukać oraz jak wspomagać i edukować innych*, https://antyweb.pl/smishing-jak-nie-dac-sie-oszukac [dostęp: 13.03.2024].
Uwaga Smishing, https://www.gov.pl/web/cyfryzacja/smishing [dostęp: 13.03.2024].

Cybertreats on the Internet – Case Analysis

Abstract

The article describes issues regarding ransomware attacks and specific phishing attacks that are intended to lead to ransomware attacks. The aim of the study is to suggest possible solutions to overcome the situation when the user has already become a victim of an attack without succumbing to the attacker's blackmail. Moreover, the examples of attacks presented are intended to teach how to distinguish phishing messages from authentic ones. The article uses real examples of attacks, the discussion of which will help increase the vigilance of Internet users and minimize the effects of a possible cybercriminal attack, and perhaps also reduce the number of victims of ransomware attacks.

Key words: ransomware, phishing, smishing, cybertreats, cybercriminals