openAudit
Bezpieczeństwo szyte na miarę

RANSOMWARE – REALNE ZAGROŻENIE DLA DANYCH

Analiza

Bezpieczeństwo biznesu każdej organizacji zależne jest od jej wizerunku w oczach klientów. Spektakularne włamania do systemów teleinformatycznych, ataki socjotechniczne, na które narażeni są pracownicy firm skutkują ogromnym ryzykiem, odpowiedzialnością karną oraz zaburzeniem stabilności prowadzonej firmy.

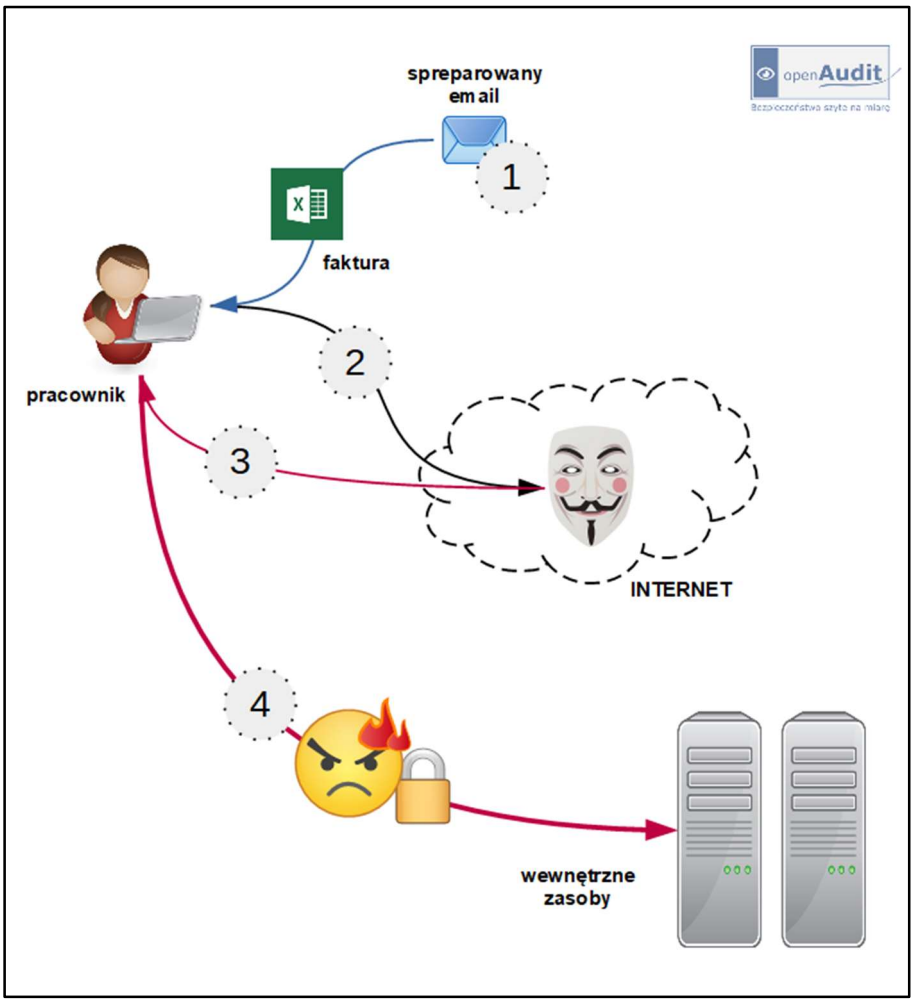
I. WPROWADZENIE

Ataki wykorzystujące pocztę elektroniczną są bardzo powszechne od czasu rozpowszechnienia się tej metody komunikacji zarówno wśród użytkowników prywatnych, jak i firm czy instytucji. Cele wykorzystywane w tych atakach są proste: kradzież lub zniszczenie danych dla osiągnięcia korzyści finansowych. „Phishing", bo o nim tu mowa jest wciąż jedną z najczęściej wykorzystywanych metod ataków wykorzystujących socjotechnikę – w tym słabości ludzkie.

II. JAKIE ZASOBY SĄ ZAGROŻONE TYM TYPEM ATAKU?

Złośliwe oprogramowanie typu Ransomware jest bardzo agresywne. Podstawową jego aktywnością jest przeszukiwanie lokalnej sieci pod kątem działających w niej urządzeń (systemów) oraz wykrywanie udostępnionych zasobów plikowych, baz danych czy repozytoriów kopii bezpieczeństwa. Oprogramowanie to stanowi zagrożenie dla **integralności, poufności i dostępności** wartościowych danych dla organizacji, ponieważ pliki są usuwane lub szyfrowane. W każdym scenariuszu aktywności tego oprogramowania, organizacja traci dostęp do danych.

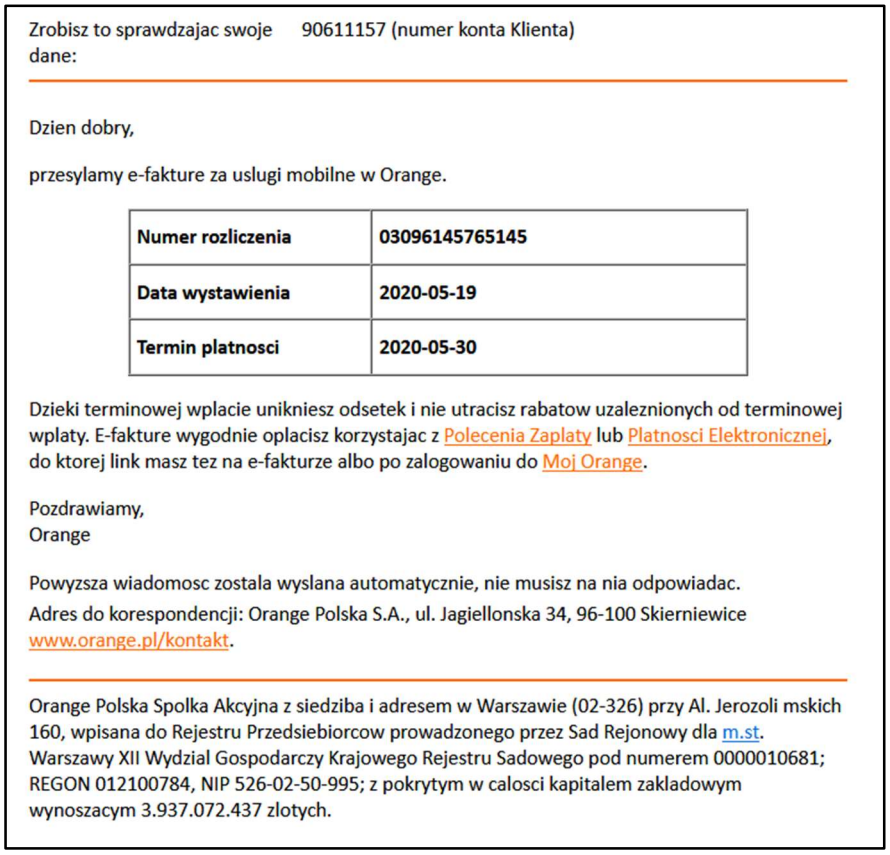
III. SCENARIUSZ ATAKU



Rysunek 1 Scenariusz ataku

Scenariusz ataku jest bardzo prosty, ale wciąż odnotowywane są duże ilości ofiar na całym świecie - w tym w Polsce.

- **KROK 1: Odebranie spreparowanej wiadomości.** Osoba obsługująca główne skrzynki pocztowe otrzymuje wiadomość email, która do złudzenia przypomina otrzymywane do tej pory wiadomości za usługi telekomunikacyjne (**Rysunek 2**). Bez chwili wahania, wiadomość zostaje przekazana dalej do działu księgowości oraz do działu ogólnego, zarządzającego całą organizacją. W zależności od organizacji kampanii phishingowej, do wiadomości email może być dołączony plik z fałszywą fakturą lub mogą być to odnośniki do takich materiałów zlokalizowanych na różnych zasobach w sieci Internet.



Zrobisz to sprawdzajac swoje dane: 90611157 (numer konta Klienta)

Dzien dobry,

przesylamy e-fakture za uslugi mobilne w Orange.

Numer rozliczenia	**03096145765145**
Data wystawienia	**2020-05-19**
Termin platnosci	**2020-05-30**

Dzieki terminowej wplacie unikniesz odsetek i nie utracisz rabatow uzaleznionych od terminowej wplaty. E-fakture wygodnie oplacisz korzystajac z Polecenia Zaplaty lub Platnosci Elektronicznej, do ktorej link masz tez na e-fakturze albo po zalogowaniu do Moj Orange.

Pozdrawiamy,
Orange

Powyzsza wiadomosc zostala wysłana automatycznie, nie musisz na nia odpowiadac.
Adres do korespondencji: Orange Polska S.A., ul. Jagiellonska 34, 96-100 Skierniewice
www.orange.pl/kontakt.

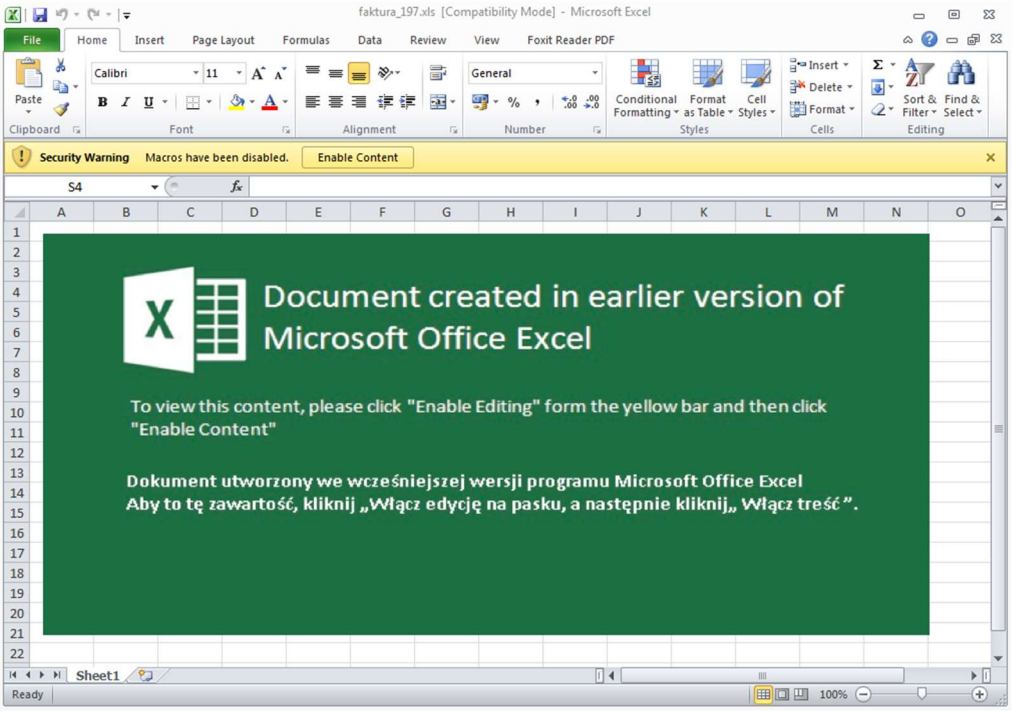
Orange Polska Spolka Akcyjna z siedziba i adresem w Warszawie (02-326) przy Al. Jerozoli mskich 160, wpisana do Rejestru Przedsiebiorcow prowadzonego przez Sad Rejonowy dla m.st. Warszawy XII Wydzial Gospodarczy Krajowego Rejestru Sadowego pod numerem 0000010681; REGON 012100784, NIP 526-02-50-995; z pokrytym w calosci kapitalem zakladowym wynoszacym 3.937.072.437 zlotych.

Rysunek 2 Przykład fałszywej faktury od Orange

- **KROK 2: Otwarcie pliku z fałszywą fakturą.** Każda osoba w organizacji, która będąc przekonaną o prawdziwości przesłanej wiadomości otworzy dołączony plik, naraża lokalne zasoby na ogromne niebezpieczeństwo. Jak widać na **Rysunku 3**, twórcy arkusza zachęcają potencjalną ofiarę na włączenie aktywnej zawartości, aby zapoznać się z jego treścią.

  Włączenie aktywnej treści arkusza powoduje, że bez wiedzy użytkownika nawiązywana jest komunikacja ze złośliwymi serwerami w sieci Internet, które dystrybuują właściwy już destrukcyjny kod.

Jest to bardzo groźna sytuacja, gdyż w tym momencie oprogramowanie antywirusowe często nie wykrywa zagrożenia, gdyż aktywna część arkusza nie jest jeszcze groźna sama w sobie.



Rysunek 3 Przykładowy podgląd arkusza ze złośliwym kodem

- **KROK 3: Pobranie złośliwej zawartości na lokalny komputer i właściwe rozpoczęcie infekcji.** Po włączeniu aktywnej treści arkusza (jak zostało opisane w kroku 2), pobierana jest i uruchamiana na lokalny komputer właściwa złośliwa aplikacja z Ransomware. W tym momencie rozpoczyna się infekcja i poszukiwanie podatnych na atak zasobów wewnątrz organizacji.
- **KROK 4: Destrukcyjne działanie Ransomware.** W tym kroku właściwe już złośliwe oprogramowanie przeszukuje lokalne zasoby w sieci (inne komputery, udostępniane zasoby na serwerach, magazyny kopii bezpieczeństwa, bazy danych). Odnalezione zasoby są najczęściej szyfrowane dla okupu. Najczęściej informacja jak wpłacić okup jest wyświetlana w zainfekowanym systemie, na którym dane zostały zniszczone.

IV. JAK SIĘ OBRONIĆ?

W środowisku osób zajmujących się zabezpieczeniami systemów i danych mówi się, że nie ma 100% mechanizmów ochrony. Można jednak zmniejszyć prawdopodobieństwo zmaterializowania się ryzyka oraz ograniczyć negatywne skutki wystąpienia zagrożenia. Poniżej znajduje się lista wspólnych działań:

1. Należy uświadomić pracowników najbardziej narażonych na ten rodzaj ataku o metodach stosowanych przez cyberprzestępców oraz o ewentualnych skutkach ich działalności.
2. Należy rozważyć udostępnienie użytkownikom listy kontrahentów i umów po to, aby już na pierwszej linii móc zweryfikować czy faktura jest prawdziwa. W przypadku negatywnej weryfikacji, całą wiadomość wraz z załącznikami należy usunąć bez przesyłania wewnątrz organizacji.
3. Należy rozważyć wdrożenie zabezpieczeń uniemożliwiających skuteczne komunikowanie się złośliwych załączników z poczty elektronicznej ze złośliwymi zasobami w sieci Internet (opisane w **KROK 2**). Można to wdrożyć poprzez:
    a. Stosowanie **białych list** do których użytkownicy mają dostęp w sieci Internet.

b. Stosowanie **czarnych list** z podejrzaną zawartością w sieci Internet.

c. Korzystanie z usług **operatora internetowego**, który posiada w swoim portfolio tego typu usługi.

4. Należy rozważyć użycie dedykowanych mechanizmów ochrony przed Ransomware dostępnych w oprogramowaniu antywirusowym. Mechanizmy te stanowią dodatkową ochronę wskazanych folderów i plików (np. folderu „Moje dokumenty"), do których dostęp powinny mieć wyłącznie zaufane aplikacje. To rozwiązanie zabezpiecza pliki przed ich usunięciem lub zaszyfrowaniem nawet gdy złośliwy kod nie zostanie rozpoznany przez oprogramowanie antywirusowe.
5. Należy rozważyć uruchomienia zapory sieciowej na lokalnych systemach dla ruchu przychodzącego w taki sposób, a by komputery użytkowników nie komunikowały się ze sobą i nie udostępniały żadnych zasobów. Jakiekolwiek pliki powinny być udostępniane na wybranej „maszynie" dedykowanej do tego celu.
6. Należy zabezpieczyć kopie bezpieczeństwa w taki sposób, aby nie były narażone na modyfikację czy usunięcie poprzez sieć lokalną oraz w wyniku działania złośliwego kodu na maszynie, na której są przechowywane.

V. TABELA RYZYKA

Zagrożenie	Możliwy skutek / wpływ	Mitygacja	Poziom Ryzyka
Włączenie aktywnej zawartości w spreparowanym pliku MS Office lub PDF	Pobranie złośliwej zawartości z sieci Internet bez wiedzy użytkownika i rozpoczęcie penetracji lokalnych zasobów	Rozdział IV pkt 1, 2, 3	**WYSOKI**
Zaszyfrowanie plików na lokalnych zasobach	Utrata danych, dokumentów, kopii bezpieczeństwa, odpowiedzialność prawna	Rozdział IV pkt. 4, 5, **6**	**WYSOKI**