Ransomware i phishing niebezpieczne związki

dr hab. inż. Henryk Wyrębek, prof. uczelni
Uniwersytet w Siedlcach
Instytut Nauk o Bezpieczeństwie
ORCID: 0000-0001-9801-6905

Streszczenie

Złośliwe oprogramowanie ransomware połączone z phishingiem, cyberoszustwem wykradającym dane to obecnie główne zagrożenia bezpieczeństwa w cyberprzestrzeni, które mają paraliżujący wpływ na funkcjonowanie organizacji, często prowadząc do przerw w działalności operacyjnej, ogromnych strat finansowych oraz utraty reputacji. W artykule podjęto próbę analizy i oceny znaczenia ataków hackerskich wykorzystujących ransomware i phishing na funkcjonowanie organizacji.

Słowa kluczowe: złośliwe oprogramowanie, bezpieczeństwo systemów informatycznych, sztuczna inteligencja.

Ostatnich kilka lat charakteryzuje się niespotykanym wcześniej tempem rozwoju społeczeństwa informacyjnego oraz nowych technologii. Osiągnięcia technologiczne otworzyły nowe horyzonty i stworzyły różnorodne formy interakcji międzyludzkich[1]. Obok ogromnych korzyści, jakie niesie za sobą informatyzacja, pojawiają się istotne, nieznane wcześniej zagrożenia, które dotykają wszystkie grupy społeczne.

Ataki wykorzystujące kombinacje złośliwego oprogramowania phishing i ransomware stały się najpowszechniejszą formą cyberprzestępczości i wykładniczo rosnącym zagrożeniem dla osób i organizacji[2].

Ransomware to złośliwe oprogramowanie, które szyfruje pliki lub blokuje cały system, a następnie żąda okupu za przywrócenie dostępu do danych. Złośliwe oprogramowanie ransomware pojawiło się w 2005 roku i szybko stało się opłacalną strategią biznesową dla atakujących[3].

Ataki typu ransomware mogą powodować znaczne szkody finansowe, obniżać produktywność, zakłócać normalną działalność biznesową i szkodzić reputacji[4].

Współcześnie ataki ransomware są skoncentrowane na sektorach o szczególnym znaczeniu, takich jak infrastruktura krytyczna, opieka zdrowotna, sektor edukacyjny, dostawcy usług IT oraz instytucje samorządowe[5].

W skali globalnej liczba potwierdzonych ataków (incydentów zakończonych sukcesem) wzrosła o około 34-47% w porównaniu do roku 2024. W pierwszej połowie 2025 roku Polska znalazła się na pierwszym miejscu na świecie pod względem liczby wykrytych prób ataków ransomware, wyprzedzając USA i Ukrainę[6]. Liczba ataków ransomware wzrasta wykładniczo dzięki łatwo dostępnym zestawom narzędzi do ataków ransomware i usłudze ransomware (RaaS), która umożliwia nowicjuszom przeprowadzanie ataków[7].

Tylko 19% pracowników w Polsce rozumie termin ransomware[8]. Dla porównania, kradzież tożsamości - 78% i phishing - 60% są znacznie częściej rozpoznawane. Ten niski poziom świadomości sprawia, że organizacje są szczególnie narażone na taktykę cyberprzestępców. Problem pogłębia powszechny brak szkoleń: ponad połowa polskich pracowników nie uczestniczyła w żadnym szkoleniu z zakresu cyberbezpieczeństwa w ciągu ostatnich pięciu lat. Chociaż szkolenia są uznawane za priorytet inwestycyjny, tylko 26% pracowników ukończyło w tym czasie więcej niż jedno szkolenie.

Techniki wykrywania ransomware koncentrują się głównie na honeypotach[9], analizie ruchu sieciowego i podejściach opartych na uczeniu maszynowym[10].

W 2025 roku został użyty pierwszy ransomware oparty na sztucznej inteligencji [11]. Chociaż sztuczna inteligencja nadal generuje wysoką jakość socjotechniki, to zastosowanie zwiastuje nową erę zagrożeń. Sztuczna inteligencja stała się dominującym elementem krajobrazu zagrożeń. Na koniec 2024 roku kampanie phishingowe wspierane przez sztuczną inteligencję stanowiły ponad 80% obserwowanych działań socjotechnicznych na całym świecie[12]. Około 76% organizacji przyznało, że ma trudności z nadążeniem za tempem ataków wykorzystujących sztuczną inteligencję, która automatyzuje wybór celów i personalizację phishingu.

W 2025 roku phishing pozostał najpoważniejszym i najbardziej masowym zagrożeniem w polskim cyberbezpieczeństwie. Liczba incydentów phishingowych drastycznie wzrosła w porównaniu do roku 2024. Phishing stanowił prawie 97-98% wszystkich incydentów obsługiwanych przez krajowe służby cyberbezpieczeństwa. Phishing to głównie forma kradzieży tożsamości online. Oszuści wykorzystują inżynierię społeczną do kradzieży danych. Phishing zaczyna się od wiadomości e-mail lub innego rodzaju komunikatu, który ma na celu ułatwienie

ataku na ofiarę. Wiadomość jest stworzona tak, jakby pochodziła od zaufanego nadawcy[13]. Złośliwe oprogramowanie może zostać zainstalowane w systemie ofiary za pośrednictwem załącznika do wiadomości e-mail lub pliku do pobrania ze strony internetowej lub poprzez wykorzystanie luk w zabezpieczeniach systemu[14].

Phishing jest niezwykle skuteczną metodą oszustwa, ponieważ wykorzystuje manipulację psychologiczną (strach, ciekawość, poczucie pilności), co sprawia, że ofiary same nieświadomie pomagają w ominięciu zabezpieczeń technicznych (takich jak antywirusy czy firewalle). Połączenie tego z niszczycielskim potencjałem z ransomware tworzy potężne zagrożenie.

Phishing i ransomware są ze sobą ściśle powiązane, ponieważ phishing jest główną metodą dostarczania oprogramowania ransomware. Stanowi on pierwszy etap łańcucha cyberataku, wykorzystujący manipulację społeczną do zainfekowania systemów.

Wykorzystanie błędu ludzkiego poprzez wysłanie wiadomości phishingowej jest znacznie łatwiejsze niż próba włamania się do systemu IT, ponieważ wymaga mniej umiejętności technicznych przestępcy, a bardziej skutecznego nakłonienia pracownika do wykonania działania[15]. W 2025 roku phishing stał się punktem wyjscia dla 91% wszystkich bardziej złożonych cyberataków, w tym dla ransomware.

Ataki te tworzą niebezpieczny związek, w którym phishing odgrywa znaczną rolę[16]:

- Przestępcy wysyłają wiadomości e-mail (lub inne komunikaty, np. w komunikatorach) podszywające się pod zaufane osoby, firmy lub instytucje (np. banki, urzędy, firmy kurierskie).
- Wiadomości są tak skonstruowane, aby skłonić ofiarę do podjęcia określonego działania, najczęściej kliknięcia w złośliwy link lub otwarcia zainfekowanego załącznika.
- Kliknięcie linku lub otwarcie załącznika powoduje nieświadome pobranie i zainstalowanie oprogramowania ransomware na komputerze lub w sieci ofiary.
- Po zainfekowaniu, ransomware szyfruje dane, blokując do nich dostęp, a następnie wyświetla żądanie okupu w zamian za klucz deszyfrujący. Dodatkowo, przestępcy często grożą ujawnieniem skradzionych danych, co jest formą podwójnego wymuszenia.

Skuteczność połączenia phishingu i ransomware wynika z:

- Wykorzystania błędu ludzkiego. Pomyłki wynikają nie tylko ze złej woli, ale także z przemęczenia, nieostrożności, stresu, braku doświadczenia[17].
- Łatwości użycia. Cyberprzestępcy mogą łatwo kupić gotowe zestawy phishingowe oraz oprogramowanie ransomware w ukrytej części internetu (ang. dark web[18]), co obniża próg wejścia dla mniej doświadczonych atakujących.
- Niskiej świadomości. Niska świadomość zagrożeń, zwłaszcza w mniejszych firmach, sprawia, że pracownicy są bardziej podatni na ataki phishingowe.

Ochrona przed ransomware połączonym z phishingiem wymaga podejścia wielowarstwowego, ponieważ phishing jest najczęstszym wektorem odpowiedzialnym za większość ataków ransomware. Podejście wielowarstwowe znacznie zwiększa szanse na wykrycie ataku phishingowego i zablokowanie ransomware na wczesnym etapie.

Poziom bezpieczeństwa zasobów systemu informatycznego zależy od stanu i prawidłowego współdziałania warstw ochronnych: systemu operacyjnego, systemu baz danych, aplikacji i sieciowych[19]. Zabezpieczenia różnych warstw powinny być ze sobą logiczne powiązane tak, aby ewentualne braki występujące w jednej warstwie zostały uzupełnione przez zabezpieczenia innych warstw. Skuteczna strategia ochrony przed zagrożeniami łączy nowoczesne technologie, procedury bezpieczeństwa oraz edukację użytkowników.

---

[1] Henryk Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Siedlce 2021, s. 7.
[2] https://www.deloitte.com/lu/en/services/consulting-risk/research/phishing-ransomware-how-to-prevent-threats.html, dostęp: 07.01.2026.
[3] Ronny Richardson, Max M. North, *Ransomware: evolution, mitigation and prevention*, „International Management Review", 13(1)/2017, p. 12.
[4] Garima Jain, Neelam Rani, *Awareness learning analysis of malware and ransomware in bitcoin*, Sigapore 2020, p. 765; Ross Brewer, *Ransomware attacks: detection, prevention and cure*, „Network security", 9/2016, p. 7.
[5] Grzegorz Pilarski, *Przegląd współczesnych zagrożeń w cyberprzestrzeni*, „Problemy Techniki Uzbrojenia", Zeszyt 167 nr 5/2023, s. 97.
[6] https://wbj.pl/poland-most-frequently-targeted-by-ransomware-in-the-world-in-2025/post/146517, dostęp: 07.01.2026.
[7] Shaila Sharmeen, Yahye Abukar Ahmed, Shamsul Huda, Bari S. Koçer, Mohammad Mehedi Hassan, *Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches*, IEEE Access 2020, 8:24522–34.
[8] https://www.eset.com/pl/about/newsroom/press-releases/news/polska-najczesciej-na-swiecie-atakowana-ransomware-w-2025-roku/, dostęp: 10.01.2026.
[9] Honeypot – pułapka mająca na celu wykrycie prób nieautoryzowanego użycia systemu czy pozyskania danych. System, serwer, dane lub usługa służąca do wykrywania, analizowania i uczenia się metod cyberataków.
[10] Craig Beamana, Ashley Barkwortha, Toluwalope David Akande, Saqib Hakak, Muhammad Khurram Khan, *Ransomware: Recent advances, analysis, challenges and future research directions,* „Computers & Security", 111/2021, p. 18.
[11] https://www.eset.com/us/business/threat-report/, dostęp: 15.01.2026.

[12] ENISA THREAT LANDSCAPE 2025 TLP:CLEAR | October 2025.
[13]Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, *Study on Phishing Attacks,* „International Journal of Computer Applications", Volume 182 – No. 33/2018, p. 27.
[14] Surya Chanti, T. Chithralekha, *A literature review on classification of phishing attacks*, „International Journal of Advanced Technology and Engineering Exploration", Vol 9(89)/2022, p. 456.
[15] https://www.egress.com/blog/phishing/phishing-leads-ransomware-attacks, dostęp: 17.01.2026.
[16]https://www.deloitte.com/lu/en/services/consulting-risk/research/phishing-ransomware-how-to-prevent-threats.html, dostęp: 17.01.2026.
[17] Henryk Wyrębek, *Bezpieczeństwo w zarządzaniu informacją na poziomie systemów informacyjnych,* „Zeszyty Naukowe Uniwersytetu Przyrodniczo – Humanistycznego w Siedlcach nr 95 Seria: Administracja i Zarządzanie", 22/2012. s. 469.
[18] Dark web (pol. ciemna sieć) to ukryta część internetu, niedostępna przez standardowe wyszukiwarki i przeglądarki, która wymaga specjalistycznego oprogramowania, jak przeglądarka Tor (The Onion Router) lub I2P, do anonimowego dostępu, co utrudnia śledzenie użytkowników. Choć bywa kojarzony z nielegalnymi działaniami (handel narkotykami, danymi), służy też legalnym celom: zapewnia anonimowość dziennikarzom, sygnalistom i dysydentom w reżimach autorytarnych, umożliwiając bezpieczną komunikację i wolność słowa.
[19] Henryk Wyrębek, *Bezpieczeństwo w zarządzaniu* …, dz. cyt., s. 465.