DOI: 10.26354/bb.5.1.98.2025

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Ransomware jako zagrożenie dla bezpieczeństwa infrastruktury krytycznej, ze szczególnym uwzględnieniem systemu finansowego

Streszczenie

Cel naukowy: Artykuł ma na celu podsumowanie współczesnej wiedzy na temat zagrożeń związanych z ransomware oraz zbadanie ich wpływu na infrastrukturę krytyczną w Polsce.

Problem i metody badawcze: Problemem badawczym jest analiza rosnącego zagrożenia ransomware, zwłaszcza w kontekście jego wpływu na instytucje publiczne i prywatne. Metody badawcze obejmują krytyczną analizę literatury oraz studium przypadków rzeczywistych ataków. Na podstawie przeglądu literatury oraz analizy incydentów, artykuł omawia etapy ataku ransomware, przykłady znanych incydentów w Polsce oraz analizuje poziom zagrożenia w różnych sektorach gospodarki.

Wyniki: Analiza wykazuje, że ransomware stał się poważnym zagrożeniem dla różnych sektorów, szczególnie dla infrastruktury krytycznej, zdolnej do paraliżowania działalności instytucji oraz powodowania wycieków danych.

Wnioski: Autor podkreśla pilną potrzebę wzmocnienia zabezpieczeń oraz edukacji użytkowników jako kluczowych strategii obronnych. Rekomenduje również regularne tworzenie kopii zapasowych oraz współpracę międzynarodową w dziedzinie cyberbezpieczeństwa. Artykuł wnosi nową wiedzę na temat strategii przeciwdziałania ransomware oraz podkreśla potrzebę ciągłego rozwoju technologii zabezpieczeń w odpowiedzi na rosnące zagrożenia cyfrowe.

Słowa kluczowe: ransomware, infrastruktura krytyczna, bezpieczeństwo infrastruktury krytycznej, system finansowy, zagrożenie cyfrowe

Kody JEL: L89

* Patryk Król – Uniwersytet Ekonomiczny w Poznaniu.

Ransomware as a threat to the security of critical infrastructure, with a focus on the financial system

Abstract

Scientific objective: This article aims to summarise the contemporary knowledge of ransomware threats and to examine their impact on critical infrastructure in Poland.

Research problem and methods: The research problem is to analyse the growing threat of ransomware, especially in the context of its impact on public and private institutions. Research methods include a critical analysis of the literature and case studies of actual attacks.

Executive process: Based on a literature review and incident analysis, the paper discusses the stages of a ransomware attack, examples of known incidents in Poland and analyses the level of threat in different economic sectors.

Result of scientific analysis: The analysis shows that ransomware has become a serious threat to various sectors, especially critical infrastructure, capable of paralysing the activities of institutions and causing data leaks.

Conclusions, innovations, recommendations: The author emphasise the urgent need to strengthen security and user education as key defence strategies. They also recommend regular backups and international cooperation in the field of cyber security. The article brings new knowledge on strategies to counter ransomware and highlights the need for continuous development of security technologies in response to growing digital threats.

Keywords: ransomware, critical infrastructure, critical infrastructure security, financial system

JEL Codes: L89

Wstęp

Jednym z popularniejszych rodzajów złośliwego oprogramowania jest ransomware[1], czyli złośliwe oprogramowanie, które ma na celu zablokowanie działania, dostępu lub uniemożliwienia odczytu zapisanych danych w celu późniejszego uzyskania okupu od ofiary wirusa (O'Gorman i McDonald 2012). Ataki tego typu są coraz częstsze, powstają również coraz to nowsze rodziny programów ransomware. Ransomware jest zagrożeniem zarówno dla osób indywidualnych, jak i instytucji publicznych, gdzie przy niefrasobliwości podmiotu odpowiedzialnego za bezpieczeństwo sieci informatycznej może dojść do poważnego zakłócenia bądź uniemożliwienia właściwego działania instytucji. Narodowy Program Ochrony Infrastruktury Krytycznej wskazuje na ransomware jako jedno z potencjalnych zagrożeń dla bezpieczeństwa infrastruktury krytycznej (Rządowe Centrum Bezpieczeństwa 2023). Hakerzy mogą również skierować swoje ataki na infrastrukturę krytyczną państwa, co może prowadzić do poważnych i dewastujących konsekwencji dla bezpieczeństwa narodowego i funkcjonowania kluczowych usług. Niniejszy artykuł ma na celu podsumowanie obecnej wiedzy literaturowej odnośnie do zagrożeń

[1] Nazwa pochodzi od angielskiego słowa *ransom* (okup) oraz *software* (oprogramowanie).

ransomware oraz przybliżenie czytelnikowi kluczowej wiedzy pozwalającej na zrozumienie podstawowych zagadnień odnoszących się do tego zjawiska. Metodami badawczymi zastosowanymi w artykule są: krytyczna analiza literatury przedmiotu, analiza realnych, udokumentowanych ataków na infrastrukturę krytyczną oraz próba określenia poziomu zagrożenia ransomware w Polsce.

Zgodnie z Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590) na potrzeby tego artykułu jako obiekty infrastruktury krytycznej definiowane są systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa oraz jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

1. Etapy ataku ransomware

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) w swoim raporcie z 2022 roku wyróżnia cztery etapy przeprowadzania ataku z użyciem ransomware:

1. Uzyskanie dostępu – na tym etapie cyberprzestępca stara się uzyskać dostęp do systemu komputerowego ofiary. Złośliwe oprogramowanie może być zainstalowane samodzielnie, przez ofiarę wprowadzoną w błąd przez metody phishingowe (Król, 2024) lub przez połączenie za pomocą zdalnego pulpitu (Garg, Thakral, Nalwa i Choudhury 2018), zestawy exploitów[2] (O'Kane, Sezer i Carlin 2018), podatności i luki w zabezpieczeniach Oracle WebLogic (Snoke i Shimeall 2020), robaki komputerowe (Liu, Zhuge i Wu 2018), łamanie haseł (Cobb, Cobb, Kabay i Crothers 2012), wstrzykiwanie kodu[3] (Paul Joseph i Norman 2020) i instalację drive-by[4] (Singhal i Levine 2019).
2. Działanie – ransomware rozpoczyna działanie przez zaszyfrowanie, zablokowanie dostępu, usunięcie lub kradzież zasobów zgromadzonych w zaatakowanym systemie. Mogą to być pliki, foldery, bazy danych, ekran interfejsu, tablice alokacji pamięci dyskowej (MFT), rekordy rozruchu systemu (MBR), zasoby chmury obliczeniowej, system zarządzania zawartością serwisu internetowego (CMS) (ENISA 2022).
3. Szantaż – cyberprzestępca wysuwa wobec ofiary żądanie podjęcia określonej czynności, udostępnienia określonych danych lub najczęściej dokonania płatności żądanej sumy pieniędzy, zwykle za pomocą kryptowalut (Kshetri i Voas 2017) lub kart przedpłaconych (Simoiu, Bonneau, Gates, Goel 2019), tak, aby utrudnić namierzenie transakcji oraz sprawcy przestępstwa.

[2] *Exploit* – luka w zabezpieczeniu oprogramowania.

[3] Wstrzykiwanie kodu (ang. *Injection*) – metoda ataku polegająca na wykorzystaniu luki w zabezpieczeniach w celu „wstrzyknięciu" (umieszczeniu) do oprogramowania ofiary złośliwego kodu oprogramowania, np. SQL injection, XPath injection, LDAP injection (Allodi, Massacci 2014).

[4] Samoistna instalacja złośliwego oprogramowania przez zainfekowaną stronę internetową (niebezpiecznik.pl, n.d.).

4. Negocjacje – cyberprzestępca negocjuje z ofiarą stawkę okupu. Najczęściej pierwotna stawka jest zawyżona, a ofiara pozostaje pod fałszywą presją czasową, tak aby zgodziła się na wysokie stawki.

2. Przykłady ataków z użyciem ransomware

Przykładem ataku hakerskiego z użyciem ransomware na instytucje infrastruktury krytycznej w Polsce jest atak dokonany na Szpital Matki Polki w Łodzi. Atak został przeprowadzony przez grupę Lockbit 3.0 (jedną z najaktywniejszych grup hakerskich). Jak podaje Sekurak.pl (2022), zaszyfrowane zostały również kopie zapasowe, możliwy był wyciek danych osobowych pacjentów. Rok później, w 2023 roku, zaatakowano Centralny Szpital Kliniczny Uniwersytetu Medycznego w Łodzi, również z użyciem ransomware, co znacznie zakłóciło działalność szpitala (Sekurak.pl 2023). ENISA w raporcie „Health Threat Landcape" (2023), zwraca uwagę że ransomware stanowi 54% wszystkich incydentów bezpieczeństwa dotyczących systemu opieki zdrowotnej. Według tego raportu w Polsce między rokiem 2021 a pierwszym kwartałem 2023 roku odnotowano 6 incydentów cyberataków, w tym 1 w 2021 roku, 4 w 2022 roku i 1 w pierwszym kwartale 2023 roku. Ofiarą cyberprzestępców padł w 2022 roku również szpital w Pajęcznie, gdzie zaszyfrowane zostały niemal wszystkie pliki, a cyberprzestępcy zażądali od władz szpitala wysokiego okupu (Sekurak.pl 2022).

Rysunek 1. Interfejs ransomware WannaCry

Źródło: CERT (2017).

W przypadku sektora finansów możemy odnotować atak na Bank Spółdzielczy w Zambrowie (Sekurak.pl 2024). Na problem utrzymania i tworzenia systemów informatycznych w bankach spółdzielczych zwraca uwagę Kotliński (2022), który zauważa, że banki spółdzielcze powinny rozważyć tworzenie wspólnych systemów jednolitych dla zrzeszenia lub nawet, że należy rozważyć stworzenie rozwiązań ponadzrzeszeniowych.

Ofiarami ransomware padały także urzędy publiczne. W przypadku gminy Nowiny zaszyfrowano bazy programu kadrowo-finansowego, a do infekcji doszło prawdopodobnie w wyniku pobrania i instalacji złośliwego oprogramowania przez pracownika gminy (Sekurak.pl 2021).

3. Poziom zagrożenia ransomware w Polsce

Według CERT Orange (2024), ransomware był drugim najczęściej wykrywanym rodzajem zagrożeń w sieci mobilnej w 2023 roku, i stanowił 24% wszystkich wykrytych przypadków. Najczęściej wykrywanym zagrożeniem były adware i HiddenApps, które razem stanowiły 54% wykrytych zagrożeń. Analiza danych z CERT wskazuje, że najwięcej incydentów ransomware odnotowano w podmiotach biznesowych, gdzie zgłoszono aż 81 przypadków. Na drugim miejscu znajduje się administracja publiczna z 31 przypadkami, a na trzecim – osoby prywatne z 30 przypadkami.

Najczęściej wykorzystywane rodziny ransomware w Polsce to Phobos, który odpowiadał za 29 incydentów, LockBit z 13 przypadkami oraz MedusaLocker i Djvu z 7 przypadkami każda. Na piątym miejscu znajduje się Makop, który był odpowiedzialny za 6 incydentów. Wzrost liczby ataków ransomware w Polsce można przypisać kilku czynnikom. Po pierwsze, rosnąca cyfryzacja i zależność od technologii sprawiają, że coraz więcej podmiotów staje się potencjalnym celem dla cyberprzestępców. Po drugie, rozwój technologii szyfrujących i narzędzi do przeprowadzania ataków sprawia, że ransomware staje się bardziej zaawansowane i trudniejsze do wykrycia oraz neutralizacji.

4. Główne metody zapobiegania ransomware

Beaman, Barkworth, Akande, Hanak i Khan (2021) wyróżniają dwie główne kategorie przeciwdziałania ransomware:

1. Prewencja i mitygowanie, polegające na zatrzymaniu lub odwróceniu skutków działania ransomware. Do tychże metod zaliczamy:
   a. Kopie zapasowe – umożliwiające przywrócenie systemu do stanu sprzed ataku komputerowego; aby ta metoda mogła być zastosowana, konieczne jest cykliczne wykonywanie kopii zapasowych,
   b. Uzyskanie klucza deszyfrowania – przy niektórych typach oprogramowania można pozyskać klucz deszyfrujący z jego plików. W badaniach Bajpai

i Enbody (2020), którzy przeprowadzili atak na złośliwe oprogramowanie metodą ataku kanałem bocznym, metoda ta osiągnęła 100% skuteczności przeciw takim ransomware, jak NotPetya, WannaCry, LockCrypt, CryptoRoger. Odnotowywane są również przypadki uzyskiwania kluczy w wyniku rozbicia grupy cyberprzestępczej.

c. Świadomość użytkownika – edukowanie użytkowników na temat zagrożeń związanych z ransomware oraz najlepszych praktyk bezpieczeństwa, takich jak unikanie otwierania podejrzanych załączników i klikania w nieznane linki, co może zapobiec infekcjom.
d. Segmentacja sieci – dzielenie sieci na segmenty w celu ograniczenia rozprzestrzeniania się ransomware w przypadku infekcji. Dzięki temu złośliwe oprogramowanie ma trudniejszy dostęp do krytycznych zasobów, co może zminimalizować szkody.
e. Kontrola dostępu – wdrażanie ścisłych zasad kontroli dostępu, takich jak wielopoziomowa autoryzacja i ograniczanie uprawnień użytkowników do minimum niezbędnego do wykonywania ich obowiązków, co utrudnia ransomware zdobycie uprawnień administracyjnych i szyfrowanie całego systemu.

2. Wykrywanie ransomware:
   a. Uczenie maszynowe
   b. Honeypot
   c. Analiza ruchu sieci
   d. Analiza plików
   e. Analiza doniesień dotyczących ransomware
   f. Automat skończony
   g. Analiza systemu informatycznego (m.in. kluczy rejestru Windows oraz logów systemowych)

5. Potencjalne działania

W przypadku zainfekowania systemu CERT (2021) zaleca następujące działania:

1. Izolacja zainfekowanej maszyny, uniemożliwiająca rozprzestrzenienie się wirusa na niezainfekowane systemy.
2. Identyfikacja oraz eliminacja infekcji.
3. Identyfikacja rodziny ransomware.
4. Przywrócenie działania systemu.
5. Zgłoszenie incydentu do zespołu CSIRT NASK, do którego należy załączyć minimum 2 zaszyfrowane pliki oraz notatkę z żądaniem okupu od przestępcy. Rekomenduje się także wysłanie próbki złośliwego oprogramowania, logów z zainfekowanej maszyny oraz systemów bezpieczeństwa, a także oryginały zainfekowanych plików, jeżeli są w dyspozycji.

CERT udostępnia również bezpłatne narzędzie od odzyskiwania klucza szyfrującego ransomware Vortex.

W przypadku działań doraźnych (szczególnie jeżeli instytucja zdecyduje się na negocjacje z przestępcami), opracowanie NCC (2021) zaleca następujące działania:

1. W przypadku odnotowania przez pracownika infekcji nie należy kontynuować interakcji, aby nie aktywować licznika czasu.
2. Nie należy podejmować decyzji pod presją czasu, mimo presji wywieranej przez przestępców. Prośby o udzielenie ofiarom dłuższego czasu są zwykle skuteczne.
3. Cyberprzestępcy często zgadzają się na kwoty okupu mniejsze niż początkowo żądane (np. 350 tysięcy USD zamiast miliona USD). W opracowaniu NCC skuteczne były wiadomości ze strony firmy-ofiary o niskich dochodach i niemożności uiszczeniu żądanej kwoty, wraz z propozycją alternatywnej, mniejszej kwoty okupu.
4. Nie należy informować cyberprzestępców o posiadanym ubezpieczeniu od ransomware.
5. Należy ustalić zewnętrzny kanał komunikacji, aby uniemożliwić zakłócenia i ingerencję osób trzecich.
6. Cyberprzestępcy często dzielą się informacją o lukach systemowych w firmie, jeżeli zostaną o nie poproszeni przez ofiarę, która zgodziła się na zapłacenie okupu.

Należy tu zaznaczyć, że podjęcie decyzji o zapłaceniu okupu w całości lub w części nie gwarantuje odblokowania danych i przywrócenia systemu do sprawnego działania. Powinno być więc rozważane jako ostateczność, w przypadku, gdy jest to niezbędne do przywrócenia prawidłowego działania instytucji, a dane są niemożliwe do odzyskania lub odtworzenia w żaden inny sposób. Wskazówki odnośnie do negocjacji z cyberprzestępcami są umieszczone w tym artykule, gdyż, jak wynika z raportu ENISA (2023), ponad 60% ofiar ataków ransomware mogło zdecydować się na uiszczenie okupu. Informacja jest zatem ważna z perspektywy zmniejszenia dotkliwości ataku. CERT (2017) nie rekomenduje płacenia okupu, a rekomenduje przywrócenie systemu przy użycia kopii zapasowej lub przeniesienie zainfekowanych danych na osobny dysk i reinstalację zainfekowanego systemu operacyjnego, co ma umożliwić odszyfrowanie danych bez płacenia okupu w przyszłości.

Podsumowanie

Ransomware to rosnące zagrożenie dla bezpieczeństwa cyfrowego, które polega na blokowaniu dostępu do danych i żądaniu okupu za ich odblokowanie. W artykule przeanalizowano przypadki ataków ransomware na infrastrukturę krytyczną w Polsce, badając zarówno techniczne aspekty tych ataków, jak i ich konsekwencje dla dotkniętych podmiotów. Wykorzystując analizę przypadków, autor podkreśla wzrastającą złożoność i skuteczność tych ataków oraz ich znaczący wpływ na działalność instytucji publicznych i prywatnych.

Badania pokazują, że kluczowe etapy ataku obejmują uzyskanie dostępu do systemu, rozprzestrzenianie złośliwego oprogramowania, szyfrowanie danych i żądanie okupu. Przykłady omówionych ataków ukazują różnorodność metod stosowanych przez cyberprzestępców, od phishingu po zaawansowane exploity.

Na podstawie artykułu możemy więc wyodrębnić pięć głównych rekomendacji:

1. Wzmacnianie zabezpieczeń: instytucje powinny inwestować w zaawansowane systemy zabezpieczeń, regularnie aktualizować oprogramowanie i stosować wielowarstwowe strategie obrony przed atakami ransomware.
2. Szkolenia dla pracowników: edukacja pracowników na temat rozpoznawania prób phishingu i innych metod socjotechnicznych jest kluczowa. Regularne szkolenia mogą znacznie zmniejszyć ryzyko udanego ataku.
3. Regularne kopie zapasowe: tworzenie regularnych kopii zapasowych danych i ich bezpieczne przechowywanie offline może znacznie ograniczyć skutki ataku ransomware. Instytucje powinny opracować i testować plany przywracania danych.
4. Współpraca międzynarodowa: wzmożona współpraca międzynarodowa w zakresie dzielenia się informacjami o zagrożeniach i najlepszych praktykach może pomóc w szybszym reagowaniu na nowe rodzaje ataków ransomware.
5. Badania i rozwój: kontynuowanie badań nad nowymi metodami wykrywania i neutralizowania ransomware, jak również rozwój technologii zabezpieczeń, jest niezbędne do utrzymania przewagi nad cyberprzestępcami.

Podsumowując, artykuł ukazuje pilną potrzebę kompleksowych działań mających na celu zwiększenie odporności na ataki ransomware. Przyjęcie proaktywnych strategii i stałe doskonalenie środków obronnych mogą znacznie zmniejszyć ryzyko i skutki tych ataków, chroniąc zarówno dane, jak i ciągłość działania kluczowych instytucji.

Bibliografia

Allodi L., Massacci F. (2014), *Comparing vulnerability severity and exploits using case-control studies*, „ACM Transactions on Information and System Security (TISSEC)", 17(1).

Beaman C., Barkworth A., Akande T.D., Hakak S., Khan M.K. (2021), *Ransomware: Recent advances, analysis, challenges and future research directions*, „Computers & security", 111, 102490.

CERT (2017), WannaCry Ransomware, https://cert.pl/posts/2017/05/wannacry-ransomware/ (dostęp 12.07.2024).

CERT (2021), Poradnik ransomware.

CERT (2024), Raport roczny z działalności CERT POLSKA 2023.

CERT Orange Polska (2024), Raport CERT Orange za 2023 rok.

Cobb C., Cobb S., Kabay M.E., Crothers T. (2012), *Penetrating computer systems and networks*, Computer Security Handbook, 15-1.

ENISA (2020), Ransomware ENISA Threat Landscape.

ENISA (2023), ENISA Threat Lanscape: Health Sector

Garg D., Thakral A., Nalwa T., Choudhury T. (2018), *A past examination and future expectation: Ransomware*, [w:] *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)* (s. 243–247), IEEE.

Król P. (2024), *Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej*, „Bezpieczny Bank", 94(1), 25–42. https://doi.org/10.26354/bb.2.1.94.2024

Kshetri N., Voas J. (2017), *Do crypto-currencies fuel ransomware?*, „IT professional", 19(5).

Liu Y., Zhuge J., Wu Y. (2018), *Threat and defense of new ransomware worm in industrial control system*, „Journal of Computer Applications", 38(6), 1608.

NCC (2021), "We wait, because we know you." Inside the ransomware negotiation economics, https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/ (dostęp 6.07.2024).

Niebezpiecznik.pl (n.d.) *Masz Androida? Uważaj na ataki drive-by-download*, https://niebezpiecznik.pl/symantec/masz-androida-uwazaj-na-ataki-drive-by-download/ (dostęp: 6.07.2024).

O'Gorman G., McDonald G. (2012). *Ransomware: A growing menace*, Arizona, AZ, USA: Symantec Corporation.

O'Kane P., Sezer S., Carlin D. (2018), *Evolution of ransomware*, „Iet Networks", 7(5).

Paul Joseph D. i Norman J. (2020), *A review and analysis of ransomware using memory forensics and its tools*, [w:] *Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics*, Volume 1, Springer Singapore.

Rządowe Centrum Bezpieczeństwa. (2023), Narodowy Program Ochrony Infrastruktury Krytycznej: Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, https://www.gov.pl/attachment/02553b90-184a-42c5-8445-5f9b1f0b74ee

Sekurak.pl (2021), *Ransomware i wyciek w gminie Nowiny*, https://sekurak.pl/ransomware-i-wyciek-w-gminie-nowiny/ (dostęp 6.07.2024).

Sekurak.pl (2022a), *Szpital Matki Polki w Łodzi zainfekowany ransomware. Informują również o „możliwym wycieku"*, https://sekurak.pl/szpital-matki-polki-w-lodzi-zainfekowany-ransomware-informuja-rowniez-o-mozliwym-wycieku/ (dostęp 6.07.2024).

Sekurak.pl (2022b), *Ransomware w szpitalu w Pajęcznie: Nastąpiła „niespodziewana awaria systemu informatycznego"*, https://sekurak.pl/ransomware-w-szpitalu-w-pajecznie-nastapila-niespodziewana-awaria-systemu-informatycznego/ (dostęp 6.07.2024).

Sekurak.pl (2023), Cyberatak na Centralny Szpital Kliniczny Uniwersytetu Medycznego w Łodzi, https://sekurak.pl/cyberatak-na-centralny-szpital-kliniczny-uniwersytetu-medycznego-w-lodzi/ (dostęp 6.07.2024).

Simoiu C., Bonneau J., Gates C., Goel S. (2019), *"I was told to buy a software or lose my computer. I ignored it": A study of ransomware*, [w:] *Fifteenth symposium on usable privacy and security (SOUPS 2019)*.

Singhal M., Levine D. (2019), *Analysis and categorization of drive-by download malware*, [w:] *2019 4th International Conference on Computing, Communications and Security (ICCCS)* (s. 1–4), IEEE.

Snoke T.D., Shimeall T.J. (2020), *An updated framework of defenses against ransomware*. Technical report, Carnegie-Mellon Univ Pittsburgh, PA.