Piotr Słowiński
Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy
ORCID: 0000-0003-4177-4902

NOTPETYA – ANALIZA Z PERSPEKTYWY KRYMINALISTYKI I POLSKIEGO PRAWA KARNEGO

NotPetya – forensics and Polish criminal law perspective analysis

Wstęp

Atak, któremu badacze nadali nazwę NotPetya, w niespotykany dotychczas sposób i na nieznaną skalę pokazał możliwości wykorzystania narzędzi informatycznych do niszczenia danych i zakłócania pracy systemów informatycznych. Początkowo użyty przez sprawców typ szkodliwego oprogramowania określano jako *ransomware*, czyli podobny jak w przypadku wcześniejszego ataku WannaCry[1]. Natomiast wyniki analiz przeprowadzonych po zdarzeniu nie pozostawiały wątpliwości, że było to oprogramowanie typu *wiper*. Celem tego typu programów jest usunięcie danych bezpowrotnie bez możliwości ich odzyskania po wpłaceniu określonej sumy pieniędzy[2] (w przeciwieństwie do ataku z użyciem *ransomware*). Straty w wyniku ataku NotPetya szacowane są według Białego Domu na 10 mld dolarów amerykańskich[3], czyli o wiele więcej, niż wyniosły koszty ata-

---

1 WannaCry to globalny atak oprogramowania typu ransomware, który dotknął ponad 100 krajów i 200 tys. komputerów z systemem operacyjnym Windows, wykorzystywał exploit EternalBlue wykradziony National Security Agency (NSA). Jest przypisywany oficjalnie północnokoreańskim hakerom (szerzej – grupie Lazarus Group, inaczej nazywanej HIDDEN COBRA lub APT38), za: K. Frankowicz, *WannaCry Ransomware*, CERT.PL, https://www.cert.pl/news/single/wannacry-ransomware/; WannaCry Ransomware, EUROPOL EC3, https://www.europol.europa.eu/wannacry-ransomware; T. Bossert, *It's official: North Korea is behind WannaCry*, „The Wall Street Journal", 18.12.2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 (dostęp do wszystkich: 30.09.2020).

2 A. Ivanov, O. Mamedov, *ExPetr/Petya/NotPetya is a wiper, not ransomware*, Securelist Kaspersky, 28.06.2017, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ (dostęp 30.09.2020).

3 A. Greenberg, *The untold story of NotPetya, the most devastating cyberattack in history*, WIRED, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp 30.09.2020).

ku WannaCry. Według byłego doradcy prezydenta Trumpa T. Bosserta NotPetya można określić jako „użycie bomby atomowej w celu osiągnięcia niewielkiego taktycznego zwycięstwa i oznacza ono lekkomyślność, której nie wolno tolerować w stosunkach międzynarodowych”[4]. Ofiarami ataku były zarówno globalnie operujące przedsiębiorstwa takie jak Maersk, Merck, FedEx (konkretnie europejska spółka córka TNT Express), Mondelez, Reckitt Benckiser czy Saint-Gobain, jak i lokalne firmy, zwłaszcza ukraińskie. Szczególnie wątek ukraiński przebija się jako znaczący i jak się potem okazało, decydujący w kwestii atrybucji ataku, czyli określenia, kto go przygotował i wykonał oraz jaki był tego możliwy motyw. Z uwagi na określony przez wielu badaczy punkt początkowy incydentu, czyli właśnie Ukrainę[5], należy rozpatrywać to zdarzenie w szerszym kontekście geopolitycznym i umiejscowić je na osi czasu konfliktu rosyjsko-ukraińskiego trwającego od 2014 r. Nie powinno się go postrzegać jedynie jako indywidualnego i wyizolowanego od aktualnej sytuacji zdarzenia, ponieważ może to uniemożliwić całościową i pełną analizę. Istotne jest traktowanie ataku NotPetya w sposób kompleksowy i patrzenie na niego w szerszej perspektywie. Pozwoli to na określenie motywów, sposobu działania i możliwych działań prewencyjnych wobec tego typu zdarzeń. Wszystkie wymienione aspekty pozostają w sferze zainteresowań kryminalistyki. Istotne jest omówienie ataku w świetle przepisów polskiego prawa karnego, ponieważ polskie oddziały niektórych z wyżej wymienionych spółek ucierpiały w wyniku zdarzenia. Ponadto wykonanie takiej analizy jest korzystne na wypadek podobnego ataku w przyszłości lub zamachu skierowanego tylko w polskie terytorium lub podmioty. Wreszcie teoretyczne rozważania tego typu (teoretyczne, ponieważ żaden akt oskarżenia, według najlepszej wiedzy autora, w sprawie ataków NotPetya nie został wniesiony do sądu przez polskie organy ścigania) pozwalają rozpatrzyć ewentualne możliwe do ziszczenia się scenariusze i przygotować choćby zręby procedur w wymiarze prawnym i kryminalistycznym na wypadek zaistnienia podobnego zdarzenia.

Przebieg ataku

Atak NotPetya nastąpił krótko po innym incydencie o globalnym wpływie i bezprecedensowym zasięgu, jak stwierdził Europol[6], a mianowicie ataku

---

4 Ibidem.

5 E. Nakashima, *Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes*, „The Washington Post”, 13.01.2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html (dostęp 30.09.2020).

6 *Cyber-attack: Europol says it was unprecedented in scale*, BBC, 13.05.2017, https://www.bbc.com/news/world-europe-39907965; *WannaCry Ransomware*, op. cit.

WannaCry. Zasadne jest wspomnienie także o nim w celu zbudowania zarówno tła wydarzeń, jak i wskazania różnic między obydwoma zdarzeniami. Wykorzystujący *ransomware* atak WannaCry rozpoczął się 12 maja i trwał aż do 15 maja 2017 r.[7] Dotknął 150 krajów i około 300 tys. podmiotów oraz wywołał problemy m.in. w szpitalach i jednostkach National Health Service (brytyjskiej służby zdrowia), hiszpańskich spółkach telekomunikacyjnych[8], a także wielu przedsiębiorstwach z rynku motoryzacyjnego, energetycznego i paliwowego oraz instytucjach finansowych. Oparty był na działaniu *exploitu* EternalBlue[9], czyli podatności w niezaktualizowanych systemach Windows. Wykorzystanie luk w najbardziej popularnym i rozpowszechnionym systemie operacyjnym sprawiło, że w skali globalnej skala i dotkliwość incydentu były ogromne. WannaCry wywołał poruszenie wśród badaczy zajmujących się cyberbezpieczeństwem i nie tylko, a największa krytyka spadła na USA. Powodem był fakt, iż *exploit* EternalBlue został opracowany przez National Security Agency (NSA), a następnie wykradziony przez grupę pod nazwą ShadowBrokers. Krytyka na NSA i w szerszym wymiarze na władze amerykańskie spadła m.in. ze strony władz Microsoftu[10], E. Snowdena[11], badaczy cyberbezpieczeństwa[12] oraz przedstawicieli organów innych państw[13]. Atak udało się powstrzymać

---

7 T.B. Lee, *The WannaCry ransomware attack was temporarily halted. But it's not over yet*, Vox, 15.05.2017, https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp (dostęp 30.09.2020).

8 L.H. Newman, *The Ransomware meltdown experts warned about is here*, WIRED, 12.05.2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/ (dostęp 30.09.2020).

9 EternalBlue to exploit (typ oprogramowania wykorzystujący podatność w innym oprogramowaniu lub urządzeniu) opracowany przez amerykańską National Security Agency (NSA); umożliwia atakującym uruchamianie i wykonywanie poleceń na urządzeniu ofiary pracującym w systemie operacyjnym Windows, za: N. Grossman, EternalBlue – *Everything There Is To Know*, Checkpoint, 29.09.2017, https://research.checkpoint.com/2017/eternalblue-everything-know/ (dostęp 30.09.2020).

10 B. Smith, *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, Microsoft Blog, 14.05.2017, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ (dostęp 30.09.2020).

11 Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/Snowden/status/863425539616284673 (dostęp 30.09.2020).

12 E. Helmore, *Ransomware attack reveals breakdown in US intelligence protocols, expert says*, „The Guardian", 13.05.2017, https://www.theguardian.com/technology/2017/may/13/ransomware-cyber-attack-us-intelligence (dostęp 30.09.2020).

13 *WannaCry: BSI ruft Betroffene auf, Infektionen zu melden*, Heise Online, https://www.heise.de/newsticker/meldung/WannaCry-BSI-ruft-Betroffene-auf-Infektionen-zu-melden-3713442.html (dostęp 30.09.2020).

wspólnymi siłami wielu osób z całego świata, a jeden ze skutecznych tzw. *kill switch*[14] wykorzystał M. Hutchins[15].

Wspomnienie o ataku WannaCry nie pozostaje bez związku, lecz jest niezbędne jako tło dla początkowo podjętych działań zapobiegawczych i analitycznych. Szczególnie że oba ataki, zarówno WannaCry, jak i NotPetya, wykorzystywały ten sam *exploit* EternalBlue.

Atak NotPetya rozpoczął się 27 czerwca 2017 r. Pierwsze doniesienia o zaszyfrowanych urządzeniach pochodziły z ukraińskiej spółki energetycznej (która już wcześniej była celem ataków hakerskich) Kyivenergo oraz duńskiej spółki Maersk, zajmującej się przewozem i transportem towarów na całym świecie. Choć z początku wydawało się, że jest to wariant szkodliwego oprogramowania Petya, to badacze z Kaspersky Lab pierwsi wskazali na różnice między nimi oraz nazwali go NotPetya[16]. Jako główny aspekt podkreślono, że NotPetya miał ściśle destrukcyjny charakter – jego celem było zniszczenie danych[17]. Najbardziej dotkniętym krajem według badaczy z firmy ESET była Ukraina, gdzie rozpoznano 80% wszystkich infekcji[18]. Na terenie państwa ukraińskiego atak dotknął 300 firm, 22 banki i 4 szpitale. Ofiarami padły także lotniska i instytucje rządowe[19]. W toku analizy logów oraz późniejszych dalszych pogłębionych analiz okazało się, że źródłem incydentu było ukraińskie przedsiębiorstwo Linkos Group (wcześniej Intellect-Service[20]) odpowiedzialne za stworzenie i aktualizację oprogramo-

---

14 *Kill switch* to wbudowany (wewnętrzny) mechanizm lub metoda pozwalające na wyłączenie lub zablokowanie działania oprogramowania lub urządzenia, za: https://www.techopedia.com/definition/4001/kill-switch, https://www.pcmag.com/encyclopedia/term/kill-switch (dostęp do wszystkich: 30.09.2020).

15 A. Greenberg, *The confessions of Marcus Hutchins, the hacker who saved the Internet*, WIRED, 12.05.2020, https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/; How to accidentally stop a global cyber attacks, MalwareTech, 13.05.2017, https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html (dostęp do wszystkich: 30.09.2020).

16 Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/kaspersky/status/879749175570817024/photo/1 (dostęp 30.09.2020).

17 GReAT, *Schroedinger's Pet(ya)*, Securelist Kaspersky, 27.06.2017, https://securelist.com/schroedingers-petya/78870/ (dostęp 30.09.2020).

18 J. Wakefield, *Tax software blamed for cyber-attack spread*, BBC, 28.06.2017, https://www.bbc.com/news/technology-40428967; *"Petya" Ransomware: What we know now*, ESET, 27.06.2017, https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/ (dostęp do wszystkich: 30.09.2020).

19 C. Brumfield, *Russia's Sandworm hacking group heralds new era of cyber warfare*, CSO Online, 22.11.2019, https://www.csoonline.com/article/3455172/russias-sandworm-hacking-group-heralds-new-era-of-cyber-warfare.html (dostęp 30.09.2020).

20 *M.E.Doc developer signs agreement with SBU on countering cyberattack threats*, Interfax Ukraine, 12.07.2018, https://en.interfax.com.ua/news/general/517610.html (dostęp 30.09.2020).

wania do rozliczeń księgowych M.E.Doc[21]. Mimo zaprzeczeń ze strony firmy[22] późniejsze analizy wykazały, że złośliwe oprogramowanie zostało rozpowszechnione wraz z aktualizacjami tego programu w kwietniu, maju i czerwcu. Zdaniem badaczy z firmy ESET wskazuje to na możliwość, iż serwery przedsiębiorstwa zostały przejęte i były kontrolowane co najmniej od kwietnia[23]. Podobnego zdania co do źródła (serwera), z którego infekcja się rozprzestrzeniła w formie aktualizacji, są również badacze z Microsoft[24], Bitdefender[25], Kaspersky[26] oraz Cisco Talos[27]. Zostało to także stwierdzone w komunikacie departamentu ukraińskiej policji odpowiedzialnego za ściganie cyberprzestępstw. W tym samym komunikacie poinformowano też o wejściu w dniu 4 lipca 2017 r. przez policję i kijowską prokuraturę, z udziałem funkcjonariuszy Służby Bezpieczeństwa Ukrainy (SBU), do siedziby Linkos Group w celu dokonania przeszukania oraz zabezpieczenia serwerów i urządzeń należących do tej firmy jako dowodów niezbędnych do prowadzenia postępowania[28].

---

21 Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/CyberpoliceUA/status/879772963658235904?s=20; T. Brewster, *Is this Ukrainian company the source of the "NotPetya" ransomware explosion?*, „Forbes", 27.06.2017, https://www.forbes.com/sites/thomasbrewster/2017/06/27/medoc-firm-blamed-for-ransomware-outbreak/#7ba793fd73c8 (dostęp 30.09.2020); A. Greenberg, *The untold story...*, op. cit.

22 Post opublikowany na portalu społecznościowym Facebook, https://www.facebook.com/medoc.ua/posts/1904044929883085 (dostęp 30.09.2020).

23 A. Cherepanov, *Analysis of TeleBots' cunning backdoor*, WeLiveSecurity ESET, 04.07.2017, https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (dostęp 30.09.2020).

24 Microsoft Defender ATP Research Team, *New ransomware, old techniques: Petya adds worm capabilities*, Microsoft, 27.06.2017, https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc (dostęp 30.09.2020).

25 B. Botezatu, *Massive GoldenEye ransomware campaign slams worldwide users*, Bitdefender, 28.06.2017, https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/ (dostęp 30.09.2020).

26 GReAT, *Schroedinger's*… op. cit.; Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/craiu/status/880343543373586432 (dostęp do wszystkich: 30.09.2020).

27 A. Chiu, *New ransomware variant "Nyetya" compromises systems worldwide*, Talos Intelligence Blog, 06.07.2017, https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html (dostęp 30.09.2020).

28 Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C) (tłum. na ang.: Petya virus (Diskcoder.C) became a cover for the largest cyber attack in the history of Ukraine), Cyberpolice Ukraine, 05.07.2017, https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/; C. Cimpanu, *Ukrainian police seize servers from where NotPetya outbreak first spread*, Bleeping Computer, 04.07.2017, https://www.bleepingcomputer.com/news/security/ukrainian-police-seize-servers-from-where-notpetya-outbreak-first-spread/ (dostęp do wszystkich: 30.09.2020).

Straty finansowe poniesione przez ofiary na całym świecie wyliczone zostały w miliardach dolarów. Były pracownik Białego Domu potwierdził, że przybliżone koszty spowodowane atakiem wyniosły ponad 10 mld dolarów[29]. Według szacunków poszczególnych przedsiębiorstw około 300 mln kosztowało to Maersk[30], 400 mln FedEx[31], a firmę Merck 1,3 mld dolarów (wliczając koszty naprawy sprzętu, przywrócenia serwerów oraz pozostałych czynności niezbędnych do przywrócenia działania sieci i urządzeń zaatakowanych)[32]. Wpływ na wysokość poniesionych kosztów miał fakt, iż pliki pozostały zaszyfrowane. Wymuszało to na użytkownikach nierzadko wymianę znaczącej liczby sprzętu, np. w przypadku wspomnianego przedsiębiorstwa Maersk – ponownej konfiguracji lub instalacji wymagało około 4 tys. serwerów i 45 tys. komputerów[33]. W Polsce ataki dotknęły głównie oddziały zagranicznych firm, które najbardziej ucierpiały podczas ataku, choć nie tylko. Wśród poszkodowanych były firma Maersk, Raben, InterCars, TNT, Saint-Gobain i Mondelez[34]. W odpowiedzi na falę infekcji w Polsce zebrał się Rządowy Zespół Zarządzania Bezpieczeństwem[35]. W wyniku spotkania nie zapadły żadne decyzje o wprowadzeniu stopnia alarmowego ani nie zostały wydane konkretne rekomendacje. Ponadto nie stwierdzono, aby ofiarami ataku padły instytucje publiczne[36].

---

29 A. Greenberg, *The untold story*…, op. cit.

30 D. Palmer, *Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk*, ZDNet, 16.08.2017, https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (dostęp 30.09.2020).

31 FedEx Corp. 2019 Annual Report, https://s1.q4cdn.com/714383399/files/doc_financials/annual/2019/FedEx-Corporation-2019-Annual-Report.pdf?utm_source=InvestorRelations&utm_medium=Referral&utm_campaign=AnnualReport2018&utm_content=FinancialInformationAnnualReports (dostęp 30.09.2020).

32 D. Voreacos, K. Chiglinsky, R. Griffin, *Merck cyberattack's $1.3 billion question: Was it an act of war?*, Bloomberg, 03.12.2019, https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (dostęp 30.09.2020).

33 C. Osborne, *NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs*, ZDNet, 26.01.2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/ (dostęp 30.09.2020).

34 K. Majdan, *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware?*, Business Insider, 28.06.2017, https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2 (dostęp 30.09.2020).

35 *Kolejny groźny globalny atak: ransomware Petya (NotPetya). Ofiary także w Polsce. Dotyczy również zaktualizowanych Windowsów!*, Niebezpiecznik, 27.06.2017, https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/; *Wiele polskich firm zostało zaatakowanych przez wirusa Petya*, Polskie Radio 24, 28.06.2017, https://www.polskieradio.pl/130/3993/Artykul/1782398,Wiele-polskich-firm-zostalo-zaatakowanych-przez-wirusa-Petya (dostęp do wszystkich: 30.09.2020).

36 Rządowy zespół kryzysowy o cyberatakach, IAR, 28.06.2017, https://www.polskieradio.pl/78/1227/Artykul/1782601,Rzadowy-zespol-kryzysowy-o-cyberatakach (dostęp 30.09.2020).

Techniki, taktyki i procedury oraz kwalifikacja prawna zdarzenia

Techniki, taktyki i procedury (z ang. *Techniques*, *Tactics* and *Procedures*, w skrócie TTP) to szeroko rozpowszechnione i stosowane przez osoby zajmujące się cyberbezpieczeństwem[37] określenie wywodzące się z kręgów wojskowych[38]. Nie ma konkretnej definicji, która odbiegałaby od semantycznego znaczenia poszczególnych jego słów. Tak zwane ramy MITRE ATT&CK wyróżniają i definiują taktykę jako uzasadnienie i wskazanie motywu dla podjętych działań. Stanowi to odpowiedź na pytanie „dlaczego?", nieobce zresztą kryminalistyce (jedno z tzw. siedmiu złotych pytań kryminalistyki). Techniki są rozumiane jako sposób, w który sprawca osiągnął zamierzony cel. Procedury są natomiast określane jako szczegółowy opis metody implementacji technik w celu osiągnięcia celu, w opisywanym tu kontekście również w perspektywie historycznej ataków dokonanych wcześniej[39]. Ramy MITRE ATT&CK określają i wskazują schemat postępowania z wieloma platformami i systemami operacyjnymi w razie incydentu lub ataku z uwzględnieniem podziału na różne taktyki i sposoby ich przeprowadzenia. Dotyczy to między innymi takich aspektów jak uzyskanie dostępu, wykonanie, uzyskanie uwierzytelnienia, zbieranie danych, przejmowanie kontroli itd., wraz z przyporządkowaniem technik stosowanych w ramach każdego z wymienionych działań[40]. Przygotowane zawczasu szczegółowe rozróżnienie oparte na danych historycznych może umożliwić szybką reakcję na zidentyfikowane zagrożenie, pod warunkiem że jest ono tożsame z historycznym lub podobne (np. wykorzystujące te same narzędzia lub metody). Z punktu widzenia prawa karnego i kryminalistyki niecelowe byłoby konstruowanie nowej definicji, innej niż przytoczona wyżej. Wystarczy bowiem wykorzystanie ogólnych zasad kryminalistycznych w postaci tzw. siedmiu złotych pytań kryminalistyki i odniesienie się do definicji ram MITRE ATT&CK. W tym przypadku wymienione ramy postępowania można traktować jako rozszerzenie i ewentualnie uzupełnienie z punktu widzenia cyberbezpieczeństwa i zapobiegania incydentom komputerowym, jednak nie mogą one całkowicie zastąpić ogólnej metodologii krymi-

---

37 F. Maymí, R. Bixler, R. Jones, S. Lathrop, *Towards a definition of cyberspace tactics, techniques and procedures*, 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, s. 4674–4679, doi: 10.1109/BigData.2017.8258514, https://ieeexplore.ieee.org/document/8258514 (dostęp 30.09.2020).

38 DOD Dictionary of Military and Associated Terms, Department of Defense, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (dostęp 30.09.2020).

39 Tactics, Techniques and Procedures, Radware, 09.12.2019, https://security.radware.com/ddos-experts-insider/hackers-corner/tactics-techniques-procedures/ (dostęp 30.09.2020).

40 Enterprise Matrix, MITRE ATT&CK, https://attack.mitre.org/matrices/enterprise/ (dostęp 30.09.2020).

nalistycznej. Zamiast tego trzeba korzystać z ich „dorobku", dostosowując do potrzeb postępowania karnego.

Dla rozważań o zastosowanych przez sprawców technikach, taktykach i procedurach istotnym aspektem jest określenie, czym atak NotPetya w rzeczywistości był. Początkowo incydent określany był jako *ransomware*, czyli atak wykorzystujący szkodliwe oprogramowanie, które szyfruje pliki lub system użytkownika, a w zamian za jego odblokowanie domaga się zapłacenia okupu[41]. Aktualnie, ze względu na utrudnione metody wykrycia i śledzenia przez organy ścigania, sprawcy żądają okupu w kryptowalucie[42], tak jak np. podczas ataku WannaCry[43]. Po przeprowadzeniu czynności śledczych oraz analizy logów i urządzeń okazało się, że wykorzystany w ataku NotPetya typ oprogramowania to tzw. *wiper*. Jest to rodzaj szkodliwego oprogramowania, który ma za zadanie usunięcie, zniszczenie lub w inny sposób trwałe uszkodzenie danych i uniemożliwienie korzystania z nich[44]. Ataki oparte na *wiperach* nie są aż tak częste (choć trend ten ulega w ostatnim czasie zmianom[45]), ponieważ nie niosą ze sobą bezpośredniego wymiernego zysku dla sprawcy, np. w postaci okupu (jak w przypadku *ransomware*) lub sprzedaży danych (w razie ich kradzieży z serwera za pomocą jakiegokolwiek typu szkodliwego oprogramowania dającego dostęp do serwerów lub urządzeń ofiary). Odkrycie tego faktu w kontekście ataku NotPetya całkowicie zmieniło jego postrzeganie, a także określenie celu oraz możliwości atrybucji przeprowadzonego ataku zarówno przez badaczy cyberbezpieczeństwa[46], jak i w efekcie z punktu widzenia prawa oraz kryminalistyki. Zmiana potencjalnego motywu sprawcy (z częstszego motywu finansowego na rzadszy i do tego bliżej w tym momencie nieokreślony – polityczny, ideologiczny lub finansowy, ale niezwiązany z bezpośrednio dającym się obliczyć zyskiem) może mieć wpływ

41 Ransomware definition, w: Cambridge Dictionary Online, https://dictionary.cambridge.org/pl/dictionary/english/ransomware; Oprogramowanie ransomware, Malwarebytes, https://pl.malwarebytes.com/ransomware/ (dostęp 30.09.2020).

42 Ransomware, TrendMicro, https://www.trendmicro.com/vinfo/us/security/definition/ransomware (dostęp 30.09.2020).

43 Symantec Security Response Team, *What you need to know about the WannaCry Ransomware*, Symantec (Broadcom), 23.10.2017, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack (dostęp 30.09.2020).

44 *Malware Spotlight: What are wipers?*, Infosec Institute, 19.11.2019, https://resources.infosecinstitute.com/malware-spotlight-what-are-wipers/#gref (dostęp 30.09.2020).

45 V. Chebyshev et al., *IT threat evolution Q3 2019. Statistics, Securelist Kaspersky*, 29.11.2019, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/ (dostęp 30.09.2020).

46 D. Goodin, *Tuesday's massive ransomware outbreak was, in fact, something much worse*, Ars Technica, 28.06.2017, https://arstechnica.com/information-technology/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/ (dostęp 30.09.2020).

na możliwości uchwycenia i przypisania sprawstwa. Rozpoznanie rzeczywistej charakterystyki ataku i jego celu umożliwia wysnucie wniosków oraz wskazanie głównych problemów z punktu widzenia kryminalistyki (zdolności wykrywcze i możliwości przypisania sprawstwa konkretnym podmiotom) i prawa karnego (adekwatna i jak najbardziej zbliżona do rzeczywistości kwalifikacja prawna czynu albo czynów).

Po pierwsze, wydawać by się mogło, że w tej sprawie określenie kwalifikacji prawnej według polskiego kodeksu karnego nie będzie nastręczało problemów. W sytuacji gdyby charakter ataku nie uległ zmianie, czyli mielibyśmy do czynienia jedynie z oprogramowaniem typu *ransomware*, należałoby wskazać jako podstawę odpowiedzialności art. 269a k.k., czyli zakłócenie systemu komputerowego[47], a także art. 268 k.k. (utrudnianie zapoznania się z informacją)[48] oraz art. 269b § 1 (wytwarzanie programów komputerowych)[49]. Implikacją zmiany określenia charakterystyki użytego programu (*wiper* zamiast *ransomware*) jest fakt, iż do przytoczonych wyżej artykułów dodać należy art. 268a k.k., czyli niszczenie danych informatycznych[50]. W tym konkretnym przypadku chodzi o czynności

---

47 Art. 269a (zakłócenie systemu komputerowego): Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j. Dz. U. z 2020 r., poz. 1444), dostępny w: SIP Lex Omega (dostęp 30.09.2020).

48 Art. 268 (utrudnianie zapoznania się z informacją): § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego (ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j. Dz. U. z 2020 r., poz. 1444), dostępny w: SIP Lex Omega (dostęp 30.09.2020).

49 Art. 269b (wytwarzanie programów komputerowych): § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j. Dz. U. z 2020 r., poz. 1444), dostępny w: SIP Lex Omega (dostęp 30.09.2020).

50 Art. 268a (niszczenie danych informatycznych):
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia

opisane w § 2, co niesie ze sobą kolejne dodatkowe konsekwencje. W doktrynie wskazuje się, że dobrem ubocznym zagrożonym przez przestępstwo są interesy majątkowe osoby uprawnionej, co oznacza, że czyn z tego artykułu ma również charakter przestępstwa przeciwko mieniu[51]. W związku z tym sąd może orzec lub orzeka na wniosek pokrzywdzonego obowiązek naprawienia szkody w całości lub części, stosując przepisy prawa cywilnego. Ma to niebagatelne znaczenie z uwagi na oszacowane przez ofiary straty w wyniku atak NotPetya, niezależnie od realnych możliwości ukarania i wyegzekwowania odszkodowania lub zadośćuczynienia od sprawców. Jakakolwiek kwalifikacja zostanie przyjęta na kanwie ataku NotPetya, zagrożenie wymiarem kary będzie takie samo, czyli pozbawieniem wolności od 3 miesięcy do lat 5.

Po drugie, w kwestii zastosowanych technik można zauważyć, że atak NotPetya jest jednocześnie charakterystyczny, jak i pospolity, co nie oznacza, iż jednocześnie prosty do przeprowadzenia. Wymienione wyżej sprzeczności są tylko pozorne. Atak można określić jako pospolity z uwagi na zastosowane przez sprawców narzędzia. Pierwsze z nich, czyli EternalBlue, zostało wykradzione NSA w 2017 r., a następnie za sprawą grupy ShadowBrokers znalazło się w otwartym dostępie. Drugim jest Mimikatz, stworzony jako dowód i potwierdzenie podatności (ang. *proof-of-concept*) systemu Windows w zakresie przechowywania haseł użytkowników. EternalBlue to *exploit* (rodzaj oprogramowania, kodu lub komend wykorzystujący podatności lub błędy w programach bądź sprzęcie w celu wywołania niechcianego lub nieoczekiwanego przez użytkownika zachowania) działający dzięki luce w systemach operacyjnych Windows. Konkretnie chodzi o protokół Server Message Block (SMB) służący do udostępniania zasobów urządzenia w sieci. Mimikatz to oprogramowanie służące do wyciągania danych uwierzytelniających (loginów i haseł) profili systemu operacyjnego Windows gromadzonych w pamięci urządzeń przez system[52]. Został stworzony przez fran-

---

dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

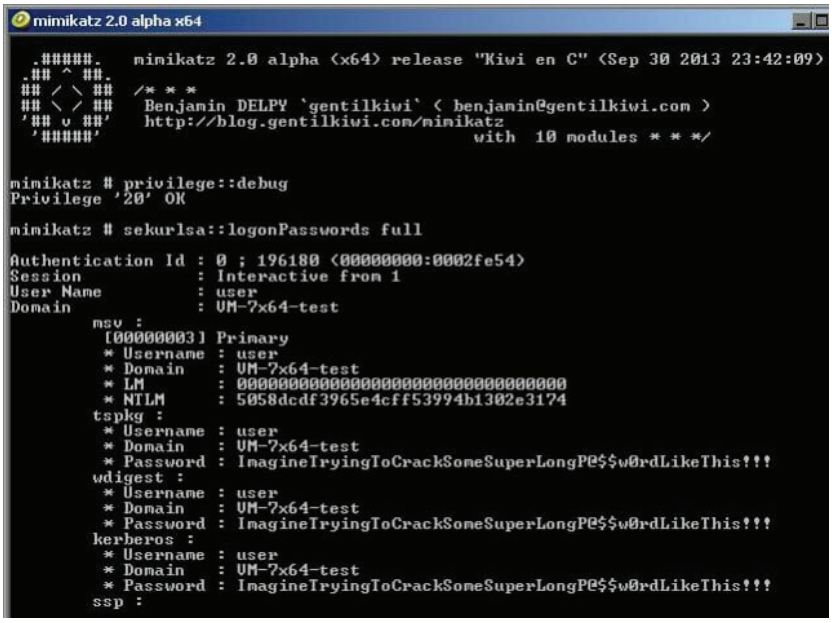
§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego (ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, tj. Dz. U. z 2020 r., poz. 1444), dostępny w: SIP Lex Omega (dostęp 30.09.2020).

51 W. Wróbel, D. Zając, *Art. 268(a)*, w: *Kodeks karny. Część szczególna*. Tom II. Część II. *Komentarz do art. art. 212–277d*. Wolters Kluwer Polska, 2017, dostępny w: SIP Lex Omega (dostęp 30.09.2020).

52 Systemy operacyjne firmy Microsoft, aż do wersji Windows 10, za pomocą zasobu o nazwie WDigest domyślnie gromadziły w pamięci urządzenia zaszyfrowane hasła i loginy wraz

cuskiego programistę Benjamina Delpy w 2007 r., a udostępniony przez twórcę na blogu i GitHub w 2017 r. Charakterystycznym elementem opisywanego ataku jest połączenie obu narzędzi – każde z nich bowiem bywało już stosowane, ale osobno. Specyficzne jest też użycie łącznie obu programów oraz wykorzystana przez sprawców metoda uzyskania dostępu do serwera, skąd rozpropagowane zostało złośliwe oprogramowanie.

Ryc. 1. Widok wyników programu Mimikatz



Źródło: https://doubleoctopus.com/security-wiki/threats-and-tools/mimikatz/, dostęp: 30.09.2020).

Po trzecie, do ataku użyto oprogramowania do rozliczeń księgowych M.E.Doc spółki Linkos Group. Sprawcy wykorzystali mechanizm wysyłający automatyczne aktualizacje z serwerów producenta bezpośrednio do komputerów klientów. Dzięki swojej obecności na serwerach (a także, jak wskazują badacze z ESET, sprawując nad nimi *de facto* kontrolę) podmienili właściwe aktualizacje na te zawierające szkodliwe oprogramowanie, a serwery Linkos Group same

z kluczem umożliwiającym ich deszyfrację, za: J.M. Porup, *What is Mimikatz? And how to defend against this password stealing tool*, CSO Online, 05.03.2019, https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html (dostęp 30.09.2020).

rozesłały je do użytkowników. Jest to metoda jednocześnie skuteczna i ograniczająca szansę wykrycia, że wysyłane jest szkodliwe oprogramowanie (automatyczna aktualizacja pochodząca z zaufanego serwera producenta oprogramowania już zainstalowanego na urządzeniach), jak i utrudniająca dotarcie do sprawcy (przynajmniej w początkowej fazie, a jeśli, tak jak w tym przypadku, sprawcy przygotowali dystrybucję aktualizacji wcześniej, powoduje to ogromne trudności nawet na dalszych etapach postępowania). Dodatkowo wpływ na powodzenie ataku i trudności w działaniach śledczych miał fakt, iż nie zaobserwowano żadnej komunikacji z zewnętrznym serwerem typu *command & control*[53] (C&C, C2). Jednocześnie powoduje to niemożliwość skorzystania z metod pozwalających na wykrycie lokalizacji sprawcy wydającego komendy i sterującego zainfekowanym serwerem oraz wskazuje na możliwość, że jako serwer C&C służył ten należący do Linkos Group (czyli zaatakowany przez sprawców i dystrybuujący zainfekowane pliki)[54]. Na powyższe wskazują następujące czynniki:

- sprawcy uzyskali dostęp do serwerów Linkos Group na długi czas przed atakiem (co najmniej w kwietniu, ponieważ pierwsza zainfekowana aktualizacja miała datę kwietniową), co pozwoliło im na odpowiednie ukrycie wtargnięcia i utrzymującej się obecności, a następnie na obfuskację wszelkich działań;
- wysyłanie szkodliwego oprogramowania lub kodu przez oficjalne serwery producenta, w szczególności jeśli ma to być planowana aktualizacja programu, co pozwala na uśpienie czujności zarówno samego producenta, jak i klientów;
- wykorzystanie jako serwerów C&C tych należących do Linkos Group, na których zlokalizowane były aktualizacje (w tym te zainfekowane), pozwoliło sprawcom na dodatkowe ukrycie i zatarcie potencjalnych śla-

[53] Serwer typu *command & control* (C&C, C2) to urządzenie kontrolowane przez atakującego lub przestępcę, które jest wykorzystywane do wysyłania komend do zainfekowanego urządzenia lub sieci oraz otrzymywania z niego wykradzionych danych, serwerem C2 mogą być np. serwery poczty lub hostingowe, co pozwala na jednolitość z normalnym, regularnym ruchem sieciowym i utrudnia ewentualne wykrycie przez programy antywiruowe, za: Command and Control (C&C) Server, TrendMicro, https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (dostęp 30.09.2020).

[54] A. Cherepanov, *Analysis of TeleBots'* op. cit.; A. Haertle, *Komputery ofiar NotPetya mogły być zainfekowane co najmniej od kwietnia*, Zaufana Trzecia Strona, 04.07.2017, https://zaufanatrzeciastrona.pl/post/komputery-zaatakowane-przez-notpetya-mogly-byc-zainfekowane-co-najmniej-od-kwietnia/; C. Cimpanu, *M.E.Doc software was backdoored 3 times, servers left without updates since 2013*, Bleeping Computer, 06.07.2017, https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/ (dostęp do wszystkich: 30.09.2020).

dów oraz uniemożliwienie powstawania nowych (np. stworzenie innego, zewnętrznego serwera C&C, który byłby kolejnym ogniwem mogącym doprowadzić do odpowiedzialnych za atak, zwiększałoby potencjalnie liczbę śladów),

- w tym przypadku powszechność wykorzystywania oprogramowania ułatwiła infekcję większej liczby urządzeń. Dotyczy to także tych zlokalizowanych poza pierwotnym krajem działania sprawców, czyli Ukrainą, np. za pośrednictwem ukraińskich oddziałów międzynarodowych korporacji lub spółek. Te z kolei infekowały komputery w innych lokalizacjach na świecie przez podłączenie do wspólnej korporacyjnej sieci.

Samoistnie ogólnodostępność narzędzi wykorzystanych w ataku może stanowić potwierdzenie na „pospolitość" incydentu; przez to określenie rozumie się fakt, że może być on dokonany przez każdego mającego podstawowe umiejętności komputerowe lub wiedzę z zakresu wykorzystywania narzędzi hakerskich. Dopiero całościowe przeanalizowanie ataku i zachowania sprawców pozwala wysnuć bardziej holistyczne wnioski. Charakterystyczne, a jednocześnie wskazujące na skomplikowany charakter ataku jest zastosowane połączenie ogólnodostępnych narzędzi, a także metoda dostania się do systemu, pozostawania w nim oraz wykorzystanie go do przeprowadzenia głównego etapu infekcji komputerów. Wspomniany całokształt zastosowanych technik, taktyk i procedur może świadczyć o zaawansowaniu technicznym sprawców oraz określonym celu do zrealizowania.

Atrybucja ataku

Atrybucja, czyli możliwość przypisania sprawstwa i obciążenia odpowiedzialnością za incydent lub atak na systemy lub sieci, jest równie ważna zarówno z perspektywy prawa karnego, jak i przygotowywania analiz z zakresu cyberbezpieczeństwa. W obu przypadkach jest to niezbędne w celu zidentyfikowania sprawcy zdarzenia, a następnie opracowania i podjęcia działań prewencyjnych. W efekcie pozwoli to na zniwelowanie negatywnych efektów ataku. Z punktu widzenia prawa karnego dodatkowym aspektem jest zgromadzenie dowodów istotnych pod kątem procedury karnej, opartych na prawdziwych ustaleniach faktycznych, umożliwiających wykrycie sprawcy lub sprawców w celu pociągnięcia do odpowiedzialności karnej. Charakter prewencyjny atrybucji pozwala na podjęcie konkretnych środków zaradczych, zarówno w wymiarze technicznym (np. uaktualnienie oprogramowania podatnego na atak), kryminalistycznym (np. aktualizacja procedur postępowania w przypadku śledztw wymagających zabezpieczenia dowodów cyfrowych lub sieciowych), jak i prawnym (np. konkretne

zmiany w krajowym ustawodawstwie regulującym aspekty cyberbezpieczeństwa lub postępowania w sprawach incydentów bezpieczeństwa). Zaobserwować można również wpływ możliwości atrybucyjnych na prowadzoną politykę w wymiarze wewnętrznym oraz zewnętrznym. Całościowa analiza skali ataku NotPetya, zastosowanych przez sprawców narzędzi oraz sposobu przeprowadzenia ataku, w tym związana z nim długotrwała obecność w systemach będących pierwotnym jego celem, pozwoliła zawęzić już na wstępie potencjalnie odpowiedzialne podmioty. Niewątpliwie z punktu widzenia kryminalistycznego i wykrywczego zarówno najbardziej właściwe, jak i efektywne wydaje się na początku ograniczenie kręgu podejrzanych. Pozwoli to na priorytetyzowanie czynności podejmowanych w toku postępowania przygotowawczego przez wykluczenie najmniej prawdopodobnych sprawców np. ze względu na zastosowane skomplikowane oprogramowanie lub metodę uzyskania dostępu do zaatakowanego urządzenia/sieci.

W przypadku ataków na taką skalę jak NotPetya oraz z uwagi na wykorzystane środki techniczne oraz taktykę sprawców atrybucja nie mogła być łatwa. Zaplanowane i wykonane z wyprzedzeniem (wskazuje się na wiosnę 2017 r.) uzyskanie dostępu do serwerów przedsiębiorstwa, które miało posłużyć jako węzeł do dalszej dystrybucji szkodliwego oprogramowania, świadczy o odpowiednim przygotowaniu, świadomym wyborze celu oraz umiejętnościach pozwalających na realizację planu oraz zatarcie śladów. Całokształt działań jest charakterystyczny dla działalności grupy APT (skrót od ang. *Advanced Persistent Threat*)[55]. Skala oraz kraj określony jako najbardziej dotknięty, a przez to jako potencjalny główny cel, dodatkowo wskazywały na działalność inspirowaną lub sponsorowaną przez państwo. Ten aspekt również sugerował działalność grupy APT.

W kwestii tożsamości sprawców ataku NotPetya państwa sojuszu wywiadowczego *Five Eyes* (FVEY), czyli Australia, Kanada, Nowa Zelandia, Wielka Brytania oraz Stany Zjednoczone, zgodnie i oficjalnie obciążyły odpowiedzialnością za zdarzenie Rosję. Jednocześnie uznały atak za najbardziej kosztowny i niszczący w skutkach w historii, a także za dowód i potwierdzenie zaangażowania Moskwy w destabilizowanie Ukrainy i trwający w niej konflikt[56]. Według in-

[55] Grupa APT to określenie grupy dokonującej ataku na sieć lub urządzenia, który polega na utrzymywaniu obecności na serwerach lub w urządzeniu wraz z zachowaniem kontroli nad nimi oraz pozostawaniu niewykrytym przez użytkownika lub administratora, za: S. Maloney, *What is an Advanced Persistent Threat (APT)?*, Cybereason, 09.01.2018, https://www.cybereason.com/blog/advanced-persistent-threat-apt; *What Is an Advanced Persistent Threat (APT)?*, Cisco, https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html (dostęp do wszystkich: 30.09.2020).

[56] E. Kovacs, *U.S., Canada, Australia attribute NotPetya attack to Russia*, Security Week, 16.02.2018, https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia (dostęp 30.09.2020).

formacji dziennikarza A. Greenberga za przeprowadzenie ataku odpowiedzialna jest grupa Sandworm, znana również jako TeleBots[57] lub GreyEnergy, w opinii autora działająca w ramach GRU[58], czyli wywiadu wojskowego Federacji Rosyjskiej, a wcześniej ZSRR[59]. Podobnego zdania są firma ESET[60], ukraińska ISSP[61] oraz brytyjskie National Cyber Security Centre (NCSC)[62]. Amerykańska National Security Agency uszczegółowia owo wskazanie i umiejscawia grupę Sandworm w strukturach GRU w Głównym Centrum Technologii Specjalnych (Main Center for Special Technologies, GTST)[63]. Tej grupie przypisuje się również ataki takie jak BlackEnergy[64], Bad Rabbit[65] oraz działania wspierające ofensywę w trakcie ataku na Gruzję[66]. Aktualnie, czego wyrazem jest m.in. atak NotPetya, głównym terenem aktywności grupy jest Ukraina. W obliczu działalności grupy Sandworm kraj ten określa się nawet jako „poligon testowy cyberbroni"[67].

---

57 *TeleBots aka Sanworm*, Malpedia, https://malpedia.caad.fkie.fraunhofer.de/actor/telebots (dostęp 30.09.2020).

58 Skrót od ros. Gławnoje Razwiedywatielnoje Uprawlenije, Główny Zarząd Wywiadowczy Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, w skrócie Główny Zarząd Wywiadowczy lub GRU, od 2004 r. funkcjonuje jako Główny Zarząd Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, w skrócie GU lub GRU, za: https://en.wikipedia.org/wiki/GRU_(G.U.), https://pl.wikipedia.org/wiki/G%C5%82%C3%B3wny_Zarz%C4%85d_Wywiadowczy (dostęp 30.09.2020).

59 A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York 2019, s. 363–372.

60 A. Cherepanov, *TeleBots are back: Supply-chain attacks against Ukraine*, WeLiveSecurity ESET, 30.06.2017, https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ (dostęp 30.09.2020).

61 L. Cerulus, *How Ukraine became a test bed for cyberweaponry*, POLITICO, 14.02.2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (dostęp 30.09.2020).

62 *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, National Cyber Security Centre UK, 03.10.2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (dostęp 30.09.2020).

63 *Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors*, National Security Agency US, 28.05.2020, https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/ (dostęp 30.09.2020).

64 J. Hultquist, *Sandworm team and the Ukrainian power authority attacks*, FireEye, 08.01.2016, https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html (dostęp 30.09.2020).

65 A. Perekalin, *Bad Rabbit: nowa epidemia ransomware*, Kaspersky Blog, 24.10.2017, https://plblog.kaspersky.com/bad-rabbit-ransomware/8396/ (dostęp 30.09.2020).

66 M.R. Pompeo, *The United States Condemns Russian Cyber Attack Against the Country of Georgia, Press Statement*, Department of State US, 20.02.2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (dostęp 30.09.2020).

67 L. Cerulus, *How Ukraine*..., op. cit.

Wnioski i podsumowanie

Prezentowany w niniejszym artykule temat implikuje potrzebę określenia w podsumowaniu wniosków dotyczących aspektów problematycznych zarówno dla polskiego prawa karnego, jak i kryminalistyki.

Sformułowanie aktualnych przepisów prawa karnego w części szczegółowej kodeksu karnego w części dotyczącej znamion. Problematycznym aspektem z punktu widzenia polskiego prawa karnego jest nieoddające rzeczywistości oraz nieuwzględniające postępu technologicznego i rozwoju technik wykorzystywanych przez przestępców sformułowanie przepisów prawa karnego. Efektem tego może być niedokładne w całości lub w części, a przez to zbyt szerokie i nieefektywne, określenie znamion przestępstw. To z kolei przełoży się na brak rozróżnienia, m.in. w zakresie wymiaru kary, między działaniami bardziej i mniej destrukcyjnymi. Aktualnie przepisy kodeksu karnego w ramach jednego przestępstwa określają szeroki zakres czynności w obrębie jednego artykułu oraz mniejszych jednostek redakcyjnych, takich jak paragrafy. Faktem jest, że niektóre z tych czynności wynikają jedne z drugich, np. w przypadku zniszczenia danych konsekwencją może być zakłócenie działania systemu lub przetwarzania danych. Natomiast brak jest wyraźnego rozróżnienia w zakresie wymiaru kary, co wynika bezpośrednio z umieszczenia zbyt wielu określeń znamion w jednym artykule. Postulatem, który mógłby ten problem rozwiązać, jest rozdzielenie czynności destruktywnych, takich jak np. niszczenie danych, wraz ze zwiększeniem wymiaru kary za nie, od czynności niedestruktywnych, przynajmniej bezpośrednio, takich jak np. blokowanie lub utrudnianie dostępu. Podobną zasadę należałoby stosować przy tworzeniu nowych przepisów, jeżeli zostaną zidentyfikowane nowe, konkretne metody wykorzystywane (aktualnie lub w przyszłości) przez sprawców, a nieujęte w dotychczas obowiązujących przepisach. „Elementy składowe", które można brać pod uwagę, to np. skala dokonanego czynu (np. ilość uszkodzonych danych, liczba zainfekowanych urządzeń, wymierne straty finansowe i wizerunkowe poniesione w wyniku ataku wpływałyby na zwiększony wymiar kary) lub rozróżnienie niszczenia od blokowania lub utrudniania dostępu. Przytoczone wyliczenie nie jest katalogiem zamkniętym i są to jedynie niektóre z propozycji kryteriów dywersyfikujących. Odnosząc się do zmian w konkretnych przepisach, można by rozważyć, czy w przypadku art. 268a, czyli dotyczącego niszczenia danych, nie byłoby zasadne rozdzielenie 'niszczenia, uszkadzania, usuwania, zmieniania" od dalszej części karalnych znamion, czyli „utrudniania dostępu do danych informatycznych albo w istotnym stopniu zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania takich danych". Uzasadnieniem dla tej zmiany byłoby wskazane wyżej postulowanie oderwanie od siebie czynności destruktywnych od niedestruktywnych, a przy-

najmniej umieszczenie ich w oddzielnych paragrafach, niekoniecznie od razu w innych artykułach. Jest to wskazane z uwagi na różny charakter tych czynności i ich konsekwencji dla ofiar lub celów. Niezależnie od tego na gruncie teorii prawa karnego i kryminalistyki wprowadzenie nawet aktualnie *stricte* teoretycznego rozróżnienia nie oznacza, że w przyszłości, wraz z rozwojem metod i technik wykrywczych i atrybucyjnych, nie będzie możliwe wykorzystanie teorii w praktyce.

Sformułowanie aktualnych przepisów prawa karnego w części szczegółowej kodeksu karnego w części dotyczącej wymiaru kary. Biorąc pod uwagę omawiane zdarzenie, należy się zastanowić, czy nie byłoby zasadne większe rozróżnienie w zakresie wymiaru kary między poszczególnymi wymienionymi w tym artykule przestępstwami (tj. art. 268, 268a, 269a i 269b). Pod rozwagę należy poddać propozycję zwiększenia górnej granicy wymiaru kary za czyny obejmujące niszczenie danych w stosunku do jedynie zakłócenia działania systemu komputerowego. Szczególnie że aktualnie brak jest takowego, a wydaje się, iż niszczenie danych powinno być traktowane inaczej niż utrudnianie dostępu do nich lub zakłócanie działania systemów. Sensowny, zwłaszcza na gruncie omawianego przypadku, wydaje się postulat zwiększonej górnej granicy wymiaru kary za niszczenie danych jako czynności potencjalnie groźniejszej np. w razie niemożliwości ich odtworzenia z różnych przyczyn. Zdarza się, jak w przypadku ataku NotPetya, że dane są niezwykle trudne lub niemożliwe do odzyskania, ponieważ zniszczeniu ulegają również kopie zapasowe i dane umożliwiające odtworzenie zniszczonych informacji. Należy taką sytuację przeciwstawić zdarzeniu, w którym zakłócenie systemu ma charakter czasowy i przykładowo po spełnieniu warunków sprawców, np. zapłaceniu okupu lub podjęciu konkretnego działania, następuje przywrócenie działania lub dostępu do systemu.

Nieodpowiednia lub nieadekwatna kwalifikacja prawna czynów przyjęta przez organy ścigania lub wymiaru sprawiedliwości. Problematycznym aspektem w przypadku polskiego prawa karnego jest odpowiednie i adekwatne, w szczególności oddające rzeczywistość, zgodne ze stanem faktycznym i realizujące cele postępowania karnego określenie kwalifikacji prawnej przyjmowanej przez organy ścigania lub organy wymiaru sprawiedliwości w postępowaniach dotyczących cyberprzestępczości. Naturalnie potwierdzenie tej tezy wymagałoby szeroko zakrojonych badań aktowych. Jednak już na tym etapie można stwierdzić, że ogólne sformułowanie przepisów dotyczących cyberprzestępstw nie ułatwia kwalifikacji prawnej czynów oraz sprzyja ewentualnym błędom lub niedopatrzeniom w tej kwestii. Po części ten aspekt jest pokłosiem opisanego w akapicie wyżej, aktualnego sformułowania przepisów. Jednak kwalifikacja prawna czynów na etapie prowadzonego postępowania jest kolejnym etapem w analizie prawa. W praktycznym wymiarze problem w odpowiednim lub adekwatnym określeniu pod kątem

prawnym czynów może nieść ze sobą trudności na etapie postępowania przygotowawczego. Decyzje odnośnie do podejmowanych czynności procesowych i pozaprocesowych, np. czy dokonywać oględzin, czy zabezpieczać sprzęt lub urządzenia, mogą wynikać z przyjętej kwalifikacji prawnej czynu. W konsekwencji ma to wpływ na zlecanie wykonania opinii przez biegłych. To z kolei znajduje swoje odzwierciedlenie w przyjmowanych wersjach kryminalistycznych oraz ewentualnym sporządzeniu i skierowaniu aktu oskarżenia. W konsekwencji (w odległej perspektywie) może to mieć skutki w postaci możliwości udanego skorzystania z drogi odwoławczej przed sądem oraz znaczenie w wymiarze statystycznym, a w tym kontekście również choćby wpływ na prowadzone badania naukowe lub statystyczne – także te oddziałujące na kształtowanie prawa przez organy ustawodawcze oraz decyzje podejmowane w organach ścigania lub wymiaru sprawiedliwości w wymiarze organizacyjnym i szkoleniowym.

Problem związany z możliwościami wykrywczymi oraz atrybucyjnymi z uwagi na metody obfuskacji kodu i ukrywania ruchu sieciowego. Obfuskacja kodu polega na umyślnym przygotowaniu go w sposób utrudniający jego zrozumienie, np. przez używanie bardziej złożonych zwrotów i konstrukcji lub wręcz tworzenie z niego zagadek, co ma utrudnić dokonanie na nim operacji inżynierii wstecznej i odkrycie jego przeznaczenia lub tożsamości autora[68]. Z ukrywaniem ruchu sieciowego mamy do czynienia, gdy użytkownicy chcą zachować lub wzmocnić anonimowość w komunikowaniu się lub innych czynnościach i działaniach podejmowanych w sieci, np. wymianie informacji. Wykorzystywać do tego można sieć TOR, sieci VPN, szyfrowane komunikatory (np. Signal czy Wire), szyfrowane usługi poczty elektronicznej (np. Protonmail czy Tutanota), kryptograficzne protokoły sieciowe (np. SSH czy SSL) lub techniki steganograficzne (ukrywanie treści w obrazach). Niezależnie od stosowanej metody ukrywanie ruchu sieciowego, czy to w postaci lokalizacji, czy danych, powoduje dodatkowe trudności dla organów ścigania. Nie są one w stanie od razu w momencie ujawnienia przeanalizować zgromadzonego materiału (w przypadku szyfrowania danych) ani określić położenia sprawcy. Spowalnia to podejmowane przez nie działania i przekłada się na wydłużenie prowadzonego postępowania, ponadto wymaga poświęcenia większych zasobów zarówno ludzkich (nierzadko osób mających specjalistyczną wiedzę), jak i materiałowych (w tym czasowych oraz specjalistycznego oprogramowania lub sprzętu).

Trudności atrybucyjne i wykrywcze wynikające z wykorzystywania przez sprawcę/sprawców ogólnodostępnego oprogramowania lub rozwiązań

[68] M. Rouse, *Obfuscation definition*, Techtarget, https://searchsoftwarequality.techtarget.com/definition/obfuscation (dostęp 30.09.2020).

technicznych. Dotyczy to możliwych problemów dla organów ścigania związanych z przypisaniem sprawstwa na podstawie poszlak lub dowodów wskazujących na wykorzystanie ogólnodostępnego, choć konkretnego oprogramowania lub rozwiązań technicznych. Może się bowiem okazać, że dowody cyfrowe lub sieciowe sugerujące użycie bardzo specyficznych i skomplikowanych (lub wręcz przeciwnie, prostych, ale cały czas charakterystycznych) programów niekoniecznie naprowadzą śledczych na ślad sprawców. Wiąże się to z faktem, iż (tak jak w przypadku opisywanego w niniejszym artykule ataku) sprawcy mogą wykorzystywać (i robią to, niezależnie od celu, coraz częściej[69]) oprogramowanie lub fragmenty kodu pozostające w otwartym dostępie. Zwiększa to krąg potencjalnych podejrzanych. Z tego powodu oparcie się tylko na narzędziach i technikach może nie być skuteczne z punktu widzenia prowadzonego postępowania, a więc również kryminalistyki. W przypadku gdy sprawcy nie modyfikują narzędzi lub nie przygotowują własnych, ale korzystają z dostępnych w sieci gotowych rozwiązań, np. na forum GitHub, możliwości atrybucji danego zdarzenia należy oprzeć na innych wnioskach lub wynikach analizy pozostałych dostępnych poszlak lub wskazówek. Warto brać pod uwagę całokształt działań podejmowanych przez atakujących, np. uwzględnić język wykorzystywany w kodzie. Można tu przywołać przykład grupy APT37, najprawdopodobniej północnokoreańskiej lub przez ten kraj inspirowanej bądź finansowanej. Starała się ona ukryć swoją tożsamość, używając w kodzie zwrotów z języka chińskiego przetłumaczonych na angielski[70]. Innym wskaźnikiem tożsamości mogą być godziny dokonania ataku. Zdarza się, że wskażą one lokalizację geograficzną sprawców pomimo stosowanych przez nich narzędzi ukrywających lub zmieniających lokalizację, jak w przypadku grupy APT29, której aktywność pokrywa się ze strefami czasowymi obowiązującymi w Moskwie i Petersburgu[71]. Dopiero całościowa analiza dowodów, dostępnych opinii biegłych oraz dodatkowych czynników poparta przeprowadzonym procesem analitycznym powinna pozwolić na wysnucie najbardziej oddających rzeczywistość wniosków lub chociaż zminimalizowanie ryzyka popełnienia błędu w prowadzeniu śledztwa lub dochodzenia.

---

69 D. Palmer, *Security warning: Attackers are using these five hacking tools to target you*, ZD-Net, 11.10.2018, https://www.zdnet.com/article/security-warning-attackers-are-using-these-five-hacking-tools-to-target-you/ (dostęp 30.09.2020).

70 Threat Intelligence Report OPERATION 'Rocket Man', Security Response Center (ESRC), 08.2018, http://blog.alyac.co.kr/attachment/cfile24.uf@99219C4F5BC3F4E01751D3.pdf (dostęp 30.09.2020).

71 The Dukes. 7 Years of Russian Cyberespionage, F-Secure, 09.2016, https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf (dostęp 30.09.2020).

Kryminalistyka i prawo dowodowe wobec nowych zagrożeń cyberbezpieczeństwa. W rozumieniu kryminalistycznym, z uwagi na wszystkie powyższe wnioski i wyzwania, opisywany atak jest problematyczny pod wieloma względami. Podstawowym wskaźnikiem, zarówno z teoretycznego (na sali wykładowej), jak i praktycznego (na sali sądowej) punktu widzenia, źródłem i podstawą do skazania powinny być dowody, które podlegają ściśle określonemu przez doktrynę i praktykę reżimowi. W przypadku tradycyjnych przestępstw możliwe jest potencjalne powiązanie konkretnego narzędzia (choćby seryjnie produkowanego) z miejscem lub zdarzeniem. Pozwala na to wykonanie badań kryminalistycznych przy dochowaniu staranności oraz naukowych standardów. W przypadku oprogramowania komputerowego nie zawsze jest to jednak w aż takim stopniu możliwe lub wykonalne. W odniesieniu do cyberprzestępczości i cyberbezpieczeństwa niezbędne jest kompleksowe spojrzenie na ataki na sieci, systemy i urządzenia, nierzadko z uwzględnieniem uwarunkowań geopolitycznych oraz gospodarczych. To z kolei wymaga konkretnych oraz często rzadkich cech i umiejętności wśród śledczych i prokuratorów. Znajomość oraz dochowanie wszelkich znanych oraz dostępnych standardów i dobrych praktyk zabezpieczania materiału cyfrowego mogą być niewystarczające. Odzyskany lub zabezpieczony przez techników kod, niezależnie, czy jest to jego fragment czy całość, niekoniecznie pozwoli na wykorzystanie go w atrybucji, a następnie w postępowaniu. Nie będzie to możliwe nie tyle z uwagi na jego niekompletność, ile właśnie dlatego, że ewentualny brak cech charakterystycznych (takich jak w przypadku „klasycznych" narzędzi) nie pozwoli na powiązanie z konkretną grupą lub osobą. To z kolei uniemożliwi wykorzystanie go jako narzędzia bezpośrednio wskazującego sprawcę lub wiążącego go ze zdarzeniem. Należy pamiętać, że wiedza lub wskazówki dotyczące jakiegoś zjawiska niekoniecznie muszą oznaczać możliwość wykorzystania ich jako dowodów. W możliwościach i efektach wykorzystania zebranych lub pozyskanych w toku dochodzenia bądź śledztwa informacji, a następnie na etapie postępowania sądowego, można upatrywać jednego ze wskaźników efektywności praktycznego zastosowania kryminalistyki. W związku z powyższym nasuwa się wniosek, iż pewnym niedostatkiem jest kierowanie się ściśle wskazaniami kryminalistyki stosowanymi do pozostałych działów techniki kryminalistycznej w stosunku do współczesnych zagrożeń cyberprzestępczością. Postuluje się zatem, by w odniesieniu do cyberprzestępczości, szczególnie tak zaawansowanej jak w omawianym przykładzie, nauki kryminalistyczne włączyły w swoje procedury dorobek z zakresu nauk o bezpieczeństwie (np. strategii bezpieczeństwa poszczególnych państw i zależności z innymi sektorami działalności państwa), nauk ścisłych (w szczególności informatycznych w aspekcie technicznym), nauk ekonomicznych (np. w zakresie międzynarodowej wymiany handlowej) oraz

nauk politycznych, w szczególności dotyczących stosunków międzynarodowych. Cyberprzestępczość jako globalny fenomen, niepoddający się dotychczas istniejącym ograniczeniom i granicom, wymaga interdyscyplinarnego podejścia, nawet w tak wąskim wymiarze, jakim jest zapobieganie i ściganie przestępczości. Bez podejścia łączącego wiedzę w perspektywie można liczyć na negatywny wpływ nie tylko na działania pozostające w zakresie nauk kryminalistycznych, lecz także w pozostałych wymienionych wyżej dyscyplinach.

Streszczenie

Celem artykułu jest przeanalizowanie ataku cybernetycznego NotPetya pod kątem kryminalistyki oraz polskiego prawa karnego. Omówienie aspektów kryminalistycznych obejmuje charakterystykę technik, taktyk i procedur wykorzystanych przez sprawców do ataku, w tym zastosowanego szkodliwego oprogramowania, oraz wskazanie ofiar wraz z uzasadnieniem ich doboru przez atakujących. Ponadto podkreślono trudności z atrybucją sprawców. Analiza prawna obejmowała wskazanie możliwych kwalifikacji prawnych czynów popełnionych przez sprawców na gruncie polskiego kodeksu karnego. Praca zakończona jest oceną znaczenia ataku i wnioskami *de lege ferenda* zarówno dla kryminalistyki, jak i prawa karnego.

Słowa kluczowe: cyberprzestępczość, NotPetya, szkodliwe oprogramowanie, Internet, kryminalistyka, prawo karne

Summary

The aim of the article is to analyse NotPetya's cyber-attack in terms of forensics and Polish criminal law. The discussion of forensic aspects includes the identification of techniques, tactics and procedures used by the perpetrators to launch the attack, including the malicious software used, the identification of victims and the justification for their selection by the attackers. In addition, difficulties in identifying the perpetrators have been outlined. The legal analysis included an indication of the possible legal classification of acts committed by the perpetrators under the Polish criminal code. The work concludes with an assessment of the significance of the attack, conclusions de lege ferenda, both for forensics and criminal law.

Keywords: cybercrime, NotPetya, malware, Internet, forensics, criminal law

Bibliografia

Literatura

Greenberg A., *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York 2019.

Maymí F., Bixler R., Jones R., Lathrop S., *Towards a definition of cyberspace tactics, techniques and procedures*, 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, doi: 10.1109/BigData.2017.8258514, https://ieeexplore.ieee.org/document/8258514.

Wróbel W., Zając D., *Art. 268(a)*, w: *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212–277d*, Wolters Kluwer Polska, 2017, dostępny w: SIP Lex Omega.

Źródła prawa

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2020 r., poz. 1444).

Źródła internetowe

Bossert T., *It's official: North Korea is behind WannaCry*, „The Wall Street Journal", 18.12.2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 (dostęp 30.09.2020).

Botezatu B., *Massive GoldenEye ransomware campaign slams worldwide users*, Bitdefender, 28.06.2017, https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/ (dostęp 30.09.2020).

Brewster T., *Is this Ukrainian company the source of the "NotPetya" ransomware explosion?*, Forbes, 27.06.2017, https://www.forbes.com/sites/thomasbrewster/2017/06/27/medoc-firm-blamed-for-ransomware-outbreak/#7ba793fd73c8 (dostęp 30.09.2020).

Brumfield C., *Russia's Sandworm hacking group heralds new era of cyber warfare*, CSO Online, 22.11.2019, https://www.csoonline.com/article/3455172/russias-sandworm-hacking-group-heralds-new-era-of-cyber-warfare.html (dostęp 30.09.2020).

Cerulus L., *How Ukraine became a test bed for cyberweaponry*, POLITICO, 14.02.2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (dostęp 30.09.2020).

Cherepanov A., *Analysis of TeleBots' cunning backdoor*, WeLiveSecurity ESET, 04.07.2017, https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (dostęp 30.09.2020).

Cherepanov A., *TeleBots are back: Supply-chain attacks against Ukraine*, WeLiveSecurity ESET, 30.06.2017, https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ (dostęp 30.09.2020).

Chiu A., *New ransomware variant "Nyetya" compromises systems worldwide*, Talos Intelligence Blog, 06.07.2017, https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html; (dostęp 30.09.2020).

Cimpanu C., *M.E.Doc software was backdoored 3 times, servers left without updates since 2013*, Bleeping Computer, 06.07.2017, https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/; (dostęp 30.09.2020).

Cimpanu C., *Ukrainian police seize servers from where NotPetya outbreak first spread*, Bleeping Computer, 04.07.2017, https://www.bleepingcomputer.com/news/security/ukrainian-police-seize-servers-from-where-notpetya-outbreak-first-spread/ (dostęp 30.09.2020).

Command and Control (C&C) Server, TrendMicro, https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (dostęp 30.09.2020).

Cyber-attack: Europol says it was unprecedented in scale, BBC, 13.05.2017, https://www.bbc.com/news/world-europe-39907965 (dostęp 30.09.2020).

DOD Dictionary of Military and Associated Terms, Department of Defense, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (dostęp 30.09.2020).

Enterprise Matrix, MITRE ATT&CK, https://attack.mitre.org/matrices/enterprise/ (dostęp 30.09.2020).

Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors, National Security Agency US, 28.05.2020, https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/ (dostęp 30.09.2020).

FedEx Corp. 2019 Annual Report, https://s1.q4cdn.com/714383399/files/doc_financials/annual/2019/FedEx-Corporation-2019-Annual-Report.pdf?utm_source=InvestorRelations&utm_medium=Referral&utm_campaign=AnnualReport2018&utm_content=FinancialInformationAnnualReports (dostęp 30.09.2020).

Frankowicz K., *WannaCry Ransomware*, CERT.PL, https://www.cert.pl/news/single/wannacry-ransomware/ (dostęp 30.09.2020).

Goodin D., *Tuesday's massive ransomware outbreak was, in fact, something much worse*, Ars Technica, 28.06.2017, https://arstechnica.com/information-technology/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/ (dostęp 30.09.2020).

GReAT, *Schroedinger's Pet(ya)*, Securelist Kaspersky, 27.06.2017, https://securelist.com/schroedingers-petya/78870/ (dostęp 30.09.2020).

Greenberg A., *The confessions of Marcus Hutchins, the hacker who saved the Internet*, WIRED, 12.05.2020, https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/ (dostęp 30.09.2020).

Greenberg A., *The untold story of NotPetya, the most devastating cyberattack in history*, WIRED, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp 30.09.2020).

Grossman N., *EternalBlue – everything there is to know*, Checkpoint, 29.09.2017, https://research.checkpoint.com/2017/eternalblue-everything-know/ (dostęp 30.09.2020).

Haertle A., *Komputery ofiar NotPetya mogły być zainfekowane co najmniej od kwietnia*, Zaufana Trzecia Strona, 04.07.2017, https://zaufanatrzeciastrona.pl/post/komputery-zaatakowane-przez-notpetya-mogly-byc-zainfekowane-co-najmniej-od-kwietnia/ (dostęp: 30.09.2020).

Helmore E., *Ransomware attack reveals breakdown in US intelligence protocols, expert says*, „The Guardian", 13.05.2017, https://www.theguardian.com/technology/2017/may/13/ransomware-cyber-attack-us-intelligence (dostęp 30.09.2020).

How to Accidentally Stop a Global Cyber Attacks, MalwareTech, 13.05.2017, https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html (dostęp 30.09.2020).

https://en.wikipedia.org/wiki/GRU_(G.U.) (dostęp 30.09.2020).

https://pl.wikipedia.org/wiki/G%C5%82%C3%B3wny_Zarz%C4%85d_Wywiadowczy (dostęp 30.09.2020).

https://www.pcmag.com/encyclopedia/term/kill-switch (dostęp: 30.09.2020).

https://www.techopedia.com/definition/4001/kill-switch (dostęp 30.09.2020).

Hultquist J., *Sandworm team and the Ukrainian power authority attacks*, FireEye, 08.01.2016,

https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html (dostęp 30.09.2020).

Ivanov A., Mamedov O., *ExPetr/Petya/NotPetya is a wiper, not ransomware*, Securelist Kaspersky, 28.06.2017, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ (dostęp 30.09.2020).

Kolejny groźny globalny atak: ransomware Petya (NotPetya). Ofiary także w Polsce. Dotyczy również zaktualizowanych Windowsów!, Niebezpiecznik, 27.06.2017, https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/ (dostęp 30.09.2020).

Kovacs E., *U.S., Canada, Australia attribute NotPetya attack to Russia*, Security Week,16.02.2018, https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia (dostęp 30.09.2020).

Lee T.B., *The WannaCry ransomware attack was temporarily halted. But it's not over yet*, Vox, 15.05.2017, https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp (dostęp 30.09.2020).

M.E.Doc developer signs agreement with SBU on countering cyberattack threats, Interfax Ukraine, 12.07.2018, https://en.interfax.com.ua/news/general/517610.html (dostęp 30.09.2020).

Majdan K., *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware?*, Business Insider, 28.06.2017, https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2 (dostęp 30.09.2020).

Maloney S., *What is an Advanced Persistent Threat (APT)?*, Cybereason, 09.01.2018, https://www.cybereason.com/blog/advanced-persistent-threat-apt (dostęp: 30.09.2020).

Malware Spotlight: What are wipers?, Infosec Institute, 19.11.2019, https://resources.infosecinstitute.com/malware-spotlight-what-are-wipers/#gref (dostęp 30.09.2020).

Microsoft Defender ATP Research Team, *New ransomware, old techniques: Petya adds worm capabilities*, Microsoft, 27.06.2017, https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc (dostęp 30.09.2020).

Nakashima E., *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes*, „The Washington Post", 13.01.2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html (dostęp 30.09.2020).

Newman L.H., *The ransomware meltdown experts warned about is here*, WIRED, 12.05.2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/ (dostęp 30.09.2020).

Oprogramowanie ransomware, Malwarebytes, https://pl.malwarebytes.com/ransomware/ (dostęp 30.09.2020).

Osborne C., *NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs*, ZDNet, 26.01.2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/ (dostęp 30.09.2020).

Palmer D., *Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk*, ZDNet, 16.08.2017, https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (dostęp 30.09.2020).

Palmer D., *Security warning: Attackers are using these five hacking tools to target you*, ZDNet, 11.10.2018, https://www.zdnet.com/article/security-warning-attackers-are-using-these-five-hacking-tools-to-target-you/ (dostęp 30.09.2020).

Perekalin A., *Bad Rabbit: nowa epidemia ransomware*, Kaspersky Blog, 24.10.2017, https://plblog.kaspersky.com/bad-rabbit-ransomware/8396/ (dostęp 30.09.2020).

Petya Ransomware: What we know now, ESET, 27.06.2017, https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/; (dostęp 30.09.2020).

Pompeo M.R., *The United States Condemns Russian Cyber Attack Against the Country of Georgia, Press Statement*, Department of State US, 20.02.2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (dostęp 30.09.2020).

Porup J.M., *What is Mimikatz? And how to defend against this password stealing tool*, CSO Online, 05.03.2019, https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html (dostęp 30.09.2020).

Прикриттям наймасштабнішої кібератаки в історії України став вірус *Petya (Diskcoder.C)* (tłum. na ang.: *Petya virus (Diskcoder.C) became a cover for the largest cyber attack in the history of Ukraine*), Cyberpolice Ukraine, 05.07.2017, https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/ (dostęp 30.09.2020).

Ransomware definition, w: *Cambridge Dictionary Online*, https://dictionary.cambridge.org/pl/dictionary/english/ransomware (dostęp 30.09.2020).

Ransomware, TrendMicro, https://www.trendmicro.com/vinfo/us/security/definition/ransomware; (dostęp 30.09.2020).

Reckless campaign of cyber attacks by Russian military intelligence service exposed, National Cyber Security Centre UK, 03.10.2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (dostęp 30.09.2020).

Rouse M., *Obfuscation definition*, Techtarget, https://searchsoftwarequality.techtarget.com/definition/obfuscatio (dostęp 30.09.2020).

Rządowy zespół kryzysowy o cyberatakach, IAR, 28.06.2017, https://www.polskieradio.pl/78/1227/Artykul/1782601,Rzadowy-zespol-kryzysowy-o-cyberatakach; (dostęp 30.09.2020).

Smith B., *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, Microsoft Blog, 14.05.2017, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ (dostęp 30.09.2020).

Symantec Security Response Team, *What you need to know about the WannaCry Ransomware*, Symantec (Broadcom), 23.10.2017, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack (dostęp 30.09.2020).

Tactics, Techniques and Procedures, Radware, 09.12.2019, https://security.radware.com/ddos-experts-insider/hackers-corner/tactics-techniques-procedures/ (dostęp 30.09.2020).

TeleBots aka Sanworm, Malpedia, https://malpedia.caad.fkie.fraunhofer.de/actor/telebots (dostęp 30.09.2020).

The Dukes. 7 Years of Russian Cyberespionage, F-Secure, 09.2016, https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf (dostęp 30.09.2020).

Threat Intelligence Report OPERATION 'Rocket Man', Security Response Center (ESRC), 08.2018, http://blog.alyac.co.kr/attachment/cfile24.uf@99219C4F5BC3F4E01751D3.pdf (dostęp 30.09.2020).

V. Chebyshev et al., *IT threat evolution Q3 2019. Statistics*, Securelist Kaspersky, 29.11.2019, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/ (dostęp 30.09.2020).

Voreacos D., Chiglinsky K., Griffin R., *Merck cyberattack's $1.3 billion question: Was it an act of war?*, Bloomberg, 03.12.2019, https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (dostęp 30.09.2020).

Wakefield J., *Tax software blamed for cyber-attack spread*, BBC, 28.06.2017, https://www.bbc.com/news/technology-40428967 (dostęp 30.09.2020).

WannaCry Ransomware, EUROPOL EC3, https://www.europol.europa.eu/wannacry-ransomware; (dostęp 30.09.2020).

WannaCry: BSI ruft Betroffene auf, Infektionen zu melden, Heise Online, https://www.heise.de/newsticker/meldung/WannaCry-BSI-ruft-Betroffene-auf-Infektionen-zu-melden-3713442.html (dostęp 30.09.2020).

What Is an Advanced Persistent Threat (APT)?, Cisco, https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html (dostęp 30.09.2020).

Wiele polskich firm zostało zaatakowanych przez wirusa Petya, Polskie Radio 24, 28.06.2017, https://www.polskieradio.pl/130/3993/Artykul/1782398,Wiele-polskich-firm-zostalo-zaatakowanych-przez-wirusa-Petya (dostęp 30.09.2020).

Media społecznościowe

Post opublikowany na portalu społecznościowym Facebook, https://www.facebook.com/medoc.ua/posts/1904044929883085 (dostęp 30.09.2020).

Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/craiu/status/880343543373586432 (dostęp 30.09.2020).

Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/Snowden/status/863425539616284673 (dostęp 30.09.2020).

Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/kaspersky/status/879749175570817024/photo/1 (dostęp 30.09.2020).

Post opublikowany na portalu społecznościowym Twitter, https://twitter.com/CyberpoliceUA/status/879772963658235904?s=20 (dostęp 30.09.2020).

Konflikt interesów

Brak

Źródło finansowania

Brak