Maksymilian Bogut

e-mail: 177332@ue.wroc.pl

ORCID: 0009-0006-4451-6027

Uniwersytet Ekonomiczny we Wrocławiu

Zagrożenie cyberbezpieczeństwa w Europie Środkowo-Wschodniej związane z działalnością grupy *Advanced Persistent Threat Sandworm*

DOI: 10.15611/2024.80.2.02
JEL Classification: L86, Y90

Cytuj jako: Bogut, M. (2024). Zagrożenie cyberbezpieczeństwa w Europie Środkowo-Wschodniej związane z działalnością grupy *Advanced Persistent Threat Sandworm*. W: H. Dudycz (red.), *Informatyka w biznesie* (s. 23-35). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Streszczenie: Artykuł koncentruje się na działalności grup *Advanced Persistent Threat* (APT) i ich ogromnego wpływu na zagrożenie cyberbezpieczeństwa w Europie Środkowo-Wschodniej. Zdefiniowano w nim aktualne zagrożenia bezpieczeństwa oraz sklasyfikowano typy aktorów, w tym grupy APT. Szczegółowej analizie poddano grupę APT o nazwie Sandworm, tj. jej funkcjonowanie w Europie Środkowo-Wschodniej wraz z przebiegiem podejmowanych działań i ich skutków dla tego regionu.

Słowa kluczowe: cyberbezpieczeństwo, APT, Europa Środkowo-Wschodnia, złośliwe oprogramowanie, Sandworm

1. Wstęp

Bezpieczeństwo cyfrowe stało się jednym z najważniejszych wyzwań współczesnego świata. W tym kontekście ataki grupy *Advanced Persistent Threat* (APT) stanowią jedno z najpoważniejszych zagrożeń dla organizacji, instytucji oraz państw. W Europie Środkowo-Wschodniej, gdzie czynniki geopolityczne i historyczne odgrywają od wieków istotną rolę, działalność takich grup jak Sandworm może mieć znaczące konsekwencje dla stabilności i bezpieczeństwa regionu. Ataki te, charakteryzujące się zaawansowaniem technologicznym, wytrwałością i złożonością operacyjną, mogą być prowadzone pod wpływem różnych motywacji, w tym politycznych, ekonomicznych czy strategicznych. Ich cele mogą obejmować szpiegostwo, destabilizację polityczną, a nawet eskalację konfliktów międzynarodowych.

Grupy APT operujące w Europie Środkowo-Wschodniej często wykorzystują unikatowe narzędzia i techniki dostosowane do specyfiki regionu i jego infrastruktury informatycznej. Przykładami takich działań, które miały miejsce w ostatnich latach, są ataki na instytucje rządowe, przedsiębiorstwa energetyczne, a nawet media. Powodują one nie tylko bezpośrednie szkody dla ofiar, ale także podważają zaufanie do instytucji i destabilizują środowisko biznesowe i społeczne.

W kontekście dynamicznie zmieniającego się krajobrazu cyberbezpieczeństwa badanie ataków grup APT w Europie Środkowo-Wschodniej ma poważne implikacje dla polityki bezpieczeństwa, zarządzania ryzykiem oraz strategii obronnych. Odpowiednie zrozumienie zagrożeń i skuteczne reagowanie na nie wymaga współpracy międzynarodowej, innowacji technologicznej, a także ciągłego doskonalenia umiejętności i narzędzi obronnych. Niniejsza praca stanowi zatem wkład w dyskusję na temat bezpieczeństwa cybernetycznego w Europie Środkowo-Wschodniej oraz może przyczynić się do opracowania bardziej efektywnych strategii obronnych i polityk bezpieczeństwa.

Celem artykułu jest przedstawienie wyników przeprowadzonego badania, obejmującego analizę działań wybranych grup APT w ostatnich latach w Europie Środkowo-Wschodniej, które miały znaczący wpływ na szeroko rozumiane społeczeństwo. Skoncentrowano się przede wszystkim na przestawieniu grupy APT o nazwie Sandworm, prowadzonych przez nią kampaniach i stosowanych metodach, typowych dla cyberprzestępczości, oraz na identyfikacji obszarów wymagających wzmocnienia ochrony. Kluczowe pytanie badawcze brzmi: Jakie skutki mogą wynikać z prowadzonej działalności przez grupy *Advanced Persistent Threat*?

W podjętym badaniu połączono kilka metod: studia przypadków, analizę złośliwych dokumentów, sumy kontrolne oraz wykorzystanie różnych dokumentów pochodzących od firm specjalizujących się w dziedzinie cyberbezpieczeństwa.

2. Definicja zagrożeń cybernetycznych

Cyberbezpieczeństwo, znane również jako bezpieczeństwo informatyczne, to obszar nauki zajmujący się ochroną systemów informatycznych, sieci komputerowych, danych elektronicznych oraz infrastruktury cyfrowej przed atakami, nieautoryzowanym dostępem, utratą poufności, niszczeniem lub kradzieżą informacji (Cisa, b.d.). Celem cyberbezpieczeństwa jest zapewnienie integralności, dostępności i poufności danych, a także zabezpieczenie systemów przed wszelkimi zagrożeniami związanymi z przestrzenią cybernetyczną (Wikipedia, 2023).

Zagrożenie cybernetyczne określa się jako m.in. „działanie, które może skutkować nieautoryzowanym dostępem, wyciekiem, manipulacją lub naruszeniem integralności, poufności lub dostępności systemu informatycznego lub informacji przechowywanych, przetwarzanych lub przesyłanych przez system informacyjny" (National Institute of Standards and Technology, b.d.).

Według kryterium podziału sposobu przeprowadzenia ataku wyróżnia się następujące główne kategorie zagrożeń cybernetycznych (Cisco, 2018):

- złośliwe oprogramowanie (*malware*) – obejmuje m.in.: wirusy, trojany, robaki komputerowe i *ransomware*, które infiltrują systemy w celu zniszczenia, zakłócenia lub kradzieży danych;
- ataki hackerskie – polegają na nieautoryzowanym dostępie do systemów komputerowych, sieci czy baz danych w celu kradzieży informacji, zakłócenia działania systemów lub ich zniszczenia;
- *phishing* – wysyłanie fałszywych wiadomości;
- ataki odmowy dostępu – obejmują przeciążanie systemu czy serwera dużą liczbą żądań, uniemożliwiając normalne funkcjonowanie usługi lub dostępu do zasobów;
- ataki na systemy IoT (*Internet of Things*) – cyberprzestępcy mogą celować w urządzenia związane z Internetem, takie jak kamery, urządzenia domowe czy samochody, aby przejąć kontrolę nad nimi lub wykorzystać do szkodliwych działań;
- ataki na aplikacje internetowe – polegają na wykorzystywaniu podatności w oprogramowaniu internetowym do nieautoryzowanego dostępu do danych czy naruszenia prywatności użytkowników;
- zagrożenia związane z socjotechniką – atakujący wykorzystują manipulację psychologiczną, np. poprzez inżynierię społeczną, aby oszukać użytkowników i zdobyć poufne informacje;
- zagrożenia związane z nieaktualnym oprogramowaniem: ataki na podatności w systemach lub aplikacjach, które nie zostały zaktualizowane, aby wykorzystać słabe punkty w zabezpieczeniach.

Najpopularniejszą metodą dostarczenia złośliwego oprogramowania jest *phishing*. Polega on na wysyłaniu wiadomości e-mail do użytkowników w celu nakłonienia ich do ujawnienia danych osobowych lub kliknięcia łącza. Atak phishingowy często kieruje użytkownika na złośliwą stronę internetową, która przedstawia się użytkownikowi jako legalna witryna oraz używa elementów socjotechniki (Trendmicro, 2016).

Podsumowując, zagrożenia cybernetyczne występują w wielu formach, a każda z nich niesie specyficzne ryzyko dla systemów informatycznych. Różnorodność tych zagrożeń sprawia, że są one trudne do przewidzenia i zwalczania. Zrozumienie typologii zagrożeń jest kluczowe dla oceny ryzyka i skutecznego reagowania na incydenty cybernetyczne.

3. Rodzaje aktorów zagrożeń oraz definicja i charakterystyka działania grup *Advanced Persistent Threat*

Aktorami zagrożeń są osoby, grupy lub organizacje odpowiedzialne za szeroko rozumiane szkodliwe działania. Motywowani są często zyskiem finansowym, korzyściami politycznymi lub po prostu chęcią wyrządzenia szkody (Gibson, 2017, s. 22). Dzięki zrozumieniu koncepcji aktorów zagrożeń organizacje i jednostki mogą być bardziej świadome i lepiej przygotowane do obrony przed złośliwymi atakami.
Wyróżniamy następujące rodzaje aktorów (Gibson, 2017, s. 23):

- aktorzy państwowi – finansują ich rządy państw, związani są z wieloma atakami zwłaszcza na systemy krytyczne, takie jak energetyka czy bankowość. Cele aktorów państwowych to głównie szpiegostwo i uzyskanie przewagi strategicznej, ale także cele czysto komercyjnie. Niektóre państwa sponsorują wiele grup przeciwników, a te grupy mogą mieć różne dążenia, zasoby i stopnie współpracy między sobą (Cisa, b.d.);
- przestępczość zorganizowana – wielu krajach cyberprzestępczość przewyższa pospolite przestępstwa zarówno pod względem liczby incydentów, jak i strat. Grupa przestępczości zorganizowanej może działać w poza strefą jurysdykcji, której podlega, co zwiększa złożoność procesu sądowego. Przestępczość zorganizowana wykorzystuje każdą okazję do osiągnięcia zysków, a jej typowymi działaniami są oszustwa finansowe przeciwko jednostkom i firmom oraz szantaż (McAfee, 2021);
- Haktywiści – mogą próbować pozyskać i ujawnić poufne informacje publicznie, przeprowadzać ataki typu „odmowa usługi" (ang. *distributed denial of service* – DDoS) lub dokonywać ataków typu *defacement* na strony internetowe. Najbardziej narażone na ataki tych grup są instytucje i firmy działające we wrogim kraju. Atakowane są podmioty z sektora politycznego, medialnego i finansowego, a także krytyczna infrastruktura państwa. Grupy haktywistyczne, takie jak Anonymous Russia (Radware, 2024), Killnet (Avertium, 2022) czy NoName057(16) (Watt, 2024), wykorzystują cyberbronie do promowania agendy politycznej;
- *Script Kiddie* – jest to osoba korzystająca z narzędzi hakerskich, niekoniecznie rozumiejąca ich działanie ani nieposiadająca zdolności do tworzenia nowych ataków. Ataki ze strony *Script Kiddie* mogą nie mieć konkretnego celu poza zdobyciem uwagi lub udowodnieniem umiejętności technicznych. Mimo to przeprowadzane przez takie osoby działania mogą wyrządzać znaczne szkody, jeżeli cel ataków nie jest odpowiednio zabezpieczony (Okta, 2024).

Termin *Advanced Packaging Tool* pierwotnie odnosił się do grupy stojącej za kampanią, ale znaczenie tego wyrażenia zostało rozszerzone na narzędzia przez nią wykorzystywane. Taka koncepcja pomaga lepiej modelować zagrożenia. Natomiast ataki APT są zazwyczaj wymierzone w duże organizacje, takie jak instytucje finansowe, firmy w służbie zdrowia i inne, które przechowują duże liczby poufnych danych

osobowych, szczególnie gdy te informacje dotyczą ważnych osobistości w państwie, jak chociażby polityków (Marchant, 2023).

Grupy APT wyróżniają się zestawem cech definiujących, które odróżniają je od innych rodzajów zagrożeń cyberbezpieczeństwa. Zrozumienie tych podstawowych cech ma kluczowe znaczenie dla dokładnej identyfikacji grupy APT i odróżnienia jej od innych rodzajów cyberataków.

Dzięki różnym metodom analiz działań grup cyberprzestępczych, ich infrastruktury i indykatorów kompromitacji, analitycy dokonują atrybucji ataków do danej grupy. Wiodące firmy w zakresie analiz cyberzagrożeń mają różne nazewnictwa grup, np. w nomenklaturze firmy CrowdStrike określenie „BEAR" reprezentuje Rosję, „CHOLLIMA" – Koreę Północną, „PANDA" – Chiny, „KITTEN" – Irak, a nazwa „SPIDER" jest używana, gdy dana grupa nie ma wsparcia rządowego. Z kolei Microsoft dla grup z Rosji używa określenia „Blizzard", dla grup z Chin – „Typhoon" itd. Ta różnica w nazewnictwie wynika z różnych danych, które obsługują te przedsiębiorstwa (Crowdstrike, 2024).

W przypadku uniwersalnego systemu nazewnictwa grupa, która nie została jeszcze oficjalnie zidentyfikowana, jak APT1 lub APT37, może zostać błędnie przypisana do innej grupy. Mając osobne nazewnictwo, mimo że bywa ono uciążliwe dla badaczy ze względu na sporą liczbę nazw dla jednej grupy atakujących, jest ona opisywana z większą rzetelnością na podstawie dostępnych danych i analiz (Poireault, 2023).

Podsumowując, grupy APT stanowią zaawansowane i długotrwałe zagrożenia, które często mają strategiczne cele dyktowane przez stojące za nimi państwa. Aktorzy zagrożeń cybernetycznych różnią się pod względem motywacji i metod działania, co sprawia, że stanowią poważne wyzwanie dla bezpieczeństwa informatycznego. Zrozumienie tych zagrożeń jest kluczowe dla skutecznego przeciwdziałania ich wpływowi.

4. Charakterystyka grupy Sandworm

Sandworm to rosyjska grupa APT, która jest przypisywana Głównemu Zarządowi Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Jest ona określona również takimi nazwami, jak: Blue Echidna. ELECTRUM, FROZENBARENTS, G0034, IRIDIUM, IRON VIKING, Quedagh, Seashell Blizzard, TEMP.Noble, TeleBots, UAC-0113, VOODOO BEAR (Malpedia, 2024). Działając od co najmniej 2011 roku, grupa prowadzi operacje głównie w celach szpiegostwa, dezinformacyji i destrukcji. Cyberoperacje związane z GRU są często kojarzone z Jednostką Wojskową 74455, znaną również jako Główne Centrum Technologii Specjalnych (Malpedia, 2024).

Zasadniczym celem działań Sandworm, według oceny badaczy, jest przyczynianie się do operacji mających na celu degradację, delegitymizację lub wpływanie na zaufanie publiczne do instytucji państwowych i sektorów przemysłowych w krajach docelowych.

Sandworm brał udział w atakach destrukcyjnych i zakłócających przeciwko celom na Ukrainie zwłaszcza pomiędzy 2015 a 2017 rokiem oraz od lutego 2022 roku. Publiczne oskarżenia ze strony rządu USA łączą operatorów Sandworm z operacjami intruzji wobec wyborów stanowych w USA w 2016 roku, a także wsparciem publicznego rozpowszechniania poufnych danych uzyskanych poprzez kompromitację międzynarodowych organizacji sportowych (Departament of Justice, 2020).

Sandworm wspiera również z wysokim prawdopodobieństwem rozpowszechnianie danych uzyskanych w ramach innych kampanii cybernetycznych prowadzonych przez GRU, stosując różne pozorne atrybucje. APT brała również udział w atakach zakłócających, w tym atakach rozproszonych w usłudze odmowy dostępu (DDoS) wymierzonych w ukraińskie instytucje finansowe w listopadzie 2016 roku oraz w naruszaniu stron internetowych Gruzji w październiku 2019 (Pompeo, 2020).

Operacje grupy Sandworm obejmują dostosowane warianty powszechnie używanych złośliwych programów, zaawansowane specjalnie opracowane złośliwe oprogramowanie z możliwościami destrukcyjnymi (np.: Industroyer, NotPetya, BadRabbit, OlympicDestroyer) oraz nowatorskie taktyki instalacji początkowego ładunku. W ramach strategii dezinformacji niektóre narzędzia używane przez Sandworm zawierają fałszywe wskazania pochodzenia kryminalnego, takie jak maskowanie się jako *ransomware* lub inne zasadzone artefakty techniczne mające utrudnić dokładną atrybucję (Hultquist, 2022).

Podsumowując, grupa Sandworm jest znana z wielu sposobów zaawansowanych ataków cybernetycznych. Jest uważana za jedną z najbardziej aktywnych grup APT związanych z rosyjskimi interesami. Jej działania skupiają się na celach o strategicznym znaczeniu, takich jak infrastruktura energetyczna i polityczne instytucje. Sandworm jest znana z wykorzystania zaawansowanych narzędzi i technik, w tym złośliwego oprogramowania. Jej operacje cechuje wysoki poziom złożoności i skoordynowania, co czyni je trudnymi do wykrycia przez systemy bezpieczeństwa.

5. Analiza działalności grupy Sandworm

W niniejszym punkcie chronologicznie uporządkowano ataki oraz kampanie grupy Sandworm wraz z omówieniem narzędzi stosowanych przez atakujących i etapach ich rozwoju, przeprowadzono analizę pozyskanych plików zawierających złośliwe oprogramowanie, a także przedstawiono motywacje, cele i techniki działania grupy wraz z geopolitycznym tłem.

Nazwa grupy wzięła się z analizy dokumentu Powerpoint zawierającego lukę *zero-day* w 2014 roku. Luka tego typu jest określeniem branżowym i oznacza ukrytą lukę w zabezpieczeniach oprogramowania, o której nie wie firma tworząca i utrzymująca oprogramowanie. Podmiot odpowiadający za oprogramowanie ma w zasadzie „zero dni" na reakcję i opublikowanie aktualizacji w celu ochrony użytkowników.

Sama prezentacja zawierała jeden slajd z tłem w kolorach ukraińskiej flagi, na którym znajdowało się wiele nazwisk rzekomych terrorystów – osób, które stanęły

po stronie rosyjskiej w toczącym się konflikcie. Antyrosyjska treść miała na celu przykucie uwagi potencjalnej ofiary. Po otwarciu załącznika następowała infekcja znanym w środowisku hakerskim złośliwym oprogramowaniem BlackEnergy.

Analiza kodu i przebiegu infekcji dokumentu Powerpoint pozwoliła badaczom z firmy iSight na odnalezienie klucza deszyfrującego kod programu, a kolejne tygodnie ciężkiej pracy odkryły konfigurację złośliwego oprogramowania. Zawierała ona kod kampanii i tag związany z wersją BlackEnergy – „arrakis02". Zwrot pochodził z powieści *science fiction* Franka Herberta *Diuna*. Analiza kolejnych próbek znalezionych na stronie Virustotal pozwoliła na odkrycie kolejnych nawiązań do powieści, a także treści dokumentów, które – jak się okazało – nie były rozsyłane wyłącznie na Ukrainie. Jeden z dokumentów dotyczył wydarzenia związanego z NATO, które odbywało się na Słowacji, inny dotyczył międzynarodowego spotkania w Walii, na którym miano omawiać aktualną sytuację Ukrainy, a jeszcze inny skierowany został do polskiej firmy energetycznej (Ward, 2014).

W dniu 23 grudnia 2015 roku Prykarpattyaoblenergo, firma dostarczająca energię w zachodniej części Ukrainy, w regionie Iwano-Frankiwsk, padła ofiarą ataku cybernetycznego, który spowodował przerwę w dostawie prądu w regionie. Tego samego dnia przedsiębiorstwo Kyivoblenergo, inny ukraiński dostawca energii, potwierdziło, że cybernetyczne włamanie do systemów kontrolnych spowodowało przerwę w dostawie prądu w ich sieci. Tego typu atak był zgodny z charakterystyką działań grupy APT Sandworm (Greenberg, 2021, s. 76-78).

Po niszczycielskich atakach w grudniu zaobserwowano serię wiadomości phishingowych skierowanych przeciwko ukraińskim podmiotom z sektora rządowego i energetycznego, w tym organizacjom, na które wcześniej miały wpływ operacje z oprogramowaniem wymazującym dane. Treść tych wiadomości była związana z planowaniem w sektorze energetycznym, a każda z nich zawierała załączony złośliwy dokument Microsoft Office, który zawierał osadzony makroskrypt uruchamiający instancję BlackEnergy. Była to ta sama technika, którą używano w atakach na sektor energetyczny (Trendmicro, 2016).

Od czasu tej zmiany nie zaobserwowano nowych kopii BlackEnergy, natomiast przez cały 2016 rok zidentyfikowano kolejne wersje GCat[1] wdrażane przez ten sam skrypt makr ukryty w złośliwych dokumentach.

Podejrzewa się, że zmiana narzędzi i złośliwego oprogramowania była częścią reorganizacji aktora w związku z przykuciem uwagi międzynarodowych mediów szczególnie po atakach na Ukrainę w 2015 roku. Do prowadzenia kolejnych destrukcyjnych i dezinformacyjnych działań grupa potrzebowała nowych narzędzi, których nie dało się przypisać Rosji, a które mogłyby celowo wprowadzać w błąd analityków cyberzagrożeń podczas analizy programów. Dlatego użycie narzędzia publicznie dostępnego i przerobienie go miało łączyć atakujących ze zwykłymi cybeprzestępcami lub grupą rosyjskich haktywistów. Złośliwe oprogramowanie BlackEnegy za bardzo

[1] Zob. https://github.com/byt3bl33d3r/gcat

kojarzono medialnie i politycznie z działalnością GRU i to zapewne było jednym z powodów odstąpienia od używania go. Dodatkowo firmy w Ukrainie korzystały z analiz zagranicznych analityków, a stworzone przez nich kolejne reguły antymalware pozwalały coraz lepiej wykrywać BlackEnergy mimo zmieniających się wersji oprogramowania.

Między styczniem a marcem 2017 roku Sandworm z dużym prawdopodobieństwem wykorzystywał skrypt Microsoft Visual Basic Script (VBS) w celu uzyskania początkowego dostępu do zainfekowanych systemów. Artefakty techniczne w analizowanym dokumencie o sumie kontrolnej MD5:

c478ca76cd80fe2e82bcb0c40ba00ac8[2]

wskazują, że ten *backdoor* prawdopodobnie był używany w kampanii przeciwko ukraińskiej instytucji finansowej. Został on zaprojektowany w celu zapewnienia początkowego przyczółku dla atakujących i wsparcia lateral movementu. W ramach trwających działań operacyjnych grupa atakowała również łańcuchy dostaw ukraińskich instytucji państwowych.

Począwszy od 18 maja 2017 roku, odnotowano infekcje ukraińskich systemów przez złośliwe oprogramowanie ransomware o nazwie XDATA za pośrednictwem nieznanego wektora infekcji. Późniejsze dochodzenia wykazały, że infekcja rozprzestrzeniała się poprzez aktualizacje ukraińskiego oprogramowania M.E. Doc (Greenberg, 2021, s. 221).

W dniu 27 czerwca 2017 roku jedna z firm zajmująca się cyberbezpieczeństwem wydała ostrzeżenie o nowym oprogramowaniu ransomware o nazwie NotPetya, szybko rozprzestrzeniającym się w sieciach z głównym źródłem infekcji na Ukrainie przy użyciu tych samych metod co XDATA. Atak zbiegł się w czasie z ukraińskim świętem – Dniem Konstytucji, który został prawdopodobnie wybrany przez atakujących z powodu potencjalnie opóźnionego czasu reakcji ze strony obrońców sieci, a także w celu wykorzystania psychologicznego wpływu zakłóceń.

Zawieszenie Rosyjskiego Komitetu Olimpijskiego w prawach członka Międzynarodowego Komitetu Olimpijskiego przed zimowymi igrzyskami olimpijskiego w Pyeongchangu w 2018 roku spowodowało międzynarodową aferę. W odwecie Kreml przeprowadził liczne kampanie phishingowe, a następnie podczas ceremonii otwarcia 9 lutego 2018 roku wdrożył złośliwe oprogramowanie, nazwane potem OlympicDestroyer. Destrukcyjne oprogramowanie zawierało wiele wskaźników technicznych, mających na celu zmylenie osób analizujących kod programu i miało nakłonić badaczy do atrybucji OlympicDestroyera do aktorów z Korei Północnej.

W dniu 28 maja 2020 roku amerykańska Agencja Bezpieczeństwa Narodowego (NSA) wydała komunikat opisujący wykorzystanie luki w oprogramowaniu *open-source Exim mail transfer agent* (MTA) przez operatorów z rosyjskiego Głównego

[2] Zob. https://www.virustotal.com/gui/file/587b6377a3e069c1f399cb480729bbc70665cdd25af95f859f4b0a767463b3d3/detection

Zarządu Wywiadowczego od co najmniej sierpnia 2019 roku. W raporcie wyraźnie przypisano działania wykorzystujące tę konkretną lukę w zabezpieczeniach (CVE-2019-10149) do Głównego Centrum Technologii Specjalnych GRU, znanego szerzej jako Jednostka GRU 74455, którą badacze cyberbezpieczeństwa łączą z grupą Sandworm (National Security Agency, 2020).

W dniu 6 marca 2022 roku do repozytorium Virustotal została przesłana próbka złośliwego oprogramowania HermeticWizard – robaka, który propagował DriveSlayer, destrukcyjnego wipera wdrożonego w kilku ukraińskich podmiotach przed rosyjską inwazją na Ukrainę 24 lutego 2022 roku.

Zaawansowanie techniczne, ukierunkowanie, wpływ psychologiczny i wysokopoziomowe techniki HermeticWizard i DriveSlayer są podobne do wcześniejszych operacji przypisywanych grupie Sandworm.

HermeticWizard został celowo zaprojektowany tak, aby ograniczyć jego rozprzestrzenianie się do sieci lokalnej, ograniczając infekcje głównie do Ukrainy. Kontrastuje to z oprogramowaniem NotPetya, którego infekcja rozpoczęła się na Ukrainie, ale szybko rozprzestrzeniła się w sieciach międzynarodowych.

Zespół Reagowania na Incydenty Komputerowe Ukrainy (CERT-UA) 12 kwietnia 2022 roku wydał oświadczenie, identyfikując nowe ataki wymierzone w ukraiński sektor energetyczny z operacjami grupy Sandworm. Ataki te obejmowały nowy wariant złośliwego oprogramowania zbudowanego dla systemu Windows, który został wykorzystany do ataku na ukraińskiego dostawcę energii w 2016 roku – znany również jako Industroyer lub CrashOverride. Nowy wariant oprogramowania składał się z pojedynczego pliku binarnego, który w dużym stopniu przypominał jeden z modułów z oryginalnego ataku z 2016 roku i zawierał zakodowaną na stałe konfigurację (CERT-UA, 2022).

Podsumowując przeprowadzoną analizę działalności grupy Sandworm, można stwierdzić, że jest to zaawansowana cyberjednostka, której funkcjonowanie jest powiązywane z rosyjską służbą wywiadowczą GRU. Grupa zasłynęła z przeprowadzania destrukcyjnych cyberataków na różne cele na całym świecie. Najbardziej znane operacje obejmują atak na ukraińską sieć energetyczną w 2015 roku, który spowodował przerwy w dostawach prądu dla setek tysięcy ludzi, oraz operację NotPetya w 2017 roku, która miała katastrofalne skutki dla wielu globalnych przedsiębiorstw, powodując miliardowe straty. Grupa jest także powiązywana z atakami na infrastrukturę informatyczną igrzysk olimpijskich w Pjongczangu w 2018 roku oraz wieloma innymi atakami na sektory rządowe, finansowe i energetyczne w różnych krajach. Działania Sandwormu są często interpretowane jako element cyberwojny hybrydowej, mającej na celu destabilizację przeciwników Rosji oraz wywołanie chaosu na arenie międzynarodowej.

6. Skutki działalności grupy Sandworm

Przeprowadzana analiza działalności badanej grupy pokazuje wykorzystanie cyberataków do procesu destabilizacji politycznej w krajach Europy Środkowo-Wschodniej. Krajem wymagającym szczególnej uwagi jest Ukraina, która była i nadal jest wykorzystywana jako poligon doświadczalny dla rosyjskich i białoruskich grup. Właśnie tam wykorzystują one nowe narzędzia i techniki na podatnych systemach informatycznych, a przy okazji sprawdzają integralność Unii Europejskiej, jak i NATO w kontekście reakcji na ataki, dostarczając cennej wiedzy wywiadowi własnych państw. Do osiągania tych celów wykorzystywane są coraz bardziej złożone metody ataków, a także wyszkolony personel związany z państwowymi służbami.

Skutki działalności grupy Sandworm mają zdecydowanie znaczący wpływ na bezpieczeństwo i stabilność w Europie Środkowo-Wschodniej. Są one następujące:

1. Naruszenie Bezpieczeństwa Narodowego – ataki grup APT mogą prowadzić do poważnych naruszeń bezpieczeństwa narodowego, zwłaszcza jeśli są one powiązane z państwowymi instytucjami czy krytyczną infrastrukturą, taką jak sektor energetyczny czy komunikacyjny. Wdrażając swoje zaawansowane techniki, grupy te mogą zagrażać suwerenności państw i ich zdolności do obrony.
2. Szpiegostwo przemysłowe – działania grup APT mogą prowadzić do kradzieży poufnych danych, technologii i informacji handlowych, co z kolei może prowadzić do znaczących strat finansowych oraz utraty konkurencyjności firm i branż.
3. Destabilizacja polityczna – ataki grup APT mogą mieć na celu destabilizację polityczną w regionie poprzez manipulację informacjami, dezinformację oraz ingerencję w procesy demokratyczne. Wykorzystując cyberprzestrzeń do propagowania fałszywych narracji, mogą podsycić konflikty i napięcia społeczne.
4. Usługi dla państw sponsora – grupy APT często działają na zlecenie państw-aktorów, które wykorzystują je do realizacji swoich politycznych, militarnych czy gospodarczych celów. Działając jako narzędzia agresji hybrydowej, mogą prowadzić ataki w ramach szerszych kampanii wpływu.
5. Wzrost kosztów obrony – działalność grup APT wymusza na państwach oraz firmach zwiększone wydatki na obronę cybernetyczną. Wdrażanie zaawansowanych narzędzi, szkolenie personelu oraz stała aktualizacja zabezpieczeń stają się niezbędne dla zachowania odporności na tego typu zagrożenia.
6. Utrata zaufania społecznego – ataki grup APT mogą prowadzić do utraty zaufania społecznego do instytucji, organizacji i technologii cyfrowych. Poczucie bezpieczeństwa jednostek i podmiotów gospodarczych może zostać naruszone, co z kolei wpływa na funkcjonowanie społeczeństwa oraz gospodarki.

Wnioski płynące z przeprowadzonej analizy działalności badanej grupy APT wskazują na konieczność zwiększenia świadomości oraz wzmocnienia obronności w Europie Środkowo-Wschodniej. Wdrażanie kompleksowych strategii bezpieczeństwa cybernetycznego, współpraca międzynarodowa oraz inwestycje w nowoczesne technologie są kluczowe dla zapewnienia odporności na ataki grup APT

i zachowania bezpieczeństwa w regionie. Ponadto analiza ta podkreśla konieczność dalszych badań nad metodami i strategiami działania grup APT oraz adaptacji obronnych środków w celu skuteczniejszego przeciwdziałania temu typowi zagrożeń w przyszłości.

7. Zakończenie

W niniejszym artykule dokonano szczegółowej analizy ataków grup APT w Europie Środkowo-Wschodniej ze szczególnym uwzględnieniem działania rosyjskiej grupy Sandworm. Analizując te zagrożenia, zidentyfikowano ich charakterystyczne cechy, sposoby działania oraz konsekwencje dla regionu. Wyniki przeprowadzonego badania pozwalają na lepsze zrozumienie mechanizmów, jakimi posługują się cyberprzestępcy, oraz identyfikację obszarów wymagających wzmocnienia ochrony.

Analiza działań grup takich jak Sandworm pokazuje, że cyberataki mogą być elementem większej strategii konfliktu hybrydowego, w którym cyberoperacje są połączone z innymi formami agresji – dezinformacją lub wojną informacyjną. To zwraca uwagę na potrzebę rozwoju koncepcji i teorii dotyczących zagrożeń hybrydowych.

Aby zrozumieć pełny kontekst badania i jego wpływów na dalsze prace naukowe warto przedstawić potencjalne ograniczenia bieżących, jak i przyszłych badań. W przypadku badania działań grup *Advanced Persistent Threat*, jak Sandworm, uzyskanie pełnych informacji na temat ich operacji jest niezwykle trudne. Działania te są przeważnie utajnione, co może prowadzić do niepełnych i błędnych wniosków. Informacje o działalności grup często pochodzą z raportów komercyjnych firm zajmujących się cyberbezpieczeństwem, które mogą mieć własne interesy w przedstawianiu swoich odkryć, co może wprowadzać błąd w interpretacji danych. Raporty mogą być również bazowane na przypuszczeniach, a nie twardych faktach. Warto również wspomnieć o dynamice zagrożeń cybernetycznych, która jest wyjątkowo zmienna. Narzędzia, taktyki i techniki grup mogą się bardzo szybko zmieniać w czasie, a więc wnioski wyciągnięte z badania mogą stać się szybko nieaktualne oraz nie odzwierciedlać bieżącego stanu zagrożenia.

Jednym z kluczowych wniosków płynących z tej pracy jest konieczność zacieśnienia współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa. Ataki grup APT, tak jak całe cyberbezpieczeństwo, nie znają granic państwowych, dlatego też efektywna obrona wymaga wspólnych działań i wymiany informacji pomiędzy krajami. Dalsze inwestycje w rozwój mechanizmów detekcji i reagowania na ataki oraz szkolenie personelu odpowiedzialnego za bezpieczeństwo informatyczne są niezbędne dla zwiększenia odporności regionu na tego typu zagrożenia.

Należy również podkreślić rolę edukacji i świadomości cyberbezpieczeństwa w społeczeństwie. Wiedza o potencjalnych zagrożeniach oraz umiejętność rozpoznawania ich może znacząco zmniejszyć ryzyko udanego ataku grupy APT. W związ-

ku z tym należy kontynuować kampanie informacyjne oraz szkolenia adresowane do różnych grup społecznych, aby podnieść poziom świadomości i umiejętności w zakresie ochrony danych i systemów informatycznych.

Perspektywy na przyszłość obejmują dalsze badania nad ewolucją technik i narzędzi stosowanych przez grupy APT oraz opracowanie skuteczniejszych strategii obronnych. Konieczne jest również monitorowanie sytuacji geopolitycznej, która może wpływać na dynamikę cyberkonfliktów w regionie. Tylko poprzez stałą analizę i adaptację strategii obronnych da się skutecznie przeciwdziałać zagrożeniom ze strony grup APT oraz utrzymać bezpieczeństwo cyfrowe w Europie Środkowo-Wschodniej.

Wnioski wypływające z tej pracy stanowią istotny wkład w dyskusję na temat bezpieczeństwa cybernetycznego w regionie. W rezultacie skuteczna obrona przed atakami grup APT wymaga współpracy, innowacji i zaangażowania ze strony zarówno sektora publicznego, jak i prywatnego. Jednakże, wraz z rozwojem technologicznym i ewolucją zagrożeń, konieczne będzie ciągłe doskonalenie strategii i narzędzi obronnych, aby dotrzymać tempa dynamicznie zmieniającemu się krajobrazowi zagrożeń.

Literatura

Avertium. (2022, 18 października). *An In-Depth Look at Russian Threat Actor, Killnet.* Avertium.com. Pobrano 18 września 2024 z https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-russian-threat-actor-killnet

CERT-UA. (2022). *Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435).* Cert.gov.ua. Pobrano 16 lutego 2024 z https://cert.gov.ua/article/39518

Cisa. (2021, 1 lutego). *What is Cybersecurity?* America's Cyber Defence Agency. Cisa.gov. Pobrano 13 stycznia 2024 https://www.cisa.gov/news-events/news/what-cybersecurity

Cisa. (b.d.). *Nation-State Cyber Actors.* America's Cyber Defence Agency. Cisa.gov. Pobrano 18 września 2024 z https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Cisco. (2018). *What Is a Cyberattack?* Cisco.com. obrano 24 stycznia 2024 z https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Crowdstrike. (2024). *Global Threat Landscape*. Crowdstrike.com. Pobrano z https://www.crowdstrike.com/adversaries/

Departament of Justice. (2020, 19 października). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. Justice.gov. Pobrano 10 stycznia 2024 z https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Github. (b.d.). *Gcat.* Github.com. Pobrano 17 stycznia 2024 z https://github.com/byt3bl33d3r/gcat

Gibson, D. (2017). *CompTIA Security+: Get Certified Get Ahead.* YCDA LLC.

Greenberg, A. (2021). *Sandworm. Nowa era cyberwojny i polowanie na najbardziej niebezpiecznych hakerów Kremla*. Wydawnictwo Naukowe PWN.

Hultquist, J. (2022, 7 stycznia). *Sandworm Team and the Ukrainian Power Authority Attacks*. Mandiant.com. Pobrano 10 stycznia 2024 z https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team

Malpedia. (2024). *Sandworm.* Pobrano 10 stycznia 2024 z https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm

Marchant, G. (2023). *The Official CompTIA CySA+ Student Guide.* CompTIA.

McAfee. (2021). *Organized Cybercrime: The Big Business Behind Hacks and Attacks.* Mcafee.com. Pobrano 18 września 2024 z https://www.mcafee.com/blogs/internet-security/organized-cybercrime-the-big-business-behind-hacks-and-attacks/

National Institute of Standards and Technology. (b.d.). *Cyber Threat.* Csrc.nist.gov. Pobrano 14 stycznia 2024 z https://csrc.nist.gov/glossary/term/cyber_threat

National Security Agency. (2020, 28 maja). *Sandworm Actors Exploiting Vulnerability in Exim Mail Transfer Agent.* Media.defense.gov. Pobrano 16 lutego 2024 z https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf

Okta. (2024, 9 lutego). *Script Kiddies and Skiddies: Identifying Unskilled Hackers.* Okta.com. Pobrano 18 września 2024 z https://www.okta.com/identity-101/script-kiddie/

Poireault, K. (2023, 5 maja). *What's in a Name? Understanding Threat Actor Naming Conventions*, infosecurityeurope.com. Pobrano 18 września 2024 z https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/understanding-threat-actor-naming-conventions.html

Pompeo, M. (2020, 20 lutego). *The United States Condemns Russian Cyber Attack Against the Country of Georgia.* State.gov. Pobrano 10 stycznia 2024 z https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/

Radware. (2023). *Anonymous Russia.* Radware.com Pobrano 18 września 2024 z https://www.radware.com/cyberpedia/ddos-attacks/anonymous-russia/

Trendmicro. (2016, 6 stycznia). *First Malware-Driven Power Outage Reported in Ukraine.* Trendmicro.com. Pobrano 16 lutego 2024 z https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/first-malware-driven-power-outage-reported-in-ukraine

Ward, S. (2014, 14 października). *iSIGHT Discovers Zero-Day Vulnerability CVE-2014-4114 Used in Russian Cyber-Espionage Campaign.* Isightpartners.com. Pobrano 15 stycznia 2024 https://web.archive.org/web/20160211122039/http://www.isightpartners.com/2014/10/cve-2014-4114/

Watt, C. (2024, 18 kwietnia). *Threat Intelligence NoName057(16) Threat Actor Profile.* Quorum Cyber. Pobrano 18 września 2024 z https://www.quorumcyber.com/wp-content/uploads/2024/04/TI-NoName057-Threat-Actor-Profile-1.pdf

Wikipedia. (2023). *Cyberprzestrzeń.* Wikipedia.pl. Pobrano 14 stycznia 2024 z https://pl.wikipedia.org/wiki/Cyberprzestrze%C5%84

Cybersecurity Threat in Central and Eastern Europe Linked to the Activities of the Advanced Persistent Threat Sandworm Group

Abstract: This article focuses on the activities of Advanced Persistent Threat (APT) groups and their huge impact on the cybersecurity threat in Central and Eastern Europe. It defines current security threats and classifies the types of actors, including APT groups. The Advanced Persistent Threat group Sandworm and its operation in Central and Eastern Europe are analysed in detail, along with the course of action and its impact on the Central and Eastern European region.

Keywords: cybersecurity, APT, Central and Eastern Europe, malware, Sandworm