



fundacja instytut
CYBERBEZPIECZEŃSTWA

**Techniczne
niebezpieczeństwa
związane z grami
komputerowymi**

Wiktor Sędkowski

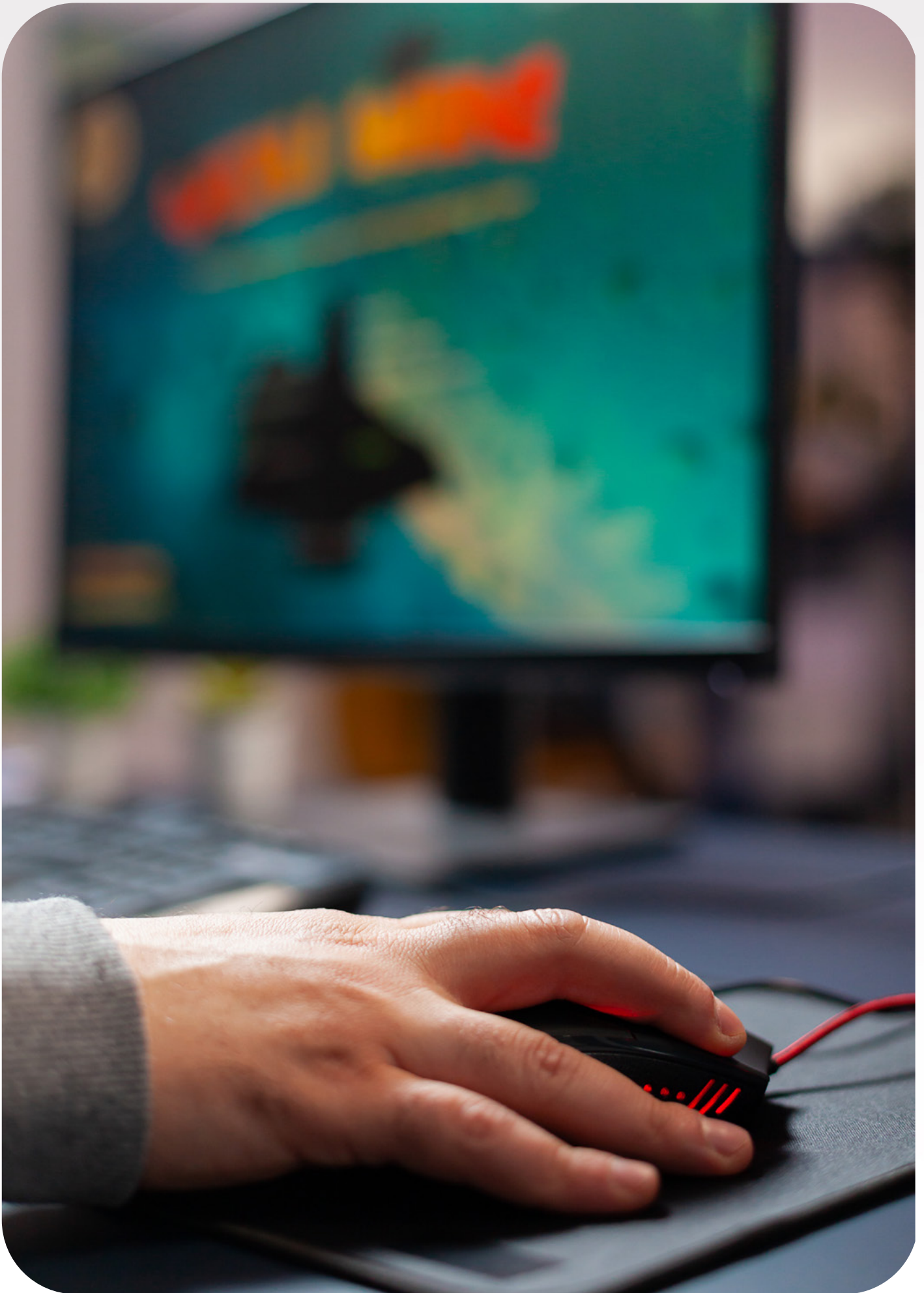


Fundusz
Sprawiedliwości



Ministerstwo
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



Branża gier komputerowych stanowi jeden z najszybciej rozwijających się sektorów rozrywki na świecie. Generuje przychody przekraczające 200 miliardów dolarów rocznie. Jednak wraz ze wzrostem popularności gier komputerowych i rosnącą liczbą graczy na całym świecie znacznie zwiększyła się skala zagrożeń cybernetycznych związanych z tym sektorem. Najnowsze badania wskazują na niepokojące trendy: liczba ataków na platformy gier wzrosła o 94% między pierwszym kwartałem 2023 r. a pierwszym kwartałem 2024 r.¹ Szczególnie alarmujące są dane dotyczące młodych użytkowników. Według raportu Kaspersky w pierwszej połowie 2024 r. o 30% więcej dzieci i młodzieży zostało zaatakowanych przez cyberprzestępców w porównaniu z drugą połową 2023 r.² W samym okresie od lipca 2023 do lipca 2024 r. odnotowano ponad 6,6 miliona prób ataków skierowanych przeciwko młodym graczom.

Mechanizmy ataków

Jednym z zagrożeń dla graczy jest pobieranie niebezpiecznych modyfikacji gier, trenerów i innych programów pomagających uzyskać przewagę w grze. Badania przeprowadzone przez Cisco Talos wykazały fundamentalną zmianę w podejściu cyberprzestępców do wykorzystywania modyfikacji gier jako wektora ataku. Jak zauważa Holger Unterbrink

z Cisco Talos: *Wystarczająco dużo pieniędzy krąży teraz w systemach gier, aby kradzież wirtualnych dóbr Steam stała się prawdziwym biznesem dla wykwalifikowanych hakerów. Praktycznie każde aktywne konto Steam jest teraz celem*³. To przede wszystkim z powodów finansowych atakowani są gracze.

- 1 S. Williams, Cyber threats surge in gaming industry through 2024, SecurityBrief, 22.08.2024, <https://securitybrief.co.uk/story/cyber-threats-surge-in-gaming-industry-through-2024>.
- 2 30 percent more young gamers targeted by cybercriminals in H1 2024 vs. H2 2023, Kaspersky Press Releases, 6.09.2024 r., <https://www.kaspersky.com/about/press-releases/30-percent-more-young-gamers-targeted-by-cybercriminals-in-h1-2024-vs-h2-2023>.
- 3 D. Johnson, Video game cheat mod malware demonstrates risks of unlicensed software, SCWorld, 2021.

Ataki przy użyciu zmodyfikowanych plików gier działają według sprawdzonego schematu. Cyberprzestępcy wykorzystują popularność konkretnych tytułów oraz chęć graczy do instalowania modów i cheatów z nieoficjalnych źródeł. Ponieważ są one rozpowszechniane głównie na stronach trzecich, napastnicy mają idealną możliwość maskowania malware przez podszywanie się pod te aplikacje. Przykładem tego typu malware jest rodzina trojanów z grupy Scavenger, która często ukrywana jest przez przestępców w pozornie niewinnych modyfikacjach i cheatach do popularnych gier, takich jak *Grand Theft Auto 5* czy *Oblivion Remastered*. Mechanizm działania tego malware jest dobrze przemyślany i wieloetapowy.

Łańcuch infekcji rozpoczyna się, gdy użytkownicy pobierają archiwa ZIP rzekomo poprawiające wydajność w grach. Archiwa te zawierają zmodyfikowane biblioteki dynamiczne (.dll), czasami przemianowane z rozszerzeniami takimi jak .ASI, aby przypominały legalne formaty wtyczek. Gdy użytkownik postępuje zgodnie z instrukcjami instalacji, złośliwa biblioteka zostaje umieszczona w tym samym folderze co docelowa gra. Jeśli gra nie sprawdza prawidłowo swoich bibliotek, trojan ładuje się automatycznie podczas uruchamiania. Po załadowaniu malware przy użyciu szyfrowanej komunikacji nawiązuje kontakt z serwerem dowodzenia i kontroli. Ten proces obejmuje weryfikację kluczy szyfrowania i sprawdzanie spójności znaczników czaso-

wych, co ma na celu unikanie analizy i blokiowanie wykrycia przez oprogramowanie antywirusowe.

W kolejnym etapie infekcji wdrażany jest dodatkowo złośliwy kod, który często osadza się w przeglądarkach opartych na Chromium, takich jak Chrome, Edge czy Opera. Złośliwe oprogramowania przez ingerencję w proces przeglądarki wyłączają weryfikację rozszerzeń i zastępują legalne rozszerzenia zmodyfikowanymi wersjami. Te zbierają frazy mnemoniczne, klucze prywatne i przechowywane hasła, które następnie są przekazywane na serwery atakujących. Łupem padają też portfele kryptowalut, takie jak MetaMask i Phantom, a także menedżery haseł, np. Bitwarden i LastPass.

W 2024 r. grą najczęściej wykorzystywaną przez cyberprzestępców był Minecraft⁴. Odnotowano ponad 3 miliony prób ataków związanych z tym tytułem, co stanowi znaczną część ze wspomnianego ogółu 6,6 miliona prób ataków na młodych graczy. Popularność Minecrafta wśród młodych użytkowników, połączona z możliwością instalowania modów z zewnętrznych źródeł, czyni go idealnym wektorem dla dystrybuowania malware.

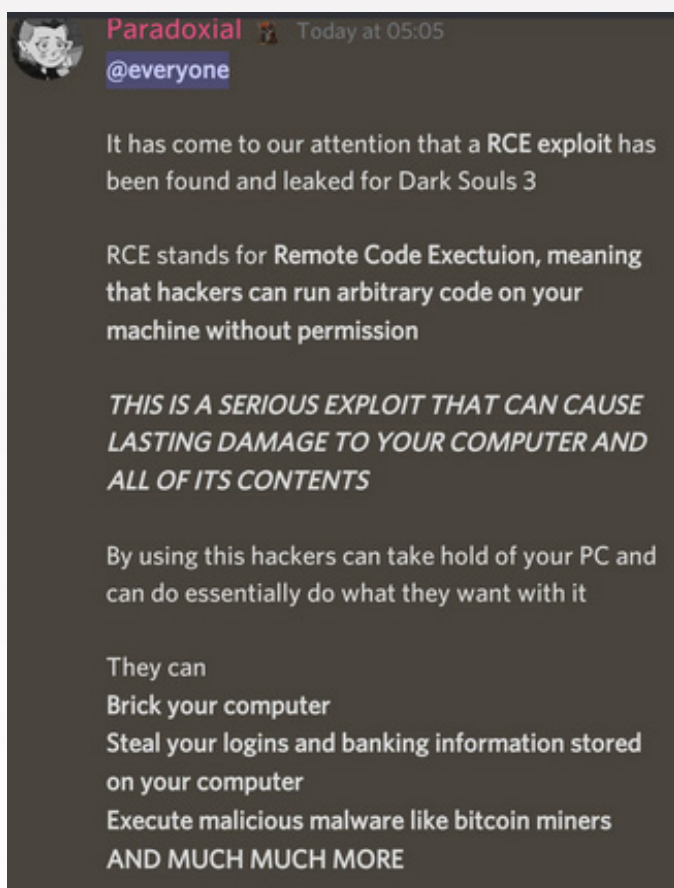
Mechanizm ataków w przypadku Minecrafta jest szczególnie podstępny, ponieważ młodzi gracze często poszukują modów poprawiających rozgrywkę lub dodających nowe funkcje. Cyberprzestępcy wykorzystują tę potrzebę i oferują pozornie atrakcyjne modyfikacje, które w rzeczywistości zawiera-

4 30 percent more young gamers targeted by cybercriminals...

ją złośliwy kod. Co więcej, w społeczności Minecrafta gracze bardzo często dzielą się

modyfikacjami między sobą, co dodatkowo ułatwia rozprzestrzenianie się malware.

Luki bezpieczeństwa w grach



Rysunek 1: Informacja o eksploicie w Dark Souls 3⁵

Seria gier *Dark Souls* stała się jednym z najbardziej spektakularnych przypadków luk bezpieczeństwa w historii gier komputerowych. Luka Remote Code Execution (RCE),

oznaczona jako CVE-2022-24126, umożliwiała atakującym przejście pełnej kontroli nad komputerem ofiary podczas rozgrywki online. Luka ta jest doskonałym przykładem tego, jak poważne mogą być zagrożenia bezpieczeństwa w grach multiplayer.

William Tremblay, student matematyki i informatyki na Uniwersytecie McGill⁶, odkrył tę lukę w styczniu 2022 r. W czasie gdy luka stała się znana w styczniu 2022 r., sześć lat po pierwotnym wydaniu, w *Dark Souls 3* codziennie grało średnio 15 000 graczy. W szczytowym momencie było ich około 75 000. Gdyby ta luka została odkryta wcześniej lub przez złośliwego napastnika, większość z tych graczy mogła zostać ofiarą w ciągu kilku minut.

Luka została zademonstrowana⁷ podczas transmisji na żywo na Twitchu przez gracza o pseudonimie „The_Grim_Sleeper”. W trakcie sesji online gra nagle się zawiesiła, po czym uruchomił się syntezytor mowy Microsoft, który zaczął odczytywać komentarze dotyczące rozgrywki. Ten publiczny pokaz był celowym działaniem gracza, któ-

5 https://www.reddit.com/r/Eldenring/comments/s9wai2/it_is_now_possible_for_dark_souls_3_invaders_to/.

6 <https://flashpoint.io/blog/rce-vulnerability-dark-souls/>

7 <https://clips.twitch.tv/GlamorousDarlingEggnogBudStar-t7dxGTY8KFWVHkL4>.



ry próbował zwrócić uwagę na problem, po tym jak jego wcześniejsze zgłoszenia do FromSoftware (producenta gry) zostały zignorowane.

Mechanizm ataku opierał się na dwóch fundamentalnych błędach w kodzie gry. Pierwszy dotyczył braku sprawdzania granic w parserze listy wpisów dla funkcji matchmakingu. Drugi występował w parserze NRSessionSearchResult, gdzie przepełnienie bufora mogło prowadzić do korupcji stosu. Jednoczesne wykorzystanie tych błędów pozwalało na zdalne wykonanie dowolnego kodu.

FromSoftware był zmuszony tymczasowo wyłączyć serwery dla wszystkich gier z serii *Dark Souls*. Problem dotknął nie tylko *Dark Souls 3*, lecz także *Dark Souls 2*, *Dark Souls: Remastered* i *Dark Souls: Prepare to Die Edition*. Co więcej, odkryto, że podobne luki występowały również podczas testów w grze *Elden Ring*, chociaż zostały one naprawione przed jej oficjalnym wydaniem.

Kolejnym tytułem z poważną luką bezpieczeństwa jest *Heroes of Might and Magic III*, kultowa gra strategiczna z 1999 r. Występuje w niej błąd w parsowaniu plików map (.h3m), który umożliwia wykonanie dowolnego kodu przygotowanego przez atakujących. Ta luka, choć dotyczy starszej gry, pokazuje, jak długotrwałe mogą być problemy bezpieczeństwa w oprogramowaniu rozrywkowym. Występują one bowiem nawet w najnowszej wersji gry dostępnej na platformie GOG.

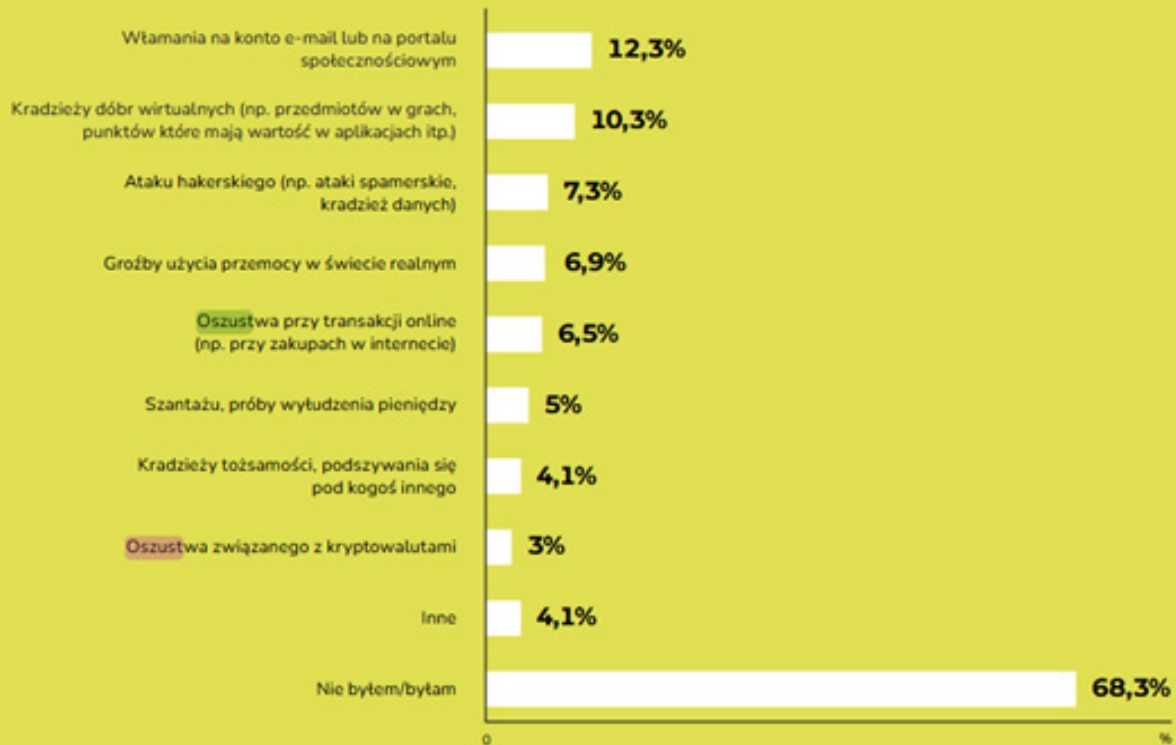
Luka CVE-2015-37716⁸ jest związana z przepełnieniem bufora podczas wczytywania nazw obiektów w plikach map. Badacze John Åkerblom i Pierre Lindblad wykazali, że można utworzyć mapę, która w edytorze gry nie wzbudza podejrzeń, ale potajemnie wykonuje złośliwy kod, gdy zostanie wczytana. Mechanizm ataku opiera się na manipulacji strukturą danych w pliku mapy w taki sposób, aby spowodować przepełnienie bufora i umożliwić wykonanie shellcode'u. Co szczególnie niepokojące, mapa zawierająca exploit może zostać rozpowszechniona przez społeczność graczy jako normalny dodatek do gry. Gracze mogą nieświadomie pobrać i instalować taką mapę, przekonani, że otrzymują nową zawartość związaną z danym tytułem.

Najnowszym z przykładów poważnej luki bezpieczeństwa jest sytuacja z lipca 2025 r., kiedy *Call of Duty: WWII* zostało tymczasowo wyłączone dla platformy PC po odkryciu luki Remote Code Execution. Gracze wykorzystywali ją do przeprowadzania spektakularnych, choć niebezpiecznych demonstracji. Ataki obejmowały otwieranie wiersza poleceń na komputerach ofiar, wysyłanie żartobliwych wiadomości przez Notepad, wymuszanie zdalnych wyłączeń komputerów oraz zmianę tapet pulpitu na nieodpowiednie treści. Chociaż te konkretne przypadki miały raczej charakter żartów niż poważnych ataków, to pokazały one potencjał luk do przeprowadzania przez atakujących znacznie bardziej destrukcyjnych działań.

8 <https://www.exploit-db.com/exploits/37716>.



Czy w internecie byłeś/byłaś poszkodowany/poszkodowana w wyniku... (Wielokrotny wybór)



Rysunek 2: Wyniki raportu Nastolatki 3.0.

Źródło: Thinkstat NASK, Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców, 2023, s. 95.

Activision była zmuszona podjąć natychmiastowe działania i tymczasowo wycofała grę z platformy Steam i innych platform dystrybucji cyfrowej. To posunięcie pokazuje, jak

poważnie producenci gier traktują obecnie luki bezpieczeństwa, szczególnie w świetle rosnącej wśród graczy świadomości na temat zagrożeń cybernetycznych.

Kradzież kont i dóbr cyfrowych

Największą platformą dystrybucji cyfrowej gier na PC jest platforma Steam. Stała się ona głównym celem cyberprzestępców specjalizujących się w kradzieży kont graczy. Według danych firmy Valve, właściciela platformy Steam, 77 000 kont zostaje przejętych każdego miesiąca⁹. Firma zauważyła to już lata temu i przyznała, że (...) *praktycznie każde aktywne konto Steam ma teraz wystarczającą wartość, by było warte czasu hakera. Zasadniczo wszystkie konta Steam są teraz celami. Aby zabezpieczyć konta graczy, wdrożono liczne środki zapobiegawcze, takie jak wymóg 2FA dla kont na platformie.*

Współczesne gry oferują rozbudowane systemy wirtualnych przedmiotów, które mają realną wartość finansową. Skiny do broni w grach takich jak *Counter-Strike* mogą być warte setki, a nawet tysiące dolarów. Karty kolekcjonerskie, emotikony, tła profilu i inne cyfrowe przedmioty tworzą złożony ekosystem ekonomiczny, w którym gracze inwestują znaczne sumy pieniędzy, co przyciąga cyberprzestępców. Wykorzystują oni różne metody do przejmowania kont. Najczęściej stosowane techniki to malware, keyloggery kradnące hasła z komputerów ofiar, phishing na fałszywych stronach imitujących oficjalne platformy, wykorzysty-

wanie luk w grach oraz ataki na słabe hasła poprzez credential stuffing.

Z osobnym problemem wiążą się dobra cyfrowe. Badanie przeprowadzone wśród duńskich dzieci i nastolatków przez Uniwersytet w Kopenhadze ujawnia niepokojącą skalę oszustw związanych z handlem wirtualnymi przedmiotami¹⁰. Wyniki wskazują, że 35,8% uczestników handlujących wirtualnymi przedmiotami lub kontami gier doświadczyło oszustwa w ciągu ostatnich 12 miesięcy. Te dane są szczególnie alarmujące, jeśli weźmie się pod uwagę, że dotyczą one młodych ludzi, którzy często nie mają doświadczenia w rozpoznawaniu zagrożeń cybernetycznych. Badanie ujawniło również interesujące wzorce demograficzne i behawioralne związane z ryzykiem oszustwa. U dziewczynek występuje 1,8 razy większe ryzyko padnięcia ofiarą oszustwa niż u chłopców, co może być związane z różnicami w podejściu do zarządzania ryzykiem online. Statystyki te pokazują, jak ważne jest zrozumienie ekosystemu handlu wirtualnymi przedmiotami i związanych z nim zagrożeń. Młodzi ludzie, przyciągnięci możliwością zarobku lub uzyskania rzadkich przedmiotów, często nie zdają sobie sprawy z zagrożeń związanych z interakcjami z nieznanymi w środowisku online.

9 G. Cluley, 77,000 Steam accounts are hacked and raided every month, Bitdefender, 11.12.2015, <https://www.bitdefender.com/en-us/blog/hotforsecurity/77000-steam-accounts-are-hacked-and-raided-every-month> (dostęp:).

10 S. Kristiansen, A.V. Jensen, Victimization in online gaming-related trade scams: A study among young Danes, "Nordic Journal of Criminology" 2023, vol. 24, iss. 2. <https://doi.org/10.18261/njc.24.2.6>.

Krajobraz zagrożeń w Polsce

roblem cyberbezpieczeństwa w sektorze gier nabiera szczególnego znaczenia również w Polsce. Według raportu Ministerstwa Cyfryzacji za 2024 r. liczba zgłoszeń dotyczących potencjalnych naruszeń systemów teleinformatycznych wzrosła aż o 60% w porównaniu z poprzednim rokiem. CSIRT NASK odnotował 103 449 incydentów, co oznacza wzrost o 29% w stosunku do 2023 r. – obsługiwał on średnio 283 incydenty dziennie. Raport NASK *Nastolatki 3.0* realizowany przez zespół Thinkstat ujawnia niepokojące trendy dotyczące młodych polskich graczy. Zgodnie z wynikami badania polski nastolatek spędza w sieci średnio ponad 5,5 godziny dziennie, a co czwarty z nich wskazuje gry online jako swoją najczęstszą aktywność w internecie. Co więcej, prawie połowa młodych ludzi (48,8%) przynajmniej raz doświadczyła przemocy w grach online, obejmującej wyzwiska, zastraszanie i hejt. Według danych raportu prawie 1/3 polskich nastolatków była poszkodowana w wyniku swojej aktywności w internecie, a 10% ucierpiało w wyniku kradzieży dóbr wirtualnych.

Niepokojące są też dane dotyczące uzależnienia od gier, problem ten dotyka już 8,3% polskich nastolatków. NASK ostrzega ponadto przed ukrytymi w grach mechanizmami hazardowymi, takimi jak loot boxy i inne systemy, które sprytnie wymuszają mikropłatności. Szacuje się, że do 2031 r.

cały rynek loot boxów może osiągnąć wartość nawet 30 miliardów dolarów.

Zagrożenia cybernetyczne w grach komputerowych nie znikną. Napędza je globalny rynek o ogromnym zasięgu, skupiający miliony użytkowników na całym świecie. Skala ataków stale rośnie, a metody stają się coraz bardziej wyrafinowane, atakujący wykorzystują zarówno techniczne luki w oprogramowaniu, jak i słabości użytkowników. Szczególnie niepokojące jest atakowanie młodych graczy, którzy często nie mają odpowiedniej wiedzy o zagrożeniach cybernetycznych oraz są bardziej skłonni do podejmowania ryzykownych działań online.

Ewolucja branży gier w kierunku większej integracji z technologiami blockchain, sztucznej inteligencji i rozszerzonej rzeczywistości prawdopodobnie przyniesie nowe rodzaje zagrożeń, które będą wymagały ciągłej adaptacji środków bezpieczeństwa. Najważniejszym elementem obrony jest edukacja użytkowników, wdrażanie odpowiednich środków bezpieczeństwa oraz podnoszenie odpowiedzialności branży gier za bezpieczeństwo swoich platform i korzystających z nich osób. W miarę jak gaming staje się coraz bardziej zintegrowany z codziennym życiem cyfrowym, bezpieczeństwo w tej sferze będzie miało coraz większy wpływ na ogólne bezpieczeństwo społeczeństwa.

Bibliografia:

- 30 percent more young gamers targeted by cybercriminals in H1 2024 vs. H2 2023, Kaspersky Press Releases, 6.09.2024, <https://www.kaspersky.com/about/press-releases/30-percent-more-young-gamers-targeted-by-cybercriminals-in-h1-2024-vs-h2-2023>.
- Amtz P., Gamers hacked playing Call of Duty: WWII—PC version temporarily taken offline, MalwareBytes, 7.07.2025, <https://www.malwarebytes.com/blog/news/2025/07/gamers-hacked-playing-call-of-duty-wwii-pc-version-temporarily-taken-offline>.
- Cluley G., 77,000 Steam accounts are hacked and raided every month, Bitdefender, 11.12.2015, <https://www.bitdefender.com/en-us/blog/hotforsecurity/77000-steam-accounts-are-hacked-and-raided-every-month>.
- <https://flashpoint.io/blog/rce-vulnerability-dark-souls/>.
- <https://clips.twitch.tv/Glamorous-DarlingEggnogBudStar-t7dxGTY8K-FWVHkL4>.
- <https://www.exploit-db.com/exploits/37716>.
- Johnson D., Video game cheat mod malware demonstrates risks of unlicensed software, SCWorld, 2021.
- Kristiansen S., Jensen A.V., Victimization in online gaming-related trade scams: A study among young Danes, “Nordic Journal of Criminology” 2023, vol. 24, iss. 2. <https://doi.org/10.18261/njc.24.2.6>.
- Thinkstat NASK, Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców, 2023.
- Udinmwen E., Gamers at risk as scammers are using malware-infected cheats and mods to steal passwords and crypto, techradar, 1.08.2025, <https://www.techradar.com/pro/gamers-at-risk-as-scammers-are-using-malware-infected-cheats-and-mods-to-steal-passwords-and-crypto-heres-how-to-stay-safe>.
- Williams S., Cyber threats surge in gaming industry through 2024, SecurityBrief, 22.08.2024, <https://securitybrief.co.uk/story/cyber-threats-surge-in-gaming-industry-through-2024>.



Fundusz
Sprawiedliwości



Ministerstwo
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl



fundacja instytut
CYBERBEZPIECZEŃSTWA