**Od Ukrainy po całą Europę:**

**cyberkonflikt osiąga punkt zwrotny**

* **W raporcie Thales Cyber Threat Intelligence Report opublikowanym w lutym 2023 roku eksperci prezentują wyniki pogłębionych analiz cyberataków w minionym roku w Europie**
* **Trzeci kwartał 2022 roku był punktem zwrotnym w dziedzinie cyberbezpieczeństwa w związku z konfliktem na Ukrainie. Raport pokazuje, że cyberkonflikt wszedł w kolejną fazę – od cyberwojny skoncentrowanej na obszarze Ukrainy i Rosji do konfliktu hybrydowego o wysokiej intensywności, w którym ataki skierowane są przede wszystkim przeciwko Polsce oraz krajom bałtyckim i nordyckim. Ataki coraz częściej dotyczą kluczowych sektorów państwowych takich jak lotnictwo, energetyka, infrastruktura zdrowotna, bankowość i instytucje publiczne.**
* **W pierwszej fazie wojny dominowały celowane kampanie. Obecnie prorosyjscy haktywiści stosują głównie działania partyzanckie, wykorzystując ataki DDoS[[1]](#footnote-1), aby czasowo uniemożliwić dostęp do serwerów i zakłócić działanie usług. Ataki te są częścią rosyjskiej strategii angażowania się w wojnę informacyjną jako sposobu na osłabienie podmiotów prywatnych i publicznych w państwach ościennych.**

**Europa Wschodnia i Północna na pierwszej linii cyberkonfliktu**

W ciągu ostatnich 12 miesięcy zmienił się zasięg terytorialny ataków prowadzonych przez prorosyjskie grupy hakerskie. Na samym początku konfliktu większość incydentów dotyczyła przede wszystkim Ukrainy (50,4% w porównaniu z 28,6% w trzecim kwartale 2022 r.), jednak w ciągu ostatnich sześciu miesięcy w krajach Unii Europejskiej odnotowano gwałtowny wzrost incydentów związanych z konfliktem (9,8% w porównaniu z 46,5% globalnych ataków).

Tego lata w krajach UE było prawie tyle samo incydentów związanych z konfliktem, co w Ukrainie (85 wobec 86), a w pierwszym kwartale 2023 roku przytłaczająca większość incydentów (80,9%) miała miejsce już na terenie Unii Europejskiej.

Coraz częściej celem ataków są również państwa kandydujące do członkostwa we Wspólnocie Europejskiej, takie jak Czarnogóra i Mołdawia: 0,7% ataków w pierwszym kwartale 2022 r. wobec 2,7% na koniec 2022 r. Polska z kolei doświadcza bezustannych i zmasowanych aktów cyberprzestępczości – w ciągu ostatniego roku na tym obszarze odnotowano rekordową liczbę 114 incydentów związanych z konfliktem. Wojenni haktywiści obrali sobie za cel szczególnie kraje bałtyckie (157 incydentów w Estonii, na Łotwie i Litwie) oraz kraje nordyckie (95 incydentów w Szwecji, Norwegii, Danii i Finlandii). W Niemczech w 2022 roku odnotowano 58 incydentów. Zgodnie z analizami ekspertów w innych krajach takich jak Francja (14 ataków), Wielka Brytania (18 ataków), Włochy (14 ataków) i Hiszpania (4 ataki) intensywność cyberprzemocy jest mniej intensywna.

- "W trzecim kwartale 2022 roku Europa została wciągnięta w hybrydową cyberwojnę o wysokiej intensywności. Dla naszego kontynentu to absolutny punkt zwrotny, obserwujemy zwłaszcza ogromną falę ataków DDoS, szczególnie w krajach nordyckich i bałtyckich oraz w Europie Wschodniej. Działania w cyberprzestrzeni są obecnie kluczową bronią w arsenale nowych sposobów prowadzenia wojny, obok dezinformacji, manipulacji opinią publiczną, wojny ekonomicznej, sabotażu i taktyki partyzanckiej. W miarę jak konsekwencje konfliktu w Ukrainie rozlewają się na resztę Europy, państwa Europy Zachodniej powinny zwrócić szczególną uwagę na ten aspekt bezpieczeństwa narodowego. Prawdopodobieństwa ataków na infrastrukturę krytyczną znacząco wzrasta, a wojna w cyberprzestrzeni będzie nabierała przyspieszenia – Pierre-Yves Jolivet, VP Cyber Solutions, Thales.

**Od haktywistów wojennych do cyberharcerzy**

Ze wszystkich cyberataków zgłoszonych na całym świecie od początku konfliktu, 61% zostało dokonanych przez prorosyjskie grupy haktywistów, a w szczególności przez Anonymous Russia, KillNet i Russian Hackers Teams, które od początku konfliktu prowadziły akcje przeciwko haktywistami z Ukrainy. Te nowe grupy działają w sposób znacznie bardziej ustrukturalizowany i korzystają z zasobów użytkowanych przez grupy cyberprzestępcze, w tym zasoby typu botnet-as-a-service[[2]](#footnote-2), takie jak Passion Botnet. Ich celem jest wywarcie nacisku na państwa zachodnie, które wspierają Ukrainę. Te grupy niezależnych, cywilnych hacktivistów pojawiły się jako nowa strona konfliktu. Można je przyrównać do organizacji cyberprzestępczej o określonych celach i interesach politycznych, działającej z przekonania, ale nie wspieranej bezpośrednio przez żaden rząd. Członkowie takich grup pochodzą z różnych środowisk, mają zaawansowane umiejętności techniczne i doświadczenia.

W trzecim kwartale 2022 r. nastąpiło przejście do fali ataków DDoS, w przeciwieństwie do pierwszego kwartału 2022 r., w którym odnotowano szereg różnych rodzajów ataków, podzielonych mniej więcej po równo między wycieki danych i kradzież, ataki DDoS, szpiegostwo, kampanie wpływu, włamania, ataki typu ransomware, phishing, wiper i infostealer[[3]](#footnote-3). Cyberatakujący od tego czasu preferują ataki DDoS (75%) przeciwko firmom i rządom. To systematyczne nękanie często ma niewielki wpływ operacyjny, ale podtrzymuje atmosferę niepokoju wśród zespołów bezpieczeństwa i decydentów. Ich celem nie jest wywarcie dużego wpływu operacyjnego, ale nękanie celów i zniechęcenie ich do wspierania Ukrainy.

Na drugim krańcu tego spektrum jeśli chodzi o szkodliwość, znajdują się ataki typu wiper, które mogą zniszczyć systemy przeciwnika, a długotrwałe cyberszpiegostwo może wręcz podważyć integralność systemów bezpieczeństwa zaatakowanego. Należy jednak pamiętać, że przygotowanie takich rozwiązań informatycznych trwa znacznie dłużej i wymaga większych zasobów. Dlatego destrukcyjne operacje cyberwojskowe z komponentem szpiegostwa stanowią jedynie 2% całkowitej liczby incydentów i są skierowane głównie przeciwko ukraińskim organizacjom sektora publicznego.

Władze rosyjskie regularnie wykorzystują cybernetykę do wywierania presji na swoich przeciwników bez angażowania się w bezpośrednią konfrontację.

Akty wojny cybernetycznej wciąż mają miejsce na Ukrainie. Przykładem zmasowanych działań tego typu był dokonany w rocznicę wybuchu wojny (23 lutego 2023 roku) atak ATK256 (UAC-0056), który swoim zasięgiem objął kilka istotnych ukraińskich instytucji publicznych. Choć na samej Ukrainie cyberwojna wciąż się nasila, coraz częściej uwaga państwa zachodnich koncentruje się na działaniach partyzanckich prowadzonych na coraz szerszą skalę w całej Europie.

**Coraz większa liczba sektorów cywilnych w Europie pod presją**

W pierwszym kwartale 2022 r. większość cyberataków była wymierzona w ukraińską obronną bazę przemysłową oraz administrację publiczną tego kraju. Obecnie cyberataki coraz częściej dotyczą także innych krajów europejskich i dotykają m.in. administrację publiczną (30 incydentów), sektor finansowy (162), sektor transportowy (132), telekomunikację (90), media (89) i sektor energetyczny (66). Chociaż wcześniej konflikt był stosunkowo mało dotkliwy, europejski sektor opieki zdrowotnej, rządy, przemysł, usługi informatyczne i sektor lotniczy są coraz częściej celem ataków, których celem jest wywarcie presji na zachodnie społeczeństwa.

**Wkład firmy Thales w ochronę infrastruktury krytycznej**

Thales dostarcza rozwiązania z zakresu cyberbezpieczeństwa dla dziewięciu z dziesięciu największych komercyjnych graczy internetowych oraz pomaga chronić systemy informatyczne ponad 130 agencji rządowych i dostawców usług kluczowych. Zatrudniając ponad 3 500 ekspertów ds. cyberbezpieczeństwa, firma zapewnia rządom i operatorom infrastruktury krytycznej zintegrowane rozwiązania w zakresie wykrywania i reagowania na incydenty, w tym informacje o zagrożeniach cybernetycznych, suwerenne sondy, dedykowane centra bezpieczeństwa i systemy szyfrowania, aby zapobiec naruszeniom danych. Portolio Thales zawiera trzy najważniejsze kategorie produktowe: programu suwerenne, platformy ochrony danych oraz usług z zakresu cyberbezpieczeństwa i usług cyberbezpieczeństwa. Łączna sprzedaż w oparciu o tę ofertę rozwiązań cybernetycznych wygenerowała dla Grupy ponad 1,5 mld euro w 2022 roku.

|  |
| --- |
| **O Thales** Thales (Euronext Paris: HO) jest globalnym liderem technologicznym obsługującym rynki lotnicze, obronne oraz Digital Identity & Security. Nasze rozwiązania pomagają uczynić świat bezpieczniejszym, bardziej ekologicznym i sprzyjającym integracji.Inwestujemy blisko 4 mld euro rocznie w badania i rozwój, napędzając innowacje w kluczowych obszarach, takich jak technologie kwantowe, architektury chmurowe, 6G i cyberbezpieczeństwo.Grupa zatrudnia 77 000 pracowników w 68 krajach W 2022 roku osiągnęła przychody w wysokości 17,6 mld euro w 2022 r.1**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**1 bez dywizji transportowej  |

**kontakt dla mediów:**

**Thales Media Relations**

**Marion Bonnet**

+33 (0)6 60 38 48 92

marion.bonnet@thalesgroup.com

 Więcej informacji:

[Cybersecurity solutions | Thales Group](https://www.thalesgroup.com/en/markets/transverse-markets/cybersecurity-solutions)

[Cyberthreat Hitmap (thalesgroup.com)](https://cyberthreat.thalesgroup.com/)

1. Rozproszony atak typu denial-of-service (DDoS) ma na celu uczynienie jednej lub więcej usług niedostępnymi poprzez wykorzystanie luki w oprogramowaniu lub sprzęcie albo nasycenie przepustowości sieci w celu uniemożliwienia dostępu użytkownikom. [↑](#footnote-ref-1)
2. Sprzedaż lub wynajem sieci proxy innym wrogim podmiotom w celu wykorzystania jej do przeprowadzania cyberataków. [↑](#footnote-ref-2)
3. Phishing to próba sprawienia, aby użytkownik ujawnił informacje. Wiper to rodzaj złośliwego oprogramowania używanego do usuwania danych z zainfekowanego systemu. Infostealer to rodzaj oprogramowania szpiegującego używanego do zbierania informacji z systemu. [↑](#footnote-ref-3)