**Pół roku później: rola cyberataków w inwazji Rosji
na Ukrainę**

**Kraków, 22 września – Według ukraińskiej Państwowej Służby Łączności Specjalnej i Ochrony Informacji (SSSCIP), od początku inwazji Ukraina doświadczyła aż 1123 cyberataków. 37% celów hakerów było związanych z instytucjami rządowymi i obroną. Co czwarty atak bazował na złośliwym kodzie, a 27% miało na celu kradzież poufnych informacji. Chester Wisniewski, ekspert Sophos podsumowuje intensywność, skuteczność oraz cel cyberataków we wciąż toczącym się konflikcie.**

**Chester Wisniewski, Principal Research Scientist w firmie Sophos:**

Działania Rosjan na cyfrowym froncie można podzielić na kilka kategorii: destabilizujące, dezinformacyjne, cyberterrorystyczne i szpiegowskie. Z danych udostępnionych przez SSSCIP wynika, że rosyjscy hakerzy jeszcze w styczniu zaczęli rozsyłać szkodliwe oprogramowanie, które miało utrudniać lub wręcz uniemożliwiać pracę ukraińskich firm, agencji rządowych i infrastruktury krytycznej.

23 lutego 2022 r. około godziny 16:00, na dzień przed rozpoczęciem inwazji lądowej, eksperci ds. bezpieczeństwa zanotowali wzmożoną liczbę ataków typu DDoS (zmasowane ataki polegające na generowaniu sztucznego ruchu internetowego i ciągłym wysyłaniu zapytań do serwera, w celu sparaliżowania jego pracy) oraz wiper (wymazanie danych z systemów). Tego typu ataki występowały przez pierwsze sześć tygodni konfliktu, potem ich natężenie osłabło. Zdecydowaną większość z nich przeprowadzono w pierwszych dniach wojny.

**Działania destrukcyjne**

Prawdopodobnie najbardziej dotkliwym był atak Rosjan tuż po rozpoczęciu inwazji na system łączności satelitarnej Viasat, używany w całej Europie Środkowej i Wschodniej. Według informacji agencji Reuters zakłócenia komunikacyjne miały przyczynić się do zdobycia przewagi militarnej. Ukraińscy dowódcy byli jednak w stanie przegrupować się i ustanowić alternatywną komunikację, aby zminimalizować wpływ ataku. Należy jednak zaznaczyć, że wyrządził on szkody także w państwach NATO. Spowodował m.in. zakłócenie działania ponad 5800 turbin wiatrowych w Niemczech.

Po sześciu miesiącach są dowody wskazujące, że to Rosja miała większe problemy z komunikacją w łańcuchu dowodzenia niż Ukraina. Ataki mające na celu destabilizację nie miały większego wpływu na wynik żadnej z dotychczasowych bitew.

**Działania dezinformacyjne**

Rosja kreuje narracje o amerykańskich laboratoriach z bronią biologiczną, denazyfikacji Ukrainy czy rzekomym ludobójstwie dokonywanym przez ukraińską armię. Ma to poddać w wątpliwość informacje o inwazji przedstawiane przez zachodnie media. Źródłem dezinformacji są głównie konta w serwisach społecznościowych, które już wcześniej podawały treści o takim charakterze.

Rosyjskie kampanie w mediach społecznościowych czy wykorzystujące SMS-y nie przyniosły oczekiwanych efektów w postawach ukraińskiego społeczeństwa. Dezinformacja mogła za to odnieść większy sukces tam, skąd pochodzi – sondaże sugerują, że rosyjskie społeczeństwo popiera „specjalną operację wojskową” na terenie Ukrainy. Trzeba pamiętać, że jest to jedyna opinia, którą można tam publicznie wyrazić, a dostęp do niezależnych mediów jest utrudniony. Tak czy inaczej, rosyjska dezinformacja, podobnie jak ataki destrukcyjne, nie wpływa bezpośrednio na wynik wojny.

**Działania cyberterrorystyczne**

Niektóre znane grupy cyberprzestępcze, takie jak Conti i Lockbit, od razu zadeklarowały, po której stronie konfliktu się opowiadają. Na początku inwazji obserwowaliśmy wzmożoną aktywność tzw. haktywistów: ataki DDoS, usuwanie stron internetowych, włamania do niezabezpieczonych systemów. Zarówno w Ukrainie, jak i w Rosji nie wywarły one trwałego wpływu.

Wciąż jednak można natknąć się na przykłady takiej „partyzanckiej” działalności. Niedawno w Moskwie nieznani sprawcy zhakowali aplikację Yandex Taxi i zamówili przez nią kilkadziesiąt taksówek pod jeden adres, tworząc w centrum miasta olbrzymi korek.

**Działania wywiadowcze**

W przeciwieństwie do działań destrukcyjnych, te o charakterze szpiegowskim są wymierzone nie tylko w Ukrainę, ale iw wspierające ją państwa i podmioty. Taka aktywność jest trudniejsza do sklasyfikowania, a często także do namierzenia.

Nie jest niczym nowym, że Rosja atakuje Stany Zjednoczone, Unię Europejską i państwa członkowskie NATO, korzystając ze złośliwego oprogramowania i phishingu. W niektórych przypadkach istnieją jednak przekonujące dowody na to, że te ataki mają bezpośredni związek z inwazją na Ukrainę.

W marcu 2022 roku Grupa Analiz Zagrożeń firmy Google (TAG) opublikowała raport dokumentujący rosyjskie i białoruskie ataki phishingowe na amerykańskie organizacje pozarządowe, siły wojskowe jednego z państw bałkańskich oraz ukraińską firmę przemysłu zbrojeniowego. Z kolei z badań firmy Proofpoint wynika, że europejscy urzędnicy zajmujący się uchodźcami z Ukrainy stali się celem kampanii phishingowych, które prowadzone są z adresu e-mail członka ukraińskich sił zbrojnych. Jego konto zostało bowiem wcześniej zhakowane przez rosyjskie służby wywiadowcze. W lipcu Rosjanie wzięli na celownik media. Próbowali pozyskać dostęp do ich systemów poprzez nowo odkrytą lukę „Follina” w pakiecie Microsoft Office.

Po ponad pół roku trwania inwazji na Ukrainę można powiedzieć, że Rosja okazała się słabo przygotowana nie tylko pod kątem militarnym, ale także cyfrowym. Podjęte próby cyberataków mogły mieć o wiele bardziej niszczycielski wpływ. Trzeba jednak pamiętać, że to kraj rządzony przez Władimira Putina kontroluje sporą część dostaw energii do Europy Zachodniej.

Czy w obliczu nadchodzącej zimy szykują się nowe kampanie dezinformacyjne, wywierające presję na europejskich przywódców, aby złagodzili sankcje? Czy sytuację wykorzystają też grupy cyberprzestępcze, których celem mogą stać się koncerny energetyczne? Rola cyberataków w przyszłych tygodniach i miesiącach może ulec zmianie, którą trudno jest przewidzieć. Jednak lekcją, którą z inwazji na Ukrainę można wyciągnąć już teraz, jest to, że silna obrona może być bardzo skutecznym atakiem.

**Informacje o firmie**

Jako światowy lider zabezpieczeń nowej generacji, Sophos chroni przed najbardziej zaawansowanymi cyberzagrożeniami ponad 400 tys. firm różnej wielkości w ponad 150 krajach. Rozwiązania Sophos wykorzystują chmurę i sztuczną inteligencję, aby zabezpieczać urządzenia końcowe (laptopy, serwery i urządzenia mobilne) oraz sieci przed ewoluującymi metodami cyberprzestępców. Przy wsparciu SophosLabs – globalnego zespołu badającego zagrożenia – firma odpowiada na zagrożenia takie jak ransomware, malware, exploity, eksfiltracja danych, phishing czy indywidualnie dokonywane włamania przez cyberprzestępców. Platforma do zarządzania w chmurze Sophos Central integruje całe portfolio produktów nowej generacji Sophos w jeden system „zsynchronizowanej ochrony”, dostępny przez zestaw interfejsów API i obejmujący m.in. rozwiązanie Intercept X dla urządzeń końcowych oraz zaporę sieciową nowej generacji z rodziny XG Firewall. Firma oferuje również usługi łączące posiadaną technologię oraz aktywne przeciwdziałanie zagrożeniom (Managed Threat Response), szczególnie istotne w zmieniającym się dynamicznie świecie.

Sophos dąży do rozwijania i oferowania rozwiązań nowej generacji, aby zapewnić każdemu przedsiębiorstwu najwyższej klasy ochronę, zachowując jednocześnie prostotę zarządzania i umożliwiając redukcję kosztów. Wykorzystuje do tego m.in. zaawansowane funkcje infrastruktury chmurowej, uczenie maszynowe, interfejsy API, automatyzację i zarządzanie sposobami reagowania na zagrożenia. Firma sprzedaje swoje produkty i usługi za pośrednictwem globalnej sieci ponad 47 tys. partnerów i dostawców usług zarządzanych (MSP). Z innowacyjnych technologii Sophos mogą skorzystać także konsumenci indywidualni dzięki rodzinie rozwiązań Sophos Home. Firma ma siedzibę w Oksfordzie w Wielkiej Brytanii.

Więcej informacji można znaleźć na stronie www.sophos.com