Raport CERT Orange Polska za rok 2024: oszustwa na fałszywe inwestycje, nowe metody ataków wymuszających dane i okup. CyberTarcza w sieci Orange działa już 10 lat.

Informacja prasowa, 16 kwietnia 2025

CyberTarcza w sieci Orange w ubiegłym roku najczęściej blokowała strony internetowe z fałszywymi inwestycjami - skala tego typu oszustw z roku na rok wzrosła dwukrotnie. Łącznie w 2024 roku zablokowano 305 tysięcy fałszywych stron internetowych, chroniąc 4,85 mln klientów, którzy kliknęli w fałszywe linki. Eksperci CERT Orange Polska zauważają także nowe metody działania cyberprzestępców: większą specjalizację grup zajmujących się wykradaniem i zarabianiem na danych, precyzyjne dobieranie ofiar, a także wykorzystywanie luk w zabezpieczeniach urządzeń.

Raport CERT Orange Polska za rok 2024 to podsumowanie kluczowych danych i statystyk dotyczących zagrożeń wykrytych i zablokowanych w sieci Orange, a także analizy najnowszych trendów w dziedzinie cyberbezpieczeństwa.

- Dane z najnowszego raportu CERT pozwalają na umiarkowany optymizm – liczba osób, które kliknęły w fałszywy link, zablokowany wcześniej przez CyberTarczę, jest niższa niż rok wcześniej. To znaczy, że edukacja działa, rośnie świadomość zagrożeń. Niemniej, to wciąż miliony osób, które bez naszej ochrony mogły stracić swoje oszczędności. Dlatego wprowadzamy nowe rozwiązania by zwiększać bezpieczeństwo naszych klientów. To chociażby serwis Hasło Alert, gdzie mogą sprawdzić, czy ich dane logowania wyciekły, lub Centrum Bezpieczeństwa w aplikacji Mój Orange. A dla firm otworzyliśmy nowoczesne Centrum Doświadczeń Cyberbezpieczeństwa, gdzie w bezpiecznych warunkach zobaczą jakie skutki może mieć cyberatak na ich organizację. Działania te wzmacniają

bezpieczeństwo społeczeństwa w sieci, a także umożliwiają zawczasu budować cyberodporność– mówi Piotr Jaworski, członek zarządu ds. Sieci i Technologii Orange Polska

Od wielu lat, główne rodzaje zagrożeń, na jakie narażeni są internauci, pozostają praktycznie bez zmian. W ubiegłym roku, wg danych CERT Orange Polska, po raz kolejny numerem jeden był phishing (45%), na kolejnych miejscach utrzymują się ataki DDoS (15%) oraz złośliwe oprogramowanie (blisko14%). Co roku rozwijają się jednak metody działania przestępców.

Phishing: dwukrotny wzrost oszustw na fałszywe inwestycje.

W 2024 wśród metod phishingowych dominowały **fałszywe inwestycje** – stanowiły aż 60% wszystkich oszustw, dwukrotnie więcej niż rok wcześniej. Linki do fałszywych stron rozpowszechniane były głównie za pomocą reklam w mediach społecznościowych. Drugie najpowszechniejsze oszustwo (około 30%) to fałszywe płatności, w tym popularne oszustwo na kupującego. W całym ubiegłym roku CyberTarcza zablokowała 305 tysięcy domen phishingowych, podczas gdy rok wcześniej było ich 360 tys. Nie oznacza to jednak mniejszą aktywność przestępców. To efekt lawinowego już wykorzystania blokad typu „wildcard” w 2024 roku. To blokady wszystkich subdomen w obrębie jednej domeny podstawowej.

- *Mija dziesięć lat od kiedy w sieci Orange działa CyberTarcza – nasze autorskie rozwiązanie. Przez ten czas rozwijaliśmy ją tak, by radziła sobie z coraz to nowszymi zagrożeniami. Dziś stoją za nią zaawansowane algorytmy, infrastruktura i zespół analityków CERT Orange Polska. Ale skuteczność CyberTarczy wspierają też internauci reagujący na zagrożenia. Tylko w minionym roku na numer 508 700 900, otrzymaliśmy blisko 4 tysiące SMS-ów z informacjami o podejrzanych wiadomościach, fałszywych reklamach czy stronach internetowych. Informacje, którymi się dzielą z nami internauci, pozwalają nam identyfikować coraz to nowe zagrożenia i aktywnie im przeciwdziałać* – mówi Robert Grabowski, szef CERT Orange Polska.

W przypadku smishing-u, czyli phishingu realizowanego poprzez SMS-y, większość złośliwych wiadomości dotyczyła dostaw paczek, podszycia pod bank, oszustw na członka rodziny (na dziecko), na kupującego w portalach ogłoszeniowych oraz giełd kryptowalut, czy fałszywych nagród i konkursów.

Jak zauważają eksperci CERT Orange Polska, charakter cyberataków się zmienia. Ataki są coraz bardziej zestandaryzowane - około 90% powstaje na bazie jednego szablonu, domeny są produkowane automatycznie, na masową skalę. Następnie jednak indywidualnie wybierane są ofiary - dokładnie rozpoznawane przez przestępców pod kątem potencjału finansowego i prawdopodobieństwa podatności na oszustwo.

DDoS – więcej ataków średniej wielkości, wzrosła częstotliwość

Częstość występowania ataków DDoS od końca roku 2023 znacznie wzrosła. Najwięcej alertów zarejestrowano na przełomie września i października (nawet ponad 10 tys. na dobę). W tym czasie obserwowano zwiększoną liczbę ataków typu carpet bombing, czyli takich, w których celem są całe podsieci, a nie pojedyncze konkretne adresy IP.

Najwięcej alertów – ponad połowa - dotyczyło ataków o średnim stopniu nasilenia. W porównaniu do 2023 r., w ub. roku było ich wyraźnie więcej (wzrost o blisko 9 pp.) **Średnia wielkość natężenia ataku DDoS** zaobserwowana w sieci Orange Polska sięgnęła **ponad 7,2 Gb/s (nieco ponad 3,2 Gb/s w roku 2023).** Z kolei **największa odnotowana wartość** natężenia ruchu w szczycie ataku **to ok. 586 Gb/s** (przy niemal 543 Gb/s w 2023).

Coraz częściej obserwowane były ataki bardziej wyrafinowane, dopasowane do rozpoznanego celu ataku, w których o ich dotkliwości nie stanowi tylko jak największa siła, ale też treść i format wysyłanych pakietów czy zapytań aplikacyjnych.

Podatności i złośliwe oprogramowanie: istotne zagrożenie teraz i w przyszłości

Cyberprzestępcy skupiają się na kradzieży danych i ich monetyzowaniu. Eksperci dostrzegają prężnie rozwijający się ekosystem cyberprzestępczy, w którym operatorzy **malware**, brokerzy początkowego dostępu (pozyskujący dostępy do infrastruktury np. poprzez urządzenia brzegowe czy komputery) i grupy ransomware działają w ramach wyspecjalizowanych segmentów łańcucha ataku.

To sprawia, że **ataki** stają się coraz **bardziej modułowe i profesjonalne** – niektóre grupy koncentrują się wyłącznie na początkowej fazie ataku, inne specjalizują się w wykradaniu (eksfiltracji) danych, ich analizie i wykorzystaniu do dalszych operacji.

Wcześniej głównym celem ataków **ransomware** było szyfrowanie danych ofiary i blokowanie dostępu do kluczowych systemów. Obecnie nacisk kładziony jest na bardziej złożone mechanizmy wymuszeń, które zapewniają atakującym większe szanse na skuteczne wyłudzenie pieniędzy, takie jak metody podwójnego lub nawet potrójnego nacisku (Double czy Triple Extortion) polegające na szyfrowaniu, ujawnianiu skradzionych danych i wymuszania okupu. W ostatnim czasie pojawił się także trend wtórnego szantażu (Re-Extortion), w którym dane pochodzące z wcześniejszych wycieków są wykorzystywane do nowych wymuszeń.

Cyberprzestępcy coraz częściej wykorzystują **gorzej zabezpieczoną infrastrukturę firm trzecich** jako sposób na uzyskanie **dostępu do właściwego celu ataku**.

W ostatnim czasie wiele krytycznych **podatności** zostało odkrytych **w urządzeniach sieciowych i systemach bezpieczeństwa**. Cyberprzestępcy błyskawicznie wykorzystują te luki, zanim organizacje zdołają zabezpieczyć systemy oficjalnymi aktualizacjami. Po przejęciu urządzenia atakujący często zyskuje dostęp uprzywilejowany lub może podsłuchiwać i manipulować ruchem sieciowym.

Trendy – AI, podatności, APT, kryptowaluty, rozwiązania chmurowe i haktywizm – to one zdefiniują przyszłość cyberprzestrzeni

Eksperci CERT Orange Polska przewidują, iż wykorzystanie sztucznej inteligencji przez cyberprzestępców prawdopodobnie stanie się bardziej zaawansowane i powszechne, zagrażając różnym obszarom bezpieczeństwa. Cyberprzestępcy wykorzystają AI do dezinformacji i bardziej efektywnego manipulowania opinią publiczną.

Podatności będą opierać się głównie na „wstrzyknięciach” (direct/indirect prompt injection) doprowadzających do wycieków danych. Z kolei opracowywane długoterminowe strategie

będą polegały na głębokiej infiltracji firm z sektorów strategicznych przez zaawansowane grupy, których głównym celem jest cyberszpiegostwo.

Jednym z głównych celów ataków będą rozwiązania chmurowe. Trend wykorzystania dostępów partnerskich doskonale wpisuje się w rosnącą falę ataków na łańcuchy dostaw.

Rynek kryptowalut staje się obecnie podstawowy dla grup hakerskich, zarówno na poziomie detalicznym, jak i tym bardzo mocno zorganizowanym. Eksperci podkreślają, że ataki malware (w modelu Malware-as-a-Service) mają na celu również wszelkiego rodzaju nośniki/portfele kryptowalut. Dzięki temu przestępcy mogą łatwiej transferować skradzione środki oraz anonimizować transakcje, co utrudnia ich śledzenie. Zauważają także trend, w którym cyberprzestępcy dokonują dobrze przygotowanych kradzieży o dużej wartości (okradając giełdy lub instytucje finansowe).

Firmy powinny być szczególnie czujne

Ze względu na rosnące zagrożenia, firmy muszą być szczególnie czujne, zwłaszcza w kontekście ataków na łańcuch dostaw.

- *Istotne stało się nie tylko monitorowanie swoich systemów, ale także dostawców i kontrahentów oraz regularne przeprowadzanie audytów bezpieczeństwa, aby zidentyfikować potencjalne luki. Zabezpieczanie dostępu do danych i systemów, powinno być priorytetem dla każdej firmy. Ważne jest również przestrzeganie podstawowych zasad bezpieczeństwa, regularne aktualizacje oprogramowania oraz edukacja pracowników na temat zagrożeń. Wiele incydentów wynika z błędów ludzkich, dlatego inwestycja w szkolenia i świadomość pracowników jest kluczowa. Pomaga w tym także nasze Centrum Doświadczeń Cyberbezpieczeństwa* – mówi Piotr Markowicz, dyrektor rozwoju i strategii ICT w Orange Polska.

Podczas wdrażania nowych technologii, w tym sztucznej inteligencji, firmy powinny zawsze uwzględniać bezpieczeństwo. Innowacje mogą przynieść znaczne korzyści biznesowe, ale ich implementacja bez odpowiednich zabezpieczeń stwarza dodatkowe ryzyka. Tylko w ten sposób firmy mogą zbudować solidne fundamenty bezpieczeństwa w dynamicznie zmieniającym się środowisku technologicznym.

Raport CERT Orange Polska za rok 2024 jest dostępny tu. Warto na bieżąco śledzić aktualności i ostrzeżenia na stronach CERT Orange Polska, na Twitterze @CERT_OPL, a także w każdy czwartek na blogu Orange. Wiadomości z linkami, które wzbudzają nasz niepokój - SMS-y lub wiadomości z komunikatorów, czy podejrzane reklamy w mediach społecznościowych, można przesłać na numer 508 700 900. Pozwoli to na skuteczniejszą ochronę wielu osób przed oszustwem. Wysłanie wiadomości na 508 700 900 jest darmowe dla klientów usług mobilnych Orange Polska.

Źródło: blog Orange Polska https://biuroprasowe.orange.pl