**Całkowite koszty ataków ransomware siedmiokrotnie przekraczają wartość okupu! Czy polskie firmy są bezpieczne?**

**Globalna liczba ataków ransomware wzrosła aż o 24 proc., natomiast okup za odszyfrowanie danych potrafi sięgnąć 5 proc. rocznych przychodów przedsiębiorstwa. Okazuje się jednak, że to niewielka część rzeczywistych kosztów poniesionych przez zaatakowane przedsiębiorstwa. Te mogą być nawet siedmiokrotnie wyższe od samego okupu – wynika z analiz Check Point Research, przeprowadzonych na podstawie danych Kovrr oraz wyciekach informacji z rosyjskiej grupy hakerskiej Conti.**

Ataki hakerskie to intratny biznes dla cyberprzestępców, o czym przekonało się wiele międzynarodowych korporacji płacących okup za odszyfrowanie swoich danych po atakach ransomware. Z analiz Check Point Research, przeprowadzonych na podstawie analiz bazy danych o incydentach cybernetycznych firmy Kovrr, wynika, że przeciętna wartość okupu oczekiwanego przez organizacje cyberprzestępcze waha się od 0,7 do 5 proc. rocznych przychodów. Cios wymierzony w zaatakowane przedsiębiorstwa jest jednak dużo większy, bowiem szacunki mówią o nawet siedmiokrotnie wyższych (niż okup) stratach finansowych, które związane są m.in. z zakłóceniem działalności przedsiębiorstwa oraz stratami wizerunkowymi.

W pierwszym kwartale roku 1 na 53 organizacje na świecie doświadczyła próby ataku ransomware, co przełożyło się na 24 proc. wzrostem względem analogicznego okresu w roku 2021. W regionie EMEA wzrosty są jeszcze wyższe i sięgają 37 proc., natomiast w samej Europie oscylują w granicach 18 proc. Co interesujące, w Polsce tendencja jest odwrotna i w pierwszym kwartale br. liczba ataków spadła aż o 44 proc. Zaledwie 1 na 104 organizacje doświadczyły tego typu działalności cyberprzestępców. Nie oznacza to jednak, że nasze przedsiębiorstwa są lepiej zabezpieczone, a raczej z faktu, że zapewniają niższy zwrot z „inwestycji” w postaci solidnie zaplanowanego ataku. Sytuacja ta może ulec zmianie m.in. ze względu na rosnącą ilość tego typu ataków globalnie oraz fakt, że część systemów do ich przeprowadzania jest dostępna w Darknecie za relatywnie niską opłatą. Oznacza to, że kolejni cyberprzestępcy będą musieli szukać coraz to nowszych celów, być może z niższym potencjałem finansowym.

Zdaniem ekspertów Check Point Research w ostatnim roku skrócił się czas trwania ataku z 15 do 9 dni, a grupy ransomware zaczynają mieć jasno ustalone procedury negocjacyjne. Bazują one na dokładnie oszacowanej sytuacji finansowej swoich ofiar, jakości eksfiltrowanych danych czy wykupionego cyberubezpieczenia. Informacje te udało się potwierdzić dzięki dalszym analizom wycieków z rosyjskiej grupy cyberprzestępczej Conti, specjalizującej się właśnie w atakach ransomware.

*- W naszym badaniu szczegółowo przyjrzeliśmy się atakom ransomware zarówno z perspektywy atakujących, jak i ofiar. Kluczowym wnioskiem jest to, że zapłacony okup nie jest najistotniejszą wartością w ekosystemie oprogramowania ransomware. Zadziwiającym jest fakt, że cyberprzestępcy posiadają własną metodologię w określaniu kwoty okupu i prowadzeniu negocjacji. Nic nie jest tu przypadkowe. Na uwagę zasługuje również fakt, że dla ofiar dodatkowe koszty ataków ransomware są nawet 7-krotnie wyższe niż okup, który płacą. Nasze analizy podkreślają zatem, że zbudowanie odpowiedniej cyberobrony, a zwłaszcza dobrze zdefiniowanego planu reakcji, może zaoszczędzić organizacjom dużo pieniędzy –* mówi Sergey Shykevich, menedżer grupy odpowiadającej za wywiad zagrożeń w Check Point Software

**W jaki sposób polskie firmy powinny chronić się przed ransomware?** Oto podstawowe wskazówki:

**1. Solidna kopia zapasowa danych.** Celem ransomware jest zmuszenie ofiary do zapłacenia okupu w celu odzyskania dostępu do zaszyfrowanych danych. Jest to jednak skuteczne tylko wtedy, gdy cel faktycznie utraci dostęp do swoich danych. Solidne, bezpieczne rozwiązanie do tworzenia kopii zapasowych danych to skuteczny sposób na złagodzenie skutków ataku ransomware.

**2. Szkolenie w zakresie świadomości cybernetycznej.** Wiadomości phishingowe to jeden z najpopularniejszych sposobów rozpowszechniania złośliwego oprogramowania. Nakłaniając użytkownika do kliknięcia łącza lub otwarcia złośliwego załącznika, cyberprzestępcy mogą uzyskać dostęp do komputera pracownika i rozpocząć na nim proces instalacji i uruchamiania programu ransomware. Częste szkolenia uświadamiające mają kluczowe znaczenie dla ochrony organizacji przed oprogramowaniem ransomware.

**3. Silne, bezpieczne uwierzytelnianie użytkownika.** Egzekwowanie silnych zasad dotyczących haseł, wymagające korzystania z uwierzytelniania wieloskładnikowego oraz edukowanie pracowników w zakresie ataków phishingowych mających na celu kradzież danych logowania to kluczowe elementy strategii cyberbezpieczeństwa organizacji.

**4. Aktualne poprawki.** Aktualizowanie komputerów i stosowanie poprawek zabezpieczeń, zwłaszcza tych oznaczonych jako krytyczne, może pomóc ograniczyć podatność organizacji na ataki ransomware.