Cyberdefence 24

02.08.2021

RANSOMWARE ROŚNIE LAWINOWO. PONAD 304 MLN ATAKÓW W CIĄGU PÓŁ ROKU

W ciągu pierwszego półrocza 2021 roku liczba ataków typu ransomware wzrosła do 304,7 mln – wynika z analizy firmy SonicWall. Na szczycie listy ofiar są użytkownicy i podmioty z USA, Wielkiej Brytanii, Niemiec, Południowej Afryki i Brazylii.

Ransomware to złośliwe oprogramowanie (malware), które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

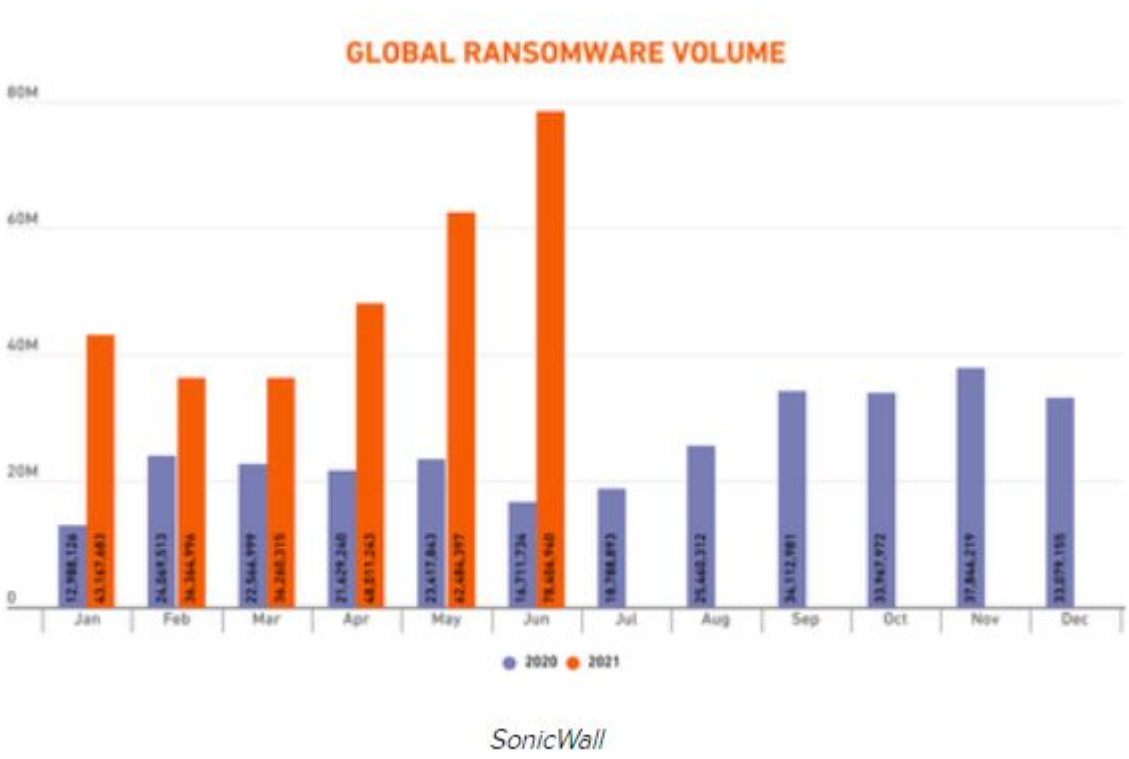
Najprostsze typy programów typu ransomware jedynie zakładają na system blokadę, stosunkowo łatwą do zlikwidowania dla doświadczonych użytkowników komputera. Bardziej zaawansowane formy stosują natomiast technikę zwaną kryptowirusowym wymuszeniem – szyfrują pliki ofiary, uniemożliwiając tym samym ich normalny odczyt i żądają okupu w zamian za deszyfrację danych.

W prawidłowo przeprowadzonym ataku, przywrócenie danych bez posiadania klucza deszyfrującego jest praktycznie niemożliwe.

Skala ataków ransomware rośnie lawinowo

Z danych opracowanych przez zajmującą się cyberbezpieczeństwem firmę SonicWall wynika, że skala ataków ransomware rośnie dynamicznie na całym świecie.

W pierwszej połowie 2021 roku zanotowano globalnie 304,7 mln ataków z wykorzystaniem ransomware. To oznacza, że w ciągu minionego półrocza liczba ataków przekroczyła tę z całego 2020 roku, gdy incydentów typu ransomware było 304,6 mln. **Według analityków podane liczby oznaczają wzrost aktywności ransomware o 151 proc.**



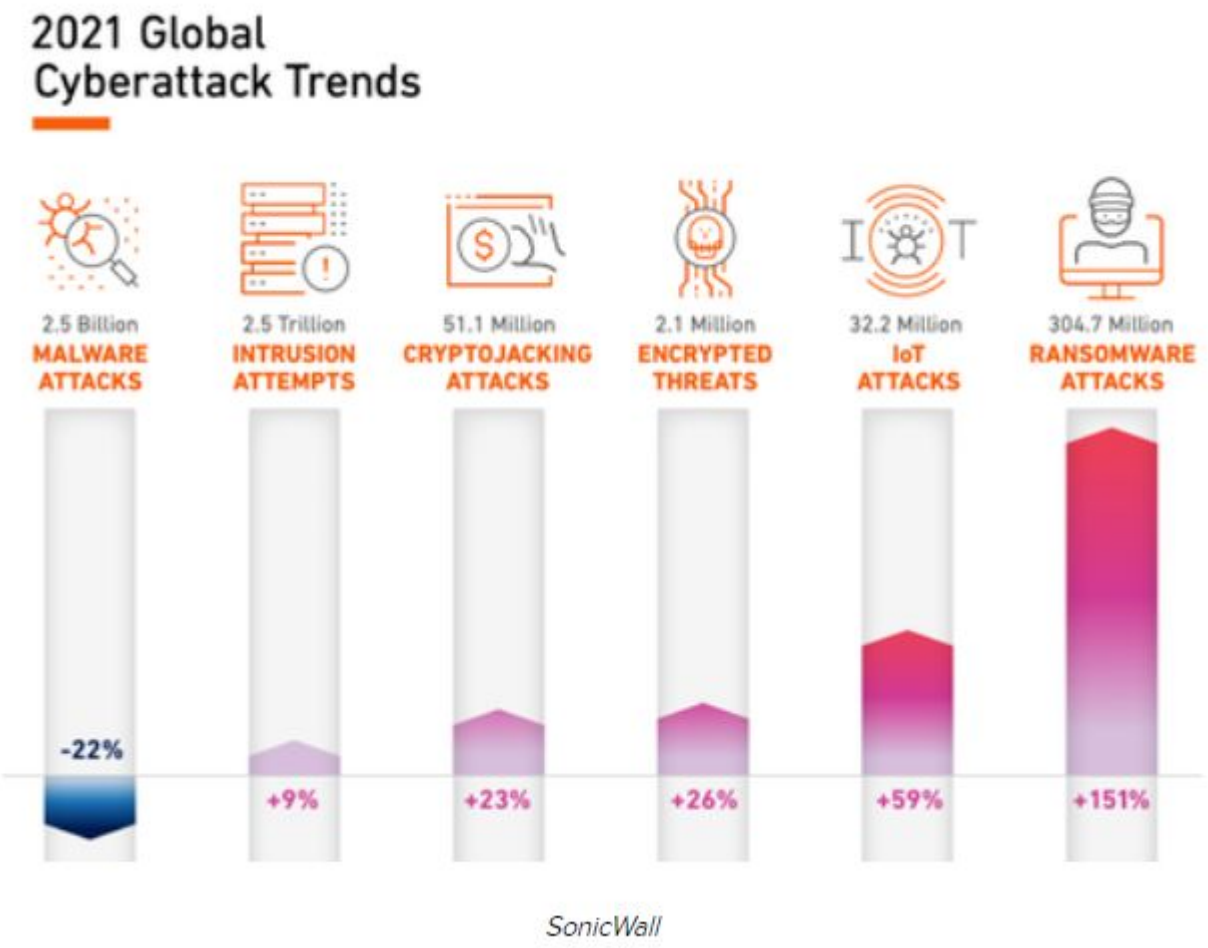
Fot. SonicWall

W pierwszej połowie 2021 najwięcej ataków ransomware dokonano w lipcu (78,4 mln), choć tendencja wzrostowa była wyraźnie widoczna także w kwietniu i maju.

Zgodnie z reportem SonicWall, podstawowym celem cyberprzestępców były Stany Zjednoczone (wzrost ransomware o 185 proc.), na drugim miejscu znalazła się Wielka Brytania, a na kolejnych – Niemcy, RPA oraz Brazylia.

W USA największy, trzykrotny wzrost ataków odnotowały tamtejsze instytucje rządowe i publiczne, podmioty z sektora edukacji oraz segment związany z ochroną zdrowia.

Analitycy SonicWall przewidują, że do końca 2021 roku tendencja wzrostowa dotycząca aktywności cyberprzestępców zostanie zachowana. Na wznoszącej fali oprócz ransomware będą m.in. ataki w segmencie IoT oraz te dotyczące nielegalnego wykorzystania zasobów informatycznych do pozyskiwania kryptowalut.



Fot. SonicWall

Czy płacić za ransoware?

Celem ransomware padają najczęściej większe i mniejsze firmy, które przez tego typu ataki mogą wiele stracić. Powstaje więc pytanie, czy zaatakowane podmioty powinny płacić cyberprzestępcom, czy też szukać innych rozwiązań problemu?

Według Łukasza Bromirskiego, eksperta Cisco odpowiedzialnego za rozwój produktów z obszaru cyberbezpieczeństwa, odpowiedź na to pytanie nie jest prosta.

"Patrząc na sprawę z dystansu – wyobraźmy sobie, że firma X decyduje się na zapłatę. W ten sposób bezpośrednio finansuje nielegalne działania przestępców". – przyznaje Łukasz Bromirski. "Pośrednio pokazuje to, że ufa tym, którzy właśnie włamali się do jej sieci i uczynili z niej zakładnika. Nie ma przecież gwarancji, że po wpłaceniu okupu intruzi odblokują dane. Jeśli nawet to uczynią, wciąż trzeba będzie stawić czoła kolejnym zagrożeniom. Dzisiaj w szczególności duże firmy z reguły jednak decydują się zapłacić. Na tę sytuację powoli negatywnie zaczynają reagować ubezpieczyciele, którzy podnoszą składki" - ocenia.

Według ekspertów **po pierwsze, zapłacenie okupu nie sprawi, że cyberprzestępcy samoistnie znikną z zaatakowanego środowiska.** Płatność nie naprawi również błędów w zabezpieczeniach, a to przecież za ich sprawą atakującym udało się zdobyć przyczółek w sieci. W większości wypadków, cyberprzestępcy nie dzielą się nawet wiedzą jak udało im się włamać, a nawet jeśli to zrobią – na ile można im ufać, że podzielili się wszystkimi informacjami? Zaatakowana organizacja nie ma pewności czy faktycznie poznała wszystkie możliwe do wykorzystania furtki. Cyberprzestępcy na pewno skorzystają z kolejnej okazji, jeżeli taka się nadarzy.

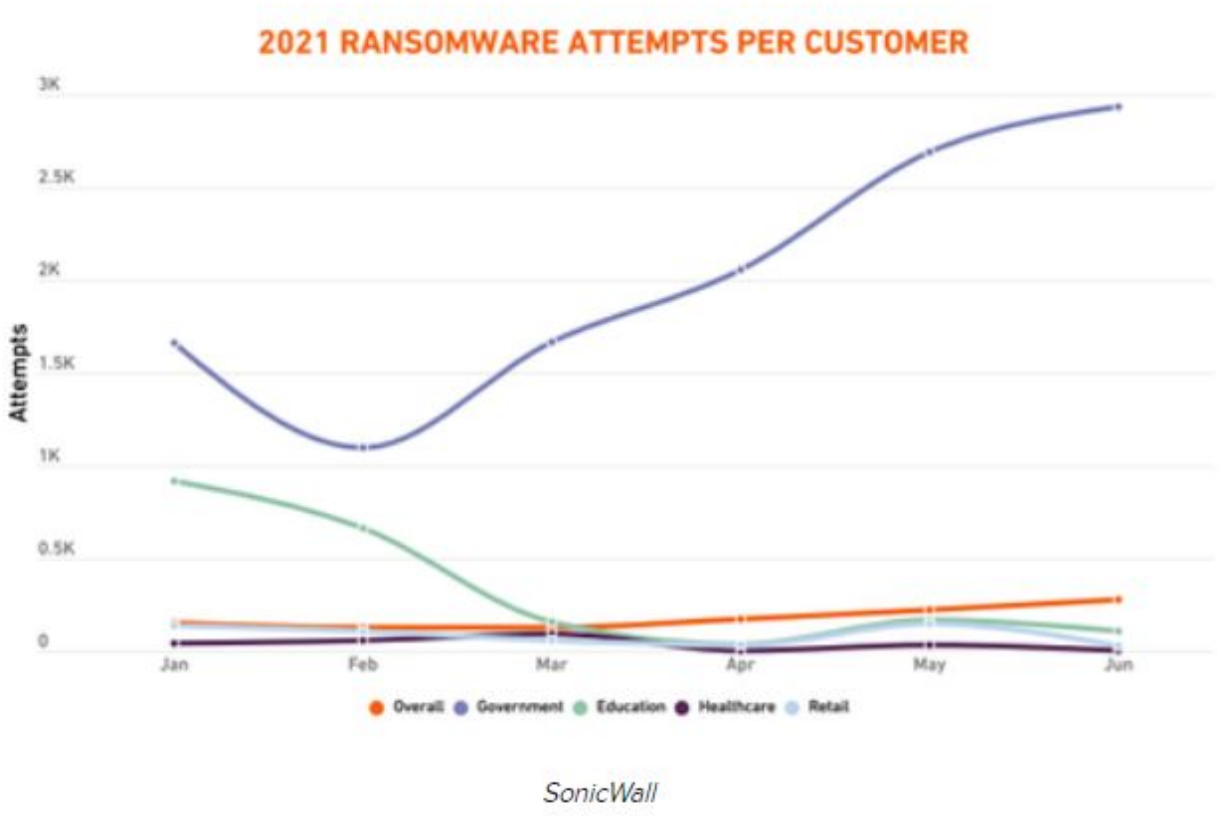
Po drugie, biznesowa zasada mówi, że łatwiej jest generować przychody z istniejących klientów, niż szukać nowych. Ta prawidłowość ma zastosowanie również wśród hakerów. Nawet bez sprawdzonej ścieżki ataku, wykonali już mapowanie sieci, aplikacji i **być może mają znacznie więcej danych i dostępów, niż przyznają.** Przykładowo pełną listę kont z uprawnieniami administratora, do których hasła już złamali, albo złamią w ciągu najbliższych godzin czy dni. Mogą chcieć ponownie „spróbować szczęścia" z tą samą organizacją.

Po trzecie, nigdy nie można mieć pewności, że odblokowane dane nie zostały przypadkowo uszkodzone. Zawsze coś może pójść nie tak, nawet jeśli atakujący za pomocą oprogramowania ransomware stara się postępować „zgodnie ze sztuką". Przypadki, gdy „oprogramowanie odszyfrowujące" lub po prostu klucz wpisany do złośliwego oprogramowania uszkadzał pliki w wyniku zwykłych ludzkich błędów programistycznych (cyberprzestępca-programista to nadal „tylko" programista) są liczne.

"W efekcie kwota okupu to tak naprawdę tylko jeden z pierwszych kosztów" – podkreśla Łukasz Bromirski. "Zaatakowana firma będzie musiała ponieść też inne nakłady finansowe, począwszy od gruntownego audytu, łatania platform IT w celu usunięcia pierwotnej przyczyny włamania (jeśli jest znana) czy wreszcie organizacji szkoleń z zakresu cyberbezpieczeństwa, jeśli wektorem ataku był np. udany phishing. W przeciwnym razie, choć gwarancji nie ma przecież nigdy, firma znowu padnie ofiarą ataku i stanie przed tym samym wyborem: płacić okup czy nie" – podkreśla Łukasz Bromirski z Cisco.

Eksperci Cisco radzą, aby **spojrzeć na swoją firmę tak, jak zrobiłby to napastnik.** Dzięki temu można łatwiej dostrzec słabe punkty w ramach całej architektury IT. Kolejny krok to ustalenie priorytetów i zniwelowanie podatności na atak.

Departament Sprawiedliwości Stanów Zjednoczonych, Europol oraz kilka największych firm technologicznych na świecie, w tym Cisco, utworzyły grupę zadaniową ds. oprogramowania ransomware, aby zwalczać problem u źródła. Inicjatorzy przedsięwzięcia zgodnie uznali, że współpraca międzynarodowa i publiczno-prywatna mają kluczowe znaczenie dla osiągnięcia tego celu.



Fot. Reklama

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.

Fot. Reklama