**Hakerzy tworzą armię botnetów oraz kradną dane z kart kredytowych**

**Złośliwe botnety wielofunkcyjne dotknęły 28% wszystkich organizacji na całym świecie, natomiast o 20% wzrosły statystyki ukierunkowanych ataków ransomware - wynika z Raportu Bezpieczeństwa Cybernetycznego 2020 firmy Check Point. Raport wskazuje na główne taktyki stosowane przez cyberprzestępców do atakowania organizacji na całym świecie we wszystkich branżach, a także zapewnia specjalistom ds. bezpieczeństwa cybernetycznego i kadrze kierowniczej na poziomie C informacje potrzebne do ochrony ich organizacji przed współczesnymi zagrożeniami.**

Raport bezpieczeństwa na rok 2020 ujawnia kluczowe wektory i techniki ataków zaobserwowane przez badaczy Check Point w ubiegłym roku. Najważniejsze z nich to:

l **Kryptominery nadal dominują w środowisku złośliwego oprogramowania -** mimo że w 2019 r. spadła powszechność kopania kryptowalut, związana ze spadkiem ich wartości i zamknięciem działalności malware’u Coinhive, 38% firm na całym świecie zostało dotkniętych przez koparki kryptowalut, w porównaniu do 37% w 2018. Wynika to z faktu, że ataki za pomocą kryptominerów pozostają przestępstwem o niskim ryzyku i wciąż relatywnie wysokim zyskiem.

l **Wzrost liczby armii botnetów** - aktywność botnetów dotknęła 28% organizacji na całym świecie, co stanowi wzrost o ponad 50% w porównaniu z 2018 rokiem. Emotet był najczęściej wykorzystywanym złośliwym oprogramowaniem, przede wszystkim ze względu na jego wszechstronność w zakresie usług dystrybucji złośliwego oprogramowania i spamu. Inne działania botnetów, takie jak aktywność sekstoracyjna i ataki DDoS, również gwałtownie wzrosły.

l **Ukierunkowane oprogramowanie ransomware uderza z dużą siłą** - chociaż liczba atakowanych organizacji jest stosunkowo niska, dotkliwość ataku jest znacznie wyższa - jak widać w szkodliwych atakach na administrację miast w USA w 2019 r. Przestępcy ostrożnie wybierają swoje cele związane z oprogramowaniem ransomware w celu wyłudzenia maksymalnego możliwego dochodu.

l **Spadek ataków na urządzenia mobilne** - 27% organizacji na całym świecie zostało dotkniętych cyberatakami, które dotyczyły urządzeń mobilnych w 2019 r., w porównaniu z 33% w 2018 r. Podczas gdy krajobraz zagrożeń mobilnych dojrzewa, organizacje są coraz bardziej świadome zagrożenia i wdrażają rozwiązania bezpieczeństwa dla urządzeń mobilnych.

l **Rok, w którym ataki Magecart stały się epidemią** - ataki, które wstrzykują złośliwy kod do witryn handlu elektronicznego w celu kradzieży danych o płatnościach klientów, przeprowadzone były na setki witryn w 2019 r., Zagrożenie dotyczyło głównie sieci hotelowych przez gigantów handlowych, aż po małe i średnie firmy działające na wszystkich platformach.

l **Wzrost liczby ataków w chmurze -** obecnie ponad 90% przedsiębiorstw korzysta z usług w chmurze, a jednak 67% zespołów ds. bezpieczeństwa skarży się na brak wglądu w infrastrukturę chmury, bezpieczeństwo i zgodność. Skala ataków i naruszeń w chmurze nadal rośnie. Błędna konfiguracja zasobów w chmurze jest nadal główną przyczyną ataków, jednak teraz obserwujemy również rosnącą liczbę ataków skierowanych bezpośrednio do dostawców tych usług.

- *Rok 2019 przedstawił złożony krajobraz zagrożeń, w którym państwa narodowe, organizacje zajmujące się cyberprzestępczością i prywatni kontrahenci przyspieszyli wyścig zbrojeń cybernetycznych -* powiedział Lotem Finkelsteen, główny oficer wywiadu, Check Point Software Technologie. - *Nawet jeśli organizacja jest wyposażona w najbardziej kompleksowe, najnowocześniejsze produkty bezpieczeństwa, nie można całkowicie wyeliminować ryzyka naruszeń. Poza wykrywaniem i naprawą organizacje muszą przyjąć proaktywny plan, aby wyprzedzać cyberprzestępców i zapobiegać atakom. Wykrywanie i automatyczne blokowanie ataku na wczesnym etapie może zapobiec wielu zagrożeniom. W raporcie bezpieczeństwa Check Point 2020 wskazano, na co organizacje muszą zwracać uwagę i jak wygrać wojnę z cyberatakami dzięki dobrym praktykom.*

Raport bezpieczeństwa Check Point 2020 opiera się na danych z wywiadu ThreatCloud Check Point, największej sieci współpracy do walki z cyberprzestępczością, która dostarcza dane o zagrożeniach i trendy ataków z globalnej sieci czujników zagrożeń; z badań prowadzonych przez Check Point w ciągu ostatnich 12 miesięcy oraz informacji uzyskanych od specjalistów IT i kadry kierowniczej na poziomie C, oceniających ich gotowość na dzisiejsze zagrożenia. Raport analizuje najnowsze pojawiające się zagrożenia dla różnych sektorów przemysłu i zawiera kompleksowy przegląd trendów zaobserwowanych w krajobrazie złośliwego oprogramowania, pojawiających się wektorów naruszających dane oraz cyberataków.

Aby uzyskać więcej informacji należy pobrać [pełny raport](https://pages.checkpoint.com/cyber-security-report-2020.html) lub wejść na [blog](https://blog.checkpoint.com/2020/01/15/the-2020-check-point-cyber-security-annual-report-is-available/) **firmy Check Point**.