**Działy IT nieświadome zagrożeń ze strony cryptominerów**

**W zeszłym roku cryptominery zaraziły ponad 10 razy więcej organizacji niż ransomware, jednak wciąż ten rodzaj zagrożenia jest niedoceniany przez firmy – to główny wniosek drugiej części Raportu Bezpieczeństwa, stworzonego przez analityków firmy Check Point Software Technologies. Największy procentowy udział tego typu ataków zaobserwowano na kontynentach amerykańskich (42%).**

**W Raporcie Bezpieczeństwa opisano w jaki sposób narzędzia używane do popełniania cyberprzestępstw, zostały zdemokratyzowane – stały się powszechni wykorzystywane przez każdego, kto zechce za nie zapłacić. Zjawisko nazwano “malware-as-a-service”. Badacze firmy Check Point prezentują znaczny wzrost zaawansowanych ataków zaprojektowanych w sposób niewidoczny dla firmowych działów ds. bezpieczeństwa.** Pokazują również rodzaje cyberataków, które specjaliści od zabezpieczeń uznają za największe zagrożenia dla organizacji, w których pracują.

**Wg analityków, główną zmorą firm były niewykryte cryptominery pracujące w sieciach korporacyjnych.** Cryptominery zaraziły ponad 10 razy więcej organizacji niż ransomware w 2018 roku, ale tylko jeden na pięciu pracowników bezpieczeństwa IT był świadomy, że sieć należąca do jego firmy została zarażona złośliwym oprogramowaniem. 37% firm na świecie zostało zaatakowanych cryptominerami w 2018 roku i 20% firm jest nadal co tydzień celem tego typu ataków, pomimo 80% spadku wartości kryptowalut.

**Zagrożenie spowodowane przez cryptominery jest jednak często niedoceniane.** Spośród ekspertów zapytanych o to, co jest największym zagrożeniem dla ich firm, tylko 16% odpowiedziało, że cryptomining. Pozostałe odpowiedzi to: ataki DDoS (34%), wycieki danych (53%), ransomware (54%) i phishing (66%). Jest to niepokojące, gdyż cryptominery mogą stanowić ukryty backdoor służący do pobrania i uruchomienia innych typów złośliwego oprogramowania.

Eksperci Check Pointa, zwracają również uwagę na rozwój malware-as-a-service, czyli udostępnianie złośliwego oprogramowania jako płatnej usługi. Przykładowo, przypadek [GandCrab Ransomware-as-a-Service affiliate](https://research.checkpoint.com/gandcrab-ransomware-mindset/) ukazuje, w jaki sposób amatorzy mogą czerpać zyski z tego typu działań. Użytkownicy CandCrab zachowują 60% z okupów wpłaconych przez ofiary, a developerzy pobierają pozostałe 40%. GandCrab ma ponad 80 aktywnych partnerów i w ciągu dwóch miesięcy w 2018 roku zainfekował ponad 50 000 ofiar, wymuszając okupy w łącznej wysokości około 300 000 - 600 000 dolarów.

*- Druga część naszego Raportu Bezpieczeństwa 2019 pokazuje, w jaki sposób cyberprzestępcy rozwijają nowe, trudniejsze do wykrycia techniki i nowe modele biznesowe, takie jak np. programy partnerskie złośliwego oprogramowania, w celu maksymalizacji zysków, jednocześnie redukując ryzyko złapania. Nie możemy jednak powiedzieć, że czego oczy nie widzą, tego sercu nie żal: pomimo tego, że ataki w 2018 roku były rzadziej wykrywane, nadal stanowiły niebezpieczeństwo i ryzyko strat dla firm* - powiedział Peter Alexander, szef działu Marketingu firmy Check Point Software Technologies.

Raport Bezpieczeństwa 2019 firmy Check Point opiera się na danych pochodzących z Check Point ThreatCloud, największej, kolaboracyjnej sieci powstałej w celu walki z cyberprzestępczością, która dostarcza danych o zagrożeniach i trendach ataków z globalnej sieci wykrywaczy zagrożeń, z badań Check Point w ostatnich 12 miesiącach oraz z nowej ankiety dla specjalistów IT i kadry zarządzającej, która bada gotowość na nowoczesne zagrożenia. Raport ten analizuje najnowsze zagrożenia w różnych sektorach gospodarki, a także zawiera kompleksowy przegląd trendów dotyczących złośliwego oprogramowania, nowopowstałych wektorów wycieków danych oraz ataków na struktury państwowe. Zawarto w nim również analizy ekspertów firmy Check Point, aby pomóc organizacjom zrozumieć i przygotować się na teraźniejsze i przyszłe złożone cyberzagrożenia piątej generacji.

**Pełny raport jest dostępny pod adresem:**

<https://research.checkpoint.com/2019-security-report-vol-2-under-the-hood-of-cyber-crime>

**O Check Point Research**

Check Point Research dostarcza istotnych danych o zagrożeniach sieciowych klientom firmy Check Point Software i całej społeczności bezpieczeństwa. Grupa badawcza zbiera i analizuje dane o atakach zgromadzone w ThreatCloud w celu powstrzymania hakerów, jednocześnie upewniając się, że wszystkie produkty firmy Check Point mają najnowsze zabezpieczenia. Grupa badawcza składa się z ponad 100 analityków i badaczy współpracujących z innymi firmami zajmującymi się bezpieczeństwem oraz zespołami reagowania na zagrożenia internetowe.