Cyberdefence 24

**aut. Szymon Palczewski** 31.07.2020

# „CYBERNAJEMNICY" ATAKUJĄ EUROPĘ. FINTECHY I FIRMY PRAWNICZE OBIEKTEM SZPIEGOSTWA

Grupa hakerów działających na zlecenie odpowiada za kampanie prowadzone w Europie, których celem były firmy prawnicze oraz fintechy. Złośliwe operacje bazują na spear phishingu, który ma ułatwić kradzież tajemnic biznesowych oraz finansowych. Metody działania hakerów charakteryzują się prostotą, ale i dużym sprytem.

Eksperci Kapsersky odkryli nową grupę hakerów, specjalizujących się w szpiegostwie. Eksperci nazwali ją Deceptikons, a zebrane materiały wskazują, że cyberprzestępcy świadczą usługi na zlecenie od prawie dekady. „Grupa nie jest technicznie zaawansowana i, o ile nam wiadomo, nie wdrożyła exploitów zero-day" – czytamy w oficjalnym komunikacie Kaspersky. Według firmy mamy do czynienia z „cybernajemnikami".

Specjaliści podkreślają, że zestaw narzędzi i złośliwego oprogramowania Deceptikons jest „przebiegły, a nie zaawansowany technicznie". Grupę charakteryzuje również wytrwałość w działaniu. Powtarzające się cyberataki na podmioty komercyjne i pozarządowe są dość nietypowe dla aktorów APT. Vicente Diaz, ekspert Kaspersky, stwierdził, że złośliwe działania Deceptikons były skierowane przede wszystkim przeciwko firmom prawniczym i fintechom.

Kaspersky wskazuje, że w 2019 roku hakerzy przeprowadzili kampanię spear phishingową, której celem były głównie firmy na terenie Europy. Wówczas grupa instalowała na urządzeniach ofiary złośliwe oprogramowanie PowerShell. Było to możliwe poprzez skłonienie użytkowników do interakcji z zainfekowanymi plikami. To z kolei pozwalało hakerom złamać zabezpieczenia systemów i zainstalować backdoora.

„Najprawdopodobniej motywacją grupy była chęć uzyskania określonych informacji finansowych czy szczegółów negocjacji" – tłumaczą specjaliści Kaspersky w komunikacie. Vicente Diaz dodał na łamach ZDNet, że Deceptikons koncentruje się na kradzieży tajemnic biznesowych i finansowych, a nie informacji związanych z rządem. Co więcej, zaznaczył, że hakerzy skupiają się na europejskich podmiotach, ale złośliwe kampanie były również obserwowane w krajach Bliskiego Wschodu, takich jak Izrael, Jordania i Egipt.

Eksperci nie wskazali konkretnej liczby ofiar ani żadnych innych szczegółów na temat poszkodowanych podmiotów. Nie odnieśli się również do możliwego pochodzenia hakerów Deceptikons. Zgodnie z zapowiedzią Kaspersky, bardziej szczegółowa analiza zostanie opublikowana w najbliższym czasie.

**Czytaj też:** Polska celem Korei Północnej. Hakerzy wykradali dane i środki finansowe