**Uwaga na zainfekowane CV i zwolnienia lekarskie**

**• Eksperci alarmują, że w załącznikach z plikami CV może kryć się złośliwe oprogramowanie – to rosnący trend wśród hakerów, którzy chcą wykorzystać rosnące bezrobocie na świecie.**

 **• Aż 1 na 450 zidentyfikowanych złośliwych plików wykorzystywany jest do oszustw typu CV scam, co stanowi podwojenie tego typu scenariuszów ataku w ciągu ostatnich 2 miesięcy.**

 **• Ogólna liczba ataków za pośrednictwem malware’u wzrosła aż a o 16%**

Pod koniec maja CNN poinformował, że ponad 40 milionów Amerykanów złożyło wniosek o zasiłek dla bezrobotnych z powodu utraty pracy w wyniku kryzysu koronawirusowego. Aż 1 na 4 dotychczas pracujących Amerykanów ubiegało się o status bezrobotnego – to najwyższy odsetek w historii, większy od tego w czasach wielkiego kryzysu lat 30. XX wieku.

**Jak informuje Check Point, z powodu wysokiej stopy bezrobocia ludzie stali się bardziej podatni na oszustwa internetowe i ataki phishingowe, próbujące wykorzystać m.in. motyw pakietów pomocowych. Ogólna liczba ataków za pośrednictwem malware’u wzrosła aż a o 16%, a coraz popularniejszym trendem stają się fałszywe pliki CV.**

Tego typu zainfekowane dokumenty CV są rozsyłane przez cyberprzestępców do różnych firm. Gdy ofiary otwierają załączone pliki, aplikacja prosi ich o „*włączenie treści”,* która instaluje na komputerze ofiarymalware ZLoader, będący trojanem bankowym zaprojektowanym w celu kradzieży danych uwierzytelniających i innych poufnych informacji. Dzięki skradzionym danym złośliwe oprogramowanie pozwala hakerom połączyć się z bankiem ofiary i dokonywać nielegalnych transakcji finansowych – ostrzega Check Point.

 Zdaniem analityków aż 1 na 450 zidentyfikowanych złośliwych plików wykorzystywany jest do oszustw typu CV scam, co stanowi podwojenie tego typu scenariuszów ataku w ciągu ostatnich 2 miesięcy.

*- Bezrobocie wciąż rośnie, natomiast cyberprzestępcy pracują coraz intensywniej. Używają CV, aby zdobyć cenne informacje, szczególnie w odniesieniu do naszych finansów i bankowości. Zachęcam wszystkich, którzy otwierają wiadomość e-mail z załączonym CV, aby zastanowili się dwa razy. Swoich decyzji możemy później żałować –* mówi Omer Dembinsky, kierownik ds. Analizy danych w Check Point.

Specjaliści firmy Check Point zauważyli ponadto krążące drogą mailową złośliwe formularze zwolnień lekarskich. Dokumenty, używając nazw takich jak „COVID -19 FLMA CENTER.doc”, zainfekowały ofiary tym złośliwym oprogramowaniem IcedID, atakującym banki, dostawców kart płatniczych, dostawców usług mobilnych, a także witryny handlu elektronicznego. IcedID na celu oszukać użytkowników, aby podali swoje dane uwierzytelniające na fałszywych stronach, które są następnie wysyłane na serwer osoby atakującej. W treści maila lub tytule znajduje się najczęściej tekst: *Poniżej znajduje się nowy formularz wniosku pracownika o urlop w ramach Ustawy o urlopie rodzinnym i lekarskim (FMLA).*

Wiadomości e-mail zostały wysłane z różnych domen, takich jak „medical-center.space”, aby zachęcić ofiary do otwarcia złośliwych załączników.

Check Point zaobserwował w maju średnio 158.000 ataków związanych z koronawirusem tygodniowo. W ciągu ostatnich 4 tygodni zarejestrowano kolejne 10 704 nowe domeny dotyczące koronawirusa, z czego 256 było złośliwych, natomiast 1744 zostały uznane za podejrzane.