Cyberdefence 24

aut. Szymon Palczewski 30.07.2020

„POSZUKUJEMY PRACOWNIKA”. AMERYKAŃSKI SEKTOR OBRONNY OFIARĄ HAKERÓW KOREI PÓŁNOCNEJ

Hakerzy Korei Północnej wykorzystują kryzys gospodarczy związany z Covid-19 do prowadzenia złośliwej kampanii wymierzonej w amerykański sektor obronny, lotniczy, a także inne istotne z punktu widzenia państwa branże. Cyberprzestępcy podszywają się pod pracodawców, rozsyłając oferty pracy, które w rzeczywistości są nośnikiem złośliwego oprogramowania. Głównym zadaniem hakerów Pjongajnagu jest gromadzenie danych na temat ofiar i sektorów, w jakich pracują.

Kryzys związany z pandemią koronawirusa przełożył się również na sektor gospodarczy. Obecnie na rynku jest znacznie więcej kandydatów na stanowiska niż wolnych miejsc pracy. Sytuacja ta jest wykorzystywana przez złośliwych aktorów do przeprowadzania kampanii hakerskich. Cyberprzestępcy nakłaniają nieświadome ofiary do otwierania zainfekowanych plików w celu instalowania na ich urządzeniach wirusa. Taką też taktykę przyjęli północnokoreańscy hakerzy w ramach najnowszej kampanii.

Specjaliści McAfee Advanced Threat Research (ATR) zaobserwowali wzrost złośliwej aktywności wymierzonej w amerykański przemysł obrony, sektor lotniczy i inne kluczowe branże. W ramach kampanii mającej miejsce w 2020 roku, eksperci zidentyfikowali serię zainfekowanych plików i innych dokumentów, zawierających ogłoszenia o pracę, które rzekomo miały pochodzić od czołowych podmiotów wspominanych wyżej sektorów. Atrakcyjne dla nieświadomych pracowników pliki służyły jako „wabiki”. Były one rozsyłane w wiadomościach spearphishingowych. W ten sposób hakerzy infekowali urządzenia ofiar złośliwym oprogramowaniem przeznaczonym do zbierania danych – czytamy w oficjalnym komunikacie McAfee.

Analiza kampanii wykazała, że fikcyjne dokumenty były kierowane do osób, posiadających określone zdolności oraz doświadczenie w danej branży. Podobne działania ze strony hakerów zaobserwowano w 2017 i 2019 roku, kiedy cel północnokoreańskiej grupy Hidden Cobra stanowiło gromadzenia danych o kluczowych technologiach wojskowych i obronnych w Stanach Zjednoczonych.

„Techniki, taktyka i procedury działania w 2020 roku są bardzo podobne do tych z poprzednich kampanii” – wskazują eksperci McAfee ATR. – „Modus operandi jest ten sam, jaki obserwowaliśmy w 2017 i 2019 roku”.

Specjaliści dodają, że obecne działania są najprawdopodobniej kontynuacją kampanii z ubiegłego roku na co wskazują liczne podobieństwa. Są one widocznie zarówno w kodzie Visual Basic, jak i w niektórych podstawowych funkcjach złośliwego oprogramowania. To wszystko prowadzi do wniosku, że za najnowszą kampanią stoją hakerzy Pjongjangu.

Działalność grupy Hidden Cobra została przypisana Korei Północnej przez amerykański rząd. Jej

hakerzy odpowiadają za realizowanie globalnych operacji, wymierzonych w organizacje z różnych sektorów, co od wielu lat jest dokumentowane w licznych raportach i analizach. Głównym celem Hidden Cobra jest kradzież kryptowalut, a także gromadzenie danych dotyczących technologii wojskowych.

Badania kampanii z 2020 roku wykazały, że hakerzy za pomocą atrakcyjnie wyglądających dokumentów nakłaniali swoje ofiary do klikania w konkretny link lub plik w celu zainstalowania złośliwego oprogramowania. „Zainfekowane dokumenty Worda zawierały treści związane z legalnymi ofertami pracy u czołowych pracodawców" – czytamy w komunikacie. W ramach dokumentów znajdowały się szczegółowe opisy stanowisk w sektorze obronnym, lotnictwie i innych kluczowych branżach. Według szacunków kampania trwała od 31 marca do 18 maja bieżącego roku.

Następnie hakerzy wykorzystywali zainstalowane złośliwe oprogramowanie do szpiegowania swoich celów. Wirus został zaprojektowany w ten sposób, aby zapewnić skutecznie zbieranie informacji na temat ofiar i miejsca ich pracy. Pozyskane materiały miały być podstawą do realizacji bardziej zaawansowanych operacji.

Specjaliści wskazują, że hakerzy zawsze podejmują wysiłek w celu ukrycia swojej działalności, dlatego też często stosują techniki „naśladowania użytkownika". Takie podejście pozwala im na realizację zadań minimalizując ryzyko wykrycia kampanii.

Dogłębna analiza wykazała, że jedną z „przynęt" hakerów jest również tematyka związana z polityką prowadzoną przez Koreę Północną. Hidden Cobra stworzyła dokumenty w różnych językach, które miały zainteresować odbiorców i zachęcić ich do dalszej interakcji. Przykładem może być plik zatytułowany „US-ROK Relations and Diplomatic Security". Został on wydany w języku koreańskim i angielskim – czytamy w komunikacie McAfee.

„Lista ofiar nie jest dokładnie znana ze względu na brak odkrytych wiadomości e-mail typu spear phishing" – wyjaśniają eksperci. Jak dodają, można jedynie wyciągnąć ogólne wnioski na podstawie analizy dokumentów służących jako przynęty. Zawierały one opisy stanowisk dla inżynierów i kierowników projektów w związku z aktywnymi kontraktami obronnymi. Taki stan rzeczy wskazuje, że złośliwa kampania była wymierzona określoną grupę pracowników i specjalistów, pracujących we wrażliwych dla państwa sektorach.

Czytaj też: Ewolucja Lazarus Group. Hakerzy Pjongjangu z nową bronią i strategią