Cybergang Cloud Atlas uaktualnia swój arsenał

ID artykułu: 58219 / 2264

URL: http://www.publikuj.org/58219

Cloud Atlas, cyberprzestępcze ugrupowanie APT znane również pod nazwą Inception, wzbogaciło swój arsenał o nowe narzędzia, które pozwalają uniknąć wykrycia za pomocą standardowych wskaźników infekcji. Uaktualniony łańcuch infekcji został zidentyfikowany przez badaczy z firmy Kaspersky w różnych organizacjach w Europe Wschodniej, Azji Środkowej oraz Rosji. Cloud Atlas to ugrupowanie, które posiada długą historię operacji cyberszpiegowskich, których celem są różne branże, agencje rządowe oraz inne podmioty. Po raz pierwszy zostało zidentyfikowane w 2014 r. i od tego czasu pozostaje aktywne. Niedawno badacze z firmy Kaspersky wykryli ataki tego ugrupowania skierowane przeciwko branży międzynarodowych stosunków gospodarczych oraz przestrzeni kosmicznej, jak również organizacji rządowych i religijnych znajdujących się między innymi w Portugalii, Rumunii, Turcji, na Ukrainie, w Rosji, w Turkmenistanie, Afganistanie oraz Kirgistanie. Po skutecznej infiltracji Cloud Atlas:

zbierał informacje dotyczące systemu, do którego uzyskał dostęp,

gromadził hasła,

przesyłał niedawno utworzone pliki .txt .pdf .xls .doc do serwera kontrolowanego przez cyberprzestępców.

Chociaż ugrupowanie nie zmieniło znacząco swoich taktyk od 2018 r., z badania niedawnej fali ataków wynika, że zaczęło stosować nowy sposób infekowania swoich ofiar oraz dalsze rozprzestrzenianie infekcji w ich sieciach.

Wcześniej Cloud Atlas wysyłał potencjalnej ofierze spersonalizowaną wiadomość phishingową zawierającą szkodliwy załącznik. Jeśli atak powiódł się, następowało wykonywanie załączonego szkodliwego oprogramowania PowerShower, które służyło do przeprowadzania wstępnego rekonesansu oraz pobierania dodatkowych szkodliwych modułów, a następnie cyberprzestępcy przechodzili do dalszego etapu operacji.

W uaktualnionym łańcuchu infekcji wykonanie szkodnika PowerShower zostaje przesunięte w czasie do późniejszego etapu. Zamiast tego, zaraz po początkowej infekcji na atakowaną maszynę zostaje pobrana i wykonana szkodliwa aplikacja HTML. Następnie aplikacja ta zbiera wstępne informacje dotyczące zaatakowanego komputera, jak również pobiera i wykonuje VBShower kolejny szkodliwy moduł. VBShower usuwa ślady obecności szkodnika w systemie i za pomocą serwerów kontroli kontaktuje się z osobami, które stoją za operacją, w celu podjęcia decyzji odnośnie dalszych działań. W zależności od otrzymanego polecenia szkodnik pobiera, a następnie wykonuje oprogramowanie PowerShower lub inne szkodliwe oprogramowanie znajdujące się w arsenale grupy Cloud Atlas.

Nowy łańcuch infekcji jest znacznie bardziej skomplikowany niż poprzedni model, jednak główna różnica polega na tym, że szkodliwa aplikacja HTML oraz moduł VBShower są polimorficzne. To oznacza, że kod w obu modułach będzie nowy i unikatowy w każdym przypadku infekcji. Według ekspertów z firmy Kaspersky uaktualniona wersja ma na celu ukrycie szkodliwego oprogramowania przed rozwiązaniami zabezpieczającymi wykorzystującymi do ochrony jedynie znane wskaźniki infekcji.

Jedną z dobrych praktyk w społeczności związanej z cyberbezpieczeństwem jest udostępnianie zidentyfikowanych wskaźników infekcji dotyczących szkodliwych operacji. Dzięki temu możemy dość szybko reagować na bieżące międzynarodowe operacje cyberszpiegowskie, zapobiegając ewentualnym dalszym szkodom. Jednak, jak przewidywaliśmy już w 2016 r., wskaźniki infekcji przestały być niezawodnym narzędziem identyfikowania ataku ukierunkowanego w sieci. Po raz pierwszy stało się to jasne w przypadku ProjectSauron, który tworzył unikatowy zestaw wskaźników infekcji dla każdej ze swoich ofiar oraz korzystał z narzędzi typu open source w operacjach szpiegowskich. Kontynuacją tego trendu jest opisywany,

zidentyfikowany niedawno przykład szkodliwego oprogramowania polimorficznego. Nie znaczy to, że trudniej jest schwytać takich cyberprzestępców, wskazuje natomiast na konieczność rozwoju umiejętności i narzędzi wykorzystywanych do ochrony przed cyberzagrożeniami, tak jak ma to miejsce w przypadku umiejętności i narzędzi cyberprzestępców powiedział Felix Aime, badacz ds. cyberbezpieczeństwa w firmie Kaspersky.

Eksperci z firmy Kaspersky zalecają, aby organizacje wykorzystywały rozwiązania zabezpieczające przed atakami ukierunkowanymi udoskonalone o wskaźniki ataków, które uwzględniają w szczególności taktyki, techniki oraz działania, jakie mogą zastosować cyberprzestępcy podczas przygotowywania się do ataku. Wskaźniki ataków pozwalają namierzyć wykorzystywane techniki niezależnie od tego, jakie konkretne narzędzia są stosowane. Najnowsze wersje rozwiązań Kaspersky Endpoint Detection and Response oraz Kaspersky Anti Targeted Attack zawierają nową bazę wskaźników ataków, prowadzoną i aktualizowaną przez własnych ekspertów firmy Kaspersky zajmujących się wyszukiwaniem zagrożeń. Produkty te oferują również nowe funkcje, które upraszczają proces prowadzenia prac dochodzeniowych oraz udoskonalają wyszukiwanie zagrożeń.

Więcej informacji na temat nowej aktywności cybergangu Cloud Atlas znajduje się na stronie https://r.kaspersky.pl/3JuhJ.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 12/08/19 13:51, odsłony: 66