SneakyPastes: operacja ugrupowania Gaza

ID artykułu: 57248 / 2264

URL: http://www.publikuj.org/57248

W 2018 roku ugrupowanie przestępcze Gaza, o którym obecnie wiadomo, że składa się z kilku grup różniących się stopniem zaawansowania, przeprowadziło operację cyberszpiegostwa, której cel stanowiły osoby oraz organizacje związane z kwestią polityczną regionu Bliskiego Wschodu.

W kampanii, określanej jako SneakyPastes, wykorzystano jednorazowe adresy e-mail w celu rozprzestrzeniania infekcji za pośrednictwem phishingu, a następnie instalowano szkodliwe oprogramowanie z wykorzystaniem różnych darmowych stron. Dzięki takiemu niewymagającemu znacznych nakładów finansowych, a jednocześnie skutecznemu podejściu ugrupowanie zdołało zaatakować około 240 ofiar w 39 krajach, wśród których znalazły się między innymi znane organizacje polityczne, dyplomatyczne, działające w branży mediów oraz aktywistyczne. Wyniki badania Kaspersky Lab zostały przekazane organom ścigania i przyczyniły się do zlikwidowania znacznej części infrastruktury wykorzystywanej do przeprowadzania ataków.

Cybergang Gaza to arabskojęzyczne, motywowane względami politycznymi ugrupowanie złożone z powiązanych ze sobą organizacji przestępczych, aktywnie atakujących cele na Bliskim Wschodzie oraz w Afryce Północnej, w szczególności na Terytoriach Palestyńskich. W ramach tego gangu Kaspersky Lab zidentyfikował co najmniej trzy grupy o podobnych intencjach i celach ataków (cyberszpiegostwo związane z interesami politycznymi na Bliskim Wschodzie), ale odmiennych narzędziach, technikach oraz poziomach zaawansowania. W pewnym stopniu operacje poszczególnych grup nakładają się na siebie.

Operation Parliament oraz Desert Falcons stanowią bardziej zaawansowane grupy, znane odpowiednio od 2018 i 2015 r. Natomiast o działaniu mniej złożonej grupy, MoleRats, wiadomo było już od co najmniej 2012 r. Wiosną 2018 roku grupa ta rozpoczęła operację SneakyPastes.

Kampania SneakyPastes rozpoczęła się od ataków phishingowych związanych tematycznie z polityką, w których wiadomości były rozprzestrzeniane przy użyciu adresów e-mail i domen jednorazowego użytku. W wyniku kliknięcia szkodliwego odsyłacza lub pobrania załącznika na urządzeniu ofiary instalowało się szkodliwe oprogramowanie.

W celu uniknięcia wykrycia oraz ukrycia lokalizacji serwera kontroli na urządzenia ofiar pobierane było dodatkowe szkodliwe oprogramowanie z wykorzystaniem licznych darmowych stron, w tym Pastebin oraz Github. Różne szkodliwe implanty wykorzystywały szereg mechanizmów w celu zapewniania odporności i długotrwałej obecności szkodnika w zainfekowanych systemach. Ostatni etap ataku stanowił trojan umożliwiający zdalny dostęp, który kontaktował się z serwerem kontroli, a następnie gromadził, kompresował, szyfrował oraz wysyłał do przestępców różnego rodzaju skradzione dokumenty oraz arkusze.

Badacze z Kaspersky Lab współpracowali z organami ścigania w celu wykrycia pełnego cyklu ataku oraz włamania dotyczącego operacji SneakyPastes. Wysiłki te zaowocowały nie tylko dogłębnym poznaniem stosowanych narzędzi, technik oraz celów ataków, ale również zlikwidowaniem znaczącej części infrastruktury omawianego cyberugrupowania.

Operacja SneakyPastes była prowadzona najintensywniej w okresie od kwietnia do połowy listopada 2018 r., koncentrując się na niewielkiej liczbie celów, które stanowiły placówki dyplomatyczne oraz rządowe, organizacje pozarządowe oraz związane z branżą mediów. Przy użyciu telemetrii Kaspersky Lab oraz innych źródeł ustalono, że istnieje około 240 ofiar, obejmujących zarówno znane osoby, jak i organizacje z 39 krajów na całym świecie zlokalizowanych głównie na Terytoriach Palestyńskich, w Jordanii, Izraelu oraz w Libanie. Wśród ofiar znalazły się ambasady, podmioty rządowe, organizacje z branży mediów oraz dziennikarze, aktywiści, partie polityczne oraz osoby fizyczne, jak również organizacje edukacyjne, bankowe czy związane

z opieką zdrowotną.

Wykrycie Desert Falcons w 2015 r. stanowiło punkt zwrotny w krajobrazie zagrożeń, ponieważ było to pierwsze znane wówczas arabskojęzyczne ugrupowanie cyberprzestępcze. Teraz wiemy, że jego rodzic, gang Gaza, aktywnie atakował osoby i organizacje związane z interesami bliskowschodnimi od 2012 r., początkowo polegając głównie na działaniach stosunkowo mało zaawansowanej, ale nieugiętej grupy tej samej, która w 2018 roku przeprowadziła operację SneakyPastes. Jest ona dowodem na to, że brak infrastruktury czy zaawansowanych narzędzi nie stanowi przeszkody w osiągnięciu sukcesu. Spodziewamy się, że szkody wyrządzone przez wszystkie trzy grupy gangu Gaza wzrosną, a ataki rozszerzą się na inne regiony związane z kwestią palestyńską powiedział Amin Hasbini, szef centrum badań dot. Bliskiego Wschodu, Globalny Zespół ds. Badań i Analiz (GReAT), Kaspersky Lab.

Wszystkie produkty firmy Kaspersky Lab skutecznie wykrywają i blokują omawiane zagrożenie.

Aby nie paść ofiarą ataku ukierunkowanego znanego lub nieznanego cyberugrupowania, badacze z Kaspersky Lab zalecają stosowanie następujących środków bezpieczeństwa:

Korzystaj z zaawansowanych narzędzi zabezpieczających, takich jak Kaspersky Anti Targeted Attack Platform (KATA), i zadbaj o to, aby zespół ds. bezpieczeństwa posiadał dostęp do najnowszych danych analitycznych dot. cyberzagrożeń.

Dopilnuj, aby wszystkie programy w organizacji były regularnie aktualizowane, szczególnie gdy zostanie udostępniona nowa łata bezpieczeństwa. W automatyzacji tych procesów pomocne mogą być produkty zabezpieczające oferujące funkcje oceny luk w zabezpieczeniach oraz zarządzania łatami.

Aby zapewnić skuteczną ochronę przed znanymi i nieznanymi zagrożeniami, w tym exploitami dnia zerowego, wybierz sprawdzone rozwiązanie zabezpieczające, takie jak Kaspersky Endpoint Security, które jest wyposażone w funkcje wykrywania oparte na analizie zachowania.

Zadbaj o to, aby personel posiadał podstawową znajomość higieny związanej z cyberbezpieczeństwem, ponieważ wiele ataków ukierunkowanych rozpoczyna się od prostego phishingu lub zastosowania innej metody socjotechnicznej.

Raport dotyczący operacji SneakyPastes cyberugrupowania Gaza znajduje się na stronie https://r.kaspersky.pl/6yqVi.

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

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie http://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: 11/04/19 10:58, odsłony: 68