Zaawansowane cyberzagrożenia w II kwartale 2019 r

ID artykułu: 58161 / 2264

URL: http://www.publikuj.org/58161

W drugim kwartale 2019 r. aktywność związana z zaawansowanymi długotrwałymi cyberzagrożeniami (APT) obejmowała wiele operacji wymierzonych w cele na Bliskim Wschodzie lub w Korei Południowej, jak również ataki przeprowadzane z tamtych regionów. Chociaż celem sporej części tych działań było cyberszpiegostwo lub zysk finansowy, wydaje się, że co najmniej jedna kampania została przeprowadzona z zamiarem szerzenia dezinformacji. W maju badacze z firmy Kaspersky przeanalizowali należące do irańskiego podmiotu zasoby cyberszpiegowskie, które wyciekły do internetu, i doszli do wniosku, że za wyciek ten może odpowiadać Hades, ugrupowanie powiązane z kampanią ExPetr oraz cyberatakiem na infrastrukturę Zimowych Igrzysk Olimpijskich w Pjongczangu. W drugim kwartale 2019 r. badacze z firmy Kaspersky zaobserwowali interesującą aktywność na Bliskim Wschodzie. Obejmowała ona serię wycieków online dotyczących takich zasobów jak kod, infrastruktura, dane ugrupowania oraz ofiar, które rzekomo należały do znanych perskojęzycznych cybergangów OilRig oraz MuddyWater. Wycieki pochodziły z różnych źródeł, wszystkie jednak pojawiły się w odstępie kilku tygodni. W ramach trzeciego wycieku do internetu, który rzekomo ujawniał informacje związane z podmiotem o nazwie RANA institute, materiał w języku perskim pojawił się na stronie o nazwie Hidden Reality. Analizując materiały, infrastrukturę oraz wykorzystaną stronę internetową, badacze z firmy Kaspersky doszli do wniosku, że z wyciekiem tym może być powiązane cyberugrupowanie Hades. Grupa ta stoi za incydentem OlympicDestroyer podczas Zimowych Igrzysk Olimpijskich w Pjongczangu, jak również robakiem ExPetr oraz różnymi kampaniami, których celem była dezinformacja, takimi jak wyciek e-maili dotyczących kampanii prezydenckiej Emmanuela Macrona we Francji w 2017 r.

Pozostałe kluczowe wydarzenia związane z aktywnością APT w II kwartale 2019 r.:

Rosyjskoj ęzyczne ugrupowania nieustannie udoskonalają dotychczasowe oraz tworzą nowe narzędzia, jak również przeprowadzają nowe operacje. Na przykład od marca gang Zebrocy wydaje się kierować swoją uwagę ku pakistańskim/indyjskim wydarzeniom, urzędnikom, dyplomatom i wojskowym, utrzymując jednocześnie stały dostęp do lokalnych i odległych sieci rządowych w Azji Środkowej. Ataki ugrupowania Turla nadal charakteryzowały się wykorzystywaniem szybko ewoluującego zestawu narzędzi, a w jednym przypadku przypuszcza się, że grupa ta uprowadziła infrastrukturę należącą do OilRig.

Odnotowan o wysoki stopień aktywności związanej z Koreą, podczas gdy w pozostałej części Azji Południowo-Wschodniej panował większy spokój w porównaniu z wcześniejszymi kwartałami. Operacje, które zasługują na uwagę, to atak przeprowadzony przez ugrupowanie Lazarus na firmę z branży gier mobilnych w Korei Południowej oraz kampania przeprowadzona przez BlueNoroff, podgrupę gangu Lazarus, której celem był bank zlokalizowany w Bangladeszu.

Badacze zaobserwowali również aktywną kampanię wymierzoną w podmioty rządowe w Azji Środkowej, która została przeprowadzona przez rosyjskojęzyczne ugrupowanie APT SixLittleMonkeys z wykorzystaniem nowej wersji trojana Microcin oraz, na ostatnim etapie, narzędzia zdalnej administracji, któremu firma Kaspersky nadała nazwę HawkEye.

Drugi kwartał 2019 r. pokazuje, jak mglisty i zwodniczy stał się obecnie krajobraz zagrożeń i jak często rzeczywistość okazuje się zupełnie inna, niż wydawała się wcześniej. Przykładem może być ugrupowanie cyberprzestępcze, które porwało infrastrukturę mniejszego gangu, oraz grupa, która prawdopodobnie wykorzystała serię wycieków do internetu w celu szerzenia dezinformacji oraz podważenia wiarygodności ujawnionych zasobów. Branża bezpieczeństwa mierzy się z coraz bardziej złożonym zadaniem demaskowania pozorów w celu dotarcia do faktów i danych analitycznych dot. zagrożeń, na których opiera się cyberbezpieczeństwo. Jak zawsze warto dodać, że nie posiadamy pełnego obrazu i pewne aktywności mogły nam umknąć lub nie zostały przez nas w pełni zrozumiane powiedział Vicente Diaz, główny badacz ds.

cyberbezpieczeństwa z firmy Kaspersky.

Raport dotyczący trendów APT w II kwartale podsumowuje wyniki przedstawione w raportach opartych na analizie zagrożeń dostępnych wyłącznie dla subskrybentów specjalnej usługi firmy Kaspersky, które obejmują również wskaźniki infekcji (IoC) oraz reguły YARA mogące pomóc w informatyce śledczej oraz wyszukiwaniu szkodliwego oprogramowania. Więcej informacji na ten temat można uzyskać pod adresem intelreports@kaspersky.com .

Pełny raport dotyczący trendów związanych z zaawansowanymi cyberzagrożeniami w II kwartale 2019 r. jest dostępny na stronie https://r.kaspersky.pl/b8RNR.

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: 02/08/19 11:26, odsłony: 75