**NetTraveler wraca z nowymi sztuczkami**

**Firma Kaspersky Lab zidentyfikowała nowe ataki przeprowadzane w ramach cyberszpiegowskiej kampanii NetTraveler (znanej również jako „Travnet”, „Netfile” oraz „Red Star”) stanowiącej zaawansowane, długotrwałe zagrożenie, które zainfekowało już setki ofiar wysokiego szczebla w ponad 40 państwach.**

Znane cele NetTravelera obejmują aktywistów tybetańskich/ujgurskich, firmy z branży naftowej, centra i instytucje naukowo-badawcze, uniwersytety, prywatne firmy, rządy i instytucje rządowe, ambasady oraz firmy współpracujące z wojskiem.

Natychmiast po [publicznym ujawnieniu operacji NetTraveler](http://securelist.pl/blog/7224%2Cnettraveler_is_running_ukierunkowane_ataki_na_ofiary_wysokiego_szczebla.html) w czerwcu 2013 r. cyberprzestępcy zamknęli wszystkie znane centra kontroli i przenieśli je na nowe serwery w Chinach, Hong Kongu i Tajwanie. Co więcej, jak pokazuje najnowszy incydent, ataki były kontynuowane bez przeszkód.

W ciągu ostatnich dni eksperci z Kaspersky Lab odnotowali kilka e-maili wysłanych licznym aktywistom ujgurskim. Do dystrybucji nowej wersji NetTravelera cyberprzestępcy wykorzystują lukę w Javie, która została załatana całkiem niedawno – w czerwcu 2013 r. Wariant ten jest znacznie skuteczniejszy od swojego poprzednika, który wykorzystywał załataną w kwietniu 2013 r. lukę w pakiecie Microsoft Office.

Oprócz wykorzystywania phishingowych wiadomości e-mail, cyberprzestępcy zastosowali technikę „watering hole” (przekierowania sieciowe i ataki drive-by download na sfałszowanych domenach) w celu infekowania ofiar surfujących po internecie.

W ciągu minionego miesiąca specjaliści z Kaspersky Lab przechwycili i zablokowali wiele prób infekcji z domeny “wetstock[dot]org”, która jest powiązana z poprzednimi atakami NetTravelera. Przekierowania te wydają się pochodzić ze stron związanych z aktywistami ujgurskimi, które zostały zainfekowane przez osoby odpowiedzialne za NetTravelera.

Eksperci z Globalnego Zespołu ds. Badań i Analiz (GReAT) z Kaspersky Lab przewidują, że osoby odpowiedzialne za NetTravelera mogą wkrótce zastosować kolejne metody infekowania swoich ofiar i przedstawiają zalecenia pozwalające zabezpieczyć się przed tego typu działaniami cyberprzestępczymi:

Uaktualnij Javę do najnowszej wersji lub, jeżeli nie używasz Javy, odinstaluj ją.

Uaktualnij Microsoft Windows i pakiet Office do najnowszych wersji.

Uaktualnij oprogramowanie osób trzecich, takie jak Adobe Reader.

Korzystaj z bezpiecznej przeglądarki, takiej jak Google Chrome, która posiada szybszy cykl rozwoju i publikacji łat niż domyślna w systemie Windows przeglądarka Internet Explorer.

Bądź ostrożny, klikając odsyłacze i otwierając załączniki od nieznanych osób.

*„W przypadku grupy stojącej za NetTravelerem nie zaobserwowaliśmy jeszcze wykorzystania luk, dla których nie istnieją łaty (zero-day). Kampania ta jest jednak aktywna, a cyberprzestępcy ciągle rozwijają swoją platformę i dlatego będziemy uważnie przyglądać się ich ruchom”* – powiedział Costin Raiu, dyrektor Globalnego zespołu ds. badań i analiz (GReAT), Kaspersky Lab.

Więcej informacji na temat nowego ataku z udziałem NetTravelera pojawi się już wkrótce w serwisie SecureList.pl prowadzonym przez Kaspersky Lab.

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/news>.