**Kaspersky Lab analizuje aktywną kampanię cyberszpiegowską wycelowaną głównie w organizacje z Korei Południowej**

**Kaspersky Lab informuje o przeprowadzeniu analizy aktywnej kampanii cyberszpiegowskiej Kimsuky, wycelowanej przede wszystkim w organizacje z Korei Południowej. Działania wykonywane przez cyberprzestępców w ramach kampanii są precyzyjnie wyselekcjonowane i ściśle ukierunkowane.**

Analiza techniczna wykazała, że cyberprzestępcy byli zainteresowani atakowaniem jedenastu organizacji z Korei Południowej oraz dwóch z Chin, łącznie z Sejong Institute, Korea Institute For Defense Analyses (KIDA), Ministerstwem Zjednoczenia Korei Południowej, Hyundai Merchant Marine oraz grupami popierającymi zjednoczenie Korei.

Najstarsze ślady aktywności tego zagrożenia są datowane na 3 kwietnia 2013 r., a pierwsze próbki trojana Kimsuky pojawiły się 5 maja br. Szkodnik ten to niespecjalnie zaawansowany program szpiegowski, zawierający kilka podstawowych błędów w kodowaniu. Komunikacja z zainfekowanymi komputerami odbywa się za pośrednictwem konta założonego na serwerach bułgarskiego dostawcy bezpłatnych usług pocztowych (mail.bg).

Pierwotne mechanizmy dostarczania szkodliwego programu pozostają nieznane, jednak badacze z Kaspersky Lab twierdzą, że Kimsuky najprawdopodobniej infekował komputery poprzez ukierunkowane wiadomości spamowe (tzw. spear-phishing). Po udanej infekcji szkodnik może wykonywać następujące operacje: przechwytywanie znaków wprowadzanych z klawiatury, gromadzenie informacji o zawartości wybranych folderów, zezwalanie na zdalny dostęp oraz kradzież dokumentów HWP, pochodzących z południowokoreańskiego edytora tekstu wykorzystywanego wyłącznie przez rząd (pakiet Hancom Office). Atakujący użyli także zmodyfikowanej wersji aplikacji TeamViewer pozwalającej na uzyskiwanie zdalnego dostępu do komputerów.

Do kradzieży plików HWP trojan Kimsuky wykorzystuje specjalnie przygotowany szkodliwy program, co sugeruje, że dokumenty te należą do jednego z podstawowych celów grupy cyberprzestępczej.

Ślady wykryte przez ekspertów z Kaspersky Lab pozwalają na domniemywanie północnokoreańskiego pochodzenia atakujących. Po pierwsze, cele ataków mówią same za siebie – należą do nich uniwersytety z Korei Południowej prowadzące badania z dziedziny stosunków międzynarodowych i tworzące polityki obrony dla rządu, narodowa firma przewozowa oraz grupy popierające zjednoczenie Korei. Po drugie, badacze z Kaspersky Lab wykryli w kodzie szkodnika koreańskie słowa (można je przetłumaczyć jako „atak” oraz „wykonanie”). I wreszcie, dwa adresy, na które zainfekowane maszyny mają wysyłać skradzione informacje - iop110112@hotmail.com oraz rsh1213@hotmail.com – zostały zarejestrowane z następującymi nazwami: “kimsukyang” oraz “Kim asdfa”. Mimo że sama nazwa nie jest twardym dowodem na pochodzenie atakujących, ich źródłowe adresy IP wydają się to potwierdzać – wszystkie znajdują się w pulach charakterystycznych dla chińskiego segmentu internetu. Działający w tym regionie dostawcy internetu świadczą swoje usługi także w Korei Północnej.

Kolejną interesującą „geopolityczną” cechą trojana Kimsuky jest to, że po instalacji wyłącza on tylko jeden produkt antywirusowy, tworzony przez AhnLab – południowokoreańską firmę z branży bezpieczeństwa IT.

Produkty Kaspersky Lab neutralizują trojana Kimsuky – jest on wykrywany jako Trojan.Win32.Kimsuky. Zmodyfikowana wersja aplikacji TeamViewer jest wykrywana jako Trojan.Win32.Patched.ps.

Więcej informacji na temat kampanii cyberszpiegowskiej Kimsuky znajdzie się już wkrótce w serwisie [SecureList.pl](http://www.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>.