**Kaspersky Lab wykrywa „The Mask”: jedną z najbardziej zaawansowanych, globalnych operacji cyberszpiegowskich w historii**

**Eksperci z Kaspersky Lab wykryli „The Mask” (inna nazwa: Careto) - zaawansowane hiszpańskojęzyczne szkodliwe oprogramowanie, zaangażowane w globalne operacje cyberszpiegowskie, które istnieje co najmniej od 2007 roku.**

The Mask wyróżnia się złożonością zestawu narzędzi wykorzystywanych przez atakujących. Obejmuje niezwykle wyrafinowane szkodliwe oprogramowanie, rootkita, bootkita, wersje dla systemu OS X oraz Linux i prawdopodobnie wersje dla Androida oraz iOS (iPad/iPhone). Ofiary operacji „The Mask” zlokalizowano w państwach na cały świecie, w tym w Polsce.

Na celowniku „Maski” znajdują się przede wszystkim instytucje rządowe, placówki dyplomatyczne i ambasady, firmy z branży energetycznej, organizacje badawcze oraz aktywiści. Ofiary tego ataku ukierunkowanego zostały zidentyfikowane w 31 firmach zlokalizowanych na całym świecie – od Bliskiego Wschodu i Europy po Afrykę i Ameryki.

Głównym celem osób atakujących jest gromadzenie poufnych danych z zainfekowanych systemów. Obejmują one oficjalne dokumenty, jak również różne klucze szyfrowania, konfiguracje VPN, klucze SSH (służące do identyfikacji użytkownika na serwerze SSH) oraz pliki RDP (wykorzystywane podczas korzystania ze zdalnego pulpitu).

„Kilka rzeczy sugeruje, że możemy mieć do czynienia z kolejną kampanią sponsorowaną przez państwo. Po pierwsze, procedury operacyjne stojącej za tym atakiem grupy cechuje bardzo wysoki poziom profesjonalizmu. Od zarządzania infrastrukturą, zamykania operacji, ukrywania się po reguły dostępu i czyszczenie zamiast usuwania plików dziennika zdarzeń. To wszystko sprawia, że omawiany atak wyprzedza [Duqu](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=1600) pod względem wyrafinowania, stanowiąc obecnie jedno z najbardziej zaawansowanych znanych zagrożeń” – powiedział **Costin Raiu**, dyrektor Globalnego Zespołu ds. Badań i Analiz (ang. GReAT) z Kaspersky Lab. „Ten poziom bezpieczeństwa operacyjnego nie jest zwykle spotykany w przypadku grup cybernetycznych” – dodał ekspert.

Badacze z Kaspersky Lab wpadli na trop Careto w zeszłym roku, gdy zaobserwowali próby wykorzystania załatanej pięć lat temu luki w zabezpieczeniach produktów firmy. Exploit zapewniał szkodliwemu oprogramowaniu możliwość uniknięcia wykrycia. Naturalnie, sytuacja ta wzbudziła zainteresowanie ekspertów i w ten sposób rozpoczęto dochodzenie.

Infekcja Careto może mieć katastrofalne skutki dla ofiar. Careto przechwytuje wszystkie kanały komunikacji i zbiera najistotniejsze informacje z maszyny ofiary. Z uwagi na funkcje ukrywania się, wbudowane możliwości i dodatkowe moduły cyberszpiegowskie wykrycie tego szkodnika jest niezwykle trudne.

**Główne ustalenia z dochodzenia ekspertów z Kaspersky Lab**

Autorzy wydają się posługiwać hiszpańskim jak swoim językiem ojczystym, co stanowi rzadkość w przypadku tego typu ataków.

Do stycznia 2014 r. kampania prowadzona była już przez co najmniej pięć lat (niektóre próbki Careto zostały skompilowane w 2007 r.). Podczas dochodzenia prowadzonego przez Kaspersky Lab zamknięto serwery kontroli (C&C) wykorzystywane przez atakujących.

Doliczono się ponad 380 unikatowych ofiar. Infekcje zostały zidentyfikowane w: Algierii, Argentynie, Belgii, Boliwii, Brazylii, Chinach, Kolumbii, na Kostaryce, Kubie, w Egipcie, we Francji, w Niemczech, na Gibraltarze, w Gwatemali, Iranie, Iraku, Libii, Malezji, Meksyku, Maroku, Norwegii, Pakistanie, Polsce, Afryce Południowej, Hiszpanii, Szwajcarii, Tunezji, Turcji, Wielkiej Brytanii, Stanach Zjednoczonych oraz Wenezueli.

O specjalnym charakterze omawianej operacji cyberszpiegowskiej świadczy złożoność i uniwersalność zestawu narzędzi, jakimi posługiwały się osoby atakujące. Należy tu wymienić wykorzystywanie zaawansowanych exploitów, niezwykle wyrafinowane szkodliwe oprogramowanie, rootkita, bootkita, wersje dla systemów OS X oraz Linux i prawdopodobnie wersje dla Androida oraz iPad/iPhone (iOS). W ramach operacji „The Mask” przeprowadzano również ukierunkowany atak na produkty firmy Kaspersky Lab.

Pod względem wektorów ataku wykorzystano przynajmniej jeden exploit dla Adobe Flash Playera (CVE-2012-0773), który powstał dla tej aplikacji w wersjach starszych niż 10.3 i 11.2. Exploit ten został pierwotnie wykryty przez VUPEN i wykorzystany w 2012 r. do obejścia piaskownicy w przeglądarce Google Chrome w celu wygrania konkurencji Pwn2Own (CanSecWest).

**Metody infekcji i funkcjonalność „Maski”**

Jak wynika z raportu analitycznego firmy Kaspersky Lab, w kampanii „The Mask” wykorzystywane są ukierunkowane e-maile phishingowe zawierające odsyłacze do szkodliwych stron internetowych. Zainfekowana witryna zawiera różne exploity, których celem jest zainfekowanie osoby odwiedzającej w zależności od konfiguracji systemu. Po skutecznej infekcji szkodliwa strona przekierowuje użytkownika do nieszkodliwego zasobu wskazanego w e-mailu, np. filmu w serwisie YouTube lub portalu informacyjnego.

Należy podkreślić, że strony zawierające exploity nie infekują automatycznie osób, które je odwiedzają; zamiast tego, atakujący umieszczają exploity w specjalnych folderach na stronie internetowej, do których bezpośrednie odnośniki znajdują się tylko w szkodliwych wiadomościach e-mail. Niekiedy agresorzy wykorzystują subdomeny na stronach zawierających exploity, aby dodać im większej wiarygodności. Subdomeny te przypominają podsekcje najpopularniejszych gazet w Hiszpanii, jak również kilku międzynarodowych tytułów, takich jak „The Guardian" i „Washington Post".

Omawiany szkodliwy program przechwytuje wszystkie kanały komunikacji i gromadzi najważniejsze informacje z zainfekowanego systemu. Jego wykrycie jest niezwykle trudne ze względu na zaawansowane funkcje ukrywania się. ”Maska” to wysoce modułowy system; obsługuje wtyczki i pliki konfiguracyjne, które umożliwiają wykonanie wielu funkcji. Niezależnie od wbudowanej funkcjonalności operatorzy Careto mogli również udostępnić dodatkowe moduły mogące wykonać dowolne szkodliwe zadanie.

Produkty firmy Kaspersky Lab wykrywają i usuwają wszystkie znane wersje szkodliwego oprogramowania The Mask/Careto.

Więcej szczegółów technicznych dotyczących wykrytej kampanii cyberszpiegowskiej pojawi się już wkrótce w serwisie [SecureList.pl](http://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>.