OPERACJA CEPHEUS

Data publikacji 29.11.2019

Polska Policja wzięła udział w międzynarodowej operacji wymierzonej przeciwko sprzedawcom i użytkownikom oprogramowania IM-RAT, które zapewniało całkowitą kontrolę nad komputerem ofiary. Dochodzenie prowadzone było przez australijską policję federalną (AFP), przy współpracy międzynarodowej koordynowanej przez Europol i Eurojust. W operacji udział wzięły organy ścigania z kilkunastu krajów w Europie, Kolumbii i Australii.

Imminent Monitor Remote Access Trojan (IM-RAT) to specjalne oprogramowanie, które pozwalało cyberprzestępcom na całkowite przejęcie kontorli nad komputerem ofiary. Ten trojan używany był w 124 krajach i sprzedany został 14,5 tys. użytkownikom. Dzięki skoordynowanym przez Europol i Eurojust międzynarodowym działaniom IM-RAT jest już bezużyteczny.

Pierwsze nakazy przeszukania zostały wydane i zrealizowane w Australii i Belgii w czerwcu 2019 r. Dotyczyły dewelopera i pracownika IM-RAT. W dalszej kolejności działania zostały rozszerzone i w listopadzie przeprowadzono międzynarodowy tydzień działań, w wyniku których usunięto stronę Imminent Monitor.

Na terenie Polski w dniach 25-29 listopada br. w operacji CEPHEUS wzięło udział 139 funkcjonariuszy. W wyniku działań policjanci przeszukali 42 miejsca, przesłuchali 56 osób i zabezpieczyli 176 nośników.

Potężne narzędzie do przejmowania kontroli nad komputerem

RAT to podstępne oprogramowanie, które po zainstalowaniu pozostaje niezauważalne i daje cyberprzestępcom całkowitą swobodę w działaniach na komputerze ofiary. Hakerzy byli w stanie wyłączyć oprogramowanie antywirusowe i anty-malware. Mogli rejestrować naciśnięcia klawiszy, kraść dane, loginy i hasła oraz obserwować ofiary za pomocą kamer internetowych. Wszystko to działo się bez wiedzy właściciela komputera.

Ze względu na jego cechy, łatwość użycia i niski koszt RAT został uznany za poważne zagrożenie i niebezpieczne oprogramowanie. Każdy, kto miał skłonności do szpiegowania ofiar lub chciał skraść dane osobowe, mógł to zrobić za jedyne 25 USD. Szacuje się, że liczbę ofiar sięga dziesiątek tysięcy, a śledczy zidentyfikowali już część skradzionych danych osobowych, haseł, prywatnych zdjęć, materiałów wideo i danych. Trwa analiza kryminalistyczna znacznej liczby zabezpieczonych komputerów i kont internetowych.

Steven Wilson, szef Europoean Cybercrime Center (EC3), powiedział: „Żyjemy teraz w świecie, w którym za zaledwie 25 USD cyberprzestępca może z drugiego końca świata za pomocą jednego kliknięcia myszy uzyskać dostęp do twoich danych osobowych lub zdjęć bliskich, a nawet cię szpiegować. Globalna współpraca w zakresie egzekwowania prawa, którą widzieliśmy w tej sprawie, jest integralną częścią walki z grupami przestępczymi, które opracowują takie narzędzia. Ważne jest również, aby pamiętać, że niektóre podstawowe kroki mogą zapobiec temu, by nie stać się ofiarą takiego oprogramowania szpiegującego: w dalszym ciągu zachęcamy społeczeństwo do zapewnienia aktualności systemów operacyjnych i oprogramowania zabezpieczającego ”.

Daniela Buruiana, przedstawiciel krajowy Rumunii w Eurojust i przewodnicząca zespołu ds. Cyberprzestępczości, powiedziała: „Cyberprzestępcy sprzedający i wykorzystujący IM-RAT mieli wpływ na komputery dziesiątek tysięcy ofiar na całym świecie. Chcielibyśmy podziękować wszystkim zaangażowanym organom sądowym i organom ścigania za doskonałe wyniki osiągnięte w tej operacji. Organy te wykazały niezwykle wysoki poziom zaangażowania oraz wiedzę prawną i techniczną. Ze względu na skalę globalną i techniczne wyrafinowanie tego rodzaju przestępstw, skuteczna współpraca i koordynacja między wszystkimi odpowiednimi podmiotami ma zasadnicze znaczenie w pokonywaniu przeszkód w prowadzonych dochodzeniach”.

Jak uniknąć zainfekowania RAT

Osoby prywatne i firmy mogą w kilku prostych krokach chronić się przed takim złośliwym oprogramowaniem:

- aktualizuj oprogramowanie, w tym oprogramowanie antywirusowe;
- zainstaluj dobrą zaporę ogniową;
- nie otwieraj podejrzanych załączników lub adresów e-mail - nawet jeśli pochodzą od osób z Twojej listy kontaktów;
- twórz silne hasła.

Aby uzyskać więcej porad na temat zapobiegania, jak chronić się przed trojanami zdalnego dostępu, zapoznaj się z poradami Europolu dotyczącymi zapobiegania przestępczości.

(Biuro do Walki z Cyberprzestępczością / dm)

Aby obejrzeć film włącz obsługę JavaScript w swojej przelądarce.

Pobierz plik (format mp4 - rozmiar 18.12 MB)

PLIKI DO POBRANIA

Jak nie dać się zhakować i co zrobić jeśli padłeś ofiara hakera
467.85 KB