-Wspólne śledztwo w sprawie przestępstw w internecie zakończyło się trzema aresztowaniami; kolejne w toku
-Dane osobiste i finansowe zostały zagrożone w wyniku ogromnego cyberataku, który objął prawie 13 mln unikalnych adresów IP oraz 50 proc. firm z rankingu Fortune 1000
-Wstępne straty szacuje się na miliony dolarów

Jak donoszą firmy z branży zabezpieczeń **Defence Intelligence** oraz **Panda Security**, została zamknięta sieć botnet **Mariposa** - potężna sieć zainfekowanych komputerów stworzona do kradzieży informacji wrażliwych. Hiszpańskie organy ścigania zatrzymały trzy osoby podejrzane o zarządzanie tą siecią. Mariposa kradła informacje oraz dane dostępowe do kont w portalach społecznościowych i serwisach e-mail, bankowe dane uwierzytelniające oraz numery kart kredytowych. Botnet stale infiltrował osobiste, korporacyjne, rządowe oraz uniwersyteckie adresy IP w ponad 190 krajach. Botnet został zamknięty i zneutralizowany 23 grudnia 2009 roku dzięki wspólnym wysiłkom ekspertów w dziedzinie zabezpieczeń oraz organów ścigania, w tym firmy Panda Security, Defence Intelligence, FBI i hiszpańskiej Straży Obywatelskiej.

Obejmując ponad 13 milionach zainfekowanych komputerów Mariposa jest jednym z największych botnetów w historii. Christopher Davis, dyrektor generalny Defence Intelligence, który jako pierwszy odkrył botnet Mariposa wyjaśnia: „Łatwiej byłoby mi podać listę firm z rankingu Fortune 1000, których ochrona nie została naruszona, niż długą listę zagrożonych organizacji".

Po odkryciu sieci **Mariposa** w maju 2009 roku Defence Intelligence, Panda Security oraz Georgia Tech Information Security Center stanęły na czele Grupy Roboczej Mariposa, której celem była likwidacja botnetu i ujęcie przestępców przy współpracy innych ekspertów w zakresie bezpieczeństwa oraz międzynarodowych organów ścigania. Na początku tego miesiąca aresztowany został główny botmaster o pseudonimach „Netkairo" i „hamlet1917" oraz bezpośrednio współpracujący z nim operatorzy sieci „Ostiator" i „Johnyloleante".

Pedro Bustamante, starszy doradca naukowy w Panda Security, powiedział: „Z naszej wstępnej analizy wynika, że operatorzy botnetu nie posiadali zaawansowanych umiejętności hakerskich. To bardzo niepokojące, ponieważ świadczy o tym, jak wyspecjalizowane i skuteczne stało się oprogramowanie do rozpowszechniania złośliwych kodów, umożliwiając nawet niewykwalifikowanym cyberprzestępcom powodowanie ogromnych szkód i strat finansowych. Jesteśmy niezwykle dumni ze skoordynowanych wysiłków wszystkich członków Grupy Roboczej Mariposa oraz szybkości, z jaką udało nam się zneutralizować ten potężny botnet i ująć stojących za nim przestępców".

W zeszłym roku Grupa Robocza Mariposa przeniknęła do struktur sterowania i kontroli Mariposa w celu obserwowania kanałów komunikacji, z których korzystali podejrzani botmasterzy. Są to typowe kanały przekazujące sprawcom informacje z zarażonych komputerów, podobne do stosowanych w botnetach Zeus, Conficker i Koobface lub innych, wykrytych niedawno w wyniku operacji Google/Aurora. Po przeanalizowaniu głównych serwerów sterowania i kontroli Grupa Robocza mogła przeprowadzić skoordynowaną, globalną akcję zamknięcia botnetu Mariposa 23 grudnia. Aktualnie Panda Security prowadzi kompleksową analizę złośliwego oprogramowania oraz koordynuje międzynarodową wymianę informacji pomiędzy firmami antywirusowymi w celu zaktualizowania sygnatur.
Najważniejsze informacje ze wstępnej analizy Panda Security:

Po zainfekowaniu botem Mariposa administrator sieci instalował inne złośliwe oprogramowanie (m.in. zaawansowane programy typu keylogger przechwytujące wszystko, co jest wpisywane na klawiaturze, trojany bankowe takie jak Zeus, trojany zdalnego dostępu) w celu zdobycia dalszej kontroli na komputerami zombie.
Botmaster zarabiał na sprzedaży części botnetu, instalacji pasków narzędzi „pay-per-install", sprzedaży skradzionych danych uwierzytelniających do usług internetowych i wykorzystywaniu informacji bankowych oraz danych kart kredytowych do przeprowadzania transakcji przy pomocy zagranicznych „mułów pieniężnych".
Botnet Mariposa rozprzestrzeniał się niezwykle skutecznie poprzez sieci P2P, napędy USB i linki MSN.

Bardziej szczegółowy raport z ekspertyzy Panda Security będzie dostępny już wkrótce na stronie:

http://pandalabs.pandasecurity.com. Krótką charakterystykę oprogramowania botnetu Mariposa można znaleźć pod adresem: http://www.pandasecurity.com/homeusers/security-info/217587/ButterflyBot.A.

„Po raz kolejny skoordynowane wysiłki wielu organów ścigania na całym świecie oraz hiszpańskiej Straży Obywatelskiej przy współpracy z branżą zabezpieczeń internetowych umożliwiły walkę z globalnym zagrożeniem, jakim są cyberprzestępstwa", powiedział Juan Salom, inspektor Jednostki Straży Obywatelskiej ds. Przestępstw w internecie.

Dave Dagon z Georgia Tech Information Security Center mówi: „Zamiast rysować wykresy kołowe powinniśmy traktować botnety jako miejsca popełnienia przestępstwa, a nie tylko obiekty badań".

Grupa Robocza Mariposa oficjalnie przejęła kontrolę nad kanałami komunikacji wykorzystywanymi przez Mariposa, skutecznie odcinając twórcom botnetu dostęp do sieci. Prawdopodobnie w akcie zemsty wkrótce po zamknięciu botnetu w grudniu przeprowadzony został atak DDoS (ang. Distributed Denial of Service) na Defence Intelligence. Atak był na tyle silny, że jego skutki odczuł jeden z dużych operatorów internetowych, którego klienci stracili dostęp do internetu na kilkanaście godzin.

Przedstawiciel CDmon, operatora biorącego udział w śledztwie, na którego serwerach znajdowały się przestępcze domeny, mówi: „Cieszymy się, że mogliśmy wesprzeć tą międzynarodową operację, w której uczestniczyła hiszpańska Straż Obywatelska, Panda Security, Defence Intelligence i inne organy ścigania, oraz pomóc zlikwidować botnet. CDmon zależy na wysokiej jakości ofercie internetowej, gwarantującej wysoki poziom bezpieczeństwa wszystkich naszych usług. Ta wspólna akcja to wielkie zwycięstwo w walce z cyberprzestępczością".

studio PRowokacja