Zagrożenia internetowe i szkodliwa aktywność w Polsce, II kwartał 2014 r.

Autor:

Maciej Ziarek
Ekspert ds. bezpieczeństwa IT
Kaspersky Lab Polska sp. z o.o.

O raporcie

Niniejszy raport jest poświęcony zagrożeniom wykrywanym przez produkty Kaspersky Lab na terenie Polski. Wszystkie dane i statystyki zostały dostarczone przez Kaspersky Security Network (KSN). KSN integruje w produktach dla klientów indywidualnych i korporacyjnych technologię bazującą na chmurze i jest to obecnie jedna z najważniejszych technologii bezpieczeństwa firmy Kaspersky Lab.

KSN pomaga ekspertom z Kaspersky Lab w wykrywaniu zagrożeń w czasie rzeczywistym, kiedy nie istnieją jeszcze odpowiednie sygnatury i informacje heurystyczne. KSN pomaga zidentyfikować źródło rozprzestrzeniania się szkodliwego oprogramowania w internecie i blokuje dostęp użytkownika do niego. Dzięki błyskawicznej odpowiedzi na nowe zagrożenia, jesteśmy w stanie blokować nowe programy zanim uruchomią się na komputerach użytkowników, w kilka sekund po tym jak zostaną wykryte, a do tego bez uaktualniania bazy danych antywirusa.

Statystyki w tym raporcie bazują na całkowicie anonimowych danych, uzyskanych z produktów Kaspersky Lab zainstalowanych na komputerach użytkowników w Polsce i zostały zgromadzone za zgodą użytkowników. Żadne dane gromadzone w ramach KSN nie pozwalają na zidentyfikowanie konkretnych użytkowników – są to dane zdepersonalizowane. Informacje o spamie pochodzą dodatkowo z innych źródeł, niezwiązanych z użytkownikami produktów Kaspersky Lab.

Zagrożenia webowe

Ataki poprzez przeglądarkę są głównym sposobem rozprzestrzeniania szkodliwych programów. Poniższe metody były najczęściej używane przez cyberprzestępców do infiltracji systemów.

Wykorzystanie luk w przeglądarkach i wtyczkach (ataki drive-by download)

Do infekcji w ramach tego ataku dochodzi w momencie odwiedzenia zainfekowanej strony internetowej, bez jakiejkolwiek interakcji ze strony użytkownika i bez jego wiedzy. Ta metoda ataku jest numerem jeden, jeżeli chodzi o częstotliwość wykorzystania przez cyberprzestępców. Ochrona przed takimi zagrożeniami wymaga zastosowania rozwiązania typu Internet Security, które jest w stanie wykrywać zagrożenia w momencie rozpoczęcia pobierania niebezpiecznych obiektów.

Jedną z kluczowych technologii Kaspersky Lab pozwalających na walkę z tego typu zagrożeniami jest Automatyczne zapobieganie exploitom, zaprojektowane w celu wykrywania niebezpiecznych działań wykorzystujących luki w systemie operacyjnym i zainstalowanych aplikacjach.

Socjotechnika

Te ataki wymagają udziału użytkownika – musi on pobrać szkodliwy program na swój komputer. Dzieje się tak, gdy cyberprzestępcy uda się oszukać ofiarę, by uwierzyła, że pobiera nieszkodliwy program lub klika legalny odnośnik. Do ochrony przed tą formą ataku wymagany jest program antywirusowy wykrywający zagrożenia w momencie zainicjowania pobierania niebezpiecznych obiektów z internetu.

W okresie kwiecień-czerwiec 2014 produkty Kaspersky Lab, wykryły **w Polsce 2 163 985** szkodliwych programów atakujących poprzez internet.

W sumie, w badanym okresie 21,5% użytkowników produktów Kaspersky Lab było atakowanych szkodnikami infekującymi poprzez strony internetowe.

Polska plasuje się na 79 miejscu na świecie, jeżeli chodzi o zagrożenia związane z surfowaniem po internecie.

Miejsce	Kraj	Odsetek użytkowników
1	Rosja	48,1%
2	Kazachstan	46,7%
3	Armenia	43,5%
4	Azerbejdżan	43,0%
5	Ukraina	42,5%
...	...	...
79	Polska	12,5%

Odsetek użytkowników atakowanych podczas przeglądania zasobów online, II kwartał 2014 r.

Zagrożenia lokalne

Statystyki dotyczące lokalnych infekcji na komputerach użytkowników stanowią bardzo istotny wskaźnik. Najczęściej incydenty te związane są z robakami i zawirusowanymi plikami. Dane te obrazują, jak często użytkownicy są atakowani przez szkodliwe oprogramowanie rozprzestrzeniające się poprzez przenośne pamięci USB, płyty CD i DVD, oraz inne kanały, które nie wymagają dostępu do internetu.

Ochrona przed takimi zagrożeniami wymaga nie tylko programu antywirusowego radzącego sobie z zainfekowanymi plikami, ale także zapory sieciowej, zabezpieczenia przed rootkitami (szkodliwymi programami ukrywającymi się w systemie) oraz możliwości zaawansowanej kontroli wymiennych nośników danych.

W okresie kwiecień-czerwiec 2014, produkty Kaspersky Lab zablokowały **6 072 534** lokalnych ataków szkodliwego oprogramowania na komputerach użytkowników z Polski.

Podsumowując, **28,7%** użytkowników z Polski było atakowanych lokalnie w badanych okresie. Daje to Polsce **127** miejsce na świecie.

Miejsce	Kraj	Odsetek użytkowników
1	Wietnam	60,5%
2	Mongolia	56,1%
3	Algieria	53,4%
4	Jemen	53,0%
5	Bangladesz	52,5%
...	...	...
127	Polska	28,7%

Odsetek użytkowników atakowanych lokalnie, II kwartał 2014 r.

Serwery przechowujące szkodliwą zawartość

Kiedy użytkownicy Kaspersky Lab są atakowani przez zagrożenie online, zapisujemy źródło tego niebezpieczeństwa - lokalizację szkodliwego programu, który próbuje zainfekować system. Wg tych informacji, incydenty ze szkodliwym oprogramowaniem przechowywanym na serwerach w Polsce wyniosły **0,13% - 518 840** przypadków we wskazanym okresie. Daje to Polsce **26** miejsce w skali świata.

Miejsce	Kraj	Odsetek incydentów
1	Niemcy	25,34%
2	USA	21,31%
3	Holandia	13,03%
4	Rosja	8,57%
5	Kanada	6,65%
...	...	...
26	Polska	0,13%

Odsetek użytkowników atakowanych przez szkodliwą zawartość przechowywanych na serwerach zlokalizowanych w danym kraju, II kwartał 2014 r.