25% nowych robaków stworzonych w tym roku rozprzestrzenia się przez urządzenia USB. Co roku 48% małych i średnich firm na całym świecie pada ofiarą infekcji. Przyczyną jednej trzeciej z nich są robaki szerzące się przez urządzenia USB - to tylko jeden z wniosków badania „Second International SMB Security Barometer", którym objęto ponad 10 tys. firm w Europie i obu Amerykach.

Według PandaLabs, laboratorium badawczego firmy Panda Security, 25% nowych robaków w 2010 r. zaprojektowano specjalnie tak, by rozprzestrzeniały się przez urządzenia USB podłączane do komputerów. Zagrożenia tego typu są w stanie samodzielnie skopiować swój kod na dowolne urządzenia przechowujące dane: telefony komórkowe, dyski zewnętrzne, pamięci flash, odtwarzacze MP3/MP4, itp.

Zebrane informacje sugerują, że taka technika dystrybucji zagrożeń jest wysoce skuteczna. Według opublikowanego przez firmę Panda Security barometru bezpieczeństwa małych i średnich firm „Second International SMB Security Barometer", którym objęto 10 470 firm w 20 krajach, około 48% firm (posiadających do 1000 komputerów) przyznaje, że w zeszłym roku ich systemy zostały zainfekowane jakimś złośliwym kodem. 27% z nich potwierdziło, że źródłem infekcji było urządzenie USB podłączone do komputera.

Luis Corrons, dyrektor techniczny PandaLabs, mówi: „Aktualnie wiele zagrożeń będących w obiegu zostało zaprojektowanych tak, by rozprzestrzeniać się przez USB. Złośliwe kody nie tylko kopiują się na urządzenia przenośne, ale także automatycznie uruchamiają się, gdy tylko zainfekowany sprzęt zostanie podłączony do innego komputera. Infekcja kolejnego systemu jest praktycznie niezauważalna dla użytkownika. Tak było w przypadku wielu infekcji odnotowanych w zeszłym roku, m.in. przy dystrybucji botnetu Mariposa".

Infekcje tego typu są nadal mniej liczne niż te rozpowszechnianie poprzez korespondencję e-mail, ale ich liczba stale rośnie. „Na rynku jest teraz tak wiele urządzeń, które można podłączyć do komputera przez port USB: kamery cyfrowe, telefony komórkowe, odtwarzacze MP3 i MP4…" - dodaje Corrons. „To oczywiście duża wygoda dla użytkowników, ale takie urządzenia posiadają karty pamięci lub pamięci wewnętrzne, więc bardzo łatwo za ich pomocą można przenosić wirusy".

Jak to działa?
Działanie zagrożeń rozprzestrzeniających się przez urządzenia i dyski przenośne (karty memory stick, odtwarzacze MP3, kamery cyfrowe itp.) wygląda następująco: system Windows wykorzystuje plik Autorun.inf na tych urządzeniach lub dyskach w celu sprawdzenia, jaką czynność ma wykonać po ich każdorazowym podłączeniu do komputera. Taki plik, który znajduje się w katalogu głównym urządzenia, umożliwia automatyczne uruchomienie części zawartości już w momencie połączenia się z komputerem. Cyberprzestępcy wykorzystują tę funkcję do rozpowszechniania wirusów poprzez modyfikację plików Autorun.inf za pomocą poleceń, tak by zagrożenia przenoszone, na przykład na napędzie USB, uruchamiały się automatycznie, gdy urządzenie połączy się z komputerem. Wywoła to natychmiastową infekcję.

Skuteczna szczepionka
Aby temu przeciwdziałać, firma Panda Security opracowała szczepionkę Panda USB Vaccine – bezpłatny produkt zapewniający podwójną warstwę ochrony poprzez wyłączenie funkcji AutoRun na komputerach, napędach USB i innych urządzeniach. „To bardzo pożyteczne narzędzie. Dzięki niemu w prosty sposób możemy wyłączyć funkcję AutoRun w Windows i tym samym zyskać wysoki poziom ochrony przed infekcjami rozprzestrzeniającymi się przez napędy i urządzenia przenośne" - wyjaśnia Luis Corrons, dyrektor techniczny PandaLabs.

Panda USB Vaccine można pobrać bezpłatnie ze strony:
http://www.pandasecurity.com/homeusers/downloads/usbvaccine/.

Więcej informacji o badaniu „Second International SMB Security Barometr" dostępnych jest na stronie:
http://press.pandasecurity.com/wp-content/uploads/2010/08/2nd-International-Security-Barometer.pdf

Panda Security Polska