

W kwietniu cyberprzestępcy pomimo natychmiastowej reakcji firmy Adobe na wykryte luki bezpieczeństwa w oprogramowaniu AcrobatReader, skutecznie wykorzystali okazję do przeprowadzenia nowej fali ataków. Według analiz ekspertów G Data SecurityLab wśród złośliwych programów kwietnia niekwestionowanym numerem 1 został szkodnik „JS:Pdfka-OE” oraz zaprojektowany specjalnie do ataku na bezpłatne usługi pocztowe takie jak Yahoo, Hotmail i Google, trojan Win32:Rodecap[Trj].

Popularne pliki **PDF** i stosowane oprogramowanie do ich odczytu dotychczas uchodziło za bezpieczne narzędzia służące do wymiany informacji. Obecnie oprogramowanie umożliwiające odczytanie formatu PDF jest osadzone w kodzie Acrobat JavaScript, którego luki pozwalają atakującemu wstrzyknąć własny szkodliwy kod. Użytkownicy tego formatu ze względu na bezpieczeństwo muszą jak najszybciej przeprowadzić aktualizację oprogramowania a pliki PDF odbierać jako źródło potencjalnie niebezpiecznego kodu. Dodatkowo aby zminimalizować ryzyko ataku po przez dokumenty PDF zaleca się wyłączenie funkcji JavaScript.

Zestawienie najpopularniejszych szkodników minionego miesiąca doskonale ilustruje doskonałą organizację i dynamikę działania cyberprzestępczego świata. Nowo wykryta luka bezpieczeństwa natychmiastowo zostaje wykorzystana do rozpowszechniania złośliwego oprogramowania co bezpośrednio wpływa na popularność danego szkodnika w minionym miesiącu.

Kwietniowe ranking internetowych zagrożeń

„Łukasz Nowatkowski dyrektor techniczny w G Data Software „Nadużywanie i konkretne wykorzystanie luk bezpieczeństwa jest skutecznym sposobem infekowania komputerów oraz przeprowadzania ataków na rzecz twórców złośliwego oprogramowania. Innym równie niebezpiecznym zagrożeniem jest domyślnie włączona funkcja systemu Windows Autorun, umożliwiająca działanie groźnych plików rozprzestrzenianych poprzez zewnętrzne nośniki danych. Użytkownikom systemów operacyjnych Windows, dla których funkcja Autostartu nie jest pilnie potrzebna ze względów bezpieczeństwa zaleca się jej wyłączenie.”

G Data Software