

ROSJANIE ZHAKOWALI SZTAB WYBORCZY MACRONA

Hakerzy pracujący dla wywiadu wojskowego Rosji wykradli maile sztabu wyborczego Emmanuela Macrona przed wyborami prezydenckimi we Francji w 2017 roku - poinformował "Le Monde". Gazeta powołuje się na ustalenia specjalnego zespołu Google'a i organizacji FireEye.

FireEye specjalizuje się w tropieniu bardzo wyrafinowanych cyberataków, zwłaszcza związanych z rosyjskimi służbami. Analizy FireEye i Google'a potwierdziły, że dwa zespoły hakerów powiązane z rosyjskim wywiadem zaatakowały zaplecze wyborcze Macrona.

Najpierw grupa APT28 w marcu 2017 roku rozpoczęła ataki typu spearphishing, polegające na wysyłaniu maili od rzekomo zaufanego nadawcy, których celem jest uzyskanie poufnych informacji, takich jak hasła dostępowe. Według Google'a w maju 2017 roku, na dwa dni przed drugą turą wyborów prezydenckich we Francji, grupa Sandworm, rozpoczęła następną rundę ataków, przy użyciu tej samej metody.

Macron oskarżył wtedy Rosję o to, że prowadzi we Francji "operację destabilizacji", która miała na celu "sianie niepokoju i dezinformacji".

W lutym "Financial Times" napisał, że grupa APT28, łączona z cyberatakami na Demokratów w USA i wyciekami maili sztabu Macrona, działa jak agencja wywiadowcza, "gromadząca dane geopolityczne i informacje pomagające w kształtowaniu rosyjskiej polityki".

"FT" napisał też wówczas, powołując się na FireEye, że hakerzy z grupy Sandworm "są bardziej dyskretni niż APT28, ale atakują wiele rządów i władz lokalnych w Europie za pomocą personalizowanych ataków (spear phishing), zwłaszcza w Polsce".

Japońska firma Trend Micro zajmująca się cyberbezpieczeństwem jako pierwsza w kwietniu 2017 roku ostrzegła, że APT28 atakuje sztab wyborczy Macrona, ale informacji tych nie udało się wtedy potwierdzić.