# Kaspersky otkrio operaciju Crveni oktobar

U izvještaju objavljenom 14. siječnja Kaspersky lab otkriva detalje o špijunskoj operaciji koju su nazvali Crveni oktobar, prema knjizi i filmu "Lov na Crveni oktobar". Radi se o mreži inficiranih računala koja je služila za krađu povjerljivih informacija i dokumenata. Zanimljivo je da operacija traje još od 2007. godine, a otkrivena je tek potkraj prošle godine.

Napad bi započinjao ciljanim *phishing* mailovima slanim diplomatskim predstavništvima, vladinim i znanstveno-istraživačkim organizacijama širom svijeta. Većina napadnutih organizacija je u Istočnoj Europi, Aziji, ali su trojanci pronađeni i na računalima u Europi i SAD. Napadači su ciljali ambasade i konzulate, trgovačka predstavaništva, nuklearna postrojenja i istraživačke ustanove, gdje su prikupljali dokumente, čak i one zaštićene enkripcijom koju koristi NATO, ili obrisane datoteke. Po svemu sudeći, tražili su informacije koje se mogu skupo prodati.

Poruke su u privitku nosile Word ili Excell dokumente koji bi nakon otvaranja na primateljevo računalo spustili trojanca. Sam napad je prilično elementaran, koristili su exploite za poznate propuste, CVE-2009-3129 [1] (MS Excel), CVE-2010-3333 [2] (MS Word) i CVE-2012-0158 [3] (MS Word). Složenost ovog napada otkriva se tek nakon infekcije. Trojanac je bio u stanju s mreže skidati module za krađu zaporki i povijesti surfanja, snimanje sadržaja ekrana, krađu kontakata i sadržaja kalendara, *keyboard logger* te module za ekstrakciju informacija s pametnih telefona. Prikupljene informacije bile bi kriptirane i slane kontrolnim serverima. No oni su zapravo samo prva od tri razine *proxyja* koji su služili za prikrivanje krajnjeg odredišta, koje još nije okriveno.

Nagađa se da su autori ovog napada iz ruskog govornog područja, na što navode imena varijabli u kodu, kao i činjenica da trojanac aktivira kodnu stranicu za ćirilicu (naredba chcp 1251), no stručnjaci su oprezni jer to može biti i metoda zavaravanja.

Srpski mediji navode da je u Srbiji otkriveno nekoliko kompromitiranih računala. Čini se da su pogođena i računala u Bosni i Hrvatskoj, no detalji nisu objavljeni.

Radoznali mogu pročitati izvještaj Kaspersky laba, na ovoj poveznici [4].

pet, 2013-01-18 10:02 - Aco Dmitrović**Vote:** 3.5

Vaša ocjena: Nema Average: 3.5 (4 votes)

**Source URL:** https://sysportal.carnet.hr/node/1184

**Links**
[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3129
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333
[3] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158
[4] http://tinyurl.com/buo6ttz