Kad printer poludi

Ako Vaš pisač iznenada „poludi“ i krene ispisivati besmislice sve dok ne ostane bez papira, vjerojatno je došlo do infekcije trojancem nazvanim **Milicenso**. Stopa detektiranja ovog trojanca je vrlo niska, no otkriva ga ispis besmislica. Primarni cilj ovog trojanca nije trošenje papira, već je napravljen da posluži kao ulaz za drugi *malware*. Put prijenosa su prilozi emailova, linkovi i sl.

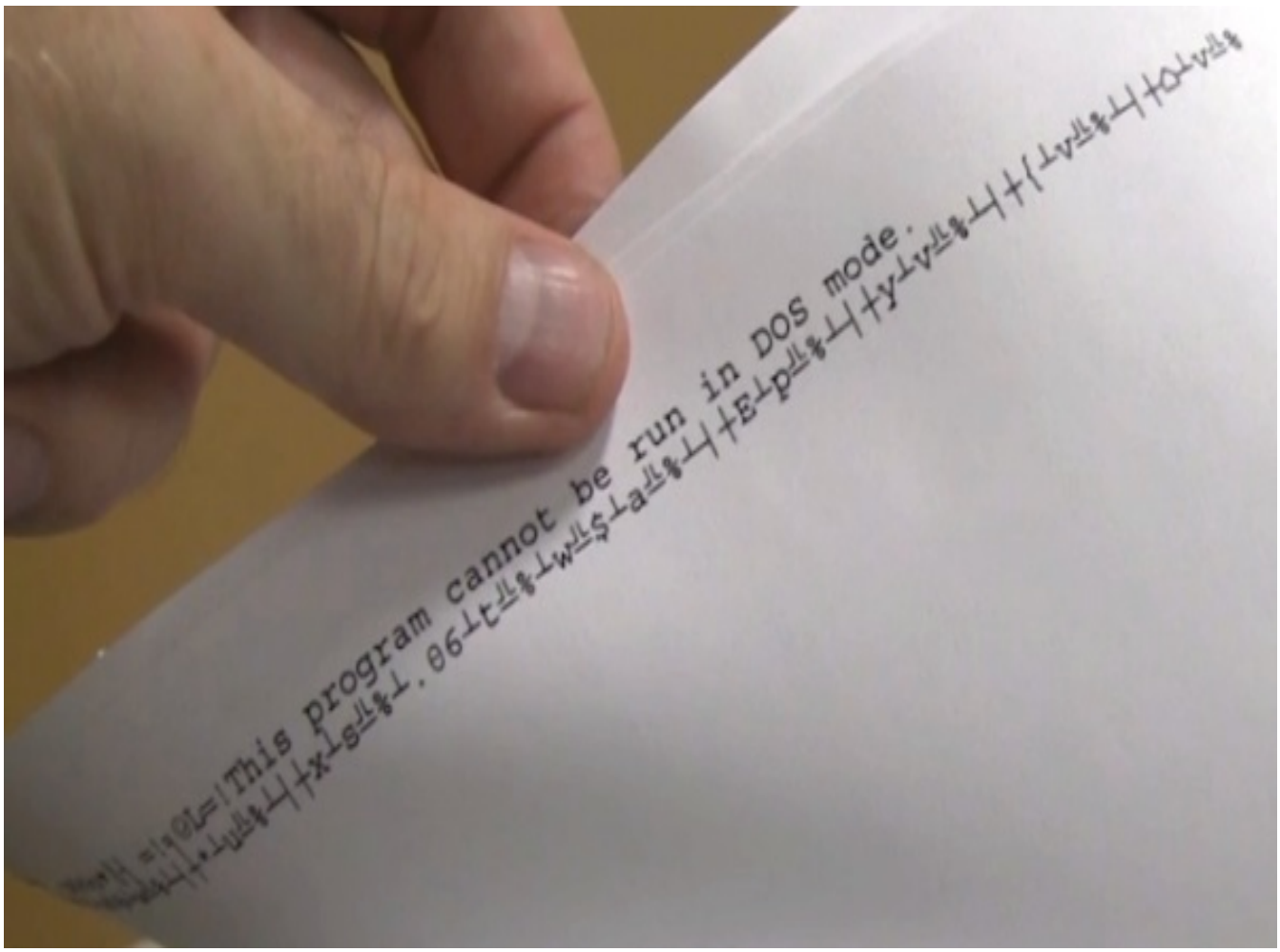
Trojanac kreira i pokreće dropper EXE datoteku, koja kreira DLL fajl u “%System% folder”. Kodirana DLL datoteka kreira brojne EXE i DLL datoteke i potom pokušava otkriti je li okruženje za izvršenje datoteke virtualna mašina, javni *malware sandbox* ili slično.

Odmah nakon otkrivanja ovog trojanca, otkriven je još jedan zlonamjerni program koji radi sličnu štetu, nazvan je **W32.Printlove**. Ovdje je riječ o crvu koji inficira računala u lokalnoj mreži koristeći ranjivost koda u Microsoft Windows Print Spool servisu. Ranjivost ima oznaku CVE-2010-2729, te je već zakrpana 2010. godine.

Problem iznenadnog aktiviranja pisača može se pojaviti nakon neuspješnog pokušaja W32.Printlove da inficira računalo s Windowsima XP u lokalnoj mreži. Crv šalje ciljanom računalu zahtijev za ispis koji koristi spomenutu ranjivost. Ako pokušaj bude uspješan, kopija malvera se smiješta u sistemski direktorij Windows-a i zatim se izvršava.

Međutim, ako je sustav zakrpan i tako siguran od iskorištavanja ranjivosti CVE-2010-2729, kopija crva nalazi se u %SystemRoot%\system32\spool\printers kao nasumično nazvana .spl (Windows Printer Spool) datoteka. Računalo ovu datoteku interpretira kao novi zahtijev za ispis i daje instrukcije mrežnom pisaču da ispiše sadržaj datoteke, trošeći tako papir i toner pisača.Crv povremeno pokušava inficirati druga računala, pa se incidenti s ispisom ponavljaju. Otkrivanje izvora problema može biti kompliciranо kada je u pitanju višestruka infekcija u mreži.

Više o ovom problemu pročitajte na Symantecovim [1] stranicama, gdje možete pogledati i video uradaka poludjelog printera.



sri, 2012-07-04 15:06 - Ivan Sokač**Vijesti:** Sigurnost [2]
Kategorije: Antivirus [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1057

Links
[1] http://www.symantec.com/connect/blogs/printer-madness-w32printlove-video
[2] https://sysportal.carnet.hr/taxonomy/term/13
[3] https://sysportal.carnet.hr/taxonomy/term/31