Trojanac napada Windows, Mac i Linux računala

Tvrtka F-Secure objavila je otkriće *web exploita* koji provjerava operativni sustav računala s kojeg se posjećuju inficirane web stranice. Nakon detekcije OS-a, na računala se distriburira trojanac čiji je izvršni kod prilagođen operativnom sustavu. *Exploit* je nazvan **Trojan-Downloader:Java/GetShell.A**. Trojanci koji se instaliraju na korisnička računala dobili su nazilve **Backdoor:W32/GetShell.A**, **Backdoor:OSX/GetShell.A** i **Backdoor:Linux/GetShell.A**.

Nakon instalacije trojanac se prijavljuje *Command & Control* serverima i čeka daljnje upute. Zasada one još nisu izdane, ali s tehničkog stanovišta sve je spremno. Vjerojatno će zaražena računala biti prodana na aukciji, pa će daljnji postupci ovisiti o kupcu.

Zanimljivo je da je za detekciju OS-a iskorišten Social-Engineer Toolkit (SET [1]), alat otvorenog koda napisan u Pythonu koji se inače koristi pri provjeri ranjivosti. Sam *exploit* koji otkriva OS napisan je u Javi.

Primjer ovog trojanca pokazuje da napadi postaju tehnički sve složeniji i da su osim Windowsa, koji su tradicionalna meta radi svoje rasprostranjenosti, sada zanimljivi i drugi operativni sustavi, budući da se njihov udio relativno povećava.

```
if (str4.indexOf("win") >= 0)
{
  str6 = getParameter("WINDOWS");
  str7 = getParameter("STUFF");
  str8 = getParameter("64");
  str9 = getParameter("86");
  str10 = getParameter("ILIKEHUGS");
  i = 0;
  str2 = str2 + str1 + ".exe";
}
else if (str4.indexOf("mac") >= 0)
{
  str6 = getParameter("OSX");
  i = 1;

  if (str2.startsWith("/var/folders/")) str2 = "/tmp/";
  str2 = str2 + str1 + ".bin";
}
else if ((str4.indexOf("nix") >= 0) || (str4.indexOf("nux") >= 0))
{
  str6 = getParameter("LINUX");
  i = 2;
  str2 = str2 + str1 + ".bin";
}
```

pet, 2012-07-13 09:01 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1063

Links
[1] https://www.trustedsec.com/downloads/social-engineer-toolkit/
[2] https://sysportal.carnet.hr/taxonomy/term/13