Conficker počeo donositi zaradu

Neposredno prije prvog travnja, tvrtka **Symantec** objavila je priopćenje u kojem umiruje javnost, tvrdeći da su opasnost od crva **Confiker** napuhali senzacionalistički mediji, te da su sve organizacije koje dobro održavaju računala i koriste antivirusni softver sigurne. Očigledno je da je poruka smišljena kako bi umirila kupce njihovog zaštitnog softvera.

No u našoj akademskoj zajednici nisu sva računala pod kontrolom IT osoblja, pa se i zakrpe neredovito instaliraju. Osim toga, crv odmah po instalaciji na računalo onemogući instalaciju zakrpa i ažuriranje antivirusne baze. Loše prognoze ipak su se, usprkos umirujućim izjavama, ostvarile.

Dok su verzije **A** i **B** crva **Confiker** nastojale zauzeti što više računala, verzija **C** se pritaji i čeka aktivaciju. Sada se pojavila nova inačica, **Conficker.E**, koja se ponovo agresivno širi. Ova inačica konačno radi posao radi kojeg je **Conficker** i napravljen: svojim tvorcima donosi zaradu. Crv instalira dodatni softver i tako proširaje funkcionalnost. Dio inficiranih računala prodan je spamerskoj grupi **Waledac**, koja je preuzela kontrolu nad inficiranim računalima i s njih odašilje spamove. Neki su proizvođači **AV** softvera zato ovu verziju nazvali **Confiker.E-Waledac**.

Kasperski lab javlja kako ga druga kriminalna skupina koristi za prodaju lažnog antivirusnog softvera. Korisnicima se otvara prozor u kojem ih se upozorava da je njihov računalo inficirano, a zatim se nudi rješenje problema: kupovina **AV** programa za 49,99$.

U međuvremenu, **Fjodor** je izdao novu inačicu nmapa koja još bolje detektira **Confickera**:

http://nmap.org/dist/nmap-4.85BETA7-setup.exe [1]

Kolege s kojima komuniciram javljaju da je novi **nmap** otkrio još inficiranih računala. Evo što verzija **beta7** javlja kad pronađe sumnjivo računalo:

```
Host 192.168.2.52 is up (0.00s latency).
Interesting ports on 192.168.2.52:
PORT STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:1A:4B:E6:4B:E4 (Hewlett Packard)
```

```
Host script results:
|  smb-check-vulns:
|  MS08-067: PATCHED (possibly by Conficker)
|  Conficker: Likely INFECTED
|_ regsvc DoS: FIXED
```

Najjednostavnij način da provjerite je li PC zaražen je pokušaj spajanja na URL http://update.microsoft.com [2]. Ako to ne uspije, znači da je virus obavio svoje. Pokušajte osvježiti definicije virusa, ako ni to ne uspije, sve je jasno.

Ako ostavite takva računala da preko praznika šalju spamove, vrlo je vjerojatno da će vaša domena dospjeti na crnu listu, pa će mail promet biti blokiran prema domenama koje konzultiraju crne liste.

Preporučujem i da svoje korisnike redovito obavještavate o novostima s antivirusne fronte, jer ćete tako osigurati njihovu suradnju i podizati svijest o potrebi za provođenjem mjera informacijske sigurnosti.

uto, 2009-04-14 12:29 - Aco Dmitrović**Vijesti:** Windows [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/556

Links
[1] http://nmap.org/dist/nmap-4.85BETA7-setup.exe
[2] http://update.microsoft.com
[3] https://sysportal.carnet.hr/taxonomy/term/12
[4] https://sysportal.carnet.hr/taxonomy/term/30