Maliciozni Python

 Da i programski jezici mogu biti metom napada, pokazuje nedavno objavljena informacija da su u repozitorij programskog jezika Python ubačeni maliciozni moduli. Doduše, cijela priča više “vuče” na nečiji eksperiment nego na pravi kriminalni napad, no u svakom slučaju demonstrira ključni sigurnosni propust: nepostojanje racionalnog mehanizma sigurnosne provjere modula.

PyPI (https://pypi.python.org/pypi [1]) je repozitorij modula za programski jezik Python; moduli su biblioteke koje sadrže već gotove funkcije koje programeri mogu po potrebi uključiti u vlastiti program i koristiti. Napadači su iskoristili nisku razinu sigurnosti kako bi u repozitorij ubacili deset biblioteka koje su u svojoj naravi kopije stvarnih biblioteka sa minimalnom promjenom u nazivu modula i sa izvjesnim “dodatnim kodom”. Programeri koji bi se zabunili i pogrešno napisali ime modula (typosquatting (https://en.wikipedia.org/wiki/Typosquatting [2])) – primjerice “setup-tools” umjesto “setuptools” ili “urlib3” umjesto “urllib3” - instalirali bi maliciozni modul umjesto pravog i pritom izvršili “dodatni kod”.

Malicioznih modula je deset:

– acqusition (uploaded 2017-06-03 01:58:01, impersonates acquisition)
– apidev-coop (uploaded 2017-06-03 05:16:08, impersonates apidev-coop_cms)
– bzip (uploaded 2017-06-04 07:08:05, impersonates bz2file)
– crypt (uploaded 2017-06-03 08:03:14, impersonates crypto)
– django-server (uploaded 2017-06-02 08:22:23, impersonates django-server-guardian-api)
– pwd (uploaded 2017-06-02 13:12:33, impersonates pwdhash)
– setup-tools (uploaded 2017-06-02 08:54:44, impersonates setuptools)
– telnet (uploaded 2017-06-02 15:35:05, impersonates telnetsrvlib)
– urlib3 (uploaded 2017-06-02 07:09:29, impersonates urllib3)
– urllib (uploaded 2017-06-02 07:03:37, impersonates urllib3)

No, ono što ovu priču čini zanimljivom je činjenica da maliciozni kod ne čini nikakvu štetu, već na IP adresu 121.42.217.44:8080 [3] dojavljuje naziv instaliranog malicioznog modula, korisničko ime i ime računala na kojem je modul pokrenut. Maliciozni kod dug je dvadesetak linija, a posebno zanimljiv je ovaj dio:

```
except Exception,e:
# Welcome Here! ?
# just toy, no harm ?
pass
```

Kod je pisan za Python 2, i na trojci će prijaviti greške.

Ovakav komentar sugerira da autor nije imao kriminalnih namjera, već je vjerojatno riječ o eksperimentu ili PoC aktivnosti čiji je cilj ispitati sigurnost repozitorija, dokazati ranjivost i izmjeriti koliki utjecaj može imati, tj. koliko se lako može širiti.

Dapače, prije dvije godine netko se na Redditu zapitao upravo to: koliko je sigurno koristiti PyPI module: https://www.reddit.com/r/Python/comments/2kq4a0/pypi_packages_safe/ [4]

Otprilike u to vrijeme, isto se pitanje ponovilo na Stackexchange: https://security.stackexchange.com/questions/79326/which-security-measures-does-pypi-and-similar-third-party-software-repositories [5]

Ovo nije jedini takav “napad” - već je otprije primjećen problem loše organizacije PyPI repozitorija koji dozvoljava stvari koje bi zdravorazumski trebale biti zabranjene: https://hackernoon.com/building-a-botnet-on-pypi-be1ad280b8d6 [6]

Čak i ako je ovo, kako se čini, djelo nekoga sa potencijalno dobrim namjerama, valja nam imati na umu da ne smijemo slijepo vjerovati repozitorijima koji nemaju ugrađen sustav provjere datoteka koje nude, kao i to da jednostavne provjere autentičnosti datoteke (hash) ne garantiraju da u njoj nema malicioznog koda. Typosquatting je dosta nezgodan problem i za takav napad potreban je ljudski faktor, a u takvom slučaju dužna pažnja je najbolja preventiva.

Puni advisory možete pronaći ovdje: http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/ [7]

sri, 2017-09-20 15:35 - Radoslav Dejanović**Vote:** 0

No votes yet

story_tag: python [8]

Source URL: https://sysportal.carnet.hr/node/1762

Links
[1] https://pypi.python.org/pypi

[2] https://en.wikipedia.org/wiki/Typosquatting
[3] http://121.42.217.44:8080
[4] https://www.reddit.com/r/Python/comments/2kq4a0/pypi_packages_safe/
[5] https://security.stackexchange.com/questions/79326/which-security-measures-does-pypi-and-similar-third-party-software-repositories
[6] https://hackernoon.com/building-a-botnet-on-pypi-be1ad280b8d6
[7] http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/
[8] https://sysportal.carnet.hr/taxonomy/term/142