A replica of AlphaBay market used to steal login credentials

February 12, 2016 By Pierluigi Paganini

Fraudsters operating on the AlphaBay darknet market have deployed a replica of the popular marketplace to steal login credentials from peers.

Paul Mutton, security experts at Netcraft, discovered a fake version of the Alphabay Market (pwoah7foa6au2pul.onion), one of the most popular black markets hosted in the dark web.

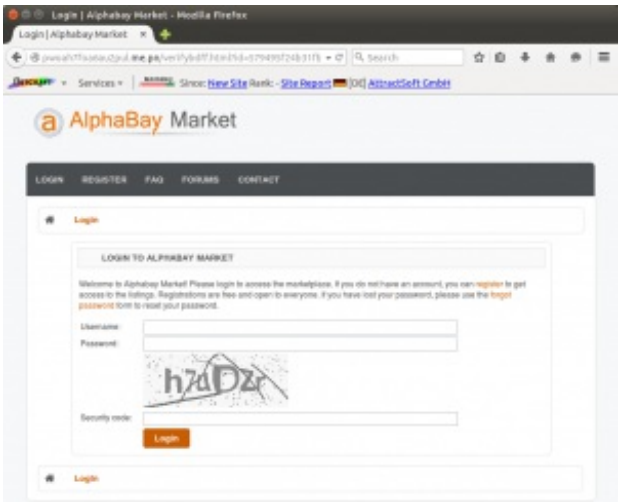
Paul Mutton speculates that fraudsters have deployed the fake version of the Alphabay Market in an attempt to steal login credentials.

"Fraudsters operating on the AlphaBay darknet market are using phishing attacks to steal login credentials from other criminals. In this particular attack, the phishing site mimics the address of one of AlphaBay's Tor hidden services." wrote Mutton.

AlphaBay is today one of the most interesting black markets, it offers any kind of illegal products and

important black market for payment card frauds.

The fake website mimics the login page of the Alphabay black market, including the CAPTCHA protection mechanism.



When Alphabay users login to the bogus website are redirected to the legitimate AlphaBay Market.

In order to replicate the legitimate website it was necessary to reproduce also the .onion address that is associated to the hidden service. This address is derived from the public key used to authenticate the connection, this means that it is very difficult to convincingly impersonate the site without having access to the owner's key pair.

Fraudsters have computed a partial match using tools such as scallion and generate a similar address like **pwoah7f**5ivq74fmp.onion.

*"However, in the case of this phishing attack, the fraudster has simply created a lookalike domain on the public internet, using the address **pwoah7foa6au2pul**.me.pn." wrote Mutton.*

"This phishing attack makes use of a me.pn domain, which was likely chosen because addresses under this domain can be registered for free, and the ".me.pn" string bears a (somewhat tenuous) similarity to the .onion TLD, at least in terms of its length."

As explained by Mutton, this phishing attack is another example of fraudsters defrauding fraudsters.

It’s obvious that similar attacks represents a threat only for new users who are deceived by the replica, meanwhile AlphaBay veteran members will never fall victim of such kind of attack.

Pierluigi Paganini

(Security Affairs – Black Market, dark web)

AlphaBay | black market | Cybercrime | Dark Web | Deep Web | Hacking | phishing

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over

20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Interview with Troels Oerting on cybersecurity in modern organizations

NEXT ARTICLE

The FBI requests $38 Million to counter the threat of Going Dark

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6

Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

---

1. Best Antivirus Software 

2. Remove Antivirus Scan 

3. Cheap Laptops Online 

4. Cell Phone Reviews 

5. Top 10 Cell Phones 

6. Password Management Software 

7. Computer Repair Services 

8. Protect Your Privacy 

Back to top