

Forum:[Hack Forums](#)

Thread: [Puu.sh update was infected \[steals passwords\] *important if you were using Puu.sh](#)

Herbert - April 1, 2015, 5:06 am

headsup,

Screenshot-sharing app Puush has inadvertently infected Windows users with malware. Over the weekend, the Puush server was breached and a fake, malware-infected program update was put in place. This means that anyone updating to version r94 of the software is infected.

The malware tries to grab passwords from infected systems, and was noticed after users complained on Twitter that the latest update had been flagged up by BitDefender. As a precautionary measure, the update server has been taken offline, and a clean update has been made available as a standalone download.

Puush is quick to point out that it is only the Windows version of the app that is affected -- the iOS and OS X apps remain clean. It is not yet clear what happens to passwords that have been collected as tests have not shown them to be sent to another computer. Another update has already been produced, version r100, and this has not only been checked to be clean, but also tidies up after the malware infected r94.

In a statement, Puush said:

The malware may be collecting locally stored passwords, but we are yet to confirm these have been transmitted back to a remote location. We have been running the malware in sandboxed environments and have not been able to reproduce any such behaviour. Even so, we recommend you change any important passwords which were stored on your PC (unless they were in a secure password manager). This includes chrome/firefox saved passwords.

The statement also recognizes the fact that some people may have been put off using Puush. For these users, a cleanup and removal tool is available:

We have created a cleaner for people who do not wish to continue using puush. It is stand-alone and will tell you if you were infected (assuming you have not already updated to r100). You can obtain this here: http://puush.me/dl/puush_is_sorry.exe

source: <http://betanews.com/2015/03/30/fake-puush-update-steals-passwords-from-windows-users/>

FuZiioN - April 1, 2015, 5:09 am

Please tell me this is a fucking troll.

Herbert - April 1, 2015, 5:14 am

(Apr 1, 2015 05:09 AM)?erser Wrote: [\[CITE\]](#) Please tell me this is a fucking troll.

No, this is not a joke.

I was affected by this as well, received yesterday backdoor bots from malware bytes named, gizmoSE and LicenseSE.

I'm not sure if those were from puu.sh or others.

Tokyo - April 1, 2015, 5:17 am

(Apr 1, 2015 05:14 AM)John Herbert Wrote: [\[CITE\]](#) No, this is not a joke.

I was affected by this as well, received yesterday backdoor bots from malware bytes named, gizmoSE and LicenseSE.

I'm not sure if those were from puu.sh or others.

Inb4 Aeonhack decided to backdoor .Net Seal and make the biggest botnet known to man

Spoiler [\(Click to View\)](#)lel jk, or am I?

Meow - April 1, 2015, 5:20 am

Damn,thanks for warning man! How I have to change all my passwords -.-

Herbert - April 1, 2015, 6:07 am

I'm writting a guide on how to secure your account(s) that have been affected by this.