Featured news

- OpenWPM: An automated, open source framework for measuring web privacy
- Good practice guide on disclosing vulnerabilities
- Cybersecurity recommendations for medical device manufacturers
- LostPass: A worryingly simple phishing attack aimed at LastPass users
- Casino operator sues Trustwave for failing to spot and stop hackers
- Endpoint security really can improve user experience
- How email in transit can be intercepted using DNS hijacking
- Unexpected implications arising from the Internet of Things
- Flaw allows malicious OpenSSH servers to steal users' private SSH keys
- 250 Hyatt hotels around the world hit with PoS malware
- Cheap web cams can open permanent, difficult-to-spot backdoors into networks
- Microsoft ends support for Windows 8, IE8 through 10: What does this mean for you?
- Have I been hacked? The indicators that suggest you have

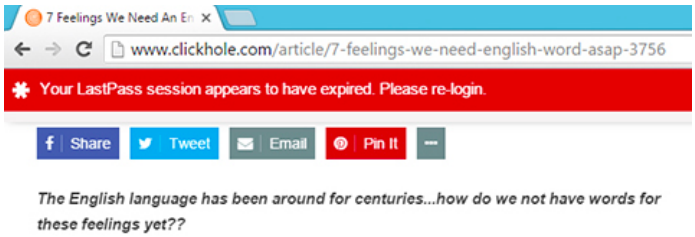
LostPass: A worryingly simple phishing attack aimed at LastPass users

Posted on 18 January 2016.

Security researcher (and Praesido CTO) Sean Cassidy has demonstrated at ShmooCon how easy it can be for hackers to steal LastPass users' email, password, and two-factor authentication code via a simple phishing attack.

With this information in hand, the attackers can access the victim's LastPass vault and all the information in it - passwords, sensitive info, etc. - without the victim's knowledge, and change certain settings so that they continue to have access to it in the future.

The attack - dubbed LostPass by Cassidy - relies on the fact that LastPass effectively trained users to expect notifications in the browser viewport (the area below the tab bar and URL address bar (as seen here):



The LastPass login screen and two-factor prompt are shown in the viewport as well.

By luring victims to a malicious website or a real one that is vulnerable to XSS, the attackers are able to show a fake login expired notification. Due to the fact that LastPass is also vulnerable to a logout CSRF flaw, the website can also log any user out of LastPass, so the fake notification is even more convincing.

"Once the victim clicks on the fake banner, direct them to an attacker-controlled login page that looks identical to the LastPass one," Cassidy explained.

"The victim will enter their password and send the credentials to the attacker's server. The attacker's server will check if the credentials are correct by calling LastPass's API. The API will inform us if two-factor authentication is required."

If the credentials are incorrect, the victim will see an "Invalid Password" message. If the user has two-factor authentication, they will see a two-factor prompt and enter the needed code.

Armed with all that info, the hackers can access the vault and download all of the victim's information from the LastPass API, and "backdoor" the account by disabling two-factor authentication, adding themselves as the emergency contact, and adding their server as a trusted device.

Cassidy says this attack works on the latest version of LastPass (4.0), and best on Chrome. He even provided a tool that can be used to perform this attack and which can be used by companies to "pen-test themselves to make an informed decision about this attack and respond appropriately."

Users can check whether they have already been attacked by viewing their LastPass Account History and see if there have been suspicious login attempts from unexpected IP addresses.

Cassidy advised users and companies to disable mobile login, log all logins and failures, and ignore notifications in the browser window in order to protect themselves and their employees. The latter should also be informed of the potential attack, so that they could avoid becoming victims.

Spotlight 1 2 3 4 5

LostPass: A worryingly simple phishing attack aimed at LastPass users

Security researcher Sean Cassidy has demonstrated at ShmooCon how easy it can be for hackers to steal LastPass users' email, password, and two-factor authentication code via a simple phishing attack.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address Subscribe

Daily digest

Receive a daily digest of the latest security news.

Email @ Address Subscribe

LastPass knows of these problems, and has already instituted some fixes, and is looking to make some more.

Author: Zeljka Zorz, HNS Managing Editor

Follow @zeljkazorz

authentication passwords phishing software vulnerability

DON'T MISS
Tue, Jan 19th

- **OpenWPM: An open source framework for measuring web privacy**
- **Endpoint security really can improve user experience**
- **How email in transit can be intercepted using DNS hijacking**
- **Cheap web cams can open permanent, difficult-to-spot backdoors**
- **Have I been hacked? The indicators that suggest you have**

Back to TOP