Click Studios
ABN: 84 321 815 001

Level 3, 97 Pirie St
Adelaide, SA, 5000
Australia

Phone:+61 88120 0630

sales@clickstudios.com.au
www.clickstudios.com.au

clickstudios PASSWORDSTATE

INCIDENT MANAGEMENT ADVISORY #05

Dated: 14th May 2021, 11:00 AM (Australian CST)

Click Studios advises that any customer that has performed an In-Place Upgrade between 20th April 2021 8:33 PM UTC and 22nd April 2021 0:30 AM UTC had the potential to download a malformed Passwordstate_upgrade.zip file.

Advisory Summary:
The number of affected customers remains extremely low. Only customers that performed In-Place Upgrades between the times stated above are believed to be affected. The Phishing Attack uses a similar approach to the original exploit and tries to harvest Passwordstate credentials. All Passwordstate controlled upgrade packages are confirmed as being unaltered.

Analysis of Phishing Attack:
A very small number of customers had reported receiving the phishing attack email. The email recipients are not consistent with nominated contacts registered for those organizations. The body of that email is almost identical to Click Studios correspondence that had been scanned and uploaded to social media.

The email states to download a version of the hotfix Moserware.zip file containing a malformed Moserware.SecretSplitter.dll. The link for the hotfix file references an alternate Content Distribution Network not controlled by Click Studios. The email also quotes a checksum value that isn't correct or published on Click Studios website.

On loading into memory, the Moserware.SecretSplitter.dll attempts to download a new payload file Moserware_Amazon.zip containing a .ICO file, with additional obfuscation/encryption making it more challenging to disassemble.

This .ICO file is converted into a DLL in memory and attempts to harvest similar data as the original exploit. To obtain information from Passwordstate it attempts to read the web.config file to connect to the Passwordstate database, harvest password credentials and post these to yet another Content Distribution Network. Retrieving details from the web.config file is not successful if the details are encrypted.

Comparison of Checksums for All Packages:
Click Studios has downloaded copies of all software to confirm if any others were affected. This included copies from the Click Studios website and Click Studios controlled CDN. The checksum for packages at the .ZIP level and file level have been checked. All matched 100% showing no evidence of being tampered with.

Identification, Remedial Actions and Advice:
Click Studios number one priority is working with our customers, identifying if they have been affected and advising them of the required remedial actions. The ACSC (Australian Cyber Security Centre) is aware of the incidents, providing advice to Click Studios. Any Australian organizations that believe they have been affected should contact them via ASD.Assist@defence.gov.au or 1300 CYBER1.

Request for Additional Information:
All requests for information are directed to our Advisories webpage, where advisories will detail all known facts, including any Passwordstate functionality that has been compromised. **If we have not explicitly stated that functionality is compromised then it is safe to use**.