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 #03

Dated: 27th April 2021, 11:00 AM (Australian CDT)

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:
As stated in previous advisories the number of affected customers, based on the window of opportunity, the initial compromise and subsequent exploit, and confirmed by customers provision of information, is still very low. Only customers that performed In-Place Upgrades between the times stated above are believed to be affected. We have taken down our Blog and Forum sites as a precaution. We confirm there was only one modified Passwordstate file. If customers are unsure about performing Manual Upgrades they should hold off until further notice.

Blog and Forum Sites:
There is speculation that Click Studios Blog and Forum websites have been compromised. Once invoked our Incident Management Process stipulates Blog and Forum websites are to be taken down as a priority to reduce potential attack vectors and publishing of unauthorized content. They will be analysed at a later date as part of the preparation for resumption of normal operations.

Updated Analysis:
We have performed multiple full comparisons of the checksum values, for all files contained within Click Studios legitimate Passwordstate_upgrade.zip, against the bad actors malformed version of that ZIP file.

These comparisons confirm the only modified file in the bad actors Passwordstate_upgrade.zip was moserware.secretsplitter.dll. All other files were unmodified. This indicates the bad actor has not modified copies of original source code and compiled these. Having done so would have changed the checksum vales for those files compared to those supplied by Click Studios.

Performing Manual Upgrades:
We confirm that performing a Manual Upgrade, as outlined under **Section 6 Manual Upgrade Instructions** in our online documentation, is safe. However, we understand some customers are unsure of this process and therefore recommend those customers refrain from performing any upgrades at this time. Assisting customers with Manual Upgrade issues is currently prioritized lower than incident identification and remediation activities.

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 incident and is 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**.