computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-007

Unauthorized Personal Data Sharing

March 29, 2018 — v1.0

History:

- *29/03/2018 — v1.0: Initial publication*

Summary

We have observed the usage of software tools and components that might lead to unauthorized personal data leakage. These components are often available in the form of browser extensions or plugins, or e-mail clients plugins. Examples include: Zoominfo, Data.com, InsideView, NetProspex, DiscoverOrg, or LeadIQ.

Depending on the machine configuration and policy, these components may be often installed by the users themselves – without any need for administrator access. Once installed, these components typically gather contact information (address books, etc.), which are then exfiltrated and shared with third parties. Such indiscriminate sharing of corporate address books and other similar data creates potential issues under the new European GDPR directive, and hence should be avoided.

Technical Details

While several products exist, this description of technical details focuses on a specific example of Zoominfo, which is relevant to most organizations using Outlook e-mail client and Exchange e-mail server.

Zoominfo is providing an Outlook plugin – `ZoomInfoContactContributor` – used to share contacts and receive access to the Zoominfo database. During the installation of the plugin additional components are downloaded from `freshcontacts.com`. In most cases (but depending on local policy and configuration of the end-user machine), the **administrative rights are not needed** for the installation of the plugin.

Once the plugin is installed it starts sharing the addressbook entries with the Zoominfo database (and its customers).

Recommendations

Check if you are affected by searching in your network logs hits to domains such as `zoominfo.com` and `freshcontacts.com`.

More broadly search for other potential unwanted tools and components that might be used for data leakage such as Data.com, InsideView, NetProspex, DiscoverOrg, LeadIQ, and others.

In case you are affected report to your Data Protection Authority. In any case, check that you have the necessary controls in place by for instance following the ENISA guide [1].

To prevent the possibility of unauthorized personal data sharing through the components described in this advisory, consider enforcing a policy that would prevent end-users from installing browser arbitrary browser extensions as well as e-mail client plugins.

References

[1] https://www.enisa.europa.eu/publications/art4_tech