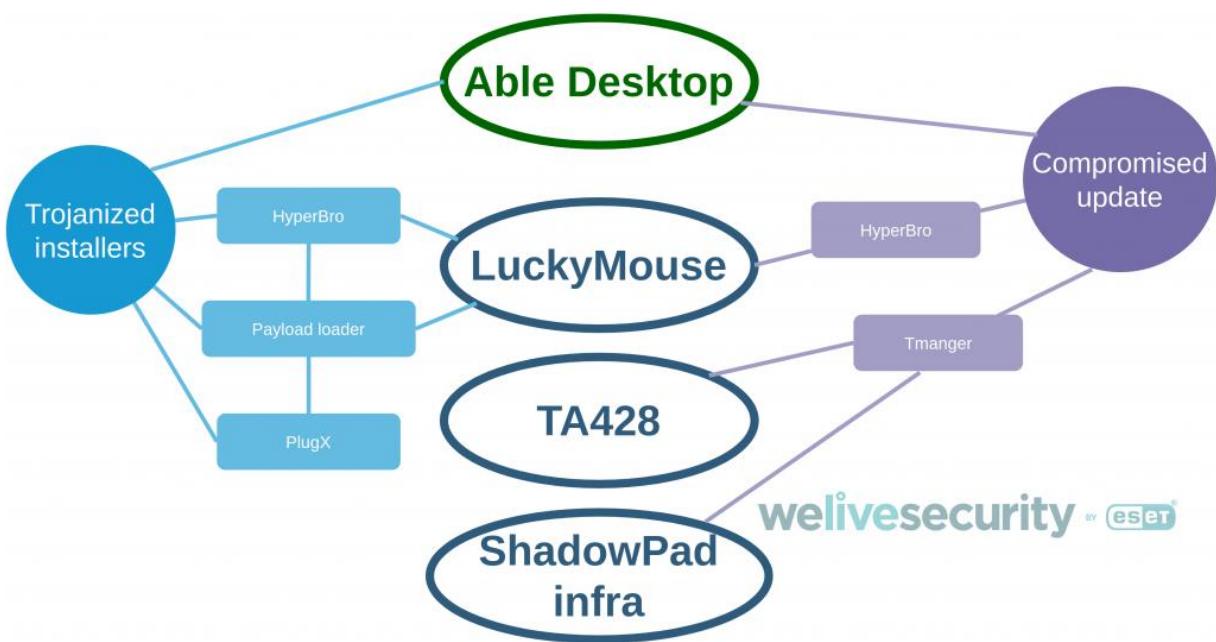


A.5 ABLE DESKTOP: CHAT SOFTWARE

- **Introduction of ABLE DESKTOP:** Able Desktop is chat software included as part of the Able business management suite used in Mongolia. It is a Chromium-based JavaScript app making use of the NodeJS library. According to Able, their software suite is used by 430 government agencies in Mongolia.
- **The method in attack:** During that campaign, the attackers compromised an unknown company that was providing government institutions in East Asia and leveraged that compromise to deliver HyperBro by email.



Regarding the attribution of Operation StealthyTrident, considering that HyperBro is commonly attributed to LuckyMouse, that Tmanger was attributed to TA428 and that it uses one of the ShadowPad C&C servers, multiple competing hypotheses exist:

- LuckyMouse has access to Tmanger and ShadowPad.
- LuckyMouse share its access to the compromised Able Desktop update server with the TA428 group or some other group having access to Tmanger.
- HyperBro is now shared with TA428 or some other group having access to Tmanger and ShadowPad.
- LuckyMouse and TA428 are subgroups of the same threat actor.
- **Conclusion:** Apart from the use of HyperBro, developed and commonly used by LuckyMouse, we found no significant overlap with the LuckyMouse toolset or network infrastructure. Does this mean that LuckyMouse has access to ShadowPad and Tmanger or did LuckyMouse share their access to a compromised Able Desktop update server with the TA428 group? Another hypothesis could be that, similarly to ShadowPad, HyperBro is now shared with other threat actors. Finally, one last hypothesis could be that LuckyMouse and TA428 are closely related threat actors or are actually the same.