ShadowPad is sold privately to a limited set of customers. SentinelOne has identified at least five activity clusters of ShadowPad users since 2017:

- NCPH 5.0 Remote Control Software, developed back in 2005, was powered by whg and Rose.
- Another subgroup, LEAD, also used ShadowPad along with other backdoors to attack victims for both financial and espionage purposes. They were reported to attack electronic providers and consumers, universities, and the gaming industry.
- APT41 is the model and ecosystem observed that some threat groups stopped developing their own backdoors after they gained access to– for instance, analysis on the relationship between indicators, long-term monitoring on the activities and campaigns– in the ShadowPad samples built by the controller by default. There is no configuration in the builder to allow the user to choose which plugins are compiled into the generated sample, so this setting can only be managed by the developer of the controller.
- However, the control interfaces of the plugins are hardcoded in the "Manager" page of the ShadowPad controller, and the controller can add new functionalities to the backdoor freely.
- An intriguing question to address is whether ShadowPad is a privately shared attack framework or a privately developed malware?

To answer those questions, we conducted a comprehensive study on the origin, usage and ecosystem of ShadowPad. ShadowPad emerged in 2015 as the successor to PlugX. However, it was not until several infamous supply-chain operations in multiple campaigns, including the CCleaner, NetSarang, and ASUS supply-chain attacks, that ShadowPad gained widespread attention. Since then, ShadowPad has been regularly updated with more advanced anti-detection and persistence techniques.

ShadowPad is still regularly updated with more advanced anti-detection and persistence techniques.

Selling the Plugins Separately Rather than Giving a Full Bundle by the Controller.

If ShadowPad was not originally designed as an open framework, the following question is whether it is freely shared among the group members. The controller provides: how ShadowPad affects the threat landscape of Chinese espionage attacks

YI-JHEN HSIEH

AUGUST 19, 2021