#HITB2021SIN D1T1 SHADOWPAD: Chinese Espionage Malware-as-a-Service - Yi-Jhen Hsieh & Joey Chen

Published: 2021-09-01 · Archived: 2026-04-05 15:10:28 UTC

SHADOWPAD emerged in 2015 as the successor to PlugX. However, it was not until several infamous supply-chain attack incidents happened – CCleaner, NetSarang and ShadowHammer – that it started to receive wide discussions in public. Unlike publicly-sold PlugX, SHADOWPAD is privately shared among a limited set of customers. Its plugin-based design and the capability of inserting plugins during runtime give it good extensibility on the functionalities for its users. Whilst collecting IoCs and connecting the dots, we asked ourselves: Who is using SHADOWPAD, and in which part is it special to own a page? What is the possible ecosystem behind each attack where SHADOWPAD was involved? And ultimately, what is the business model of this central piece of malware? To answer those questions, SentinelLabs did a comprehensive study on the origin, the use and the business of SHADOWPAD. Firstly, a brief walk-through will be given on the technical details of SHADOWPAD and at least 4 clusters of the users behind the backdoor. Afterwards, we will dig deeply into the potential business model of how the owners of SHADOWPAD charge their customers, which we believe the owners sell the plugins separately rather than a full bundle at once. At the end, we will discuss how its emergence changes the attacking strategies of some China-based threat actors and affects the threat landscape of Chinese espionage attacks. === Yi-Jhen Hsieh is a Threat Intelligence Researcher at SentinelOne, specializing in threat intelligence and malware analysis. Prior to joining SentinelOne, she worked as a Tier-3 analyst to support IR case analysis. She also has experience in spamming botnet tracking and solution delivery. --- Joey Chen is working as a Cyber Threat Researcher for SentinelOne Incorporated in Taiwan. His major areas of research include incident response, APT investigation, malware analysis and cryptography analysis. He not only has been a speaker at CODEBLUE, DeepIntel, HITCON and CYBERSEC conferences but also got 2018 Training Ambassador & Trainer prize in TrendMicro. Now he is focusing on the security issues of target attack, emerging threats and IOT systems. He also develops an automation intelligence platform to help his team get more sleep at night.
