Tracking the entire iceberg long term APT malware C2 protocol emulation and scanning Takahiro Haru

Published: 2022-10-26 · Archived: 2026-04-05 13:12:21 UTC

Presented at the VB2022 conference in Prague, 28 - 30 September, 2022. ↓ Slides: https://www.virusbulletin.com/uploads... ↓ Paper: https://www.virusbulletin.com/uploads... → Details: https://www.virusbulletin.com/confere... ✪ PRESENTED BY ✪ • Takahiro Haruyama (VMware) ✪ ABSTRACT ✪ Malware analysts normally obtain IP addresses of malware's command & control (C2) servers by analysing samples. This approach works in commoditized attacks or campaigns. However, with targeted attacks using APT malware, it's difficult to acquire a sufficient number of samples for organizations other than anti-virus companies. As a result, malware C2 IOCs collected by a single organization are just the tip of the iceberg. For years, I have reversed the C2 protocols of high-profile APT malware families then discovered the active C2 servers on the Internet by emulating the protocols. In this presentation, I will explain how to emulate the protocols of two long-term pieces of malware used by PRC-linked cyber espionage threat actors: Winnti 4.0 and ShadowPad. Both pieces of malware support multiple C2 protocols like TCP/TLS/HTTP/HTTPS/UDP. It's also common to have different data formats and encoding algorithms per each protocol in one piece of malware. I'll cover the protocol details while referring to unique functions such as server-mode in Winnti 4.0 and multiple protocol listening at a single port in ShadowPad. Additionally, I'll share the findings for the Internet-wide C2 scanning. After the presentation, I'll publish over 120 C2 IOCs with the date ranges in which they were discovered. These dates are more helpful than just IP address information since the C2s are typically found on hosted servers, meaning that the C2 could sometimes exist on a specific IP only for a very limited time. 65% of these IOCs have 0 detection on VirusTotal as of the time of this writing.
