Monitoring Winnti 4.0 C2 Servers for Two Years

By Takahiro Haruyama

Published: 2021-11-15 · Archived: 2026-04-05 13:49:00 UTC

The VMware Threat Analysis Unit (TAU) continually monitors the latest threats and attacks affecting our customers and businesses worldwide. For years, TAU has reversed and emulated the network Command and Control (C2) protocols of high-profile malware families, especially used for cyber espionage, in order to discover active C2 servers on the Internet. One family that TAU has tracked for years is Winnti 4.0 malware. TAU reported last year that nine C2 servers were found.

Winnti is a prominent malware family used by the multiple Chinese threat actors like APT41 for many years. The malware is a modularized Remote Access Trojan (RAT) supporting multiple C2 protocols.

Continuing its research, TAU has discovered additional Winnti 4.0 C2 servers actively used over the last two years. Contrary to our expectation, the threat actor didn't stop using the malware after our blog post. Instead, they have continued to deploy new servers using the same methodology and infrastructure. While the presence of this threat actor has increased regularly, there has been minimal reporting on this threat. **The number of the active servers continues to rise and even old servers, disclosed earlier by TAU, are still active as of the time of this writing**. In order to alert the cyber-security community to this threat, TAU decided to release the latest C2 IOCs.

The IOCs are located at our corporate github page. There are 43 servers (34 unique IPs) in total. Please note that the log entries each contain a first_seen and a last_seen date. TAU routinely scans these servers and notes approximately when they were first seen and when we last saw them as a server. As these are typically hosted servers, there are cases where the server may have been reappropriated to a legitimate use. It is advisable to verify any positive results in your environment to prevent false positives.

VMware Carbon Black EDR customers can utilize this intelligence by enabling the Known IOC Watchlist, under the Active C2 report.
