

# Closing Remarks - Diago Lima

---

 [urien.gitbook.io/diago-lima/abusing-tls-callbacks-for-payload-execution/introduction](https://urien.gitbook.io/diago-lima/abusing-tls-callbacks-for-payload-execution/introduction)

Thread Pool Injection is a powerful and innovative execution technique, and fixes one of the toughest issues many malware developers have faced for quite some time: the need to avoid creating remote threads.

While it certainly isn't a standalone technique per se, it can work very effectively alongside other malware techniques to accomplish an unprecedented level of stealth and evasion. The technique, in my opinion, marks a turning point in the continuous cat-and-mouse game between security solutions and their adversaries.

I believe it's quite powerful, but it isn't without its weaknesses. Defenders should configure their security solutions, if possible, to look for handle duplication of the three main handle types targeted in this technique: TpWorkerFactory, IoCompletion, and IRTimer. EDR drivers receiving callbacks for duplication of these handles should immediately investigate the source of the request, as this is highly irregular. In my opinion, this is the most reliable method of catching this technique.

←

Previous

Attacking Timer Queues

Next

Abusing TLS Callbacks For Payload Execution

→

Last modified 11d ago