tDiscoverer (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:55:39 UTC

tDiscoverer

aka: HAMMERTOSS, HammerDuke

Actor(s): APT29

F-Secure described tDiscoverer (also known as HammerDuke) as interesting because it is written in .NET, and even more so because of its occasional use of Twitter as a C&C communication channel. Some HammerDuke variants only contain a hardcoded C&C server address from which they will retrieve commands, but other HammerDuke variants will first use a custom algorithm to generate a Twitter account name based on the current date. If the account exists, HammerDuke will then search for tweets from that account with links to image files that contain embedded commands for the toolset to execute.

References

There is no Yara-Signature yet.
