The Chicken Keeps Laying New Eggs: Uncovering New GC MaaS Tools Used By Top-tier Threat Actors

By QuoScient GmbH

Published: 2020-06-26 · Archived: 2026-04-05 21:05:24 UTC

Note: *This article was initially written by the QuoINT Team as part of QuoScient GmbH. Since the foundation of QuoIntelligence in March 2020, this article was transferred to the QuoIntelligence website on 21 April 2020.*

TerraRecon is a reconnaissance tool used in highly targeted attacks that occurred at least between 2016 and 2018. Although we are unaware of the full kill-chain that led to the execution of TerraRecon, it is fair to assume that attackers used it as a second or third stage malware.

TerraRecon's primary objective is to scan the infected system for the presence of very specific hardware and software used in the retail and money transfer services, like:

- Western Union Software likely used in offices located in Italy
- Western Union and Wacom Signing Pads
- Yubico's Yubikeys

QuoINT was able to map three different versions of TerraRecon, and — based on the compilation timestamps of the samples analyzed and the timeline when they were likely used — concluded that the malware family potentially existed since at least 2013.

To keep reading*, please visit the official QuoIntelligence Blog or access the article here: https://quointelligence.eu/2020/01/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors/.*
