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

By Allison Ebel

Published: 2020-01-27 · Archived: 2026-04-05 18:52:25 UTC

During the code analysis of TerraRecon, it was evident that the standalone executable file shares a significant amount of code with TerraLoader, including string obfuscation, key brute-forcing, runtime function resolution, and a kill-switch feature. We assess with high confidence that the same person, either the MaaS operator or a separate malware author, coded both TerraRecon and TerraLoader. As we have previously noted, the MaaS operator's business model also relies on ad-hoc development request, so the custom development of TerraRecon seems to be a reasonable request.

Due to TerraRecon's focused reconnaissance, we assess with high confidence that the tool was developed for a specific customer, or limited group, having the financial capability to pay for its development. This conclusion likely indicates the request originates from a mid to top tier e-crime operator. By corroborating the scope of the tool, its objectives, its C2 infrastructure, and the sightings timelines, we attributed the exclusive use of TerraRecon to FIN6 with high confidence.

TerraRecon gathers system information, checks for file paths, and Active X controls related to very specific software and hardware.

TerraRecon v3 first brute-forces the string XOR encryption key and checks if the current year is 2018, and if not, it stops. By design, the variant includes a kill-switch functionality indicating that the malware will only operate during the specified year. The malware also performs an Internet connectivity check, as it attempts to resolve the hostname `ocsp.comodoca.com`, which which is the valid Online Certificate Status Protocol (OCSP) URL for Comodo used to check the status of a certificate. To note, none of the analyzed TerraRecon variants bear digital signatures. In addition, we did not observe the kill-switch functionality or internet connectivity check in either TerraRecon v2 or v1.

The malware will begin the reconnaissance activity on the victim machine by extracting the *pc_name* and *user_name* of the system. Next, it walks through a checklist of very specific software/hardware of interest, and whenever one of the checks is successful, a flag is set to make a callback to the C2. If the flag is not set by the end of the checklist, the malware will not callback. If the initial callback fails, the malware will only attempt one additional time. After reporting the checklist matches, it will delete itself via a BAT file.

All the analyzed TerraRecon samples make method calls on specific ActiveX controls (COM Object) to determine if the prerequisites on the checklist exist on the victim machine. Essentially, ActiveX controls are a small piece of software used by programs to make it available in the browser. TerraRecon establishes its C2 communication via HTTP GET request and transmits the results of the victim machine check as parameters in the URL. TerraRecon v3 transmits its results with a long version of the parameters whereas TerraRecon v1 and v2 use a shortened

version. Another difference between the variants is that TerraRecon v3 is written in PureBasic, in contrast to TerraRecon v1 and v2 which are written in Visual Basic.

The table below lists all main characteristics of TerraTV variants by focusing on the checks they perform on the targeted systems.

Interestingly, the file name of the TerraRecon v3 sample that was uploaded to VirusTotal in March 2019 was '*ETDAniConf.exe*', which imitates the name of a driver used by ELAN (ELAN Microelectronics Corp.) Smart-Pads (multi-finger touch pad) for many PC manufacturers.

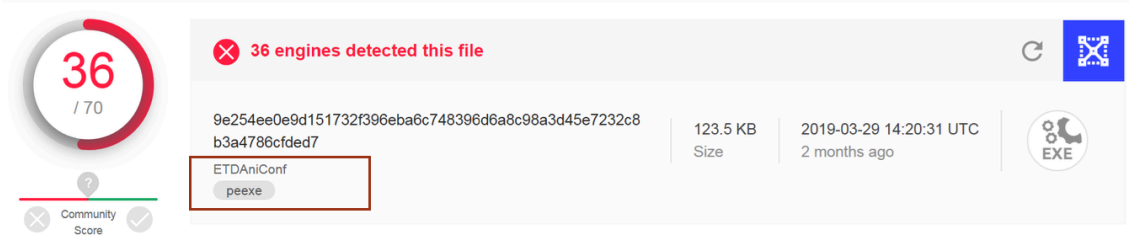

Figure 5 — TerraRecon sample's information from VirusTotal

Source: https://quointelligence.eu/2020/01/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors/