Trojan.TrickBot | Malwarebytes Labs

Archived: 2026-04-05 13:00:24 UTC

Short bio

Trojan.TrickBot is Malwarebytes' detection name for a banking Trojan targeting Windows machines.

Developed in 2016, TrickBot is one of the more recent banking Trojans, with many of its original features inspired by Dyreza (another banking Trojan). Besides targeting a wide array of international banks via its webinjects, Trickbot can also steal from Bitcoin wallets.

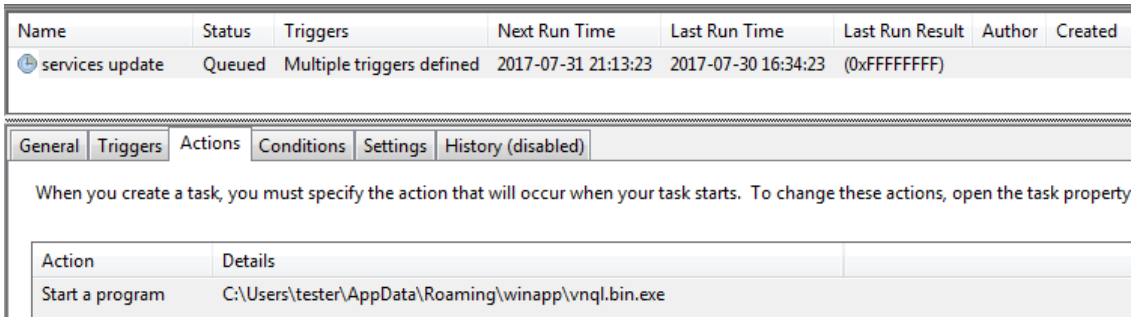
Some of its other capabilities include harvesting emails and credentials using the Mimikatz tool. Its authors also show an ability for constant new features and developments.

Trojan.TrickBot comes in modules accompanied by a configuration file. Each module has a specific task like gaining persistence, propagation, stealing credentials, encryption, and so on. The C&Cs are set up on hacked wireless routers.

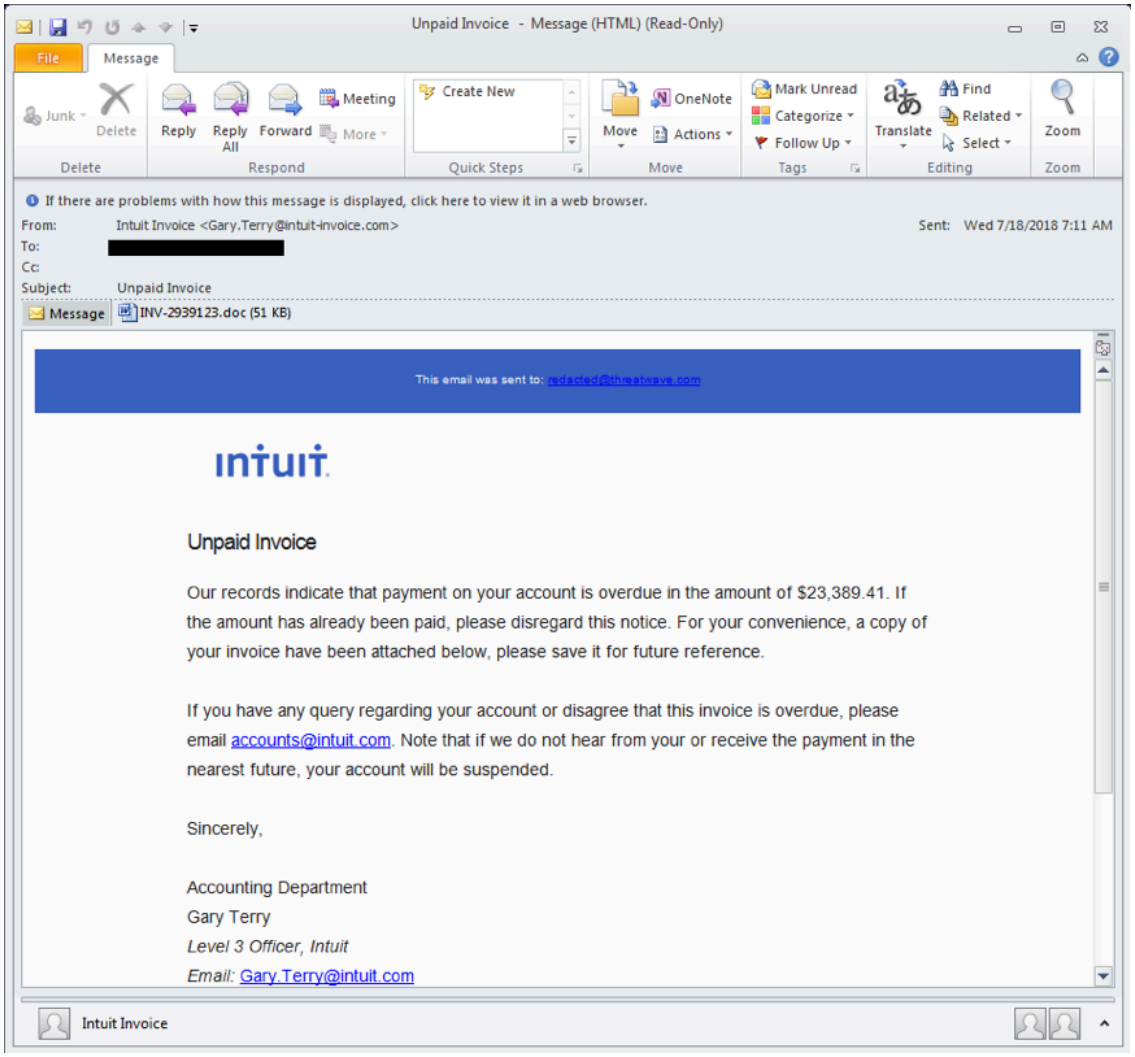
Symptoms

The endpoint user will not notice any symptoms of a Trickbot infection. However, a network admin will likely see changes in traffic or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with Trickbot's command and control infrastructure to exfiltrate data and receive tasks.

Trojan.TrickBot gains persistence by creating a Scheduled Task.

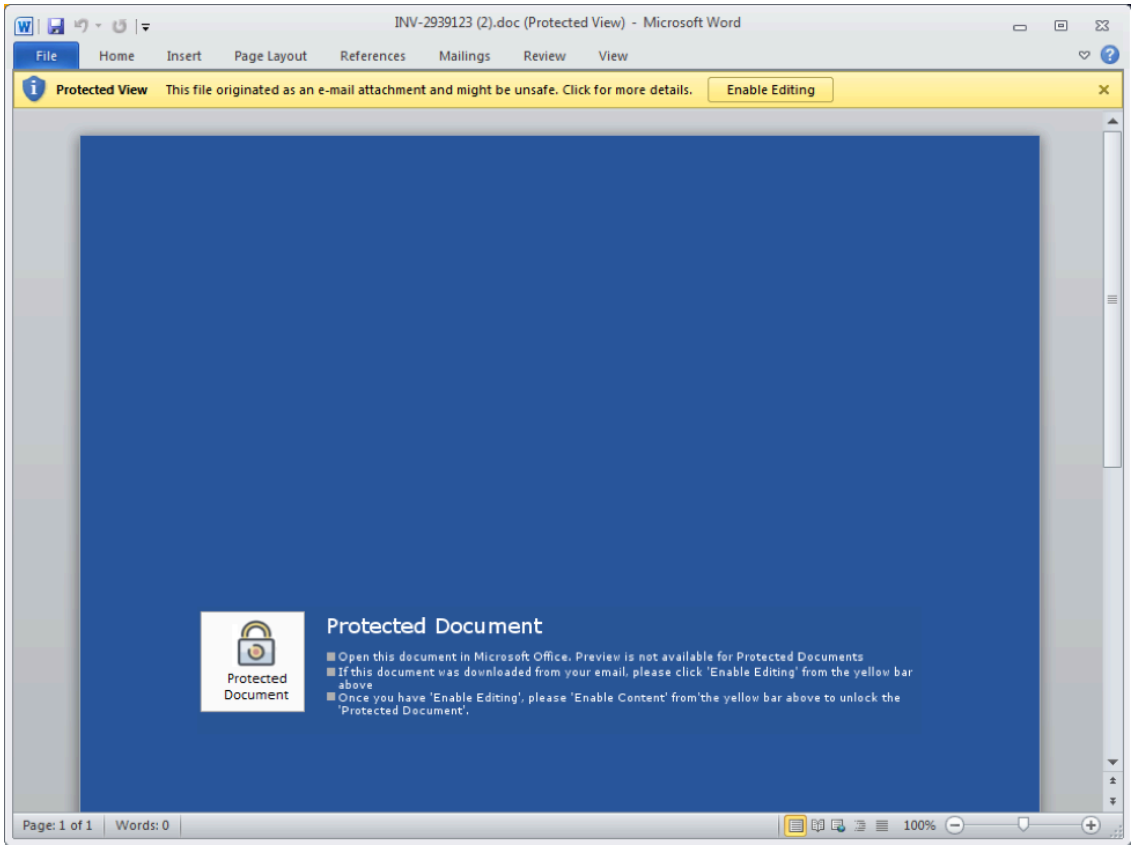


Type and source of infection



Example malspam distributing Trickbot

Other methods of propagation include infected attachments and embedded URLs. Trojan.TrickBot is also seen as a secondary infection dropped by Trojan.Emotet.



Malicious document with macro

Source: https://blog.malwarebytes.com/detections/trojan-trickbot/