NetTraveler

By Contributors to Wikimedia projects

Published: 2017-07-04 · Archived: 2026-04-05 19:27:49 UTC

From Wikipedia, the free encyclopedia

NetTraveler or **TravNet** is spyware that dates from 2004 and that has been actively used at least until 2016, infecting hundreds of often high-profile servers in dozens of countries.[1]

The name of this malware is based on the fact that early versions of it contained the string "NetTraveler is Running!". It is used by attackers for advanced persistent threats to survey their victims. It can transfer large amounts of private information from systems of victims to C&C servers, functioning as a trojan horse and backdoor to these systems.[2][3]

Spear-phishing with Office documents like MS Word documents is used to infect vulnerable systems, targeting the CVE-2012-0158 and CVE-2010-3333 vulnerabilities.[2] The attackers use news articles that are relevant to their targets for their spear fishing.[1]

Kaspersky Lab found that certain victims that were infected with NetTraveler were also infected by Red October, although no direct relation with this malware was established. The multiple infections might be accounted for by the fact that these were high-profile victims like government agencies, nuclear power installations and embassies in dozens of countries.[4]

Command and Control servers that were involved in NetTraveler attacks were located in the United States, Hong Kong and China, which used more than 100 URLs. These C&C servers mostly ran IIS 6/7.

According to Kaspersky Lab, NetTraveler is *used by a medium-sized threat actor group from China.*

There are several ways to get rid of NetTraveler on an infected system, like with Virus Removal Tools and the SpyHunter Removal Tool. It is also possible to remove this malware manually.[3]

Specially targeted countries included Russia, India, Pakistan, Mongolia, Kyrgyzstan and Kazakhstan.[5]

1. ^ Jump up to: *a* *b* *"NetTraveler APT Targets Russian, European Interests"*. *Proofpoint. July 7, 2016. Archived from the original on April 23, 2017.*
2. ^ Jump up to: *a* *b* *"The NetTraveler (a.k.a. 'Travnet')"* *(PDF). Kaspersky Lab. Archived (PDF) from the original on November 16, 2017.*
3. ^ Jump up to: *a* *b* *"How to Remove NetTraveler Completely From Your PC?"*. *pc-remover.com.* {{cite web}} : CS1 maint: deprecated archival service (link)
4. ^ *Constantin, Lucian. "Cyberespionage campaign 'NetTraveler' siphoned data from hundreds of high-profile targets". CSO Online. Retrieved 2018-03-29.*

5. ^ *"Kaspersky Lab Uncovers 'Operation NetTraveler,' a Global Cyberespionage Campaign Targeting Government-Affiliated Organizations and Research Institutes"*. *kaspersky.com. 26 May 2021.*

- The NetTraveler (aka ‘Travnet’) by Global Research and Analysis Team of Kaspersky Lab

---

Source: https://en.wikipedia.org/wiki/NetTraveler