NetTraveler Gets a Makeover for 10th Anniversary

By Kaspersky

Published: 2014-08-27 · Archived: 2026-04-05 18:36:14 UTC

Kaspersky Lab has observed a rise in attacks with an updated version of the “red star” APT backdoor

Kaspersky Lab has observed a rise in attacks with an updated version of the “red star” APT backdoor.

In 2014 the actors behind global cyberespionage campaign “Operation NetTraveler” celebrate ten years of activity. Although the earliest samples appeared to have been compiled in 2005, certain indicators point to 2004 as the year when the malicious activity started. For 10 years, NetTraveler has targeted more than 350 high-profile victims in 40 countries. This year Kaspersky Lab observed an uptick in the number of attacks against Uyghur and Tibetan supporters using an updated version of the NetTraveler backdoor with a new encryption scheme. During the investigation, Kaspersky Lab discovered seven C&C servers located in Hong Kong and one – in the USA.

Recent NetTraveler victims by industries

Most recently, the main focus of interest for cyber-espionage activities revolved around diplomatic (32%), government (19%), private (11%), military (9%), industrial and infrastructure (7%), airspace (6%), research (4%), activism (3%), financial (3%), IT (3%), health (2%) and press (1%).

Infection method: a “newer” backdoor

Traditionally for this malicious group, the attacks started with spear-phishing e-mails targeted activists. The e-mail had two attachments, a non-malicious JPG file and a Microsoft Word .DOC file appeared to be a container with an exploit for the CVE-2012-0158 vulnerability for Microsoft Office. Kaspersky Lab determined that this malicious web archive file has been created on a system using Microsoft Office - Simplified Chinese.

If run on a vulnerable version of Microsoft Office, the exploit drops the main module – Trojan-Spy. The malware configuration file has a slightly new format compared to “older” NetTraveler samples. Obviously, the developers behind NetTraveler have taken steps to try to hide the malware’s configuration.

After the successful injection, NetTraveler exfiltrates common file types such as DOC, XLS, PPT, RTF and PDF.

The discovered C&C servers

Kaspersky Lab identified several command-and-control (C&C) servers. Seven out of eight malicious C&C servers were registered by Shanghai Meicheng Technology, and the IPs are located in Hong Kong (Trillion Company, Hongkong Dingfengxinhui Bgp Datacenter, Sun Network Limited and Hung Tai International Holdings), while the one was registered by Todaynic.com Inc with IP located in the USA (Integen Inc). Kaspersky Lab’s experts recommend blocking all malicious hosts in the firewall.

"While investigating the NetTraveler attacks, we calculated the amount of stolen data stored on NetTraveler's C&C servers to be more than 22 gigabytes. This is an ongoing cyber-espionage campaign and, according to the last attacks against the activists, it will probably stay this way perhaps for another ten years. The most sophisticated threats appeared on surgical table of IT security companies not that long ago, but NetTraveler example shows that a disease could persist out of radar for long time". - says Kurt Baumgartner, Principal Security Researcher at Kaspersky Lab.

Recommendations on how to stay safe from updated NetTraveler malware

- Block the mentioned hosts in your firewall
- Update Microsoft Windows and Microsoft Office to the latest versions.
- Be wary of clicking on links and opening attachments from unknown persons.
- Use a secure browser such as Google Chrome, which has a faster development and patching cycle than Microsoft's Internet Explorer.

Kaspersky Lab's products detect and neutralize the malicious programs and its variants used by the NetTraveler Toolkit, including ***Trojan-Dropper.Win32.Agent.lifr****,* Trojan-Spy.Win32.TravNet, ***Trojan-Spy.Win32.TravNet.qfr, Trojan.BAT.Tiny.b*** *and* Downloader.Win32.NetTraveler.

Kaspersky Lab's products detect the Microsoft Office exploits used in the spear-phishing attacks, including Exploit.MSWord.CVE-2010-333, Exploit.Win32.CVE-2012-0158, ***Exploit.MSWord.CVE-2012-0158.db***..

To learn more about the NetTraveler operation, please read the blog post available at Securelist.com.

Cyberthreat real-time map

Additional reading

- NetTraveler APT Gets A Makeover For 10th Birthday
- "NetTraveler is Running!" - Red Star APT Attacks Compromise High-Profile Victims
- NetTraveler Is Back: The 'Red Star' APT Returns With New Tricks

---