“NetTraveler is Running!” – Red Star APT Attacks Compromise High-Profile Victims

securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/

Authors

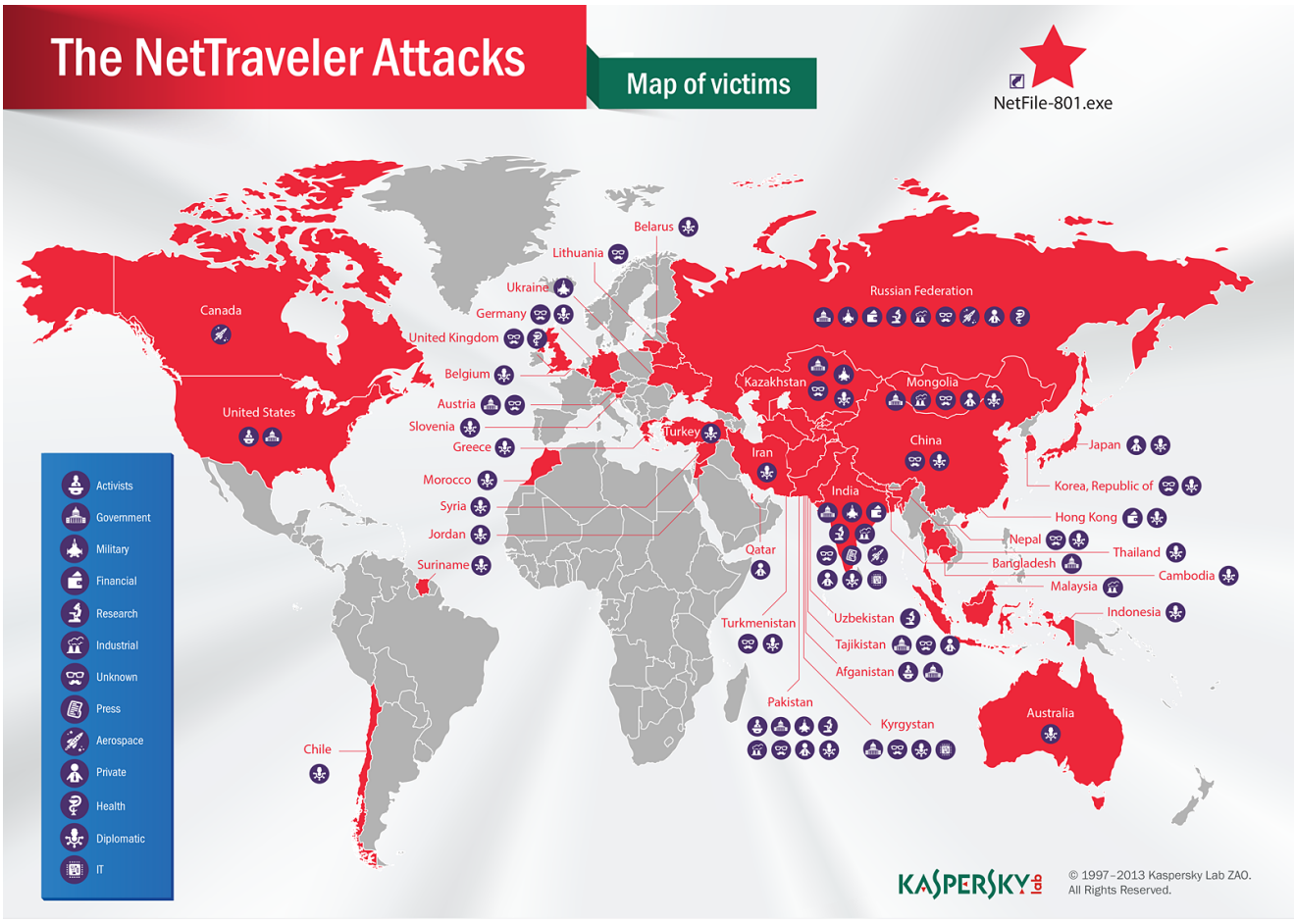
Expert GReAT

Over the last few years, we have been monitoring a cyber-espionage campaign that has successfully compromised more than 350 high profile victims in 40 countries. The main tool used by the threat actors during these attacks is NetTraveler, a malicious program used for covert computer surveillance.

The name NetTraveler comes from an internal string which is present in early versions of the malware: NetTraveler Is Running! This malware is used by APT actors for basic surveillance of their victims. Earliest known samples have a timestamp of 2005, although references exist indicating activity as early as 2004. The largest number of samples we observed were created between 2010 and 2013.

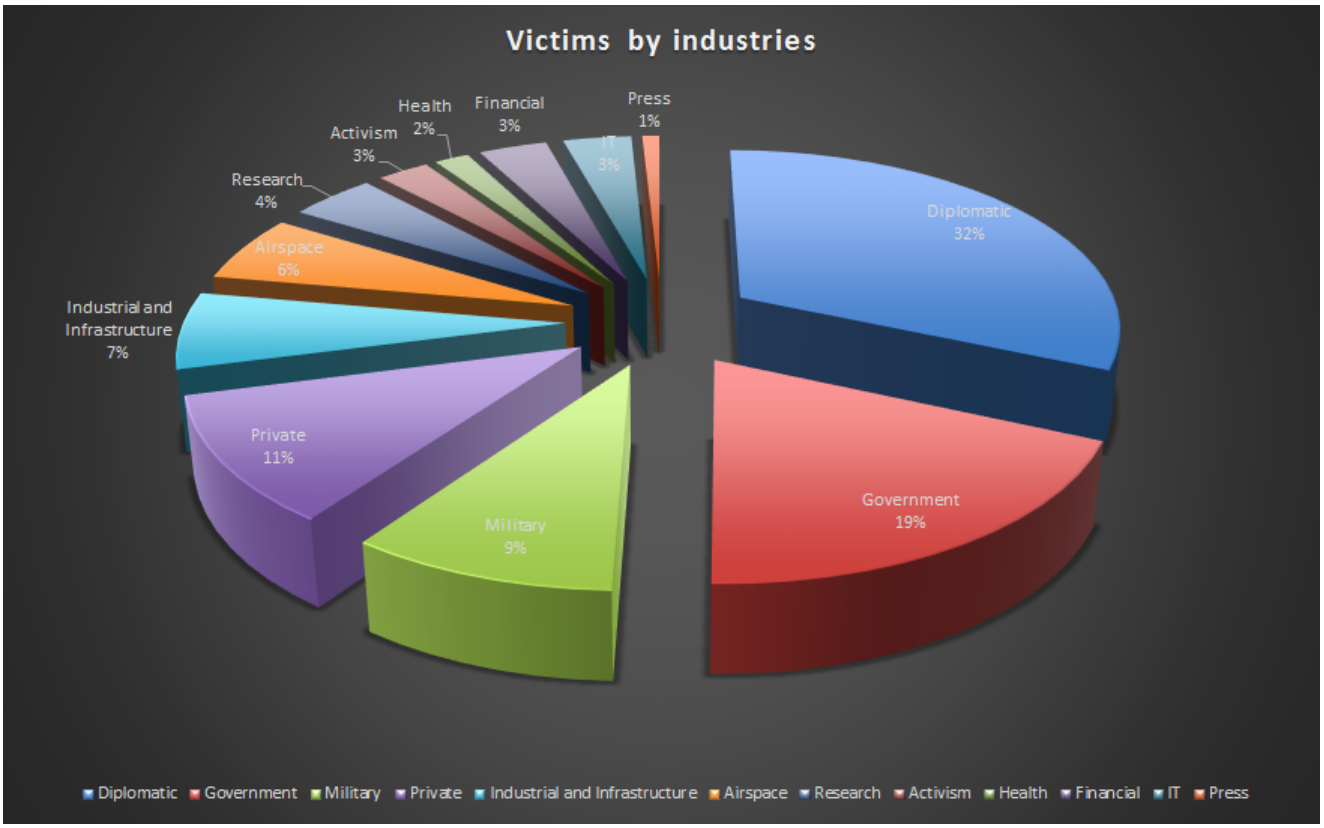
The NetTraveler builder icon

Known targets of NetTraveler (also known as Travnet or Netfile) include Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors:



The NetTraveler victims map

The following map lists the victim profiles by industry:



Note: this chart does not include the victims that couldnt be identified.

Key findings on the NetTraveler attacks:

- The highest number of infections was located in Mongolia, followed by India and Russia. In total, infections were identified in 40 countries including Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain, Germany, the United States, Canada, the United Kingdom, Chile, Morocco, Greece, Belgium, Austria, Ukraine, Lithuania, Belarus, Australia, Hong Kong, Japan, China, Iran, Turkey, Pakistan, Thailand, Qatar, and Jordan.
- The group has infected victims across multiple industries including government institutions, embassies, oil and gas industry, research institutes, military contractors and activists.
- Most recently, the NetTraveler groups main domains of interest for cyber-espionage activities include space exploration, nanotechnology, energy production, nuclear power, lasers, medicine and communications.
- During our research, we identified six victims that had been infected by both NetTraveler and Red October.

- Kaspersky Labs products detect and neutralize the malicious programs and its variants used by the NetTraveler Toolkit, including Trojan-Spy.Win32.TravNet and Downloader.Win32.NetTraveler. Kaspersky Labs products detect the three Microsoft Office exploits used in the spear-phishing attacks, including Exploit.MSWord.CVE-2010-3333, Exploit.Win32.CVE-2012-0158.

Based on collected intelligence, we estimate the group size to about 50 individuals, most of which speak Chinese natively and have working knowledge of the English language NetTraveler is designed to steal sensitive data as well as log keystrokes, and retrieve file system listings and various Office or PDF documents.

The NetTraveler Attacks – Part 1 (public):

- Executive summary
- Attack analysis
- C&C infrastructure
- Statistics
- Mitigation
- Conclusions

For more information, read our full paper TheNetTravelerAttacks, Part 1 [PDF]

- APT
- Cyber espionage
- NetTraveler
- Targeted attacks
- Vulnerabilities

Authors

GReAT

“NetTraveler is Running!” – Red Star APT Attacks Compromise High-Profile Victims

---

Your email address will not be published. Required fields are marked *