Kaspersky Lab Uncovers ‘Operation NetTraveler,’ a Global Cyberespionage Campaign Targeting Government-Affiliated Organizations and Research Institutes

kaspersky.com/about/press-releases/2013_kaspersky-lab-uncovers--operation-nettraveler--a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes

May 26, 2021

Malicious NetTraveler Toolkit Infects 350 High-Profile Victims for Data Theft and Surveillance

Today Kaspersky Lab’s team of experts published a new research report about NetTraveler, which is a family of malicious programs used by APT actors to successfully compromise more than 350 high-profile victims in 40 countries. The NetTraveler group has infected victims across multiple establishments in both the public and private sector including government institutions, embassies, the oil and gas industry, research centers, military contractors and activists.

According to Kaspersky Lab’s report, this threat actor has been active since as early as 2004; however, the highest volume of activity occurred from 2010 – 2013. Most recently, the NetTraveler group’s main domains of interest for cyberespionage activities include space exploration, nanotechnology, energy production, nuclear power, lasers, medicine and communications.

Infection Methods:

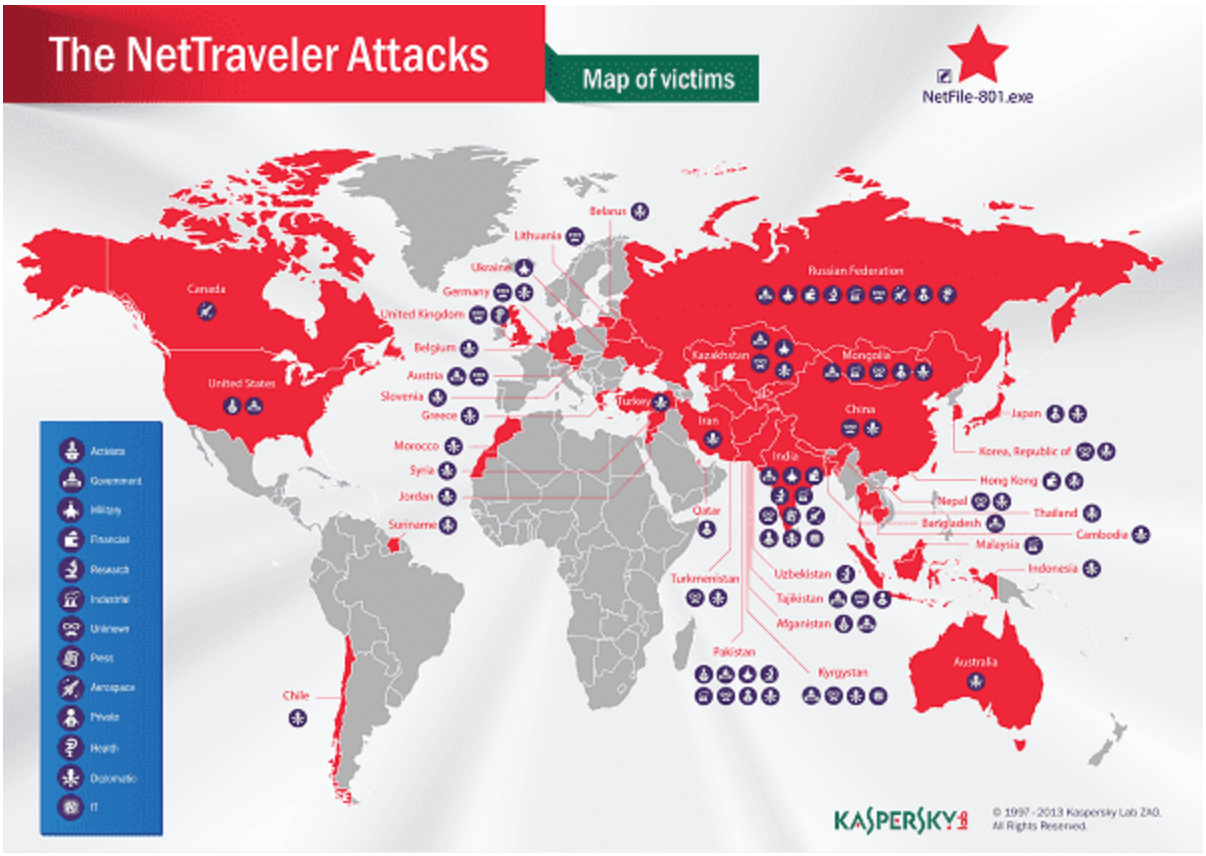
- Attackers infected victims by sending clever spear-phishing emails with malicious Microsoft Office attachments that are rigged with two highly exploited vulnerabilities (CVE-2012-0158 and CVE-2010-3333). Even though Microsoft already issued patches for these vulnerabilities they're still widely used for exploitation in targeted attacks and have proven to be effective.
- The titles of the malicious attachments in the spear-phishing emails depict the NetTraveler group's dogged effort of customizing their attacks in order to infect high-profile target. Notable titles of malicious documents include:
    - Army Cyber Security Policy 2013.doc
    - Report - Asia Defense Spending Boom.doc
    - Activity Details.doc
    - His Holiness the Dalai Lama's visit to Switzerland day 4
    - Freedom of Speech.doc

Data Theft & Exfiltration:

- During Kaspersky Lab's analysis, its team of experts obtained infection logs from several of NetTraveler's command and control servers (C&C). C&C servers are used to install additional malware on infected machines and exfiltrate stolen data. Kaspersky Lab's experts calculated the amount of stolen data stored on NetTraveler's C&C servers to be more than 22 gigabytes.
- Exfiltrated data from infected machines typically included file system listings, keyloggs, and various types of files including PDFs, excel sheets, word documents and files. In addition, the NetTraveler toolkit was able to install additional info-stealing malware as a backdoor, and it could be customized to steal other types of sensitive information such as configuration details for an application or computer-aided design files.

Global Infection Statistics:

- Based on Kaspersky Lab's analysis of NetTraveler's C&C data, there were a total of 350 victims in 40 countries across including the United States, Canada, United Kingdom, Russia, Chile, Morocco, Greece, Belgium, Austria, Ukraine, Lithuania, Belarus, Australia, Hong Kong, Japan, China, Mongolia, Iran, Turkey, India, Pakistan, South Korea, Thailand, Qatar, Kazakhstan, and Jordan.
- In conjunction with the C&C data analysis, Kaspersky Lab's experts used the Kaspersky Security Network (KSN) to identify additional infection statistics. The top ten countries with victims detected by KSN were Mongolia followed by Russia, India, Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain and Germany.



Additional Findings

> During Kaspersky Lab's analysis of NetTraveler, the company's experts identified six victims that had been infected by both NetTraveler and Red October, which was another cyberespionage operation analyzed by Kaspersky Lab in January 2013. Although no direct links between the NetTraveler attackers and the Red October threat actors were observed, the fact that specific victims were infected by both of these campaigns indicates that these high-profile victims are being targeted by multiple threat actors because their information is a valuable commodity to the attackers.

To read Kaspersky Lab's full research analysis, including indicators of compromise, remediation techniques and details of NetTraveler and its malicious components, please visit Securelist.

Kaspersky Lab's 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 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****.*

Kaspersky
Malicious NetTraveler Toolkit Infects 350 High-Profile Victims for Data Theft and Surveillance

kaspersky