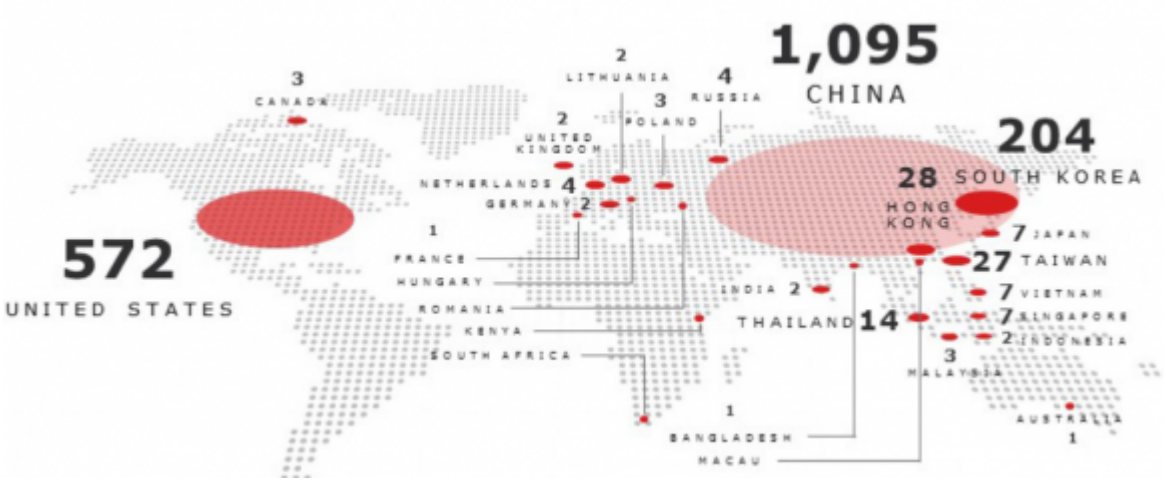
Chinese VPN Service as Attack Platform?

Published: 2015-08-04 · Archived: 2026-04-05 23:09:05 UTC

Hardly a week goes by without a news story about state-sponsored Chinese cyberspies breaking into Fortune 500 companies to steal intellectual property, personal data and other invaluable assets. Now, researchers say they've unearthed evidence that some of the same Chinese hackers also have been selling access to compromised computers within those companies to help perpetrate future breaches.

The so-called "Great Firewall of China" is an effort by the Chinese government to block citizens from accessing specific content and Web sites that the government has deemed objectionable. Consequently, many Chinese seek to evade such censorship by turning to virtual private network or "VPN" services that allow users to tunnel their Internet connections to locations beyond the control of the Great Firewall.



Security experts at **RSA Researc**h say they've identified an archipelago of Chinese-language virtual private network (VPN) services marketed to Chinese online gamers and those wishing to evade censorship, but which also appear to be used as an active platform for launching attacks on non-Chinese corporations while obscuring the origins of the attackers.

Dubbed by RSA as "Terracotta VPN" (a reference to the Chinese Terracotta Army), this satellite array of VPN services "may represent the first exposure of a PRC-based VPN operation that maliciously, efficiently and rapidly enlists vulnerable servers around the world," the company said in a report released today.

The hacker group thought to be using Terracotta to launch and hide attacks is known by a number of code names, including the "Shell_Crew" and "Deep Panda." Security experts have tied this Chinese espionage gang to some of the largest data breaches in U.S. history, including the recent attack on the U.S. Office of Personnel Management, as well as the breaches at U.S. healthcare insurers Anthem and Premera.

According to RSA, Terracotta VPN has more than 1,500 nodes around the world where users can pop up on the Internet. Many of those locations appear to be little more than servers at Internet service providers in the United States, Korea, Japan and elsewhere that offer cheap virtual private servers.

But RSA researchers said they discovered that many of Terracotta's exit nodes were compromised Windows servers that were "harvested" without the victims' knowledge or permission, including systems at a Fortune 500 hotel chain; a hi-tech manufacturer; a law firm; a doctor's office; and a county government of a U.S. state.

The report steps through a forensics analysis that RSA conducted on one of the compromised VPN systems, tracking each step the intruders took to break into the server and ultimately enlist the system as part of the Terracotta VPN network.

"All of the compromised systems, confirmed through victim-communication by RSA Research, are Windows servers," the company wrote. "RSA Research suspects that Terracotta is targeting vulnerable Windows servers because this platform includes VPN services that can be configured quickly (in a matter of seconds)."

RSA says suspected nation-state actors have leveraged at least 52 Terracotta VPN nodes to exploit sensitive targets among Western government and commercial organizations. The company said it received a specific report from a large defense contractor concerning 27 different Terracotta VPN node Internet addresses that were used to send phishing emails targeting users in their organization.

"Out of the thirteen different IP addresses used during this campaign against this one (APT) target, eleven (85%) were associated with Terracotta VPN nodes," RSA wrote of one cyber espionage campaign it investigated. "Perhaps one of the benefits of using Terracotta for Advanced Threat Actors is that their espionage related network traffic can blend-in with 'otherwise-legitimate' VPN traffic."

DIGGING DEEPER

RSA's report includes a single screen shot of software used by one of the commercial VPN services marketed on Chinese sites and tied to the Terracotta network, but for me this was just a tease: I wanted a closer look at this network, yet RSA (or more likely, the company's lawyers) carefully omitted any information in its report that would make it easy to locate the sites selling or offering the Terracotta VPN.

RSA said the Web sites advertising the VPN services are marketed on Chinese-language Web sites that are for the most part linked by common domain name registrant email addresses and are often hosted on the same infrastructure with the same basic Web content. Along those lines, the company did include one very useful tidbit in its report: A section designed to help companies detect servers that may be compromised warned that any Web servers seen phoning home to **8800free[dot]info** should be considered hacked.

A lookup at Domaintools.com for the historic registration records on 8800free[dot]info show it was originally registered in 2010 to someone using the email address "**xnt50@163.com**." Among the nine other domains registered to xnt50@163.com is **517jiasu[dot]cn,** an archived version of which is available here.

Domaintools shows that in 2013 the registration record for 8800free[dot]info was changed to include the email address "**jzbb@foxmail.com."** Helpfully, that email was used to register at least 39 other sites, including quite a few that are or were at one time advertising similar-looking VPN services.

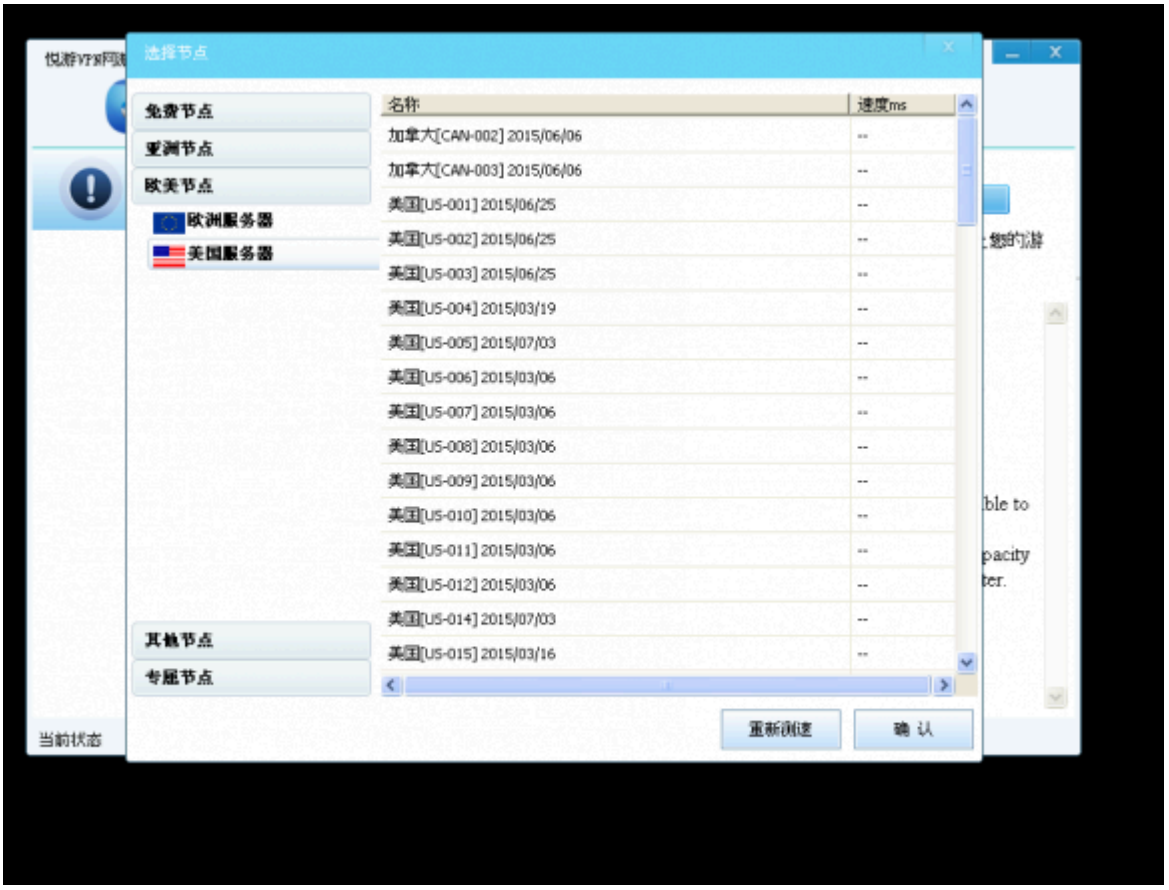
Pivoting off the historic registration records for many of those sites turns up a long list of VPN sites registered to other interesting email addresses, including "adsyb@163.com," "asdfyb@hotmail.com" and "itjsq@qq.com" (click the email addresses for a list of domains registered to each).

Armed with lists of dozens of VPN sites, it wasn't hard to find several sites offering different VPN clients for download. I installed each on a carefully isolated virtual machine (don't try this at home, kids!). Here's one of those sites:

A Google-translated version of one of the sites offering the VPN software and service that RSA has dubbed "Terracotta."

All told, I managed to download, install and use at least three VPN clients from VPN service domains tied to the above-mentioned email addresses. The Chinese-language clients were remarkably similar in overall appearance and function, and listed exit nodes via tabs for several countries, including the Canada, Japan, South Korea and the United States, among others. Here is one of the VPN clients I played with in researching this story:

This one was far more difficult to use, and crashed repeatedly when I first tried to take it for a test drive:



None of the VPN clients I tried would list the Internet addresses of the individual nodes. However, each node in the network can be discovered simply by running some type of network traffic monitoring tool in the background (I used Wireshark), and logging the address that is pinged when one clicks on a new connection.

RSA said it found more than 500 Terracotta servers that were U.S. based, but I must have gotten in on the fun after the company started notifying victim organizations because I found only a few dozen U.S.-based hosts in any of the VPN clients I checked. And most of the ones I did find that were based in the United States appeared to be virtual private servers at a handful of hosting companies.

The one exception I found was a VPN node tied to a dedicated Windows server for the Web site of a company in Michigan that manufactures custom-made chairs for offices, lounges and meeting rooms. Contacted by KrebsOnSecurity, the company confirmed that its serve was infected and beaconing home to the control servers described in the RSA report.

In addition to the U.S.-based hosts, I managed to step through a huge number of systems based in South Korea. I didn't have time to look through each record to see whether any of the Korean exit nodes were interesting, but here's the list I came up with in case anyone is interested. I simply haven't had time to look at and look up the rest of the clients in what RSA is calling the Terracotta network. Here's a more simplified list of just the organizational names attached to each record.

Assuming RSA's research is accurate (and I have no reason to doubt that it isn't) the idea of hackers selling access to hacked PCs for anonymity and stealth online is hardly a new one. In Sept. 2011, I wrote about how the Russian cybercriminals responsible for building the infamous TDSS botnet were selling access to computers sickened with

the malware via a proxy service called AWMProxy, even allowing customers to pay for the access with PayPal, Visa and MasterCard.

It is, after all, incredibly common for malicious hackers to use systems they've hacked to help perpetrate future cybercrimes – particularly espionage attacks. A classified map of the United States obtained by NBC last week showing the victims of Chinese cyber espionage over the past five years lights up like so many exit nodes in a VPN network.

Source: NBC

Update, 2:34 p.m. ET: Updated the story to note that I heard back from the furniture company victim named in the story, and that the company was able to confirm a breach of its servers by this VPN service.

Source: https://krebsonsecurity.com/2015/08/chinese-vpn-service-as-attack-platform/