EIN PRESSWIRE

China affiliated ISPs in the U.S. Create Beachhead for North Korean Cyber Attacks Against U.S. Assets

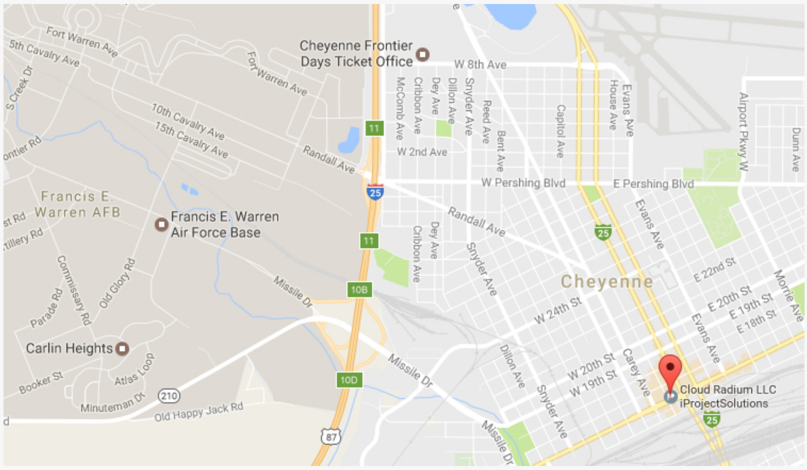
Leaked NSA Cyber Weapons that exploit SMB Port 445 Vulnerabilities have almost a half million easy targets within U.S. Borders, Some Near Nuclear Launch Bases!

Cyber Security Researcher & Noted Computer Forensics Expert @ leeneubecker.com

CHICAGO, IL, USA, May 23, 2017 /EINPresswire.com/ -- Cyber Security Firm Symantec reported yesterday that it was "highly likely" a hacking group connected to North Koreas was behind the recent Wanna Cry Malware attacks that impacted Countries around the globe. Cyber Security researcher and noted computer forensics expert Lee Neubecker performed analysis this week on U.S. based Internet Service Providers, including web hosts, that appear to have the greatest vulnerability to the recently leaked NSA Double Pulsar Server Message Block SMB Port 445 exploit. The vulnerability allows a remote attacker to take over a target without needing the target to perform any action. Wanna Cry utilized some of the leaked NSA exploit within its code. Any unpatched computer that has port 445 open is at risk if it can be seen by another attacker.

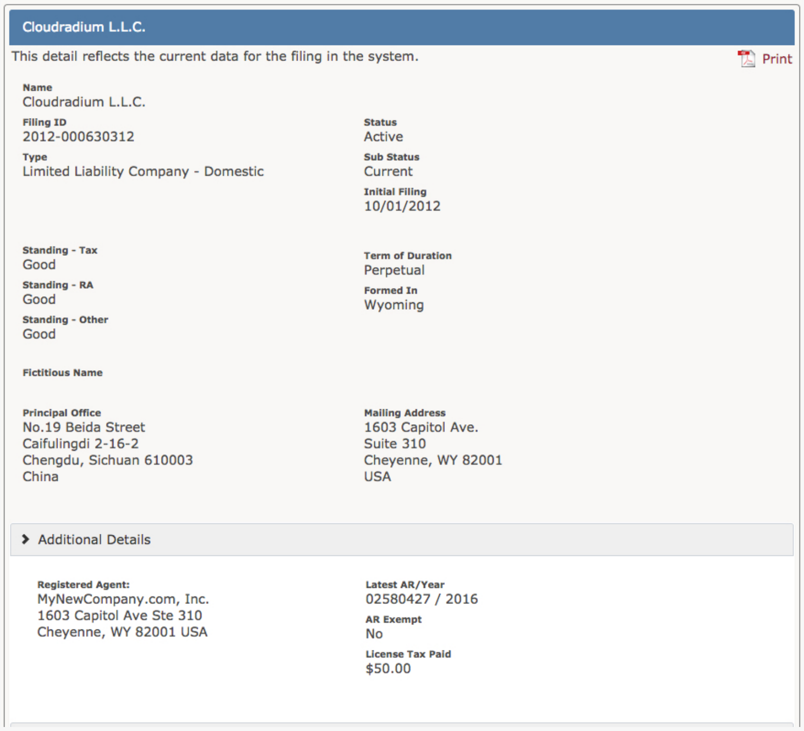
> “I am concerned that so many ISPs have not followed US-CERT recommended instructions in blocking port 445, potentially leaving our nation's cyber security at great risk.”
>
> *Lee Neubecker*

Neubecker summarized some of his findings posted to his blog by stating, "I performed a search last week of publicly exposed computers on the vulnerability search engine shodan.io and discovered almost a half a million computers vulnerable to port 445 attacks. I later learned that the number 2 most vulnerable City to the leaked NSA exploit was Cheyenne Wyoming. Upon further investigation, I discovered a single company named CloudRadium LLC responsible for most of the attack surface within Cheyenne. The CloudRadium LLC business registration indicates the company is Chinese owned and was first registered with the Wyoming Secretary of State in October of 2012. This one company has the equivalent of 35,000 plus zombie like computers vulnerable for take over and happens to be based within near field communication distance to the nearby Francis E. Warren Air Force Base that includes the 90th Missile Wing. The nearby U.S. military base is equipped with Intercontinental LGM-30G Minuteman III Missiles and serves as the U.S. Air Force's Global Strike Command. These computers could be exploited by anyone around the world with knowledge of how to carry out the exploit that has been publicly leaked for around two months now."



Map showing close proximity of CloudRadium to U.S. Air Force Nuclear Launch Base

The Most Vulnerable Cities as of today are:
1. Los Angeles, California
2. Cheyenne, Wyoming
3. Thousand Oaks, California
4. Phoenix, Arizona
5. Buffalo, New York
6. San Jose, California
7. Burbank, California
8. Ashburn, Virginia
9. Dallas, Texas
10. Chicago, Illinois



Cloudradium L.L.C.

This detail reflects the current data for the filing in the system.

Name Cloudradium L.L.C.	
Filing ID 2012-000630312	**Status** Active
Type Limited Liability Company - Domestic	**Sub Status** Current
	Initial Filing 10/01/2012
Standing - Tax Good	**Term of Duration** Perpetual
Standing - RA Good	**Formed In** Wyoming
Standing - Other Good	
Fictitious Name	
Principal Office No.19 Beida Street Caifulingdi 2-16-2 Chengdu, Sichuan 610003 China	**Mailing Address** 1603 Capitol Ave. Suite 310 Cheyenne, WY 82001 USA

> Additional Details

Registered Agent: MyNewCompany.com, Inc. 1603 Capitol Ave Ste 310 Cheyenne, WY 82001 USA	**Latest AR/Year** 02580427 / 2016
	AR Exempt No
	License Tax Paid $50.00

State of Wyoming Secretary of State Business Registration for CloudRadium LLC

Last month, the City of Dallas was the target of a cyber attack that resulted in Tornado Warning Sirens screeching uncontrollably throughout the City. Workers had to manually shut off all of the sirens. Such an attack on infrastructure could easily take place with enough compromised computers throughout the City. Dallas still has over eight thousand computers that remain vulnerable to port 445 attacks, which could have easily been key to how last month's hack transpired.

A complete list of the Top 25 most vulnerable ISP's as of the 5/22/2017 data collection date and additional details relating to Neubecker's investigation is available at https://www.leeneubecker.com/china-us-isp-invasion/

Lee Neubecker
leeneubecker.com
202-830-0494
email us here

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.