FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

Potential APT30 Targeting against a Global Energy Company in India

Date: July 6th, 2015 **Tags:** apt30, india, backspace, energy-utilities, china, lecna, targeting

Summary

This past quarter, FireEye detected a new BACKSPACE variant at the India office of a global oil and gas service company that had previously entered into a joint venture with a major Chinese oil company and had supported oil exploitation in the South China Sea. It is possible this system was infected by APT30, a China-based threat group, given their exclusive use of this backdoor, but we haven't confirmed attribution. However, this activity aligns with APT30's prior targeting. It is unclear if this activity is new (as in, representative of APT30 activity but occurring subsequent to our public report on them) or is simply an older infection.

Activity Overview

BACKSPACE, also known as "Lecna," is a backdoor that appears to be used exclusively by APT30. Given that the system in question was located in India, this incident is consistent with APT30's previous targeting, which has focused predominantly on industry and government in Southeast Asia and India. APT30 typically relies on social engineering and tailored spear phishing e-mails to gain initial access to a system.

APT30 Targeting Advances Beijing's Priorities

This recent infection is consistent both with established patterns of APT30 targeting and with China's national priorities. APT30 has engaged in a highly targeted regionally-focused cyber espionage campaign. While using relatively consistent tools, tactics, and infrastructure for over a decade, APT30 has remained successful in acquiring sensitive data from a variety of targets. Although APT30's targeting has typically focused on sensitive information relative to regional political,

military, and economic issues, the group has also targeted a variety of industries, including aerospace, defense, energy, high-tech, and utilities. Among APT30's principle areas of focus has been the South China Sea dispute, as the group has engaged in extensive cyber espionage against rival claimants and actively targeted Association of Southeast Asian Nations meetings. Additionally, APT30 previously targeted a Southeast Asian oil company that had sought to develop oil blocks in the area.

APT30's targeting of this U.S.-based oil and gas services company appears to align closely with the Chinese government's current energy priorities. The company in question focuses on the sustainable development of energy resources and specializes in innovative technologies and techniques for drilling, including for the exploitation of shale gas and for use in deep waters. This company also had entered into a joint venture with a major Chinese oil company and had supported oil exploitation in the South China Sea.

China-based APT groups frequently target U.S. and international oil and gas production and services companies, coalmining companies, and power distribution companies. China is highly sensitive to its reliance on imported energy, particularly the extent of its dependence on the Middle East and vulnerability to naval blockade. Therefore, Beijing is seeking to expand and diversify its sources of energy, including through increasing the exploitation of domestic energy resources. For instance, the success of hydraulic fracturing (fracking) in the U.S. has piqued the interest of China's leadership, since the country possesses large reserves of natural gas that could potentially be exploited through fracking. Additionally, due to China's acute environmental problems, transitioning to more sustainable energy portfolio and increasing energy efficiency have become key objectives.

In this context of recent developments, this and similar energy companies could be particularly high-value targets. Beijing's interest in increasing its control over this sector is evident. The Chinese leadership has reportedly been exploring mergers among state-owned energy companies, in order to create national champions that could operate more efficiently and even take on major international oil companies.[1] In particular, China is highly interested in exploiting oil and gas in the South China Sea. Last May, China's first deep water drilling rig, the billion-dollar Haiyang Shiyou 981, was moved into waters claimed by Vietnam to explore for oil. Although the U.S. Energy Information Agency has estimated that the South China Sea could contain up to 11 billion barrels of oil and 190 trillion cubic feet of natural gas, the exploitation of these resources has been limited thus far by technological challenges, due to the limited expertise of China and other South China Sea claimants in deep water drilling.[2] Therefore, cutting-edge technologies and

techniques for the exploitation of oil and gas under these conditions would be especially of interest to Chinese oil companies.

Conclusion

Although further details on this likely APT30 infection are not yet available, this incident is a further indication of the longstanding trend of China-based APT groups' extensive targeting of companies in the energy sector. Due to China's prioritization of advancing energy security and enhancing sustainability, companies in this sector are likely to remain high-value targets for APT groups for the foreseeable future. In particular, companies that have developed efficient, cutting-edge means for the extraction, processing, and utilization of hydrocarbon resources could be seen as a potential source of critical technical knowledge.

1 Spegele, Brian and Lingling Wei. "China Considering Mergers Among Its Big State Oil Companies." *Wall Street Journal*. February 17, 2015. <http://www.wsj.com/articles/china-considering-mergers-among-its-big-state-oil-companies-1424176242>

2 Energy Information Agency. "South China Sea." February 7, 2013. <http://www.eia.gov/beta/international/regions-topics.cfm?RegionTopicID=SCS>