Report: Chinese government is behind a decade of hacks on software companies

By Dan Goodin

Published: 2018-05-05 · Archived: 2026-04-05 14:36:10 UTC

Kaspersky said it discovered ShadowPad through a referral from a partner in the financial industry that observed a computer used to perform transactions was making suspicious domain-name lookup requests. At the time, NetSarang tools were used by hundreds of banks, energy companies, and pharmaceutical manufacturers.

Opsec mistakes

ProtectWise said since the beginning of the year, members of Winnti have waged phishing attacks that attempt to trick IT workers in various organizations to turn over login credentials for accounts on cloud services such as Office 365 and G Suite. One campaign that ran for eight days starting on March 20 used Google's goo.gl link-shortening service allowed ProtectWise to use Google's analytics service to glean key details. An image of the message appears at the top of this post.

The service showed that the link was created on February 23, some three weeks before the campaign went live. It also showed the malicious phishing link had been clicked a total of 56 times: 29 times from Japan, 15 times from the US, two times from India, and once from Russia. Chrome browsers clicked on the link 33 times, and 23 clicks came from Safari users. Thirty clicks came from Windows computers, and 26 from macOS hosts.

Attackers who got access to targets' cloud services sought internal network documentation and tools for remotely accessing corporate networks. Attackers who succeed typically used automated processes to scan internal networks for open ports 80, 139, 445, 6379, 8080, 20022, and 30304. Those ports indicate an interest in Web, file storage services, and clients that use the Ethereum digital currency.

Most of the time, the attackers use their command-and-control servers to conceal their true IP addresses. In a few instances, however, the intruders mistakenly accessed the infected machines without such proxies. In all those cases, the block of IPs were 221.216.0.0/13, which belongs to the China Unicom Beijing Network in the Xicheng District.

"The attackers grow and learn to evade detection when possible but lack operational security when it comes to the reuse of some tooling," the report concluded. "Living off the land and adaptability to individual target networks allow them to operate with high rates of success. Though they have at times been sloppy, the Winnti umbrella and its associated entities remain an advanced and potent threat."
