Symantec Exposes Crackerjack Cybercriminal Group

By admin-ectnews

Published: 2013-09-17 · Archived: 2026-04-05 19:07:48 UTC

Symantec on Tuesday disclosed the existence of a group of 50 to 100 top-rate hackers.

Named “Hidden Lynx” after a string of code Symantec found in its command-and-control server communications, the group is an advanced persistent threat that has skills well ahead of similar organizations in the region, such as APT1, Symantec said.

“The Hidden Lynx group is methodical in its approach and leverages zero days quickly, most recently affecting Internet Explorer and Java, and have used three zero-day vulnerabilities since 2011,” Vikram Thakur, a researcher at Symantec Security Response, told TechNewsWorld.

However, Symantec’s claim that Hidden Lynx has skills superior to those of APT1 — which cybersecurity firm Mandiant has depicted as a unit of the People’s Liberation Army — is suspect, saidTaia Global CEO Jeffrey Carr.

If Symantec’s claim is true, it means we should be more concerned about a team of 50 Chinese hackers than the PLA,” he pointed out, “but “I think most analysts would suspect that the reverse is true.”

What Hidden Lynx Apparently Did

Hidden Lynx’s most notable attack was VOHO, Symantec said. That attack reportedly used watering hole tactics to infect nearly 1,000 businesses, government agencies and nonprofit organizations. The cybercriminals identified websites their intended victims visited regularly, seeded those sites with code redirecting them to poisoned servers that infected their computers, and then pounced on the information in the computers.

“The Hidden Lynx group continued to attack the defense industry post-VOHO,” Thakur pointed out. “In another campaign, named SCADEF, manufacturers and suppliers of military-grade computers were observed installing a Trojanized Intel driver application.”

Hidden Lynx steals intellectual property for a fee, Thakur said.

The Power of the Lynx

Hidden Lynx is divided into two teams Symantec has named after the malware they use, Thakur said.

Team Moudoor launches large-scale campaigns by distributing the backdoor Trojan Moudoor across several industries. Team Naid uses the backdoor Trojan Naid, and is reserved for more limited attacks against high-value targets.

Both Moudoor and Naid are reasonably well known Trojans but like other well-known malware, they are still in use because they remain effective, thanks to poor patching practices and outdated security software, said NSS Labs Research Director Randy Abrams.

“The most widespread threats are not necessarily the newest,” he told TechNewsWorld.

The Moudoor team uses that Trojan liberally without fear of being discovered because it lets the attackers grab some information swiftly — and, more importantly, serves as a smokescreen for the Naid attack, Symantec’s Thakur said.

Deconstructing the Lynx

The Hidden Lynx group pioneered the watering hole attack, according to Symantec.

“No, no, no — they ripped that off from adware and the advertising industry,” NSS Labs’ Abrams maintained. “Get ’em at the watering hole has been the strategy of advertising since before there were computers.”

The group’s command-and-control servers are hosted in China, “but we cannot confirm who is actually behind [it],” Symantec’s Thakur said.

It’s possible that cybercriminals from other countries have leased C&C servers in China.

Pointing to China could be simple misdirection. “Given the revelations of the NSA’s collusion with big players, it is not beyond the realm of believability that attribution to the Chinese serves a [U.S.] governmental purpose,” suggested NSS Labs’ Abrams.

As for Symantec’s report, “it’s a marketing piece rather than a serious research report,” Carr stated. “The authors don’t provide any evidence to support their conjecture regarding the number of teams involved or who they are.”

Protecting Against the Lynx

Multiple layers of security have to be used to protect against a targeted attack “and sometimes the defenses will still fail,” NSS Labs’ Abrams said.

“You need multiple levels of protection mechanisms — data loss prevention, encryption, network and endpoint security solutions are a few,” Symantec’s Thakur said.

“Security is a lot like a windshield,” Abrams remarked. “One small pit can spiderweb out and cause irreparable damage.”
