Stealing US business secrets: Experts ID two huge cyber 'gangs' in China

By Mark Clayton

Archived: 2026-04-05 21:12:42 UTC

Sneaky Panda. The Elderwood Gang. The Beijing Group.

These are three code names bestowed by US experts on a single cyberespionage organization that, from 9 to 5 Beijing time each day, is at work siphoning the crown jewels of US corporations' proprietary data out of their networks – and into computers in China.

In January 2010, Internet search giant Google disclosed that someone had hacked into its network (not to mention 20 other tech companies). That someone was the Elderwood Gang, says a new report by Symantec, a cybersecurity company.

The Symantec report hints at what other US cybersecurity experts are saying with increasing conviction: that Elderwood is one of two large Chinese economic cyberespionage organizations – employing perhaps hundreds of people – which are working to vacuum business ideas and advanced designs from American computer networks.

For example, these experts are now connecting Elderwood and a second Chinese hacking group to attacks on top cybersecurity company RSA, defense-industry giant Lockheed Martin, and perhaps several US natural gas pipeline companies.

It has long been claimed by US cybersecurity experts that cyberspying to harvest intellectual property, rather than quick cash from online bank accounts, was a practice emanating mostly from China. Plausible deniability remains because attribution is so uncertain in cyberspace. Chinese embassy officials in Washington routinely deny any responsibility for cyberespionage on US targets.

Yet there are signs now that the attribution problem is closer to being solved, US experts say.

"We're tracking over a dozen nation-state groups right now that are affiliated with China," says Dmitri Alperovitch, chief technology officer for CrowdStrike, a startup cybersecurity company focused on taking undisclosed "offensive" security measures. "We have a deep understanding of them and attribution down to the individual level. They're operating in China, and we're watching them. Even though they're unlikely be brought to justice in the US, we understand a lot today."

Among the 20 or so identifiable Chinese cyberespionage groups, the two that dwarf the others are the Elderwood Gang and the Comment Crew. The two have many different names, with researchers giving them different monikers. To Dell Secureworks cyber counterspy expert Joe Stewart, they are the Beijing Group and the Shanghai Group because of where their activities seem to originate. To Mr. Alperovitch of CrowdStrike, they are Sneaky Panda and Comment Panda.

Symantec called the first group “Elderwood” because the name appears in a source-code variable used by the attackers. In Google's case, the gang reportedly made off with at least some of the search company's source code – secret algorithms that have made it so successful. Nobody knows exactly how much was stolen from the networks of the other companies.

Today, 2-1/2 years later, Google has abandoned the Chinese market, but Elderwood is alive and doing quite well, its cyberspies busy as ever, the Symantec analysis shows. Second-tier defense industry suppliers that make electronic or mechanical components for top defense companies are the gang's specialty. Those firms then become a cyber "stepping stone to gain access to top-tier defense contractors," the report says.

But Elderwood's appetite for information is broad and its capacity far larger than the defense industry alone. So, in at least eight major "campaigns" in less than two years, the gang has slipped into the networks of US shipping, aeronautics, arms, energy, manufacturing, engineering, electronics, financial, and, of course, software companies, Symantec reports.

In most cases, Elderwood uses a convincing "spear-phishing" fake e-mail to fool an employee into clicking an infected e-mailed link or into opening a Trojan software-infected attachment that creates a digital backdoor for the cyberspies. In many cases, these attacks have utilized costly "zero-day" malware that takes advantage of a previously unknown flaw against which no defense exists. Such technology would sell for at least six figures on the cyber black market, leading many to conclude the group is exceedingly well funded.

Lately, however, Elderwood has taken to infecting legitimate websites frequented by employees of the target company – a so-called "water hole" attack, just as lions stake out a watering hole for their prey. Elderwood infects these less-secure sites with malware that downloads to a computer that clicks on the site. After that, the gang snoops inside the network to which the infected computer is connected, finding and finally downloading executives' e-mails and critical documents on company plans, decisions, acquisitions, and product designs.

"Victims are attacked, not for petty crime or theft, but for the wholesale gathering of intelligence and intellectual property," Symantec reports. "The resources required to identify and acquire useful information – let alone analyze that information – could only be provided by a large criminal organization, attackers supported by a nation state, or a nation state itself."

This sort of activity is hardly unknown to US cybersecurity experts, who have long dubbed it the "advanced persistent threat" – a euphemism taken to mean espionage threats originating from China. Mr. Stewart of Dell Secureworks has traced the activity of the Elderwood Gang (which he calls the Beijing Group) and the Comment Crew (which he calls the Shanghai Group) back to 2005-2006. He says they are responsible for perhaps 90 percent of all economic espionage against the US today.

"Both groups surface time and again in different reports you read," he says. "Someone discovers some malware and gives it a snazzy name. But it's all the same activity underneath."

Technical links – including IP addresses, domain names, malware signatures, and other technical factors – show Elderwood was behind the attack on Google, which is known as Operation Aurora, he says.

Stewart also ties Elderwood to other major hacks, including one against Tibetan activists – the "GhostNet" global cyberespionage network documented by University of Toronto Researchers in 2010 – and the major hack of RSA,

the Bedford, Mass., cybersecurity subsidiary of EMC corporation.

In 2010, Alperovitch of CrowdStrike was vice president of threat research for McAfee, the cybersecurity company that analyzed the Aurora intrusion at Google. He agrees with Stewart that the group behind Aurora is the same one that hacked RSA and later attempted to hack defense giant Lockheed Martin.

[**Editor's note:** *The original version of this story misidentified Mr. Alperovitch's role at McAfee.*]

In 2011, while still at McAfee, he went on to reveal Comment Crew (which he calls Comment Panda) operating alongside Elderwood. It's called that because the group so often uses a technique involving internal software "comment" features on web pages as a tool to infiltrate target computers.

Comment Crew, Alperovitch found, had infiltrated at least 72 organizations including defense companies, the International Olympic Committee, and the United Nations. He dubbed Comment Crew's campaign Operation ShadyRAT – "RAT" standing for "remote access tool," the name for malware used to control computer systems remotely.

Stewart then discovered a flaw in the malicious software used by the Operation ShadyRAT operators, and that allowed him to track back pilfered data to the perpetrators' computer addresses in Shanghai.

Both big hacker groups were involved in the RSA hack, he has concluded.

Evidence was already strong that at least one and perhaps both were involved in one of this year's major cyberespionage attacks – infiltrating the networks of US natural gas pipeline companies, an attack first reported by the Monitor in May.

Digital signatures, domain names, and other indicators used by the hackers in the RSA case, which were Chinese in origin, lined up with those in the pipeline case, experts told the Monitor at the time.

"The indicators DHS provided to hunt for the gas-pipeline attackers included several that, when we checked them, turned out to be related to those used by the perpetrators of the RSA attack," Robert Huber, co-founder of Critical Intelligence, an Idaho Falls, Idaho, security company told the Monitor at the time. "It makes it highly likely that the same actor was involved in both intrusions."

Stewart, who has spent the past 20 months cataloging the digital infrastructure of the two groups, is staggered by the number of personnel that must be involved. He has discovered hundreds of families of custom made malware, suggesting hundreds of employees and maybe even thousands – some hackers, but many more researchers that support their activities, as well as analysts to cull and process the stolen information.

It suggests a state-supported or at least state-tolerated institution of large and well-funded proportions. Supporting this conclusion, he says, is the fact that the pair of attackers routinely target entire industry groups, not just individual companies.

"Everyone that does cybersecurity for a living should know about these two groups," Stewart says. "It's taken about five years for experts to understand what's really going on – and it's pretty well understood now. But people in our industry don't share this kind of information very freely so it's hard to get up to speed. Just getting antivirus vendors to agree on a name would be a huge leap."