REUTERS/RICK WILKING

IN CYBERSPY VS. CYBERSPY, CHINA HAS THE EDGE

Hackers connected to the Chinese army have stolen terabytes of sensitive data from the United States and the attacks are multiplying.

BY BRIAN GROW AND MARK HOSENBALL
ATLANTA, APRIL 14

AS AMERICA AND CHINA grow more economically and financially intertwined, the two nations have also stepped up spying on each other. Today, most of that is done electronically, with computers rather than listening devices in chandeliers or human moles in tuxedos.

And at the moment, many experts believe China may have gained the upper hand.

Though it is difficult to ascertain the true extent of America's own capabilities and activities in this arena, a series of secret diplomatic cables as well as interviews with experts suggest that when it comes to cyber-espionage, China has leaped ahead of the United States.

"THE ATTACKS COMING OUT OF CHINA ARE NOT ONLY CONTINUING, THEY ARE ACCELERATING."

According to U.S. investigators, China has stolen terabytes of sensitive data -- from usernames and passwords for State Department computers to designs for multi-billion dollar weapons systems. And Chinese hackers show no signs of letting up. "The attacks coming out of China are not only continuing, they are accelerating," says Alan Paller, director of research at information-security training group SANS Institute in Washington, DC.

Secret U.S. State Department cables,

obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches -- colorfully code-named "Byzantine Hades" by U.S. investigators -- to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.

Privately, U.S. officials have long suspected that the Chinese government and in particular the military was behind the cyber-attacks. What was never disclosed publicly, until now, was evidence.

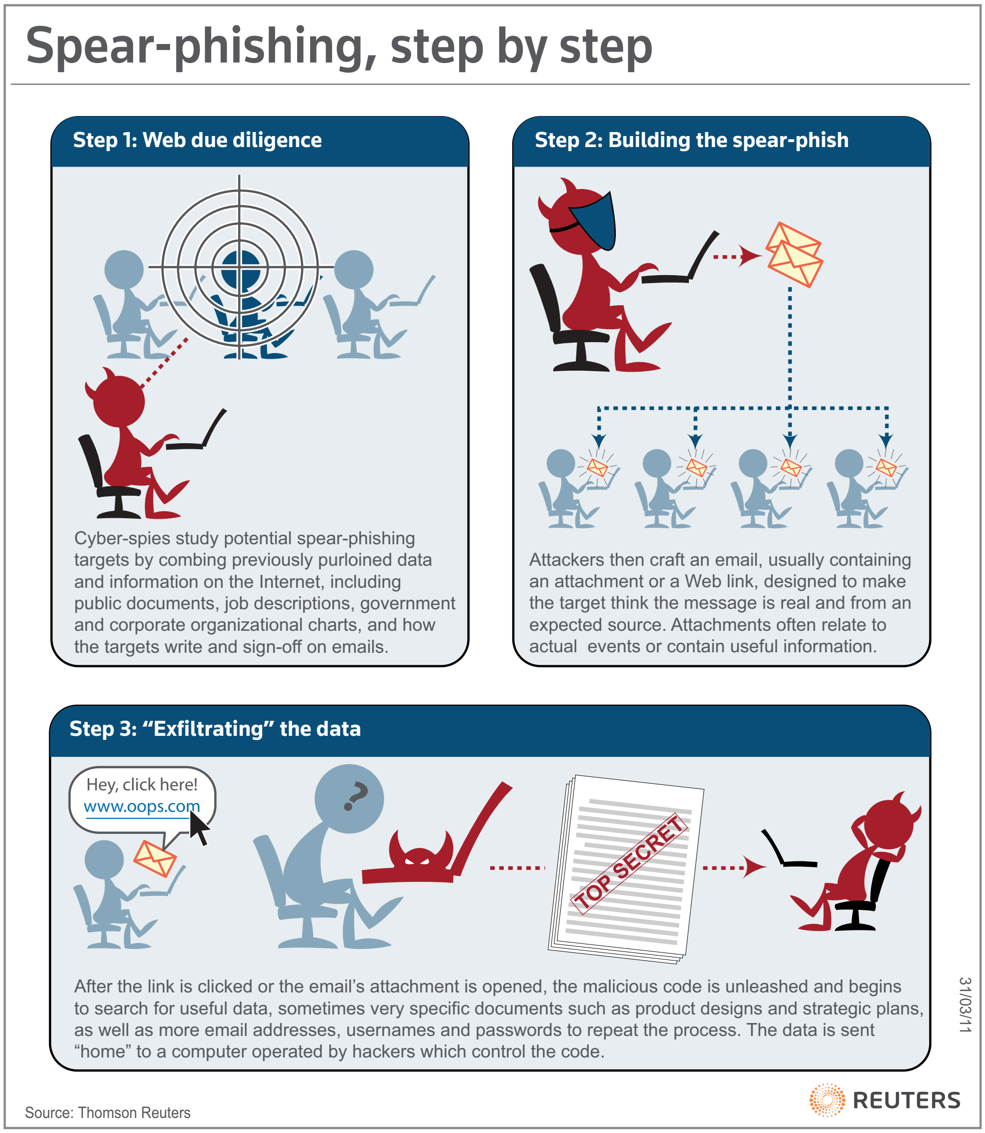
U.S. efforts to halt Byzantine Hades hacks are ongoing, according to four sources familiar with investigations. In the April 2009 cable, officials in the State Department's Cyber Threat Analysis Division noted that several Chinese-registered Web sites were "involved in Byzantine Hades intrusion activity in 2006."

The sites were registered in the city of Chengdu, the capital of Sichuan Province in central China, according to the cable. A person named Chen Xingpeng set up the sites using the "precise" postal code in Chengdu used by the People's Liberation Army Chengdu Province First Technical Reconnaissance Bureau (TRB), an electronic espionage unit of the Chinese military. "Much of the intrusion activity traced to Chengdu is similar in tactics, techniques and procedures to (Byzantine Hades) activity attributed to other" electronic spying units of the People's Liberation Army, the cable says.

Reconnaissance bureaus are part of the People's Liberation Army's Third Department, which oversees China's electronic eavesdropping, according to an October 2009 report by the U.S.-China Economic and Security Commission, a panel created by Congress to monitor potential national security issues related to U.S-China relations. Staffed with linguists and technicians, the Third Department monitors communications systems in China and abroad. At least six Technical Reconnaissance Bureaus, including the Chengdu unit, "are likely focused on defense or exploitation of foreign networks," the commission report states.

The precise relationship with the Chinese Army of suspected hacker Chen Xingpeng could not be immediately determined by Reuters. A spokesman for the Chinese embassy in Washington did not respond to multiple requests for comment. The U.S. State Department declined to comment.

But the leaked cables and other U.S.



Spear-phishing, step by step

Step 1: Web due diligence

Cyber-spies study potential spear-phishing targets by combing previously purloined data and information on the Internet, including public documents, job descriptions, government and corporate organizational charts, and how the targets write and sign-off on emails.

Step 2: Building the spear-phish

Attackers then craft an email, usually containing an attachment or a Web link, designed to make the target think the message is real and from an expected source. Attachments often relate to actual events or contain useful information.

Step 3: "Exfiltrating" the data

After the link is clicked or the email's attachment is opened, the malicious code is unleashed and begins to search for useful data, sometimes very specific documents such as product designs and strategic plans, as well as more email addresses, usernames and passwords to repeat the process. The data is sent "home" to a computer operated by hackers which control the code.

31/03/11

Source: Thomson Reuters

REUTERS

Reuters graphic/Stephen Culp

KEEPING TABS: Josh Mayeux, network defender, works at the Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado Springs, Colorado July 20, 2010. **REUTERS/RICK WILKING**

MODERN WARFARE: Medallions for (L-R) the U.S. Air Force, Air Force Space Command, Air Force Cyber Command and he Air Force Space Command Network Operations & Security Center (NOSC) are seen outside the NOSC at Peterson Air Force Base in Colorado Springs, Colorado July 20, 2010. **REUTERS/RICK WILKING**

government reports underscore how Chinese and other state-sponsored and private hackers have overwhelmed U.S. government computer networks. In the last five years, cyber-intrusions reported to the U.S. Computer Emergency Response Team, a unit of the Department of Homeland Security, have increased more than 650 percent, from 5,503 incidents in fiscal 2006 to 41,776 four years later, according to a March 16 report by the Government Accountability Office.

THE BUSINESS OF SPYING

THE OFFICIAL FIGURES don't account for intrusions into commercial computer networks, which are part of an expanding cyber-espionage campaign attributed to China, according to current and former U.S. national security officials and computer-security experts.

In the last two years, dozens of U.S. companies in the technology, oil and gas and financial sectors have disclosed that their computer systems have been infiltrated.

In January 2010, Internet search giant Google announced it was the target of a sophisticated cyber-attack using malicious code dubbed "Aurora," which compromised the Gmail accounts of human rights activists and succeeded in accessing Google source code repositories.

The company, and subsequent public reports, blamed the attack on the Chinese government.

The Google attack "was certainly an escalation of Chinese network operations against the U.S.," says Joel Brenner, former counterintelligence chief for the Office of the Director of National Intelligence. "Thousands" of U.S. companies were targeted in the Aurora attacks, Brenner says -- far more than the estimated 34 companies publicly identified as targets so far -- a scale which Brenner says demonstrates China's "heavy-handed use of state espionage against economic targets."

WORRIED: Joel Brenner, former director of the counterintelligence for the Office of the Director of National Intelligence and author of a forthcoming book on cyber-espionage titled "America the Vulnerable: New Technology and the Next Threat to National Security," in his office in Washington, March 22, 2011. **REUTERS/HYUNGWON KANG**

Many firms whose business revolves around intellectual property -- tech firms, defense group companies, even Formula One teams -- complain that their systems are now under constant attack to extract proprietary information. Several have told Reuters they believe the attacks come from China.

Some security officials say firms doing business directly with Chinese state-linked companies -- or which enter fields in which they compete directly -- find themselves suffering a wall of hacking attempts almost immediately.

The full scope of commercial computer intrusions is unknown. A study released by computer-security firm McAfee and government consulting company SAIC on March 28 shows that more than half of some 1,000 companies in the United States, Britain and other countries decided not to investigate a computer-security breach because of the cost. One in 10 companies will only report a security breach when legally obliged to do so, according to the study.

"Simply put, corporations cannot afford negative publicity (about computer security breaches)," says Tom Kellermann, vice president of security awareness at Core Security Technologies and a contributor to the study.

GONE PHISHING

WHAT IS KNOWN is the extent to which Chinese hackers use "spear-phishing" as their preferred tactic to get inside otherwise forbidden networks. Compromised email accounts are the easiest way to launch spear-phish because the hackers can send the messages to entire contact lists.

The tactic is so prevalent, and so successful, that "we have given up on the idea we can keep our networks pristine," says Stewart Baker, a former senior cyber-security official at the U.S. Department of Homeland Security and National Security Agency. It's safer, government and private experts say, to assume the worst -- that any network is vulnerable.

Two former national security officials involved in cyber-investigations told Reuters that Chinese intelligence and military units, and affiliated private hacker groups, actively engage in "target development" for spear-phish attacks by combing the Internet for details about U.S. government and commercial employees' job descriptions, networks of associates, and even the way they sign their emails -- such as U.S. military

CYBER WARRIORS: A map is displayed on one of the screens at the Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado Springs, Colorado July 20, 2010.
REUTERS/RICK WILKING

personnel's use of "V/R," which stands for "Very Respectfully" or "Virtual Regards."

The spear-phish are "the dominant attack vector. They work. They're getting better. It's just hard to stop," says Gregory J. Rattray, a partner at cyber-security consulting firm Delta Risk and a former director for cyber-security on the National Security Council.

Spear-phish are used in most Byzantine Hades intrusions, according to a review of State Department cables by Reuters. But Byzantine Hades is itself categorized into at least three specific parts known as "Byzantine Anchor," "Byzantine Candor," and "Byzantine Foothold." A source close to the matter says the sub-codenames refer to intrusions which use common tactics and malicious code to extract data.

A State Department cable made public by WikiLeaks last December highlights the severity of the spear-phish problem. "Since 2002, (U.S. government) organizations have been targeted with social-engineering online attacks" which succeeded in "gaining access to hundreds of (U.S. government) and cleared defense contractor systems," the cable said. The emails were aimed at the U.S. Army, the Departments of Defense, State and Energy, other government entities and commercial companies.

Once inside the computer networks, the hackers install keystroke-logging software and "command-and-control" programs which allow them to direct the malicious code to seek out sensitive information. The cable says that at least some of the attacks in 2008 originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department, which oversees intelligence-gathering from electronic communications.

THE SPEAR-PHISH ARE "THE DOMINANT ATTACK VECTOR. THEY WORK. THEY'RE GETTING BETTER. IT'S JUST HARD TO STOP."

Between April and October 2008, hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency," the cable says.

Investigators say Byzantine Hades intrusions are part of a particularly virulent form of cyber-espionage known as an "advanced persistent threat." The malicious code embedded in attachments to spear-phish emails is often "polymorphic" -- it changes form every time it runs -- and burrows deep into computer networks to avoid discovery. Hackers also conduct "quality-assurance" tests in advance of launching attacks to minimize the number of anti-virus programs which can detect it, experts say.

As a result, cyber-security analysts say advanced persistent threats are often only identified after they penetrate computer networks and begin to send stolen data to the computer responsible for managing the attack. "You have to look for the 'phone home,'" says Roger Nebel, managing director for cyber-security at Defense Group Inc., a consulting firm in Washington, DC.

BLOG

Find more Reuters special reports at our blog The Deep End here:
http://link.reuters.com/heq72q

It was evidence of malicious code phoning home to a control server -- a computer that supervises the actions of code inside other computers -- that provided confirmation to U.S. cyber-sleuths that Chinese hackers were behind Byzantine Hades attacks, according to the April 2009 State Department cable.

As a case study, the cable cites a 10-month investigation by a group of computer experts at the University of Toronto which focused in part on cyber-intrusions aimed at Tibetan groups, including the office of the exiled Dalai Lama in Dharamsala, India.

Referencing the Canadian research, the cable notes that infected computers in the Dalai Lama's office communicated with control servers previously used to attack Tibetan targets during the 2008 Olympics in Beijing. Two Web sites linked to the attack also communicated with the control server.

TARGETS DETAILED

THE SAME SITES HAD also been involved in Byzantine Hades attacks on U.S. government computers in 2006, according to "sensitive reports" cited in the cable -- likely a euphemistic reference to secret intelligence reporting.

The computer-snooping code that the intrusion unleashed was known as the Gh0stNet Remote Access Tool (RAT). It "can capture keystrokes, take screen shots, install and change files, as well as record sound with a connected microphone and video with a connected webcam," according to the cable.

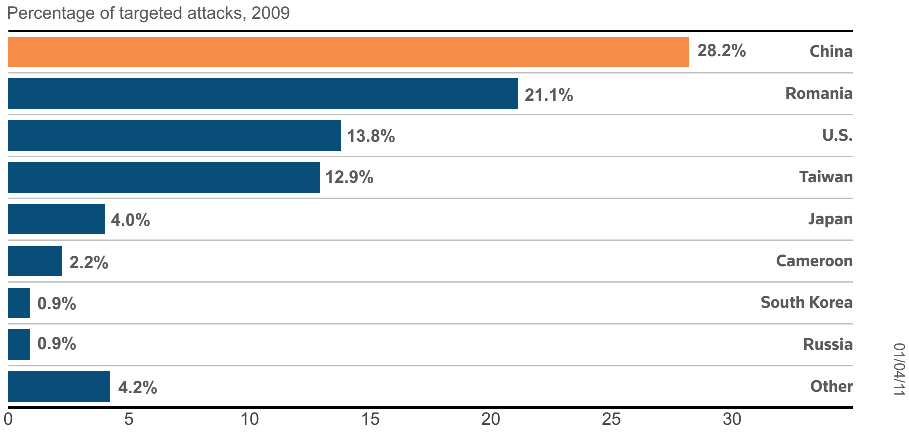
Gh0st RAT succeeded in invading at least one State Department computer. It "has been identified in incidents -- believed to be the work of (Byzantine Hades) actors -- affecting a locally employed staff member at the U.S. Embassy in Tokyo, Japan," according to the cable.

Evidence that data was being sucked out of a target network by malicious code also appears to have led cyber-security investigators to a specific hacker, affiliated with the Chinese government, who was conducting cyber-espionage in the United States. A March, 2009 cable identifies him

HACKED: A cleaner sweeps the logo of Google China outside its company headquarters in Beijing, January 19, 2010. **REUTERS/ALFRED JIN**

Spear-phished: targeted attacks by country

In 2009, China was the source nation of more than one fourth of the world's targeted email attacks.



Source: Messagelabs "The Nature of Cyber-Espionage," March 2010

REUTERS

Reuters graphic/Stephen Culp

as Yinan Peng. The cable says that Peng was believed to be the leader of a band of Chinese hackers who call themselves "Javaphile."

Peng did not respond to three emails seeking comment.

The details of alleged Chinese military-backed intrusions of U.S. government computers are discussed in a half dozen State Department cables recounting intense global concern about China's aggressive use of cyber-espionage.

In a private meeting of U.S., German, French, British and Dutch officials held at Ramstein Air Base in September 2008, German officials said such computer attacks targeted every corner of the German market, including "the military, the economy, science and technology, commercial interests, and research and development," and increase "before major negotiations involving German and Chinese interests," according to a cable from that year.

French officials said at the meeting that they "believed Chinese actors had gained access to the computers of several high-level French officials, activating microphones and Web cameras for the purpose of eavesdropping," the cable said.

TESTING THE WATERS

THE LEAKED STATE DEPARTMENT cables have surfaced as Reuters has learned that the U.S. is engaged in quiet, proxy-led talks with China over cyber issues.

Chronic computer breaches have become a major source of tension in U.S. relations with China, which intensified after the major Google hack was disclosed in January 2010, according to U.S. officials involved in the talks. Even before the Google hack, Chinese officials had recognized the problem as well.

In mid-2009, representatives of the China Institutes for Contemporary International Relations, a nominally-independent research group affiliated with China's Ministry of State Security, contacted James A. Lewis, a former U.S. diplomat now with the Center for Strategic and International Studies.

Lewis said that in his first meeting with his Chinese counterparts, a representative of the China Institutes asked: "Why does the Western press always blame China (for cyber-attacks)?" Lewis says he replied: "Because it's true."

There was no response to request for comment on the talks from the Chinese embassy in Washington.

Preliminary meetings at CSIS have blossomed into three formal meetings in Washington and Beijing over the last 14 months. According to two participants, the talks continue to be marked by "a lot of suspicion." Attendees have focused on establishing a common understanding of cyber-related military, law enforcement and trade issues. Cyber-espionage isn't being discussed directly, according to one participant, because "the Chinese go rigid" when the subject is raised.

One reason: for China, digital espionage is wrapped into larger concerns about how to keep China's economy, the world's second largest, growing. "They've identified innovation as crucial to future economic growth -- but they're not sure they can do it," says Lewis. "The easiest way to innovate is to plagiarize" by stealing U.S. intellectual property, he adds.

There have been a few breakthroughs. U.S. and Chinese government officials from law enforcement, intelligence, military and diplomatic agencies have attended in the wings of each discussion. "The goal has been to get both sides on the same page," says Lewis. "We're building the groundwork for official discussions."

A former senior national security official who has also attended the talks says, "Our reports go straight to the top policymakers" in the Obama administration.

Chinese participants have sought to allay U.S. concerns about a Chinese cyber-attack on the U.S. financial system. With China owning more than $1.1 trillion in U.S. government debt, Lewis says China's representatives acknowledged destabilization of U.S. markets would, in effect, be an attack on China's economy, itself.

Despite the talks, suspected Chinese cyber-espionage has hardly tapered off. Documents reviewed by Reuters show that CSIS itself recently was the target of a spear-phish containing malicious code with a suspected link to China.

On March 1, an email sent from an address on an unofficial U.S. Armed Forces family welfare network called AFGIMail was sent to Andrew Schwartz, chief spokesman for CSIS. Attached to the message was an Excel spreadsheet labeled "Titan Global Invitation List."

An analysis conducted for Reuters by a cyber-security expert who asked not to be identified shows the email may have been sent from a compromised AFGIMail email server. The Excel spreadsheet, if opened, installs malicious code which searches for documents on the victim's computer. The code then communicates to a Web-site hosting company in Orange County, California that has additional sites in China.

(Reporting by Brian Grow in Atlanta and Mark Hosenball in Washington; additional reporting by Peter Apps in London; editing by Jim Impoco and Claudia Parsons)

CHINESE GUARDS: Honour guards stand in a line before an official welcoming ceremony inside the Great Hall of the People in Beijing, February 25, 2010. **REUTERS/JASON LEE**

COVER PHOTO: Sgt James Ortiz looks over a rack in the server room at the Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado Springs, Colorado July 20, 2010. **REUTERS/RICK WILKING**

FOR MORE INFORMATION CONTACT:

JIM IMPOCO,
ENTERPRISE EDITOR, AMERICAS
+1 646 223 8923
jim.impoco@thomsonreuters.com

BRIAN GROW
+1 202 450 9219
brian.grow@thomsonreuters.com

MARK HOSENBALL
+1 202 354 5821
mark.hosenball@thomsonreuters.com

REUTERS