- # Bloomberg

  Connecting decision makers to a dynamic network of information, people and ideas, Bloomberg quickly and accurately delivers business and financial information, news and insight around the world.

  ## For Customers

- Bloomberg Anywhere Remote Login
- Software Updates
- Manage Products and Account Information

Support

Americas+1 212 318 2000

EMEA+44 20 7330 7500

Asia Pacific+65 6212 1000

-

Company

- Bloomberg London
- About
- Careers
- Diversity and Inclusion
- Philanthropy and Engagement
- Sustainability
- Tech

Communications

- Press Announcements
- Press Contacts

Follow

- Facebook
- Twitter
- LinkedIn
- Instagram
-

Products

- Bloomberg Terminal
- Execution and Order Management

- Data and Content
- Financial Data Management
- Integration and Distribution
- Bloomberg Tradebook

Industry Products

- Bloomberg Law
- Bloomberg Tax
- Bloomberg Government
- Bloomberg Environment
- Bloomberg New Energy Finance

Media

- Bloomberg Markets
- Bloomberg Technology
- Bloomberg Pursuits
- Bloomberg Politics
- Bloomberg Opinion
- Bloomberg Businessweek
- Bloomberg Live Conferences
- Bloomberg Apps
- Bloomberg Radio
- Bloomberg Television
- News Bureaus

Media Services

- Bloomberg Media Distribution
- Advertising

Company

- Bloomberg London
- About
- Careers
- Diversity and Inclusion
- Philanthropy and Engagement
- Sustainability
- Tech

Communications

- Press Announcements
- Press Contacts

Follow

- Facebook
- Twitter
- LinkedIn
- Instagram

Products

- Bloomberg Terminal

- Execution and Order Management
- Data and Content
- Financial Data Management
- Integration and Distribution
- Bloomberg Tradebook

Industry Products

- Bloomberg Law
- Bloomberg Tax
- Bloomberg Government
- Bloomberg Environment
- Bloomberg New Energy Finance

Media

- Bloomberg Markets
- Bloomberg Technology
- Bloomberg Pursuits
- Bloomberg Politics
- Bloomberg Opinion
- Bloomberg Businessweek
- Bloomberg Live Conferences
- Bloomberg Apps
- Bloomberg Radio
- Bloomberg Television
- News Bureaus

Media Services

- Bloomberg Media Distribution
- Advertising

Bloomberg

Connecting decision makers to a dynamic network of information, people and ideas, Bloomberg quickly and accurately delivers business and financial information, news and insight around the world.

For Customers

- Bloomberg Anywhere Remote Login
- Software Updates
- Manage Contracts and Orders

Support

Americas+1 212 318 2000

EMEA+44 20 7330 7500

Asia Pacific+65 6212 1000

markets

Hackers Linked to China's Army Seen From EU to D.C.

Michael Riley and Dune Lawrence
July 26, 2012, 7:00 PM EDT

The hackers clocked in at precisely 9:23 a.m. Brussels time on July 18 last year, and set to their task. In just 14 minutes of quick keyboard work, they scooped up the e-mails of the president of the European Union Council, Herman Van Rompuy, Europe's point man for shepherding the delicate politics of the bailout for Greece, according to a computer record of the hackers' activity.

Over 10 days last July, the hackers returned to the council's computers four times, accessing the internal communications of 11 of the EU's economic, security and foreign affairs officials. The breach, unreported until now, potentially gave the intruders an unvarnished view of the financial crisis gripping Europe.

And the spies were themselves being watched. Working together in secret, some 30 North American private security researchers were tracking one of the biggest and busiest hacking groups in China.

Observed for years by U.S. intelligence, which dubbed it Byzantine Candor, the team of hackers also is known in security circles as the Comment group for its trademark of infiltrating computers using hidden webpage computer code known as "comments."

During almost two months of monitoring last year, the researchers say they were struck by the sheer scale of the hackers' work as data bled from one victim after the next: from oilfield services leader Halliburton Co. to Washington law firm Wiley Rein LLP; from a Canadian magistrate involved in a sensitive China extradition case to Kolkata-based tobacco and technology conglomerate ITC Ltd.

Gathering Secrets

The researchers identified 20 victims in all -- many of them organizations with secrets that could give China an edge as it strives to become the world's largest economy. The targets included lawyers pursuing trade claims against the country's exporters and an energy company preparing to drill in waters China claims as its own.

"What the general public hears about -- stolen credit card numbers, somebody hacked LinkedIn -- that's the tip of the iceberg, the unclassified stuff," said Shawn Henry, former executive assistant director of the FBI in charge of the agency's cyber division until leaving earlier this year. "I've been circling the iceberg in a submarine. This is the biggest vacuuming up of U.S. proprietary data that we've ever seen. It's a machine."

Exploiting a hole in the hackers' security, the researchers created a digital diary, logging the intruders' every move as they crept into networks, shut off anti-virus systems, camouflaged themselves as system administrators and covered their tracks, making them almost immune to detection by their victims.

Every Move

The minute-by-minute accounts spin a never-before told story of the workaday routines and relentless onslaught of a group so successful that a cyber unit within the Air Force's Office of Special Investigations in San Antonio is dedicated to tracking it, according to a person familiar with the unit.

Those logs -- a record of the hackers' commands to their victims' computers -- also reveal the highly organized effort behind a group that more than any other is believed to be at the spear point of the vast hacking industry in China. Byzantine Candor is linked to China's military, the People's Liberation Army, according to a 2008 diplomatic cable released by WikiLeaks. Two former intelligence officials verified the substance of the document.

Hackers and Spies

The methods behind China-based looting of technology and data -- and most of the victims -- have remained for more than a decade in the murky world of hackers and spies, fully known in the U.S. only to a small community of investigators with classified clearances.

“Until we can have this conversation in a transparent way, we are going to be hard pressed to solve the problem,” said Amit Yoran, former National Cyber Security Division director at the Department of Homeland Security.

Yoran now works for RSA Security Inc., a Bedford, Massachusetts-based security company which was hacked by Chinese teams last year. “I’m just not sure America is ready for that,” he said.

What started as assaults on military and defense contractors has widened into a rash of attacks from which no corporate entity is safe, say U.S. intelligence officials, who are raising the alarm in increasingly dire terms.

In an essay in the Wall Street Journal July 19, President Barack Obama warned that “the cyber threat to our nation is one of the most serious economic and national security challenges we face.” Ten days earlier, in a speech given in Washington, National Security Agency director Keith Alexander said cyber espionage constitutes “the greatest transfer of wealth in history,” and cited a figure of $1 trillion spent globally every year by companies trying to protect themselves.

Harvesting Secrets

The networks of major oil companies have been harvested for seismic maps charting oil reserves; patent law firms for their clients’ trade secrets; and investment banks for market analysis that might impact the global ventures of state-owned companies, according to computer security experts who asked not to be named and declined to give more details.

China’s foreign ministry in Beijing has previously dismissed allegations of state-sponsored cyberspying as baseless and said the government would crack down if incidents came to light. Contacted for this story, it did so again, referring to earlier ministry statements.

Private researchers have identified 10 to 20 Chinese hacking groups but said they vary significantly in activity and size, according to government investigators and security firms.

Group Apart

What sets the Comment group apart is the frenetic pace of its operations. The attacks documented last summer represent a fragment of the Comment group’s conquests, which stretch back at least to 2002, according to incident reports and interviews with investigators. Milpitas, California-based FireEye Inc. alone has tracked hundreds of victims in the last three years and estimates the group has hacked more than 1,000 organizations, said Alex Lanstein, a senior security researcher.

Stolen information is flowing out of the networks of law firms, investment banks, oil companies, drug makers, and high technology manufacturers in such significant quantities that intelligence officials now say it could cause long-term harm to U.S. and European economies.

’Earthquake Is Coming’

“The activity we’re seeing now is the tremor, but the earthquake is coming,” said Ray Mislock, who before retiring in September was chief security officer for DuPont Co., which has been hacked by unidentified Chinese teams at least twice since

2009.

“A successful company can’t sustain a long-term loss of knowledge that creates economic power,” he said.

Even those offline aren’t safe. Y.C. Deveshwar, 65, a businessman who heads ITC, India’s largest maker of cigarettes, doesn’t use a computer. The Comment hackers last year still managed to steal a trove of his documents, navigating the conglomerate’s huge network to pinpoint the machine used by Deveshwar’s personal assistant.

On July 5, 2011, the thieves accessed a list of documents that included Deveshwar’s family addresses, tax filings, and meeting minutes, as well as letters to fellow executives, such as London-based British American Tobacco Plc chairman Richard Burrows and BAT chief executive, Nicandro Durante, according to the logs. They tried to open one entitled “YCD LETTERS” but couldn’t, so the hackers set up a program to steal a password the next time his assistant signed on.

Keeping Quiet

When Bloomberg contacted the company in May, spokesman Nazeeb Arif said ITC was unaware of the breach, potentially giving the hackers unimpeded access to ITC’s network for more than a year. Deveshwar said in a statement that “no classified company related documents” were kept on the computer.

Companies that discover their networks have been commandeered usually keep quiet, leaving the public, shareholders and clients unaware of the magnitude of the problem. Of the 10 Comment group victims reached by Bloomberg, those who learned of the hacks

chose not to disclose them publicly, and three said they were unaware they'd been hacked until contacted for this story.

This account of the Comment group is based on the researchers' logs, as well as interviews with current and former intelligence officials, victims, and more than a dozen U.S. cybersecurity experts, many of whom track the group independently.

Private Investigators

The researcher who provided the computer logs asked not to be named because of the sensitivity of the data, which included the name of victims. He was part of a collaborative drawn from 20 organizations that included people from private security companies, a university, internet service providers and companies that have been targeted, including a defense contractor and a pharmaceutical firm. The group included some of the top experts in the field, with experience investigating cyberspying against the U.S. government, major corporations and high profile political targets, including the Dalai Lama.

Like similar, ad hoc teams formed temporarily to study hackers' techniques, the group worked in secret because of the sensitivities of the investigation aimed at state-sponsored espionage. A smaller version of the group is continuing its research.

As the surge in attacks on businesses and non-government groups over the last five years has pulled private security experts into the hacker hunt, they say they're gradually catching up with U.S. counterintelligence agencies, which have been tackling the problem for a decade.

Espionage Tools

One Comment group trademark involves hijacking unassuming public websites to send commands to victim computers, turning mom-and-pop sites into tools of foreign espionage, but also allowing the group to be monitored if those websites can be found, according to security experts. Sites it has commandeered include one for a teacher at a south Texas high school with the website motto "Computers Rock!" and another for a drag racing track outside Boise, Idaho.

Adding a potentially important piece to the puzzle, researcher Joe Stewart, who works for Dell SecureWorks, an Atlanta-based security firm and division of Dell Inc., the computer technology company, last year uncovered a flaw in software used by Comment group hackers. Designed to disguise the pilfered data's ultimate destination, the mistake instead revealed that in hundreds of instances, data was sent to Internet Protocol (IP) addresses in Shanghai.

Military Link?

The location matched intelligence contained in the 2008 State Department cable published by WikiLeaks that placed the group in Shanghai and linked it to China's military. Commercial researchers have yet to make that connection. The basis for that cable's conclusion, which includes the U.S.'s own spying, remains classified, according to two former intelligence specialists.

Lanstein said that although the make-up of the Comment group has changed over time -- the logs show some inexperienced hackers in the group making repeated mistakes, for example --the characteristics of a single group are unmistakable. The code and tools used by Comment aren't public, and anyone using it would have to be given entre into the hackers' ranks, he said.

By October 2008, when the diplomatic cable published by WikiLeaks outlined the group's activities, the Comment group had raided the networks of defense contractors and the Department of State, as well as made a specialty of hacking U.S. Army systems. The classified code names for China's hacking teams were changed last year after that leak.

Cybersecurity experts have connected the group to a series of headline-grabbing hacks, ranging from the 2008 presidential campaigns of Barack Obama and John McCain to the 72 victims documented last year by the Santa Clara, California-based security firm McAfee Inc., in what it called Operation Shady Rat.

Nuclear Break-In

Others, not publicly attributed to the group before, include a campaign against North American natural gas producers that began in December 2011 and was detailed in an April alert by the Department of Homeland Security, two experts who analyzed the attack said. In another case, the hackers first stole a contact list for subscribers to a nuclear management newsletter, and then sent them forged e-mails laden with spyware.

In that instance, the group succeeded in breaking into the computer network of at least one facility, Diablo Canyon nuclear plant, next to the Hosgri fault north of Santa Barbara, according to a person familiar with the case who asked not to be named.

Last August, the plant's incident management team saw an anonymous Internet post that had been making the rounds among cybersecurity professionals. It purported to identify web domains being used by a Chinese hacking group, including one that suggested a possible connection to Diablo plant operator Pacific Gas & Electric Co., according to an internal report obtained by Bloomberg News.

Partial Control

It's unclear how the information got to the Internet, but when the plant investigated, it found that the computer of a senior nuclear planner was at least partly under the control of the hackers, according to the report. The internal probe warned that the hackers were attempting "to identify the operations, organizations, and security of U.S. nuclear power generation facilities."

The investigators concluded that they had caught the breach early and there was "no solid indication" data was stolen, according to the report, though they also found evidence of several previous infections.

Blair Jones, a spokesman for PG&E, declined to comment, citing plant security.

Around the time the hackers were sending malware-laden e-mails to U.S. nuclear facilities, six people at the Wiley Rein law firm were ushered into hastily called meetings. In the room were an ethics compliance officer and a person from the firm's information technology team, according to a person familiar with the investigation. The firm had been hacked, each of the six were told, and they were the targets.

Lawyers' Files

Among them were Alan Price and Timothy Brightbill. Firm partners and among the best known international trade lawyers in the country, they've handled a series of major anti-dumping and unfair trade cases against China. One of those, against China's solar cell manufacturers, in May resulted in tariffs on more than $3 billion in Chinese exports, making it one of the largest anti-dumping cases in U.S. history.

Dale Hausman, Wiley Rein's general counsel, said he couldn't comment on how the breach affected the firm or its clients. Wiley Rein has since strengthened its network security, Hausman said.

"Given the nature of that practice, it's almost a cost of doing business. It's not a surprise," he said.

E-Mails to Spouses

Tipped off by the researchers, the firm called the Federal Bureau of Investigation, which dispatched a team of cyber investigators, the person familiar with the investigation said. Comment hackers had encrypted the data it stole, a trick designed to make it harder to determine what was taken. The FBI managed to decode it.

The data included thousands of pages of e-mails and documents, from lawyers' personal chatter with their spouses to confidential communications with clients. Printed out in a stack, the cache was taller than a set of encyclopedias, the person said.

Researchers watching the hackers' keystrokes last summer say they couldn't see most of what was stolen, but it was clear that the spies had complete control over the firm's e-mail system. The logs also hold a clue to how the FBI might have decrypted what was stolen. They show the simple password the hackers used to encrypt the files: 123!@#. Paul Bresson, a spokesman for the FBI in Washington, declined to comment.

Following the Crisis

In case after case, the hackers' trail crisscrossed with geopolitical events and global headlines. Last summer, as the news focused on Europe's financial crisis, with its import for China's rising economic power, the hackers followed.

The timing coincided with an intense period for EU Council President Van Rompuy, set off by the failure July 11 of the EU finance ministers to agree on a second bailout package for Greece. Over the next 10 days, the slight and balding former Belgian prime minister presided over the negotiations, drawing European leaders, including German Chancellor Angela Merkel, to a consensus.

Although the monitoring of Van Rompuy and his staff occurred during those talks, researchers say that the logs suggest a broad attack that wasn't timed to a specific event. It was the cyber equivalent of a wiretap, they say -- an operation aimed at gathering vast amounts of intelligence over weeks, perhaps months.

'Big Implications'

Richard Falkenrath, former deputy homeland security adviser to President George W. Bush, said China has succeeded in integrating decision-making about foreign economic and investment policy with intelligence collection.

"That has big implications for the rest of the world when it deals with the country on those terms," he said.

Beginning July 8, 2011, the hackers' access already established, they dipped into the council's networks repeatedly over 10 days. The logs suggest an established routine, with the spies always checking in around 9 a.m. local time. They controlled the council's exchange server, which gave them complete run of the e-mail system, the logs show. From there, the hackers simply opened the accounts of Van Rompuy and the others.

Week of E-Mails

Moving from one victim to the next, the spies grabbed e-mails and attached documents, encrypted them in compression files and catalogued the reams of material by date. They grabbed a week's worth of e-mails each time, appearing to follow a set protocol. Their other targets included then economic adviser and deputy head of cabinet, Odile Renaud-Basso, and the EU's counter-terrorism coordinator. It's unclear how long the hackers had been in the council's network before the researchers' monitoring began -- or how long it lasted after the end of July last year.

There's no indication the hackers penetrated the council's offline system for secret documents. "Classified information and other sensitive internal information is handled on separate, dedicated networks," the council press office said in a statement when asked about the hacks. The networks connected to the Internet, which handle e-mail, "are not designed for handling classified information."

What the EU did about the breach is unclear. Dirk De Backer, a spokesman for Van Rompuy, declined to comment on the incident, as did an official from the EU Council's press office. A member of the EU's security team joined the group of researchers in late July, and was provided information that would help identify the hackers' trail, one of the researchers said.

"No Knowledge"

Zoltan Martinusz, then principal adviser on external affairs and one of two victims reached by Bloomberg who would address the issue, said, "I have no knowledge of this." The other official, who wasn't authorized to discuss internal security and asked not to be identified, said he was informed last year that his e-mails had been accessed.

The logs show how the hackers consistently applied the same, simple line of attack, the researchers said. Starting with a malware-laden e-mail, they moved rapidly through networks, grabbing encrypted passwords, cracking the coding offline, and then returning to mimic the organization's own network administrators. The hackers were able to dip in and out of networks sometimes over months.

The approach circumvented the millions of dollars the organizations collectively spent on protection.

Security Switched Off

As the spies rifled the network of Business Executives for National Security Inc., a Washington-based nonprofit whose advisory council includes former Secretary of State Henry Kissinger and former Treasury Secretary Robert Rubin, the logs show them switching off the system's Symantec anti-virus software. Henry Hinton Jr., the group's chief operations officer, said in June he was unaware of the hack, confirming the user names of staff computers that the logs show were accessed, his among them.

The records show the hackers' mistakes, but also clever tricks. Using network administrator status, they consolidated onto a single machine the computer contents of the president and seven other staff members of the International Republican Institute, a nonprofit group promoting democracy.

220 Documents

With all that data in one place, the hackers on June 29, 2011, selected 220 documents, including PDFs, spreadsheets, photos and the organization's entire work plan for China. When they were done, the Comment group zipped up the documents into several encrypted files, making the data less noticeable as it left the network, the logs show.

Lisa Gates, a spokeswoman for the IRI, confirmed that her organization was hacked but declined to comment on the impact on its programs in China because of concern for the safety of staff and people who work with the group. A funding document describes activities including supporting independent candidates in China, who frequently face harassment by China's authorities.

As a portrait of the hackers at work, the logs also show how nimbly they could respond to events, even when sensitive government networks were involved. The hackers accessed the network of the Immigration and Refugee Board of Canada July 18 last year, targeting the computer of Leeann King, an immigration adjudicator in Vancouver.

King had made headlines less than a week earlier when she temporarily freed Chinese national Lai Changxing in the final days of a long extradition fight. Chinese authorities had been chasing Lai since he fled to Canada in 1999, alleging that he ran a smuggling ring that netted billions of dollars.

Cracking Court Accounts

Monitoring by Cyber Squared Inc., an Arlington, Virginia-based company that tracks Comment independently and that captured some of the same activity as the researchers, recorded the hackers as they worked rapidly to break into King's account. Beginning only with access to computers in Toronto, the hackers grabbed and decrypted user passwords, gaining access to IRB's network in Vancouver and ultimately, the logs show, to King's computer. From start to finish, the work took just under five hours.

Melissa Anderson, a spokeswoman for the board, said officials had no comment on the incident other than to say that any such event would be fully investigated. Lai was eventually sent back to China on July 23, 2011 after losing a final appeal. He was arrested, tried, and in May of this year, a Chinese court sentenced him to life in prison.

Controlling the Networks

In case after case, the hackers had the run of the networks they were rifling. It's unclear how many of the organizations researchers contacted, but in only one of those cases was the victim already aware of the intrusion, according to one member of the group. Halliburton officials said they were aware of the intrusion and were working with the FBI, one of the researchers said.

Marisol Espinosa, a spokeswoman for the publicly traded company, declined to comment on the incident.

The trail last summer led to some unlikely spots, including Pietro's, an Italian restaurant a couple of blocks from Grand Central station in New York. In business since 1932, guests to the dim, old-fashioned dining room can choose linguine with clam sauce (red or white) for $28. The Comment group stopped using the restaurant's site to communicate with hacked networks sometime last year, said FireEye's Lanstein, who discovered that the hackers had left footprints there. Traces are still there.

'Ugly Gorilla'

Hidden in the webpage code of the restaurant's site is a single command: ugs12, he said. It's an order to a captive computer on some victim's network to sleep for 12 minutes, then check back in, he explained. The "ug" stands for "ugly gorilla," what security experts believe is a moniker for a particularly brash member of Comment, a signal for anyone looking that the hackers were there, said Lanstein.

"We're so good even hackers want us!" joked Bill Bruckman, the restaurant's co-owner, when he was told his website had been part of the global infrastructure of a Chinese hacking team. "Hey, put my name out there -- any business is good business," he said.

Bruckman said he knew nothing about the breach. A few friends reported trouble accessing the site about six months ago, though he said he'd never figured out what the problem was.

Outside a moment later, smoking a cigarette, Bruckman added a more serious note.

"Think of all that effort and information going down the drain. What a waste, you know what I mean?"