Smart Grid Solutions Strengthen Electric Reliability and Customer Services in Florida

With 4.6 million customers, nearly 70,000 miles of power lines and 16 power plants, Florida Power and Light Company (FPL) is one of the nation's largest electric utilities. FPL says maintaining reliable service while keeping rates affordable is "Job One." While pursuing its mission, FPL is implementing "Energy Smart Florida," which is the largest and one of the most comprehensive of the U.S. Department of Energy's (DOE), Smart Grid Investment Grant (SGIG) projects. FPL had already committed to smart meters and had been running pilots for several years in preparation for SGIG upgrades. The DOE grant enabled FPL to accelerate its plans and undertake additional grid modernization improvements for the entire electric delivery system, including transmission, distribution and metering. The total budget of $800 million includes $200 million in DOE funds.

Before SGIG funding, FPL's investment plans called for implementing only a handful of smart grid projects a year. FPL explains that the SGIG funds have had a catalytic effect on these plans. For example, because of SGIG funds, FPL has been able to implement thousands of additional improvements, test new systems and strategies, and begin to explore innovations for product and service offerings on the customer side of the meter. In many instances, these activities go well beyond those in their previous plans. According to Bryan Olnick, FPL's Vice President of Customer Service Smart Grid Solutions and Meter Services, "FPL's typical residential electricity bills are the lowest in the state, and the service we provide customers is among the most reliable in the country. With support from DOE, our SGIG project enables us to enhance service reliability while putting more control than ever before in the hands of customers over their power consumption and costs."

Preventative Maintenance is Avoiding Power Outages

FPL's smart grid plans involve a deliberate and phased approach. To date, equipment is installed and operational for about:

- 98 percent of the SGIG project's planned transmission system improvements,
- 50 percent of the planned distribution system improvements, and
- 75 percent of the planned smart meter change-outs.

Smart devices have been installed on 78 substation transformer banks.

In fact, as of April 2012, FPL had installed more than 5,000 intelligent monitors, sensors, and controls on their transmission and distribution grid, making it possible to predict and prevent outages and enhance service reliability to customers. This installation effort included replacing about 50 electro-mechanical protective relay systems with state-of-the-art computer-based systems, and installing feeder breaker and regulator

intelligent electronic devices at nearly 100 substations, more than 200 automatic feeder switches, and 45 phasor measurement units.

These improvements are already producing measurable benefits. Specifically, one of the new SGIG-enabled FPL capabilities involves "enhanced diagnostic systems," which collect and interpret data from substation devices such as battery banks and transformers and transmit that information to FPL diagnostic centers for problem detection and outage prevention.

For example, FPL's SGIG-upgraded Transmission Performance and Diagnostic Center (TPDC) remotely monitors power transformers in 500 FPL substations. New bushing monitors – monitors that can detect and diagnose problems before they occur – have been installed on some of those transformers to evaluate the health of both the high and low voltage bushings, including capacitance, power factor, and the extent of current imbalance. Bushing failures can damage transformers, which means costly repairs and the possibility of extended service interruptions. In January 2012, a newly installed monitor detected an out-of-tolerance high voltage bushing. Customers served by this transformer were temporarily switched to another one, and the affected transformer was removed from service. Meanwhile, the faulty bushing was replaced, preventing an outage that would have affected several thousand customers.

FPL's Performance and Diagnostic Centers help to monitor the health of the grid

The TPDC is also monitoring the battery banks that provide power to 500 FPL substations. The battery banks are monitored for both high and low voltage levels, and high impedance. In February 2011, a TPDC monitor received an alarm signal indicating a battery problem at a substation located in a remote section of FPL's service territory. A local field engineer was dispatched to the site and found the alarm was caused by a loose interconnection strap. The repair was made and prevented a battery malfunction which might have resulted in an extended outage for the hundreds of customers served by that substation.

The TPDC is also monitoring capacitance voltage transformers (CVTs) and is measuring voltage levels and other power flow variables. TPDC engineers implemented an algorithm that uses these data to detect early CVT degradation so preventative maintenance measures can be taken. In September 2011, the TPDC received an alarm signal indicating potential problems with a degraded phase on a CVT. Local field engineers were dispatched, located the damaged CVT, removed the affected transmission line section from service, and replaced the defective CVT, thus preventing a failure that could have resulted in an extended outage and affected several thousand customers.

Customer Information and Education is Helping Reduce Bills

Another of FPL's new smart grid capabilities involves providing customers with information and data displays so they can better control their electricity consumption and costs. Each customer with an activated smart meter can view his or her own "Energy Dashboard" through FPL's website. The dashboard displays information about consumption and costs a day after it has been recorded by the smart meter. Each customer can view his or her own power use by the hour, day, and month and can receive bill estimates based on current usage patterns. Information from the dashboard is also available by calling FPL and talking to a representative or accessing the interactive voice response system.

The dashboard is helping users make more informed choices about electricity consumption and costs throughout the month. While similar web portals and displays are becoming more common, getting customers to use them has been a challenge for many utilities. FPL is pursuing several approaches to drive expanded use, including email reminders and, with Miami-Dade College, sponsoring a course on

Example screen shot of an "Energy Dashboard" available to FPL's smart meter customers.

how to use the dashboard to reduce power costs. About 900 of FPL's customers have taken the course, which is designed for senior citizens and lower-income customers, and the course will also be offered this year by Broward College and Palm Beach Community College.

Results of these education efforts are encouraging. In fact, many customers are regular dashboard users and have provided comments to FPL on how much they like it. For example, one FPL customer said, "If people choose to use the customer portal, they will definitely see benefits. Changing our energy habits has saved our family about $100 dollars a month compared to similar homes in our area." Another customer noted, "I think the online portal is the greatest tool FPL has to offer. In today's economy, every dollar is important. Thanks to the smart grid, my family is saving as much as $30 a month."

Expanded Capabilities Provide Future Opportunities

FPL plans to build on its SGIG-enabled smart grid capabilities for future products, services, and applications. According to Mr. Olnick, "The improvements we're making now to our electric grid enable us to add customer benefits for years to come. For example, we're putting a lot of attention toward outage restoration because we understand how important it is to our customers. We are conducting pilot projects to learn how the new smart meters work with other components on the system to help us pinpoint and fix outages fast. We are taking a disciplined, measured approach to these and other pilot projects, including testing new products and services involving home-area networks. We plan to leverage all of the smart grid information to make our service more reliable and offer our customers greater choices, convenience, and control."

In planning for the future, FPL has found workforce training to be an important success factor. For example, FPL offers a one-day, highly interactive "Introduction to Smart Grid" course to both technical and non-technical employees. Students learn that the smart grid goes beyond smart meters and includes a wide variety of changes to business practices and protocols (both technical and administrative). In many instances, students also learn that these changes involve new roles within an employee's respective business unit and require new skills in information technologies and systems integration for solving problems with large databases at headquarters and equipment installations in the field. FPL is developing follow-up curricula for technical training in capacitor bank protections and controls, distribution substation scheme upgrades, feeder breakers, and intelligent electronic devices.

Like other power companies in the SGIG program, FPL is learning that smart grid technologies come with an implied commitment to education and training, for both employees and customers. Armed with new knowledge from smart grid data, workers are changing traditional ways of doing business, and customers are changing consumption patterns with subsequent efficiency improvements and cost savings for both the utility and its customers. Supported with SGIG funding, FPL is planning for a smooth transition from traditional to new ways of delivering electricity and in the process involving employees and customers in identifying and realizing smart grid benefits.

Learn More

The American Recovery and Reinvestment Act of 2009 (Recovery Act) provided the U.S. Department of Energy with $4.5 billion to fund projects that modernize the Nation's energy infrastructure and enhance energy independence. For more information about the status of other Recovery Act projects, visit www.smartgrid.gov. To learn about DOE's Office of Electricity Delivery and Energy Reliability's national efforts to modernize the electric grid, visit www.oe.energy.gov.

Bloomberg

Spyware Matching FinFisher Can Take Over IPhone and BlackBerry

By Vernon Silver - Aug 29, 2012

FinFisher spyware made by U.K.-based Gamma Group can take control of a range of mobile devices, including Apple Inc. (AAPL)'s iPhone and Research in Motion Ltd. (RIM)'s BlackBerry, an analysis of presumed samples of the software shows.

The program can secretly turn on a device's microphone, track its location and monitor e-mails, text messages and voice calls, according to the findings, being published today by the University of Toronto Munk School of Global Affairs' Citizen Lab. Researchers used newly discovered malicious software samples to further pull back the curtain on the elusive cyber weapon.

The hunt for clues to the software's deployment has gained speed since July, when research based on e-mails obtained by Bloomberg News identified what looked like a FinFisher product that infects personal computers. In that case, the malware targeted activists from the Persian Gulf kingdom of Bahrain.

The latest analysis, led by security researcher Morgan Marquis-Boire, may demonstrate how such spyware can reach a broader range of devices to follow their owners' every move.

"People are walking around with tools for surveillance in their pockets," says John Scott-Railton, a doctoral student at the University of California Los Angeles' Luskin School of Public Affairs who assisted with the research. "These are the tools that can be used to turn on your microphone and turn your phone into a tracking device."

Transforming Surveillance

The findings -- which are consistent with Gamma's own promotional materials for a FinFisher product called FinSpy Mobile -- illustrate how the largely unregulated trade in offensive hacking tools is transforming surveillance, making it more intrusive as it reaches across borders and peers into peoples' digital devices.

FinFisher products can secretly monitor computers, intercepting Skype calls, turning on Web cameras and recording keystrokes. They are marketed by Gamma for law enforcement and government use.

“I can confirm that Gamma supplies a piece of mobile intrusion software -- FinSpy Mobile,” Gamma International GmbH Managing Director Martin J. Muench said in an Aug. 28 e-mail. “I certainly don’t intend to discuss how or on what platforms it works. I do not wish to inform criminals of how any of our detection systems are used against them.”

Muench, who is based in Munich, said his company didn’t sell FinFisher spyware to Bahrain. “I am still investigating how a piece of our software went astray,” he said in his e-mail.

In a news release today, Gamma said that information from its sales demonstration server had been stolen at an unknown time by unknown methods.

FinSpy Marker

“The information that was stolen has been used to identify the software Gamma used for demonstration purposes,” the release said. “No operations or clients were compromised by the theft.” The Gamma statement said that while its demo products contain the word “FinSpy” -- a marker the researchers used to help identify samples -- its more sophisticated operational products don’t.

Gamma International GmbH in Germany is part of U.K.-based Gamma Group. The group also markets FinFisher through Andover, England-based Gamma International UK Ltd. Muench leads the FinFisher product portfolio.

Muench says that Gamma only sells to governments and their agencies and complies with the export regulations of the U.K., U.S. and Germany.

More Samples

The July report on Bahrain led security professionals and activists to give Marquis-Boire’s team additional samples of malware for testing.

Several of those samples became the basis of the new report, and include what appear to be a FinSpy Mobile demonstration copy and live versions sent to actual targets.

The report contains no information about any individuals who were targeted, or whether devices were infected.

In December, anti-secrecy website WikiLeaks published a promotional brochure and video for FinSpy Mobile. The video shows a BlackBerry user receiving a message to click on a link for a fake update -- and then making the mistake of doing so.

“When FinSpy Mobile is installed on a mobile phone it can be remotely controlled and monitored no

matter where in the world the Target is located," a FinSpy brochure published by WikiLeaks says.

Systems that can be targeted include Microsoft Corp. (MSFT)'s Windows Mobile, the Apple iPhone's iOS, BlackBerry and Google Inc. (GOOG)'s Android, according to the company's literature. Today's report says the malware can also infect phones running Symbian, an operating system made by Nokia Oyj (NOK1V), and that it appears the program targeting iOS will run on iPad tablets.

Simple Process

A mobile device's user can become infected by being tricked into going to a Web link and downloading the malware, which can be disguised as something other than FinSpy.

As Gamma's promotional video illustrates, the process can be as simple as sending someone a text message with a link that looks like it comes from the phone maker, and asking the user to "please install this system update," Marquis-Boire says.

Otherwise, without the use of a previously undiscovered vulnerability, the person sneaking the program onto a phone must gain physical access to the device or know its passwords, the study says.

The spyware doesn't appear to take advantage of any vulnerability in the phones or their operating systems, the study says.

FinSpy software written for Windows Mobile shouldn't be able to infect the newer Windows Phone system, which Microsoft introduced in 2010, said Claudio Guarnieri, a researcher for Boston-based security risk-assessment company Rapid7, who analyzed the Windows portion of the malware for the new report.

'Avoid Clicking'

Redmond, Washington-based Microsoft said its anti-malware software blocks the FinSpy Trojan, and that Windows Phone does not allow for the installation of unknown, third-party software.

"We strongly encourage Windows Mobile owners to avoid clicking on or otherwise downloading software or links from unknown sources, including text messages," Microsoft said in a statement.

"BlackBerry smartphones give customers control over what can be installed on the device in addition to prompting users to grant permissions to third-party applications," Waterloo, Ontario-based RIM said in a statement. "We recommend customers only download applications from trusted sources to help protect against potentially malicious software."

Espoo, Finland-based Nokia's press office issued a statement saying users would need to actively

choose to install an application such as FinFisher.

“Though we have seen claims made for similar products in the past, we have not had any reported incidents from customers as a result of such spyware,” the statement said. Nokia decided last year to abandon Symbian in favor of Windows Phone.

Global Reach

Cupertino, California-based Apple and Mountain View, California-based Google declined comment, spokeswomen for the companies said.

The new study also sheds light on FinFisher’s global reach, bolstering separate findings by researchers who said on Aug. 8 that computers in at least 10 countries on five continents show signs of being command servers to which computers infected by FinFisher send their pilfered data. That study was led by Guarnieri of Rapid7.

The research published today used the original Bahraini samples to establish a unique pattern in which command computers communicate with infected machines -- and then scanned computer networks for such patterns.

More Clues

The scanning effort, led by Bill Marczak, a computer science doctoral candidate at the University of California Berkeley, turned up many of the same machines found by Guarnieri, who had used a different method. It also identified new countries, bringing the total number of nations with suspected command servers to at least 15.

The mobile-infecting samples obtained for the report, which transmit data via the Internet and text message, also provided clues to FinFisher’s deployment.

In one case, a sample was found transmitting to the same Internet address in the Czech Republic that Guarnieri had identified in his study as a likely FinFisher command computer.

It’s unclear if any government agencies in the countries identified in the studies are Gamma clients or if the users may be based in other countries.

A spokesman at the Czech Republic’s interior ministry said he has no information of Gamma being used there, nor any knowledge of its use at other state institutions. A spokeswoman for the Defense Ministry said it has never used Gamma products. The Czech secret service didn’t respond to an e-mailed request for comment.

FinFisher Oversight

Gamma's Muench said the focus on his product was unfair because there are other intrusion tools that lack the oversight provided by FinFisher, which is designed to gather evidence for use in court and is only sold to governments.

He pointed to Rapid7, which while investigating Gamma also distributes Metasploit, a product downloadable for free that contains a database of exploits, which hackers can use to take advantage of vulnerabilities in systems or software. Rapid7 markets Metasploit as a defensive tool for testing if computers can be penetrated.

"Why is no one making a fuss about the free malware available through their website which is completely unrestricted and could and does go anywhere?" Muench said in his e-mail. "Can Rapid7 claim that they have never directly or indirectly supplied malwares worldwide?"

Rapid7 said in a statement that it provides the security industry with a way to test their defenses against known exploits that are already being abused, and levels the playing field with malicious attackers. "Metasploit is not malware," the statement said.

The research published today can be found at: https://citizenlab.org/2012/08/the-smartphone-who-loved-me- finfisher-goes-mobile.

To contact the reporter on this story: Vernon Silver in Rome at vtsilver@bloomberg.net;

To contact the editor responsible for this story: Melissa Pozsgay at mpozsgay@bloomberg.net

CNET News

Virus knocks out computers at Qatari gas firm RasGas

RasGas confirms corporate network is down because of an unknown virus.

by **Elinor Mills** | August 30, 2012 11:17 AM PDT

Less than two weeks after 30,000 computers at a Saudi oil company fell prey to a virus, a Qatari gas firm's Web site and corporate network are also down because of a virus.

An unknown virus has affected office computer systems since Monday, a spokesman for RasGas, the second largest producer of liquified natural gas in the world, told **Arabian Oil and Gas.com [http://www.arabianoilandgas.com/article-10582-exclusive-virus-attack-takes-rasgas-offline/]** today. The company's Web site, **Rasgas.com [http://rasgas.com/]**, remained down, as well.

The virus has not impacted production operations or cargo deliveries, said the unidentified RasGas spokesman. The company is a joint venture between Qatar Petroleum and ExxonMobil.

Related stories

- **Saudi oil firm says 30,000 computers hit by virus [http://www.cnet.com/8301-1009_3-57501066-83/saudi-oil-firm-says-30000-computers-hit-by-virus/]**
- **Massive targeted cyber-attack in Middle East uncovered [http://www.cnet.com/8301-1009_3-57442473-83/massive-targeted-cyber-attack-in-middle-east-uncovered/L]**
- **Behind the 'Flame' malware spying on Mideast computers (FAQ0 [http://www.cnet.com/8301-1009_3-57443975-83/behind-the-flame-**

malware-spying-on-mideast-computers-faq/]

James Herron, EMEA Energy News Editor at Dow Jones Newswires and the Wall Street Journal, **tweeted this morning [http://twitter.com/djopec/status/241211806494896128]** : "Sources tell us the virus that shut down RasGas computers is also Shamoon, the virus widely-believed to have hit Aramco earlier this month."

Last weekend, **Saudi Aramco confirmed that 30,000 of its work stations had been hit with a "malicious" undisclosed virus [http://www.cnet.com/8301-1009_3-57501066-83/saudi-oil-firm-says-30000-computers-hit-by-virus/]** August 15 and took more than a week to get back online.

A hacker group calling itself Cutting Sword of Justice issued a public statement the day Saudi Aramco was attacked, claiming it had sent a virus to destroy 30,000 computers to protest the Al-Saud regime's support for government repression in neighboring countries. A subsequent public message from hackers indicated that the Shamoon virus was used in the attack.

[http://www.cnet.com/profile/elinormills/]

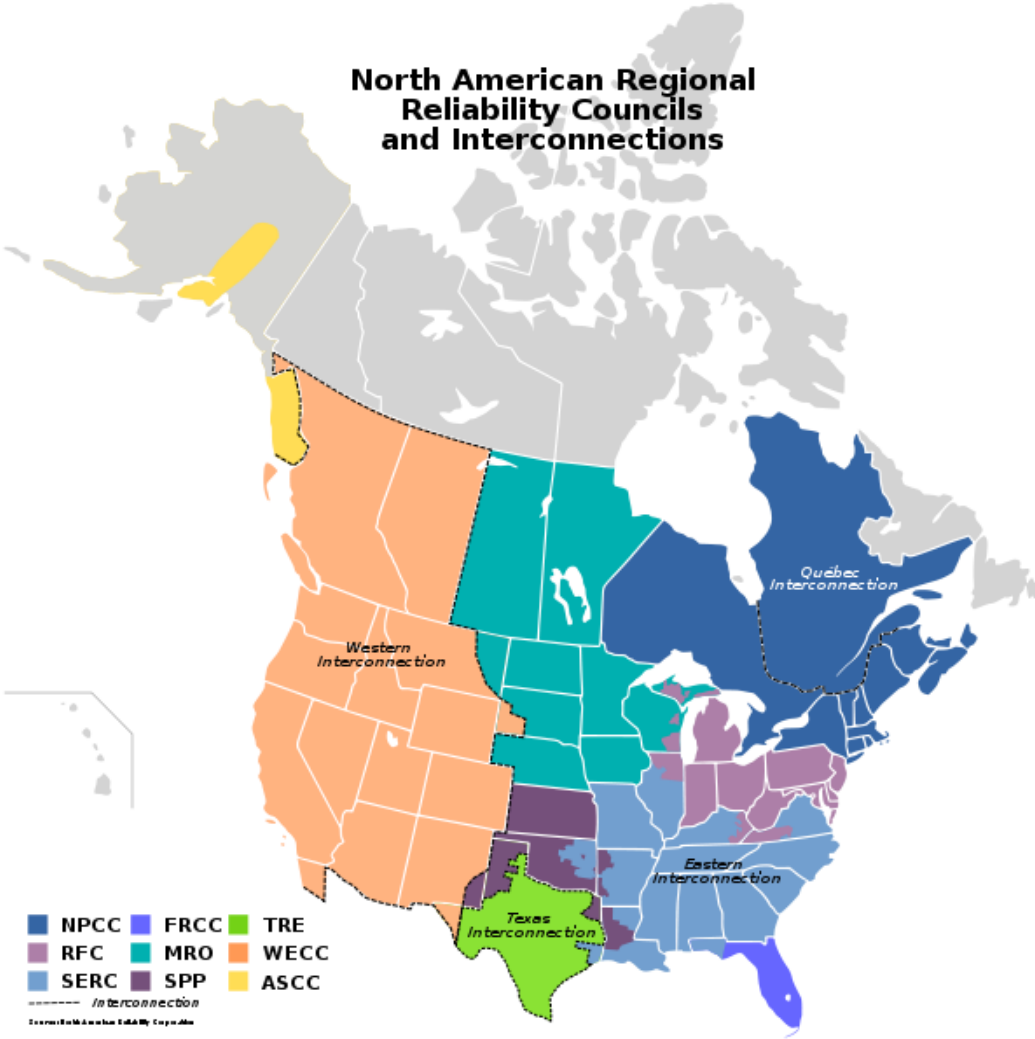
[http://www.cnet.com/profile/elinormills/]

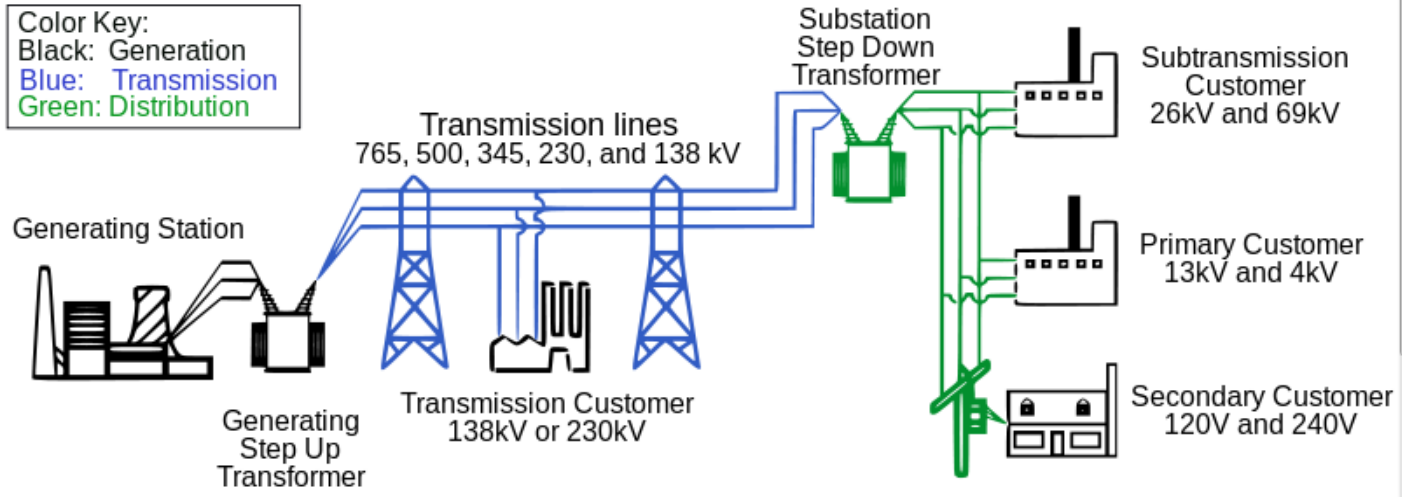
nternet security and privacy. She joined CNET News in 2005 after correspondent for Reuters in Portugal and writing for The Industry [illegible] News Service, and the Associated Press.

[http://plus.google.com/114359738470992181937/]

-
-
-

close


North American Regional
Reliability Councils
and Interconnections
Quebec
Interconnection
Western
Interconnection
Eastern
Interconnection
Texas
Interconnection
NPCC
RFC
SERC
FRCC
MRO
SPP
TRE
WECC
ASCC
Interconnection


Color Key:
Black: Generation
Blue: Transmission
Green: Distribution
Generating Station
Generating Step Up Transformer
Transmission lines
765, 500, 345, 230, and 138 kV
Transmission Customer
138kV or 230kV
Substation Step Down Transformer
Subtransmission Customer
26kV and 69kV
Primary Customer
13kV and 4kV
Secondary Customer
120V and 240V

Visualizing The U.S. Electric Grid

The U.S. electric grid is a complex network of independently owned and operated power plants and transmission lines. Aging infrastructure, combined with a rise in domestic electricity consumption, has forced experts to critically examine the status and health of the nation's electrical systems.

About This Map »

Click on the links below to switch layers on and off.

EXISTING LINES

- 345-499 kV
- 500-699 kV
- 700-799 kV
- 1,000 kV (DC)

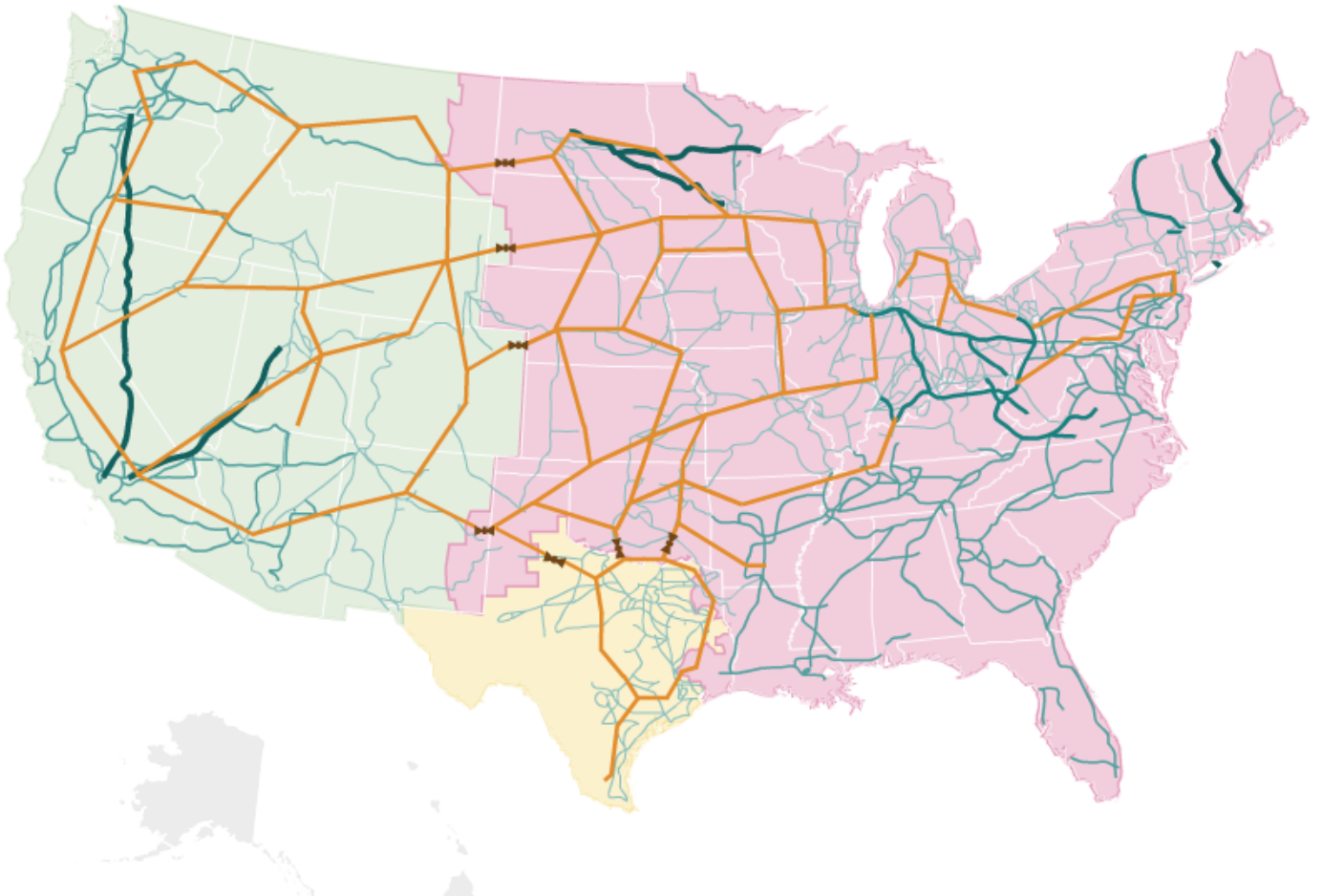
PROPOSED LINES

- New 765 kV
- AC-DC-AC Links

INTERCONNECTIONS

Major sectors of the U.S. electrical grid

- Eastern
- Western
- Texas (ERCOT)



Source: American Electric Power, American Wind Energy Association, Center for American Progress, Department of Energy, Edison Electric Institute, Energy Information Administration, Electric Power Research Institute, Federal Energy Regulatory Commission, National Renewable Energy Laboratory, U.S. Environmental Protection Agency, Western Resource Advocates

Credit: Producer: Andrew Prince; Designer: Alyson Hurt; Editors: Avie Schneider and Vikki Valentine; Supervising Editors: Anne Gudenkauf and Quinn O'Toole; Additional Research: Jenny Gold; Database and GIS Analysis: Robert Benincasa

Map of Power Reactor Sites

List of Power Reactor Units

Page Last Reviewed/Updated Thursday, March 29, 2012

Verdict Shows Samsung Needs to Copy Apple Design Culture
Q

Fracking Boom Seen Aiding Obama in Ohio
Q

Singapore Mega-Church Faithful Invest in Malls
Q

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

By Michael Riley and Dune Lawrence - Jul 26, 2012 7:00 PM ET

56 COMMENTS Q QUEUE

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.

July 30 (Bloomberg) -- Bloomberg's Megan Hughes reports on the work of a Chinese hacking group that is

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

believed to have breached the electronic security of various institutions around North America and Europe, from government agencies to large private companies. (Source: Bloomberg)

July 30 (Bloomberg) -- Bloomberg's Megan Hughes reports on the w ide-ranging targets of a Chinese hacking group and the U.S. researchers w ho unveiled their plot, w atching and tracking their every keystroke. (Source: Bloomberg)

July 27 (Bloomberg) -- Alex Lanstein, systems architect at FireEye Inc., talks about China-based hacking operations targeting U.S. companies. (Source: Bloomberg)

Enlarge image

Digital tracks have given investigators a hacker's eye view of China's cyber spies. Photographer: Qilai Shen/Bloomberg

Enlarge image

The Comment group is named for its trademark of infiltrating computers using hidden HTML code know n as "comments." These are screenshots of the w ebsite for Pietro's, a restaurant in New York, w here a command is left behind in HTML code.

Enlarge image

As Euro Zone countries struggled to

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. (HAL) 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. (ITC)

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 (LNKD) -- 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

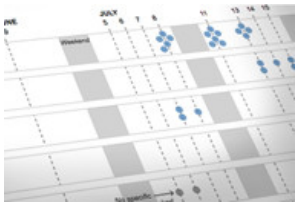
The methods behind China-based looting of technology and

hash out agreements on the Greek bailout and future of the European Union last summer, the hackers rifled the computers of European Council president Herman Van Rompuy and his advisors. Photographer: Jock Fistick/Bloomberg

Enlarge image

A leaked state department cable identified Byzantine Candor as Shanghai-based and linked it directly to China's military, the People's Liberation Army. Photographer: Sim Chi Yin/Bloomberg

Enlarge image



The Comment group of hackers is extraordinary for the scope of its activities and the number of victims. w ell over 20 in less than a month of activity.

Enlarge image

The Comments Group succeeded in breaking into the computer netw ork of the Diablo Canyon nuclear plant in California. Photographer: David Paul Morris/Bloomberg

Enlarge image

The Rongguang Building, a commercial block on Changshun Road in Shanghai is an address used to register multiple IPs linked to a major hacking group in

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.

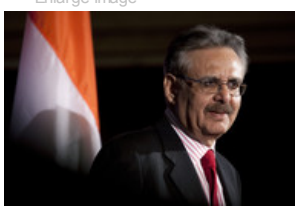
Private researchers have identified 10 to 20 Chinese hacking groups but said they vary significantly in activity and size, according to government investigators and security firms.

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

China, which has hit victims from government leaders to big corporations. Photographer: Liza Lin/Bloomberg

Enlarge image



In one hack tracked by the researchers, the spies breached the network of ITC Ltd., a technology and tobacco conglomerate headed by influential Indian businessmen Y. C. Deveshwar. Photographer: Joshua Roberts/Bloomberg

Enlarge image

Byzantine Candor has been linked to a string of high profile hacks never attributed to a specific group before, including a multi-year assault against the defense contractor QinetiQ. Photographer: Chris Ratcliffe/Bloomberg

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 (BATS) 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. (DELL), 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?"

To contact the reporters on this story: Michael Riley in Washington at michaelriley@bloomberg.net; Dune Lawrence in New York at dlawrence6@bloomberg.net

To contact the editor responsible for this story: Melissa Pozsgay at mpozsgay@bloomberg.net; Michael Hytha at mhytha@bloomberg.net

Bloomberg moderates all comments. Comments that are abusive or off-topic w ill not be posted to the site. Excessively long comments may be moderated as w ell. Bloomberg cannot facilitate requests to remove comments or explain individual moderation decisions.

Like  and 2 others liked this.

Add New Comment

Login

Type your comment here.

Showing 3 Of 56 Comments On Hackers Linked to China's Army Seen From EU to D.C.

dk01ndkfnsdd 1 month ago

Chinese Military...no surprise. This is what happens when you invest in a totalitarian dictatorship assuming they will become a free society and a friend to the West and its neighbors. China is an adversary and Western Industry is acting like naive teenagers at their first dance. Lenin once said, "the West will sell them (Soviets) the rope to hang themselves (us) with". That needs to be updated. The West will outsource the making of the rope to the Chinese to hang ourselves with.

Like Reply

andao 1 month ago

Once again the FBI and anti-virus companies tell us how badly we're being hacked and how many billions of dollars worth of info is being stolen, and once again the response is...do absolutely nothing.

Like Reply

Cédric Boitte 1 month ago

A chinese Echelon (who needs far less equipment).

1 Like Like Reply

Load more comments

Recommended Stories

Singapore Mega-Church Faithful Invest in Malls: Southeast Asia
Q

Merkel, Monti Lead Diplomatic Push as Draghi's Plan Takes Shape
Q

Gold Wagers on Rally Jump to Five-Month High on Stimulus
Q

Biggest Airline Debt Spurs GoI Asset Sale Talk
Q

Ohio's Gas-Fracking Boom Seen Aiding Obama in Swing State
Q

Samsung Tokyo Victory Shows U.S. Jury Verdicts Don't Sway Judges
Q