Exclusive: Operation Shady rat—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza

For at least five years, a high-level hacking campaign—dubbed Operation Shady rat—has infiltrated the computer systems of national governments, global corporations, nonprofits, and other organizations, with more than 70 victims in 14 countries. Lifted from these highly secure servers, among other sensitive property: countless government secrets, e-mail archives, legal contracts, and design schematics. Here, *Vanity Fair*'s Michael Joseph Gross breaks the news of Operation Shady rat's existence—and speaks to the McAfee cyber-security expert who discovered it.

Photographs by Molly Riley/Reuters/Landov (Hillary) and Paul Sakuma/A.P. Images (Google); illustration by Brad Holland (center).

When the history of 2011 is written, it may well be remembered as the Year of the Hack.

Long before the saga of *News of the World* phone hacking began, stories of computer breaches were breaking almost every week. In recent months, Sony, Fox, the British National Health Service, and the Web sites of PBS, the U.S. Senate, and the C.I.A., among others, have all fallen victim to highly publicized cyber-attacks. Many of the breaches have been attributed to the groups Anonymous and LulzSec. Dmitri Alperovitch, vice president of threat research at the cyber-security firm McAfee, says that for him, “it’s been really hard to watch the news of this Anonymous and LulzSec stuff, because most of what they do, defacing Web sites and running denial-of-service attacks, is not serious. It’s really just nuisance.”

"Just nuisance," that is, compared with a five-year campaign of hacks that Alperovitch discovered and named Operation Shady rat—a campaign that continues even now, and is being reported for the first time today, by vanityfair.com, and in a lengthier report on the larger problem of industrial cyber-espionage in the September issue of *Vanity Fair*. Operation Shady rat ranks with Operation Aurora (the attack on Google and many other companies in 2010) as among the most significant and potentially damaging acts of cyber-espionage yet made public. Operation Shady rat has been stealing valuable intellectual property (including government secrets, e-mail archives, legal contracts, negotiation plans for business activities, and design schematics) from more than 70 public- and private-sector organizations in 14 countries. The list of victims, which ranges from national governments to global corporations to tiny nonprofits, demonstrates with unprecedented clarity the universal scope of cyber-espionage and the vulnerability of organizations in almost every category imaginable. In Washington, where policymakers are struggling to chart a strategy for combating cyber-espionage, Operation Shady rat is already drawing attention at high levels. Last week, Alperovitch provided confidential briefings on Shady rat to senior White House officials, executive-branch agencies, and congressional-committee staff. Senator Dianne Feinstein (D-CA), chairman of the Senate Select Committee on Intelligence, reviewed the McAfee report on Shady rat and wrote in an e-mail to *Vanity Fair:* "This is further evidence that we need a strong cyber-defense system in this country, and that we need to start applying pressure to other countries to make sure they do more to stop cyber hacking emanating from their borders." McAfee says that victims include government agencies in the United States, Taiwan, South Korea, Vietnam, and Canada, the Olympic committees in three countries, and the International Olympic Committee. Rounding out the list of countries where Shady rat hacked into computer networks: Japan, Switzerland, the United Kingdom, Indonesia, Denmark, Singapore, Hong Kong, Germany, and India. The vast majority of victims—49—were U.S.-based companies, government agencies, and nonprofits. The category most heavily targeted was defense contractors—13 in all.

In addition to the International Olympic Committee, the only other victims that McAfee has publicly named are the World Anti-doping Agency, the United Nations, and ASEAN, the Association of Southeast Asian Nations (whose members are Indonesia, Malaysia, the Philippines, Singapore, Thailand, Brunei, Burma [Myanmar], Cambodia, Laos, and Vietnam).

In an e-mail to vanityfair.com, I.O.C. communications director Mark Adams wrote, "If proved true, such allegations would be disturbing. However, the IOC is transparent in its operations and has no secrets that would compromise either our operations or our reputation." WADA spokesman Terence O'Rourke wrote in an e-mail that "WADA is constantly alert to the dangers of cyber hacking and maintains a vigilant security system on all of its computer programs." He added that "WADA's Anti-Doping Administration & Management System (ADAMS), which is on a completely different server to WADA's emails, has never been compromised and remains a highly-secure system for the retention of athlete data."

A prominent cyber-security expert who was briefed by McAfee on the intrusions says that the Associated Press was also a victim. McAfee declined to comment on that suggestion. Jack Stokes, A.P. media-relations manager, said, "We don't comment on our network security," when I asked if it was true that the A.P. was among Shady rat's victims. Alperovitch believes the hacking was state-sponsored, pointing to Shady rat's targeting of Olympic committees and political nonprofits as evidence, and contending that "[t]here's no economic gain" to spying on them. Citing McAfee company policy, he refused to speculate on which country was behind Shady rat.

One leading cyber-espionage expert, however, thinks the likely culprit's identity is clear. "All the signs point to China," says James A. Lewis, director and senior fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies, adding, "Who else spies on Taiwan?"

Alperovitch first picked up the trail of Shady rat in early 2009, when a McAfee client, a U.S. defense contractor, identified suspicious programs running on its network. Forensic investigation revealed that the defense contractor had been hit by a species of malware that had never been seen before: a spear-phishing e-mail containing a link to a Web page that, when clicked, automatically loaded a malicious program—a remote-access tool, or rat—onto the victim's computer. The rat opened the door for a live intruder to get on the network, escalate user privileges, and begin exfiltrating data. After identifying the command-and-control server, located in a Western country, that operated this piece of malware, McAfee blocked its own clients from connecting to that server. Only this March, however, did Alperovitch finally discover the logs stored on the attackers' servers. This allowed McAfee to identify the victims by name (using their Internet Protocol [I.P.] addresses) and to track the pattern of infections in detail.

The evolution of Shady rat's activity provides more circumstantial evidence of Chinese involvement in the hacks. The operation targeted a broad range of public- and private-sector organizations in almost every country in Southeast Asia—but none in China. And most of Shady rat's targets are known to be of interest to the People's Republic. In 2006, or perhaps earlier, the intrusions began by targeting eight organizations, including South Korean steel and construction companies, a South Korean government agency, a U.S. Department of Energy laboratory, a U.S. real-estate company, international-trade organizations of Western and Asian nations, and the ASEAN Secretariat. (According to McAfee's "Operation Shady rat" white paper, "[t]hat last intrusion began in October [2006], a month prior to the organization's annual summit in Singapore, and continued for another 10 months.") In 2007, the activity ramped up to hit 29 organizations. In addition to those previously targeted, new victims included a technology company owned by the Vietnamese government, four U.S. defense contractors, a U.S. federal-government agency, U.S. state and county government organizations, a computer-network-security company—and the national Olympic committees of two countries in Asia and one in the West, as well as the I.O.C. The Olympic organizations, strikingly, were targeted in the months leading

up to the 2008 Olympic Games in Beijing. Shady rat's activity continued to build in 2008, when it infiltrated the networks of 36 organizations, including the United Nations—and reached a crest of 38 organizations, including the World Anti-doping Agency, in 2009. Since then, the victim numbers have been dropping, but the activity continues. Shady rat's command-and-control server is still operating, and some organizations, including the World Anti-doping Agency, were still under attack as of last month. (As of Tuesday, according to a WADA spokesman, the group was unaware of any breach, but "WADA is investigating" McAfee's discovery.) The longest compromise duration—"on and off for 28 months," according to McAfee's report—was one Asian country's Olympic committee. Many others were compromised for two full years. Nine organizations were compromised for one month or less. All others were compromised for a minimum of one month, potentially allowing for complete access to all data on their servers.

Alperovitch says that McAfee is "working closely with U.S.government agencies, a variety of them, law enforcement and others," in hopes of eventually shutting down Shady rat's command-and-control server. (He declined to say whether U.S. intelligence agencies are involved in the investigation.)

Alperovitch's diagnosis of the problem raised by Shady rat is troubling: "It's clear from this and other attacks we've been witnessing that there is an unprecedented transfer of wealth in the form of trade secrets and I.P., primarily from Western organizations and companies, falling off the truck and disappearing into massive electronic archives. What is happening to this data? Is this being accumulated in a giant, Indiana Jones–type warehouse? Or is it being used to create new products? If it's the latter, we won't know for a number of years. But if so, it's not just a problem for these companies, but also for the governments of the countries where these companies are located, because they're losing their economic advantage to competitors in other parts of the world overnight. That is a national-security problem, insofar as it leads to loss of jobs and lost economic growth. That's a serious threat."

His account of attempting to inform some of Shady rat's victims may be even more troubling. Some victims seem determined to deny they've been attacked, even when offered empirical proof that a smash-and-grab has taken place. Two weeks ago, McAfee sent e-mails to officials at four organizations, informing them that their computer networks had been compromised. To each, Alperovitch wrote, "We would be glad to work with you and provide our assistance … to help you determine the impact of the intrusion … or how to prevent this type of infiltration in the future." Three of those organizations—including one whose breach is ongoing—made no response to McAfee's notifications. Even after McAfee's second attempt to offer information about the breaches to two of the groups, Alperovitch says, they expressed no interest in learning details of the intrusions. The spokesman for one of those organizations, WADA, told me that he considered Alperovitch's first e-mail to be "spam." He said, "We are conducting our own investigation of the allegations." When asked why WADA chose not to accept McAfee's offer to provide detailed information that could help in that investigation, the spokesman answered, "I am under no obligation to answer your questions about my investigation." (Later that day, according to McAfee, WADA did request information concerning the attack.)

"We've seen this before," Alperovitch says. "Victims don't want to know they're victims. I guess that's just victim psychology: if you don't know about it, it's not really happening."