

The Washington Post

Organized Crime Behind a Majority of Data Breaches

By Brian Krebs

washingtonpost.com Staff Writer

Wednesday, April 15, 2009; 10:22 AM

A string of data breaches orchestrated principally by a handful of organized cyber-crime gangs translated into the loss of hundreds of millions of consumer records last year, security experts say.

The size and scope of the breaches, some of which have previously not been disclosed, illustrate the extent that organized cyber thieves are methodically targeting computer systems connected to the global financial network.

Forensics investigators at Verizon Business, a firm hired by major companies to investigate breaches, responded to roughly 100 confirmed data breaches last year involving roughly 285 million consumer records. That staggering number -- nearly one breached record for every American -- exceeds the combined total breached from break-ins the company investigated from 2004 to 2007.

In all, breaches at financial institutions were responsible for 93 percent of all such records compromised last year, [Verizon reported](#). Unlike attacks studied between 2004 and 2007 -- which were characterized by hackers seeking out companies that used computer software and hardware that harbored known security flaws -- more than 90 percent of the records compromised in the breaches Verizon investigated in 2008 came from targeted attacks where the hackers carefully picked their targets first and then figured out a way to exploit them later.

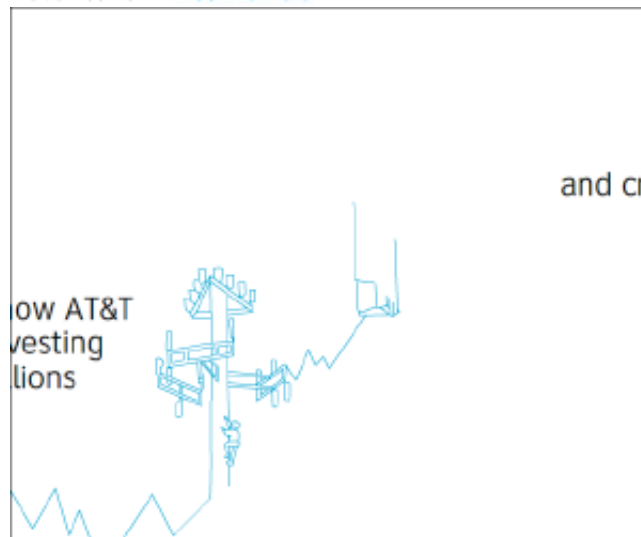
Bryan Sartin, director of investigative response at Verizon Business, said criminals in Eastern Europe played a major role in breaches throughout 2008.

"About 50 percent of the confirmed breach cases we investigated shared perpetrators," Sartin said. "Organized crime is playing a much larger part of the caseload we're seeing. We've seen that both [the FBI] and the Secret Service have initiatives underway to go back through their cyber crime case histories over the past several years, to start tying together all of the common characteristics of the attacks to individuals, to really try and get a firm handle on the individuals responsible for these attacks."

For example, a single organized criminal group based in Eastern Europe is believed to have hacked Web sites and databases belonging to hundreds of banks, payment processors, prepaid card vendors and retailers over the last year. Most of the activity from this group occurred in the first five months of 2008. But some of that activity persisted throughout the year at specific targets, according to experts who helped law enforcement officials respond to the attacks, but asked not to be identified because they are not authorized to speak on the record.

Shawn Henry, assistant director of the FBI's cyber division, said the bureau is making real progress in working with foreign law enforcement to track down the major sources of cyber crime.

Advertisement » Your Ad Here



"The sophistication of these attacks has gone up, the bravado has gone up, and our commitment is steadfast," Henry said. "We're working very closely with foreign law enforcement and with some of the victims, and we certainly recognize how significant these threats are coming from all over Eastern Europe."

One hacking group, which security experts say is based in Russia, attacked and infiltrated more than 300 companies -- mainly financial institutions -- in the United States and elsewhere, using a sophisticated Web-based exploitation service that the hackers accessed remotely. In an 18-page alert published to retail and banking partners in November, VISA described this hacker service in intricate detail, listing the names of the Web sites and malicious software used in the attack, as well as the Internet addresses of dozens of sites that were used to offload stolen data.

"This information was recently used by several entities to discover security breaches that were otherwise undetected," VISA wrote.

The Washington Post obtained a partial list of the companies targeted by the Russian hacking group from a security researcher, which was left behind on one of the Web servers the attackers used. More than a dozen companies on that list acknowledged first learning about intrusions after being contacted by law enforcement agencies tracking the activities of the cyber gang.

This group's most high profile and lucrative haul last year came from Atlanta-based payment processor and payroll card giant RBS WorldPay. In that attack, which the company disclosed on Dec. 23, 2008, the hackers siphoned nearly \$10 million from the U.S. banking system by artificially inflating the balances on prepaid credit or cash cards. The thieves extracted money from the system by distributing the cards to dozens of so-called "money mules," who used them to withdraw millions in cash from ATMs in cities across the country in a coordinated heist that took less than 24 hours.

The same hacking group also was responsible for a breach last year at Okemo Mountain Ski Resort in Ludlow, Vermont. In that attack, which Okemo disclosed on April 1, 2008, the criminals stole payment data encoded on more than 28,000 credit and debit card that the company processed from skiers during a 16-day period in early February.

A month prior to that, this hacker group broke into OmniAmerican Bank, based in Fort Worth, Texas. As a result, criminals were able to fabricate debit cards and PINs, and then withdraw an undisclosed amount of cash from ATMs in Russia and Ukraine.

Other breaches attributed to this group has not been disclosed until now. The Web site for Euronet Worldwide, a Leawood, Kan., based electronic payment processor that operates a major ATM network in Europe, Asia and the Middle East, also was included on the hacker group's hit list. Euronet spokeswoman Shruthi Fielder confirmed that the company learned in March 2008 that "a portion of its Indian subsystem was attacked by a sophisticated cyber-crime group through a Web-facing program." Data concerning 38,000 bankcards was compromised in the breach. The company said it did not previously disclose the breach until contacted by a Washington Post reporter because the victims resided outside of the United States and beyond the reach of domestic data breach disclosure laws.

The attackers weren't always able to make off with cash or bank account data after successfully breaching a financial institution last year. The same group of attackers also broke into TSYS, currently the world's second largest credit and debit card processor on March 8, 2008.

TSYS spokesman Cyle Mims said the break-in was quickly detected and contained by the company's security staff.

"We found out about it and corrected it within hours, and no proprietary data of any kind was taken," Mims

said, adding that the FBI contacted the company several months later to inform them that TSYS systems may have been targeted.

Attackers in this group also went after FirstData ATM Services, a division of Greenwood Village, Colo., based payment processor First Data Corp., which provides technology-based ATM and POS solutions to financial institutions and independent sales organizations nationwide.

A spokeswoman for the FirstData declined to say whether the attackers were successful in breaking in. The company would say only that no personal data was stolen.

"As with many other commercial Web sites, firstdataatm.com experiences unauthorized attempts to access information contained within the site," the company said in a written statement. "Our security infrastructure has been able to detect and prevent the unauthorized access of any personal information from the site."

Experts say a different cyber-crime gang operating out of Eastern Europe was responsible for what may turn out to be last year's biggest cyber heist. Princeton, N.J., based credit card processor Heartland Payment Systems disclosed on Jan. 20 that hackers had breached its systems last summer, planting malicious software designed to capture and secretly siphon account numbers as they traversed the company's internal processing networks.

Heartland, which processes roughly 100 million credit and debit card transactions per month, hasn't disclosed how many accounts may have been compromised. Company officials declined to comment for this story, citing pending class-action litigation against Heartland by entities affected by the breach. But so far, more than 600 banks have reported cards compromised as a result of the Heartland breach, according to Bankinfosecurity.com.

Steve Santorelli, director of investigations at Team Cymru, a small group of researchers who work to discover who is behind Internet crime, said the hackers behind the Heartland breach and the other break-ins mentioned in this story appear to have been aware of one another and unofficially divided up targets.

"There seem, on the face of anecdotal observations, to be at least two main groups behind many of the major database compromises of recent years," Santorelli said. "Both groups appear to be giving each other a wide berth to not to step on each others' toes."

In Feb. 2009, the Secret Service and FBI issued a rare joint advisory through VISA's Web site, warning banks and retailers about the techniques the hackers were using and some of telltale signs that hackers may have broken in.

"Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry," the advisory begins. It goes on to list a variety of methods online merchants can use to detect and block the most common types of attacks.

In all of specific attacks mentioned above, the methods used and tools used by the hackers were remarkably similar: The crooks scanned hundreds of financial company Web sites or partner sites for known security holes. Once they had exploited those holes and had made their way to the target's internal network, the attackers would install a variety of hacking tools and begin mapping the network.

According to the FBI and Secret Service, those tools usually included "sniffer" programs designed to capture credit and debit card information flowing across the bank or processor's internal networks. In addition, the crooks also installed "beacons" that allowed the attackers to connect back to the hacked sites in the future, as well as offload stolen data.

Verizon's Sartin, said hackers last year mostly went after entities that held large stores of debit card information and corresponding PINs, information that criminals could use to extract cash from ATMs once they had imprinted the stolen data on fabricated cards.

Unlike credit card fraud, debit card fraud often hits consumers directly in the pocketbook.

"ATM fraud is a much different story, because meanwhile your cash assets are missing and the burden is now on you to prove that it wasn't you who took all the money out of the account," Sartin said.

Nicholas Percoco, vice president of SpiderLabs, the incident response department at Chicago-based security vendor Trustwave, said that the methods described by federal investigators are consistent with a large number of the successful break-ins they examined.

Percoco said a majority of the breaches at financial institutions last year show strong signs of being the work of organized criminal gangs in Russia and Eastern Europe.

In August 2008, the Justice Department announced its largest identity theft and hacking case ever prosecuted, against 11 members of what it called "international hacking rings" allegedly responsible for the theft and sale of more than 40 million debit and credit card numbers stolen from various retailers, including JX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW.

Sartin said that regardless of whether the criminals behind these attacks are apprehended, the breach reports from last year will be trickling in for some time, while other breaches may never be disclosed.

"About a third of the breaches investigated by our team last year are publicly disclosed. More, especially those toward the end of the year, are likely to follow. Others will likely remain unknown to the world as they do not fall under any legal disclosure requirements," he said.

[View all comments](#) that have been posted about this article.

Post a Comment

[View all comments](#) that have been posted about this article.

You must be logged in to leave a comment. [Login](#) | [Register](#)

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the [full rules](#) governing commentaries and discussions. You are fully responsible for the content that you post.