SECURITY dark READING
Protect The Business Enable Access

'Freakshow' Provides Inside Look At Real Malware Behind Big Breaches

Forensic specialists who investigated hacks of a hotel chain, casino, and restaurant share details on the sophisticated malware used to successfully steal confidential data

By Kelly Jackson Higgins, DarkReading
Aug. 31, 2009
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=219500666

They planted malware that siphoned data from memory, deployed a bot, and camouflaged a keylogger, but all three of these real attacks were after the same thing: credit and debit-card data.

Nicholas Percoco, senior vice president of SpiderLabs, and Jibran Ilyas, senior forensics investigator at SpiderLabs, will talk about real and unique malware they discovered in major forensics investigations of breaches at a hotel chain, a casino, and a restaurant at the upcoming SecTor security conference in Toronto in a session entitled "Malware Freakshow."

"The old way was 'smash and grab,' where they'd find a database and the data they were looking for, download it, and leave," Percoco says. "Today they're going in and camping out for months or years. They're learning those systems better than the IT admins running them."

The malware samples the researchers will highlight at SecTor are all different, but with the main goal of grabbing credit and debit card data off the wire, input device, or from memory in hopes of selling them or creating counterfeit cards. The cases were a hotel in New York, a casino in Las Vegas, and a restaurant in Michigan, and they also had in common weak network controls: "A lot of their perimeter controls were very lax," Percoco says. "A simple vulnerability got them in."

In two of the cases, the attackers targeted a particular victim from the get-go; in the the other, they stumbled onto the victim. "Once the attacker first gets into the system, he uses reconnaissance malware that tells them these special processes [indicate] it's a hotel or restaurant," Percoco says.

One of the most advanced attack methods of the three breaches was the so-called "memory dumping" performed on the hotel chain to steal credit-card data. The attackers initially got inside a member hotel via its LAN, according to the researchers, which is where most hotels' computer systems also run.

In a memory-dumping attack, the attacker reads the unencrypted transaction or other information that sits in memory before it goes to the actual application. The hotel attack included several pieces of malware, including code that dumps the contents of the memory onto the attacker's machine, and another that performs data parsing. "One piece installs itself as a service so the malware can come back when it needs to boot up," Ilyas says.

Attackers are moving to methods like memory dumping to steal card information because more and more databases are getting encrypted, as are point-of-sale applications. "Once they get that track data, they can make counterfeit credit cards out of it," Percoco says. "They're trying to get the data as soon as it's swiped, like a keylogger. But some AV products are picking up keyloggers, so attackers are going to memory dumping."

Memory dumping isn't usually detected as malicious because many debuggers work similarly, he says.

The attackers were able to infiltrate the network and guess a weak administrative password on the hotel's own server. Then they used their parsing malware to search for credit and debit-card information and "dumped that data to disk," Percoco says.

The stolen card information was encrypted using a Russian version of a popular archiving and compression tool, the researchers say, which was their only clue to the actual attackers themselves. "But they were exporting the data to a system in South Korea," Percoco says.

Remaining under the radar is crucial for these types of attacks, and they typically get discovered only when the credit card company contacts the victim with reports of a wave of credit card fraud cases affecting customers who stayed at the hotel or shopped at the store, for instance.

"If they stay in the system long enough, say three months, they can learn it and test all of their activity, like memory dumping and data parsing on one computer...and if they know [the hotel's] 35 other locations are using the exact same infrastructure, then they exploit those other locations," Ilyas says. In the Las Vegas casino club's breach, the attackers planted an elusive keylogger that stole credit and debit card numbers. Even if the casino's IT staff had been running tools to look for suspicious programs, they wouldn't have found it, Ilyas says. "It was hidden from the system...we went in and found its processes running," he says. "The keylogger was just targeting the processed credit card transactions."

The casino had been hit by previous malware infections and thought they were clean after cleaning them up. But not so: "In this case, their systems got infected with a couple of other things, and they had written them off as benign," Ilyas says. "This happens quite often as viruses are always floating around in corporate networks...The casino administrator saw something [more] was going on."

In the restaurant breach in Michigan, the establishment's server was bot-infected and then used to help plant a malicious packet sniffer between the point-of-sale system and server. The restaurant didn't encrypt its internal point-of-sale application traffic, so it became an easy mark for the bad guys to steal its card data. They sent configuration files via Internet Relay Chat (IRC) for the malware.

The attack was more random than targeted -- the bad guys had discovered an open port at the site while scanning the geographic area. "This sniffer attack is unique because of the IRC capability -- usually people use commercial sniffers, but this one was custom-designed," Percoco says. And the sniffer required a Microsoft .NET framework, so the attackers downloaded .NET to the victim's machine.

"They had to upgrade the system to make it work."

Percoco and Ilyas, meanwhile, also plan to reveal a new, bleeding-edge generation of malware they call "credential malware," which is a rare but powerful tool for attacking kiosks, such as DVD rental machines. They wouldn't provide any details of the victim that was hit by the attack, but they used an example of a fictional video poker machine to illustrate it.

The attack initially requires physical contact with the kiosk: someone posing as a repairman, for instance, could install the malware, which is aimed at stealing data from these types of closed-network devices. "The chances of getting data out via the Internet from these machines are very slim. The only way to get the data you're looking for is to go face-to-face with that device, and they have limited interfaces and no keyboards," Percoco says.

So malware writers have created special code that can use the limited controls available in a kiosk machine. "The malware has a password file embedded in this, and when it sees a particular string of data, it activates," he explains.

The researchers will demonstrate how specially crafted paper vouchers, such as those you get when you cash out of a slot machine, act as the interface to the poker machine in order to steal credit and debit-card data. "We've seen in some cases criminals getting jobs to repair machines or work in a restaurant to get the malware onto the [kiosk] system," he says.

Have a comment on this story? Please click 'Discuss' below. If you'd like to contact Dark Reading's *editors directly, send us a message.*