
Print

How a Las Vegas casino was infected by malware

The biggest threat to your POS terminals is a malware infection, according to security experts at this week's SecTor conference in Toronto. Read about three real attacks and how the hackers were able to so easily infect, control, and export data from these terminals

By: Rafael Ruffolo

ComputerWorld Canada (07 Oct 2009)

Malware represents the biggest threat to point-of-sale terminals and servers, with everyone from Las Vegas casinos to name-brand restaurants and hotels still failing to protect against the attack, according to Chicago-based data security firm Trustwave Inc.

Speaking to IT security professionals at Wednesday's SecTor security conference in Toronto, two experts from Trustwave's SpiderLabs security team hammered home just how easy it is for a hacker to enter into the average POS machine.

For Nicholas Percoco, head of SpiderLabs, the target for cyber criminals is the compute memory and data input. Typical vulnerabilities include the lack of a segmented network, weak passwords (often set to whatever default the original system integrator used), poor logging and monitoring practices, ineffective firewalls, and outdated hardware.

Hackers are increasingly getting their hands on administrative passwords and infecting these machines right under the nose of IT administrators. These attackers can often steal credit card information or other sensitive data for upwards of two years without being detected, Percoco said.

"We've had cases where literally the hardware was full of (the hacker's stolen) data, so IT actually went out and bought more disk space," Percoco said, adding that while IT administrators often suspects something is fishy, they usually just brush it off as a normal upgrade.

Over the last year, Percoco and his team have performed about 150 forensic investigations. In his conference speech, he along with his senior forensic analyst at SpiderLabs, Jibran Ilyas, outlined a few typical attacks and where the companies went wrong.

What happens in Vegas doesn't always stay in Vegas

Sometimes it doesn't matter if an organization's POS terminals allow their employees to access the Internet or not.

At an unnamed club connected to a major Las Vegas casino, the fatal flaw for its POS server was that it allowed online access for the systems integrator to provide remote desktop support. The problem with that, Percoco said, was that both the username and password was simply the POS vendor's name.

"Most default passwords are well-known by attackers," he added.

In this case, the POS terminals actually contained customer data from the two previous owners of the systems, which means that the integrator bought the terminal used and didn't properly wipe out its data.

"Another big problem was the casino's network was very flat and lacked physical network security controls," Percoco said.

This allowed the hacker to come in through the remote desktop, easily figuring out the username and password, and then downloading an unprotected SFX archive from an FTP site. This archive contained a keylogger and a PuTTY executable, which is terminal emulator app used to remote-control the system.

All of these files were hidden and would probably go unnoticed to the average IT administrator, Percoco added. On top of that, when the malware runs, it creates an encrypted file of all the credit card data it collects, meaning that even if an administrator were to discover this file and open it up in WordPad, its contents would be a jumbled mess.

"They're capturing (all the credit card data) from the input device, intercepting it before it even goes to the application," Llyas said, adding that if the data were to get into the terminal, it would be encrypted and then erased.

Another trick to throwing off the scent, according to Llyas, is the fact that the malware sometimes disguises itself as a Windows update file, leading the average IT administrator to actually think their computer is being patched.

Four of a kind, all the time

Sticking on the casino theme, Percoco also presented a case study about some video poker machines in Lake Tahoe, Calif., introducing the concept of credentialed malware, which is aimed at systems without an external network or Internet access.

Because these poker machines are controlled by tokens or ticket vouchers, hackers have to use a different method to exploit the terminal's functions. Often, criminals will disguise themselves as repair personnel and access the inner workings of the machine through those means.

For Percoco, the best defence against this is obviously proper security monitoring techniques, but this is still lacking in some casinos.

Inside the poker machines are often low-end PCs, Percoco said, and usually have similar, vendor-default passwords assigned to them. Hackers can quickly infect these machines via USB keys.

Some machines are even infected at the factory level and many times go completely unchecked by casino security staff, he said.

Once a hacker has an infected machine, without a keyboard or mouse, they are able to control the malware via the various "hold," "bet," and "fold" buttons, Percoco said. The hold buttons might be able to modify the odds of the machine, modify the amount of credits the user has (basically allowing them to steal as much money as they want), or uninstall the malware when they are finished using it.

If it can make it there, it can make it anywhere

In addition to casinos, hotels and restaurants also see a heavy dose of daily credit card activity.

Earlier this year, Percoco conducted an investigation at a name-brand hotel in New York.

The POS terminal and servers were set up up in a similar fashion to the casino club, but with one exception. "There was a connection up to the hotel's corporate offices, which in turn had connections back to hundreds of locations across the country," Percoco said.

The architecture problems didn't stop there, he said, adding that no anti-virus programs were installed on the hotel's systems, the firewall was nothing more than a consumer router, and the whole environment lacked any kind of network segmentation.

Llyas added that the hotel's Wi-Fi was actually on same network as the POS systems.

In this case, the hackers were able to branch out to 35 of the hotel's locations and steal an enormous amount of credit card data. The attackers used variations of the same techniques found in the casino club, covering their tracks by encrypting the data they were stealing and hiding suspicious files from the administrators.

And because of their malware techniques actually required it, the hackers were even running Windows patches and updates to ensure their malicious programs would actually run properly.