Hackers Hit Vacation Spots

Peter Silva, 2011-14-09

Just when you were having all that fun running around the waterpark and playing those arcade games comes news that the card processing system of Vacationland Vendors Inc., a Wisconsin Dells firm that supplies arcade games and installs vending machines, was breached. From the notice on their website, they say, '*Vacationland Vendors recently discovered that an unauthorized person wrongfully accessed certain parts of the point of sales systems that Vacationland Vendors uses to process credit and debit transactions at the Wilderness Resorts*.' Up to 40,000 debit or credit cards that were used in the arcades any time between December 2008 to May 2011 at the Wilderness Waterpark Resort near Wisconsin Dells and a companion resort in Tennessee are potentially compromised. The hackers, according to Vacationland Vendors, improperly acquired credit card and debit information and around 20 accounts have shown irregular activity. Reservation and restaurant transactions were not involved in the breach, only the point-of-sale devices. Malware was the apparent culprit.

Point-of-sale devices and the networks they are connected to are often the target of malicious hackers. These 'kiosks' are typically unattended and might be in locations where observation is limited. A couple years ago, Target's breach was the result of hackers gaining access via the customer service kiosks and the huge hit at Heartland Payment Systems, resulting in tens of millions of exposed credit and debit cards was from a breach of the company's point-of-sale network. After successful installation of malicious software, thieves are able to sniff and intercept payment card data as the information is transmitted within the internal network or to the bank for authorization. It might not even be encrypted as it travels. If it was, then the crooks wouldn't have the info. Many people may think these kiosk point-of-sale devices are safe since it is taking credit card data and merchants need to be PCI compliant. While the overall deadline for PCI 1.2 compliance was a couple years ago (and PCI 2.0 at the end of this year), the deadline for unattended point-of-sale devices was July 2010, a little over a year ago. That's why you've seen a whole slew of new gas station pumps at your favorite fueling stations and just like regular compliance, it's going to take time to update all the point-of-sale devices. Now, I'm not insinuating that the arcade devices were not PCI compliant since nothing has been reported about that, but what I am saying is be careful with those since you may not know if it is or not. If it looks a few years old, then most likely, it is not.

With this and other similar point-of-sale breaches, many security experts (and even the Heartland CEO) believe end-to-end encryption is necessary, even if transmitting on the internal network, from the time the card is swiped all the way until the data reaches the the processor or bank. Many credit card swipe terminal vendors are building encryption into the hardware itself and F5 can help keep that information encrypted while it's travelling the great unknown. Our BIG-IP APM and BIG-IP Edge Gateway (voted Best Secure Remote Access Product by TechTarget Readers) can easily encrypt any traffic, internal or external. Heck, even a couple BIG-IP LTM running our latest v11 code can initiate a secure tunnel between them, creating an instant, secure WAN connection.

With the advent of credit card swiping capabilities on mobile phones now in full force, I'm not sure if this is going to get better or worse. The terminal might be fine but if you install a hacked mobile payment app, then you can skim credit card info like the pros. Remember, humans will often trade privacy for convenience.

ps

Related blogs & articles:

- Vending machine company announces major data breach
- Vending Company Reports Significant Data Breach
- Security breach affects card users tied to Wilderness arcade
- Vacationland Vendors Notice
- Encryption Anywhere and Everywhere
- Will you Comply or just Check the Box?
- PCI Turns 2.0
- CloudFucius Wonders: Can Cloud, Confidentiality and The Constitution Coexist?
- Identity Theft Resource Center

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com