KEVIN POULSEN SECURITY 05.01.13 6:00 AM

USE A SOFTWARE BUG TO WIN VIDEO POKER? THAT'S A FEDERAL HACKING CASE

kellyThe Game King in an IGT promotional photo.

ON MONDAY, JULY 6, 2009, two engineers from Nevada's Gaming Control Board showed up at the Silverton Casino Lodge. The off-the-strip Las Vegas casino is best known for its mermaid aquarium, but the GCB geek

squad wasn't there to see swimmers in bikini tops and zip-on fish tails. They'd come to examine machine 50102, a Game King video poker unit on the casino floor that had been waiting for them, taped off like a crime scene, all weekend.

Manufactured by International Game Technology – a gambling leviathan that boasts $2 billion in revenue a year — the Game King is the [redacted] keep [redacted]e play. Players can select from three cash levels and nearly three dozen different game variations, like Deuces Wild, Jacks or Better, Double Double Bonus and One-Eyes Jacks.

A Vegas local named John Kane had been the final player at machine 50102, and he'd opted for Triple Play Triple Double Bonus Poker, winning three hands at once at the maximum $10 denomination. His last game was still on the screen: three aces, four aces, three aces again. At payout odds of 820-to-1 he'd scored an $8,200 bonanza.

But the casino had been suspicious, and Kane didn't collect the last win. For one thing, Kane, now 54, had enjoyed a lot of big payouts that day: in about an hour he'd scored five jackpots large enough to require a hand pay and IRS paperwork. The GCB engineers yanked the machine's logic tray and EEPROM and took them back to the lab.

There they discovered the secret behind Kane's lucky streak: he was exploiting a previously-unknown firmware bug present in the Game King and nine other IGT machines – one that had been hidden for seven years.

Now Kane and the bug he exploited are at the center of a high-stakes legal battle before a federal judge in Las Vegas. The question: was it a criminal violation of federal anti-hacking law for Kane and a friend to knowingly take advantage of the glitch to the tune of at least half-a-million dollars? Prosecutors say it was. But in a win for the defense, a federal magistrate found last fall that the Computer Fraud and Abuse Act doesn't apply, and recommended the hacking charge be dismissed.

The issue is now being argued in front of U.S. District Court Judge Miranda Du, who's likely to rule this month.

It's the latest test of the Computer Fraud and Abuse Act, a 1986 law originally intended to punish hackers who remotely crack defense or banking computers over their 300 baud modems. Changes in technology and a string of amendments have pushed the law into a murky zone where prosecutors have charged people for violating website terms-of-service or an employer's computer use policies. After the January suicide of Aaron Swartz, who'd been charged under the CFAA and other laws, Representative Zoe Lofgren (D-CA) drafted "Aaron's Law" to reform the act. But that bill hasn't been introduced. In the meantime, Andrew "Weev" Auernheimer was sentenced last March to three-and-a-half years in prison under the CFAA for running a script that downloaded 120,000 customer e-mail addresses that AT&T exposed on their iPad support website.

In the Game King case, the arguments are largely focused on whether Kane and his codefendant, Andre Nestor, exceeded their legal access to video poker machines by exploiting the bug. Kane's attorney, Andrew Leavitt, says Kane played by the rules imposed by the machine, and that's all that matters.

"What you see in most gambling cheating cases is the guy's got a magnet in his boot or he's shocking the machine with static electricity." says Leavitt, a veteran Vegas defense attorney. "All these guys did is simply push a sequence of buttons that they were legally entitled to push."

In court filings, prosecutors counter that the complex series of button-presses Kane and Nestor used to exploit the bug makes it more akin to computer hacking than poker-playing. As detailed in GCB's report,

attached to a defense filing (.pdf), the bug was indeed complex.

Kane began by selecting a game, like Triple Double Bonus Poker, and playing it at the lowest denomination the machine allows, like the $1.00 level. He kept playing, until he won a high payout, like the $820 at the Silverton.

Then he'd immediately switch to a different game variation, like straight "Draw Poker." He'd play Draw Poker until he scored a win of any amount at all. The point of this play was to get the machine to offer a "double-up", which lets the player put his winnings up to simple high-card-wins draw. Through whatever twist of code caused the bug, the appearance of the double-up invitation was critical. Machines that didn't have the option enabled were immune.

At that point Kane would put more cash, or a voucher, into the machine, then exit the Draw Poker game and switch the denomination to the game maximum — $10 in the Silverton game.

Now when Kane returned to Triple Double Bonus Poker, he'd find his previous $820 win was still showing. He could press the cash-out button from this screen, and the machine would re-award the jackpot. Better yet, it would re-calculate the win at the new denomination level, giving him a hand-payout of $8,200.

It takes a lot of video poker play to stumble upon a bug like that. And Kane, according to his lawyer, played a lot of video poker. "He's played more than anyone else in the United States," claims Leavitt. "I'm not exaggerating or embellishing. ... In one year he played 12 million dollars worth of video poker" and lost about a million, he says. "It's an addiction."

It was during one of his video poker binges that Kane discovered the bug. "He accidentally hit a button too soon, and presto," says Leavitt, "It was a fluke. There was no research... Just playing."

When Kane found the double-up bug in April 2009, he contacted Nestor in Pennsylvania. Nestor, now 41, flew out to Vegas, and over the

following weeks one or both of the men allegedly showed up at the Fremont, the Golden Nugget, the Orleans, the Texas Station, Harrah's, the Rio, the Wynn, and the Silverton, beating the house everywhere they went.

"These guys kind of kept it a secret," says Leavitt. "If this had got out... this would have been a bad thing for the casinos."

In June, Nestor returned to Pennsylvania, and began working the exploit with a crew. He showed up at the casino of the Meadows Racetrack in Washington County with ex-cop Kerry Laverde, who acted as Nestor's bodyguard, occasionally flashing his old police badge to casino staff. Nestor's associate Patrick Loushil tagged along to collect some of the payouts, perhaps so they didn't all wind up on Nestor's tax bill.

With all the appearance of a high-roller, complete with entourage, Nestor was able to persuade a casino staffer to enable the double-up feature on an IGT Draw Poker machine in the Meadows' "high limit"

room. A supervisor immediately reversed the decision, and the staffer went through the procedure to turn off the feature again, but neglected to save the change.

It would prove a costly mistake. Nestor and his crew returned to that same machine 15 times over the next two months, collecting $429,945 from 61 payouts. (Adding insult to injury, the Meadows was later fined $48,900 for turning on the double-up feature without regulator approval.)

As Nestor played in Pennsylvania, Kane continued to work Vegas, until the Silverton incident put the bug in front of the Gaming Control Board's 25-person Technology Division. Formed in the mid-1980s as video gambling began its Las Vegas ascent, the Technology Division is the center of a vast software integrity operation: its computer and electrical engineers maintain a database of about 300,000 approved program variations, says its director. Over the course of three years, every location in Las Vegas with a gaming machine gets a visit from a GCB inspector, who cracks open the machines and checks the SHA-1 hashes against the database, to ensure that only approved code is taking money from the tourists.

The GCB also investigates suspected fraud and theft, sometimes reported by a casino, sometimes by a patron who's convinced a game machine isn't paying out properly. Much of the cheating the Technology Division deals with comes from professionals, who will buy a used game machine, put it in their garage and plumb it for vulnerabilities.

"They are looking to explore how they can exploit the machine from a mechanical standpoint," says Jim Barbee, chief of the division. That means physical hacks aimed at the coin hopper or the bill reader. Software vulnerabilities like Kane's are nearly unheard of. "I've been

here about 14 years, and in my tenure, none pop into mind other than the one that you're referring to," he says. "Possibly one or two others, but it is an extreme rarity"'

Using the Silverton's surveillance video as a tutorial, the GCB engineers quickly reproduced the Game King bug. They alerted IGT, which sent an urgent notice to its customers.

"Replacement programs are being expedited," the company wrote on July 7, 2009. "It is important to note that some of these programs have been in the field over seven years without incident except for the recent issue." Because the exploit would only work on units that had the double-up option available, IGT recommended that casinos disable that option as a work-around. (IGT declined to comment for this story). Even after the notice, Nestor and his crew were still returning to the vulnerable Draw Poker machine at the Meadows, until August 28, 2009, when an agent of the Pennsylvania Gaming Control Board observed Nestor win a $20,000 jackpot and send his associate Loushil to collect it. An investigation followed, and the Pennsylvania GCB rediscovered the double-up bug themselves.

The local district attorney prosecuted Nestor on scores of charges. But on the first day of jury selection, U.S. marshals swooped in with an

arrest warrant out of Las Vegas, where Nestor and Kane had been charged with federal wire fraud and computer hacking.

Interviewed by a local television crew on his way out of the Pennsylvania courthouse, Nestor was apoplectic.

"I'm being arrested federally for winning on a slot machine," he said. "It's just like if someone taught you how to count cards, which we all know is not illegal. You know. Someone told me that there are machines that had programming that gave a player an advantage over the house. And that's all there is to it....

"Who would not win as much money as they could on a machine that says, 'Jackpot'? That's the whole idea!"

Under the relevant section of the CFAA, Kane and Nestor aren't charged with hacking into the Game King from the outside, but rather with exceeding their otherwise legitimate access "to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

"In short, the casinos authorized defendants to play video poker," wrote Assistant U.S. Attorney Daniel Bogden. "What the casinos did not do was to authorize defendants 'to obtain or alter information' such as previously played hands of cards. To allow customers to access previously played hands of cards, at will, would remove the element of chance and obviate the whole purpose of gambling. It would certainly be contrary to the rules of poker."

The "exceeds authorized access" provision of the CFAA is controversial. "Aaron's Law" would strike that language entirely. But the bill hasn't been introduced, and instead of reform, activists had to rally to tamp down yet another broadening of the CFAA last month – a draft bill that

would have boosted sentences and made CFAA violations a RICO predicate. "In the middle of us pushing CFAA reform, this Bizarro proposal was floated by House Republicans making CFAA worse," says EFF's Trevor Timm.

The most serious rollback of the provision came, not from Congress, but from the U.S. 9th Circuit Court of Appeals in *U.S. v Nosal*, a case that stands now as Kane's and Nestor's best hope.

David Nosal was a former executive at a corporate recruiting firm who persuaded two employees to violate company policy and give him valuable information from the firm's lead database. Prosecutors charged Nosal under the "exceeds authorized access" provision of the CFAA.

In April the 9th Circuit threw out those charges, noting that the firm employees didn't hack into the database, they just violated company policy on what they're allowed to do with the information within it. If that's a crime under the CFAA, then so is violating the terms-of-service on a website, or watching sports highlights on ESPN.com on company time.

"For example, it's not widely known that, up until very recently, Google forbade minors from using its services," wrote chief judge Alex Kozinski. "Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents."

Nosal was later convicted at trial on other charges, but the appeals court ruling is a landmark, and it's binding law in nine western U.S. states, including Nevada.

Last month Judge Du asked both sides in the Vegas case to weigh in on how the ruling changes things for them. "In light of *United States v.*

Nosal ... and the considerable legislative history demonstrating that Congress intended the CFAA to punish computer hacking, rather than computer misuse, was Defendants' conduct comparable to hacking or misuse?" she asked in an April 15 order (.pdf).

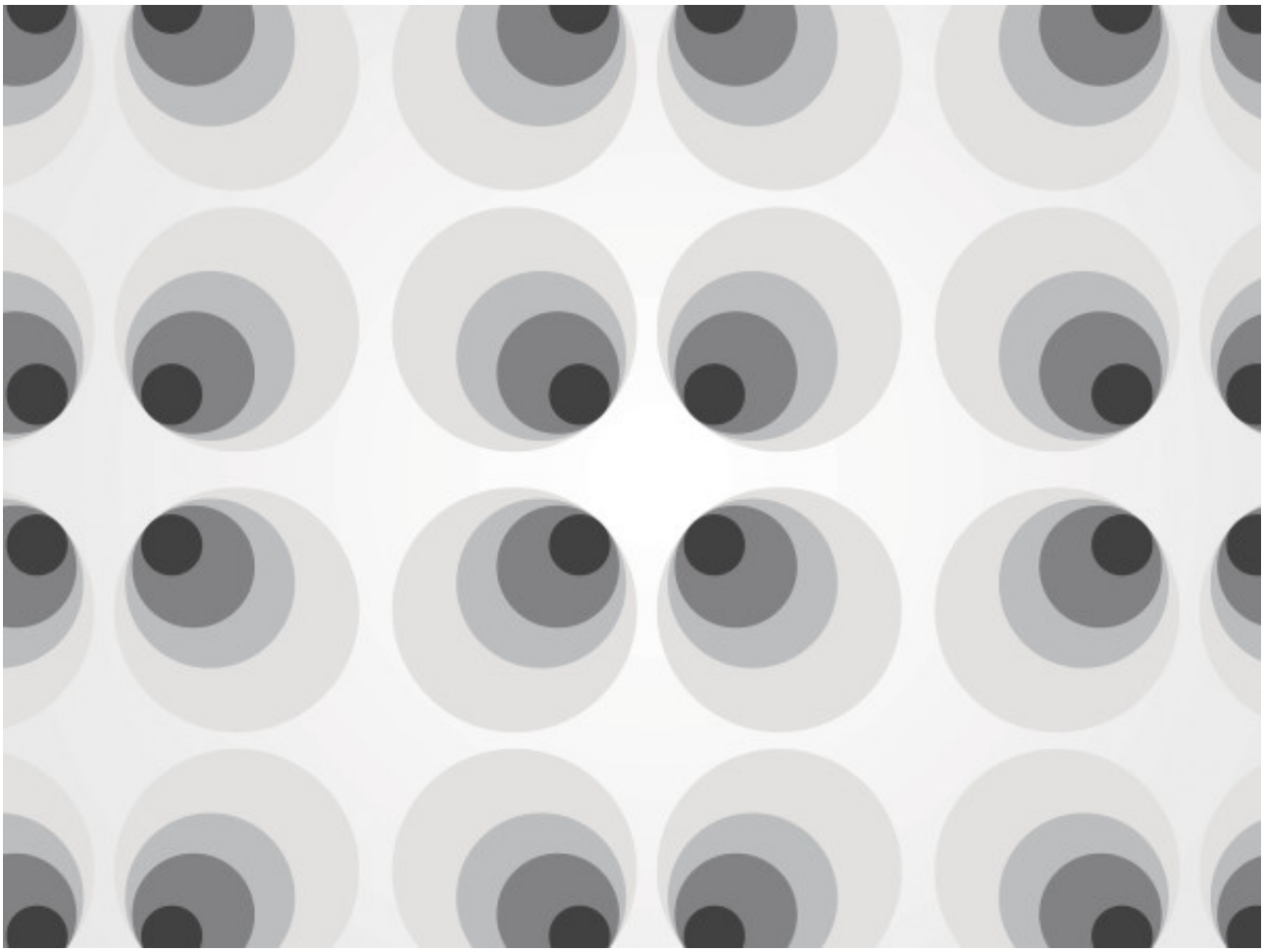
"It's a sign of progress, I think," says Orin Kerr, a law professor at the George Washington University Law School, who's representing, Andrew Auernheimer on appeal. "A few years ago, judges never questioned broad readings of the CFAA."

Written filings are due on May 8, and the trial is currently set for August 20. If the CFAA charges are thrown out, Kane and Nestor still face wire fraud charges for their lucky streak. Leavitt, who spoke with Wired prior to the April 15 order, said he likes his odds on those counts. "They're going to have real tough time with the wire fraud," he says. "I never really understood why the federal government took this case in the first place."

(Disclosure: As a hacker 20 years ago, the author pleaded guilty under an uncontroversial application of the CFAA.)

#CFAA #THE COURTS

MORE SECURITY



SECURITY

Security News This Week: Hacked Toymaker VTech Now Makes Home Monitoring Tech

2 DAYS

SPOILER ALERT

The Winner of WIRED's Third CES Smartphone Thunderdome Is

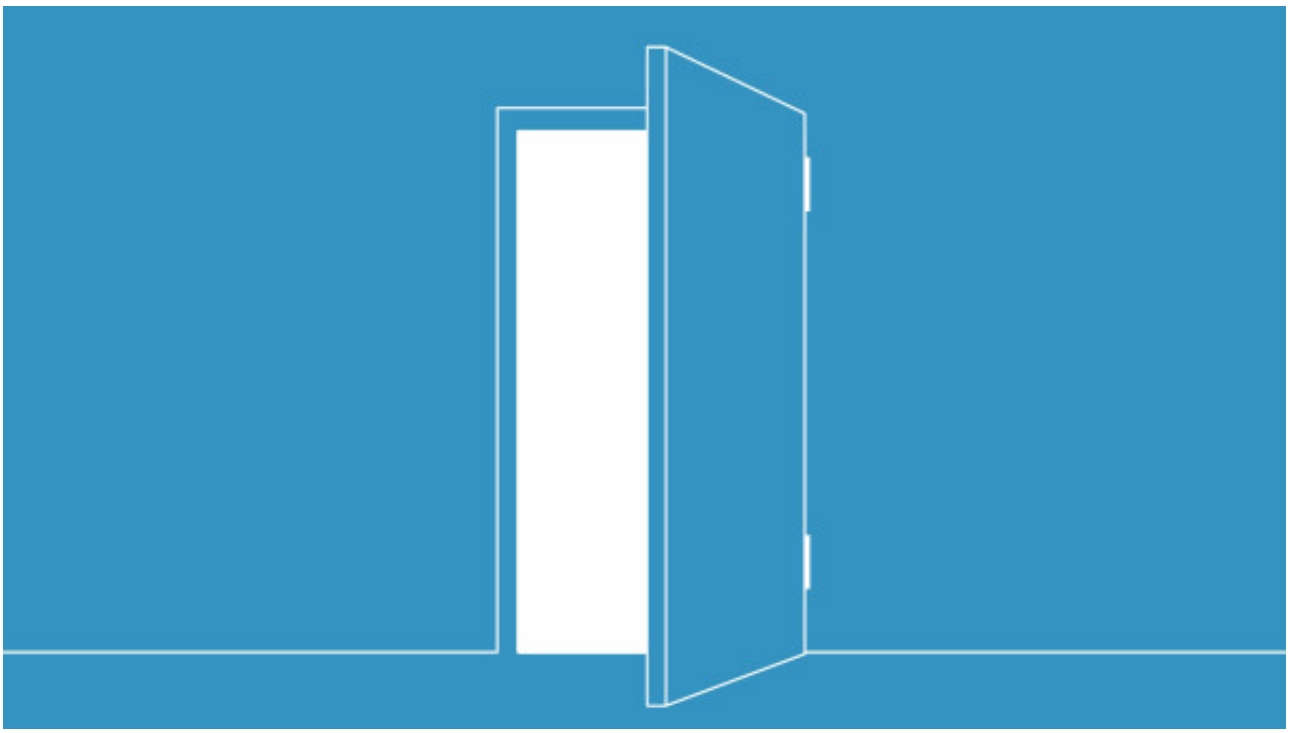
The Winner of WIRED's Third CES Smartphone Thunderdome Is...

2 DAYS

EXPLAINED

Answers to Your Burning Questions on the Ashley Madison Hack

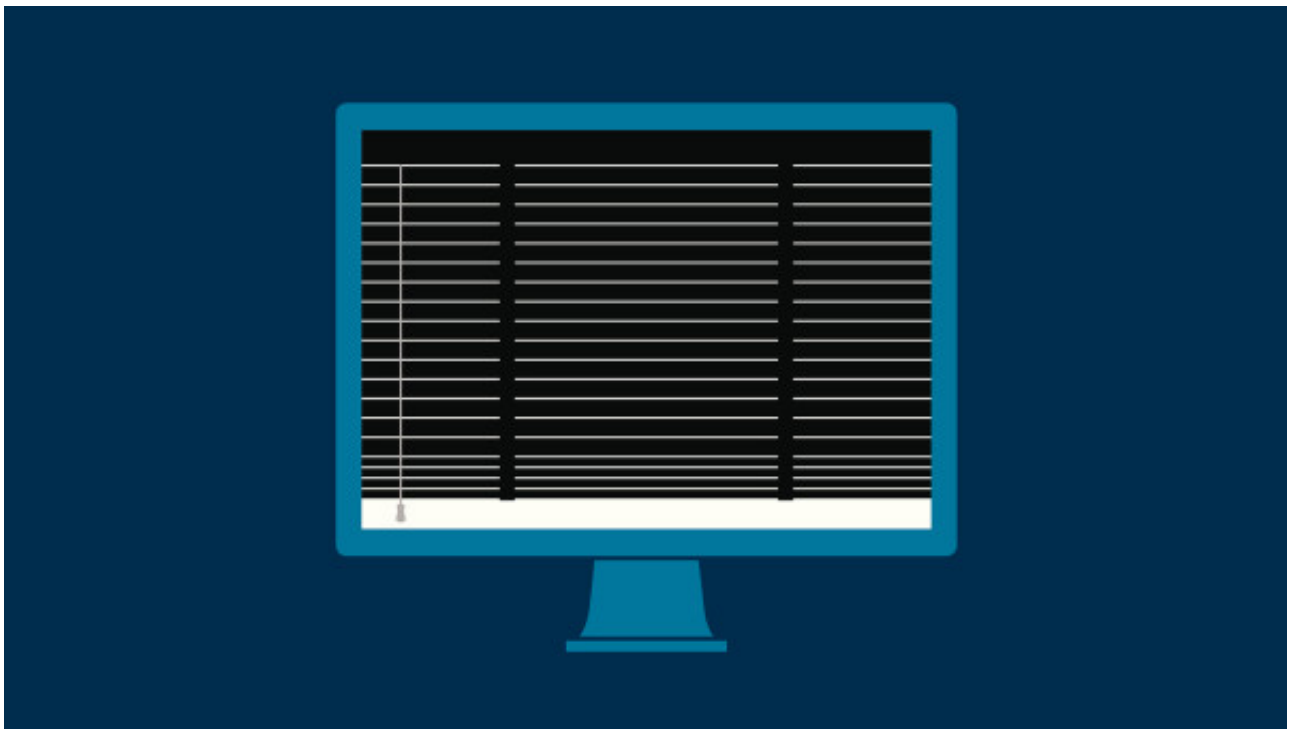
08.21.15



SECURITY

New Discovery Around Juniper Backdoor Raises More Questions About the Company

3 DAYS



PRIVACY

ProPublica Launches the Dark Web's First Major News Site

01.07.16

WE RECOMMEND

CADE METZ

The Porn Business Isn't Anything Like You Think It Is

TIM MOYNIHAN

Video: Smart Fridges Are Getting Smarter

WIRED SCIENCE

Drought, Anti-Vaxxers, and Cancer Made For a Great 2015

TIM MOYNIHAN

8K Televisions Arrive Soon. Here's What to Know

8K Televisions Arrive Soon. Here's What to Know

WUNDERBROW ON HEALTH&STYLE

Make-up artist reveals best Eyebrow product of 2015