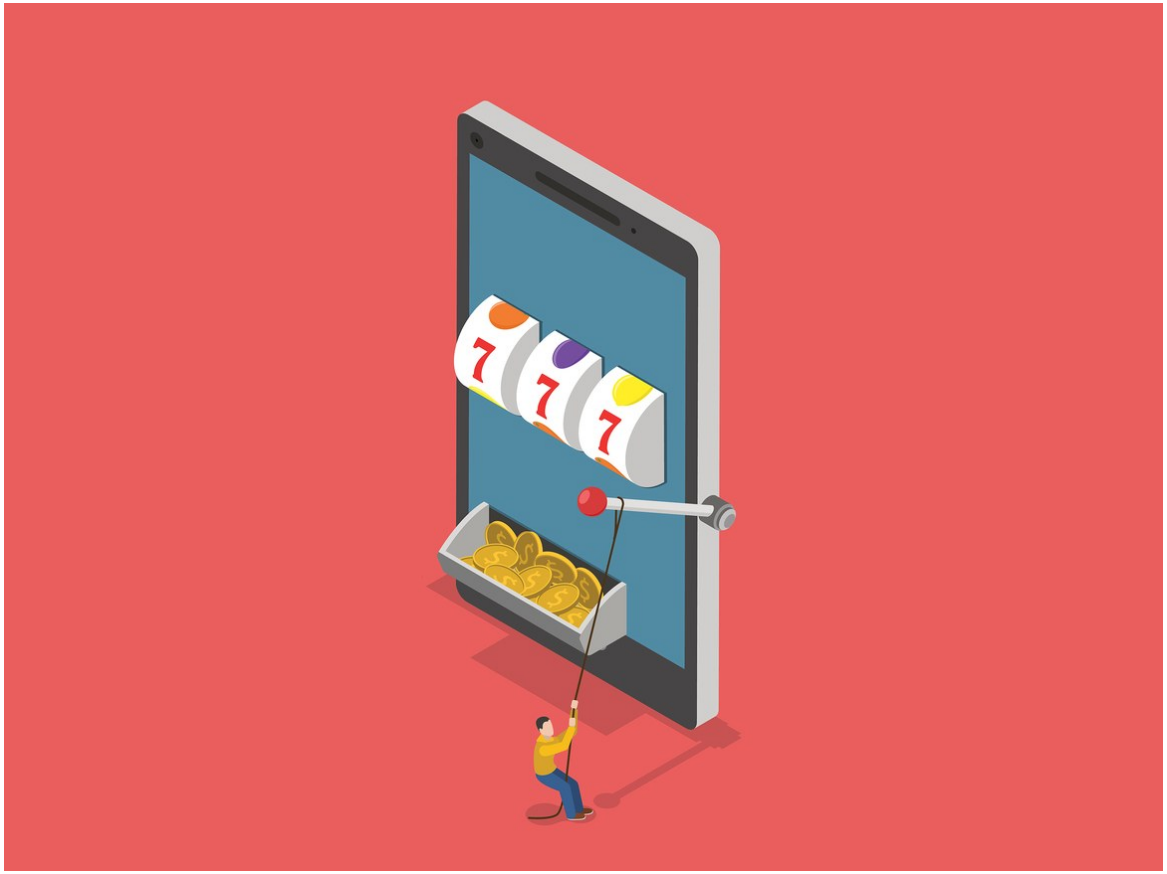
BRENDAN I. KOERNER SECURITY 02.06.17 7:00 AM

RUSSIANS ENGINEER A BRILLIANT SLOT MACHINE CHEAT—AND CASINOS HAVE NO FIX



GETTY IMAGES

IN EARLY JUNE 2014, accountants at the Lumiere Place Casino in St. Louis noticed that several of their slot machines had—just for a couple of days—gone haywire. The government-approved software that powers such machines gives the house a fixed mathematical edge, so that casinos can be certain of how much they'll earn over the long haul—say, 7.129 cents for every dollar played. But on June 2 and 3, a number of

Lumiere's machines had spit out far more money than they'd consumed, despite not awarding any major jackpots, an aberration known in industry parlance as a negative hold. Since code isn't prone to sudden fits of madness, the only plausible explanation was that someone was cheating.

Casino security pulled up the surveillance tapes and eventually spotted the culprit, a black-haired man in his thirties who wore a Polo zip-up and carried a square brown purse. Unlike most slots cheats, he didn't appear to tinker with any of the machines he targeted, all of which were older models manufactured by Aristocrat Leisure of Australia. Instead he'd simply play, pushing the buttons on a game like Star Drifter or Pelican Pete while furtively holding his iPhone close to the screen.

He'd walk away after a few minutes, then return a bit later to give the game a second chance. That's when he'd get lucky. The man would parlay a $20 to $60 investment into as much as $1,300 before cashing out and moving on to another machine, where he'd start the cycle anew. Over the course of two days, his winnings tallied just over $21,000. The only odd thing about his behavior during his streaks was the way he'd hover his finger above the Spin button for long stretches before finally jabbing it in haste; typical slots players don't pause between spins like that.

On June 9, Lumiere Place shared its findings with the Missouri Gaming Commission, which in turn issued a statewide alert. Several casinos soon discovered that they had been cheated the same way, though often by different men than the one who'd bilked Lumiere Place. In each instance, the perpetrator held a cell phone close to an Aristocrat Mark VI model slot machine shortly before a run of good fortune.

By examining rental-car records, Missouri authorities identified the Lumiere Place scammer as Murat Bliev, a 37-year-old Russian national. Bliev had flown back to Moscow on June 6, but the St. Petersburg–based organization he worked for, which employs dozens of operatives to manipulate slot machines around the world, quickly sent him back to the United States to join another cheating crew. The decision to redeploy Bliev to the US would prove to be a rare misstep for a venture that's quietly making millions by cracking some of the gaming industry's most treasured algorithms.

From Russia With Cheats

Russia has been a hotbed of slots-related malfeasance since 2009, when the country outlawed virtually all gambling. (Vladimir Putin, who was prime minister at the time, reportedly believed the move would reduce the power of Georgian organized crime.) The ban forced thousands of casinos to sell their slot machines at steep discounts to whatever customers they could find. Some of those cut-rate slots wound up in the hands of counterfeiters eager to learn how to load new games onto old circuit boards. Others apparently went to Murat Bliev's bosses in St. Petersburg, who were keen to probe the machines' source code for vulnerabilities.

By early 2011, casinos throughout central and eastern Europe were logging incidents in which slots made by the Austrian company Novomatic paid out improbably large sums. Novomatic's engineers could find no evidence that the machines in question had been tampered with, leading them to theorize that the cheaters had figured out how to predict the slots' behavior. "Through targeted and prolonged observation of the individual game sequences as well as possibly recording individual games, it might be possible to allegedly identify a kind of 'pattern' in the game results," the company admitted in a February 2011 notice to its customers.

Recognizing those patterns would require remarkable effort. Slot machine outcomes are controlled by programs called pseudorandom number generators that produce baffling results by design. Government regulators, such as the Missouri Gaming Commission, vet the integrity of each algorithm before casinos can deploy it.

But as the "pseudo" in the name suggests, the numbers aren't truly random. Because human beings create them using coded instructions, PRNGs can't help but be a bit deterministic. (A true random number generator must be rooted in a phenomenon that is not manmade, such as radioactive decay.) PRNGs take an initial number, known as a seed, and then mash it together with various hidden and shifting inputs—the time from a machine's internal clock, for example—in order to produce a result that appears impossible to forecast. But if hackers can identify the various ingredients in that mathematical stew, they can

potentially predict a PRNG's output. That process of reverse engineering becomes much easier, of course, when a hacker has physical access to a slot machine's innards.

Knowing the secret arithmetic that a slot machine uses to create pseudorandom results isn't enough to help hackers, though. That's because the inputs for a PRNG vary depending on the temporal state of each machine. The seeds are different at different times, for example, as is the data culled from the internal clocks. So even if they understand how a machine's PRNG functions, hackers would also have to analyze the machine's gameplay to discern its pattern. That requires both time and substantial computing power, and pounding away on one's laptop in front of a Pelican Pete is a good way to attract the attention of casino security.

The Lumiere Place scam showed how Murat Bliev and his cohorts got around that challenge. After hearing what had happened in Missouri, a casino security expert named Darrin Hoke, who was then director of surveillance at L'Auberge du Lac Casino Resort in Lake Charles, Louisiana, took it upon himself to investigate the scope of the hacking operation. By interviewing colleagues who had reported suspicious slot machine activity and by examining their surveillance photos, he was able to identify 25 alleged operatives who'd worked in casinos from California to Romania to Macau. Hoke also used hotel registration records to discover that two of Bliev's accomplices from St. Louis had remained in the US and traveled west to the Pechanga Resort & Casino in Temecula, California. On July 14, 2014, agents from the California Department of Justice detained one of those operatives at Pechanga and confiscated four of his cell phones, as well as $6,000. (The man, a Russian national, was not indicted; his current whereabouts are unknown.)

The cell phones from Pechanga, combined with intelligence from investigations in Missouri and Europe, revealed key details. According to Willy Allison, a Las Vegas–based casino security consultant who has been tracking the Russian scam for years, the operatives use their phones to record about two dozen spins on a game they aim to cheat. They upload that footage to a technical staff in St. Petersburg, who analyze the video and calculate the machine's pattern based on what they know about the model's pseudorandom number generator. Finally, the St. Petersburg team transmits a list of timing markers to a custom app on

the operative's phone; those markers cause the handset to vibrate roughly 0.25 seconds before the operative should press the spin button.

"The normal reaction time for a human is about a quarter of a second, which is why they do that," says Allison, who is also the founder of the annual World Game Protection Conference. The timed spins are not always successful, but they result in far more payouts than a machine normally awards: Individual scammers typically win more than $10,000 per day. (Allison notes that those operatives try to keep their winnings on each machine to less than $1,000, to avoid arousing suspicion.) A four-person team working multiple casinos can earn upwards of $250,000 in a single week.

Repeat Business

Since there are no slot machines to swindle in his native country, Murat Bliev didn't linger long in Russia after his return from St. Louis. He made two more trips to the US in 2014, the second of which began on December 3. He went straight from Chicago O'Hare Airport to St. Charles, Missouri, where he met up with three other men who'd been trained to scam Aristocrat's Mark VI model slot machines: Ivan Gudalov, Igor Larenov, and Yevgeniy Nazarov. The quartet planned to spend the next several days hitting various casinos in Missouri and western Illinois.

Bliev should never have come back. On December 10, not long after security personnel spotted Bliev inside the Hollywood Casino in St. Louis, the four scammers were arrested. Because Bliev and his cohorts had pulled their scam across state lines, federal authorities charged them with conspiracy to commit fraud. The indictments represented the first significant setbacks for the St. Petersburg organization; never before had any of its operatives faced prosecution.

Bliev, Gudalov, and Larenov, all of whom are Russian citizens, eventually accepted plea bargains and were each sentenced to two years in federal prison, to be followed by deportation. Nazarov, a Kazakh who was granted religious asylum in the US in 2013 and is a Florida resident, still awaits sentencing, which indicates that he is cooperating with the authorities: In a statement to WIRED, Aristocrat representatives

noted that one of the four defendants has yet to be sentenced because he "continues to assist the FBI with their investigations."

Whatever information Nazarov provides may be too outdated to be of much value. In the two years since the Missouri arrests, the St. Petersburg organization's field operatives have become much cagier. Some of their new tricks were revealed last year, when Singaporean authorities caught and prosecuted a crew: One member, a Czech named Radoslav Skubnik, spilled details about the organization's financial structure (90 percent of all revenue goes back to St. Petersburg) as well as operational tactics. "What they'll do now is they'll put the cell phone in their shirt's chest pocket, behind a little piece of mesh," says Allison. "So they don't have to hold it in their hand while they record." And Darrin Hoke, the security expert, says he has received reports that scammers may be streaming video back to Russia via Skype, so they no longer need to step away from a slot machine to upload their footage.

The Missouri and Singapore cases appear to be the only instances in which scammers have been prosecuted, though a few have also been caught and banned by individual casinos. At the same time, the St. Petersburg organization has sent its operatives farther and farther afield. In recent months, for example, at least three casinos in Peru have reported being cheated by Russian gamblers who played aging Novomatic Coolfire slot machines.

The economic realities of the gaming industry seem to guarantee that the St. Petersburg organization will continue to flourish. The machines have no easy technical fix. As Hoke notes, Aristocrat, Novomatic, and any other manufacturers whose PRNGs have been cracked "would have to pull all the machines out of service and put something else in, and they're not going to do that." (In Aristocrat's statement to WIRED, the company stressed that it has been unable "to identify defects in the targeted games" and that its machines "are built to and approved against rigid regulatory technical standards.") At the same time, most casinos can't afford to invest in the newest slot machines, whose PRNGs use encryption to protect mathematical secrets; as long as older, compromised machines are still popular with customers, the smart financial move for casinos is to keep using them and accept the occasional loss to scammers.

So the onus will be on casino security personnel to keep an eye peeled for the scam's small tells. A finger that lingers too long above a spin button may be a guard's only clue that hackers in St. Petersburg are about to make another score.