MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

BACKDOORING THE LOTTERY AND OTHER TALES IN GAMING

Gus Fritschie

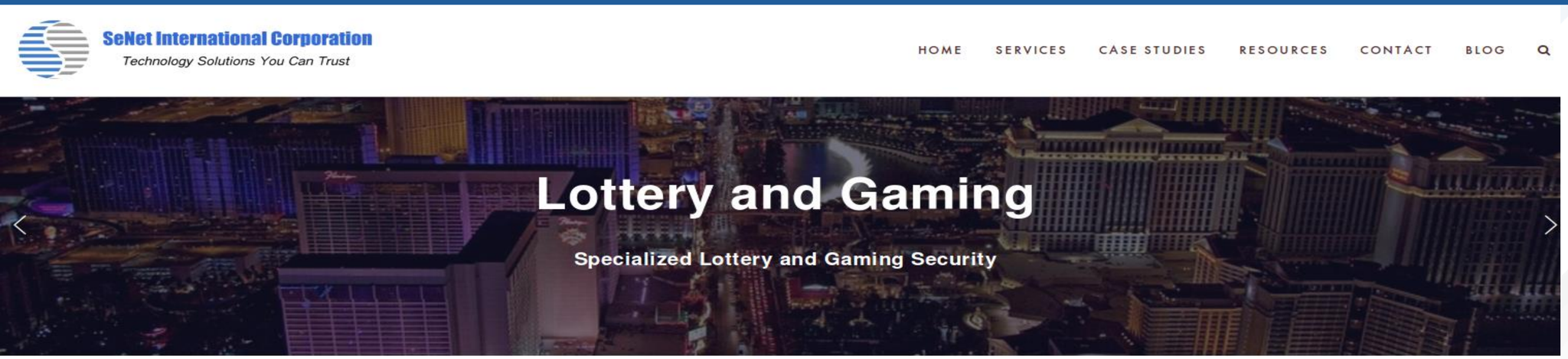
CTO

@gfritschie

PRESENTATION OVERVIEW

1. Introductions
2. What has happened since 2011
3. Historical overview of security incidents in gaming
4. Eddie Tipton and the lottery
5. Russian slot attacks
6. Conclusion

WHO WE ARE – SENET INTERNATIONAL



WHO WE ARE – GUS FRITSCHIE

Gus Fritschie has been involved in information security since 2000. About 6 years ago he transitioned a significant portion of his practice into the gaming sector.

Since then he has established himself and SeNet as the IT security leader in gaming. He has supported a number of clients across the gaming spectrum from iGaming operators, land-based casinos, gaming manufacturer, lotteries, tribal gaming, and daily fantasy sports.

WHO WE ARE – EVAN TEITELMAN

Evan used to work and live in the Washington DC area. He is the founder of BlackArch Linux and specializes in reverse engineering and secure application development.

In his free time he enjoys hiking, climbing, and working on his van.

WHAT HAS HAPPENED SINCE 2011

Getting F***** on the River

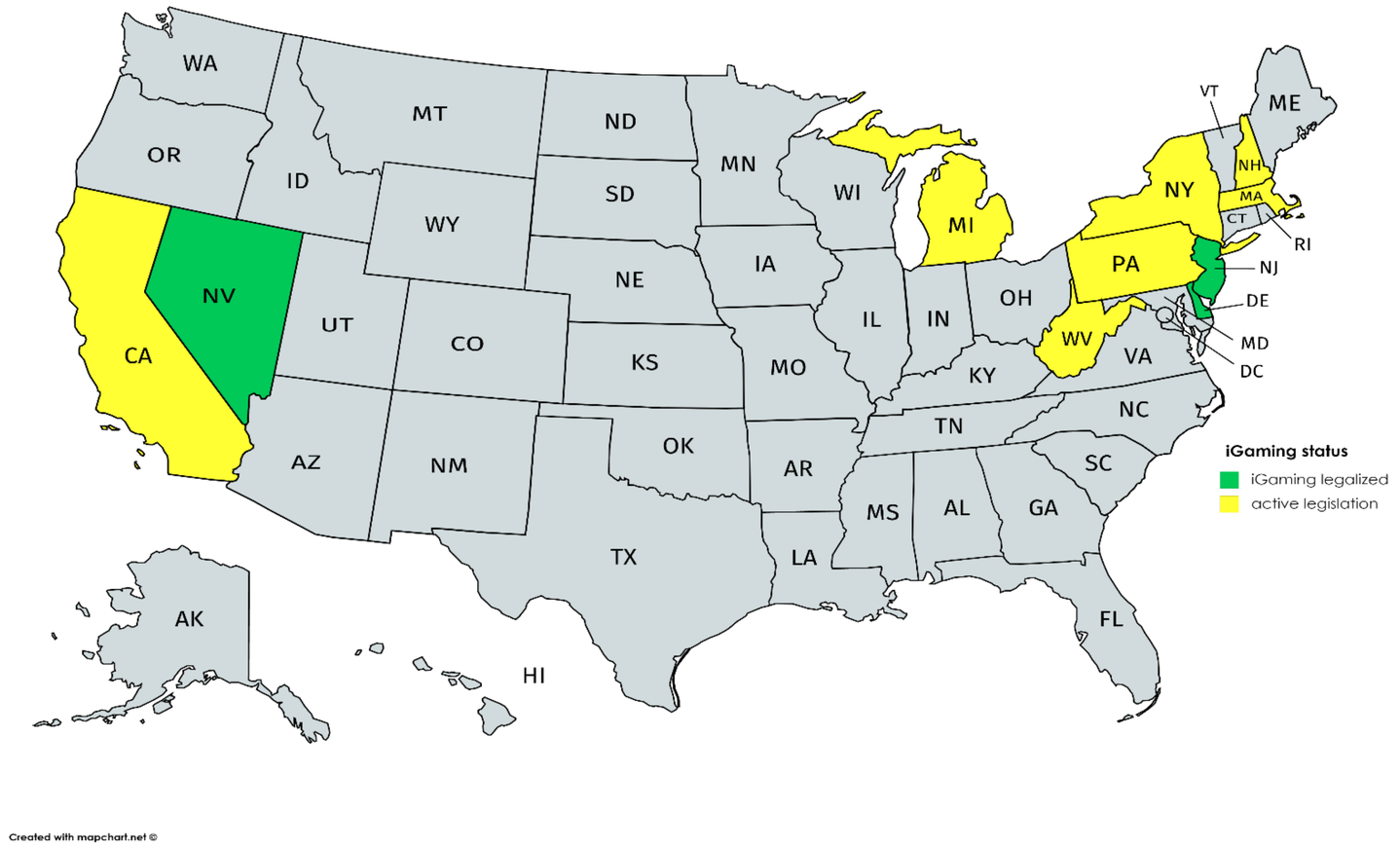
Gus Fritschie and Steve Witmer
with help from

Mike Wright, and JD Durick

August 6, 2011

SeNet International Corporation
e-Security – We Make It Practical

iGAMING LEGISLATION



HIGHLIGHTED SECURITY INCIDENTS IN GAMING SINCE 2011

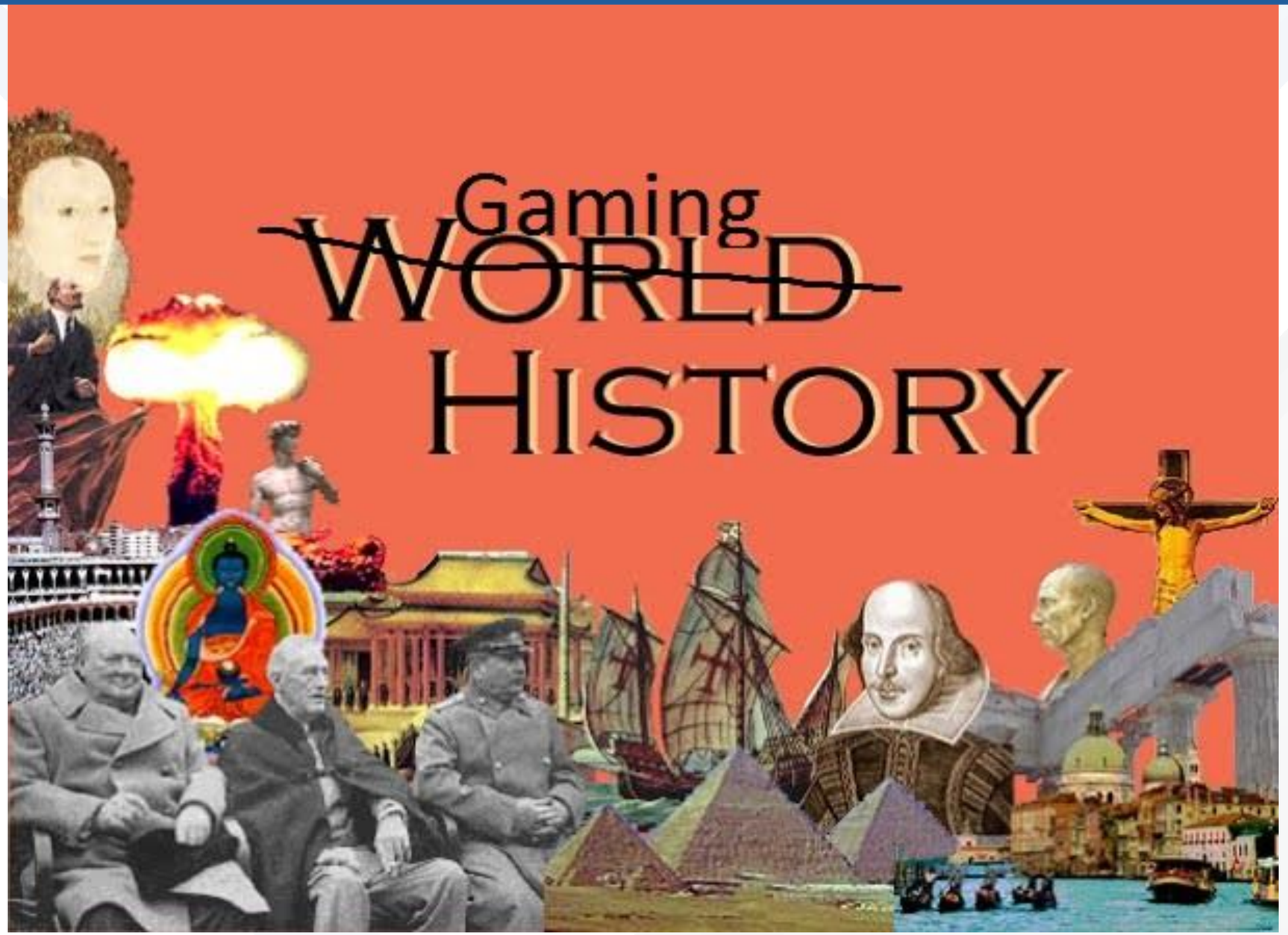
None of these will be discussed in detail but are listed to illustrate that this sector is not immune to these threats. Only a small sampling.

- Las Vegas Sands hack
- NJ iGaming DDOS attacks
- Affinity Gaming breach
- Hard Rock Hotel & Casino data breach
- Casino Rama Resort in Ontario
- Peppermill Resort Spa Casino in Reno credit card breach
- Weaknesses in Daily Fantasy Sports (DFS) protections

LAS VEGAS SANDS

Sands website hacked

HISTORY CLASS



EARLY ATTACKS AGAINST SLOT MACHINES

EARLY ATTACKS AGAINST SLOT MACHINES (CONT.)

Shaved, fake coins and yo-yoing

Banknote validators

EARLY ATTACKS AGAINST SLOT MACHINES (CONT.)

Tommy Carmichael

Monkey Paw, a taut string attached to a bent metal rod.

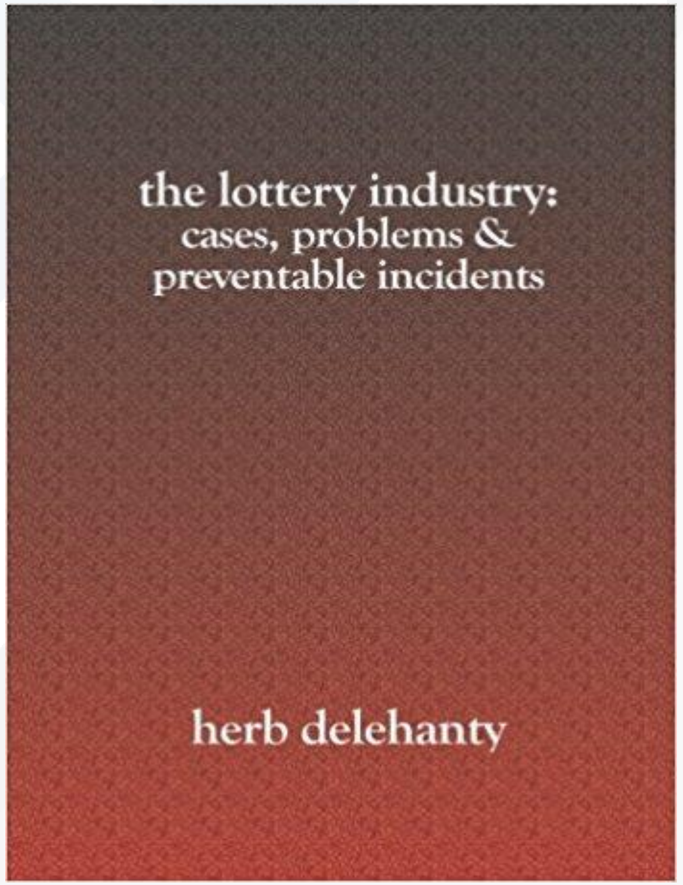
By blinding the optical sensor, the Light Wand made it impossible for the machine to know how much money it was releasing.

1980 PENNSYLVANIA LOTTERY SCANDAL

April 24th 1980 the lottery reaches its liability limits on the Daily Number (3-digit game) on 8 of the possible combinations of 6s and 4s (444, 446, 464, 644, 646, 664, 666)

Winning number was 666.

Later in the evening rumors surfacing that illegal bookmakers were not paying.



RON HARRIS ATTACKS AGAINST SLOTS AND KENO

Ronald Dale Harris is a computer programmer who worked for the Nevada Gaming Control Board in the early 1990s and was responsible for finding flaws and gaffes in software that runs computerized casino games.

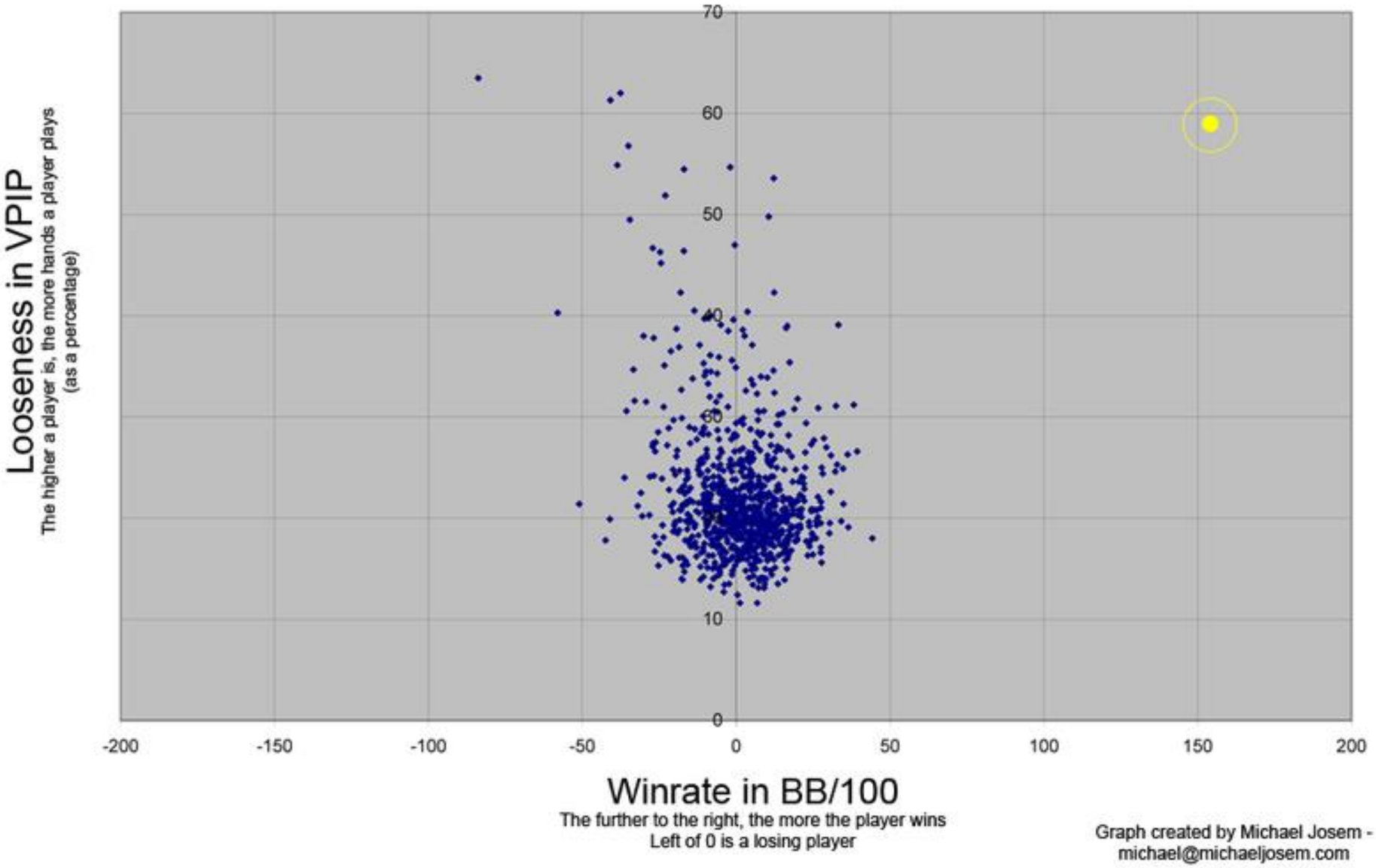
RON HARRIS ATTACKS AGAINST SLOTS AND KENO (CONT.)

Harris surreptitiously coded a hidden software switch -- tripped by inserting coins in a predetermined sequence -- that would trigger cash jackpots.

RON HARRIS ATTACKS AGAINST SLOTS AND KENO (CONT.)

Harris shifted his focus to the probability game Keno, for which he developed a program that would determine which numbers the game's pseudorandom number generator would select beforehand.

PREVIOUS iGAMING HACKS/SCANDALS (UB/AP)



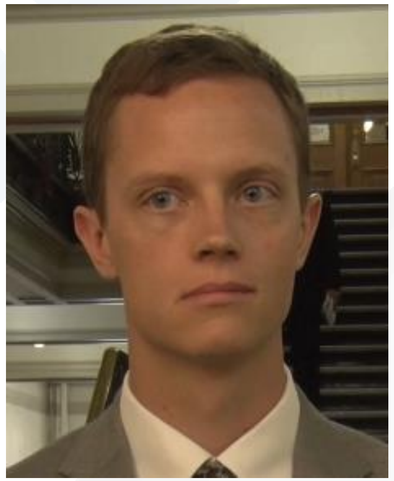
CURRENT EVENTS

EDDIE TIPTON HOT LOTTO RNG RIGGING

Eddie Tipton

Tommy Tipton

Robert Rhodes

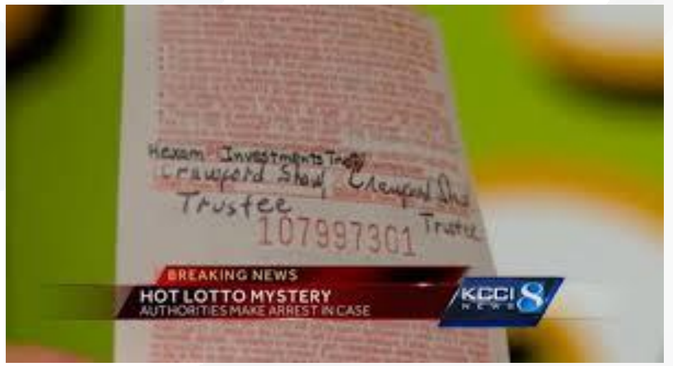


Rob Sand – Iowa Assistant Attorney General (lead prosecutor)

TIPTON OVERVIEW

Lottery Fraud Case
Involving a $14.3 million
prize!

Lottery ticket purchased at a QuikTrip near Interstate Highway 80 on Dec. 23, 2010.



Prize went unclaimed for almost a year.

TIPTON OVERVIEW (CONT.)

Lottery officials refused to release the prize.

Claim to prize was withdrawn in January 2012.

- Iowa Lottery officials asked the Iowa Attorney General's Office and Iowa DCI to investigate.

On Oct. 13, authorities received a tip from an out-of-state employee of the Multi-State Lottery Association that Tipton was the man in the video.

Investigators analyzed Tipton's cellphone records.

TIPTON OVERVIEW (CONT.)

Eddie was convicted in 2015 of two counts of fraud following a weeklong trial.

He was sentenced to 10 years in prison, but is out on bond pending appeal.

June 29, 2017 Tipton pleaded guilty to three felony charges in Iowa and Wisconsin. The other states where fraud occurred have agreed not to prosecute.

TIPTON TIMELINE

March 2003 – Eddie Tipton is hired at MUSL
November 23, 2005 – Colorado Lottery fraud
December 29, 2007 – Wisconsin Lottery fraud
December 29, 2010 – Kansas Lottery fraud
December 29, 2010 – Iowa Hot Lotto fraud
November 23, 2011 – Oklahoma Lottery fraud
January 15, 2015 – Eddie Tipton arrested
March 2015 – Rhodes was arrested on 2 counts of fraud
July 20, 2015 – Eddie Tipton Convicted
September 9, 2015 – Sentenced to 10 years, but free on bond pending appeal
October 2015 – New criminal charges filed related to 2005 and 2007 fraud
March 30, 2016 – Tommy Tipton charged
June 29th, 2017 – Eddie pleads guilty in Iowa

HOW TO RIG THE LOTTERY

Steps to rig the lottery:

1. Become a lottery RNG developer
2. Write code to make the numbers predictable
3. Have your friends buy tickets with the winning numbers

HOW HE RIGGED THE LOTTERY

HOW HE RIGGED THE LOTTERY (REALLY)

- In 2003 Eddie got a job as an RNG developer at MUSL
  - Wrote code which made the numbers predictable on three dates
- The source code and RNG binaries were certified by one of the major testing labs

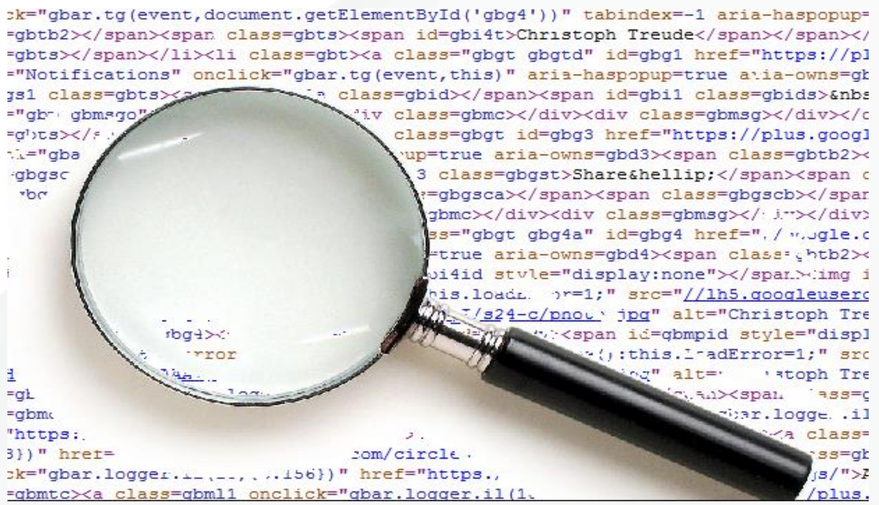
HOW HE RIGGED THE LOTTERY (CONT.)

- In 2016 SeNet was contracted to perform imaging of one of the rigged lottery RNGs
- In 2016 after Eddie was convicted SeNet was given permission to review the RNG images
- Eddie didn’t seem smart enough to write a rootkit which could change lottery numbers in memory
- Despite the official explanation (from which he was convicted) for how he rigged the lottery, I assumed he simply slipped some code into the RNG which rigged it…
- At this point we only had the binaries (no source code)

REVERSE ENGINEERING

- The RNG consisted of an executable (QV.EXE) which contained the front-end material
- A DLL (QVRNG.DLL) which contained the PRNG
- And a DLL (AWRAND.DLL) which interfaced with the hardware RNG
- QVRNG.DLL was an obvious first choice for an RNG rigger

- So I looked at QVRNG.DLL first
- I briefly skimmed through all of the functions. One of them caught my eye…



LOGIC BOMB

- At this point we also knew that all of the alleged illicit lottery wins related to the case were on two different days: November 23rd and December 29th (November 22nd and December 28th on leap years)
- This function full of references to date checks and the PRNG internals was pretty suspicious
- Also the function was at the end of the binary (as if it had been tacked on to the end of a source file) which was suspicious
- At this point we were able to obtain the source code for the RNG
- Sure enough there were 25 functions in the source code and 26 functions in the binary

LOGIC BOMB (CONT.)

- The date calls corresponded to the two known dates of lottery rigging
- Plus one additional date: May 27th (May 26th on leap years)
- Additional conditions for the RNG rigging were identified and correlated with known illicit winnings
- For example, the RNG was only rigged on Wednesdays and Saturdays

LOGIC BOMB (CONT.)

- The method by which the function reseeded the RNG with predictable numbers was identified

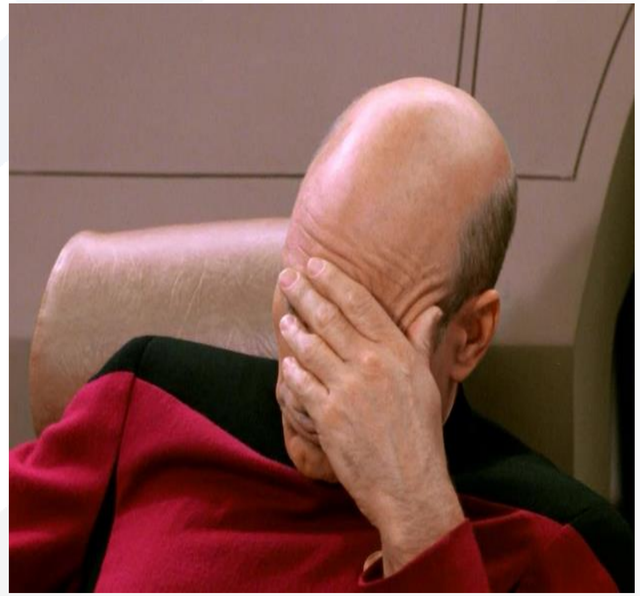
- Took various game parameters:
  - number of numbers per draw
  - maximum and minimum numbers in the game
- Summed ASCII values of the letters in the computer name
- Then took that and added it to the day of the year and added in the product of the number of times the RNG had run since last reboot

- This number then used to seed the PRNG.

- He drew a quantity of numbers from the RNG corresponding the quantity of numbers which had been drawn since the RNG last restarted. The last number drawn was then used to seed the PRNG a second time.

WHY DIDN'T CERTIFICATION WORK?

- The RNG was certified by one of the major testing labs
- The certification ran the output of the RNG through statistical tests to ensure unbiased results…
- But the output of the rigged RNG was statistically unbiased
- The lab performed an audit of the source code…



HOW HE COULD HAVE DONE IT BETTER

- Rigging the lottery on only three dates made it easier to identify illegal winnings
- Making numbers dependent on variables like the computer name and time of day meant he had to buy multiple tickets for each drawing
- The method of rigging the RNG could have been more discreet

HOW CAN THIS BE PREVENTED IN THE FUTURE?

- RNG source code should undergo in-depth third-party reviews
- The binaries (including updates) should be compiled and checked (e.g. via Bindiff) against the binaries provided by the RNG vendor
- The machine itself should be imaged and configured either by a third party or in a supervised manner

RUSSIAN SLOT MACHINE HACKING

https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/

https://www.wired.com/story/meet-alex-the-russian-casino-hacker-who-makes-millions-targeting-slot-machines/

https://www.youtube.com/watch?v=W_vdoaKsP5Y (*Willy Allison World Game Protection Conference*)

RUSSIAN SLOT MACHINE HACKING (CONT.)

- In 2009 Russia made majority of gambling illegal, this led to a number of slot machines being sold to whomever they could find
- By 2011 casinos in Europe were noticing suspicious payouts
- In June of 2014 in a casino in Missouri noticed unusual activity with some slot payouts, Missouri Gaming Commission was notified
- December of 2014 the same individuals were arrested back in Missouri
- 2016 some more were arrested and prosecuted in Singapore

RUSSIAN SLOT MACHINE HACKING (CONT.)

- Slot machine software was reversed engineered and a weakness discovered in the PRNG
- Phones were used to record about 24 spins
- Data uploaded and using video footage they were able calculate the pattern based on the slots PRNG
- Information is transmitted to a custom app with a listing of timing marks that cause the mobile to vibrate 0.25 seconds before the spin button should be pressed
- Not always successful, but the result is higher payout than expected

WHAT CASINOS AND OPERATORS CAN DO TO PROTECT THEMSELVES

- Understand that compliance != security
- Similar to other verticals more budget needs to be spent on information security
- Operators need to question game manufacturers on their security controls

CURRENT GAMING REGULATIONS WITH SECURITY COMPONENTS

- Maryland Gaming Commission requires an annual IT Security Assessment be performed by an independent and approved 3rd party on an annual basis.
- New Jersey Division of Gaming Enforcement has written in their iGaming standard that a security assessment be performed once a year on the iGaming platforms. Also includes other requirements such as auditing, password complexity, etc…
- Various tribal Minimum Internal Controls (MICs), however, these are typically very high-level.
- Also your typical regulatory compliance standards (i.e. PCI)
- Often left up to the operator to determine what level of security is implemented.

CONCLUSION

While regulated gaming has added additional controls there is still room for improvement (both from operators and regulators).

In our opinion, a major risk exists in the code and SDLC process (this is an area that is not really examined by regulators).

With gaming (all formats) becoming more widely accepted across the United States, it is important that the operators and regulators work together to protect the integrity of the games.

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Gus Fritschie

CTO

@gfritschie