Getting F***** on the River

Gus Fritschie and Steve Witmer
with help from

Mike Wright, and JD Durick
August 6, 2011
Presentation Overview

Preflop
Who We Are
What is Online Poker
Online Poker History
Current Events

Flop
Past Vulnerabilities
RNG
SuperUser
SSL
Account Compromise
Poker Bots

Turn
Online Poker Architecture
Poker Client=Rootkit
Web Application Vulnerabilities
Authentication Vulnerabilities
Attacking Supporting Infrastructure

River
Defenses – Application
Defenses – User
Next Steps in Research
Conclusion
Questions
Who We Are – SeNet International

**SeNet International is a Small Business Founded in 1998 to Deliver Network and Information Security Consulting Services to Government and Commercial Clients**

- **High-End Consulting Services Focus:**
  - Government Certification and Accreditation Support
  - Network Integration
  - Security Compliance Verification and Validation
  - Security Program Development with Business Case Justifications
  - Complex Security Designs and Optimized Deployments

- **Proven Solution Delivery Methodology:**
  - Contract Execution Framework for Consistency and Quality
  - Technical, Management, and Quality Assurance Components

- **Exceptional Qualifications:**
  - Executive Team—Security Industry Reputation and Active Project Leadership
  - Expertise with Leading Security Product Vendors, Technologies, and Best Practices
  - Advanced Degrees, Proper Clearances, Standards Organization Memberships, and IT Certifications

- **Corporate Resources:**
  - Located in Fairfax, Virginia
  - Fully Equipped Security Lab
  - Over 40 full time security professionals
Who We Are – Gus Fritschie

CTO of a security consulting firm based in the DC metro area. Enjoys penetrating government networks (with their permission), playing golf (business development) and teaching my daughter to gamble.
Sr. Security Analyst in the Northern Virginia area working for a small company supporting government contracts. Responsible for conducting application assessments, penetration testing, secure configuration reviews, NIST C&A/ST&E and other security mumbo-jumbo. He enjoys scuba diving and big speakers.

Prior to his current job, Steve spent 5 years as a road warrior working for clients all over the world ranging from Fortune 500 to churches and delivering any kind of engagement a client would pay for: aka, a security whore.
Who We Are – Mike Wright

Contractor for the United States Coast Guard (blame them for not seeing my pretty face tonight) and security consultant.

Hobbies include the broad spectrum of Information Technology, but more geared towards security and hacking around.

Currently trying to bleach my hat white but still seeing shades of gray…
Digital forensics examiner in the northern Virginia area working for a large defense contractor. Responsible for conducting network forensics as well as hard drive and malware analysis on network-based intrusions involving commercial and government computer systems.

Experience as a software engineer, network security consultant, INFOSEC engineer, and digital forensic examiner for the past 15 years.
What is Online Poker
Online Poker Timeline

• Early 90’s – IRC Poker is the 1st Virtual Poker
• 1998 – Planet Poker Launched, 1st Real Money Site
• 1999 – Kahnawake Gaming Commission Regulations
• 2000 – UB Launches
• 2001 – Party Poker and Poker Stars
• 2003 – Moneymaker and Poker Boom
• 2004 – Full Tilt Poker
• 2005 – Online Poker Becomes $2 Billion Industry
• 2006 – UIGEA
• 2007 – UB/AP Cheating Scandal
• 2010 – Online Poker Industry Reaches $6 Billion
• 2011 – 4/15 Black Friday
• DOJ has seized the following poker sites on charges of illegal gambling and money laundering: Poker Stars, Full Tilt, UB/Absolute, and Doyles Room

• Poker Stars has paid players, not other site has.

• Development of new features and functionality seems to be in a holding pattern.
Online Poker Revenue

(Billions $)

2004 2005 2008 2010

Online Poker Revenue

Online Gambling Revenue

(Billions $)

2001 2002 2003 2004 2005 2006 2007 2008 2009 2010

Online Gambling Revenue

Source: Christiansen Capital Advisors
In other words there is a lot of money in online poker
Regulation\Compliance

• For an industry that makes a decent amount of revenue there is little to no regulation\compliance
• Isle of Man Gambling Supervision Commission and Kahnawake Gaming Commission
• Party Poker and other sites do not allow players from the USA and in certain countries (i.e. UK) it is regulated and taxed.

“Licensed and regulated by the Government of Gibraltar, our games are powered by the bwin.party systems which are independently tested to ensure that our games operate correctly, are fair, their outcomes are not predictable and that the system is reliable, resilient and otherwise up to the highest standards of software integrity, including access control, change control recording, fingerprinting of the executables and regular monitoring of all critical components of our systems.”
There is a need for compliance related activities if online poker is to become regulated and safe to play in the USA.

A standard needs to be developed and companies that provide these services need to be audited. Not just from the financial perspective, but the technical perspective.

Why will this happen?
Because there is a lot of money in online poker
Past Vulnerabilities

- Random Number Generator Vulnerability
- UB/Absolute Super User Issue
- SSL Exploit
- Misc. Account Compromise
- Poker Bots
• Documented in 1999 and originally published in Developer.com

• PlanetPoker had published their shuffling algorithm to demonstrate the game’s integrity

• ASF Software developed the shuffling algorithm
• In a real deck of cards, there are 52! (approximately $2^{226}$) possible unique shuffles.
• In their algorithm only 4 billion possible shuffles can result from this algorithm.
• Seed for the random number generator using the Pascal function Randomize()
• Number reduces to 86,400,000
• They were able to reduce the number of possible combinations down to a number on the order of 200,000 possibilities.
• Based on the five known cards their program searched through the few hundred thousand possible shuffles to determine the correct one.
• These days companies have their RNG audited by reputable 3rd parties
• From Poker Stars site: “Cigital, the largest consulting firm specializing in software security and quality, has confirmed the reliability and security of the random number generator (RNG) that PokerStars uses to shuffle cards on its online poker site, showing the solution meets or exceeds best practices in generating unpredictable and statistically random values for dealing cards.”
• Do you believe this?
• Full story is almost like a soap opera.

• Cheating is thought to have occurred between 2004-2008 when members of online poker forum began investigating.

• Still actively being investigated by people such as Haley (http://haleyspokerblog.blogspot.com/).
• Story is owner suspected cheating and asked software developer to put in a tool to “help catch the cheaters”

• Hired an independent contractor to put in a tool which became known as “god mode”

• God Mode worked like this: the tool couldn’t be used on the same computer that someone was using. Someone else would need to log into UB and turn the tool on. That person could then see all hole cards on the site—and then feed the information.

• 23 accounts. 117 usernames. $22 million dollars
• Lessons learned:
  • Configuration Management
  • Separation of Duties
  • Code Reviews
  • SDLC
  • Auditing
SSL Exploit

Discovered by Poker Table Ratings in May 2010.

Why use SSL when you can just XOR it........

Fixed 11 days later (hard to implement SSL)

UB/Absolute and Cake network were vulnerable
Misc. Account Compromise

- **will641 account hacked, please help! - Internet Poker - Online**
  Hi, Sorry if this is posted in the wrong place, I know some of you guys were at this table this morning so I'm looking for your help. This morning, my.
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached

- **My Neteller account has been hacked.. need advice - Internet Poker**
  Came home from school today, sat down by my laptop and logged in on MSN. Right awah I get a email from the neteller support that my $600 transfer has.
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached

- **The 2+2 Forum Archives: ACCOUNT HACKED!!!! FTP quick action saves ...**
  10 posts - 6 authors - Last post: Nov 30, 2007
  >>Subject: Re: URGENT ACCOUNT HACKED!!!! (XXXXXXXXXXXXXXXXXXXXX) >>Date: Fri, 30 Nov 2007 13:09:32 -0800 (PST) >> >>Hello XXXXXXXXXXXX, ...
  archives.1.twoplustwo.com › Internet Gambling › Internet Gambling - Cached

- **my accounts have been hacked - High Stakes Poker Pot Limit and No ...**
  Apr 21, 2009 ... stars tomluc and porkom ftp. Does anybody know what I'm supposed to do?
  forumserver.twoplustwo.com › ... › High Stakes PL/NL - Cached - Similar

- **Account hacked, guy plans on hacking more.... - Internet Poker**
  May 7, 2009 ... ORIGINALLY POSTED ON ANOTHER FORUM ON MAY 4TH..... My Full Tilt and Pokerstars account was hacked last night and approx $12000 drained out ...
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached

- **Full Tilt Account hacked - Internet Poker - Online Poker Forum**
  Mar 17, 2011 ... I hope this is some kind of software glitch but I am afraid my account at FTP has been hacked and cleaned out.
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached

- **Full Tilt Account hacked - Internet Poker - Online Poker Forum**
  Dec 23, 2010 ... my account got hacked 3 hours ago. turned out a guy from belgium(looked it up in the login details) logged in and made a 10$ deposit with ...
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached

- **fulltilt account hacked - Internet Poker - Online Poker Forum**
  Oct 19, 2010 ... I have returned to fulltilt about a month ago,after playing on another site.My account has been hacked and my money (2000 dollars) was ...
  forumserver.twoplustwo.com › Internet Poker › Internet Poker - Cached
• Poker bots are not new, but until recently they were not very good.
• Artificial intelligence has come a long way in the last few years.
• Chess bot vs. poker bot
• http://www.codingthewheel.com/archives/how-i-built-a-working-poker-bot
• http://bonusbots.com/
• Windowing & GDI
• Windows Hooks
• Kernel objects
• DLL Injection (in general: the injecting of code into other processes)
• API Instrumentation (via Detours or similar libraries)
• Inter-process Communication (IPC)
• Multithreading & synchronization
• Simulating user input
• Regular expressions (probably through Boost)
• Spy++
• Poker Sites have been cracking down on bots

• How do they catch them:
  • Betting patterns
  • Tendency
  • Program Flaws (always click same pixel)
  • Scanning

• When a player is identified as a bot, Full Tilt or PokerStars removes them from our games as soon as possible.” Their winnings are confiscated, he said, and the company will “provide compensation to players when appropriate.”
• Full Tilt – Banned after finding evidence of a poker bot on your hard drive:

On Sat, Oct 16, 2010 at 2:03 PM, Full Tilt Poker - Security
<security@fulltiltpoker.com> wrote:
Hello <#FAIL>,

As outlined in the email you received, you have been found guilty of a violation of our rules regarding the use of prohibited software. Specifically you have been found to have used the Shanky Technologies Bot. The email you were sent has been included below for reference. This decision was the result of an extensive and exhaustive review of your account activity on Full Tilt Poker.

Do not attempt to play on Full Tilt Poker in the future on a new or existing account. If you are found playing on the site again, your account will be suspended and all remaining funds will be forfeited.

We will not enter into any further discussion regarding this matter.

Regards
Security & Game Integrity
Full Tilt Poker
Online Poker Network Architecture
Online Poker Network Architecture (Cont.)
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 0.001109</td>
<td>10.0.0.10</td>
<td>10.0.0.118</td>
<td>DNS</td>
<td>Standard query A update</td>
<td>playdata.co.uk</td>
</tr>
<tr>
<td>4 0.001929</td>
<td>10.0.0.10</td>
<td>10.0.0.118</td>
<td>DNS</td>
<td>Standard query response A</td>
<td>200.26.205.38</td>
</tr>
<tr>
<td>6 0.083014</td>
<td>CadmusCo 31:e4:98</td>
<td>Broadcast</td>
<td>ARP</td>
<td>Who has 10.0.0.118? Tel</td>
<td>10.0.0.118</td>
</tr>
<tr>
<td>6 0.098799</td>
<td>Netgear 4d:0b:1e</td>
<td>CadmusCo 31:e4:98</td>
<td>ARP</td>
<td>10.0.0.1 is at 00:1b:24:fd:0b:1e</td>
<td></td>
</tr>
<tr>
<td>7 0.098835</td>
<td>10.0.0.118</td>
<td>200.26.205.38</td>
<td>TCP</td>
<td>[SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>3 0.184738</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[SYN, ACK] Seq=0 Ack=1 Win=1380 Len=0 MSS=1380 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>9 0.184925</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>0 0.195522</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>SSL Hello, Certificate,</td>
<td>Server Hello Done</td>
</tr>
<tr>
<td>1 0.281905</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>SSL Segment of a reassembled PDU</td>
<td></td>
</tr>
<tr>
<td>2 0.282584</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>SSL Segment of a reassembled PDU</td>
<td></td>
</tr>
<tr>
<td>3 0.282728</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message</td>
<td></td>
</tr>
<tr>
<td>4 0.381306</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Change Cipher Spec, Encrypted Handshake Message</td>
<td></td>
</tr>
<tr>
<td>5 0.403784</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Change Cipher Spec, Encrypted Handshake Message</td>
<td></td>
</tr>
<tr>
<td>6 0.489680</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>7 0.520735</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>8 0.606489</td>
<td>200.26.205.38</td>
<td>10.0.0.118</td>
<td>TLSv1</td>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>9 0.816848</td>
<td>10.0.0.118</td>
<td>10.0.0.10</td>
<td>DNS</td>
<td>Standard query A lb2</td>
<td>playdata.co.uk</td>
</tr>
<tr>
<td>0 0.842570</td>
<td>10.0.0.10</td>
<td>10.0.0.118</td>
<td>DNS</td>
<td>Standard query response A</td>
<td>200.26.205.62</td>
</tr>
<tr>
<td>1 0.844691</td>
<td>10.0.0.118</td>
<td>200.26.205.62</td>
<td>TCP</td>
<td>[SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>2 0.937937</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[SYN, ACK] Seq=0 Ack=1 Win=1380 Len=0 MSS=1380 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>3 0.938110</td>
<td>10.0.0.118</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1</td>
<td></td>
</tr>
<tr>
<td>4 0.950777</td>
<td>10.0.0.118</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=1 Ack=1 Win=64860 Len=122</td>
<td></td>
</tr>
<tr>
<td>5 1.037531</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[ACK] Seq=1 Ack=123 Win=64860 Len=1380</td>
<td></td>
</tr>
<tr>
<td>6 1.038336</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[ACK] Seq=123 Ack=123 Win=64860 Len=1380</td>
<td></td>
</tr>
<tr>
<td>7 1.038411</td>
<td>10.0.0.118</td>
<td>200.26.205.62</td>
<td>TCP</td>
<td>[ACK] Seq=123 Ack=2761 Ack=123 Win=64860 Len=746</td>
<td></td>
</tr>
<tr>
<td>8 1.121393</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=2761 Ack=123 Win=64860 Len=746</td>
<td></td>
</tr>
<tr>
<td>9 1.123828</td>
<td>10.0.0.118</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=123 Ack=3507 Win=64114 Len=198</td>
<td></td>
</tr>
<tr>
<td>0 1.210024</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=3507 Ack=321 Win=64662 Len=59</td>
<td></td>
</tr>
<tr>
<td>1 1.219956</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=3566 Ack=321 Win=64662 Len=37</td>
<td></td>
</tr>
<tr>
<td>2 1.211000</td>
<td>10.0.0.118</td>
<td>200.26.205.62</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=3603 Ack=64018 Len=0</td>
<td></td>
</tr>
<tr>
<td>4 1.221370</td>
<td>10.0.0.118</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=3603 Ack=321 Win=63981 Len=53</td>
<td></td>
</tr>
<tr>
<td>5 1.314878</td>
<td>200.26.205.62</td>
<td>10.0.0.118</td>
<td>TCP</td>
<td>[PSH, ACK] Seq=3640 Ack=374 Win=64609 Len=53</td>
<td></td>
</tr>
</tbody>
</table>
While the poker client is not exactly a root kit it does exhibit some of the same characteristics. The online companies argue this is for player protection against cheating. However, in doing this there is some invasion of privacy. I don’t know about you but I don’t like people to know what web sites are in my cache.
Poker Client Behind the Scenes

Lets take a look at what one of the poker clients is doing under the covers. Below we list some of the interesting items that the Cake poker client performs.

• **Function Calls**
  - EnemyWindowNames()
  - EnemyProcessNames()
  - EnemyProcessHashs()
  - EnemyDLLNames()
  - EnemyURLs()

• **Examines the system from programs or services it deems unauthorized**
  - OLLYDBG
  - POKEREDGE
  - POKERRNG
  - WINHOLDEM
  - OPENHOLDEM
  - WINSCRAPE
  - OPENSCRAPE
  - pokertracker
  - pokertrackerhud
  - HoldemInspector
  - HoldemInspector2
  - HoldemManager
  - HMHud
Well-known modifications and behavior observed by online poker clients:

1. **Modification to the Windows host-based firewall policies which allows for automatically authorizing various poker clients**

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy \StandardProfile\AuthorizedApplications\List ”C:\Program Files\Cake Poker 2.0\PokerClient.exe“

2. **Scanning the windows process table**
   - Cake poker reads through each of your process after approximately 10-20 minutes of idle time (Reading the .exe files in 4k increments) – based on Cake poker client 2.0.1.3386

3. **Ability to read the body and title bar text from every window you have open.**
   - Extracts the window handles (HWND), caption, class, style and location of the windows.

4. **Ability to detect mouse movements in order to determine human vs. automated movements.**
   - Mouse_event API / bots work the same way by writing custom mouse or keyboard drivers
Additionally functionality found in poker clients:

1. Poker applications scan for instances of winholdem/Bonus bots (Shanky technologies) running on your workstation or VM instance.
2. Poker clients monitor table conversation for lack of table talk and longevity of sessions.
3. Numerous tools to detect monitoring of your filesystem and registry can be used.
4. Poker applications are known for monitoring Internet Caches for URL history information.
5. Cookie creation from just about every client.
- Cake Poker client is comprised of three main processes (CakePoker.exe, PokerClient.exe, and CakeNotifier.exe).

- The client scans itself during random intervals most likely protecting itself against modification or patching of the executables.

- Found the client (CakeNotifier.exe) also scanning directories containing packet capture files and reflector (a .NET decompiler)???

- **Cake poker’s executables are all obfuscated**
  - PokerClient.exe is obfuscated – 12mb in size (huge – most likely encrypted).
  - Bodog version 3.12.10.5 is only 4mb in size
- Bodog version 3.12.10.5 file monitoring and registry activity

- Prefetch files are created in C:\Windows\Prefetch

- Digital certificate directory is created - C:\Users\jd\AppData\LocalLow\Microsoft\Cryptnet\UrlCache (used for storing certificates)

- BPGame.exe modifies itself with new attributes

- Reads through your URL cache

- Loads images from Bodog poker installation directory
Queries your registry

- Looks in your HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- Queries your hardware settings on your workstation
- Read User Shell folder – the user shell folder subkey stores the paths to Windows Explorer folders for the current user of the computer.
- TCP send request from localhost to 66.212.245.235 on port 80
- (After SSL handshake) - TCP send request from localhost to 66.212.249.155 on port 7997
- Session manager (HKLM\Sysstem\CurrentControlSet\Session manager
  - Gets the environment variables of the machine
  - Username
  - Root directory of windows
  - Tmp dir
  - Path
  - Operating system
Didn't even try to filter XSS, no fun...
Web App Vulnerabilities (Cont.)

The requested resource (account)

Microsoft Internet Explorer

Just a simple XSS

OK
Web App Vulnerabilities (Cont.)
If you thought it took some advanced techniques… Fail.

- Cross-site scripting heaven (persistent and reflective); apparently the designers felt `<script>` might be needed in numeric only fields.
- Unvalidated redirects; where would you like poker sites to take you?
- Pretty much zero input validation.
- Expired SSL certificates, not necessarily a vulnerability, but seriously?
While sophisticated attacks are fun, sometimes you just need to go back to the basics. While some of the sites offer multifactor authentication these are not standard and cost extra. The sites differ widely in their password complexity requirements.

<table>
<thead>
<tr>
<th>Poker Site</th>
<th>Password Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbon</td>
<td>Between 6-20 characters</td>
</tr>
<tr>
<td>Bodog</td>
<td>At least 5 characters</td>
</tr>
<tr>
<td>Cake</td>
<td>Between 8-14 and must contain the following: Lower case, upper case, number, special character</td>
</tr>
<tr>
<td>Full Tilt</td>
<td>At least 5 characters</td>
</tr>
<tr>
<td>UB/Absolute</td>
<td>At least 6 characters</td>
</tr>
</tbody>
</table>
With passwords this strong it must be impossible to brute-force......

Especially with no account lockout

And login IDs fairly well known, thank you PTR

Can anybody say Hydra? Brutus?.........
Some poker sites use non-random numbers as UID's.

for uid in `seq 3830000 3840000`;do
echo $uid > users.txt;done

(1 Second later…)

Half the battle? Done
Several businesses have developed supporting the poker sites, these include:

- Training sites (Cardrunners, Deuces Cracked)
- Tracking sites (PTR, Sharkscope)
- Media/Forums (Two+Two)

If these sites are used by online poker players could they be leveraged in order to gain information or launch target phishing accounts with the goal to install malicious software in order to see their cards?
Last night we identified and stopped an illegal intrusion of the CardRunners servers.

While no customer credit card or financial information was compromised, we have confirmed that the following customer information related to your account may have been compromised:

- Email Address
- Encrypted Password
- IP Address

Out of an abundance of caution, we have forced your password to be reset. If you use your CardRunners username or password for other unrelated services or accounts, we recommend that you change them as well.

Your new password is: iuTeSavB

CardRunners will never contact you in any way asking for any personally identifiable information so please be vigilant in not providing such information to anyone that represents themselves as working for CardRunners.

We regret any inconvenience this causes and want to ensure you that we will continue to work to ensure that additional measures are taken to protect your private information.

Regards,
CardRunners Support
River
Need to move away from password based authentication and toward multifactor, because that can’t be hacked right (RSA)?

Maybe implement simple things, say like account lockout

Perform robust security testing and configuration management

Only allow connections from specific geographic locations

Adhere to certain standards (i.e. ISO, PCI, FISMA)
Online Poker Defenses – User

- Have dedicated VM for poker and only use it for that purpose
- Use antivirus/spyware (D’oh)
- Don’t play on insecure wirelesses networks
- Use strong, complex passwords. Better use multifactor authentication where available
- Don’t use same password across multiple sites
- Monitor your traffic
Next Steps in Research

• Continue digging deeper into the poker client
• Custom client to bypass restrictions
• Automated tool to brute-force poker passwords
• More mapping out poker networks
• In-depth look at web application vulnerabilities
Conclusion

• While we did not uncover a smoking gun, based on preliminary research there seems to be several areas that do require strengthening and further exploration is sure to identify more serious issues

• Regulation and compliance is needed to attempt to make companies develop and secure their gaming networks

• Do I feel safe playing?
Questions?