An Overview Of Online Poker Security

Luigi Auriemma[1] and Donato Ferrante[2]
ReVuln
http://revuln.com
info@revuln.com
http://twitter.com/revuln
10 April 2013

Abstract *Security research conducted against a set of online poker solutions, highlighting the current status of this lucrative industry.*

1 Introduction

Online Gaming (also known as Online Gambling and *iGaming*)[3] is a successfully growing market, and Online Poker[4] is its main sector with millions of players all around the world betting with real money.

Online gaming is a 30 billion US dollar market[5], and is highly regulated by gaming authorities of various countries in order to protect consumers, companies and its governments by making it transparent and secure. The main objectives of the gaming authorities are:

- Protecting players' rights
- Promoting responsible gaming
- Monitoring licensed companies
- Deciding the minimal level of security that must be adopted
- Collecting taxes on behalf of the governments

Companies that violate the rules, or don't take appropriate measures for the security of their systems, may have their license revoked, and in some cases become sanctioned by the gaming authorities. This means each component of the online gaming network, client and server side, must be secure.

2 About This Research

This paper provides a cursory overview of *iGaming*, and *Client Poker Software* security. Also, security vulnerabilities and design issues affecting some of the most widely used software on the market will be disclosed.

[1] http://twitter.com/luigi_auriemma

[2] http://twitter.com/dntbug

[3] http://en.wikipedia.org/wiki/Online_gambling

[4] http://en.wikipedia.org/wiki/Online_poker

[5] http://www.forbes.com/sites/afontevecchia/2012/12/06/can-online-poker-save-zynga-417b-global-gambling-market-throws-pincus-a-risky-lifeline/

Online gaming companies and players should be aware of potential security issues in the products they provide and use respectively. The security issues and information disclosed in this document covers only part of the attack surface for *Online Poker systems*.

Software systems from different companies in various countries were examined, and in this paper we detail three case studies. Some features beyond the scope of the paper were not tested. Several details of the issues and proof-of-concept have not been included in this document.

3 The Authorities

There are various authorities and commissions that regulate *iGaming* in a given country or a set of countries, depending on the license. A full list of these authorities[6] is available on the *International Association of Gaming Regulators* (IAGR) website.

4 The Companies

The large *iGaming* market consists of many companies which provide one or more services for the infrastructure[7] available to the end user. Companies can provide:

- The client and server side software
- The network[8]
- Web games for online casino
- Additional technology
- Websites[9], called *Skins* and *Poker Rooms*, which are accessed by the players.

Large operators such as PokerStars[10] will cover all of the above, and even sponsor real poker events and tournaments for professional players[11] [12]. It is quite common to have an online gaming company that provides the software and the gaming network.

5 The Skins

Understanding the role of *Skins* is important because a vulnerability in one software can affect multiple *Skins* and millions of players. Players are mistaken to believe *Skins* provide the entire infrastructure for the website. *Skins* also create the interface and software customization for the players.

[6] `http://www.iagr.org/members/`
[7] `http://www.pokerscout.com/IndustryOverview.aspx`
[8] `http://www.pokerscout.com/PokerNetworks.aspx`
[9] `http://en.wikipedia.org/wiki/Category:Gambling_websites`
[10] `http://www.pokerstars.com`
[11] `http://www.pokerstars.com/wcoop/`
[12] `http://www.pokerstars.com/poker/tournaments/`

6 The Client Software

One of the differences between online poker and the rest of the *iGaming* products is that it relies on client-side software, which runs directly on the player's computer[13]. The client software is used to improve the players experience and granting them real-time data over customized protocols adopted by the *Poker network*.

Additionally the client software allows players to customize the interface, and the software functions the same way across different platforms (Windows, MacOS and Linux).

From an external attacker's point of view, *Client Software* is interesting to analyze because it is the only part of the infrastructure which is fully available to an attacker. In fact, the software is deployed on the end-user systems, and without performing any unauthorized access to the server-side infrastructure, the security of these solutions can be analyzed. Serious client software issues include unauthorized access to players' accounts.

7 Attack Surface

The following sections describe the portion of the attack surface that was covered for this paper.

7.1 Updates

Software updates are very important for this kind of software. All *Poker software* must adhere to certain standards, and include an auto-update feature which is the first action performed by the software launcher. This mechanism can be used by attackers to inject malicious updates on the player's system, while the software is performing the update operation. For example, this can be achieved with insecure public connections[14], compromised connections[15], or malware.

Usually the main cause of malicious injection while performing an update is the lack of SSL connections or lack of digital signatures. Even if an update is signed, it's still possible to take control over a victim's system, as demonstrated by one of the vulnerabilities found in a particular *Client Software* that uses digital signatures. The same consideration above also applies to the installer. The main task of the installer is to download additional content from the Internet. It doesn't matter if the original *setup.exe* was correctly downloaded over an HTTPS connection from a trusted website because all of the remaining content downloaded by the installer from the internet, over HTTP, can be hijacked.

7.2 Ways used to store passwords and/or encrypting files

The player's *username* and *password* is usually the only obstacle that keeps an attacker away from a player's account.

All *Poker software* allows the password to be automatically saved on the player's computer. Insecure implementation of this functionality may not be secure enough

[13] `http://www.pokerscout.com/PokerNetworks.aspx`

[14] Like public Wi-Fi networks, LAN/WAN networks of a company

[15] For example private Wi-Fi with weak passwords guessed by an attacker, compromised DNS servers

to prevent password leaking. The stored password is often just obfuscated or encrypted with fixed keys. Access to registry keys or the configuration file (even remote access is possible using directory traversal vulnerabilities in other software) allows attackers to steal stored passwords easily. It's not easy to grant access to the network without effectively storing the password, but there are various levels of password security. For example, there is a difference between obfuscating a password and encrypting it with an unique key that identifies the computer.

Some companies like PokerStars have adopted RSA tokens[16] and PIN[17] to increase the security of the authentication mechanism for their *Client Software*.

7.3 Others

There are many other possibilities to perform attacks against the software. See the following sections for examples.

8 Issues

A number of different security issues were found, and some of them are described in the following sections. A proof-of-concept video[18] for some of the issues is available on our Vimeo channel[19].

8.1 DEP / ASLR / Digital Signed Executable

The following table gives an overview about *DEP*, *ASLR* and *Digital Signed Executable* for the tested solutions:

	EXE			DLLs		
Software	**ASLR**	**DEP**	**Digital signed**	**ASLR**	**DEP**	**Digital signed**
B3W	no	no	yes	-	-	-
Microgaming	yes	yes	no	no	no	no
Playtech	yes	yes	yes	no	yes	no

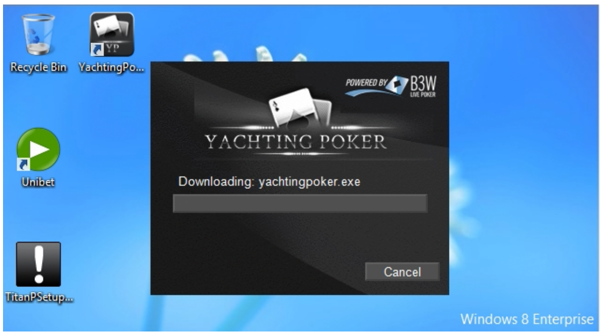
8.2 Bad update system and weak password protection in B3W

The client software developed by B3W[20] is used in many Skins[21] such as Yachting Poker and PKRaise.

The update mechanism is performed over an insecure HTTP connection to *b3w.fileburstcdn.net* where the list of updates and the files are stored without signatures and the *EXEs* (which are digitally signed) are not verified before their execution. In this situation at least three types of issues were identified:

- *Injecting of malicious* EXEs, which are executed immediately by the software for auto-updating itself:
  "*c:\path\tmp_executable.exe*" "*c:\path\executable.exe*" *update*

[16] http://www.pokerstars.com/poker/room/features/security/rsa-token/
[17] http://www.pokerstars.com/poker/room/features/security/pin/
[18] http://vimeo.com/63855488
[19] http://vimeo.com/revuln
[20] http://www.b3wgroup.com
[21] http://www.b3wgroup.com/clients/

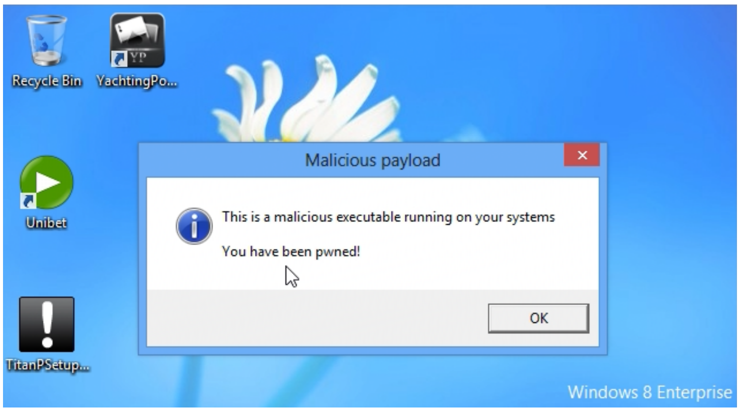


Downloading: yachtingpoker.exe

Figure 1: Yachting Poker launcher in action

- *Directory traversal* that allows any files where the software is installed to be created or overwritten.
- *Stack based buffer-overflow* while copying the newly generated update link containing the *filename* provided by the attacker:

```
_mbscpy(
   stack_buffer,
   "http://b3w.fileburstcdn.net:80/updates_SKIN/aaa...aaa"
);
```



This is a malicious executable running on your systems

You have been pwned!

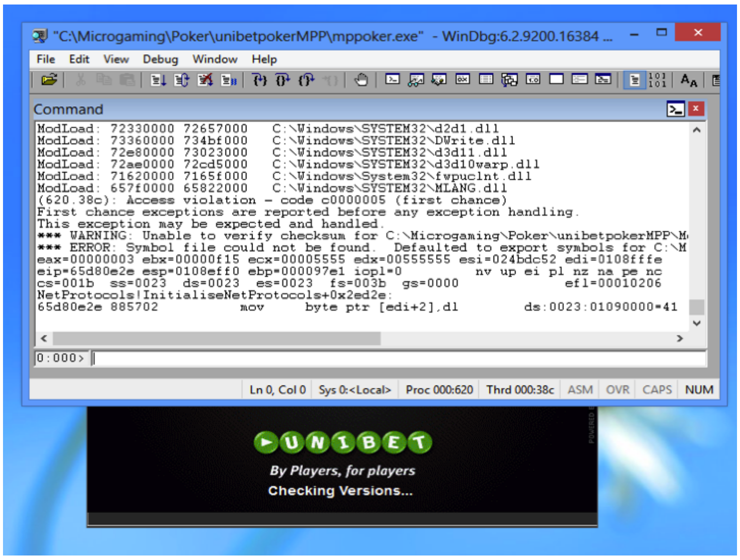
Figure 2: Malicious code executed on the victim's system

The password is stored in the *%APPDATA%\SKIN_NAME\settings.ini* file as *last_password* and is simply obfuscated, and the following algorithm can be used to read it:

```
len = hex2byte(password);
x = password[0];
for(i = 0; i < (len - 1); i++) {
    password[i] = password[i + 1] ^ x;
    x = password[i] + i;
}
password[i] = 0;
```

8.3 Bad signed update system and weak password protection in Microgaming

The Microgaming[22] software is available on various important and well known *Skins* like Unibet[23] and Ladbrokes Poker[24].



"C:\Microgaming\Poker\unibetpokerMPP\mppoker.exe" - WinDbg:6.2.9200.16384 ...
File
Edit
View
Debug
Window
Help
Command

```
ModLoad: 72330000 72657000   C:\Windows\SYSTEM32\d2d1.dll
ModLoad: 73360000 734bf000   C:\Windows\SYSTEM32\DWrite.dll
ModLoad: 72e80000 73023000   C:\Windows\SYSTEM32\d3d11.dll
ModLoad: 72ae0000 72cd5000   C:\Windows\SYSTEM32\d3d10warp.dll
ModLoad: 71620000 7165f000   C:\Windows\System32\fwpuclnt.dll
ModLoad: 657f0000 65822000   C:\Windows\SYSTEM32\MLANG.dll
(620.38c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Microgaming\Poker\unibetpokerMPP\M
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\M
eax=00000003 ebx=00000f15 ecx=00005555 edx=00555555 esi=024bdc52 edi=0108fffe
eip=65d80e2e esp=0108eff0 ebp=000097e1 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
NetProtocols!InitialiseNetProtocols+0x2ed2e:
65d80e2e 885702          mov     byte ptr [edi+2],dl          ds:0023:01090000=41
```

Figure 3: Microgaming

This software is also an interesting example of a signed update system made ineffective by the exploiting of a security vulnerability. The digital signature available at the end of the main update list file which is verified by the software, is stored as a base64 string. The problem is that the function that decodes the password doesn't verify the length of the output stack buffer resulting in a buffer-overflow that may be used to execute malicious code.

The password stored in the registry key:
HKEY_CURRENT_USER\Software\MGS\Thumper\Casino\SKIN_NAME\key is encrypted using the same mechanism adopted also for some of the files in the software folder:

- SHA1 hash of one of the following keys (the fifth one for passwords)

  1. "*C75A7F71-797A-11d2-8255-00A02455A490*"
  2. "*AE24F415-C51D-4aa2-9943-C1DD9EA33DFE*"
  3. "*{D545EBD1-BD92-11CF-8772-00A0C9039735}*"
  4. "*Cats know how we feel. They don't care, but they know.*"

[22] http://www.microgaming.co.uk/

[23] http://www.unibet.com/poker

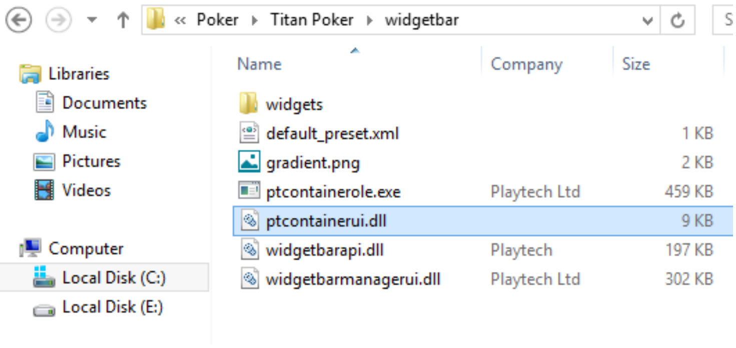
[24] http://poker.ladbrokes.com/en

5. "*BlindCaffineSubstituteFamousCurtainTrickKingTinHalcyonDaysArapaho*"
6. "*C75A7F70-797A-11d2-8255-00A02455A490*"

- Swapping of the 5 *DWORDs* composing the hash, although only 16 of the 20 bytes available will be used for the encryption
- *RC4(hash, 16, data, length)*

8.4 Unsecure update system and password protection in Playtech

Playtech[25] software and its *iPoker network* [26] are widely used by many *Skins*. The most famous are Titan Poker[27], William Hill Poker[28] and Bet365 Poker[29].



Name	Company	Size
widgets		
default_preset.xml		1 KB
gradient.png		2 KB
ptcontainerole.exe	Playtech Ltd	459 KB
ptcontainerui.dll		9 KB
widgetbarapi.dll	Playtech	197 KB
widgetbarmanagerui.dll	Playtech Ltd	302 KB

Figure 4: Playtech widgetbar injection

The software installation and the updates are handled all via HTTP, but the signatures of the signed *EXEs* and *DLLs* to install are verified. This is good only partially because all the other files (including HTML files) can be modified without any problems. For example to exploit security vulnerabilities in the software or redirecting the user on malicious websites. More interestingly is the presence of *EXEs* and *DLLs* that are not digitally signed located in the *widgetbar* folder. An attacker can use them to inject malicious code on the software.

The following is a perfect example of an update system implemented incorrectly. The password is automatically stored in the registry key:

HKEY_CURRENT_USER\Software\SKIN_NAME\password_new

A key is composed of the hash of the HDSLN value of *Windows Genuine Advantage*, plus three values of format, "*%ld%ld%ld*", are obtained via *GetSystemInfo*, where the arguments of this function are *dwProcessorType*, *wProcessorLevel* and *wProcessorRevision*.

Then the hexadecimal MD5 hash of the key and the first byte of the password are used to XOR the encrypted keyword:

[25] http://www.playtech.com
[26] http://www.ipoker.com
[27] http://www.titanpoker.com
[28] http://poker.williamhill.com
[29] http://poker.bet365.com

```
    len = hex2byte(password);
    x = password[0];
    for(i = 0; i < (len - 1); i++) {
        password[i] = password[i + 1] ^ hex_hash[i % 32] ^ x;
    }
    password[i] = 0;
```

9 Additional resources

The following examples weren't part of this research but they are a personal work of one of our researchers[30] for his password recovery tools. The following content can be used to get a better understanding of the algorithms used in the *iGaming* software.

- Cake Poker[31] in the past obfuscated the password inside the registry to XOR it with an incremental value derived from the CRC of the same password[32] while now it's saved in clear text inside the ".store" files of the CPN\SKIN_NAME user's folder.
- Full Tilt Poker[33] encrypts the password using XOR and a pseudo random scheme with the initial seed calculated on an unique 16bit value of the system in use[34].
- PartyPoker[35] uses 3DES CBC with a fixed key and ivec[36].
- PokerStars[37] adopts a particular system for the generation of the unique key and uses DES CBC for the encryption[38].

10 About ReVuln

ReVuln[39] is an international company providing various security services ranging from penetration testing to consulting, from training to vulnerability research and, last but not least, feeds regarding 0-days security vulnerabilities.

Additionally ReVuln is a Maltese company, and Malta is one of the most important countries involved in *iGaming*[40].

11 Acknowledgments

We would like to thank our friend Salvatore Fresta[41] for the additional overview of the *iGaming* sector.

[30] http://aluigi.org
[31] http://cakepoker.com
[32] http://aluigi.org/pwdrec.htm#cakepokerpwd
[33] http://www.fulltiltpoker.com
[34] http://aluigi.org/pwdrec.htm#fulltiltpwd
[35] http://www.partypoker.com
[36] http://aluigi.org/pwdrec.htm#partypwd
[37] http://www.pokerstars.com
[38] http://aluigi.org/pwdrec.htm#pokerstarspwd
[39] http://revuln.com
[40] http://www.lga.org.mt
[41] http://salvatorefresta.net

12 Revision History

- 12 April 2013: Version 1.1 released.
- 10 April 2013: Version 1.0 released.