CYBERSAFETY

Brian Regli, Ph.D, Drakontas LLC
March 18, 2015
C2P2FL
Social Media – Technical Landscape

Collaboration
- Social Bookmarking
- Social News
- Wikis

Communication
- Blogs
- Micro-blogging
- Geo-social Networking
- Social Networking Sites

Entertainment
- Virtual Worlds
- Social Games
- Console Communities
- Geo-social Games
- MMOGs

Multimedia
- Video Sharing
- Photography Sharing
- Music Sharing
- Live-casting
The Collaboration Sphere

- Social Bookmarking
- Social News
- Wikis
- Social Collaboration
The Multimedia Sphere

- Video Sharing
- Photography Sharing
- Music Sharing
- Live-casting
The Entertainment Sphere

Virtual Worlds

Social Games

Console Communities

Geo-social Games

MMOGs*

*Massively Multiplayer Online Games
Basic Facts: Gaming, Internet and Online Communities

- **59** percent of Americans play video games
- In 2013, the industry sold **160 million games** and generated more than **$21 billion** in revenue, **$7.2 billion** of which came from purchases of digital full games and add-on content, mobile apps, subscriptions and social network gaming
- The average gamer is **31** years old, and **71** percent are age 18 or older
- Nearly half (**48** percent) of gamers are female and women over the age of 18
- A majority of parents (**56** percent) say video games are a positive part of their child’s life

http://www.theesa.com/about-esa/industry-facts/
Online Communities - Components

- Email
- Text Chat
- Voice Chat
- Video Chat
- Social Networking
- File Exchange
- Currencies and Purchases
- Modifications (Mods)

The threats your child will face most likely involves the forms of interaction listed above.
Many virtual worlds and online games will have an internal email system to allow users to communicate within one another.
The Words with Friends (Zynga) application features an embedded chat functionality.

Zynga stores payment information and customer data for longer periods of time than it does in-game chat messages, according to a page on their website – see source below.

Source: http://company.zynga.com/node/886
In some virtual worlds, the chat function is integrated into the game play. The dialogue scrolls along in the game window. The chat conversation in this room included sexual banter, discussions of smoking pot, advertisements for the black market sale of Habbo coins, and requests to show your body via Skype.
Voice Chat

- Similar to text chat, voice chat allows users to communicate in real-time during game play.
- Assume that voice chat sessions are not recorded/logged by the game providers, so the evidence trail is not available, unless the conversation is privately recorded.

Second Life supports voice chat. One way to access voice chat is through the options menu under the avatar information screen.
Video Chat

- Video chat allows users to communicate in real-time before, during and after game play and see the other player/user “face-to-face.”

- Xbox 360 and PlayStation 3 give users access to popular social networking sites.

Through the gaming consoles, you can:

- Post, view, and save photos/videos
- Update profile and status
- Find new friends
- Use integrated email
- Use instant messenger
- Follow (or stalk) other users
In-App Purchases

Source: http://online.wsj.com/article/SB10001424052702303753904577452341745766920.html
Virtual Currencies and Payment Systems

• Users purchase “virtual” goods with “virtual” currency
• Virtual currency can be earned by game play or by “real” currency purchases
• Multiple payment platforms
  – In-World vs. Real-World Transactions
  – Prepaid Cards – MOL Global
  – Mobile Wallets
• Amounts range from micropayments to a $330,000 space station
• Virtual worlds support a wide range of entrepreneurial activities
Theft of Virtual Goods

'Virtual theft' leads to arrest

A Dutch teenager has been arrested for allegedly stealing virtual furniture from "rooms" in Habbo Hotel, a 3D social networking website.

The 17-year-old is accused of stealing 4,000 euros (£2,840) worth of virtual furniture, bought with real money.

Five 15-year-olds have also been questioned by police, who were contacted by the website's owners.

The six teenagers are suspected of moving the stolen furniture into their own Habbo rooms.

(Source: http://news.bbc.co.uk/2/hi/7094764.stm)

Approximately $5,246 US
Virtual & Gaming World Crimes

World of Warcraft accounts stolen

Symantec finds 44 million gaming credentials in online warehouse
By Ellen Messmer | Network World US | Published: 12:53 GMT, 27 May 10

Symantec says it has unearthed a server hosting the credentials of 44 million stolen gaming accounts - and one of the most surprising aspects of it is that the accounts were being validated by a Trojan distributed to compromised computers.

The purpose of this Trojan-based validation is apparently to figure which credentials are valid and can be sold. Symantec is calling this the Trojan.Loginck, and as described in a blog post by Symantec researcher Eoin Ward, the database of stolen information includes about 210,000 stolen accounts for World of Warcraft, 60,000 for Aion, 2 million for PlayNC and 16 million for Wayi Entertainment, all of which were being sold online.

Symantec is recommending users of these sites change their passwords.

"The particular database server we uncovered seems very much at the heart of this operation - part of a distributed password checker aimed at Chinese gaming sites. The stolen login credentials are not just from particular online games, but include user login accounts associated with sites that host a variety of online games," Ward writes.

In his blog, Ward says to turn the gaming credentials into cash, the cybercrooks have apparently written a program that checks the login details using Trojan.Loginck to make sure they are valid, which is easier than trying to log into gaming sites 44 million times.

The value of stolen accounts credentials can range from $35 to several thousand dollars, according to Symantec’s research, which sought a rough market value based on prices associated with www.playerauctions.com, described as a legitimate Web site to protect buyer and seller against fraud.

"Most botnets have the ability to download and run files, so why not push a custom piece of malware to each bot? The malware could log on to the database and download a group of user names and passwords in order to check them for validity," Ward writes. The database in question was holding 17GB of flat file data, and Symantec analyzed its attempts to validate passwords for Wayi Entertainment. There are said to be credentials for at least 18 gaming Web sites in the database.

Gaming is Everywhere!

- Interfaces to Handheld/Mobile Devices
  - Game Center (Apple)
  - Xbox Live/Windows Mobile
  - OnLive Mobile
  - Google TV, Google +

- Due to the widespread adoption of handheld/mobile devices, wireless networks, and cloud storage, users can take their games with them wherever they go
Gaming is Everywhere!

- **Security:**
  - Battle.net “high security” accounts with fob-like encryption keys (Authenticator)
  - Two-Factor Authentication features a unique on-time password with each login
  - Mobile Authenticator app for iOS, Android and BlackBerry devices
Ripped from the Headlines

- **Child Pornography Storage:** *PlayStation Sex Crime: Criminal Used Video Game to Get Girl’s Naked Pictures* – “Prosecutors in Houston say they have tracked down and arrested a man who allegedly committed an online sex crime – though, technically, he didn’t even have a computer…. Anthony Scott O’Shea of Somerset, KY., persuaded an 11-year-old girl in Houston to e-mail nude pictures of herself from her PlayStation to his.”

Level III Sex Offender Uses Xbox Live

Griefers: Examples of Cyberbullying in Minecraft

– Players interact with one another as they build structures and objects within their own “sandbox,” and they can travel from location to location and interact with each other using the same server.

– The game’s greatest benefit – its openness to multiplayer interaction – also has a significant drawback: players can destroy the work of another.
The Value of Digital Goods: Real-World Crime Example

• **Online Enticement (of Children for Sexual Acts):** *Child Pornographer Hid Behind XBox LIVE “Call of Duty: Modern Warfare 2”.* John Basto used his Xbox LIVE gaming station to meet a 10-year-old boy from Oklahoma...in order to solicit pictures of the child’s genitals.

• Basto offered the kid a deal: In exchange for the pictures, he would send the boy twenty cheat codes, which would allow the child to use elite weapons, obtain an unlimited number of game “lives,” and other advantages that are normally earned through extended rounds of play.

What hooks you? (Delmonico)

• The internet matches to personality and mood
• The internet matches to disorders.
• The internet can be both dynamic and static
• The internet stimulates many senses
• The internet impairs empathy.
Triple A Engine (Cooper)

• Computers and gaming systems permit:
  – Anonymity
  – Accessibility
  – Affordability

  Allows people do and say things they would normally not say or do.
5 Stages of Internet Grooming

- **Friendship:** Flattering a child into talking in a private chat room where they will be isolated. The child will often be asked for a non-sexual picture of themselves.

- **Forming a relationship:** Asking the child what problems they have to create the illusion of being their best friend.

- **Risk assessment:** Asking the child about the location of their computer and who else has access to it in order to assess the risk of being detected.

- **Exclusivity:** Building up a sense of mutual love and trust with the child, suggesting that they can discuss "anything".

- **Sex talk:** Engaging the child in explicit conversations and requesting sexually explicit pictures from them. At this stage the pedophile will usually try to arrange a meeting with the child.
Reporting Resources

- **GetNetWise** ([http://kids.getnetwise.org](http://kids.getnetwise.org)): is a resource that provides information for parents on online safety, safe websites for children and links to report criminal behaviors their children may experience, from sexual solicitation and luring to cyberstalking.

- **Internet Crime Complaint Center (IC3)** ([http://www.ic3.gov](http://www.ic3.gov)): is a Federal resource from the FBI and the National White Collar Crime Center (NW3C) that provides a centralized means for victims of online crime to report incidents and for law enforcement to search reported events and identify patterns across the Internet.

- **Internet Keep Safe Coalition** ([http://www.ikeepsafe.org](http://www.ikeepsafe.org)) is an international nonprofit alliance of more than 100 organizations and individuals that tracks global trends and issues surrounding digitally connected products and their affect on children. Additionally they assist K-12 organizations in the development of materials related to online and digital product safety.

- **National Crime Prevention Council (NCPC)** ([http://www.ncpc.org](http://www.ncpc.org)) is a Federal resource that provides crime-prevention strategies, including online/Internet safety best practices, for use in communities and schools.
Reporting Resources

- **School Reach.com** ([http://www.schoolreach.com](http://www.schoolreach.com)) is a system that allows parents to receive notifications from schools via their smartphone. It also manages the CyberBully Hotline ([http://www.cyberbullyhotline.com](http://www.cyberbullyhotline.com)), an anonymous two-way reporting system for administrators, students, and parents.

- **Web Wise Kids** ([http://www.webwisekids.org](http://www.webwisekids.org)) is a national nonprofit organization whose mission is to educate children, parents, and the community about making safe decisions online and to assist them in addressing sexting, bullying, piracy, fraud, cyberstalking, and other online threats.

- **WiredSafety** ([http://www.wiredsafety.org](http://www.wiredsafety.org)) is an online safety organization that provides education, awareness, and training on Internet safety, privacy, and security-related issues. They also provide victim assistance for those impacted by cybercrimes and harassment, as well as training and advice for law enforcement professionals on preventing, identifying, and investigating cybercrimes.
Talking to your Children

• Do you play video games or in virtual worlds? Do you use social networking sites?
• How many hours a week do you play? Do you play at night? During the day?
• Do you talk to people about the games you play? Do you play with friends at their houses (or do they come over to your house to play)?
• Do you talk to your friends or strangers within these games?
• Have you ever seen or heard anything offensive or have you felt threatened while playing a video game online?