Gaming Networks

Cybercrime, Terrorism and Trends

By : SW David Swan CD
Executive Vice President Defence Intelligence Group

C/DIG CSCSS / DEFENCE INTELLIGENCE GROUP

Special Report: The Potential Threat from Gaming Networks

Recently there has been mainstream media reporting that NSA had 'hacked' gamers networks. Some of the reports I reviewed seemed to have a sub-text of “are you kidding?” or “is this for real?”. A weekly podcast I listen to, scoffed at the idea of NSA monitoring 'World of Warcraft'[1] and asked why anyone would spend time in a world of 12 year olds[1]. From the attackers perspective, these networks have huge potential: for identities, money, for communications, and a lot more. This C/DIG Digest outlines the potential threat in gamers networks – from the perspective of terrorist and criminal hackers. What is Intelligence?

Gamers Networks

For people like myself who are not 'into' computer games, the scope of the gaming world is remarkable. We are not talking about casino gaming such as: on-line poker, “Texas Hold'Em”, blackjack etc. we are talking about what many think of as 'on-line kids games', such as World of Warcraft, Call of Duty, Star Trek On-Line, Battlefield, Minecraft and thousands of other titles. The size of these networks is remarkable. World of Tanks boasts seventy (70) million users. Gaming companies operate groups of servers spread across the globe. Some games allow for individuals to host 'personal' servers, accessible from the Internet, loosely linked to larger organizations. The range of capability is from individual servers that users log into to global networks of servers with internal voice, chat and e-mail. Many games allow for the transfer of 'money'[1], resources and even books between players.

Many of these networks provide for their users to create an alias. It is understood that gaming is not 'reality' so aliases are expected. Technically, some gaming networks surpass the capabilities of corporate network environments.

Gaming networks are not considered a 'high-security' environment

Games can require high demand / high load, high levels of graphics processing, high amounts of data storage, and can even have their own communication protocols. Serious gamers are often early adopters of technology because of the performance demanded by some games. High capability CPU's and graphics cards, high resolution monitors, bulk data storage and high speed network connections are common among serious gamers. In any environment there is a continuum, and there are many low-end gaming netw.orks. Each gaming network, and even stand-alone servers, offer a variety of potential services to the hacker / criminal environment

Gaming networks are not considered a 'high-security' environment. As previously stated, aliases are pretty much expected. Some gaming companies offer special features to protect personal information, however in general security practices are unremarkable. Of greater concern for companies developing games is the integrity of the game code and game features. Some environments allow for fans to add artwork and contribute to the overall game. Other companies strictly control the code and licenses.

Gaming networks show up in some unusual places. Computer games are a useful way to test networks during installation because of the high loads they place on servers and client workstations. Sometimes games installed as part of testing are left in place, even on 'secure' networks. Network file servers and application servers that support business applications sometimes host game servers in order to generate additional revenue. Since highest gaming activity tends to be outside business hours, there may not be much conflict. Some people play computer games on their workstations during noon-hour or when they are not busy. Usually they are oblivious to the threat they are posing to the rest of the network.

Criminal Use of Gaming Networks

To criminal hackers gaming networks offer interesting features. If a criminal wanted to hack the corporate side of gaming networks, game companies have personal information and credit card information. Once a game network is accessible, higher end gaming computers have the CPU required for cracking passwords and encryption. If the game code is cracked, the resources of the network could be used for Distributed Denial of Service (DDoS) attacks and spam distribution – *not attributable to the criminal organization*. In short, gaming networks offer criminals potential for revenue and as platforms for providing criminal services.

Communications is an issue for criminals. They don't want their transactions tracked – making anonymity important. Gaming networks that support internal social media such as texting, voice chat and exchanging resources has a great deal of potential for misuse. Misuse could include: buying and selling stolen property, buying and selling drugs, weapons or any other criminal activity.

Terrorism Use of Gaming Networks

Terrorist organizations can have many of the features of more conventional organizations. They can have: an organizational structure, personnel management, operations, recruiting and financial management, to name some of their features. This requires communications, preferably communications that is not tracked by Intelligence / security organizations. Global gaming networks with internal communications offer the terrorist a means to remain anonymous, while passing data.

Almost anything that can be done in the real world, can be done in the world of on-line gaming. Players can 'meet', in public or private. They can explore scenarios. The terrorist has the ability to 'hide in plain sight' while accessing the meeting from anywhere in the world. Crowds of characters moving through virtual cities provide cover for more sinister activity.

---

1 World of Warcraft is an on-line, multi-player, role playing, fantasy game. It boasts millions of players.

2 Weekly Tech Update by BCCHardware: http://www.bcchardware.com/podcast/wtu.xml This a casual format podcast that focuses on gaming and hardware. The company web page is: http://www.bcchardware.com

3 Most games don't transfer cash directly, but have some form of game based currency that can be transferred between players.

Gaming networks have interesting potential to governments

Discussing how to attack a target would be 'normal' in many shooter games, so even if the discussion was detected it might appear entirely normal or appropriate in the context of the game.

Government / Government Sponsored

Gaming networks have interesting potential to governments. If, like Russia, you wanted to disrupt another country's economy, the ability to direct one (1) million computers – that are not attributable to you – against a particular target, would be an invaluable resource. If the game network involved was high-end, then most of the computers would probably be high capacity with a significant amount of Internet bandwidth. If the attack was masked by a planned activity within the game, you could have a massive decentralized attack, controlled through a global command and control network, executed by high capacity computers, whose owners might be aware only of the game they were playing.

The paragraph above assumed that a government would use a gaming network covertly, meaning an Intelligence organization or a security organization would hack the gamers network. It is worth noting that the U.S. Army has its own gaming network: http://www.americasarmy.com/ Although this network is advertised as a recruiting and public relations tool, it remains a gaming network controlled by the American military. NATO advanced warfare training teaches "effects based warfare". In effects based warfare, if you can disable an enemy without firing a shot, that is considered a desirable way of achieving your objective.

For example if you turn off the water and power at an Air Force base, it is unlikely that that base will be able to launch many aircraft. In this example a cyber-attack on a water control system and electrical grid would probably be considered legitimate military targets. A gaming network could provide the means to conduct such an attack.

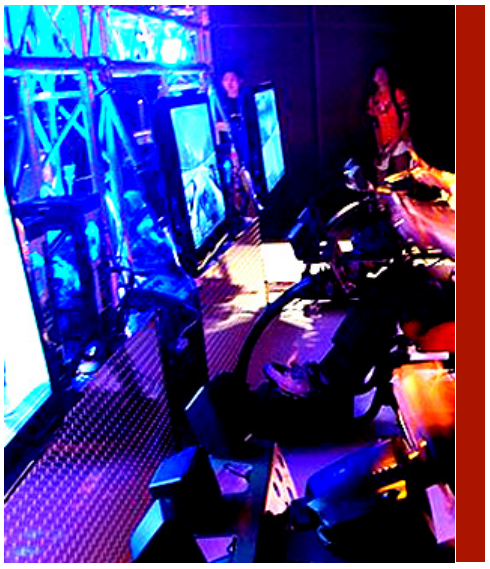
Summary

Gaming networks, in particular modern high-end games, have a number of characteristics that are potentially useful to criminals, and terrorist organizations. The range of options available to gamers and the nature of the fantasies make those networks an opportune place to conduct business without attracting attention. Couriers from disparate parts of the world can meet and exchange data while appearing to be just another element of the game. The ability to create and run simulations means operational plans can be tested with minimal fear of compromise.

In a worst case scenario a major gaming network could execute a Distributed Denial of Service (DDoS) Attack using tens of thousands of computers, with a legitimate network as cover.

Conclusion

Having security and Intelligence personnel monitor gaming networks may seem paranoid. When we examine the nature of gaming networks, the same characteristics that make for high quality gaming can be misused for radically different purposes. Globally accessible networks, catering to a wide variety of computing platforms, featuring internal communications and providing access to high performance computers offer the creative criminal a world of opportunities. We need to ensure our networks don't have games installed on them and be alert to the potential threat from gaming networks.



C/DIG Focus Reports provide detailed Intelligence examination and review of specific computer security and / or cyber-warfare incidents, events and analysis. The focus is international and transnational cyber-security events, specifically national security, critical infrastructure, defence and related events, caused by nations and/or effecting transnational relationships.

For a dedicated briefing by the CSCSS Defense Intelligence Group on the issues and challenges regarding National entities and cyber-warfare please contact us.

Contact Information
For more information on the Defence Intelligence Group or to find out how we can help you please contact us.

- Washington D.C + 571.451.0312
- London, United Kingdom +44 2035141784
- North America +877.436.6746
- Middle East +855.237.8767
- Australia +61 2 8003 7553

Email: defintel@cscss.org
www.cscss.org/defence_intelligence.php

C/DIG CSCSS / DEFENCE INTELLIGENCE GROUP

CSCSS / Defence Intelligence Group through its CSCSS subsidiaries is aligned with civilian and nation computer security & intelligence agencies. C/DIG provides defence intelligence support to mission-essential requirements at every stage of programming, product and business lifecycle. We deliver mission and technical expertise, delivery of intelligence products, and a commitment to client objectives and results at the strategic, operational and tactical levels.

The Defence Intelligence Group works in real-time to report, analyze, and forecast cyber-warfare incidents, events and trends. We provide credible, reliable, sustained intelligence services, defence intelligence expertise; skills, contingency planning, and solutions that help clients address and achieve their missions, goals and objectives securely.

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE

The **Centre for Strategic Cyberspace + Security Science** is a multilateral, international, not-for-profit organization that conducts independent cyber-research, defence intelligence, cyber security and science while addressing the threats, trends and opportunities shaping international security policies and national cyberspace security initiatives.

CSCSS, as a strategic leader in cyberspace, works jointly with key partners to address, develop and define cyber capabilities, cyber defence force capabilities, information dominance, and current operations. We deliver practical recommendations and innovative solutions and strategies to advance a secure cyberspace domain.