https://doi.org/10.48009/2_iis_2006_52-58

CYBEREXTORTION: AN OVERVIEW OF DISTRIBUTED DENIAL OF SERVICE ATTACKS AGAINST ONLINE GAMING COMPANIES

Richard A. Paulson, St. Cloud State University, rapaulson@stcloudstate.edu
James E. Weber, St. Cloud State University, jweber@stcloudstate.edu

ABSTRACT

There has been tremendous expansion in online, or internet, gambling over the past decade. Various growing pains associated with such growth have impacted the numerous online gaming companies. One issue of serious concern relates to attempts to shut down gambling websites through distributed denial of service (DDoS) attacks. These electronic extortion activities present potentially critical problems for internet gaming operations. The downtime and subsequent possible lost revenue created by these kinds of attacks can be staggering. This paper discusses the online gaming industry, describes DDoS attacks (especially as they relate to electronic gaming), and examines the impact of (and possible solutions to) those attacks against online gaming websites.

Keywords: Electronic Commerce, Distributed Denial of Service, Online Gaming

ONLINE GAMING

Prior to the middle 1990s the concept of electronic gambling was almost nonexistent. In 1996 there were roughly 20 online gaming websites [3]. Over the past decade the demand for electronic gambling has grown tremendously. Not surprisingly the supply of online gaming companies has grown as well. In 2003 the United States General Accounting Office estimated that there were at least 1,800 online gaming websites worldwide, accounting for a total of $5 billion in revenue [11]. With the recent explosion in the popularity of poker (both live and online) these numbers from a few years ago certainly underestimate the current availability of potential online gambling venues (and their corresponding revenues). Christiansen Capital Advisors, a well known gaming industry research firm, estimates 2006 internet gaming revenues in excess of $15 billion from approximately 2100 websites [6]. Roughly half of that revenue (about $7.2 billion) is expected to come from U.S. citizens [6]. The majority of these online gaming companies are located in the Caribbean. The political and economic climate in many of the Caribbean and Central American countries makes those areas logical choices for such gambling headquarters. For example, the regulatory and tax structure in Costa Rica has made that country a haven for online gaming investment [8].

Online betting websites offer a variety of wagering options, much like their physical, brick and mortar casino competitors. After setting up a wagering account a person can bet electronically on casino games (blackjack, roulette, craps, etc.) or sporting events or play poker online. Offshore gaming companies also offer some types of wagering that are not permitted in the casinos of Nevada. For instance, wagering on non-sporting events such as the academy awards or political elections is permissible through online websites, even though such wagers would not be offered in Nevada. The ease and accessibility of online wagering makes it a very enticing gaming option. All a person needs is an internet connection (or a telephone) and they are ready to gamble. It is estimated that there are currently 10-15 million U. S. citizens who gamble online. The evidence suggests that this number will continue to grow with increased opportunities and increased social acceptance [6].

DISTRIBUTED DENIAL OF SERVICE ATTACKS

Security issues are of highest priority in the design of IT systems. There are numerous areas for security applications. These range from internet communications to e-commerce to constrained wireless devices [13]. A secure system needs to provide confidentiality, integrity, availability, and authenticity [1]. Firewalls, routers, intrusion detection systems, and various vulnerability assessment tools exist to combat the different security problems that effect internet transactions.

In denial of service (DoS) attacks, hackers inundate a network or web server with thousands of requests from false communications in order to crash the network [10]. The network would receive so many queries that it would become overloaded and would be unable to handle legitimate service requests. A distributed denial of service (DDoS) attack originates from a group of computers rather from just one host machine [10]. The intent of the attacker is to deny access to the computer system in question by consuming all available resources (such as disk space or CPU time) or disrupting traffic monitoring, bandwidth capability, or physical network components. The attacks typically originate from large clusters of computers that have been commandeered by the attackers. These zombie systems are then controlled from a centralized point allowing a huge force of bandwidth to be concentrated in a single place. These zombie armies, or botnets, can utilize thousands of machines [7]. In essence the hackers try to "flood" the system with fake packets, thus preventing the use of the system for legitimate business purposes. The costs associated with these types of attacks can be economically crippling.

DDoS attacks have been occurring on the internet since 1999. In the first few years of the 21st century there has been a tremendous upward trend in the number of DDoS attacks [7]. These types of intrusions have become a very popular technique for hackers who are intent on seriously impeding the flow of information to particular websites. In launching a DDoS attack a hacker typically utilizes multiple machines that they have previously compromised. The attacker installs software on these zombie systems in order to remotely control a specific bandwidth assault from the botnet against their chosen target. Given the nature of these attacks they are very difficult to stop or prevent. One attribute of this type of system overload is the difficulty in separating the illegitimate DDoS attack generated information from legitimate business information. The end result is a system that is shut down and is unusable for its intended purpose.

TARGETING ONLINE GAMING WEBSITES

Online gaming companies are logical targets for electronic extortion attacks. While global crime has been addressed through policies such as the Organization for Economic Cooperation and Development's 1999 guidelines covering legal and regulatory international governance issues or the United Nations Convention against Transnational Organized Crime, which was enacted in 2003 to require countries to establish criminal offences for various global infractions [9], laws regulating cyber-transactions have been slow to appear. Because cyberspace is not subject to the laws of any one country or jurisdiction, universal rules are not standardized or uniformly enforceable [16]. Given the countries in which many of the companies are located, there tends to be a lack of infrastructure protections in place to combat these kinds of attacks. In many cases the regulatory environments are weak or insufficient and their technological resources are sometimes inadequate or insufficiently funded. The ability (and desire) for adequate law enforcement is often lacking. Given the ever evolving nature of the online gaming business, the relevant laws may not even be on the books. Since online betting is illegal within the United States, the country with the largest array of technological expertise and resources typically doesn't get involved in these kinds of issues and disputes. The online gambling business is potentially very lucrative (as evidenced by the above quoted revenue figures), making it a very inviting target for thieves and hustlers.

The electronic extortion attempts follow the general formula of the historic physical attempts to extort resources from business owners. The old style requests for protection money usually emphasized the possible consequences if the money wasn't paid. Those consequences varied from the potential for arson to the possibility of broken kneecaps. The business owners dilemma usually involved balancing the cost of making the extortion payments versus the cost associated with having their business (or their life) shut down. The electronic extortion threats typically follow the same pattern, without the threat of physical violence. The website operator is warned that if they don't make a particular payment within a limited amount of time then they will suffer a denial of service attack and effectively be shut down.

The following is a sample extortion letter, reprinted from a white paper distributed by Prolexic Technologies, a company that specializes in combating DDoS attacks on businesses [7]:

> Your site is under attack and will be for this entire weekend. You can increase your pipe all you want and it won't help. You have a flaw in your network that allows this to take place. You have two choices. You can ignore this email and try to keep your site up, which will cost you tens of thousands of dollars in lost (business) and customers, or you can send us $40k to make sure that your site experiences no problems.
>
> If you send the $40k your site will be protected not just this weekend, but for the next 12 months. This will let you enjoy business with no worry. If you choose not to pay for our help, then you will probably not be in business much longer, as you will be under attack each weekend for the next 20 weeks, or until you close your doors.

> You can always choose to wait, see what happens, and then contact us for our help when you realize you can't do it yourself, however, then it will cost you more and your site will still be down.
>
> The choice is yours as we await your response.
>
> P. S. The sites that were attacked and paid last weekend are happy that they paid and are protected (pg. 37).

This creates quite a financial and psychological dilemma for the website owner. Since gambling websites are involved with almost continuous financial transactions the potential consequences can be very significant. Do they pay now and hope that the problem disappears? Do they risk suffering the enormous opportunity costs associated with being shut down? What are the long term ramifications of their decision? These extortion letters tend to be timed to coincide with especially busy business periods. For instance, it would be extremely costly for a sports betting website to be closed on Super Bowl weekend. This adds to the immediacy of the problem and the difficulty of arriving at an optimal solution. The website owner has incentives (albeit negative ones) associated with each option. They must try to minimize the potential damage without really knowing all of the possible economic, legal, and social outcomes.

Numerous DDoS attack threats occurred against online gaming companies during the time period from 2000-2004. In 2003 BoDog Sportsbook and Casino in Costa Rica paid more than $20,000 to hackers who immobilized their website [14]. During that same time period World Wide Telesports in Antigua paid $30,000 to hackers after their website was temporarily shut down [14]. Their CEO Simon Noble estimated that the shut down impacted thousands of customers and cost the company $5 million in potential wagering action. Those are just two of the known examples where extortion money was requested and paid. In 2004 DK Matai, executive chairman of the security company MI2G, estimated that computer gangsters (mostly operating out of Eastern Europe) had collected protection money from between 10% and 15% of the companies that they had threatened [14]. Given the multitude of betting websites, the total number of cyberextortion threats has to be substantial. Many websites choose not to publicize such threats. The potential negative customer reaction and perceived (and real) vulnerability lead some operators to opt for silence. On a personal note, one of the authors of this paper encountered a mysteriously unavailable website when conducting research on wagering on the 2004 Super Bowl. The reason for the "temporary" blockage of this particular site (Royal Sports) was never explained. However, the timing (Super Bowl day) leads one to suspect foul play. The author has been unable to determine exactly how this specific issue was resolved.

WE FOUGHT THE OUTLAW AND THE OUTLAW LOST

Don Best Sports is a sports wagering information company. They monitor betting lines and odds from land-based and online casinos worldwide and transmit that information on a real time basis to their clients. Thus their customers are able to monitor the establishment and movement of betting odds from bookmakers around the world. This up to the minute betting information has become a necessary tool for both bookmakers who want to optimize their behavior and for gamblers who desire the most current betting information before determining their selections. Don Best is the clear leader in providing timely betting odds information [12].

In July of 2002 Don Best received an email indicating that they were currently under an electronic attack [4, 15]. The email asked for an extortion payment of $200,000 to stop the attack. The company ignored the extortion demand. Since the $200,000 payment seemed very large, the company didn't necessarily figure that the cost of ignoring the extortion demand exceeded the benefit of stalling the extortionists while trying to gain some time to analyze the situation. However, there wasn't a great deal of time to lose. Don Best's customers were irate that the site had been shut down and they weren't receiving the information that they needed (and had paid for) to run their bookmaking businesses. A computer security consultant named Barrett Lyon was summoned. Lyon helped Don Best's engineers set up a system of powerful new servers and the attackers gave up. Don Best had some temporarily unhappy customers, but overall the defense mechanism was a success. The attackers had made a few blunders. They had attacked during a slow gambling season (not football season) and had asked for too much money. Thus, the problem was temporarily "solved."

In 2003 these types of attacks resurfaced, only now they were aimed at the online gambling companies themselves. Many offshore bookmakers received extortion emails and many of the firms paid the demands, which were typically anywhere from $20,000 to $50,000 [14]. In November of 2003, Mickey Richardson, the general manager for the Costa Rican based gambling company BetCris, received an extortion email [4, 15]. He was told that their site was under attack and he had two choices. BetCris could pay a "ransom" of $40,000 to be "protected" for the next 12 months or they would be under attack effectively until they "closed their doors." Since this notification came during the football season and right before what was sure to be a busy Thanksgiving weekend of wagering action, Richardson knew that if his site was shut down they would lose tens of thousands of dollars in lost bets as their customers shifted their business to other wagering firms. Conversely, he wasn't keen on giving in to the extortion's demands. The implications were ominous regardless of his decision.

Richardson decided not to pay the money. Instead he contacted Barrett Lyon. To solve the problems associated with the flood of useless information that was disabling the BetCris system, Lyon needed to add capacity to the network (similar to the solution to the Don Best Sports problem). Unfortunately, the amount of capacity that needed to be added wasn't even feasible given the constraints of the host country. Costa Rica wasn't wired for that sort of system. There wasn't enough capacity in the entire country. So Lyon built his own network in the United States and used it to divert the attacks from BetCris. This deceived the extortionists who thought that they were attacking a relatively impotent Costa Rican system when in fact they were up against a more formidable U. S.-based operation. As Lyon worked to fend off the attacks, the attackers became more irritated and raised their extortion demands. The confrontation between the attackers and Lyon continued in a give and take manner for weeks. Lyon would add capacity and change the system and the attackers would try an alternative form of DDoS attack in an attempt to keep the website shut down.

After three weeks of this electronic competition, the attackers gave up. Even though the attackers had "lost" the game they had the satisfaction of knowing that they had inflicted significant harm on BetCris. Realistically, the company lost much more in potential revenue due to their down time than it would have cost them to pay the original $40,000 [4]. However, there certainly were various economic and psychic benefits to the cat finally catching the mouse in this situation. Barrett Lyon's efforts tremendously enhanced the body of knowledge and expertise needed to combat these DDoS attacks and other online gaming (and non gaming) companies saw the potential long term benefits of not giving in to these extortion attempts. A solid foundation was formed to fend off these attacks. Not surprisingly, Barrett Lyon was much in demand and established himself as the person to contact in these situations. As of 2005 the severity and quantity of DDoS attacks had diminished [5]. The threat still existed, but the hackers had to work on new techniques to circumvent the electronic defenses that had been implemented.

THE FUTURE OF ONLINE EXTORTION

Initially the online extortionists celebrated a good deal of success. The costs associated with fighting the hackers tended to exceed the cost of the extortion payment. So, many online companies backed down and paid the ransom. After the BetCris situation transpired online gaming firms understood that they had other options. They also realized that the long term ramifications were such that fighting the extortions might very well be the optimal course of action. The lessons learned from the past few years in the gaming industry have relevance to many other types of businesses. The attacks against these gaming websites appear to have served as a training ground for online extortionists. They seem to have learned from the experience, acquired more sophisticated technological tools, and expanded their operations into non gaming venues. Where there is a great deal of money to be made, there is probably going to be someone trying to get their hands on some of that money. Firms that stand to lose money by being offline are potential extortion targets. This could include online payment services, foreign currency exchanges, or financial services companies [4]. These types of businesses potentially face the tradeoff of paying protection money versus spending the time and resources to do battle with the attackers.

It is safe to assume that online attackers will continue to search for new ideas and ways to extort resources from web based companies. Several interesting twists on the standard DDoS attacks have surfaced recently. In one instance, a hacker pled guilty to quietly acquiring control of several hundred thousand computers, then renting the "zombie network" out to spammers and those wanting to attack Web sites [2]. Clearly the availability of rental networks to perform DDoS attacks heightens the risk of such attacks. In another case, an extortionist contacted a United Kingdom website named Blue Square and threatened to send out child pornography emails in the companies name unless their ransom demands were met [4]. Blue Square did not pay the blackmailers and the substance of the threats appears to never have materialized. However, these examples serve to illustrate new and different approaches to online extortion. There are sure to be many others. Hopefully, the recent experiences in the online gaming industry will provide a template for combating future electronic extortion attempts.

REFERENCES

1. Al-Taani, A. & Kofahi, N. (2005). Web Operating Systems and Computing on the Web. *Information Technology Journal*, *4*(4), 360-365.
2. Associated Press, (2006). 20-year-old hacker rented out attack network. Retrieved January 24, 2006 from http://www.msnbc.msn.com/id/10993580/from/ET/.
3. Barker, T. & Britz M. (2000). *Jokers Wild: Legalized Gambling in the Twenty-first Century*. Westport, CN: Praeger.
4. Berinato, S. (2005). *How a Bookmaker and a Whiz Kid Took on an Extortionist – and Won*. CSO magazine. Retrieved May 4, 2005 from http://www.majorwager.com/fusetalk/messageview.cfm?catid=22&threadid=129785.
5. Child Porn Threat to Betting Site. (2004). *BBC News*. Retrieved October 24, 2005 from http://news.bbc.co.uk/1/hi/business/3957757.stm
6. Christiansen Capital Advisors, LLC. (2006). Retrieved January 9, 2006 from http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling.
7. Distributed Denial of Service Attacks. (2004). White paper: *Prolexic Technologies*, Inc. Retrieved December 1, 2005 from http://newsite.prolexic.com/downloads/whitepapers/Prolexic_WhitePaper-DDoS-Q4-2004.pdf.
8. How Online Casinos are Doing Business in Costa Rica. (2006). Retrieved January 31, 2006 from http://www.costarica.con.Home/Business/On-Line_Gambling_Business.
9. Karofi, U. & Mwanza, J. (2006). Gobalization and Crime. *Bangladesh e-Journal of Sociology*, *3*(1), 15-16.
10. Laudon, K. & Laudon, J. (2005). *Essentials of Management Information Systems: Managing the Digital Form*. Upper Saddle River, NJ: Pearson/Prentice Hall.
11. Online Gambling. (2003). *CBC News*. Retrieved January 9, 2006 from http://www.cbc.ca/news/background/gambling/onlinegambling.html.
12. Premium Odds. (2006). Retrieved January 31 from http://www.donbest.com/product-premium.htm.
13. Rabah, K. (2005). Theory and Implementation of Data Encryption Standard: A Review. *Information Technology Journal*, *4*(4), 307-325.
14. Swartz, J. (2004). Online Betting Sites Fight Cyberextortion. *USA Today*. Retrieved March 9, 2004 from http://usatoday.printthis.clickability.com/pt/cpt?action=cpt&title=USATODAY.com+-+Onl.
15. The Zombie Hunters – On the Trail of Cyberextortionists. (2005). *The Prescription*. Retrieved October 18, 2005 from http://therx.com/blog_the-zombie-hunters---on-the-trail-of-cyberextortionists-.php.
16. Toscano, P. (2000). Taming the Cyber-Frontier: Security is Not Enough! *Crosstalk: The Journal of Defense Software Engineering*. Nov.