Volume 3, Issue 2 • 2011 • Article 5

Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention

Jonathan Basamanowicz, ***Simon Fraser University***
Martin Bouchard, ***Simon Fraser University***

Basamanowicz, Jonathan and Bouchard, Martin (2011) "Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention," *Policy & Internet*: Vol. 3: Iss. 2, Article 5.
Available at: http://www.psocommons.org/policyandinternet/vol3/iss2/art5
DOI: 10.2202/1944-2866.1125

Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention

Jonathan Basamanowicz, *Simon Fraser University*
Martin Bouchard, *Simon Fraser University*

Abstract

US federal law enforcement operations occurring between 2001 and 2005 attempted to disrupt the online piracy scene, targeting copyright piracy rings known as 'warez groups'. Previous work on warez groups has demonstrated a paradoxical situation where attempts to curtail warez group activities through policing and advancements in DRM only further encourage such groups to crack and distribute content. This study collected data on 93 convictions from these policing operations to construct a crime script of these groups' motivations and modus operandi in the release process. The results confirm previous findings that attempts to disrupt the activities of warez groups are counterproductive. To avoid the paradox, this study suggests that industry account for the motivations and modus operandi of these groups by creating DRM technologies which allow un-cracked content to seep through the testing step of the script, thereby placing a group's ability to obtain prestige at risk. Law enforcement should focus on apprehending crackers, as they are the most significant step in the release process.

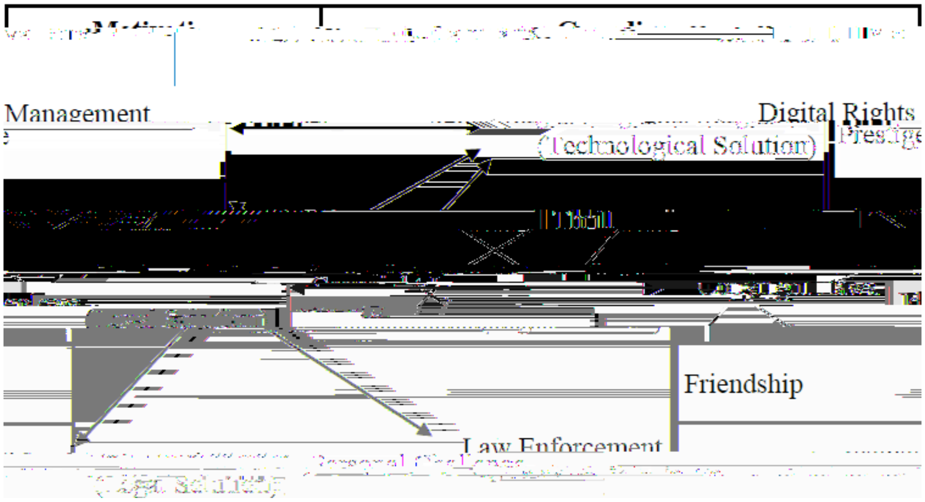
KEYWORDS: warez groups, release groups, digital piracy, situational crime prevention, crime scripts, file sharing, cracking

Author Notes: Partial funding for this project was provided by the International Cybercrime Research Centre, Simon Fraser University. The authors would like to thank the anonymous reviewers, as well as Eric Beauregard for the useful comments made on an earlier version of this paper.

Introduction

Some scholars have predicted that by 2010 copyright law would be impossible to enforce online (Pouwelse et al. 2008, 711). It has been estimated that copyright and Cruise 2006, 173).[3] Scholars have suggested methods of protecting industry from insider leaks of IP (Willison and Siponen 2009; Willison 2006; Willison and

Figure 1. Individual Motivations, Content Guardians, and the Potential for Counterproductive Prevention in the Warez Scene.



As top release groups are responsible for the majority of releases distributed online (Goode 2010; Urbas 2006; CCIPS), and as these groups can be further motivated by counterproductive obstacles imposed on them, it is in the interests of industry and law enforcers to develop prevention strategies which take these motivations into account. This article examines the motivations and *modus operandi* of release groups through a situation crime prevention framework. Employing a *crime script* (Cornish 1994) of the release process, constructed through a U.S. Department of Justice court case dataset of 93 convicted digital copyright infringers, we identify policy initiatives relevant for attempts to disrupt release group activities.

Situational Crime Prevention and Crime Scripts

Situational Crime Prevention (SCP) is a criminological perspective that traces its theoretical roots to Routine Activities Theory (Cohen and Felson 1979) and Environmental Criminology (Brantingham and Brantingham 1981; Jeffery 1977). Traditionally, SCP research has aimed to seek methods of reducing opportunities for offenders to succeed in their criminal ventures through amendments in environmental and contextual factors affecting the commission of a criminal event (Cohen 1981). For example, in a recent study on scrap metal theft from construction sites, Kooi (2010) identified 18 techniques that could be applied to reduce the commission of scrap metal theft, such as placing identification on scrap metal to discourage offenders from selecting it. By focusing on situational factors that facilitate a criminal event, SCP researchers aim to discover methods of reducing the opportunities for an offender to commit a crime (Clarke 1980; 1995). These include changing situational factors to increase the effort, increase the risk, reduce the reward, and/or reduce the provocation for an offender to offend, and/or remove excuses that offenders may use to justify their behaviors (Bullock, Clarke, and Tilley 2010; Clarke 1995).

One method for study-24a(]TJ15 -1.5 0 3r re)]TJ11.325 0 T45.0006 via Tw3(inpes ps)-5.4(7.889( )]

court documents. The initial sample was of

the second highest imprisonment rate (*n*=7; 64 percent) and served the longest mean terms of imprisonment (22 months), while none of the five crackers were sentenced to prison.

Secondary Data

By relying on court data, we are limited to the perspectives offered by defendants under threat of punishment (i.e., motivations and/or explanations of behavior that mitigate culpability), and by the courts' aiming to increase culpability (i.e., explanations of behavior which may overestimate a defendant's responsibility in the conspiracy). Additionally, although many people engage in this behavior, only a few are apprehended, and fewer are prosecuted; thus, the court data reveal only a slim minority of the larger distribution of warez scene piracy. This bias was partially reduced through the use of secondary sources. These included: DOJ press releases, websites containing interviews with warez group members,[7] warez group nfo files and scene release charts,[8] and the research literature.[9]

The Crime Script Analysis

The main aim of this article is to recreate the warez release process through a crime script analysis. Figure 2 illustrates the process as five distinct steps: supply, requirements, and visibility of each step to law enforcement. The steps are expanded upon below.

Figure 2. Crime Script of the Warez Release Process

		Administrative Function *Decision Making* (Leader, Senior Members, and Council)			
Step	**1) Supply** Č	**2) Crack** (Č	**3) Test** ċ)	**4) Package** Č	**5) Distribute** Č
Aim	*Obtain commercial content by technical skill, position, or legal purchase*	*Strip the copyright protection features*	*Ensure content is fully functional with copyright protections removed*	*Package content to scene standards*	*Distribute content sk0 Tw-.0s1 rg293.34 420.72 5103.98 re316.1.8*

Administrative Functions

Individuals who completed this function filled the role(s) of Leader(s), Senior Member(s), and/or Council Member(s). The aim was to act as the decision-making body for the group. Although not a formal "step" in the release process, administrators were heavily involved with the group's activities, sometimes performing many different roles themselves. For example, a leader in the group MaGe was cited as also supplying content and testing content after it had been cracked (US DOJ 2007). Another individual, who acted as a senior member in Fairlight, performed all the steps of a release (supply, crack, test, package, and distribute) entirely by himself, by taking advantage of his position as an editor of a video game review magazine (*USA v. Klienberg*, Case Number 3:05CR49. D. CT, 2007).

This entrenchment in the scene is exemplified by a former leader of MaGe in a letter to the judge describing his early involvement in the scene, stating:

> My involvement in the warez scene had become such a routine in my life that it completely went out of control […] I enrolled in classes, but seldom

to at least eight FTP servers controlled by the group as a reward for his contributions to the group (*USA v. Lerman*, Case Number 3:05CR50. D. CT, 2007); in contrast, Christopher Eaves, a supplier for the group aPC, was threatened with banishment from the group because of his lack of contribution (*USA v. Eaves*, Case Number 1:07CR00140, E.D. VA, 2007). Opportunities for acquisition of content can be categorized as acquisition through technical skill, acquisition through social position, and legal purchase.

Acquisition through skill can be conducted using different techniques. Craig et al. (2005, 42–54) list these as: snooping of company FTP servers; purchasing content through credit card fraud; hacking into company computer systems; and social engineering (e.g., creating fake companies or aliases to deceive victims into supplying content). Many of these methods allow the group to receive the content prior to its commercial release date. Given these methods are learned, individuals with these skills may be more difficult to replace than other suppliers. These methods may rely on illegal means, thereby increasing the visibility of their actions to law enforcement.

Acquisition through position does not specifically require skill, but depends instead on the individual’s employment or social contacts. For example, the FBI has claimed that groups such as Rabid Neurosis (RNS), an audio release group, acquire their content from music industry employees, CD manufacturing plants, and/or DJs or stores that receive copies in advance of commercial release dates (US DOJ 2009). This is the case for a number of individuals arrested during the DOJ policing operations examined here: Colin Roy Jacobson and Paul Sherman, for example, were both movie critics who received (and later sold online to warez groups) advance copies of review DVDs (*USA v. Jacobson*, Case Number 5:06CR00477. N.D. CA, 2008; *USA v. Sherman*, Case Number 5:06CR00331. N.D. CA, 2007). Sherman sold an estimated 117 films to warez groups in advance of the commercial DVD release date. Acquiring content through position is less visible to law enforcement than employing the skillful means noted above.

Legal purchase results in the slowest release of the three methods of obtaining content, as groups employing this method must wait for the product to be commercially released. This method was employed by a number of individuals in the court data, as many lacked either the social capital or skill to acquire content otherwise. The benefit of this method is that it can be performed by anyone and is invisible to law enforcement.

Generally, the *supply* step in the crime script is a point of visible criminal behavior and a point in the chain where disruption is possible by industry. Once content has been transmitted by the supplier to the cracker, it is invisible to outsiders until the final step in the crime script.

Crack

2005). One of the individuals in our dataset, Bryan T. Black, a cracker for the

The packaging stage does not ostensibly require any particular skill or privileged social position—one must merely know scene standards and know how to adequately convert files into their required formats and file sizes.

Distribute

With the content packaged into an appropriate format, the distribution step begins with a process called "pre'ing," in which content is uploaded by couriers to a hidden section of the group's/affiliates' sites. Once this is done, site administrators are instructed through an IRC bot command to make the content accessible to individuals with access to these sites (Craig et al. 2005). After a group has successfully released content, it can be distributed globally within minutes to a series of very secure FTP sites, called top sites. From here, couriers trade the content between other sites (Howe 2005), and within hours it can trickle down to more accessible sites and eventually for p2p users to access (US DOJ 2005b).

It has been suggested that couriers outnumber all other roles in the scene combined (Craig et al. 2005, 137). However, in our dataset we found few of them (only five). Couriers may operate as part of the release group, as part of a courier group, or as independent traders (Lee 2002). Generally, couriers are rewarded with a credit system from each site, called *ratio access* (See Operation Copycat Indictment/Information such as *USA v. Fish et al.*, Case Number 5:05CR00445. N.D. CA, 2008), that typically allots three download credits per one upload credit. Thus, if a Courier uploads 100mbs of data, he/she will be rewarded with 300mbs of download credits. Couriers are motivated through this reward scheme, as well as through ranking systems/magazines that rate couriers on their upload amounts (Lee 2002). There were five individuals in our dataset with the primary role of courier. Of these, limited data on the defendants' activities are only available for two cases, which describe them as moving content from one site/computer to another (*USA v. Gomez*, Case Number 1:07CR00125. E.D.VA, 2007; *USA v. Dickman*, Case Number 5:06CR00054, N.D. CA, 2006).

The distribution step is one of partial visibility to law enforcement, and the three operations in our dataset (Buccaneer, Fastlink, and Site Down) focused on this step to gain entry. For example, Operation Copycat, a sub-investigation of Site Down, was conducted by setting up a dummy site and then employing a confidential informant to convince warez groups to use it (See *USA v. Fish et al.*, Case Number 5:05CR00445. N.D. CA, 2008), demonstrating the ability for law enforcement to surveil and apprehend individuals in these networks.

Discussion

Prevention schemes must disrupt activities, through increased risk and effort or decreased reward (Cohen 1981), without further encouraging behavior through counterproductive prevention (Wortley 2001; 2003; Grabosky 1996). Thus, the question at issue is how to disrupt release groups when the methods used to prevent their behavior may serve only to further encourage it. Examining cases of individuals involved in release groups, motivations suggested by the existing literature are indeed present in this dataset, for example some individuals' perceived rewards being gained through circumventing DRM and others from the prestige gained from releasing content.

Digital content may be protected by two means: by industry, through DRM, and by law enforcement, through policing (Holsapple et al. 2008). Each of these may disrupt release group activities by increasing effort, increasing risk, reducing rewards, reducing provocations, or removing the excuses that offenders may use to justify their behaviors (Bullock, Clarke, and Tilley 2010; Clarke 1995; Cornish and Clarke 2003). Situational crime prevention is often concerned with modifying the environment, in order to control contextual factors that facilitate the commission of a criminal event. However, cybercrime is committed in a digital environment where authorities have little or no control. Thus, the traditional crime control methods suggested by SCP, such as screening exits, denying benefits, and/or discouraging imitation (Cornish and Clarke 2003) are difficult, if not impossible, to implement in the warez scene. Put simply, industry and law enforcement have no home field advantage, and such environmental modifications are impractical.

As such, when applying these SCP concepts, some are more useful than others. First, the difficulty in employing a prevention strategy targeting justifications used by individuals in war perceived by many in the warez scene to be not just a means, but an end in itself. For those seeking prestige, however, one suggestion might be to disrupt bragging channels or to disseminate disinformation. However, it is unlikely that industry or law enforcement could gain access to the private communication channels that these groups employ—and if so, more suitable disruptive measure could be employed, such as gathering information on individuals within the group, than interfering with their bragging opportunities.

Thus, the two options which are left, from a SCP perspective, are to (a) increase the effort, or to (b) increase the risk involved with releasing content. With respect to increasing effort, this is typically an issue for industry and is difficult to prescribe—and as the challenge of cracking difficult DRM technologies may be a motivating factor for these groups, adjustments in DRM to increase the effort necessary to crack them may lead to counterproductive prevention. Additionally, some consumer

ranked lower if they distribute ill-cracked content. End users will be frustrated and discouraged by wasting their time and download credits on bad or unusable content. The internal quality control methods typically employed by the scene would act against the release group's interests by making the process of obtaining prestige far more risky. Thus, copyright protection features with a latent disruptive characteristic may make it possible to make the risk of releasing a type of content too high in the eyes of the warez scene. In other words, the potential loss of prestige and peer-approval within the scene may be so high that groups will avoid releasing software with this particular copyright protection.

To give an example of this how this type of protection may operate, consider the following. Under The Game Scene Charts rules, the method of scoring releases is listed, detailing how games that require greater skill to crack are given more points. For example, a game with complex copy protections is worth 8 points; whereas a game with no copy protection but with an installation key is worth 5.5 points (TGSC Editor 2010). A game protected by a simpler form of DRM would be less desirable as a release, as it would yield fewer points for the group. Additionally, if this DRM were to enact under a latent condition, after the content has already been in use, then the content might already be distributed, resulting in damage to the group's reputation. As the content is valued less on the point scale, but carries a greater risk of failure, it may be a less desirable target and future content by that game developer may follow suit.

Significantly, these features need not be more difficult or more obtrusive than current DRM technologies. In fact, they may even be more innocuous; they only need to be latent and activate, possibly randomly, at a period of time much later in the course of using the content. Of course, as with any copyright protection, the possibility for counterproductive prevention is present; however, by accounting for, and specifically targeting, motivations that drive warez scene piracy, the objective is *not* to increase effort, but to increase risk. As an added bonus, copyright protection features of this sort may foster an environment of uncertainty by allowing ill-cracked content to be shared amongst end-users.

Law Enforcement

Regarding efforts which may aid law enforcement in policing release group piracy, law enforcement may be able to increase the effort required for groups to release content. The crime script highlights two issues that aid in this endeavor: steps in the script which are more vulnerable to disruption, and steps which are visible to law enforcement. As a few groups are responsible for most of the illicit content available online (Goode 2010; Urbas 2006; CCIPS), targeting the most prolific groups would likely have the greatest utility. Operations Buccaneer, Fastlink, and Site Down seem to have done this by targeting the likes of DoD,

required by groups to release content. The cracking step is the most significant step, and as such, individuals who fulfill this role should be a higher priority for law enforcement than others within the group. Since these individuals operate clandestinely, law enforcement may surveil visible targets, such as those operating in the supply or distribution steps, to locate and apprehend crackers. This strategy may not require an increase in policing efforts—the same investigation strategy may be employed, just focusing on different targets—nor would it require an increase in the severity of punishment, as it has been suggested that many apprehended warez traders have a low probability of recidivism (DuBose 2006). Thereby, this strategy is less likely to further strengthen the ideology held by some members in these groups.

Conclusion

Digital piracy conducted via warez groups presents a challenging puzzle, as improvements in DRM (Goode and Cruise 2006) or increased policing may further encourage warez scene piracy (Goldman 2003; 2005) or result in an need to be tested and implemented to disrupt this form of piracy. The situational crime prevention framework presented here shows that although it may be impossible to completely stop release group piracy, if the appropriate preventative and enforcement steps are introduced, it may be possible to disrupt and/or slow down the release process. As top release groups are responsible for the majority of content released (Goode 2010; CCIPS), it is in industry and law enforcements' interest to target these groups in their disruption efforts. Future research should go further inside these groups and examine the social networks of individuals involved in release group piracy.[19] An understanding of the interplay between both the micro (individuals, groups) and the macro (the size and structure of the industry) elements should also prove useful to future research and policy developments on digital piracy.

References

BanDiDo [Hew Raymond Griffiths]. "Interview with BandDiDo/DoD and RiSC [Interview by BiXen]." http://www.defacto2.net/legacy/apollo-x/bandido.htm (accessed November 1, 2010).

Beauregard, E., J. Proulx, K. Rossmo, B. Leclerc, and J. Allaire. 2007. "Script Analysis of the Hunting Process of Serial Sex Offenders." *Criminal Justice and Behavior* 34 (8) 1069-1084. doi: 10.1177/0093854807300851.

Clarke, R.V. 1980. ""Situational" Crime Prevention: Theory and Practice." *British Journal of Criminology* 20 (2): 136-147. http://bjc.oxfordjournals.org.proxy.lib.sfu.ca/content/20/2.toc.

Clarke, R.V. 1995. "Situational Crime Prevention." *Crime and Justice* 19: 91-150.

Cohen, L. 1981. "Modeling Crime Trends: A Criminal Opportunity Perspective." *Journal of Research in Crime and Delinquency* 18 (1): 138-164. doi: 10.1177/002242788101800109.

Cohen, L.E., and M. Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44 (4): 588-608.

Cornish, D.B. 1994. "The Procedural Analysis of Offending and its Relevance for Situational Prevention." In *Crime Prevention Studies*, Vol. 3, ed. R.V. Clarke. Monsey, NY: Criminal Justice Press, 151-196.

Cornish, D.B., and R.V. Clarke. 2003. "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational." In *Theory for Practice in Situational Crime Prevention*, eds. M.J. Smith, and D.B. Cornish (Crime Prevention Studies, Vol. 16). Monsey, NY: Criminal Justice Press, 41-96.

Craig, P., R. Honick, and M. Burnett. 2005. *Software Piracy Exposed*. Rockland, MA: Syngress Pub.

DuBose, M.M. 2006. "Criminal Enforcement of Intellectual Property Laws in the Twenty-First Century." *The Columbia Journal of Law & the Arts* 29: 481-496.

Goldman, E. 2003. "A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement." *Oregon Law Review* 82: 369-432.

Goldman, E. 2004. *Warez Trading and Criminal Copyright Infringement*. http://ssrn.com/abstract=487163, doi:10.2139/ssrn.487163.

Goldman, E. 2005. "The Challenges of Regulating Warez Trading." *Social Science Computer Review* 23: 24-28. doi: 10.1177/0894439304271531.

Goode, S. 2010. "Exploring the Supply of Pirate Software for Mobile Devices: An Analysis of Software Types and Piracy Groups." *Information Management & Computer Security* 18 (4): 204-225. doi: 10.1108/09685221011079171.

Goode, S., and S. Cruise. 2006. "What Motivates Software Crackers?" *Journal of Business Ethics* 65 (2): 173-201. doi: 10.1007/s10551-005-4709-9.

Grabosky, P.N. 1996. "Unintended Consequences of Crime Prevention." *Crime Prevention Studies* 5: 25. http://www.popcenter.org/library/crimeprevention/volume_05.

Gunter, W.D. 2008. "Piracy on the High Speeds: A Test of Social Learning Theory on Digital Piracy among College Students." *International Journal of Criminal Justice Sciences* 3 (1): 54-68. http://www.sascv.org/ijcjs/gunterijcjsjan2008.pdf.

Higgins, G.E., A.L. Wilson, and B.D. Fell. 2005. "An Application of Deterrence Theory to Software Piracy." *JCJPC* 12 (3): 166-184. http://www.albany.edu/scj/jcjpc/vol12.html#vol12is3.

Hinduja, S. 2006. *Music Piracy and Crime Theory*. New York, NY: LFB Scholarly Pub. LLC.

Holsapple, C.W., D. Iyengar, H. Jin, and S. Rao. 2008. "Parameters for Software Piracy Research." *The Information Society* 24 (4): 199-218. doi: 10.1080/01972240802189468.

Howe, J. 2005. "The Shadow Internet." *Wired*, January 13. http://www.wired.com/wired/archive/13.01/topsite.html.

Hunter, P. 2004. "Combating Video Piracy." *Network Security* 2004 (2): 18-19. doi: 10.1016/S1353-4858(04)00039-X.

Ingram, J.R., and S. Hinduja. 2008. "Neutralizing Music Pir

Pouwelse, J., P. Garbacki, D. Epema, and H. Sips. 2008. “Pirates and Samaritans: A Decade of Measurements on Peer Production and Their Implications for Net Neutrality and Copyright.” *Telecommunications Policy* 32 (11): 701-712. doi: 10.1016/j.telpol.2008.09.004.

Rehn, A. 2004. “The Politics of Contraband—The Honor Economies of the Warez Scene.” *Journal of Socio-Economics* 33 (3): 359-374. doi: 10.1016/j.socec.2003.12.027.

US DOJ. 2009. *Four Member of Alleged Internet Music Piracy Group Charged with Copyright Infringement Conspiracy* [Press release, September 9, 2009]. http://www.justice.gov/criminal/cybercrime/cassimPlea.pdf (accessed November 24, 2010).

Wang, W. 2004. *Steal This File Sharing Book: What They Won't Tell You About File Sharing*. San Francisco, CA: No Starch Press.

Willison, R. 2006. "Understanding the Perpetration of Employee Computer Crime in the Organisational Context." *Information and Organization* 16 (4): 304-324. doi: 10.1016/j.infoandorg.2006.08.001.

Willison, R., and J. Backhouse. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective." *European Journal of Information Systems* 15 (4): 403-414. doi: 10.1057/palgrave.ejis.3000592.

Willison, R., and M. Siponen. 2008. "Software Piracy: Original Insights from a Criminological Perspective." Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS).