

Enumerating and Reducing the Threat of Transnational Cyber-Extortion to Small and Medium Size Organizations

Abstract

Most organizations that rely on information technology to conduct business over the Internet are aware of the accompanying security threats with this enhanced connectivity. In 2003 over 97% of all companies who took part in the eighth annual FBI/CSI Computer Crime and Security Survey incorporated firewalls and anti-virus software into their suite of security technologies to defend against the most common types of attacks.¹ Although cognizant of the most commonly perceived security threats and countermeasures,² businesses relying on IT often do not address one of the most complex and potentially damaging exposures: Cyber-extortion. In a report to the United States Senate in March 2000, the director of CERT/CC detailed a cyber-extortion case where a 19-year-old Russian intruder stole 300,000 credit card numbers from an online music retailer. The intruder demanded \$100,000 in exchange for destroying the stolen data. When the company refused to pay,³ the numbers were released onto the Internet causing a public relations disaster for the retailer.³ On March 1st of 2004, four individuals were arrested for attempting to extort billions of yen from Softbank, Japan's leading broadband ISP. Again, the threat of releasing sensitive customer data was used in the attempt. After the arrest, Softbank noted it was investigating over 242 instances where customer information had been leaked. Information assets can quickly become significant liabilities.

The increasing reliance of business on internet-based e-commerce provides enormous opportunities for extortion. While some threats may fail, payoffs are certainly made to some extortionists. It seems likely, therefore, that larger and potentially more dangerous operations should be anticipated.⁴ Despite the increased publicity and corporate awareness of security threats, little mention is made of efforts to thwart extortion threats made against individuals and businesses. Why? At least 50% of the companies responding in the CSI/FBI survey admitted they did not report security breaches to authorities, with 70% of overall respondents fearing the impacts of negative publicity. From an international perspective, only 44% of responding British companies involved law enforcement after an incident occurred.⁵ Consequentially, we find that extortion statistics and published anti-extortion methods simply do not exist.

My proposal is twofold: First, I will generate non-biased anonymous data regarding extortion threats made against small and medium sized (less than 10,000 employees) organizations. The main method for accomplishing this will be via in-person interviews, plus the collection of a survey focused specifically on cyber-extortion experiences and readiness. Building on this information, I will create a list of guidelines organizations can implement to reduce their exposure to the threat of extortion. I will work closely with the surveyed organizations, local, federal, and foreign law enforcement, and subject experts (such as CERT/CC) to generate the data and guidelines. The United States Secret Service has already agreed to partner with me in producing the required data, and will be an invaluable aide in creating the guidelines for business/law enforcement cooperation. I plan to disseminate these findings and guidelines via the Department of Homeland

¹ 2003 CSI/FBI Computer Crime and Security Survey, Security Technologies Used.

² The most common types of attacks and misuse as reported by the participants of the CSI/FBI survey were virus attacks, unauthorized access and web use by insiders, and denial of service attacks. Ibid.

³ Cross, Stephen E. Cyber Security Testimony Before the Senate Armed Services Committee

⁴ Williams, Dunlevy, Shimeall. "Intelligence Analysis for Internet Security". CERT Coordination Center.

⁵ National Hi-Tech Crime Unit, "The Impact on UK Business".

Security and Carnegie Mellon's joint US-CERT organization, as well as providing copies to partner domestic and foreign law enforcement offices and all businesses taking part in the study. Some organization may never feel completely comfortable reporting extortion threats to law enforcement – these guidelines may provide their only method of threat deterrence.

Objective and Significance

The objective of my research will be to develop the first publicly available statistics on Internet-based extortion. Secondly, I aim to deliver a list of acceptable guidelines for reducing this threat to small and medium sized organizations. Specific questions to be addressed:

- **Who are the extortionists?** The majority of *reported* attempts point to Russia and Eastern Europe. Russian criminals are either recruiting or coercing hackers into breaking into Western systems.⁶ These reports are anecdotal. I plan to verify the geographical sources of the majority of these attacks, and detail whether this is a product of freelance or organized crime.
- **What are their methods?** Denial of Service (DOS) attacks may be a popular tool of extortion, but rarely are these events described as such. A more nefarious method involves placement of illegal material on a business' compromised computer system, coupled with the threat of alerting law enforcement. As part of the project's deliverable I intend to enumerate the most commonly used tactics of cyber-extortionists.
- **How can an organization reduce the threat of extortion?** If the majority of organizations opt not to involve law enforcement, how can we check the expansion of extortion? If this is a transnational problem, foreign law enforcement needs to become involved. I plan to lay the groundwork for research on this topic and increase business' awareness of this growing problem.

Two particular parties stand to benefit immediately from the generated research and guidelines: Organizations conducting business and customer relations via the Internet, and law enforcement at the local, federal, and international level. The results of this research will truly be cross-disciplinary: bridging the gap between private businesses at risk of (or current victims of) extortion and the legal authorities in the best position to aide them. Since almost no data currently exists on this subject, my research will be original, and, at a minimum, begin to raise awareness of this potentially devastating threat.

Project Design and Feasibility

The initial goal of the project is to generate accurate data on the occurrence of, methods used, and groups that gain from Internet-based extortion. The greatest challenges will involve convincing private businesses to share data on extortion attempts (successful or otherwise) made against them. The target group in my study will be non-governmental organizations with less than 10,000 employees. To gain industry perspective, I would be working with victimized businesses that have allowed themselves to be identified, discussing how they came to the decision to report, and discussing possible reasons why they may not have. In-person meetings and assurance of anonymous survey data collection should allow victimized groups an opportunity to more readily share data. The United States Secret Service has agreed to provide information, where possible, on Internet extortion cases and their origins. According to U.S. Secret Service Agent Mark Grantz, every incident of cyber-extortion he has dealt with has originated in Russia or another former Soviet Bloc country. Language and geographical barriers pose a challenge to my research, thus my focus will remain on the generation of significant statistics, and less on discussing the "why" (although detailing the Eastern European sources of extortion will remain a significant theme if supported by collected data).

Secondly, I will create a set of immediately usable guidelines to help businesses prevent cyber-extortion, as well as define actions to take if they find themselves unwitting victims. Businesses

⁶ Williams, Phil. "Russian Organized Crime, Russian Hacking, and U.S. Security".

may be able to take steps to reduce their exposure to extortion threats; many precautions may be similar to general information security practices. I plan to address the impact of these steps, based on actual implementation from participating businesses and law enforcement agencies. Since some businesses may never feel completely comfortable reporting to law enforcement in the case of extortion, this may offer the only method of threat deterrence.

After I have addressed the problems associated with avoidance of law enforcement interaction, I will draft a baseline plan of business/law enforcement cooperation. This is an extremely delicate subject among private companies, thus the plan will be created in conjunction with a variety of organizations that consider on-line information presence significant to the business operations. With these groups' input, the plan will be joined with requirements of law enforcement agencies. *The goal is to create a plan of action that is palatable to the victim groups, yet provides law enforcement the tools to track extortionists and bring them to justice.* Working with both private businesses and law enforcement, I will be able to represent both groups' point of view on cyber-extortion. The plan can not conceivably cover all potential extortion plots, nor all potential victims and law enforcement agencies; therefore recommendations of future action for research and plan development and dissemination will be included in the final report.

Presentation and Evaluation of Results

Considering the absence of any plausible data concerning cyber-extortion and its counter-measures, the final output of this project will be presented not only to Carnegie Mellon faculty and students, but delivered to my strategic research partners: all companies participating in my study, as well as any law enforcement agencies with an interest in battling these particular crimes.

Evaluation of the output of this project will take place in the form of the on-going partnership with law enforcement and business. Immediate feedback on the acceptability of guidelines by business and significance of generated data for law enforcement are the two evaluation criteria by which success will be measured. At the close of this project I will present and defend my research findings to my peers and Carnegie Mellon faculty in a public presentation, as well as my strategic partners.

Dissemination of Results

I plan to widely disseminate these findings and guidelines via the Department of Homeland Security and Carnegie Mellon's joint US-CERT organization, the United State Secret Service's Electronic Crimes Branch, as well as providing copies to partner domestic and foreign law enforcement offices taking part in the study. Submission to and distribution by the SANS Institute *Weekly Security Bulletin*, US-CERT *Cyber Security Bulletin*, and peer-reviewed *Heinz School Review* all offer active distribution methods for this project's deliverables.

Timetable

This project, including all interviews, work with partners, and presentation of results will be completed before the end of this Summer 2004 semester.

Milestone	Expected Completion Date
Research methods and perpetrators of extortion	Starting week 0 - <i>ongoing</i>
Meet with all research agencies (CERT, Secret Service, etc.) in production of survey	Week 2
Distribution of Survey	Week 3
Compilation of survey results	Week 6
Completion of methods/perpetrator research	Week 7
Complete interview of businesses, foreign law enforcement agencies	Week 8
First Draft	Week 9-10
Final Draft	Week 11