Dumpsters:
Beware of Treasures

By Robert B. Fried, BS, MS

Abstract

Take a moment and reminisce about your childhood days. Remember the chest or crate stuffed with all your favorite toys and games? Think about those adrenaline rushes you experienced each time you rummaged through and found just the toy or game you were looking for. This same kind of feeling is mimicked in the mind of a dumpster diver who sorts through mounds of rubbish while looking for that special treasure.

In this age of 'paperless offices' and technological innovations; trash cans continue to stake their place in the world. This paper will discuss dumpster diving as a form of computer attack. It will analyze the motives of those individuals who take part in attacks of this sort. Furthermore, real life scenarios of dumpster diving will be presented. Moreover, suggested methods of protection for the tangible information and objects thrown out to the world on a daily basis will be examined. Finally, several conclusions will be drawn with regards to dumpster diving.

Let's Dive Right In

An attack known as dumpster diving occurs when "waste product is examined to find information that might be helpful to the attacker" [1]. This form of attack gained popularity during the 1980s when security was rather lax. Back in the day, many people did not think about what happened to the trash they generated once they threw it out to the world. However, in the digital world of today, one has to be ever so careful in protecting their sensitive/confidential data from the spying eyes of others [2].

Dumpster diving was originally an attack done by curious individuals. These individuals wanted to know more about how a product or technology worked. They felt that the best way to find out was to go to the source. The conventional means of entry into a corporate office, by way of requesting sensitive information about particular products, was truly out of the question. The only other way to access such information then, was by diving into dumpsters [3].

Originally, the individuals who felt the need to exert their curiosity by way of dumpster diving were deemed hackers or crackers. Hackers can be characterized as "people who enjoy using computers and exploring the information infrastructure and systems connected to it" [4]. Crackers on the other hand are classified as "people who maliciously break into information systems and intentionally cause harm in doing so" [5].

Think Twice Before Taking Out the Papers and the Trash

Many of the original dumpster divers were individuals who were into the hobby of phone phreaking. These individuals were primarily interested in accessing information about telephone companies such as AT&T and learning the structure and operation of their phone systems. From the classifications above, one could make a fair assumption that the diving hacker was mainly interested in exploring how these telephone systems worked and discovering possible or known vulnerabilities. It can also be safe to assume that the diving cracker, on the other hand, was interested in developing and engaging in ways to exploit the weaknesses found within these systems. The dumpster often provided the education and answers to their questions. Often, there would be damaged or discarded manuals and equipment, readily available beneath the dumpster's lid [3].

Dumpster diving, which once was an attack targeted at phone companies, has now shifted into the mainstream. For example, with the increased usage of the Internet, there has been a continuous rise in identity theft. It is estimated that "each year, more than 500,000 Americans fall victim to identity theft, and that number is rising" [6]. Fraudulent credit card and other financial scams have also seen a steady increase in recent years. Many average individuals simply throw away billing or banking statements that often reveals confidential information such as account and social security identification numbers. "If someone can determine key pieces of information about you, such as your social security number, bank account numbers, credit card numbers, and so forth, they can pretend to be you, get access to your bank accounts, credit cards, and who knows what else" [6].

With respect to corporate targets, computer firms, software Manufactures or designers, legal firms and pharmaceutical companies are all vulnerable [7]. Corporations such as these are particularly vulnerable because they often produce unique products. For example, software manufactures/designers may produce products with specific program codes and languages. Legal firms can possess information on a particular case in litigation. Pharmaceutical companies can possess the blueprints on the chemical composition of a new drug that is still in its experimental/developmental stage and has yet to hit the market.

Pot of Gold

A dumpster can be viewed as an unlocked treasure chest to those who decide to intrude on other's trash. No, they probably would not be so fortunate to find gold, silver or jewels. However, what they could wind up finding could be things that money cannot buy. In fact, as a result of dumpster diving, individuals have found "everything from usernames and passwords written on sticky notes, all the way to important technical specifications and business communication and technical documents" [6].

With the advent of computers and technology, more and more data is being inputted and analyzed. Information can easily be at one's fingertips within a matter of seconds. However, not all information can be kept on computer. Even though methods of backing up data exist, tangible copies of documents and such must be kept on file. This sure does say a lot about the notion of a paperless office. In any event, garbage is generated. Included in this pile of trash, usually tossed within the dumpster without second thoughts are: information on company operations, marketing information, financial work sheets, research materials and even employee records [8]. Such information is usually made tangible on paper. However, computers and technology have allowed for storage of such information on digital media. This information can be kept on CD ROMS, diskette drives, microfilms, VHS tapes, audiocassette tapes and even typewriter ribbons [7]. With information such as this in the hands of a competitor, the damage can be devastating.

Taking it to the Courts

In 1988 the United States Supreme Court heard the case of California v. Greenwood. William Greenwood, a suspected drug trafficker, had his trash inspected by a sanitation worker at the request of a Laguna Beach California police officer. Upon a warrentless inspection of the rubbish by law enforcement, evidence relating to drug abuse was discovered. Following this discovery, a warrant was issued to allow for a search of Greenwood's home. This search resulted in the finding of evidence related to drug abuse. Greenwood was arrested on felony drug charges [9].

When heard before the California Supreme Court, it was said, "warrentless trash inspections violate the Fourth Amendment". Furthermore, they concluded, "the probable cause for the search of Greenwood's residence would not have existed without the evidence obtained from the illegal trash inspections, and that accordingly, all the evidence seized from the residence should be suppressed and all charges against Greenwood dismissed" [9].

The United States Supreme Court ultimately reversed the decision of the California Supreme Court in a 6-2 vote. The justices of the United States Supreme Court felt that one should not assume any expectation of privacy in garbage left out for pickup. They stated, "it is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops and other members of the public." They continue, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection" [9]. Essentially, one forfeits any rights to privacy and protection of the papers and other such garbage left for pickup.

Greenwood's case revolved around the issue of "publicly accessible rubbish". However, the law differs when trash is not accessible to the public. In the 1995 case of the United States v. Certain Real Property, this issue of accessibility was addressed. In this particular case, the defendant's trash bags, which were of interest in a police investigation, were out of sight from public view; however, were in the position indicating that they were in need of pick up by the sanitation department. To legally search the contents of these bags, law enforcement personnel would have to obtain a search warrant. It was stated, "the officer's entry into the area of the backyard immediately abutting the rear of the home constituted an intrusion into the defendant's reasonable expectation of privacy because the trash was not readily accessible to the public and the officer intentionally trespassed with the express purpose of obtaining the garbage" [9}.

Dives That Did Not Score a Perfect "10"

Transmeta, a company, which manufactures microprocessor chips, knows too well the negative impact dumpster diving can have on corporations. Many years of and millions of dollars in research have been spent on development of their newest product, the Crusoe chip. Apparently, several weeks before its release, several intruders tried to dumpster dive near their complex in Santa Clara, California. The company has been taking strong measures to fend off intruders. They have kept a very close eye on their trashcan receptacles. The last thing they wanted was a rival or competitor getting a hold of some top secret information or data about their company or the products they manufacture [10].

Trade theft has been a subject of much concern among corporations in recent years. According to a 2001 survey by the American Society for Industrial Security and Price Waterhouse Coopers it was found that, "fortune 1,000 companies lost more than $45 billion last year from trade theft". The tactics used in corporate espionage are: dumpster diving, hacking, bribery and even hiring away of key employees [10]. Industries are so competitive that many corporations need to resort to such tactics just to stay alive. Gary Clemenceau, a spokesman for Cyras Systems, an optical data switching equipment manufacture, which has stepped up security in its firm, says it best when he states, "the space is increasingly competitive and if they can't invent it, they'll try to steal it" [10].

Oracle, the world's second largest software giant was recently the subject of much scrutiny. It was discovered that Oracle had hired a detective agency, Investigative Group International (IGI), to find out some dirt on its direct competitor, Microsoft. Essentially, it was alleged that offers were made to the janitorial staff from the office of Association for Competitive Technology (ACT). ACT is a trade group, which is known to be pro-Microsoft [11]. Oracle stated that they hired IGI to investigate trade groups that were pro-Microsoft during the anti-trust case involving the world's largest software giant. In reality, such an investigation would only ultimately hurt Microsoft. Larry Ellison, chairman of Oracle, was directly involved in funding the investigation. In fact, this whole scenario has been referred to as "Larrygate" [10].

How to Prevent Dives

There are many ways one can protect himself/herself from becoming a victim of dumpster diving attacks. If you place your trash bags on your curb, anyone can legally view its contents. The best way to prevent anyone from seeing your 'private trash' is to essentially shred it. Paper shredders are inexpensive devices, which help eliminate or destroy those important documents that have found their way into the trashcan. Although, in some cases it may be possible for a skilled intruder to piece together sheets of shredded paper, the likelihood of he/she going through this trouble to uncover the contents of the shredded document is slim to none. According to a recent study, "the estimated size of the global shredder market is 700-800 million a year, with projected growth of 20-25 percent [12].

The shredder is definitely an effective tool but there are others. Experts in the field have recommended the utilization of tamper proof receptacles for confidential documents. For those corporations that can afford it, hire a document destruction company to handle those important documents that need elimination. It is also recommended that companies install magnetic wipe bins to handle any digital media. Furthermore, it is recommended that a corporate policy, if not already in effect, be put in place to state the guidelines for proper handling and disposing of sensitive documents [13].

Trash Becomes Talk of the Town

This issue of trash caused quite a stink in Hartford, Connecticut in May of 1997. In a vote of 65 to 73, a bill, oddly enough entitled "An Act Concerning Dumpster Diving" was approved amongst legislators in the state Capitol. The bill, essentially, focused on the need to "stop companies from waging dirty campaigns against competitors - by digging through their trash for trade secrets" [14].

As per the bill, dumpster diving in the state of Connecticut would be deemed a high tech crime associated with forms corporate espionage. Crimes involving corporate espionage are banned under trade secret protection laws. So with dumpster diving added to the growing list, companies who are victimized would be able to seek injunctive relief and punitive damages [14].

Many state legislators felt that the bill was necessary to protect businesses from dumpster diving attacks. Representative Lawlor, a Democrat from East Haven, Connecticut strongly supported the bill. He stated, "This is a real problem for many businesses in the state. This is a fundamental protection that ought to be afforded them" [14]. Although there were many supporters, which ultimately resulted in the approval of the bill, many people were opposed; Representative Tulisano, a Democrat from Rocky Hill, Connecticut voted "no". Tulisano believed that "court decisions have shown people have no right to privacy to the trash they throw out. Why the business community should be protected and you and I are not protected is beyond me" [14].

Summary, Conclusions, and Further Work

Let's be honest; if you saw a pot of gold, wouldn't you dive right in? Dumpster diving, once popular during the 1980s is making a considerable comeback. This form of attack is not only tending to the curious at heart, it is also being utilized as a form of corporate espionage. The topic has of trash has become such a stinky issue, even the United States Supreme Court had to waft it up for a while. It has been decided that trash found on the curbside, in plain view of the public eye is fair game to all people passing by. However, trash that is visible in the confines of one's property, outside the view of the public eye is still legally the property of its rightful owner. The average citizen tends to rely too much on their garbage lids to shield their treasures from the outside world. Yet, as the saying goes, one man's garbage can be another's man's treasure. Essentially, what is left out for sanitation is also at the full disposal to others.

A number of tools, instruments and means of protection exist to protect the garbage we generate on an every day basis. Anything from paper shredders to magnetic wipe bins are recommended. One really has to measure the value of trash before deciding how far they will go to destroy their sensitive documents or data. Two things in life are for sure: as long as human beings run rampant in the universe, data will always be created and garbage will always be generated. The best advice one can give is to really think carefully before throwing anything out to the world.

References

[1]. The All.Net Security Database: Attack 17: Dumpster Diving. http://fc@all.net
[2]. Wikipedia: Dumpster Diving.

http://www.wikipedia.com/wiki/Dumpster_diving
[3]. The New Hacker's Dictionary: Dumpster Diving.
http://www.tuxedo.org/~esr/jargon/jargon.html#dumpster%20diving
[4]. The All.Net Security Database: Threat 10: Hackers.
http://fc@all.net
[5]. The All.Net Security Database: Threat 11: Crackers.
http://fc@all.net
[6]. Craiger, Philip J. and Blaine Burnham.
"Traveling into Cyberspace: Computer Security".
http://www.siop.org/tip/backissues/TipApr01/18Craiger.htm
[7]. "A High Tech Growing Crime".
http://www.crimecontrolcenter.com/hightechcrime.cfm
[8]. "Identity Theft: Dumpster Diving".
http://www.crimecontrolcenter.com/dumpsterdiving.cfm</A>
[9]. Kakura, Thomas V. 1991 FBI Law Enforcement Bulletin "Dumpster Diving and the Law".
http://www.pimall.com/nais/n.dumpster.html</A>
[10]. Edwards, Cliff "High-Tech Spy vs. Spy". ABCNEWS.com: July 2001.
http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html
[11]. Wolf, Jim. "Oracle's Boardroom Spy Tricks".
ZDNet News: June 29, 2000.
http://www.zdnet.com/zdnn/stories/news/0,4586,2596401,00.html
[12]. "Protect Against "Dumpster Diving" With Shredder".
http://www.b4-u-buy.com/09c4700.htm"
[13]. McClure, Stuart and Joel Scambray. "Forget the Firewall; Guard Your Garbage Against “Dumpster Diving' Hackers". InfoWorld.
http://www.infoworld.com/articles/op/xml/00/07/03/000703opswatch.xml">.
[14]. Scarponi, Diane. "Lawmakers Try to Protect Companies in Vote to Garbage Espionage". Associated Press: May 09,1997.
http://www.phonelosers.org/dd.html

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).