Attitude Adjustment: Trojans and Malware on the Internet

An Update

Sarah Gordon and David Chess
IBM Thomas J. Watson Research Center
Yorktown Heights, NY

Abstract

This paper continues our examination of Trojan horses on the Internet; their prevalence, technical structure and impact. It explores the type and scope of threats encountered on the Internet - throughout history until today. It examines user attitudes and considers ways in which those attitudes can actively affect your organization’s vulnerability to Trojanizations of various types. It discusses the status of hostile active content on the Internet, including threats from *Java* and *ActiveX*, and re-examines the impact of these types of threats to Internet users in the real world. Observations related to the role of the antivirus industry in solving the problem are considered. Throughout the paper, technical and policy based strategies for minimizing the risk of damage from various types of Trojan horses on the Internet are presented

This paper represents an update and summary of our research from *Where There's Smoke There's Mirrors: The Truth About Trojan Horses on the Internet*, presented at the Eighth International Virus Bulletin Conference in Munich Germany, October 1998, and *Attitude Adjustment: Trojans and Malware on the Internet*, presented at the European Institute for Computer Antivirus Research in Aalborg, Denmark, March 1999. Significant portions of those works are included here in original form.

Descriptors: fidonet, internet, password stealing trojan, trojanized system, trojanized application, user behavior, java, activex, security policy, trojan horse, computer virus

Attitude Adjustment: Trojans and Malware on the Internet

Trojans On the Internet…

Ever since the city of Troy was sacked by way of the apparently innocuous but ultimately deadly Trojan horse, the term has been used to talk about something that appears to be beneficial, but which hides an attack within. In the remainder of this paper, we will talk about "Trojan horses" (or just “Trojans”) of a digital type; Trojan horse computer programs which some users are encountering on the Internet today. These Trojan horses are let into organizations, and their hidden behaviours come out of the bellies of programs when least expected, in some cases vanquishing your data! In this paper, we will continue to examine ways you can minimize your vulnerabilities to the Trojan horses of today. Finally, we will discuss how one’s preconceived attitude towards Trojan horses can significantly effect one’s ability to protect an environment from the potential threat, and provide a sociological as well as technical path toward reducing the risk posed by Trojan Horses.

Historical Perspective

Despite the common usage of the term Trojan horse, a good working definition of the term remains somewhat elusive. Thus, we shall offer several operational definitions of “Trojan horse”, taken from a historical perspective, before discussing some the limitations of these definitions.

In "Reflections on Trusting Trust", Ken Thompson discusses early (pre-1984) academic experiences writing self-reproducing programs and explores the possibilities of Trojan horses [1]. His examination of the functionality of a C compiler that contains instructions to deliberately miscompile code when a certain input pattern is matched illustrates how using any untrusted code can compromise a computing process. The types of academic exercises portrayed by Thompson illustrate the types of Trojans that were created as academic challenges in the late 70’s and early 80’s. As these exercises were taking place in Universities, users outside academic environments were beginning to see the impact of untrusted code. As an example,

> *Discretionary access control mechanisms restrict access to objects based solely on the identity of subjects who are trying to access them. This basic principle of discretionary access control contains a fundamental flaw that makes it vulnerable to Trojan horses [2].*
>
> *Trojan horse: A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse [3].*
>
> *At a professional meeting last week, we had a presentation by a university data center manager on a Trojan Horse attack which had shut down his operation [4].*

However, even these problems were limited due to the fact that connectivity during these early days was still basically limited to academic and government subsets of population. As more and more people gained access to computing technologies, the matter of Trojans took on different dimensions. We will explore these changes in connectivity and the evolution of Trojans in the following sections, beginning with an examination of *FidoNet* and *The Dirty Dozen*.

FidoNet and *The Dirty Dozen*

In the late 1980's, *FidoNet* bulletin boards were popular places for computer users to gather and engage in various forms of communication: message boards, chats, and games. These bulletin boards comprised the *FidoNet* network. Programs were made available from the individual systems for download. As users downloaded programs, they sometimes obtained programs that claimed (according to the documentation either on the BBS or accompanying the program) to do one thing, but which actually did another. Most often, the thing they did was something the user did not want them to do. Sometimes these programs were widely circulated. Someone came up with the idea that it might be a good idea to document the existence of these harmful programs and warn other *FidoNet* Sysops (the BBS operators) about the files so they could be removed, and to warn users about the existence and location of such Trojan horses. Out of this need and idea, *The Dirty Dozen* was born. *The Dirty Dozen* is a list that was established to provide warnings about the most common Trojans and Logic bombs. A Trojan was defined by the creators of the list thusly:

> **TROJAN* (T) These programs PURPOSEFULLY damage a user's system upon their invocation. They almost always shoot to disable hard disks, although they can, in rare cases, destroy other equipment too. There are many ways that a TROJAN can disable your hard disk. [5]*

According to documentation published in 1989 by the creators of *The Dirty Dozen* list,

> *Recently bulletin board download directories have exploded with an ever-increasing number of unlawfully modified, illegally copied, and altogether deceptive programs. The Dirty Dozen lists known examples. SysOps: Please be careful when posting files in your download libraries! A professional quality program should arouse your suspicions, particularly if it doesn't include the author's name, address, and distribution policy. The BBS community is under legislative threat at the State and Federal level. We cannot fight this threat effectively while our directories sit stocked viruses, "trojan horses, and cracked commercial games!" Let's demonstrate a little social responsibility by cleaning up our download libraries. [6]*

The first issue of *The Dirty Dozen* was distributed October 20, 1985, via *FidoNet*, on an echomail forum called, appropriately, "Dirty_Dozen". It contained a list of 12 “bad files”, identified by filename [7]. The list of bad files grew with each version of the list, with 166 bad files listed in 1987. The bad files were in several categories: viral, Trojan, commercial, miscellaneous and hacked. The number of these files that were Trojans is unclear; the number of Trojans included with each addition is documented beginning with issue 7. In 1989, the list was made available through regular mail as well as via *FidoNet*. For $10.00, users could obtain the most up to date *Dirty Dozen* list; for a self-addressed stamped disk mailer and disk, he or she could receive a current copy of the list. The January 23rd, 1989 issue of *The Dirty Dozen* listed 63 programs which were Trojans; here is an example listing, given as a filename, description of what they program is supposed to do, followed by what the program actually does [8]:

> *CDIR.COM*
>
> *This program is supposed to give you a color directory of files on your disk, but it in fact will scramble your disk's FAT table.*

Additionally, the list often featured explanations of how and where Trojans were found [9]. For example:

> *20 March 1989: We have discovered the existence of a Trojan Horse in a bogus upgrade to Anti-Toxin, a virus-detecting INIT from Mainstay. The INIT, labelled (sic) as version 2.0 in the Get Info box, attempts to format your disk and rename it "Scored!".*

The Dirty Dozen echomail message area was quite active during the early 1990's, and provided both computer hobbyists and professionals who used *FidoNet* in the course of their work with a good resource for getting information about Trojanized software. It is still active today, although much less so than prior to widespread availability of Internet technologies. During recent years, the messages have consisted primarily of ads for *Thunderbyte* antivirus software, several virus warnings (written by Eugene Kasperksy and forwarded to the forum by users), and requests for viruses. Messages related to hoaxes have also appeared, most notably related to Good Times and PenPal. Messages about actual Trojans have been few and far between, with the most notable being a warning on the *PKZIP* Trojan in 1995, and a program called Z-Modem.com in 1996.

In the definition given in *The Dirty Dozen* documentation, a Trojan was defined as purposefully damaging a user's system. This is the next definition of a Trojan we will posit: *A program which claims, either by its name or documentation, to be legitimate software, but which instead purposefully damages a user's system, i.e. files or other data on hard disks, upon invocation.* We consider these types of Trojans to be "classic Trojans".

The Dirty Dozen reflected a common way of perceiving Trojan horses in the late eighties and early nineties. Trojans were perceived as "bad programs" which were pretty easily identifiable by filenames, or by filename and location of the file on a given system. Users became accustomed to seeing warnings that named the file name, and the file's location, and instructions from experts to avoiding that file, or at least to question the file's authenticity. The people who were experiencing problems with Trojans thought of those problems in relation to their experience. This is not in and of itself remarkable: one way in which people gain knowledge is through experience. From that knowledge, solutions to problems can be developed, and *The Dirty Dozen* was a viable solution for the problem at that particular point in time. However, problems can result when the knowledge no longer reflects the reality of the situation. The common knowledge of "Trojans" became flawed, with the advent of Internet connectivity. The next section examine problems this new connectivity introduced to end-users and to administrators, beginning with problems for end users.

Trojans march into the 90's

The PKZIP Trojan

As individuals and corporations moved into the age of the Internet, downloading of programs from Bulletin Boards gradually diminished. The Trojan problem evolved into one that could take advantage of the speed and nature of the Internet. We see one form of this exploitation first evidenced in the emergence of the *PKZIP* Trojan. *PKZIP* is a popular utility that compresses files. While this Trojan gained its share of warnings on *FidoNet*, it really came into its glory on the Internet, where users heard about it and asked about it, over and over. Here is a brief history of this classic Trojan. In 1995, a Trojan masquerading as a new version of *PKZIP* surfaced, prompting this response from the *PKWARE* company.

> *!!! PKZIP Trojan Horse Version - (Originally Posted May 1995) !!!*
> *It has come to the attention of PKWARE that a fake version of PKZIP is being distributed as PKZ300B.ZIP or PKZ300.ZIP. It is not an official version from PKWARE and it will attempt to erase your hard drive if run. It attempts to perform a deletion of all the directories of your current drive. If you have any information as to the creators of this*

> *trojan horse, PKWARE would be extremely interested to hear from you. If you have any other questions about this fake version, please email* xxxxxx@xxxxxx.xxx

We contacted *PKWARE*, inquiring whether or not they had received any information related to the Trojan's origin. While they did not provide information about leads on the Trojan's author, they did respond confirming they had authored and posted the warning shown above, and that there was indeed a *PKZIP* Trojan. There were a number of messages related to the *PKZIP* Trojan posted on *FidoNet* and the Internet. Most of them were very similar to this:

> *On Wed, 20 Mar 1996, xxxx xxxxxxx wrote:*
> *> Can anybody verify the rumor that any latest version of pkunzip, when*
> *> downloaded, contains a trojan horse which will permanently destroy*
> *> your hard drive?*

People generally correctly responded that there was a *PKZIP* Trojan, but that users who got *PKZIP* from a legitimate source need not worry. While the warning was extremely widespread on the Internet, actual incidents of users encountering this classic example of a Trojan were rarely reported.

Despite the thankfully limited impact of the actual *PKZIP* Trojan, it should be noted that the growth of the Internet introduced several new aspects to the Trojan picture, including but not limited to increased user base, speed and relative bi-directional anonymity of file transfer availability. These were double-edged swords which changed the way in which people exchanged programs (and sometimes, Trojan horses) as well as information about programs. Files could be gotten from the Internet much more quickly using the Internet friendly FTP (File Transfer Protocol) than they could with generally available *FidoNet* system protocols such as ZMODEM. The FTP Protocol also allowed for multiple transfers to take place at the same time. These improvements over old-fashioned protocols meant many users could obtain files at the same time, and much faster than in the past. E-Mail messages and Usenet News Posts regarding "Trojanized" programs could also be distributed much more quickly.

There are rather obvious downsides. First, these posts can contain false information or information that may be true but does not relate to the file you happen to have of the same name. It is trivial to forge a post to Usenet with little way (if any) for the casual users to authenticate the information. Furthermore, a Trojanized program that was made available via FTP could theoretically be obtained much more quickly and by many more people as well. Finally, the identity of those that offered and received files via Internet FTP was in many cases less clearly obvious than it was with *FidoNet* systems. While this anonymity was a good thing in terms of allowing users to log in without having to spend time registering, or having an account on a system in order to obtain or make available software, it did not provide for authentication of the source or software.

While this was true in some degree in the *FidoNet* Network (i.e. there were anonymous accounts available, administrators sometimes did not verify user identity), the community nature of *FidoNet* lent itself to more accountability on the part of many, if not most, *FidoNet* System Operators. *FidoNet* possessed (and continues to posses) a hierarchical structure of "government", where consistent problems with the network can result in expulsion from the Network. Hence, while files of the same name could exist at multiple *FidoNet* sites, and while there is no way to tell by file *name* if a program has been Trojanized, users generally limited their *FidoNet* downloads to systems with which they were pretty familiar and which were often run by operators who had accountability to their users for one reason or another. Users who made use of *The Dirty Dozen* to keep themselves informed on possible trojan problems on

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE