Analysis of Malicious Software Infections

Kenneth M. Davis

ABSTRACT

The purpose of this paper is to investigate, analyze and inform within crucial topics regarding some of the most damaging and highly propagatable threats to users of any internetwork service. At the close of the year 2000, there were nearly 361 million Internet users. By April of 2011, the number of users utilizing network services grew by 480.4 percent to almost 2.1 billion users. With a world population of 6.9 billion people, this gives us an Internet penetration of the population of just over 30 percent. With a growing percentage of penetration and rising network population, it is crucial to understand the threats faced by simply plugging in your laptop within the assumed safety of your home network. The technology which affords us simplistic and easy to use network of resources on the Internet is one which is often not understood by the typical network user. Malware exposures increase astronomically faster than the number of users who fully understand the threats that they face. The goal of this paper is to explain these threats and assist users in taking steps to reduce their risk to Malware.

INTRODUCTION

Buying a computer is easier and cheaper today than it has ever been before. In 1997, the price of a standard desktop was over 1,000 Dollars [1]. Today, you can acquire a desktop with over 300 times the processing power of the 1997 model for less than half the cost. As prices lower, more and more people are able to afford computers and worldwide network penetration continues to rise. Network penetration of the population in North America alone is 78.3% and worldwide is
30.2% and climbing daily [2]. As the network population rises, so does the necessity to enable users to educate and protect themselves from the threats that they will inevitably encounter as they use services.

It is often noted that you can find anything on the Internet. This statement is close enough to fact to be accepted as true. However, what you find may not be what you were looking for. In September of 2010, Dasient reported that Internet users encountered over 1.3 million malicious Internet links per day. Dasient’s services assist in protecting Internet users from these infectious links, otherwise known as malvertisements, before they transmit data to network users but further steps and education are necessary to further limit network risks. Additionally, Dasient reports that “41 percent of malvertisements are from fake anti-virus pop-ups” [3].

With the appropriate education regarding safe browsing practices, a majority of network user infections could be prevented. With a steady increase in the number of people who use network services to perform tasks such as paying bills, keeping in contact with loved ones or shopping, the risk of revealing intimate personal information such as credit card, social security and phone numbers is great. There are fewer and fewer people who actually own postage stamps or paper checks to physically mail in a bill payment. The use of the Internet to perform these functions has given us a time-saving and convenient method of payment that many people do not bother keeping physical receipts or check stubs. Internet services have given us convenience at the cost of liability and a potentially disastrous potential for loss or disclosure of sensitive personal information. This paper will discuss commonly encountered risks associated with Internet use. The risks discussed will include malware and malvertisements, fake anti-virus and spyware. It will also discuss safe browsing practices and countermeasures which can prevent infection and defend your computer some of the most common and easily propagatable network threats.

DEFINING TERMS

Highly Propagatable:

Propagation is an objects ability to move from one point to another. When something is defined as highly propagatable in terms of Malware, it means that the Malware entity is able to transmit and infect a user and in turn infect other users through exponential propagation.
Malware:

For this paper, there will be distinctions drawn between Malware and Spyware. In the terms of this paper, Malware is defined as a propagated malicious program designed to infect users for the purpose of creating advertisement pop-ups, interrupt network services, or utilize computing resources for the purpose of causing network activity which is both unintended and transparent to the network user.

Microsoft defines Malware as “short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al.” [12]

As can be seen from the “catch-all” style of definition, it is sometimes useful to make distinctions between different classes of malicious software for purposes of discussion. However in practice, there is little difference in the overall effects of the software. The primary distinction lies in the nature by which they propagate from source to user.

Spyware:

Malware and Spyware are often grouped together due to their shared characteristics. In the terms of this paper, Spyware is defined as a category of malicious programs which are propagated for the purpose of tracking network user habits, collecting user information or other information collection purposes. It is to be noted that Spyware under this definition is not considered highly propagatable and once it resides on a user’s machine it is typically benign to other users on the network.

Malware and Spyware Propagation Paths:

Malware, as defined, is often able to travel from SOURCE to USER and additionally from USER to USER.

Spyware as defined is typically only able to travel from SOURCE to USER.

Malvertisements:

Malvertisements are web advertisements created for the sole purpose of the propagation of Malware programs by transparent transfers to end-users, automatic download through hidden windows, or deception techniques which fool end-users into performing an action [4].
Fake Anti-Virus Programs:

Fake Anti-Virus programs are typically propagated through the use of malvertisements by using deception techniques [4]. This category of Malware fools the end-user into thinking the program is an actual anti-virus program. The purpose of Fake Anti-Virus programs is to serve as a propagation catalyst by orchestrating the download and installation of additional Malware and serving as a peer-to-peer propagator.

Fake Anti-Virus can often be one of the most difficult malicious software packages to completely clean an infected system of. Due to the complex nature by which Fake AV performs its designed tasks they are often able to re-download autoloader packages or recompile the packages from a hidden source file once a portion of the program system has been eliminated or tampered with. Quite a few installations of Fake AV do not make themselves known to the user until they have fully taken root in the affected system and inexperienced users may be fooled by the complex graphical representations of real anti-virus and allow it to exist. Some of these Fake AV programs are even funded by users sending money for the, assumed, full version of the Anti-Virus which is actually causing the infection in the first place.

THE MALICIOUS ENVIRONMENT

The percentage of the world’s population that uses the Internet is constantly increasing. In 2000, there were nearly 361 million users utilizing network services. By June of 2010 the number of users utilizing network services had grown by 444.8 percent to over 1.9 billion users. By April of 2011 there were almost 2.1 billion. According to world population data from the U.S. Census Bureau there are approximately 6.9 billion people in the world. Over a fourth of the total world population is utilizing network services at the network penetration level of 30.2 percent [2]. The rate of increase in users has more than doubled the rate of increase of world population [Fig.1].
There was a time when one of the most dangerous activities someone could do on the Internet was opening an email from someone that they did not know. This was a common way for virus infections and still remains to be a threat. As network use trends change so does the method in which a majority of infections occur. ‘Sophos’, a leading network security company, recognized in September 2010 that the social media website ‘Facebook’ had become the top source of Malware infections. This revelation not only signifies a change in common source of infection but signifies a change in the methodology in which infectious propagations are instigated [5].

Infectious malicious software propagations were traditionally hosted by a website specially crafted and advertized by the creators of the malicious software. The current trend has migrated away from this and towards advertisement hijacks carried out by protocol exploits and the hacking of well known entities’ websites that are already in full trust by many users. This makes safe browsing practices inherently difficult if not futile if a user is expecting for their protection schemes to do all of the work for them. It is no longer enough of an infection deterrent to only utilize websites that are well known and assumed to be free of Malware or other malicious applications as even Microsoft and Google have been subject to propagation issues. At any time a portion of a website which you are familiar with and are required to apply trust in could be hijacked and used to propagate malicious software or a siphon of your personal information. It could be your banking site, a school webpage, or your favorite ‘Facebook’ application or mobile phone application. In addition to infection risks many websites have been accused of leaking...
personally identifiable user information. This includes unsafe user privacy practices that are problematic for many social networking sites in use by users.

The best preventative measure for avoiding the leak of personally identifiable information to parties which may attempt to steal your identity is not revealing the information in the first place or even using pseudo identities. It is also crucial to ensure that the website you have traveled to is the website you intended to go to as well. It is easy for email links to websites to be falsified or redirected to a website that looks nearly identical to what you expect to see or what you are used to seeing. This is how many phishing attempts are carried and often result in leaks of personal information. Banking websites and other sites meant to be secure exchanges of information will use HTTPS or Secure HTTP which is signified by the address being prefixed by ‘https://’. Additionally, a lock icon will be displayed on the toolbar which can be used to access and verify website certificate information which allows you to verify the website is indeed the site you expected to visit [Fig.2].

![Example of https and lock icon used by Navy Federal Bank](image)

The diseases and infections that humans are susceptible to are often able to propagate from person to person through touch. It is not uncommon for malicious software to have the ability to propagate in a similar manner. In November of 2008, the U.S. Army barred their personnel from using any portable storage device on their networks due to virus and Malware propagations commonly referred to as “Worms” [7]. These “Worms” are able to automatically propagate themselves from your home computer onto your flash drive. When you plug your flash drive into your computer at work it then transfers itself onto that computer as well. Due to the nature in which USB portable devices communicate with the computer many implementations of Anti-Virus and Malware protection software were unable to prevent a rapid epidemic of infection. To combat this, many vendors of portable storage devices implemented anti-viral software solutions which automatically scan any data transferred to and from the device. Unfortunately the rapid
changes that occur in the design of malicious software makes it so that detection schemes must be updated consistently and often to reduce the risk of infection.

According to the APWG Phishing Activity Trends Report for Q3 of 2009, 48 percent of the 22 million computers scanned were infected with malware. While this percentage is slightly lower than their previous sample in 2009, it is still a 493.6% increase in infection from 2008 [8]. By the third quarter of 2010, APWG reported that 83.12% of all phishing hosting sites had been reported. In a best case scenario that gives utilities like blacklists which prevent browsers from traversing reported sites an 83 percent chance of avoiding websites with phishing related material [9]. This cannot be mistaken for a successful ratio of avoidance however. The means available to users to avoid such malicious content are neither completely effective nor are they 100% accurate in being up to date at any given time. It has, and will continue to be, an uphill battle protecting users from malicious content which is propagated onto the internet faster than any organization can track and maintain blacklists and signatures for. In other words, 17 percent being unaccounted for is a very large, diverse, and ever changing portion of hosted content. One which a users chances of encountering on any given moment increase drastically as their safeguards become out of date.

Many common web browsers in use, as well as anti-spyware utilities, integrate malicious URL blacklisting in their update functions. One of the largest issues with the use of these utilities is the broad failure of the common user to keep these utilities up to date. Regardless of how fast a company can keep their lists current, many users fail to perform the required updates in order for their utilities to provide adequate protection for their day to day browsing habits. Additionally, many basic users are not equipped with the knowledge of proper safe browsing practices. Many infections and malicious links can be avoided simply through the users’ interaction of them, or lack of. There are several ways in which a user can determine whether or not a link or other hosted content is genuine or their intended location.

The widespread acceptance of the Internet for duties such as banking has been generally adopted due to the convenient nature by which someone can manage their funds without ever leaving their home or even while away from home by use of their cell phone. This convenience does not come without a cost. The primary cost of this convenience appears to be an overly deserved feeling of safety when utilizing such services. With a persons use of many different networked services also comes a great deal of email interaction. One of the oldest, and most basic, phishing techniques utilizes a users trust and failure to pay close attention to detail when dealing with routine informational transactions. For instance, an email from their bank requesting them to log in and update certain information may seem like a very routine activity considering the numerous
times informational popups occur at these websites requesting an update of things such as your cell phone number. However, the danger with such trust occurs when users fail to take a simple precautionary step in order to avoid low-level attempts at phishing. Simply manually typing in your banking institutions website instead of following an email link could be the difference between visiting and avoiding a maliciously crafted website. This does not necessarily result in any sort of malicious software infection, the release of personally identifiable and sensitive information is one which can create damage well beyond that of a typical computer based malicious program.

Many Malware and other malicious software infections are not completely halted or removed by anti-virus or anti-malware removal software due to lack of updates. For the best protection against infection these software suites need to be updated automatically daily. If your vendor does not provide consistent updates at least once a week then it most likely is constantly out of date and an alternative solution should be sought out. There are several free solutions for protection and removal of Malware and Spyware alike. Some of the best free options are ‘SpyBot S&D’, ‘Avira’ and ‘Malwarebytes’.

Many infections can be prevented or thwarted by immediate user action. If a user notices that a pop-up is downloading or installing something it should be closed immediately. Additionally, closing the browser and rebooting the computer can cause any temporary files used to formulate the Malware to be deleted. Pop-up blockers in common use with major web browsers do a decent job at preventing these pop-ups but they are not perfect due to rapid new developments in malicious software. Spyware prevention software such as ‘SpyBot S&D’ maintain malicious website block lists which can assist in preventing your computer from receiving or contacting a malicious website. Enabling the real-time protection of your security software, commonly called a “TeaTimer”, assists in protection and prevention by monitoring for malicious software constantly rather than only when manually ran. When coupled with automatic updates this setup is the best passive prevention that requires little user interaction or interference. Real-time monitoring and website block-lists can drastically reduce the chances of advertisement hijacks or malvertisements from affecting you while browsing commonly trusted websites. Malvertisements are very difficult to recognize and often do not exhibit any visible notification that anything is occurring. Banner ads are so common to the Internet that many users would only notice if they all of a sudden disappeared entirely rather than simply changed.

Many varieties of malicious software cause negative performance results from computers that most users falsely recognize as their computers getting older. Typically this is actually not the case. Typical processor load of a computer manufactured after 2001 should exhibit no negative
performance signs from simply browsing the web as there is actually very little to be processed in regards to displaying and interacting with web content. This symptom of negative performance commonly causes computer owners to spend money on new computers well before it would have been necessitated by their usage habits or needs and they typically find their new computer quickly exhibiting the same negative performance symptoms.

New computers, particularly those with pre-installed software from the factory, may not have all of the necessary security updates to the software required to defend against many software exploits that Malware, virii and other malicious software take advantage of. These new machines are very susceptible to infection the very moment they are connected any network. It is advised that these machines be updated if possible manually prior to any network exposure and then only connected to a firewall protected network.

MOBILE DEVICES

There was a time when telephones were one of the most private and secure ways of communicating from one person to another. This privacy aspect, even in a legal sense, does not hold particularly true with cell phone mobile devices. Luckily, as the adoption of the mobile phone increased so did the technology behind their communications. It is rather difficult for an ordinary person to wiretap or listen in to a mobile phone conversation at this technological stage. However, this was not necessarily the case 10 years ago. No different than wiretapping a cordless house phone, any person with a close enough proximity and a scanner capable of receiving the appropriate frequency could listen in on these conversations. The privacy of the call itself is probably one of the least worries with mobile phones today.

As the mobile phone was adopted and accepted as almost a part of someone’s day to day attire, the expected function of the phones themselves changed as well. A modern mobile phone is no longer just a phone. It is a small portable computer no different than a laptop or desktop. Some of them even operate micro versions of Microsoft Windows while others such as the Android use operating systems which resemble that of Linux. Users are able to integrate these devices with a large number of mobile applications which perform functions desirable to the user. Some of these apps are simply for entertainment. Applications which interface common social networking sites such as Facebook or Myspace are very common. Naturally other forms of entertainment are also available such as instant message services and games designed to take advantage of
advanced technology such as motion or touch sensors in the phone. A plethora of new applications come out daily and with them come new malicious threats to mobile users.

One of the biggest threats to the mobile user is the leak of personally identifiable information. Dasient studied over 10,000 mobile Android applications and found that over 8 percent of them leaked personal information over the network [11]. Some of these applications were observed to be generating their own network traffic as well as SMS messages, activity unknown to the user. Additionally, a mobile user can also visit malicious websites through the use of their mobile phones web browser. This can occur no differently than being infected by malware by using your desktop computer. Certain versions of mobile malware will perform activities such as finding the owners Skype credentials and accessing their Skype information and sending either users on the contact list or the persons home machine infectious links which result in further propagations of infection.

Not only are mobile phones becoming more and more prevalent. The same functions which inherently pose degrees of risk to a users information and network safety are able to be carried out with ease upon most modern mobile phones. Ranging from banking activities to transferring files to and from remote devices such as your home computer, many mobile phones have access to as much or more personal data than can be expected on a laptop. Assuredly there are plenty of users who have the misconception that their phones are safer than their laptops or home computers because they keep them securely in their pockets. There is, or at least they feel, a lower chance that their phone will be stolen than their laptop since they keep their phone much closer at hand. With this misconception of physical security being applied to network security, many users rely on their phones to record and keep certain information such as password lists or account numbers. Much like the social engineering schemes often used to gain unauthorized access to locations and networks some utilities that are intended to help users who have lost their phones or wish to backup their data remotely can be used against these users in targeted malicious attacks. With enough information about a user it can be quite difficult to safeguard against such intrusion.
CONCLUSION

Through researching and analyzing the statistics regarding Malware, malicious software infections and personal information leaks, it is strikingly clear that any computer exposed to a network is at risk for infection. Computers which do not maintain network connections remain at risk for infection through the common use of portable USB storage devices. The development of malicious software changes at a rate that prevention and removal software vendors are unable to keep up with. If the network penetration rates continue to climb as they are expected to, we will most likely see the number of Internet users double over the next 10 years. During that time, protocol changes and adaptations such as the transfer from IPv4 to IPv6 will yet again drastically make changes in the methods in which malicious software is propagated. Due to the risk of infection, a computer currently unaffected by Malware can be expected to be infected and one which is already infected can be expected to be infected again. The Internet provides users with invaluable and convenient access to information and resources but this convenience comes with a risk of infection which only requires an active internet connection or use of an infected portable storage device to initiate. It is clear given these statistics that the most appropriate action is to increase user education regarding safe browsing practices including protection of personally identifiable information and proper installation, maintenance and upkeep of anti-viral and anti-malware protection software.

In addition to safeguards typically seen with laptop and desktop devices, additional measures will have to be taken in the very near future to prevent an overwhelming outbreak of malicious software amongst the mobile device user-base. The rate in which malicious software and personal information leaks are able to propagate across any given user group can typically be observed throughout the course of one revolution of the earth. This is particularly true if it involves a website in common use by a broad range of individuals. With the rapid advance of mobile browsing applications, mobile phones are subject to the same types of malware as their much larger computer predecessors and the lack of information security demonstrated by the average user of these mobile computing devices subjects a large amount of users and personally identifiable information subject to release into malicious hands. While user education and safe browsing practices will certainly help, vendors and designers of mobile applications could probably assist in the malware fight by cutting back on bleeding edge releases of certain software packages and subjecting software to a higher degree of examination and testing. In the end, the responsibility and liability falls to the user to properly handle their devices and information.
REFERENCES


