Aditya K Sood* and Richard Enbody**

*Founder, SecNiche Security
**Associate Professor, Department of Computer Science and Engineering, Michigan State University

Information Security »

Chain Exploitation—Social Networks Malware

Social networking has completely transformed social life in the online world. It has become the most acceptable pattern of forging social connections on the web. Every new development has pros and cons in its own sphere, though, and social networking web sites are no different. Online social networks, being a part of the Web 2.0 world, are prone to attacks and malware infections.

Social networks, such as Facebook, Twitter, MySpace, Orkut, and Friendster, pose a grave threat to the security and privacy of users. This article discusses malware infection strategies used by attackers to infect social networking web sites and addresses security from the user perspectives—outlining effective, secure steps that can reduce the impact of malware infections.

Social Networks and Infection Model

With the growth of new technology trends, the online world has noticed an explosive growth in social networking. The definition of social culture has changed with the social networking revolution. The process of developing social relationships among individuals has become easier through social web sites. Recent developments in social networking have transformed the world from a social perspective; however, this new type of socializing has raised concerns about the privacy and security of Internet users.

The concern for security and privacy go hand in hand. Social networking poses an extensive threat because it is a technology-dependent culture. In general, social networks are pool networks because of the interconnectivity among various participating elements. In a real-world model, these elements are the actual users in an online network. Social networks are an ingrained part of the World Wide Web; however, they are not completely protected from various web attacks that are executed to spread malware across the web. The threat models of regular web applications and social networking web sites are similar. Social networking web sites require an appropriate security control to preserve the privacy, security and integrity of users. The model presented in Fig. 1 gives an idea of the web malware infections in a social network. The black nodes represent the users in the social networks who have interrelations. In general, it shows the interconnectivity patterns.

Broadly, this model suggests the chain infection process in a social network. The risk of infection is high because of the interrelationships. Therefore, an infection in one node can impact all of the other nodes that are interconnected with the infected node. For example, one malicious user profile in a social network can infect the other user profiles that share a mutual connection.

Recently, there has been an increase in web malware and spam[1] activities because social networks can be used to support these attacks. Social networking web sites are acting as powerful magnets[2,3] that attract fraudsters. Social networking worms such as Koobface[4] and the Twitter worm[5] have already shown their devastating nature. Primarily, the social networking worms exploit a Cross-site Scripting (XSS) vulnerability to include malicious scripts from third-party domains. XSS worms are self-replicative in nature and spread rapidly on social networking web sites because of the interconnection among various profiles. This type of malware infection is termed a chain infection because one malicious node infects another. In general, the default design of social networking web sites is exploited to conduct attacks and spread malware.

Techniques of the Trade

The following infection strategies are utilized by attackers to spread malware through social networking web sites by taking advantage of user ignorance.

Malicious Profile Generation

Social networks are based on the concept of online identities that interact together to form a virtual social network. The identities are created as user profiles that reveal the kind of information the user wants to display on the social network. It is hard to set an appropriate control on user profiles that can secure the identities completely; however, some standard controls have been defined by social networking web sites to prevent users from performing unwanted operations and to secure users by restricting the flow of information. This process is effective to some extent, but an attacker exploits the inherent nature of social networks to tempt users to perform illicit operations on the social network.

One of the most common techniques used by attackers is generating fake profiles. These profiles can be of celebrities, models, advertisements, etc. Fake profiles can be used for many purposes including monitoring users, revenge and business.

The fake profiles tempt users to read the malicious content that is posted on the messaging walls used for communication. Once users visit such profiles, embedded malicious codes start infecting the users with malicious executables.

From a security perspective, this is a clear case of identity theft in social networks, and the type of information present in fake profiles is used in a plethora of scams. Moreover, it is difficult to discount the fact that the malicious scams are uncontrollable. Facebook, Twitter and MySpace users, for example, have been victims of these kinds of scams and identity frauds because it is hard to restrict the functioning of users based on identity profiles in the network. This is the inherent vulnerability of social networks. Social networks are adding secure protocols for automatic detection of these

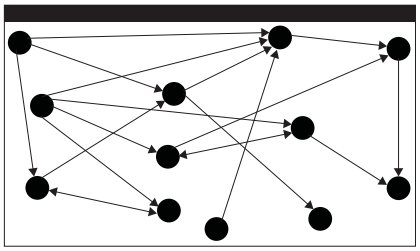

Fig. 1—Infection layout in a social network

malicious fake profiles, but the protocols are not robust enough.

Exploitation of "Social Human Touch"

"Social human touch" is an outcome of relationships among various online identities in social networks. It is defined as the trust between engaged profiles and the kind of social bond shared by them in a network. Social human touch and ignorance are two faces of an active entity, i.e., user identity in social networks.

Exploitation of online social trust is considered an entry point of malware infections. For example, by an attacker's use of spam, a user is directed to a fake profile that uses hyperlinks to redirect the users to the malicious domain. The rogue profile tempts users to visit that domain by presenting them with an attractive slogan, advertisement or caption. For example, a slogan stating "Click here for a new video release from the world's most famous musician" may entice users to visit that link. The music file starts serving malware while playing. The authors' research has shown that music players, such as Windows Media Player, and QuickTime Player, can be used to hide malicious code that acts as a backdoor for spreading malware to users. It is not possible for attackers to spread malware directly, but they play around with the psychology of legitimate users to exploit users' ignorance, thereby serving users with an unwanted gift in the form of malware and controlling users' machines afterward.

Worm Generation—Chain Infection and Reaction

Social networks have become the most susceptible platform for spreading malware. Worms exploit the nature of social networks because of the interconnection among legitimate users. Attackers follow the process of chain infection and reaction to trigger malware through worms. It can be devastating because exploitation of interconnected identities results in a diversified infection. While encountering malware on a day-to-day basis, a generic model has been designed to understand the working of worms that infect social networking web sites on a large scale. It can be explained in two steps:

1. The first step of this model involves the initiation of a malicious node that starts infecting the chain. In this type of level 1 infection, attackers try to find a legitimate user in the social network to set a base for infection. At this point, the infection is dedicated to that user only and is persistent in nature. The prime aim is to serve malware to that user continuously. Successful exploitation results in the downloading and installation of malware onto the user's machine. Primarily, the browser plays a critical role in this. Once the malware is installed in the system, it converts the system into a zombie or bot with backdoor access and generates a specific type of interface with the browser. The malware tracks the user's Internet activity and waits for the right network to start the chain infection. It not only steals the information from the victim machine, it also starts doing operations on the behalf of the victim. The infected victim machine is treated as the first node in the infection chain.
2. The second step occurs after the infection node is created. The malware waits for the user to visit and log in to a specific social networking web site. Once this occurs, the malware starts reacting. Without the user's knowledge or consent, it starts posting messages to contacts that are part of the user's social networks. This happens through the browser because malware sends a request automatically from the background, and the browser executes it in the context of an active social networking web site. When the user logs in to the web site, malware utilizes the already given access rights to infect the profiles connected to the user. As a result, the infection chain begins to flourish. All the secondary nodes become zombies and then start infecting the users who are connected to their specific social network. This process keeps on iterating and gives birth to botnets, which are networks of bots interconnected to spread malware and steal critical information. A number of profiles become nodes of this chain and keep on performing the infection and reaction operations.

The two-step infection can be mapped as one to many (1:N). Once the chain is created, it becomes prevalent and infection keeps increasing, not only at the system level but also through the World Wide Web—especially social networks.

Drive-by-Download Attacks

What happens exactly when a user visits a malicious link?

This can be explained by understanding Drive-by- Download[6] attacks. This attack is used heavily to "fingerprint" the victim browser and serve malicious executables. Drive-by-Download is defined as an attack in which a user's browser is exploited and malware is downloaded into the victim's machine without the consent or knowledge of the user. Everything happens automatically, but it is not as easy as it may seem. The malware domain fingerprints the type of browser used by the user, and based on that information, a specific exploit is served. This is done to ensure reliability. For example, if a user is running version7 of Internet Explorer (IE), the malware domain scrutinizes the version through user agent strings and serves the requisite exploit for the same version. The victim browser will not be served with an exploit if a different version of IE is running in the user environment. This methodology is used by attackers to control the infection process so that detection becomes difficult. Obfuscation techniques used by attackers may result in bypassing antivirus solutions so that malware remains undetected.

As mentioned previously, hyperlinks are used to embed the content in malicious profiles. The hyperlinks are injected using hidden inline frames (Iframes) and Document Object Model (DOM) injections. Iframes are used to render third-party content into parental web sites, and DOM is a cross-platform, independent representation of Hypertext Markup Language (HTML) objects. However, DOM uses JavaScript to trigger inbuilt calls in a browser for interaction among static and dynamic HTML and JavaScript objects, respectively. Attackers use the inbuilt functionality of browsers,

"Social networks have become the most susceptible platform for spreading malware."

such as Iframes and DOM, collectively, to conduct Drive-by-Download attacks. When a user visits those links, fingerprinting is done and malware is served. Drive-by-Download attacks are used on an extensive scale to infect large sets of victim machines by exploiting vulnerabilities in browsers and web sites. Drive-by-Download attacks are pervasive and are conducted in a stealthy manner to trigger infections. Social network malware utilizes this type of infection pattern on a large scale.

Exploitation of Custom Code and Social Networking APIs

The release of open application programming interfaces (APIs) by social networking web sites has completely transformed the realm of malware infections. In general, these APIs are used for customizing and designing applications that use social networking web sites to execute their content, meaning that a user can design a custom code to derive an interface with social networking web sites. The deployed custom applications can be accessed by a number of identities present in the social networking web site. Attackers design malicious applications using APIs to conduct attacks in a sophisticated manner by exploiting the generic design of an application development model, which makes the malicious applications look authentic.

Once the malware-driven application is accessed, APIs can be used to introduce malicious content into social networking web sites. Usually, the designed application has hidden links to the malware domain. The application remains persistent and becomes active when a user accesses any module for performing a specific set of operations. Many of the methods discussed previously can be used directly in this way.

Malicious applications can have disastrous impacts. The risk of malware infection is high because a social networking web site is a shared environment. Once a link is clicked, the payload (a malicious code in the form of JavaScript) from the third-party domain is executed in the user's browser and the infection starts. Attackers perform a number of social identity attacks and privacy hacks to extract more information about the users. It is possible to gain access to sensitive information by executing browser-based attacks through a malicious application. For example, bookmark attacks are primarily executed against social networking web sites with the intention of stealing information. Of course, this is a browser-dependent attack, and inevitably, the rate of exploitation is dependent on the specific browser's design, functionality and inherent vulnerabilities. Control is transferred either to the third party, or it can be a part of user-generated content. It is hard to trust user-generated content because it is not known whether the content is malicious or not, i.e., it may contain any type of code based on the intentions of the user.

Facebook Markup Language (FBML)[7] is used to provide a custom control for generating content. This language has been used to spread malware; however, Facebook allows custom applications[8] to be designed and hosted on one of its subdomain servers. This functionality has been used by attackers to host rogue applications on the Facebook domain to serve users with dedicated malware.

Exploitation of URL Shorteners and Hidden Links

Although URL shortening services[9,10] are used for URL optimizations in which a URL is compressed, this same tactic has been adopted by attackers to fool users because it is difficult to determine the actual URL of a compressed URL. Social networking web sites have adapted this functionality, and one can find shortened URLs on a day-to-day basis. This has become a problem, though, because attackers are utilizing these services to hide malicious links as part of the compressed URLs—users can be fooled without much complexity. As a result, phishing has become stealthier and the inherent redirection spreads malware at a more rapid rate.

Risk at Stake

As discussed previously, it is hard to make social networks completely secure. The potential risk of spreading malware is ever increasing.[11] The major factor that contributes to this process is user ignorance regarding the technology used on social networking web sites.

The threat factor becomes high when user ignorance combines with the tactics presented. As a result, user privacy and information are at high risk. Identity scams may not only result in reputational damage[12] to an individual online, but they may also influence the stature of an individual's "offline" social life.

Social networking web sites can apply controls to a certain extent, but it is difficult to provide knowledge to users about the authenticity of the hyperlinks posted to the messaging walls of their profiles. Theft of sensitive information and data can result in credit card frauds and unwanted banking transactions. The risk of compromising the user systems becomes high when a malicious binary is downloaded by clicking a hyperlink on a social networking web site. The infection entry point is the social networking web site; the infection then penetrates the user machine. The risk increases based on the user environment, such as a home personal computer (PC) or an organization-owned machine.

Organizations that use social networking web sites to advertise their products are also at a high risk when a worm outbreak occurs to spread malware across a social network, which could result Organizations that in the defamation of the use social networking organization's brand and can hamper the business to a wider web sites to advertise extent than expected. The risks their products are also posed by social networking web at a high risk. sites are becoming harder to conquer.

"Organizations that use social networking web sites to advertise their products are also at a high risk"

Recommendations and Usability

Considering the nature of web malware in social networking web sites, it is hard to make the networks foolproof. However, the impacts can be reduced to some extent by complying with the following recommendations:

- Users should educate themselves to identify fake profiles and phishing e-mails. This kind of attention requires a collaborative knowledge of technology and its applicability in social networking web sites.
- Users should secure their browsers by installing appropriate client-side

filters, such as NoScript in Mozilla, to nullify the malicious scripts when rendered in browsers. Users should choose client-side filters that are appropriate for their browsers.

- Users should not click suspicious hyperlinks. Users should try to scrutinize the origin of hyperlinks on social networks to avoid traps.
- Users should configure their profiles by applying the appropriate restrictions provided by standard social networking web sites to protect privacy.
- Users should report suspicious messages and e-mails directly to the security teams of social networking web sites. This can help administrators apply filters on the web-based social network infrastructure.
- User systems should have requisite antivirus software installed with the latest signatures to thwart infections.
- Users should upgrade their operating systems with the latest patches to avoid the exploitation of vulnerabilities in various components of installed software.

Conclusion

Social networks have given birth to new types of elemental relations among various entities in the online world. The social networking world is virtualized in nature, but it has real-time impacts on the lives of individuals. Since these networks are part of the online world, they are not untouched by the threats and flaws present on the World Wide Web. Security and privacy are considered basic elements for effective social networking; however, the aim of web malware is to infect users and steal information by exploiting various vulnerabilities through attacks in social networks. User ignorance is a big factor in the spread of malware and is quite hard to patch. It is hard to expect robustness from a user's perspective; rather, it has to be an inbuilt nature of social networking web sites.

References

[1] Sophos, "Malware and Spam Rise 70% on Social Networks, Security Report Reveals," UK, 1 February 2010, *www.sophos.com/pressoffice/news/articles/2010/02/ security-report-2010.html*

[2] Gallagher, Sean; "Social Networks a Magnet for Malware," *InternetNews.com*, 17 February 2009, *www.internetnews. com/bus-news/article.php/3803051/Social-Networks-a-Magnet-for-Malware.htm*

[3] Miller, Chuck; "Malware Most Potent on Social Networks," *SC Magazine*, 12 May 2009, *www.scmagazineus.com/ malware-most-potent-on-social-networks/article/136659*

[4] Ferguson, Rik; "New Variant of Koobface Worm Spreading on Facebook," *TrendLabs Malware Blog*, 1 March 2009, *http://blog.trendmicro.com/new-variant-of-koobface-worm-spreading-on-facebook*

[5] Miller, Chuck; "Twitter Worm Underscores Social-networking Vulnerabilities," *SC Magazine*, 13 April 2009, *www.scmagazineus.com/twitter-worm-underscores-social-networking-vulnerabilities/article/130562*

[6] Howes, Eric L.; "The Anatomy of a 'Drive-by-Download'," *www.spywarewarrior.com/uiuc/dbd-anatomy.htm*

[7] Facebook developers, "Facebook Markup Language (FBML)," Facebook, *http://developers.facebook.com/search?q=FBML*

[8] Facebook; "Application Directory," USA, *www.facebook. com/apps/directory.php*

[9] bit.ly, USA, *http://bit.ly*

[10] Tiny.cc, *http://tiny.cc*

[11] *Op cit*, Sophos

[12] Visit Vail Valley Blog, "Sherman & Howard Business Law Advisory: Internet Employment Scams Jeopardize Both Employers and Prospective Employees," Vail Valley Partnership, 17 August 2010, *http://blog.visitvailvalley. com/public/blog/258101av*

About the Authors

Aditya K Sood has more than five years of experience in computer security and has worked in the security domain for Armorize, COSEINC and KPMG. He is founder of SecNiche Security, an independent security research firm. Sood has been an active speaker at various conferences, has written content for numerous journals and magazines, and is a Ph.D. candidate in computer science at Michigan State University (USA). Sood can be contacted at adi_ks@secniche.org.

Richard Enbody, Ph.D., is an Associate Professor in the department of computer science and engineering at Michigan State University. His research interests include computer security, computer architecture, web-based distance education and parallel processing. Enbody has two patents pending on hardware buffer-overflow protection that are intended to prevent most computer worms and viruses. He is the coauthor of The Practice of Computing Using Python.

Please note that cover themes of future issues of CSI Communications are planned to be as follows -

- July 2013 - e-Business/ e-Commerce
- August 2013 - Software Project Management
- September 2013 - High Performance Computing

Articles and contributions may be submitted in the categories such as: Cover Story, Research Front, Technical Trends and Article.

Please send your contributions before 20th of a month for consideration in the subsequent month's issue.

For detailed instructions regarding submission of articles, please refer to CSI Communications March 2013 issue, where Call for Contributions is published on the backside of the front cover page.

[Issued on behalf of Editors of CSI Communications]