Marshall Eddy

CS331-001

Vincent Skimmer

7 November 2016

Malicious Code and Activity

Installed/Injected by Remote Attacker is a type of attack that is accomplished by a perpetrator with access to internal operating systems from an external source. It may be accomplished by exploiting vulnerabilities that allow remote command execution via exposed software (SQL injection into web URLs). It may also be accomplished via commands issued by malware via remote perpetrator command and control interfaces.

Phishing techniques originally were used to impersonate a bank or other institution with which a user may have an account, and encouraged the user to click a link in the email that would bring them to a site that looked like their banking site, but was actually fake. That site would either directly collect credentials, or download malware that would later collect them. As less easily detectable techniques for installing malware have been developed, random phishing techniques for malware propagation have become less common. Nevertheless, these techniques still exist and are increasingly customized as part of an overall campaign of attack.

The web is a popular attack vector for the simple reason that its use is ubiquitous. Malware injection processes that are generally classified as auto-infection occur without any overt action on the part of the user, such as inclusion of malware that automatically exploits a browser vulnerability. The propagation and infection both occur without the user’s active participation or knowledge. Malvertising, the practice of placing malware in fake (or real) online ads, is also an increasing source of auto-injection attacks [30]. Malware operators may place ads with links to malicious sites in order to spread malware or the ads could also contain scripts which execute code on the PC. High default trust settings on browsers and users operating with administrative privileges increase the effectiveness of this attack vector, which is enabled via a combination of vulnerable software and infected websites. These websites may be owned and operated by criminals, yet not conspicuously enough to be blocked by commercially available security services. They are often legitimate sites on which criminals have installed malware propagation code. Figure 8 provides an example of the types of software and search engines that are common delivery mechanisms for auto-injection attacks. It identifies the percentage of attacks per source in customer traffic observed by Cisco.

Malware writers use creative methods to lure random users into executing malicious injection code. Drive-bys can happen by simply visiting a compromised or malicious website, viewing an email message and also by clicking on deceptive pop-up windows. Many of the latter incorporate a social engineering aspect to persuade the user to follow a malicious link. (For example, a pop-up that reads, “You are infected with a virus, click here to clean your system!”).

In any of the above attack vectors, malicious software may be planted within the internal network. Although most FIs block most inbound traffic, it is rare for a commercial institution to block outbound web browsing. Malware with command and control capabilities will often connect back to the malware operator’s site using common browsing protocols, and this allows malware on the internal network to receive both software and commands from the outside. Bots will often be equipped with multiple URLs so that if a malware operator site is taken down (whether due to maintenance or by law enforcement), another will be contacted which will have the same ability to issue commands to bots. Data collection networks are supported with a large number of proxy servers configured to relay data to the malware operator and to update bots with new addresses for data collection servers as the malware network evolves (nist.gov).

Social media is a generic term for Internet sites that allow users with similar interests to create web content in a collaborative manner. Examples of these sites are Facebook, Orkut, Hi5, MySpace, LinkedIn. They are also generically referred to as social networking sites, as the groups of people that collaborate on any one site are called a social network. With the increasing popularity of social media and the large communities of Internet users that it attracts, social media sites have become fertile hunting ground for malware operators. Social media applications include functions that open communication channels with friends and acquaintances, and allow users to develop networks of people with like interests. It relies, for its operation, on trust between users. Whether or not a user on a social networking site has ever met the people with whom they communicate in person, there is an assumption that the people in a social network are friends rather than foes. The Internet provides a cloak of anonymity for people with malicious intent and allows them to use social media to masquerade as friends.

References

[www.nist.gov](http://www.nist.gov)