Boost Security in 3 Areas to Thwart Malware and Hackers

Recent electronic intrusions in some of the most well-known retailers have caused business owners around the country to question whether or not they are susceptible to cybercriminals, and what they can do to protect themselves. It is sometimes difficult for those charged with securing a Point of Sale (POS) system to know where they should focus their attention. While standards like the Payment Card Industry Data Security Standard (PCI DSS), have numerous requirements that when followed will have a positive impact on security, it can be overwhelming to start with such a large multi-faceted approach.

Holistic security should be thought of as a continual process. The concept is simple - Protect against the most prevalent threats first, and then concentrate on increasing security to address other attack vectors which are not as frequently encountered (yet are still effective). By taking this approach, meeting the requirements of a standard such as PCI becomes much less daunting. With this in mind, it is clear that the largest breaches in history relied upon malicious software, a.k.a. malware. It is therefore important to concentrate on security measures which can effectively inhibit the installation and communication of this kind of software. The following paper includes the three most critical security elements on which a retailer should focus to prevent malware from stealing data. Additionally, we provide a description of the Netsurion services that can assist in this overall endeavor.

1. Protect a Location from Incoming Internet Traffic

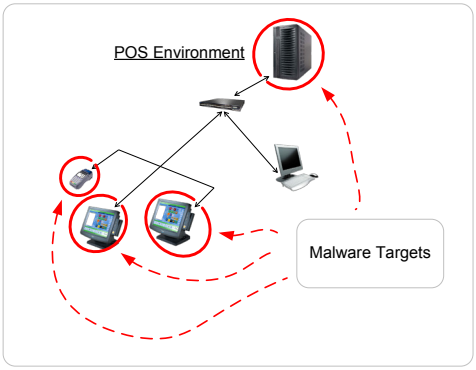
The first step in stealing data with malware is finding an avenue into the targeted business so that malware can be installed. This leads to several practical components of the POS environment that must be protected. The Internet connection used to process

credit cards must have adequate protection so that incoming traffic is thwarted and remote access is managed in such a way that unauthorized personnel cannot gain access into the network.

Netsurion provides the first line of defense in keeping hackers out of the POS environment. Using our managed firewall service known as ***Global Security MeshTM***, our centralized control of security known as ***IP Data BlockerTM with DNS Blocking***, and our ***2 Factor Secure Remote Access SSL VPN*** that includes a built-in security validation engine known as ***Forced Configuration Manager,*** Netsurion protects retailers from Internet intrusions.

2. Harden POS Systems So That They Cannot Be Infected with Malware

If a hacker manages to get malware through your outer defenses as described in #1, then the next step in stealing credit cards is to find a vulnerable system in the POS environment that can run the malware intended to gather the desired data. If a hacker cannot find a station that will allow him to install the malware, or if a retailer catches the installation before it can do any damage, then credit cards will remain secure. It is for this reason that PCI spends so much time on the internal processes and security of the POS stations.



Netsurion helps merchants with protecting their internal systems by providing a comprehensive ***Security Policy and Procedure Template*** which is included in all packages that enumerates clearly what should be done to protect the POS environment. Furthermore, Netsurion supplies a ***Penetration Testing Guide*** which is included in the Titanium Secure Package (or can be purchased separately), so that the environment can be properly examined annually to verify that the expected security is still in place. From a more proactive standpoint, Netsurion has a software client called ***LANScribe*** which is included in the Titanium Secure Package (available for purchased separately), which automatically gathers relevant security information such as unexpected software installations, and allows a merchant to look at their security notifications from the convenience of Netsurion's web portal. Netsurion

"Secure" package solutions also include an ***Internal Vulnerability Scan*** that runs automatically without any additional hardware or software installation so that system weaknesses can be addressed before a hacker tries to take advantage of them and install malware. Lastly, Netsurion will work with you to segment your network to the degree that is acceptable for the way that you do business. If the point of sale environment can be isolated, then the ability to limit access to it and monitor its activity becomes much easier to manage and more secure by an order of magnitude.

3. Manage Outbound Traffic to Prevent Data Exfiltration

Even if the first two areas of security fail, you can still prevent hackers from successfully transmitting credit cards using malware if you have a solid network security profile that limits traffic from within the POS environment to the Internet. This is similar to the first item listed above, but this time the data is being blocked from leaving the POS environment and traveling to the Internet.

Netsurion's managed firewall service, ***Global Security MeshTM***, and our central control of security policies, ***IP Data BlockerTM with DNS Blocking***, are once again key elements in protecting a POS environment. In this case, unauthorized traffic is denied access to the Internet, and malware that tries to send this type of data will be logged by the firewall. Once the malware fails to send the data through the Netsurion firewall with enough frequency, our engineers who are looking for the anomalous log traffic that indicates malware activity will flag that location and instigate a trouble ticket so that the offending software can be eliminated before it can do any harm.

In conclusion, it is important to remember that malware is currently the most common method that hackers use to steal data from retailers. It is therefore important to increase the security in a POS network that will most effectively block the communication or prevent the installation of this software. Preventing hackers can be thought of as an electronic arms race. The weapon of choice used by criminals today is malware. By understanding this, it is possible to plan an effective defense.

7324 Southwest Freeway
Suite 1700, Arena Tower II
Houston, Texas 77074

P: 713.929.0200
F: 713.541.1065
Netsurion.com