LED Digital Signage Cyber Security Topologies and Vectors of Cyber Attack

Sean York[1] and Cheng Qian[2]

***Abstract*— LED Digital Signage or Digital Billboards have proven to be attractive targets of Cyber attacks and hacking. Proper network design with a security perspective can protect your investment and prevent these attacks from having any effect. This whitepaper describes two different configurations used by Media Resources, one supporting protective measures around a basic static IP setup, while the second describes our Virtual Private Network (VPN) solution. In addition, the whitepaper lists some of the common vectors of attack to provide the reader an enhanced understanding for digital signage cyber security.**

I. INTRODUCTION

Protecting the access to your LED digital signs while they operate over a wide-open internet comes with its own set of unique challenges. There are many known instances of hackers or deviants breaching the security of these displays and showing unwanted or offensive imagery, damaging the reputations of the display owners and the industry as a whole. In other situations, attackers simply spammed the devices and drove massive data consumption charges with customer ISPs.

While there are many best-practices with regards to securing your LED sign assets physically, and operationally (such as from former employees), this document will describe some common avenues of Cyber attack and the configurations employed by Media Resources digital displays that keep them safe.

II. STANDARD CUSTOMER-SUPPLIED INTERNET CONNECTIVITY

This is the most common standard configuration shipped to customers, and allows maximum versatility to modify for most customer's needs. It also balances a good level of security with minimal setup for each display project. In this setup, the main point of entry to the sign is via the Sierra Wireless Gateway Modem configured with a static IP assignment from the Internet Service Provider (ISP). Since this setup has the modem facing the internet directly, we prevent intrusions by a combination of methods:

- minimize port forwarding on devices,
- not respond to ICMP requests,
- only allowing white-listed IPs to connect,
- disable listening on all commonly targeted ports by default (i.e. http, ftp, ssh, and VNC ports)

[1]Sean York is the Manager of IT of Media Resources Inc. s.york at mediaresources.com

[2]Cheng Qian is the Chief Product Architect of Media Resources Inc. c.qian at mediaresources.com

This minimizes the risk of an attacker being able to connect to the devices and on the occurrence a device is connected to, we block any brute force attackers by having a strong password scheme (capable of resisting a dictionary attack) in place. This is the best method to have your sign online without the use of a dedicated VPN. The majority of any remaining risk factors will be human error driven, such as phishing scams, downloading of malware, or through other types of social engineering. Fortunately, these risk factors are mitigated by Media Resources' standards of operation, where player PCs are not human-user operated such that the impacts of human error is minimized.

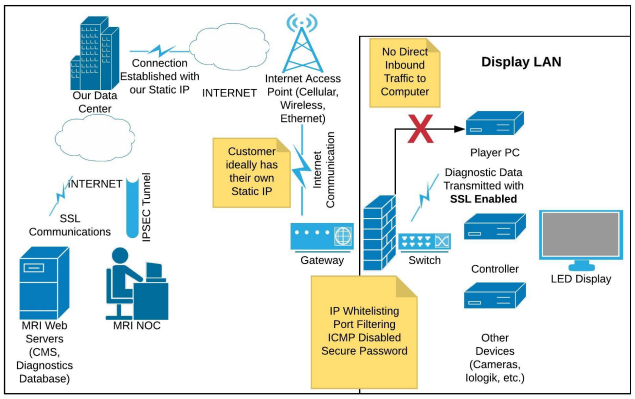

Fig. 1. Standard Configuration for Customer-Supplied Internet Connectivity Using a Basic Static IP Setup.

We describe the types of threats and their protection below:

A. Unauthorized VNC Remote Desktop Access

The most common digital billboard hijacks that resulting in lewd images being displayed were based on remote VNC connection into the displays. In the case that a display gateway resides on the internet on a static IP, and the player PC responds to VNC requests, and the password is not sufficiently strong, an attacker on the internet can eventually gain remote access into the player PC.

All of the security features in our standard configuration act as a barriers to prevent this type of attack and we are confident that this vector of attack is not possible on our displays.

B. Malware

Malware that is downloaded onto the computer can give a hacker an avenue to remote into the computer.

This configuration provides partial protection as the Player PC is embedded within the display and does not have day-to-day users who are liable to human error.

C. Phishing

Untrained users can accidentally give cyber attackers information pertaining to the device such as passwords and IP addresses.

Ensure that access to passwords and IP addresses only reside with qualified technical staff who are less likely to be phished, and issue (and revoke) temporary passwords wherever possible when giving access to persons outside your direct control.

D. Man-In-The-Middle

Also known as an Eavesdropping attack, the attacker tries to use broadcasted unencrypted traffic on a network as an avenue to gain important information such as IP addresses or passwords.

Encrypted Traffic such as SSL prevents this scenario from happening, thus the MRI standard configuration is protected. However, the displays should still be put on a VLAN if used on another local network.

E. DDOS

Distributed Denial of Service attacks occur when an attacker floods an end-point with requests (such as ICMP, Ping-of-death, etc).

The display networks are partially protected via IP whitelisting which ignores incoming traffic, unless the attacker simultaneously employs IP spoofing. Fortunately IP spoofing requires prior knowledge of whitelisted IPs, and the white list of IPs should be kept to minimum outward distribution.

F. Exploits in Hardware

An attacker may use yet to be known or known methods to get into a device. These scenarios are generally avoided by keeping network devices up to date. Media Resources maintains a regular pulse on new vulnerabilities through our subscriptions to hardware manufacturers providing networking equipment, such as Sierra Wireless.

G. Password Brute Forcing

Also known as a Dictionary Attack. An attacker spams widely used passwords, or sequentially tries (with an automated script) different combinations or words that frequently occur.

We are well protected against this by having all strong passwords on all externally accessible password prompts. Internal password prompts are completely inaccessible due to white-listing, and the configuration of key devices (such as the player PC) to simply never respond to incoming requests of any type.

H. IP Spoofing

The attacker pretends to be a friendly IP with hopes of gaining entry to the device.

They need to have knowledge of a valid IP, which cannot be discovered through the internet if the traffic is encrypted through SSL. The specific white-list of IPs should also be carefully managed so that it is only available to cognizant and responsible personnel. In the worst-case scenario that the IP white-listing is defeated, an attacker is still faced with secure passwords and lack of response from the player PC. In this way, even if the IP spoofing is successful, the attack is still unable to take over the PC or the content that is shown the display.

III. Advanced Cellular Configuration With Virtual Private Network

For customers who operate large networks, or opt to use the full Media Resources suite of hardware and services including our cellular service, we offer an enhanced configuration package. This is based on a Virtual Private Network (VPN) delivered through the cellular service provider, with access only through managed firewalls and IPSEC tunnels. In this way, the signage network is isolated and the potential points of vulnerability are significantly reduced. Please see Figure 2 for the topology.

VPNs are the current gold standard for securing remote corporate network sites, and the same standard applies for digital billboards. See Figure 2. for a diagram of the MRI implementation of cellular VPN.

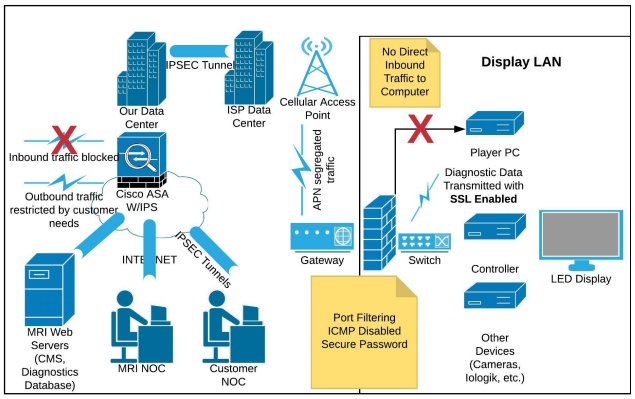

Fig. 2. Media Resources Standard Cellular VPN Option.

This is the preferred method of connecting your sign to the internet. We connect the device to our Internet of Things (IoT) network which is tied to our own and very secure Access Point Name (APN). All access to the APN is achieved by secure IPSEC tunnels; there are no inbound routes outside of the IPsec tunnels to gain access. All internet traffic is subject to the rules of our firewall, blocking all inbound traffic and actively blocking/monitoring for unapproved outbound http transport traffic. Our restrictive firewall keeps your sign very protected and restricts traffic to only what you need to accomplish with the sign, i.e. publish content and monitoring.

This not only actively blocks malware threats, but also helps keep data consumption to a minimum.

Due to the extra security provided by this method, it does have some caveats when it comes to third party integration. Since it will not allow for a user to directly connect into the remote systems (with exception of NOC teams), you can only use content management systems (CMS) that are http client driven. You will not be able to use any CMS that are push/server driven.

This method effectively addresses all of the potential attack vectors described in section 2.

IV. CUSTOMER DEFINED TOPOLOGY

While Media Resources has its own standards for implementation of network and security features, we recognize the need for customer-specific network integration, especially with customers that have functional Network Operations Centers. Media Resources is always happy and willing to create a custom configuration or work with the IT and NOC teams of our customers. We are additionally open to the review, customization and testing of our network systems to meet compliance or specialized security needs. If you should have any IT or security related questions, please feel free to reach out to either author of this whitepaper.