CIS CYBER ALERT

To: All MS-ISAC and Fusion Center Members
Date: June 3, 2014
Subject: Malicious Cyber Actor Targeting Electronic Road Signs in Multiple States

The Center for Internet Security (CIS) has confirmed that a malicious cyber actor compromised 11 electronic road signs (aka Dynamic Message Signs) in three states between May 30 and June 1, 2014. The actor posted messages on the road signs stating the signs were hacked and in at least one instance invited drivers to interact with him through Twitter.

- Investigators in one state believe the compromise may be in part due to the use of weak Simple Network Management Protocol (SNMP) community strings. Investigators in another state believe the malicious actor used Telnet port 23 and a simple password cracker to gain remote access.
- In one state the malicious actor changed the modem passwords, forcing technicians to restore to factory default settings to regain access.
- The malicious actor targeted Daktronics controllers in at least two of the states.

The malicious actor appears to be a Saudi Arabian actor who is also responsible for a couple of structured query language (SQL) injection (SQLi) compromises of databases in foreign countries over the past several years and has demonstrated an interest in the "Internet of Things" by posting compromises/instructions on compromising light bulbs and car radios, in addition to the road signs. CIS does not believe he is affiliated with any know hacktivist or actor group.

Modifications to electronic road signs are common and generally display messages meant to entertain drivers, such has "zombies ahead." However, changes to road signs create a public safety issue because instead of directing drivers through road hazards they often result in drivers slowing or stopping to view the sign and take pictures.

This activity likely coincides with the May 27, 2014, release of the video game "Watch Dogs," in which game play revolves around "hacking," with a focus on hacking critical infrastructure-based electronic devices in particular. Watch Dogs allows players to hack electronic road signs, closed circuit television cameras (CCTVs), street lights, cell phones, and other systems. On May 27, 2014, the malicious actor posted an image of the game on his Twitter feed, demonstrating his interest in the game, and the compromise of road signs occurs during game play. **CIS believes it is likely that a small percentage of Watch Dog players will experiment with compromising computers and electronic systems outside of game play, and this activity will likely affect SLTT government systems and Department of Transportation (DOT) systems in particular.**

Recommendations:

CIS suggests implementing the following recommendations for all remote DOT equipment, including roadway cameras and traffic signals.

- Use strong, complex passwords on all electronic road signs.
- Change all SNMP community strings from the default (typically "Public" or "Private") upon receiving the equipment.
- Disable the web interface and telnet functionality. Close all open ports, where possible.
- If SNMP is not used, disable it. If it is used, consider disabling the RW (Read-Write) password for SNMP. If not possible, ensure it uses a strong, complex password, different from the RO (Read-Only) password.

- If possible, use SNMP management stations so changes may only be made from pre-defined addresses.
- If possible, upgrade to the most current version of SNMP (currently version 3).
- If possible, place all road signs on a secured WAN.
- If possible, enable remote logging of all changes and monitor the logs.
- As many road sign defacements appear to be the work of local actors, ensure control panels are secured with a strong lock and access to the programming functionality requires the use of a strong, complex password.

Please report any activity targeting traffic infrastructure or possibly inspired by the Watch Dogs video game to CIS.

Center for Internet Security
Multi-State Information Sharing and Analysis Center
31 Tech Valley Drive
East Greenbush, NY 12061
518-266-3488
7x24 SOC 1-866-787-4722