Cybersecurity Recommendations for High-Profile Events — Cyber Advisory

Criticality:Yellow:Moderate — **August 23, 2018**

Summary	High-profile events, such as visits from politicians and dignitaries, major sporting events, and VIP funerals, often attract protestors and other threat actors who may attempt to disrupt or exploit the event. This advisory describes some of the potential cybersecurity threats, attack vectors, and mitigation considerations for high-profile events.
Criticality	Criticality is ***low-moderate***, based on historical incidents and the current political climate.
Likely Threat Actors	Traditionally, hacktivists are the threat actors who are most likely to conduct cyber attacks in response to a high-profile event. A hacktivist is an individual or organization that "hacks" for political or ideological reasons. They usually attempt to disrupt victim operations and/or gain publicity for their causes. Hacktivists rarely have sophisticated skills or significant resources. They take advantage of easily exploitable vulnerabilities (such as SQL injection to download information from databases) and readily available hacking tools.
Probable Cyber Threat Vectors	Listed below are the more probable cybersecurity threat vectors based on the experiences of prior high-profile events. Note that other attack vectors cannot be ruled out. • DDoS — Making computer systems unavailable through a distributed denial of service attack. • Defacement — Defacing a target's website to spread a message and/or to embarrass the target. • DOXING — Publishing private or identifying information about a particular individual on the Internet.
Types of Threats	In general, there are three types of threats: • Targeted Threats — A threat against a specific target, such as the Farm Animal Reform Movement (FARM) targeting the American Association of Meat Processors during their annual conference at Phoenix Convention Center. • Ancillary Threats — A threat against a secondary or "side" target, such as FARM's call to deface Phoenix restaurants' websites. • Cascading Threats — Domino or "ripple" repercussions of targeted and ancillary threats or cyber attacks, such as organizations canceling or moving their conventions out of Phoenix after a FARM hacktivist incident.

Recommended Actions	Listed below are recommended mitigations. **Prevent** • Apply all security patches to servers and end points (focus on web-facing devices). • Ensure anti-malware software is running and up-to-date. • Request/recommend employees remove identifiable information from social media accounts or review applicable privacy settings. • Implement multi-factor authentication for those with authorized access. • Consider or review DDoS attack mitigation tools. **Detect** • Establish, review, and maintain cyber threat information sharing channels, tools, and resources. • Monitor logs and network traffic for anomalous events and indicators of compromise. • Monitor anti-malware logs for indicators of enterprise-wide infections. **Respond** • Ensure incident response processes are up-to-date and alert key players to the potential risks. • Report/share suspected or confirmed cyber threat information to the ACTIC.
To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)
Resources	TrendMicro has a set of posters that describes how to identify indicators of compromise: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/empowering-the-analyst-indicators-of-compromise

Disclaimer	This information is provided for your situational awareness. Its purpose is to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.