Cybersecurity Alert for Malicious Activity	**Cyber Alert**
Criticality:Yellow:Medium	**02/02/2020 11:45AM** **Update: 02/04/2020 10:30AM**

Summary	An Arizona government entity experienced a breach on February 1, 2020. The threat actor gained network access via a vulnerability in the content management system used on government's web servers. The government's security tools detected and alerted them of the breach. The government implemented their cyber incident response plan, contained the incident, and is fully restored. No malware was found on their systems, and there are no indications information was exfiltrated. Update: This alert has been updated with additional information regarding the attack and indicators of compromise.
Criticality	Criticality is ***medium-high*** for those using the vulnerable software, based on the potential for harm; criticality is low for others. Note: See below for criticality criteria.
Details — Initial Compromise	The initial threat vector was a remote code execution vulnerability (CVE-2019-18935, published December 11, 2019) in Telerik, a user interface component widely used in web applications. Unknown to the government at the time, Telerik is an embedded component of Active Network, the content management system (CMS) used on the government's web servers.
Details — Privilege Escalation and Pivot	After gaining system access, the threat actor used the JuicyPotato exploit and Cobalt Strike penetration testing tool to escalate privileges and move laterally throughout the network. Reference: See "References" below for links to more information on the Telerik vulnerability, JuicyPotato exploit, and Cobalt Strike.
Details — Password Spraying	The threat actor moved beyond the web server trying to acquire additional credentials. At one point the attacker was able to build a list of all domain users and use a PowerShell script to password spray against all user accounts using the password "Winter2020." Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on.

<table>
<tr><td><b>IOCs — File Items</b></td><td>Listed below are the file-related indicators of compromise.
<table>
<tr><th>Filename</th><th>SHA1 Hash</th><th>Category</th></tr>
<tr><td>rundl1.exe</td><td>214a6e90a7dc35124717f47f75c684911d7d3d27</td><td>Cobalt Strike</td></tr>
<tr><td>JuicyPotato.exe</td><td>ec70dbe98d35611b3b55415b1f220780f8e56716</td><td>Local Privilege Escalation tool</td></tr>
<tr><td>grunt2.exe</td><td>d752ef374022636f6dd1ab6ff8dae7c28a5740d0</td><td></td></tr>
<tr><td>1580553305.4786427.dll</td><td>A60A7AEF8F83F7A5FAA01133493A5EB2964A92E7</td><td></td></tr>
<tr><td>1580553321.7575808.dll</td><td>493A11895F1DC3D7339531C22C6D29C7D46AAA05</td><td>Reverse Shell</td></tr>
</table></td></tr>
<tr><td><b>IOCs — Network-Based Indicators</b></td><td>Listed below are the network-based indicators.
<table>
<tr><th>NNBI Type</th><th>NBI Value</th></tr>
<tr><td>Domain</td><td>badgesforbullies[.]org</td></tr>
<tr><td>IP Address</td><td>50[.]63[.]197[.]203</td></tr>
<tr><td>IP Address</td><td>45[.]61[.]136[.]217</td></tr>
<tr><td>IP Address</td><td>209[.]188[.]18[.]200</td></tr>
</table></td></tr>
<tr><td><b>Details — Notification and Resolution</b></td><td>The government's security information and event management (SIEM) tool alerted them to the incident. The time from initial breach on February 1, 2020 at 03:37 to full containment at 05:45 was 2 hours 8 minutes.
In all, 33 servers were compromised. The government rebuilt all servers from clean backups and was back to 100% operational as of February 2, 2020 at 21:00.
As stated in the Summary above, no malware was found on their systems, and there are no indications information was exfiltrated.
As a precaution, the government reset all passwords.</td></tr>
<tr><td><b>Attack Motivation</b></td><td>Since the threat actor was making their way beyond the web server into the primary network, the assumption is that they were <b><i>not</i></b> looking to simply deface the government's websites.
The government shut down the threat actor while they were still working to establish a foothold on the network, so it is unknown whether this would have ended up being a data exfiltration or ransomware incident.</td></tr>
</table>

Suggested Mitigations	Important: Know whether your web (and other) applications use the vulnerable software. Telerik may be an underlying, embedded component. Listed below are a couple suggested mitigations. • As always, apply all security patches as soon as possible. • Implement the configuration changes Telerik released to help mitigate the vulnerability.
References	For more information, see • https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization • https://nvd.nist.gov/vuln/detail/CVE-2019-18935 • https://know.bishopfox.com/research/cve-2019-18935-remote-code-execution-in-telerik-ui • https://hunter2.gitbook.io/darthsidious/privilege-escalation/juicy-potato • https://github.com/ohpe/juicy-potato • https://attack.mitre.org/software/S0154/
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)

Criticality Criteria	Listed below is a general description of the criticality rating. The rating is subjective based on information currently known and the analyst's experience. • High / Red: The potential incident may impact or breach critical business, systems, and/or services without immediate intervention. There may also be indications that an attack is currently in process. • Medium / Yellow: The potential incident does not place an organization's business, systems, and/or services in immediate risk but may pose an unacceptable risk if not addressed in a timely fashion. • Low / Green: The potential incident does not pose unacceptable risk but may indicate trends or patterns that might suggest a future impact. • Informational / White: There no current potential incident. Information is for awareness.
Disclaimer	This alert contains raw intelligence that has not been analyzed. It is provided for your situational awareness 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.