IMPORTANT ALERT

Russian Malware Attack On Commercial Real Estate Thwarted by Intelligent Buildings' Managed Service

Summary: We are alerting you that we recently detected and eliminated a likely Russian malware attack on a commercial real estate building through our multi-dimensional managed service protection. We are linking the incident to Russia based on a bulletin about a specific malware threat from CISA naming the malware that we discovered.

Sequence of Events

1. **Threat Detection:** Our Asset Management and Threat Detection immediately identified a likely Russian malware threat called WhisperGate on the building management system (BMS) server. This malware is designed to destroy targeted devices resulting in boot failure.
2. **Malware Source:** The source of the malware is under investigation. It is likely from a local connection from a technician laptop that was infected.
3. **Internet Connection:** Our Zero-Trust access service made the building system invisible to inbound and outbound Internet traffic. The service denied the malware node from its attempts to communicate outbound since it was not specifically listed as "trusted." This prevented the malware from receiving instructions to encrypt files and hold the server for ransom.
4. **Server Backup & Antivirus:** Our antivirus/anti-malware service running on the BMS server quarantined and eliminated the threat while preparing to restore a backup image of the server from our secure cloud.
5. **Notification:** We notified the client about the event, mitigation workflow, forensics data, and successful prevention of damage to servers and equipment.
6. **Law Enforcement:** Client notified the FBI and CISA about the breach and prevention with forensic support from Intelligent Buildings.
7. **Audit & Training:** The technician(s) are now in an elevated cybersecurity awareness, audit and phishing regiment.

Outcome: The threat was identified and automatically mitigated, saving the organization from significant operational interruption, financial loss, and reputation damage.

Recommended Next Steps: Contact Intelligent Buildings to perform immediate, remote assessments and quickly deploy and scale our monitoring services for your portfolio.