Homeland Security
Office of Intelligence and Analysis
INTELLIGENCE NOTE
28 March 2017

(U//FOUO) Unknown Cyber Actors Target US Water and Sewage Authority Network

(U) Prepared by the Office of Intelligence and Analysis (I&A) and coordinated with the National Cybersecurity and Communications Integration Center (NCCIC).

*(U//FOUO) **Scope:** This* Intelligence Note *provides current intelligence on a specific threat to industrial control systems and networks associated with the US Water and Wastewater Systems Sector and other critical infrastructure sectors reliant on remote wireless Internet connectivity for their operations. I&A prepared this* Note *in direct support of the information sharing and analysis centers (ISACs) for water, electricity, financial services, surface transportation, and emergency management and response.*

(U//FOUO) Likely Network Device Compromise Results in Excessive Data Traffic; Device Provided Access to Industrial Control System

(U//FOUO) An unidentified actor or actors between November 2016 and January 2017 targeted a US water and sewage authority's network, resulting in excessive cellular charges and unusual traffic on ports 10000 and 9600, according to an FBI source with excellent access who spoke in confidence but whose reliability cannot be determined.[1] The FBI source indicated that four of the seven devices on the authority's cellular data plan were impacted with high data usage, which was likely a result of compromised network devices. The November 2016–December 2016 billing cycle totaled $45,000, and the December 2016–January 2017 billing cycle totaled $53,000. A typical monthly bill averages approximately $300. The devices were Sixnet devices, which had been in place for six or seven years and provided access to the authority's industrial control systems, according to the same FBI source.

(U//FOUO) Support to Computer Network Defense

(U//FOUO) Sixnet BT-5xxx and BT-6xxx series device versions prior to 3.8.21, as of May 2016, were vulnerable to a compromise that exploited a hard-coded factory password that could enable full access to the affected device, according to ICS-CERT Advisory ICSA-16-0147-02. The same advisory identifies vendor patches and firmware updates that address the issue.[2]

(U//FOUO) Sixnet BT-5xxx series industrial cellular modems and BT-6xxx machine-to-machine gateways facilitate data communications connectivity in mobile or remote environments. Ports 9600 and 10000 are used for transmission control protocol and user datagram protocol (TCP/UDP) communications, according to an online report from a firm that provides industrial automation and networking solutions.[3]

IA-0114-17

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) All US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.sgov.gov, or IA.PM@dhs.ic.gov

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870 or go to https://forms.uscert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.4.2.16, HSEC-1.4.4, HSEC-1.5.1, HSEC-1.6.2.16, HSEC-1.10.1

[1] (U//FOUO); FBI; IIR 4 213 1461 17; 172045Z FEB 17; DOI 09 FEB 2017; (U//FOUO); Industrial Control System Compromise at an Identified US Water and Sewage Authority, as of January 2017; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[2] (U); DHS; Advisory (ICSA-16-147-02); 26 MAY 2016; DOI UNK; (U); Sixnet BT Series Hard-coded Credentials Vulnerability; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[3] (U); Redlion; "BT-6000 Series IndustrialPro M2M Gateways"; 2014; www.redlion.net; accessed on 08 MAR 2017.