



SITUATIONAL INFORMATION REPORT FEDERAL BUREAU OF INVESTIGATION

Tradecraft Alert CYBER DIVISION

Approved for Release: 03 April 2017

SIR Number: SIR-00116828641

(U//FOUO) Unsecured Law Enforcement Devices Could Provide Vectors for Internet-Enabled Network Attacks

SOURCE: (U) An employee of the FBI.

(U//FOUO) Law enforcement agencies using Internet-connected and ancillary network-enabled devices could be vulnerable to compromise. Surveillance devices such as security cameras and Webcams often are targets of cyber actors due to their overall lack of security, their use of default administrative user IDs and passwords, and their open connections to the Internet, making them more vulnerable to computer-enabled intrusions. Such compromises could also bring in to question device operational integrity.

(U//FOUO) A police department discovered multiple disruptions to their surveillance cameras as a result of ransomware[1] infections in January 2017. Hackers compromised 70% of the cameras across the city, eight days before the Presidential Inauguration, which prevented officials from accessing the command and control center of the surveillance system. According to FBI reporting, the infected cameras were configured with default remote access passwords.

(U) The Federal Trade Commission (FTC) filed a complaint in January 2017 against a camera and router manufacturer due to its poor security practices and the misrepresentation to consumers that the devices are secure. The FTC alleged their Internet Protocol cameras contained a default username and password that

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the CYBER Division.

UNCLASSIFIED//FOUO

could allow cyber actors access to live feeds, stored login credentials for a mobile app in clear text without using encryption, and left its private code signing key on a public Web site for more than 6 months that could have allowed actors to use the key to sign malicious software.

(U//FOUO) The FBI anticipates other LE devices such as body cameras could provide additional points for infection. These devices require intermittent connectivity for data transfer and/or storage, and can also serve as potential infection vectors for LE networks and infrastructure.

(U) A network integrator firm was hired in November 2015 to develop a cloud-based video system to store and share video data for government and LE agencies and discovered pre-loaded malware on police body cameras. The malware was tested in a lab environment where it immediately disabled Automatic Updates and Background Intelligent Transfer Service[2] on the connected computer, in addition to disabling access to sites related to anti-virus software. The infected network activity attempted to spread to other network machines and made phone home calls to Internet sites (specifics on those sites were not provided).

(U//FOUO) Those seeking to compromise LE systems have vast resources available to assist in finding and accessing vulnerable devices. Web sites and mobile applications available on the open Internet provide cyber actors the ability to identify unsecure cameras and Internet-connected devices worldwide.

(U) A mother was notified in August 2016 that the Webcam in her children's bedroom was hacked and was live streaming on a free mobile app called 'Live Camera Viewer.' Unknown actors were able to hack the camera through a Minecraft[3] phishing attack allowing the actors to obtain the IP address and gain access to the home network on which the camera was connected.

(U) A Russia-based Web site that displays feeds of open security cameras called Insecam was created in 2014 and listed over 73,000 unsecured video cameras world-wide. A US computer security company in July 2016 analyzed over 6,000 open security cameras listed on Insecam in the United States and found North Dakota, Washington DC, and Montana had the most unsecured security cameras.

(U) Shodan, a Web site used to identify Internet-connected devices worldwide, in August 2015 launched a tool that lets its users view unsecure video camera feeds globally for a onetime fee of \$49. A computer security company in January 2016 reported the feature includes screenshots of the Webcam feeds and pairs each screenshot with a map identifying the city/country in which the device is located.

(U//FOUO) The FBI assesses the expanding use of Internet-connected technology amongst LE agencies almost certainly will increase over the next several years. The direct connectivity of devices to sensitive LE networks for data ingestion, storage, and access could pose vulnerabilities by serving as pivot points for intrusions. This could provide increased opportunities for cyber actors to gain unauthorized access to internal systems and networks used for operational functions or housing sensitive data. The continued development of Internet services and applications aimed at identifying vulnerable Internet-connected devices are expected to grow over the next several years, providing low cost methods for cyber actors with malicious intent to identify potential devices used by LE and access points for computer intrusions. Additionally, the failure of many anti-virus solutions to protect Internet of Things[4] devices - which typically run on stripped down versions of operating systems requiring anti-virus solutions different than typical networked systems - could lead to a false sense of network security even if their anti-virus is up to date. The FBI will continue to provide intelligence on emerging tactics and technologies to state and local LE in order to grow awareness of the cyber threats facing these agencies.

UNCLASSIFIED//FOUO

[1] (U) **Internet of Things** is the inter-networking of physical devices, often referred to as “smart devices,” embedded with electronics, software, sensors, actuators, and network connectivity that allows them to send and receive data.

[2] (U) **Minecraft** is a popular 3-D game about placing blocks, crafting, and going on adventures.

[3] (U) **Background Intelligent Transfer Service** transfers files between a client and a server and is most commonly used to download updates to local systems.

[4] (U) **Ransomware** is malicious software that blocks access to computer systems or files until money is paid.

(U) This report has been prepared by the CYBER Division of the FBI. Comments and queries may be addressed to the CYBER Division at 202-324-3000.

UNCLASSIFIED//FOUO

Distribution

All Fusion Centers
SLTTs
LEO

UNCLASSIFIED//FOUO

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:
Federal Bureau of Investigation
CYBER DIVISION
Missing

Customer and Product Information

SIR Tracking ID: SIR-00116828641

Product Title: (U//FOUO) Unsecured Law Enforcement Devices Could Provide Vectors for Internet-Enabled Network Attacks

Dated: _____

Customer Agency: _____

Relevance to Your Intelligence Needs

- 1. The product increased my knowledge of an issue or topic. (Check one)
 - 5. Strongly Agree
 - 4. Somewhat Agree
 - 3. Neither Agree or Disagree
 - 2. Somewhat Disagree
 - 1. Strongly Disagree

Actionable Value

- 2. The product helped me decide on a course of action. (Check one)
 - 5. Strongly Agree
 - 4. Somewhat Agree
 - 3. Neither Agree or Disagree
 - 2. Somewhat Disagree
 - 1. Strongly Disagree

Timeliness Value

- 3. The product was timely to my needs. (Check one)
 - 5. Strongly Agree
 - 4. Somewhat Agree
 - 3. Neither Agree or Disagree
 - 2. Somewhat Disagree

___1. Strongly Disagree

Comments (please use reverse or attach separate page if needed):
