SECURITY BRIEF:

The U.S. Ban on 5 Major Device Manufacturers

INTRODUCTION

The 2019 National Defense Authorization Act prevents government agencies from signing contracts with companies that use equipment, services and systems from Huawei, ZTE, Hytera, Hikvision and Dahua, or any of their subsidiaries and affiliates, citing national security concerns. When passed in August 2019, the law immediately banned the purchase of new equipment from these manufacturers and created a deadline for the removal of any existing equipment by August 13, 2020.

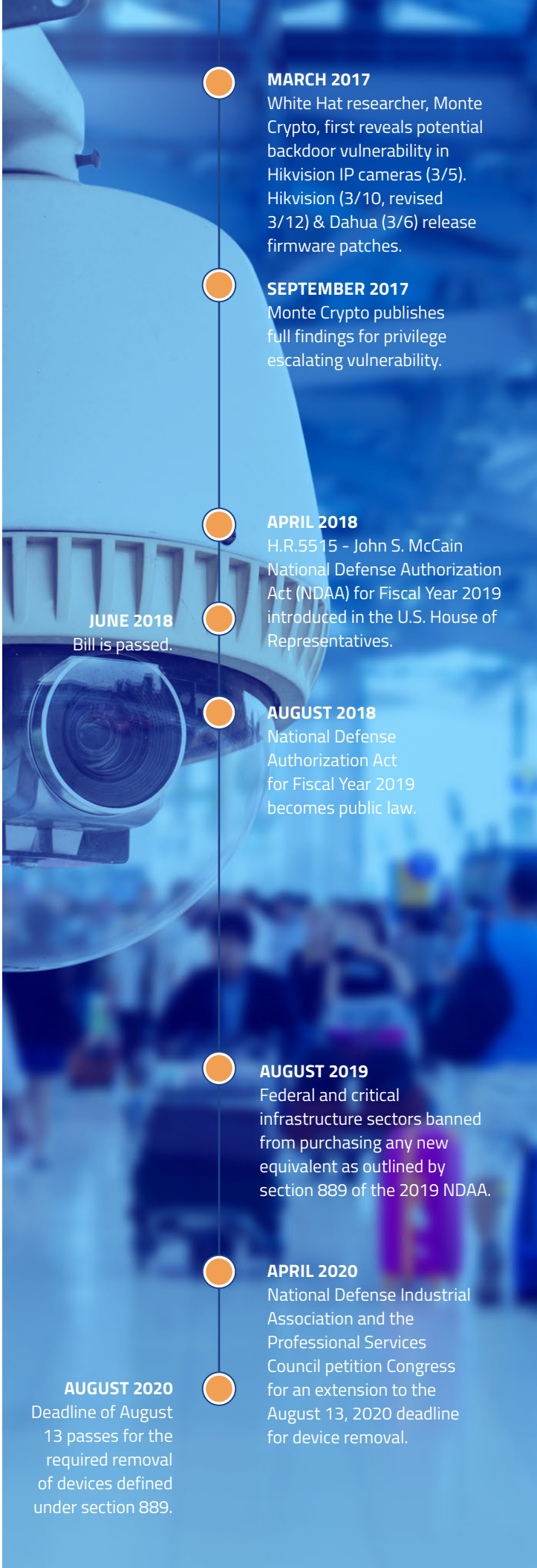
The ban initially stemmed from a vulnerability first identified by a researcher who goes by the alias Monte Crypto in March 2017. In a March 5th reddit post, the white hat – or ethical computer hacker – researcher wrote, "I would like to confirm that there is a backdoor in many popular Hikvision products that makes it possible to gain full admin access to the device." In September 2017, Monte Crypto posted a detailed report, including a timeline of events.

"I would like to confirm that there is a backdoor in many popular Hikvision products that makes it possible to gain full admin access to the device."

– Monte Crypto, White Hat Researcher

The U.S. ban impacts five manufacturers partially owned by the Chinese government. While all five have a checkered history of similar incidents, Hikvision in particular has had numerous high-profile incidents in the past decade, as reported by IPVM:

- Hikvision IP Cameras Multiple Vulnerabilities (08/13)
- Hackers Turn Security Camera DVRs Into Worst Bitcoin Miners Ever (04/14)
- Multiple Vulnerabilities Found in Hikvision DVR Devices (11/14)
- Hikvision Chinese Government User Hacked (03/15)
- Hikvision iVMS-4500 Mobile App Malware (09/15)
- Hikvision Rejects Responsibility for Hacked Hikvision Cameras (05/16)



MARCH 2017
White Hat researcher, Monte Crypto, first reveals potential backdoor vulnerability in Hikvision IP cameras (3/5). Hikvision (3/10, revised 3/12) & Dahua (3/6) release firmware patches.

SEPTEMBER 2017
Monte Crypto publishes full findings for privilege escalating vulnerability.

APRIL 2018
H.R.5515 - John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 introduced in the U.S. House of Representatives.

JUNE 2018
Bill is passed.

AUGUST 2018
National Defense Authorization Act for Fiscal Year 2019 becomes public law.

AUGUST 2019
Federal and critical infrastructure sectors banned from purchasing any new equivalent as outlined by section 889 of the 2019 NDAA.

APRIL 2020
National Defense Industrial Association and the Professional Services Council petition Congress for an extension to the August 13, 2020 deadline for device removal.

AUGUST 2020
Deadline of August 13 passes for the required removal of devices defined under section 889.

- Hikvision Cloud Security Vulnerability Uncovered (12/16)
- Hikvision Discontinuing Online Service (12/16)
- Hikvision Defaulted Devices Getting Hacked (02/17)
- Hikvision Privilege-Escalating Security Vulnerability (03/17)

In the 2 years following the report and confirmation, a series of events transpired that resulted in a U.S. Department of Homeland Security ban on IP cameras, two-way radios and device components from the five manufacturers as part of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019.

The U.S. ban impacts five manufacturers partially owned by the Chinese government.

Hikvision has since provided firmware updates for specific model numbers, which BuildingReports has added to its web-based reporting recall notification feature. BuildingReports also located these firmware updates (PDF download) for Dahua, which were posted by a forum user in March 2017. However, the availability of an update from either manufacturer has no impact on the subsequent ban.

IMPACT

Under the new law, federal facilities and any industry sectors defined as critical infrastructure were ordered to remove or replace the devices by August 13, 2020. As published in the Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, the "covered telecommunications equipment or services," as defined in the statute, include the following:

- "Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- Telecommunications or video surveillance services provided by such entities or using such equipment; or
- Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country."

BANNED HIKVISION OEMS

3xLogic
ABUS
Acegear
Activecam
ADJ
Advidia (Video Insight / Panasonic brand)
Alarm.com
Alibi (Supercircuits)
Allnet
Alula
Anaveo
Annke
Arcdyn
Armix
Aukoo Technology
Aventura Technologies
Avue
Cantek
CCTVStar
ClearWay
Covert Security
Dax Networks
DMP
Dodwell BMS
DSS
Dunlop
DVR Unlimited
Ellipse Security
Epcom
Esypop
Ezviz
Gess Technologies
Global Network Security
GovComm Intelligent Transportation Systems
Grundig
GVS Security
Hinovision
Hitachi
Hitosino
Honeywell
Hunt CCTV
Hyundai Security
Infinite Pixels
Inkovideo
Innekt
Interlogix (UTC)
Invidtech
IP Cam Talk
JFL
Jlinks
LaView
LTS
Mercury Security and Facilities Management
MicroView
Nelly's Security
Norelco SafeCam / Spider Vue / Invezia
Northern (Tri-Ed / Anixter)
Novicam
NTT
Oculur / A1 Security Cameras
Onix
Paxton (Available outside the US only)
Pnet
Power Technology
Protect Group
Raster
Remark Thermal
RVi
Safety Vision
Safire
Scati
SecurityTronix
Sentry CCTV
Sharp
Siqura / TKH
Smart CT Solutions
SnapAV / Luma
Space Technology
Syscom
Technomate
Toshiba
Trendnet
Vantage Security
Vezco CCTV
Videoteknika
Winic
Xyclop
Zicom

In addition to subsidiaries and affiliates, the ban also includes original equipment manufacturers (OEMs) and commercial off-the-shelf (COTS) hardware. IPVM has compiled directories of the OEMs included for Dahua and Hikvision:

- Dahua OEMs
- Hikvision OEMs

Under the False Claims Act, contractors found to be in violation of the NDAA after August 13 can be subject to fines ranging from $11,665 to $23,331 for each false claim made.

Under the False Claims Act, contractors found to be in violation of the NDAA after August 13th can be subject to fines ranging from $11,665 to $23,331 for each false claim made. The law applies to all federal agencies and the following industry sectors, as defined by the Cybersecurity & Infrastructure Security Agency:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
- Any institution that receives federal funding earmarked for the purchase of surveillance cameras, such as schools and local governments, may also have to comply with the law.

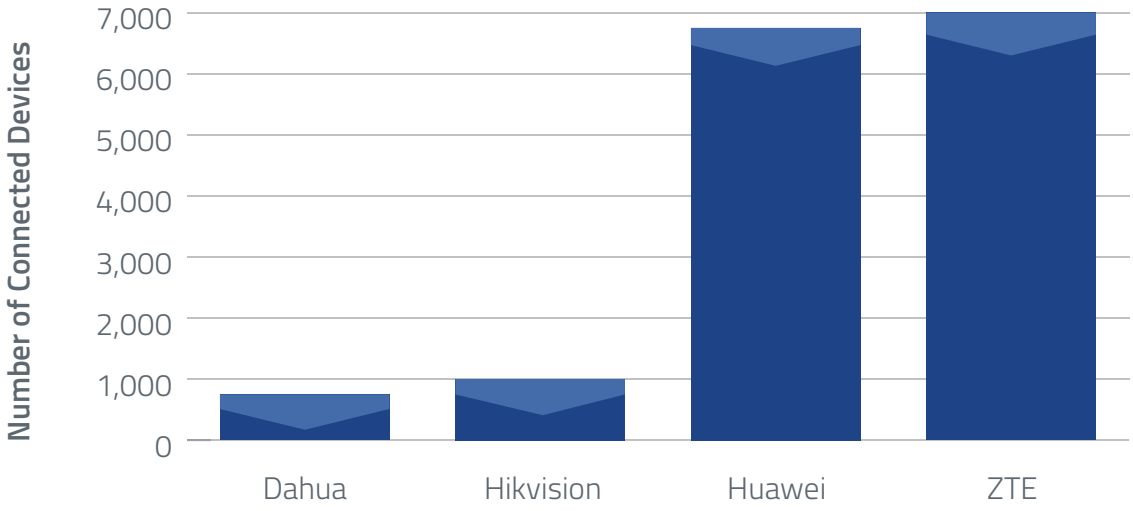
The new law primarily impacts two groups: (1) federal agencies and critical infrastructure and (2) service companies and distributors. Little is known about how successful the first group has been in the effort or how much progress has been made. These groups are also prohibited from doing business with service companies and distributors that sell, install and maintain devices covered under the law, putting valuable government and private sector contracts on the line for the second group.

BANNED DAHUA OEMS

2M CCTV
Activecam
Advidia / Panasonic
Altoros
Amcrest
Ameta
Ascendent
Backstreet Surveillance
Bosch (NVR/ DVR OEM and camera contract manufacturing)
BV Security
CCTV Security Pros
CCTV Star
CP Plus (Orange Line)
Dax Networks
eLine
ENS (formerly Eastern CCTV and SavvyTech)
Expose
Lorex
Gess Technologies
GSS
Honeywell (OEMs from both Dahua and Vivotek)
IC Realtime
Ikegami
Impath Networks
Inaxsys
IndigoVision
Infinity CCTV
Innekt
Intelbras
KBVision
Lumixen
Maxron
Montavue
Oco
Optiview
Panasonic (depends on region; no longer used in US)
People Fu
PlatinumCCTV
RedSpeed
Rhodium
RVI
Saxco
Security Camera King (Elite)
Space Technology
Speco
ToughDog
Unisight (EmPower)
VIP Vision
Watchnet
Winic
Zuum

CHALLENGE

As of July 23, 2019, Forescout Technologies, Inc., a leading security firm, estimated that around 15,000 devices from four of the manufacturers had been connected to U.S. government networks. Only a subset of those are the security devices in question (Forescout found 1,740 surveillance cameras made by Hikvision and Dahua connected to government networks as of the July date).



Numbers as of July 23, 2019. Source: Forescout

What the data helps demonstrate is the difficulty associated with the first step in complying with the law: Identifying how many of the devices are currently in service, what facilities are using the devices and where they are located. If detailed documentation has not been maintained and kept up to date, time-consuming physical audits are required to understand the scope and scale of the impact. In addition, the process of identifying gray market devices that leverage components from these manufacturers but are sold under a different brand can be difficult and confusing outside of public OEM relationships.

As of July 23, 2019, Forescout Technologies, Inc., a leading security firm, estimated that around 15,000 devices from four of the manufacturers had been connected to U.S. government networks.

Any facilities that did not act early and move quickly to rectify the violation were likely hampered by the COVID-19 pandemic in the 5 months preceding the deadline. In fact, many facilities are likely currently in violation of the law, and some may not even realize it since regular inspections of security devices are not compliance-driven based on codes and standards. It's unclear what enforcement measures have been taken or when broad-scale efforts may be undertaken to determine which facilities are in compliance with the new law.

The result has been widespread confusion, leaving many in the industry pleading for additional guidance or deadline extensions in order to comply. Several trade groups representing government contractors officially petitioned Congress in April to delay the deadline, but those requests were unsuccessful – even though the same concerns were echoed by the Department of Defense.

SOLUTION

While ironic, the answer to a problem created by technology may be technology itself. "Big Data" has been a hot topic for the past several years, and for good reason. Given the scope and scale of the effort to replace the banned devices, having a detailed, verifiable database

of facility assets across the geographic footprint of an organization or government agency would provide distinct advantages in scenarios such as this one. The analysis of that data would not only provide a detailed inventory of assets by facility, manufacturer, device type, location in the facility and current status, but also allow officials to do the following:

- Understand the scope of the effort
- Assess and rank the security risk
- Prioritize the most serious threats for immediate action
- Plan and budget effectively and accurately
- More efficiently and effectively mitigate risk and bring facilities into compliance with the law
- Track progress and status live, online, 24/7

Enter SecurityScan® from BuildingReports®, the leading mobile inspection application and web-based reporting solution for security, fire alarm, fire sprinkler, fire suppression, life safety and HVAC assets. Using a point-and-scan barcoding process, technicians create a detailed database of all corresponding system assets by type for a given facility. During each scheduled inspection or service call, the technician documents the status of each device, records any key information and uploads the data once complete to a secure cloud where any authorized stakeholder around the globe has on-demand access. In addition, BuildingReports actively manages a recall database to help service companies and facilities stay up to date on recalls that may affect their facilities and much more.

Given the scope and scale of the effort to replace the banned devices, having a detailed, verifiable database of facility assets across the geographic footprint of an organization or government agency would provide distinct advantages in scenarios such as this one.

For more information or a personalized demonstration, visit www.buildingreports.com or email info@buildingreports.com.

BUILDING REPORTS®

The most trusted name in compliance reporting

About BuildingReports

Building safety compliance is critical to service companies, building owners, and fire and safety officials who are charged with safeguarding occupants. BuildingReports' mobile and online inspection reporting tools enable inspectors to quickly gather data on fire and life safety devices to ensure they are working properly and meet code requirements, and to identify actions needed to meet compliance through easily verifiable inspection reports. With more than 14 billion square feet of floor space inspected in more than 900,000 buildings to date, BuildingReports has earned its reputation as the most trusted name in compliance reporting. Learn more at **www.buildingreports.com**.