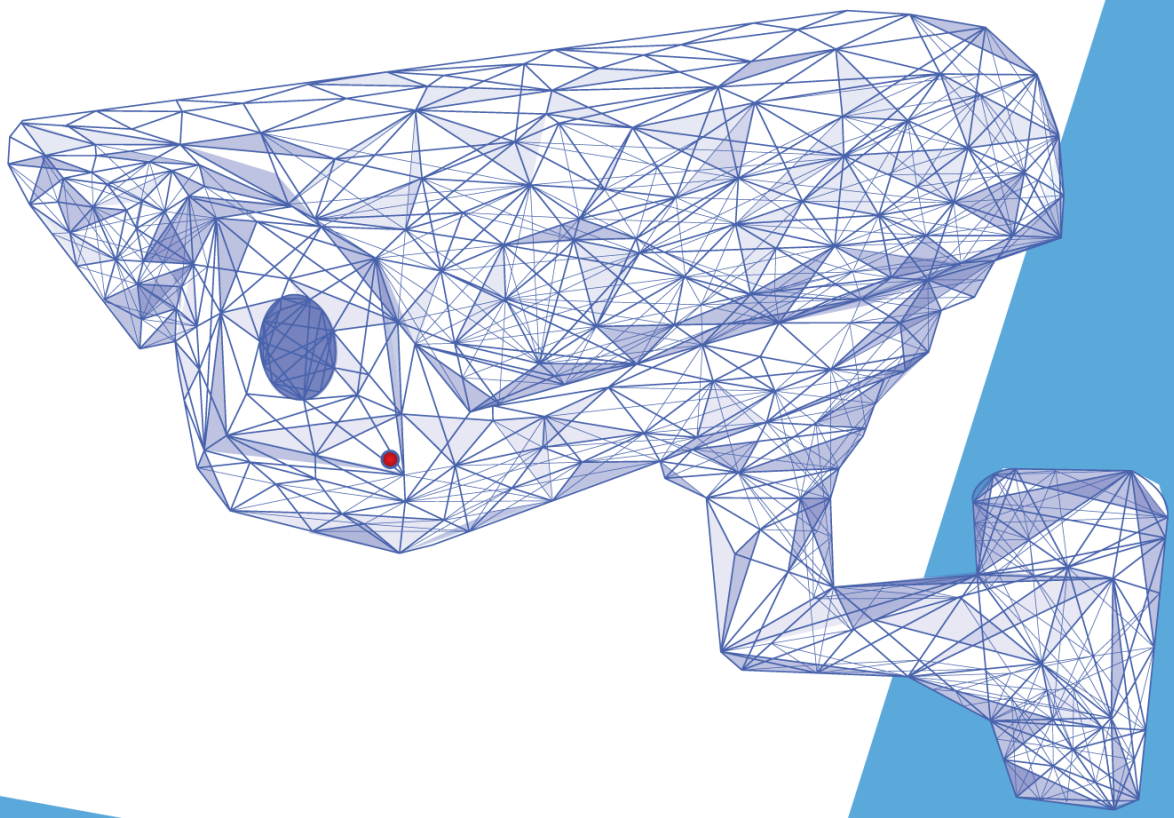


The Conundrum Of Banned Chinese Security Cameras

Whitepaper

attila SECURITY

Overview

In August 2018, the U.S. government passed a ban on the use of certain Chinese-manufactured surveillance cameras by U.S. government agencies. The terms of the ban provided the agencies with one year to identify and remove any affected cameras from their network. However, as the one-year deadline approaches, many banned cameras are still operating on government networks. This mass noncompliance by government agencies is not due to a deliberate disregard for the ban, but rather to the challenges associated with identification and removal of the devices. Many Chinese cameras have U.S. labels and other cameras – not identified in the ban – actually contain Chinese-manufactured components. Additionally, this issue is not limited to the public sector - the tainted technology has widely infiltrated private enterprises as well. Surveillance cameras are regularly deployed in highly sensitive environments as part of an organization's security strategy. It is somewhat ironic that the cameras themselves cannot be trusted, and actually pose a significant threat to data security. This whitepaper examines the problem in more detail and delivers a recommendation for securing camera data streams.

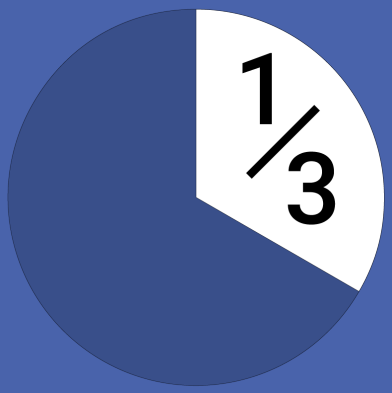
"The cameras *themselves* cannot be trusted."

Background

The National Defense Authorization Act (NDAA) for fiscal year 2019, which was passed in August 2018, included an amendment comprised of two separate Federal Acquisition Rules (FAR) that enacted the ban on Chinese surveillance cameras. [1] This first rule of the amendment bans the use of Chinese-made surveillance cameras effective August 13, 2019.

As indicated previously, government agencies are struggling to identify and remove any such cameras before the deadline. The second rule has a much greater scope. Effective August 13, 2020, government agencies will not be permitted to make purchases from organizations that utilize the banned cameras. Given its breadth, this ban will be even more difficult to implement, and this led to a request by the White House's budget director to extend the deadline by an additional two years – to August 2022.

The impetus for the ban occurred in 2017, when ReFirm Labs, a U.S. cybersecurity company, identified covert backdoors in Dahua cameras that could be used to send data to an unknown Chinese IP address. [2] While Dahua's security advisory claimed that data could only be sent to, not from, the cameras, ReFirm Labs observed two-way communication in progress. Terry Dunlap, ReFirm's co-founder, indicated that company information was observed to be trafficked offsite from the cameras to an unknown Chinese IP address. The ReFirms report stated: "Given that many other Dahua products contain this exact same backdoor, we strongly recommend against connecting any Dahua products to critical or sensitive networks." [2] Dahua later issued public notice about the vulnerability [3] and claimed to have fixed the issue.



of the global surveillance camera market is controlled by *just 2 companies*.

Both are named in the ban.

The two surveillance camera manufacturers explicitly named in the ban, Zhejiang Dahua Technology Co. (Dahua) and Hangzhou Hikvision Digital Technology Co. (Hikvision), together control one-third of the global market for surveillance cameras.

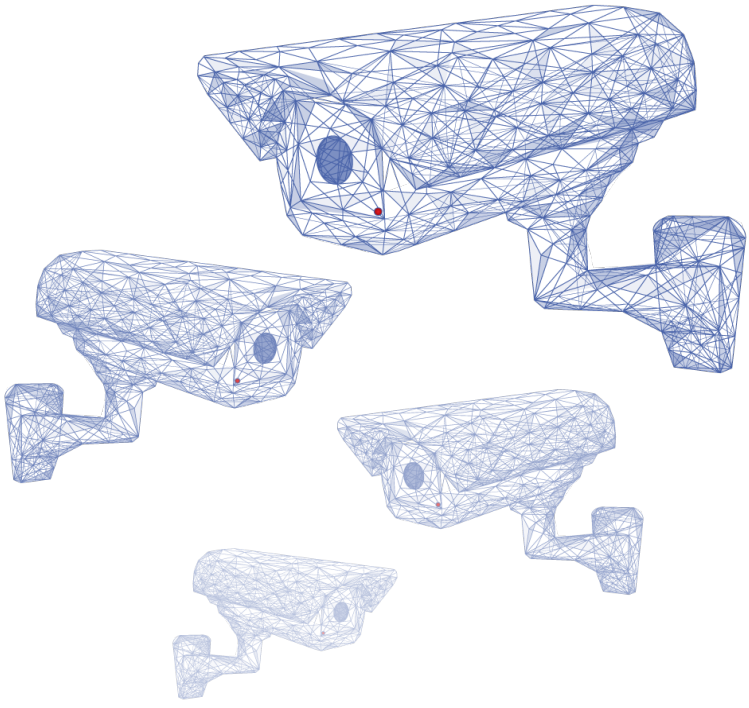
Hikvision is the largest global surveillance camera provider. Dahua has 35 subsidiaries [4] and is the second largest surveillance camera provider. Hikvision cameras provide clear, full-color images in near-darkness and fog and have built-in artificial intelligence and 3D imaging systems for facial recognition. [5]
Hikvision and Dahua were likely singled out in the ban due to their massive market share as well as the extent of the influence of the Chinese Government over both companies. For example, the Chinese government has a 42% stake in Hikvision. A Hikvision company spokesperson stated that the Chinese government is not involved in the company's daily affairs [2], but this does not mean that the government cannot influence the company. Under Chinese law, the government can force the company to turn over data that it has collected, effectively making Hikvision security cameras part of the Chinese intelligence apparatus. While the Chinese government does not have the same stake in Dahua, these same laws would apply.

The DoD ban on Chinese surveillance cameras has a human rights aspect as well. In April 2019, a group of U.S. senators and representatives petitioned for Hikvision and Dahua to be added to the U.S. Department of Commerce blacklist [6], imposing controls on exports of U.S. technology to these companies. The motivation behind this request was twofold: 1) stop contributing to China's growth as a surveillance state and 2) send a response to the use of Hikvision's and Dahua's camera facial recognition in the identification and detention of hundreds of thousands of Uighurs - a primarily Muslim ethnic minority - in China. [5]

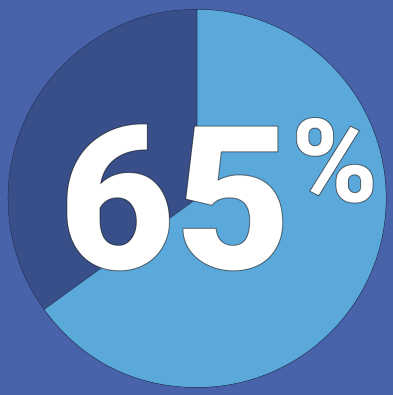
Terry Dunlap, a former National Security Agency offensive cyber operator and current co-founder and chief strategy officer at ReFirm Labs, said "If U.S. companies are buying Huawei gear, they should be on guard and exercise extreme caution. All telecom gear coming from China that is placed into our critical infrastructure needs to undergo a thorough security vetting -- from top-layer applications all the way down to the firmware level, where we see backdoor implants." [7]

Discussion

The one-year timeframe provided for U.S. government agencies to identify and remove Chinese-manufactured surveillance cameras from their networks and properties may seem reasonable, but several complications make compliance a significant challenge. The first issue is the sheer number of surveillance cameras that are affected by the ban. Hikvision and Dahua control at least one-third of the surveillance camera market. As a result, there are at least 1,700 banned cameras operating at government agencies, according to cybersecurity advisory firm, Forescout Technologies. [2] While this is a significant number of cameras to identify, remove and replace, the scope of the problem is actually much larger. While Hikvision does sell some of its cameras in the U.S. directly, it also has licensing agreements with a number of different companies, including major U.S. organizations like Panasonic and Honeywell, to white label and sell Hikvision cameras. Under a white label agreement, companies put their own packaging and branding on the equipment, making the banned product appear to have originated in the United States. When asked, Honeywell stated that it would not be able to track its white labeled cameras even if requested to do so by a federal agency. [2]



Finally, most U.S. government agencies have no means of automatically tracking the devices that are operating on their networks. While the Department of Homeland Security mandated that agencies implement such a system several years ago, a report by the Government Accountability Office (GAO) indicated that as of 2018, only 35% of agencies were compliant with this requirement. [8] This means that 65% of government agencies must manually check each camera that they own to determine if it is a model manufactured by or containing components from Dahua or Hikvision.



of government agencies will have to **manually check each camera** that they own.

Banning Hikvision and Dahua cameras from federal agencies represents a significant expenditure of time, effort and money in identifying, removing and replacing the cameras with trusted devices. Expanding the ban to organizations that do business with these agencies, which is required by August 2020 unless a requested delay is passed, only amplifies the impact of this effort. Also, finding adequate replacement cameras that do not include banned components and that have a similar caliber of features and functionality as Hikvision and Dahua cameras will not be easy. In addition to the ban on Hikvision and Dahua, the U.S. government also enacted a ban on Huawei and ZTE Technology products. Huawei is best known for its networking components; however, its chips are also included in 60% of surveillance cameras worldwide. So, while the Hikvision and Dahua ban forces government agencies to remove existing surveillance cameras, the Huawei ban may significantly impact the number and variety of cameras that agencies can acquire as replacements.

Recommendations

As it is difficult to ascertain where surveillance camera components arrive from, one defensive strategy is to layer-in a security product with each existing camera to filter all Internet and data traffic and deny unsolicited data requests. This type of solution will offer protection from cyber-attacks, identity theft and malware.

In order for it to be feasible for an organization to implement this type of solution throughout its entire video infrastructure, the product must be affordable, easy to configure and have sufficiently low power requirements so that there will be no need to re-run new power cables to all systems.

Attila Security's GoSilent is an example of an agile, simple and highly secure solution that has been successfully used by public and private enterprises to restore and maintain the security of surveillance camera live streams. This multiple-award-winning device has been widely recognized as the most portable and easiest to configure hardware VPN solution for securing network communications to and from remote locations, for any type of IP-enabled device

About Attila Security

Attila is a cybersecurity company focused on providing services that identify, control and defend against cyber threats across physical, virtual and cloud technologies. Attila has been named among the Cybersecurity 500 index of industry leaders, and has been recognized as an industry leader for its revolutionary and innovative technological advancements in completely portable, government grade, IP security as well as their suite of cloud and virtual servers. For more information, visit **www.attilasec.com** or call 410.849.9472.

attila SECURITY

References

1. https://ipvm.com/reports/omb-letter
2. https://www.bloomberg.com/news/articles/2019-07-10/banned-chinese-security-cameras-are-almost-impossible-to-remove
3. https://www.dahuasecurity.com/support/cybersecurity/details/172
4. http://pl.dahuasecurity.com/introduction.html
5. https://www.bloomberg.com/news/articles/2019-05-22/china-s-hikvision-weighed-for-u-s-ban-has-probably-filmed-you
6. https://www.reuters.com/article/us-hikvision-usa/after-huawei-u-s-could-blacklist-chinese-surveillance-tech-firm-media-idUSKCN1SS04D
7. https://searchsecurity.techtarget.com/news/252466178/Huawei-ban-may-be-loosened-but-details-unclear
8. https://www.gao.gov/assets/700/696105.pdf