Cybersecurity for IP Surveillance Devices

Cybersecurity for IP Surveillance Cameras & Trend Micro IoT Security Solutions

Abstract

Cybersecurity for IoT devices has been a hot topic in the past few years, and IP surveillance cameras are the hackers' top target because of the relatively high computing power and good internet traffic throughput. At the end of 2016, a Linux-based malware "Mirai" was used to initiate a DDoS attack which created a record-high 1.2Tbps Internet traffic. The huge traffic was triggered by remote commands and the victim devices were mainly IP surveillance cameras. Not only is Mirai source code made available on the Internet, multiple variants of Mirai-like malware are surfacing. Cybersecurity now becomes another focal point for IP surveillance devices and multiple governments are making regulations to raise the bar for cybersecurity implementation. It is becoming the next decisive factor in the competition of the IP surveillance industry.

Incentives to Hack IP Surveillance Cameras

Today, the major motivation of hacking is monetization. When it comes to monetization, IP surveillance cameras are great targets because of the following reasons:

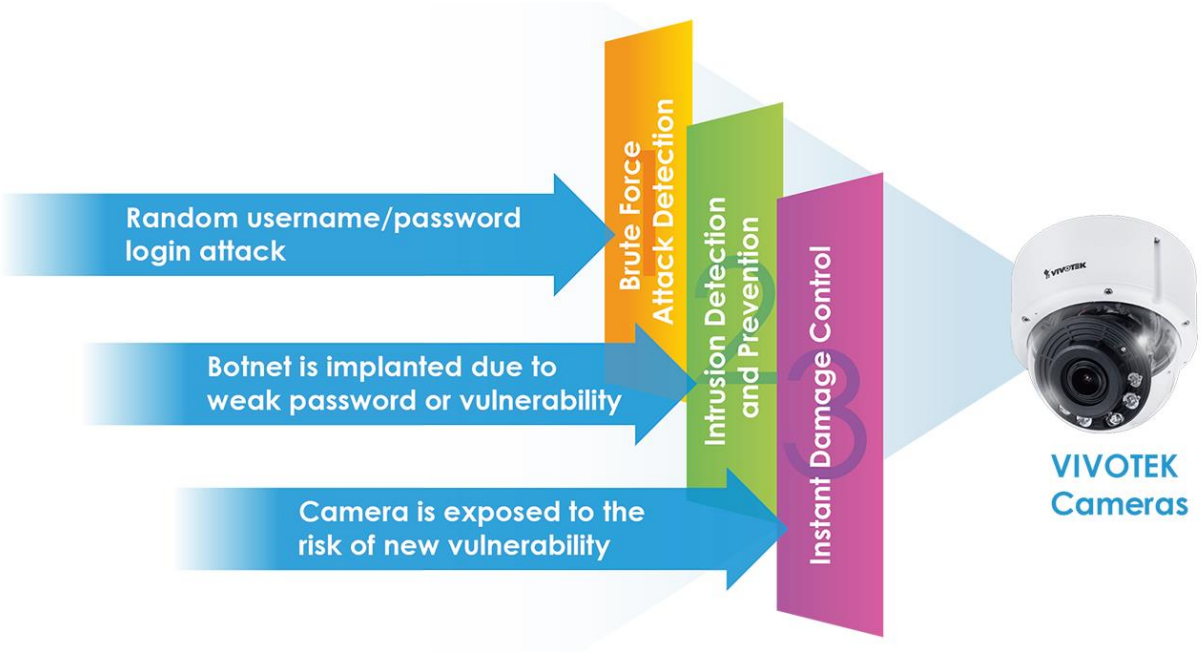
1. Constantly Connected: High exposure to the Internet making it easy for the hackers to find the device. Once hacked, the device will be constantly available to serve hackers' needs.
2. Low Hacking Investments: Unlike hacking a PC, once the hackers see a way to hack a device, the same approach can usually be applied to other devices of the similar models, making a very low per-device hacking cost.
3. Lack of Supervision: Unlike office PCs, IP surveillance cameras are not well managed by cybersecurity knowledgeable staff. Installing an after-market anti-malware application is not available as well.
4. High Performance: The idle computing power inside an IP surveillance camera is usually good enough to perform hackers' specified tasks like cryptocurrency mining, even without being noticed by end users.
5. High Internet Facing Bandwidth: The always-connect fast and huge bandwidth designed for video communication is the perfect target for hackers to initiate DDoS attacks.

Hacking/Infection Chain

The typical infection chain of IP surveillance cameras consists of the following steps:

1. Discover Address: Locate the IP address of a potential victim device, mostly done by Internet crawlers. Web services such as "Shodan" can also offer a list of discovered devices.
2. Gain Access: Use the default password, or the password dictionary to logon the device. Once getting the administrator privilege, hackers can further exploit the system for their malicious actions.
3. Exploit Vulnerabilities: Look into the system vulnerabilities and take advantages of them. System vulnerabilities are inevitable especially in a quick moving IT world where open source codes are widely used.
4. Inject Malware: Install the malware into the IP surveillance camera. The malware typically consists of an agent which handles the communication, and the main body which fulfills the main functions designed by the hackers.
5. Command and Control: Control the victims remotely to enable a specific service function. For example, hackers can initiate a DDoS attack and command all infected devices to target a specific destination.

Value Proposition of VIVOTEK + Trend Micro



The competition between hackers and device makers mainly relies on the threat knowledge, and the timing to respond to such threat knowledge. VIVOTEK in collaboration with Trend Micro aims to provide threat awareness in no time so that cameras and NVRs can react to a cyber threat one step ahead of hackers. The solution consists of three major parts:

1. **Anti-brute-force login-Attack**: A mechanism that detects automated brute-force login behavior. For people who never care to change the default password, or those who use easy-to-guess passwords, their IP surveillance devices are less secured by natural. By blocking suspicious logins, the solution reduces the possibilities of intrusion at the front line.
2. **Intrusion detection and prevention**: Powered by Trend Micro's IoT Reputation Service which is a huge cloud knowledge base that identifies malicious URLs, addresses of potentially infected devices, and malicious servers, VIVOTEK's IP surveillance devices can detect abnormal behavior inside with machine learning technology. Any connection attempting to the suspicious IP address will be blocked by Trend Micro IoT security solutions within VIVOTEK devices. Modern hackers can change the IP of the attacker devices very frequently, thus catching up with that within minimal time interval is crucial. The Trend Micro IoT Reputation Service cloud is updated every 15 minutes.
3. **Instant damage control**: When a system vulnerability is first disclosed in public it is a "race in time" between hackers and device makers. The period between the vulnerability disclosure and the release of the firmware fix usually takes a couple of weeks, which leaves hackers plenty of time to scan and attack vulnerable devices in big volumes. Like regular anti-virus software installed on a PC, the Trend Micro IoT security solution within VIVOTEK devices can update the virus pattern automatically or manually. Through this, devices are still under protection and the risk is minimized before the vulnerability is fixed in the official firmware release. In other words, although the virus might be able to affect the device due to the new disclosed vulnerability, it cannot do any harm due to the latest update of virus pattern. Furthermore, as the world's no. 1 contributor to the public vulnerability database, Trend Micro can even create attacking pattern of new virus before it is disclosed in many cases, leaving no room for the hackers to take any advantage upon a newly announced vulnerability.

Matrix Between Infection Chain and Trend Micro Protection Points

	Anti-Brute force login-attack	Intrusion detection and prevention	Instant damage control
Discover Address		V*1	
Gain Access	V*2		
Exploit Vulnerability			V*3
Inject Malware		V*4	
Command & Control		V*5	

*1: Blocks the respond to Internet crawlers.

*2: Prohibits login attempts temporarily upon anomaly detection.

*3: Shields the vulnerable points with virus pattern update.

*4: Blocks the communication to malicious peer addresses even a malware is planted.

*5: Blocks any communication from known malicious peer addresses.

Conclusion

As the concern for cybersecurity is growing due to the damage caused by cyber attack in the past years, the IP surveillance industry started to pay attention to this topic since IP cameras and NVRs have become the perfect targets for hackers. VIVOTEK is the first IP surveillance manufacturer in the market to provide anti-intrusion software within network cameras and NVRs. Powered by the renowned cybersecurity solution company Trend Micro, VIVOTEK IP devices can now detect and block the brute force login attack or any abnormal activities inside. In addition, through the automatic update of virus pattern, the risk of new vulnerabilities can be significantly reduced in no time.

VIVOTEK

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C.
|T: +886-2-82455282|F: +886-2-82455532|E: sales@vivotek.com | www.vivotek.com