Trout

Threat Intelligence and Mitigation for CCTV Systems

This whitepaper shares research on threats to CCTV systems and provides strategies to mitigate risks, outlining common vulnerabilities and recent cyber-attacks.

Introduction to CCTV Systems

Closed Circuit Television (CCTV), or video surveillance, is a crucial part of modern security systems. Unlike public broadcasting, CCTV footage is sent to a specific, secure audience. Originally developed in 1942 to monitor V2 rocket launches, CCTV technology has advanced dramatically since then. Today, whether footage is stored locally or streamed to cloud services, CCTV systems are central to security strategies, offering real-time alerts to potential breaches.

However, the features that make CCTV systems so valuable—constant monitoring of sensitive locations and assets—also make them appealing targets for cybercriminals. These attackers exploit vulnerabilities such as default passwords, outdated firmware, and poorly configured networks to gain unauthorized access. This can lead to data breaches, interruptions in surveillance, or manipulation of footage. The consequences of such breaches are severe, including privacy violations, security failures, potential operational sabotage, and a significant loss of trust in security measures.

This whitepaper explores various aspects of CCTV technology—from analog and IP cameras to advanced networked systems—and identifies the vulnerabilities in each. By examining recent cyberattacks and their impacts, this document aims to provide IT professionals with the knowledge needed to implement robust security frameworks and effectively mitigate potential threats, ensuring the integrity and reliability of their surveillance systems.

Understanding CCTV Technologies

The deployment of CCTV systems involves a variety of technologies and configurations, each with specific functionalities and vulnerabilities. This section explores the primary types of cameras, recording devices, and management systems integral to modern CCTV networks.

Types of CCTV Cameras

CCTV cameras are broadly categorized into two types based on their data transmission and processing technologies:

- **Analog Cameras:**

These cameras operate by transmitting analog video signals directly to a Digital Video Recorder (DVR) through coaxial cables. The DVR then converts these analog signals into digital format for storage and playback. Analog cameras are less susceptible to cyber threats due to their lack of direct network connection, making them suitable for environments where basic surveillance without remote access suffices.

- **IP Cameras (Internet Protocol Cameras):**

IP cameras, also known as network or digital cameras, capture and process video footage digitally within the camera itself and then transmit it over a network to a Network Video Recorder (NVR) or directly to cloud-based storage. This type of camera offers higher resolution and better quality images and facilitates remote monitoring and control. However, their connectivity to the network exposes them to potential cyber-attacks.

Each type of camera uses different methods for data transmission. Analog cameras rely on coaxial cables, while IP cameras can utilize Ethernet (Cat 5 or 6 cables), Wi-Fi, or even fiber optic cables if supported by the device. Choosing between analog and IP cameras often depends on specific security needs, budget, and the desired complexity of the installation.

Recording Solutions

CCTV systems typically employ one of two types of recording solutions:

- **DVR (Digital Video Recorder):**

DVRs are designed for use with analog cameras. They receive analog signals which are then converted into digital before storage. DVRs require a direct connection to each camera via coaxial cables, which can limit the flexibility of camera placement and contribute to a more labor-intensive installation process.

- **NVR (Network Video Recorder):**

NVRs are used with IP cameras and are more adaptable than DVRs due to their ability to receive and store digital video data sent over a network. This allows for more flexible installation options, as cameras can be positioned at considerable distances from the recorder without significant signal degradation, provided that network connectivity is maintained.
Both DVR and NVR systems have distinct security profiles. DVRs are generally more secure from network attacks due to their lack of internet connectivity, while NVRs require robust cybersecurity measures, including strong passwords, network encryption, and frequent software updates to protect against unauthorized access.

Video Management System (VMS)

A Video Management System (VMS) is crucial for the effective management of video surveillance operations. It integrates video recording, retrieval, and storage with management of multiple cameras. VMS platforms offer a variety of functionalities, including live video feeds, playback, and sophisticated analytics. Some of the leading VMS solutions include:

- **Milestone Systems: XProtect**
- **Genetec: Security Center**
- **Nexvision: NEXVMS**
- **Avigilon: Avigilon Control Center (ACC)**
- **Honeywell: MaxPro VMS**
- **Axis Communications: Axis Camera Station**
- **Qognify: VisionHub**
- **Bosch: Bosch Video Management System (BVMS)**
- **Pelco: VideoXpert**

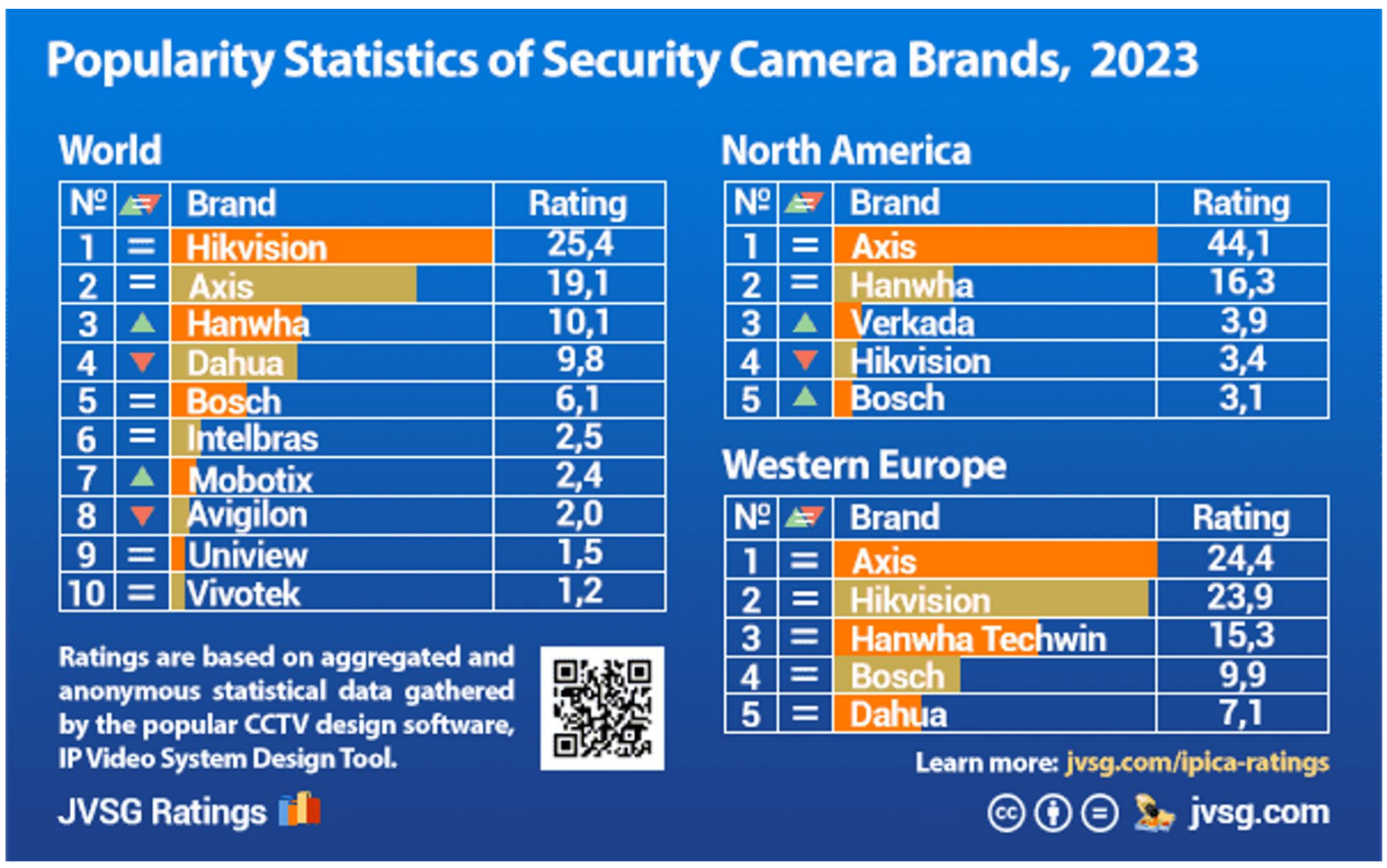
These systems can often be integrated with other enterprise management tools such as Active Directory, which aids in centralizing and streamlining user permissions and access controls across the network, enhancing both operational efficiency and security. Understanding these systems and their interactions is essential for deploying a secure and effective CCTV network. IT professionals must carefully evaluate each component's role within the broader security strategy to ensure comprehensive surveillance coverage and robust protection against both physical and cyber threats.

Key CCTV Industry Players and Market Share

The CCTV camera market is a dynamic and competitive field, with key players driving innovation and capturing significant market share. In 2019, Hikvision and Dahua were the frontrunners, holding impressive market shares of 43% and 20%, respectively. Other notable brands like Axis Communications, Bosch Security Systems, and FLIR also contributed to a global market valued at $21 billion.

By 2023, the landscape had evolved, with Hikvision and Axis consistently leading worldwide. Axis maintained its top position in North America and Western Europe, highlighting its strong reputation and widespread adoption in these regions.

Image 1: Leading CCTV Manufacturers 2023



Leading brands in the CCTV market are known for their advanced technological solutions, reliability, and comprehensive security offerings. Axis Communications is renowned for its high-quality surveillance solutions, while Hikvision is celebrated for its extensive range of products and cutting-edge technology. Other significant players, such as Hanwha Techwin, Bosch, and Dahua, continue to innovate, ensuring robust security and performance across various industrial applications.

Overall, the CCTV camera market is characterized by rapid advancements and fierce competition, with key players constantly innovating to meet the growing demand for enhanced security and surveillance solutions.

Trout

Security Incidents and Cyber Attacks on CCTV Systems

The landscape of cyber threats targeting CCTV systems has seen a range of sophisticated and impactful attacks in recent years. These incidents highlight the critical vulnerabilities within various surveillance technologies and underscore the need for enhanced security measures.

Major Cyber Attacks on CCTV Systems

Mirai Botnet Attack (2016)

A landmark in the history of cyber threats targeting IoT devices, including CCTV systems, the Mirai botnet orchestrated one of the largest DDoS attacks by exploiting devices with default usernames and passwords. It disrupted major websites and services across the US by leveraging infected devices to flood targets with overwhelming traffic. This incident illustrated the dangers of inadequate device security and the importance of regular updates and password management. Learn more

Inauguration Day (2017)

Days before President Donald Trump's inauguration, ransomware infected 70% of the storage devices recording data from Washington D.C.'s CCTV cameras. Although officials managed to rectify the situation without paying the ransom, the breach caused significant downtime and highlighted the risks of network-connected security devices. Details on the ransomware attack.

Verkada Breach (2021):

This breach exposed live feeds and archived footage from 150,000 security cameras, including those in high-security areas like hospitals and jails. Hackers accessed the cameras using a super admin account found online, showcasing the dangers of poor access control and the need for robust network segmentation and credential management. Insights into the Verkada breach.

Russia Hacking Ukraine (2022):

With the escalation of the Russo-Ukrainian war, Russian hackers targeted CCTV systems in Ukraine to monitor and interfere with the country's air defense systems, demonstrating how geopolitical conflicts can extend into cyber warfare. The incident also revealed the widespread use of insecure CCTV brands prone to hacking, such as Hikvision and Dahua. Coverage of Russian hacking activities.

Middle East Surveillance:

Various instances of hacking, such as Hezbollah accusing Israel of hacking CCTV systems and the Iranian hacker group Moses Staff gaining prolonged access to Israeli cameras, emphasize ongoing surveillance battles and the strategic importance of CCTV systems in international security. Details on the Middle East surveillance disputes.

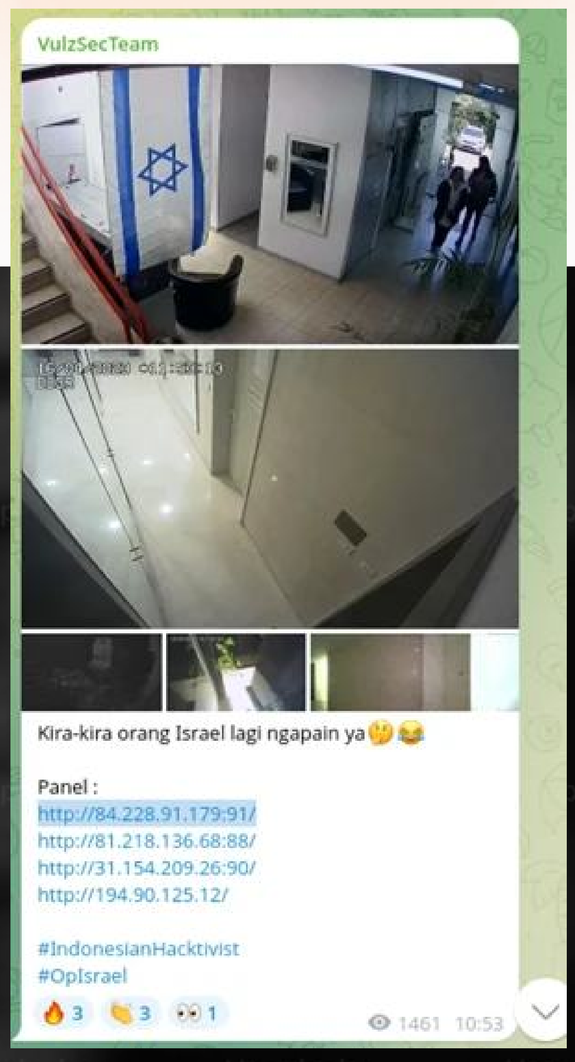


Image 3: Public Exposure of Security Camera Footage Leaked by VulzSecTeam Hacktivists - #IndonesianHacktivist #OpIsrael

Smaller-Scale CCTV Incidents

Residential and Small Business Hacks:

The numerous vulnerabilities identified in CCTV systems can result in severe security breaches affecting everyone from government officials to private individuals. Examples such as the Swann Security incident, where security flaws led to unauthorized camera access, the iLnkP2P Exploits that made millions of devices vulnerable to remote attacks, and the Dahua Camera Vulnerability Exploitation that could potentially allow attackers to take control of cameras, illustrate the wide-reaching impact of such vulnerabilities.

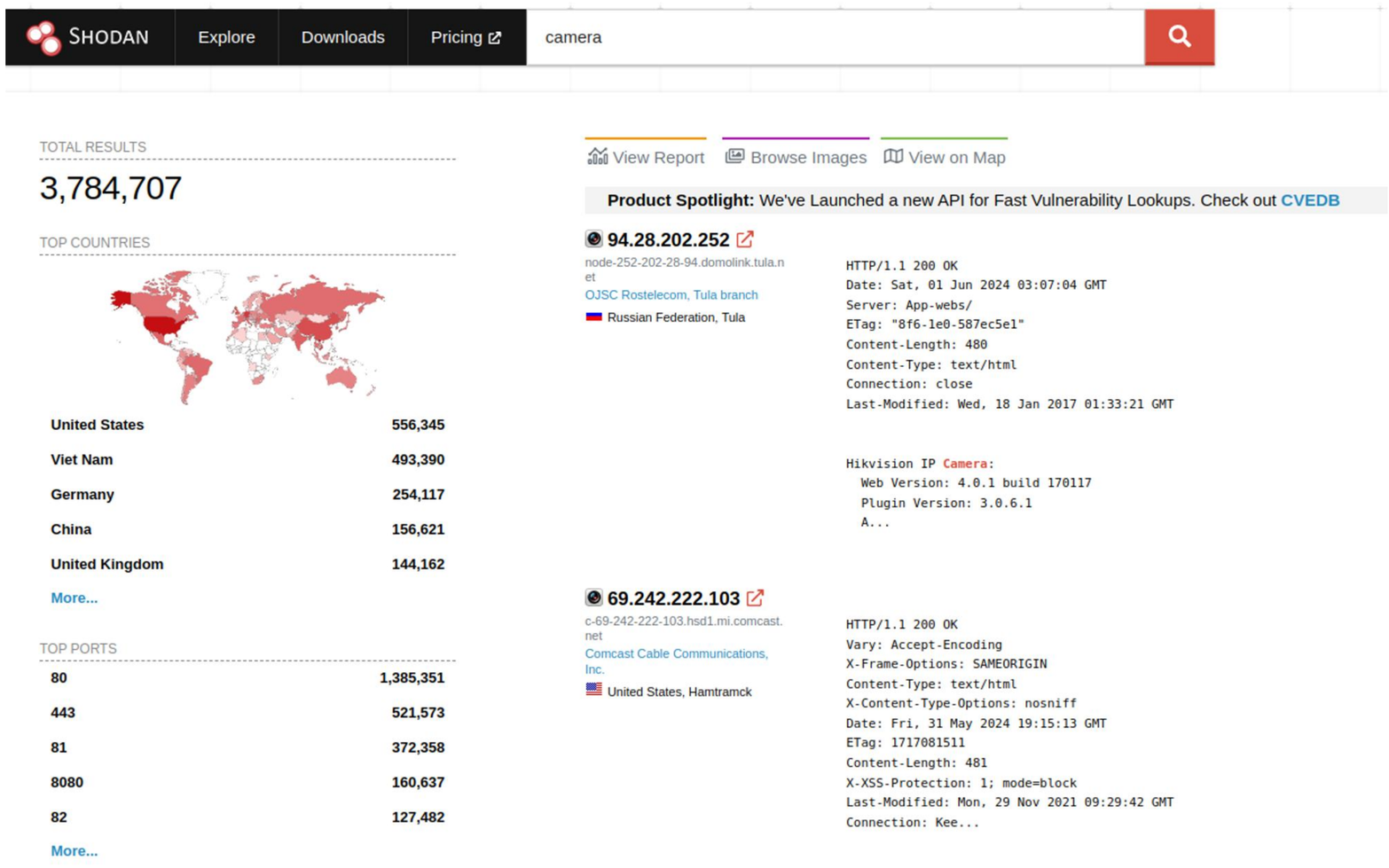
These security lapses have not only facilitated espionage and industrial spying but have also led to more personal privacy invasions. For instance, a group of Vietnamese cybercriminals hacked into residential cameras to capture and sell private footage on Telegram for as little as $16, as reported here. Additionally, a disturbing incident in Mumbai involved a young YouTuber who discovered that his private moments, captured unknowingly via a hacked home security camera, were being circulated on social media, as detailed here.

These events underscore the urgent need for robust security measures within CCTV systems to prevent unauthorized access and the misuse of sensitive and private data. Implementing stringent security protocols and continuously updating them is crucial to safeguarding the privacy and security of all individuals and organizations reliant on surveillance systems.

CCTV Security Vulnerabilities and Defense Mechanisms

When we delve into the vulnerabilities within CCTV systems, we uncover a range of security risks that cybercriminals can exploit. Let's take a closer look at some common vulnerabilities and recent findings that highlight the urgent need for strong security measures.

Image 4: Public Exposure of IP Cameras on Shodan (Screenshot from June 1, 2024)



Overview of Common Vulnerabilities

One of the biggest threats to CCTV security is the public exposure of IP cameras. Platforms like Shodan make it easy to find millions of potentially vulnerable cameras. Adding to this problem is the common use of default credentials, which is a well-known risk across many devices, from home security cameras to major network equipment.

The notorious Mirai Botnet highlighted the dangers of these vulnerabilities. It took advantage of exposed cameras with default credentials to launch widespread disruptions. This kind of exposure leaves systems open to threats like DDoS attacks and even crypto mining. Clearly, there's an urgent need for better security practices to protect these systems.
Additional vulnerabilities are frequently documented, revealing a variety of attack vectors as seen on platforms such as Vulners.

Case Studies of Documented Vulnerabilities in CCTV Systems

CVE-2024-5095 Victor Zsviot Camera 8.26.31

- **Command Injection:**

Vulnerability allowing command execution via a flaw in the special character filter, requiring prior authentication.

- **Denial of Service:**

Affects Hanwha's product discovery services; rebooting may temporarily resolve the issue.

- **Cross-Site Scripting:**

Malicious scripts can be injected into web pages, though this requires user authentication.

CVE-2024-3434 CP Plus Wi-Fi Camera

- **Improper Authorization:**

Attackers can bypass user management controls to access camera functions, with potential remote exploitability.

CVE-2022-41677 Bosch IP Cameras

- **Information Disclosure:**

Unauthenticated attackers can access sensitive device information, leading to broader network exposure.

CVE-2023-28704 Furbo Dog Camera

- **Command Injection:**

Attackers within Bluetooth range can inject commands due to insufficient input filtering.

CVE-2023-3959, CVE-2023-45225, CVE-2023-43755, CVE-2023-39435, CVE-2023-4249 Zavio IP Camera

- **Stack-based Buffer Overflows and Command Injection:**

Multiple vulnerabilities allowing for remote code execution and command injection, highlighting critical security gaps.

CVE-2017-11635, CVE-2017-11634, CVE-2017-11633, CVE-2017-11632 Wireless IP Camera 360

- **File and Data Access, Network Vulnerabilities:**

These vulnerabilities range from unauthorized access to stored recordings to the discovery of administrative credentials via exposed network services.

These examples highlight the range of vulnerabilities present in modern CCTV systems and the necessity for continuous monitoring, regular updates, and stringent security protocols to mitigate these risks effectively.

MITRE CCTV Tactics and Techniques

Tactic	Technique	Technique Name	Context
TA0108	T0883	Internet Accessible Device	A vast number of devices, including IP cameras, are discoverable on platforms like Shodan, making them vulnerable to unauthorized access if not properly secured.
TA0109	T0812	Default Credentials	Vulnerabilities such as CVE-2022-41677 (Bosch IP Cameras) and CVE-2017-11632 (Wireless IP Camera 360) involve default credentials, a common exploitation point for attackers to gain initial access. The Mirai botnet exemplifies how attackers use default credentials to infect and control devices.
TA0108/TA0109	T0866	Exploitation of Remote Services	Examples like CVE-2024-5095 (Victor Zsviot Camera) and CVE-2017-11634 (Wireless IP Camera 360) show how attackers exploit remote service vulnerabilities to gain unauthorized access. This access can lead to further network penetration, where attackers leverage the compromised cameras as entry points to potentially access more valuable network resources.
TA0107	T0814	Denial of Service	Attacks like those leveraging CVE-2024-5095 (Victor Zsviot Camera) and multiple CVEs in Zavio IP Camera illustrate how vulnerabilities can be used to launch denial of service attacks, disrupting the functionality and availability of the affected devices.
TA0108/TA0109	T0886	Remote Services	CVE-2022-41677 (Bosch IP Cameras) and CVE-2017-11633 (Wireless IP Camera 360) demonstrate attacks where remote services are exploited to extract sensitive data like RTSP credentials, posing significant privacy and security risks.
TA0106	T0855	Unauthorized Command Message	CVE-2023-28704 (Furbo Dog Camera) showcases a vulnerability that allows attackers to remotely inject unauthorized commands, potentially leading to further exploitation or control over the device.
TA0110/TA0109	T0891	Hardcoded Credentials	The presence of hardcoded credentials, as seen in CVE-2017-11632 (Wireless IP Camera 360), is a critical security flaw that attackers can exploit to gain unauthorized access, highlighting the need for stringent credential management practices.
TA0110	T0889	Modify Program	The Mirai botnet is an example of how attackers can modify the programming of devices like CCTV cameras for purposes like DDoS attacks or crypto mining, showing the versatility of the threats facing improperly secured devices.

1. Reconnaissance (Initial Access):

- **TA0108: Internet Accessible Device**

Adversaries perform reconnaissance to identify Internet-accessible devices, such as IP cameras, which can be discovered on platforms like Shodan. This stage is critical in the cyber kill chain for identifying potential targets.

---

2. Weaponization and Delivery:

This phase involves preparing and sending a malicious payload designed to exploit the identified vulnerabilities. Not explicitly detailed here, but it's typically where malware or malicious code is packaged in a way that targets the vulnerabilities discovered during reconnaissance.

---

3. Exploitation:

- **TA0109: Default Credentials**

Attackers exploit known vulnerabilities, such as default credentials in remote services like TCP ports, gaining unauthorized access. This is a common method of attack due to its simplicity and high success rate.

- **TA0108 / TA0109: Exploitation of Remote Services**

Further exploitation of remote services occurs, allowing attackers to access sensitive information or gain extended control over the system.

---

4. Installation:

This step involves installing the malware or backdoor on the target system to ensure persistence of the attack, allowing continued access and control.

5. Post-exploitation (Command and Control):

- **TA0107: Denial of Service**

Attackers may engage in denial of service attacks to disrupt services, leveraging the vulnerabilities they have exploited.

- **TA0108 / TA0109: Remote Services**

Continued exploitation of remote services enables further data theft or system manipulation.

- **TA0108 / TA0109: Remote Services**

Continued exploitation of remote services enables further data theft or system manipulation.

- **TA0106: Unauthorized Command Message**

Attackers inject unauthorized commands remotely, often leading to further system exploitation or data breaches.

- **TA0110 / TA0109: Hardcoded Credentials**

Utilization of hardcoded credentials within systems to maintain unauthorized access or control over systems.

- **TA0110: Modify Program**

Modifications to programs, such as inserting malicious code or repurposing existing functionalities for attacks like DDoS or crypto mining.

---

6. Actions on Objectives:

The final stage where attackers achieve their ultimate goal, whether it's data exfiltration, sustained access, or causing long-term damage.

Trout

MITRE Mitigation Strategies

1. Internet Accessible Device (TA0108):

- Implement stringent access controls and authentication mechanisms to prevent unauthorized access.
- Use network segmentation to isolate IoT devices from critical internal systems, reducing the lateral movement capabilities of an attacker.

---

2. Default Credentials (TA0109):

- Immediately change default passwords upon device setup.
- Enforce strong password policies and regular password changes.
- Restrict or disable remote access if not necessary, minimizing potential entry points.

---

3. Exploitation of Remote Services (TA0108 / TA0109):

- Regularly update and patch systems to fix known vulnerabilities.
- Deploy IDS/IPS systems to monitor for and respond to suspicious activities.
- Employ network segmentation to protect critical assets from compromised devices.

---

4. Denial of Service (TA0107):

- Use rate limiting and traffic shaping to mitigate the impact of potential DoS attacks.
- Configure robust failover and redundancy protocols to maintain service continuity.

---

5. Remote Services (TA0108 / TA0109):

- Disable unnecessary services and close unused ports.
- Implement strong encryption protocols for any remote communication.
- Enhance security with multi-factor authentication to verify user identities effectively.

---

6. Unauthorized Command Message (TA0106) and Hardcoded Credentials (TA0110 / TA0109):

- Sanitize all inputs to prevent command injection attacks.
- Regularly audit and update any hardcoded credentials.
- Utilize encrypted storage for sensitive information and credentials to prevent unauthorized access.

---

7. Modify Program (TA0110):

- Monitor and control software updates and modifications to detect unauthorized changes and potentially malicious activities.

Enhanced Security with Demilitarized LAN (DLAN) for CCTV Systems

The concept of Demilitarized LAN (DLAN) significantly transforms the security landscape of CCTV systems. By creating a software-defined DMZ (Demilitarized Zone) around critical assets, DLAN offers extensive monitoring capabilities, robust network defenses, and advanced filtering features.

DLAN Integration in CCTV Security

DLAN enhances CCTV security by dynamically managing network access and resource allocation in response to evolving security needs and threat landscapes. Key features include:

- **Strategic Traffic Segregation:**

DLAN isolates CCTV traffic from the broader corporate network, reducing the risk of cross-network attacks and maintaining the integrity of surveillance operations.

- **Dynamic Network Segmentation:**

Utilizing smart network switches and routers, DLAN can modify network segments in real-time, isolating compromised cameras and mitigating potential threats swiftly.

- **Enhanced Access Controls:**

Rigorous access controls and authentication measures ensure that only verified devices and personnel can access the CCTV network, with permissions adjusted dynamically based on threat levels.

Real-Time Threat Detection and Response

The integration of DLAN into CCTV systems involves deploying network behavior analysis tools that continuously monitor traffic for anomalies. When unusual activity is detected, the DLAN system can instantly reconfigure the network to counter potential threats, such as isolating compromised devices or restricting access to critical areas.

Proactive and Comprehensive Protection

This proactive strategy shields the CCTV infrastructure from external threats and addresses internal vulnerabilities, preserving the integrity and continuity of surveillance operations. DLAN technology enables real-time visibility into asset and behavior tracking, promptly identifying and mitigating security threats.

Benefits of Software-Defined DMZ

The software-defined DMZ further enhances security by providing granular control over network traffic. Each asset within the DLAN is protected by tailored Access Control Lists (ACLs) applied per specific use cases, ensuring high-level security. This approach simplifies implementation while delivering robust protection against unauthorized access and data manipulation.
DLAN is helping organizations transform their CCTV security, achieving a high level of protection with simplified deployment and enhanced operational efficiency.

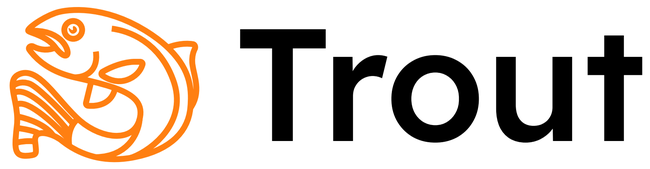
Conclusion

This whitepaper has outlined the critical role that CCTV systems play within our modern security frameworks, detailing the technological intricacies, potential vulnerabilities, and the ever-evolving landscape of cyber threats. As surveillance technologies continue to advance, so too do the methods and tactics of those who seek to exploit these systems for malicious purposes. It is clear that maintaining the security and integrity of CCTV operations is not merely a matter of implementing the right technology, but also of sustaining rigorous security protocols, continuous system monitoring, and rapid response strategies.

In response to the sophisticated cyber threats discussed, organizations must adopt a proactive security posture. This involves a multi-layered approach that includes regular updates to firmware and software, robust password management, strategic network segmentation, and comprehensive monitoring and response systems. Moreover, training and awareness for all stakeholders involved are indispensable to ensure that best practices are followed and security gaps are swiftly addressed.

The incidents and vulnerabilities highlighted throughout this document underscore the urgency for enhanced security measures. Organizations must not only aim to protect against known threats but also anticipate new challenges in an ever-shifting technological landscape. Implementing the recommended mitigation strategies will not only safeguard CCTV systems but will also enhance the overall resilience of the organizations' security infrastructure.

The goal of this whitepaper is to empower IT professionals and cybersecurity teams with the knowledge and strategies needed to defend their surveillance systems against potential breaches effectively. By staying informed of new threats and adapting to emerging technologies, we can ensure that our security systems not only serve their intended purpose but also contribute positively to our broader security culture. This proactive approach to cybersecurity will be crucial in maintaining the trust and safety that is so vital in our interconnected digital world.


Trout