Case Analysis of Yiwu Broadcasting Technology's Response to Ransomware Attack (Postprint)

Authors: Fang Daxing

Date: 2023-10-08T00:00:00+00:00

Abstract

As broadcast technology continues to evolve, the integration of broadcast program production and distribution with the Internet has become increasingly profound. In the current climate of escalating virus propagation, constructing a cross-network system that remains nearly transparent to presenters while maximizing broadcast security represents a critical challenge for broadcast technology professionals.

Full Text

Case Analysis of Yiwu Broadcasting Technology's Response to Ransomware Attacks

Abstract: With the development of broadcasting technology, broadcast program production and transmission are increasingly integrated with the Internet. In an era of rampant virus propagation, building a cross-network system that remains nearly transparent to presenters while maximizing broadcast security represents a critical challenge for broadcasting technology professionals.

Keywords: ransomware; full station network; network isolation gateway; multi-speed fast recording system

Classification Code: G222
Document Code: A
Article ID: 1671-0134(2017)11-076-03
DOI: 10.19483/j.cnki.11-4653/n.2017.11.024

Author: Fang Daxing

1. Ransomware Propagation and Prevention Requirements

On May 12, 2017, a ransomware virus named "WannaCry" attacked over 150 countries and regions worldwide, impacting government departments, healthcare services, public transportation, postal services, communications, and automotive manufacturing. Ransomware is a new type of computer virus that primarily spreads through email, Trojan programs, and malicious web pages. Once it infiltrates a local system, it automatically executes while deleting its own samples to evade detection and analysis. The ransomware then leverages local internet access permissions to connect to the hacker's C&C server, uploads machine information, and downloads encryption keys to encrypt files. After encryption, it modifies the desktop wallpaper and generates ransom notes in prominent locations, instructing victims to pay for decryption. Using various encryption algorithms, the virus renders files inaccessible, and victims generally cannot decrypt them without obtaining the private key. This can result in critical files becoming unreadable and essential data being corrupted, severely disrupting normal operations.

On May 18, the Yiwu Municipal Propaganda Department issued an emergency notice: a global ransomware worm outbreak had occurred, and all units must assign dedicated personnel to inspect their computers and report infections to the Municipal Cyberspace Administration. Organizations were required to coordinate staff and support vendors to close firewall and switch ports while completing system patch upgrades, and to promptly install antivirus software such as 360 capable of detecting and eliminating encrypted ransomware worms. The specific ports to be closed were: TCP/UDP: 135, 137, 138, 139, 9995, 9996, 593, 445, and tcp: 5554, 4444 and udp: 1434.

2.1 Yiwu Broadcast Audio Full Station Network Overview

Yiwu Broadcasting employs Infomedia's full station network system (Figure 1 [Figure 1: see original paper]), which is internally divided into broadcast and production networks. To ensure broadcast security, the broadcast network has been continuously streamlined—maintaining a simple, efficient broadcast network focused exclusively on transmission better safeguards broadcast security. Consequently, a broadcast station for a single program channel generally comprises no more than three units. Conversely, the production network has continuously expanded to meet business and development demands. The diverse requirements for broadcast program production and functions oriented toward customers and programming trends mean that a large-scale production system can satisfy various user functional needs without concern that feature additions might compromise broadcast security. The production network integrates program collection, editing, and broadcasting into a unified system, encompassing multimedia news subsystems, program production subsystems, publishing subsystems, media asset management, and other components. These subsystems all center on program broadcasting, coordinating operations with one another. The news subsystem handles news program collection and news script genera-

tion and management, while the program production subsystem manages audio program production. Finished programs can be sent to the broadcast system for transmission or distributed to other application systems via the publishing system. Programs produced by either the news management subsystem or the program production subsystem can be released through the content publishing subsystem, both for broadcast use and for other applications.

When Yiwu's broadcast production and transmission system was originally designed, cross-network segment deployment was implemented to facilitate expansion. The production network connects to the internet through a network isolation gateway (with non-IP-based connectivity between the production network and internet), while production stations are partially deployed on the internal network and mostly on the external network. External production stations can transparently access production and broadcast servers on the internal network through the network isolation gateway, with operations and usage identical to internal network stations. However, direct deployment of production stations on the external network significantly increases access to various internet-based materials and time-sensitive content for program production, greatly benefiting program quality and topicality. Other application systems can directly browse and query program data from the production system and scheduling information for each broadcast program on the transmission system through standard interfaces, and can download, use, and modify broadcast schedules within authorized permissions. The system uses a media-specific network isolation gateway that provides simplified support for basic protocols such as HTTP, FTP, and UDP, ensuring that essential webservice applications, FTP file transfer applications, and media assets can operate smoothly. With support from these middleware applications, program production across the production internal network, integrated business network, and internet can transparently penetrate the network isolation gateway, enabling secure, efficient, and collaborative program production.

With so many ports now closed, determining which ports the system requires necessitated a step-by-step walkthrough of the program collection, editing, and broadcasting workflow after closing switch ports.

2.2 Yiwu Broadcast Audio Production Workflow and Network Architecture

Program Production and Broadcasting Workflow: (1) Users log in to the XStudio production management software system; (2) Enter the personal project area for program production, create new projects, invoke the audio editor, complete audio recording and editing, and send finished programs; (3) In the task review list, perform permission-based query browsing and review functions; (4) In the production task list, view the review status of produced programs; (5) Programs sent to the production library are saved in the material finished product area; (6) Programs sent to the broadcast library are saved in the broadcast finished product area; (7) Program broadcasting, including

sending to linear program schedules, sending to JINGLE lists, and sending to broadcast finished product libraries for query, retrieval, and broadcast calling.

In addition to XStudio for program broadcasting, LogEditor can also be used to arrange daily broadcast program schedules.

Figure 1 System Network Structure Diagram

3.1 Ensuring Smooth Workflow Implementation

Broadcast program materials fall into three main categories: The first includes simultaneous slow recording of national, provincial, and sister stations' radio and television programs; the second comprises internet-based audio materials, including the latest songs and various sound effects; the third consists of high-quality programs and program manuscript systems produced by in-house hosts.

The first category uses Lianhui's PRODS slow recording system, which accesses files through folder network sharing. After closing ransomware propagation ports, same-floor access remained functional, but cross-floor slow recording systems could no longer read files. The second category of internet audio materials uses HTTP and FTP protocols when transmitting files from external workstations to the production network, enabling cross-network segment and cross-floor usage. The third category of in-house produced programs is generally completed within the production network, posing no cross-network issues. The manuscript system uses the HTTP protocol, and port closures did not affect it.

To resolve the issue of slow recording being unusable across floors, broadcasting technology addressed this by adding internal network workstations within the production network. Through internal testing and minor adjustments to the internal network structure, the entire broadcast collection, production, editing, and broadcasting process remained smooth after closing ransomware propagation ports.

3.2 Optimizing Inter-Network Security

After ensuring the entire broadcast collection, production, editing, and broadcasting workflow, broadcasting technology optimized inter-network security for the entire broadcast system.

The production network and internet are isolated using two NetGap200 network isolation gateways operating in mutual backup configuration. The two gateways work in parallel, with each handling network traffic for one floor. NetGap200 is a second-generation secure network isolation and information exchange cybersecurity product. It divides the network into trusted and untrusted sections. The initial configuration resides on the trusted network side, while the untrusted side can only accept and transmit data through specified channels, ports, and file formats mandated by the trusted side. Data exchange occurs through dedicated transmission components. The system efficiently blocks data outside specified

channels, ports, or qualified formats, preventing various network-layer and operating system-layer attacks, and achieves high-speed real-time data transmission through hardware-based SGAP systems.

The network isolation gateway restores data to its original form at the network model's application layer, then transmits it by "ferrying raw data." Network commands and TCP/IP protocol packets cannot penetrate the isolation system. NetGap200 also features powerful protocol termination, protocol inspection, and content review functions to ensure the trusted network remains unharmed and protect the security of resource, information, and data exchanges between networks.

NetGap200 has been optimized for radio and television systems' special requirements. It can configure permitted file formats according to broadcast program production process requirements. It ensures file transmission security by encrypting and decrypting audio files that pass through. It can effectively identify and prevent deceptive practices such as tampering with file name extensions or embedding malicious code in audio files. For files permitted into the internal network, we optimized the system to only allow broadcast audio S48 files.

3.3 Implementing Multi-Speed Fast Recording System and Network Re-optimization

The multi-speed fast recording system was activated to achieve complete physical isolation between the production network and the internet. The fundamental principle of the multi-speed fast recording system is audio dubbing—a safe and conservative approach. Traditional audio dubbing required manual operation, whereas the multi-speed fast recording system automates dubbing start and stop without requiring other communication mechanisms, relying solely on the audio signal itself for triggering. Commands such as audio start dubbing, stop dubbing, audio file names, and usernames are also transmitted through audio dubbing using a telegraphy-style method, as normal audio cannot contain such continuous short pulses. The system identifies these audio short pulses as codes and parses them. These audio pulse-coded signals do not exist in completed dubbed audio files, achieving fully automated dubbing start and stop.

Audio dubbing is performed using AES3 or MADI interfaces with a multiple sampling rate approach. For a 48KHz audio file, we use 192KHz for dubbing, reducing dubbing time by a factor of four. Multi-channel sound cards enable synchronous dubbing of a single file. Using an 8-channel AES3 sound card, the audio file to be transmitted is first split into eight audio files, which are simultaneously dubbed using eight AES channels at 4x speed, achieving total dubbing efficiency of 8$\times$4 = $32 times. Yiwu Broadcasting uses 64-channel MADI, achieving dubbing efficiency up to 64$\times$4=256 times. These methods reduce audio dubbing time by dozens of times—a one-hour audio file can be transmitted across networks in just one or two minutes, without requiring manual computer monitoring. Internal and external networks achieve

complete physical isolation, relying only on audio cables for dubbing.

The multi-speed dubbing system is essentially an audio device (Figures 2 [Figure 2: see original paper]~3), integrating with other systems through files as the sole carrier. Audio files requiring transmission only need to be placed in folders monitored by the multi-speed system, which automatically begins dubbing. Through the multi-speed system, broadcasting can easily enable external journalists to transmit audio materials to the internal network. The simple method (Figure 4 [Figure 4: see original paper] Multi-speed System Simple Connection) involves setting up FTP or HTTP services to receive audio file transmissions and automatically forwarding them to the multi-speed system, while complex methods (Figure 5 [Figure 5: see original paper] Multi-speed System Complex Connection) include integrating external network news collection and editing systems with the multi-speed dubbing system. This achieves complete physical isolation between internal and external network systems.

After activating the multi-speed system, its pure physical isolation provides a higher level of broadcast security assurance compared to the logical isolation of network gateways. However, Yiwu Broadcasting Technology did not abandon the network gateway system. Instead, the entire system normally operates through the multi-speed system, with the network gateway serving as a backup. Should the multi-speed system encounter problems, the network gateway can still function, providing Yiwu Broadcasting Technology with multiple security assurance methods for inter-network security.

References: [1] Peng Peng, He Shaodan. Research and Design of Broadcast Production System Based on Cloud Computing [J]. Radio & Television Technology, 2013, (7). [2] Ding Lin. “Epidemic” Sweeps the Globe, Why Is It So Virulent [J]. Friends of Science (First Half), 2017(07).

(Author’s Affiliation: Zhejiang Yiwu Radio and Television Media Group)

Note: Figure translations are in progress. See original paper for figures.