AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

How Ampcus Cyber Performed Rapid Malware Containment for Healthcare Security?

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Overview:

A healthcare organization experienced a malware infection that spread across several systems within its network, disrupting critical operations & patient records.

The Problem:

Malware Spread:

The malware infected across multiple workstations within the network, leading to increasing the risk of unauthorized access to sensitive patient data and highlighted gaps in endpoint security and patch management.

Operational Disruption:

The affected systems included critical components of the healthcare environment, leading to interruptions in routine operations. As a result, key services were delayed, impacting both clinical workflows and overall service delivery.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Actions Taken:

Our Forensic team investigated and discovered the root cause and shared recommendations. The following were the step taken by the team:

Step 1

Malware Spread Identified:

The investigation confirmed that the malware propagation was directly linked to outdated software within the environment. Unpatched systems created an entry point, enabling the threat to establish a foothold and move laterally across multiple endpoints.

Step 2

Vulnerability Remediation Needed:

Immediate remediation actions were recommended, including applying critical patches and updating affected software to close known vulnerabilities.

Step 3

Security Enhancements:

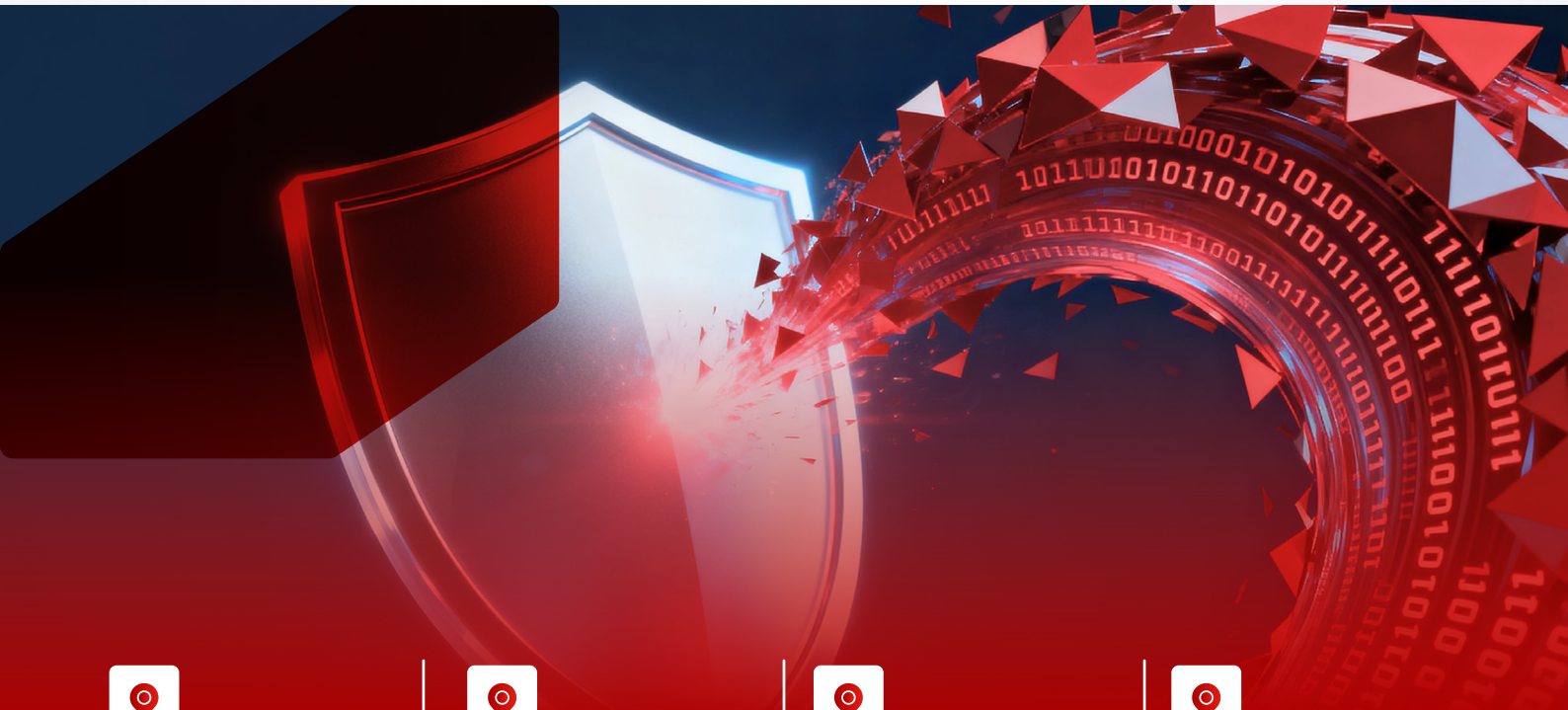
To strengthen the overall security posture, enhanced endpoint protection measures were advised. This included deploying advanced threat detection, improving monitoring capabilities, and implementing stricter controls to reduce the likelihood of future malware incidents.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Key Outcomes:

The rapid containment and forensic response enabled the organization to limit the spread of malware before it could escalate into a full-scale breach. Critical systems were stabilized, minimizing operational downtime and preventing unauthorized access to sensitive patient data. By addressing the root cause and implementing targeted remediation, the organization strengthened its endpoint security, improved patch management practices, and enhanced overall threat detection capabilities.

As a result, the healthcare provider restored operational continuity, reinforced regulatory readiness, and established a more resilient security posture against future threats.



India
601-609A, 6th Floor, Beta Block, Sigma Soft Tech Park, Varthur Kodi, Whitefield, Bangalore, Karnataka - 560066.

USA
14900 Conference Center Dr, Suite # 500, Chantilly, VA 20151.

UAE
Office 306, Building A6, Dubai Digital Park, Dubai Silicon Oasis, Dubai.

Philippines
19th floor Exxa Tower, Bridgetowne, E.Rodriguez Jr. Ave cor C5 Road, Ugong Norte, Quezon City.

www.ampcuscyber.com

letsconnect@ampcuscyber.com