WHITEPAPER

Mitigate the Risk of Ransomware Attacks Against Critical Infrastructure with XONA

+1 866-849-6629 | info@xonasystems.com

THE SITUATION

Malicious cyber actors are targeting and attacking critical infrastructure, including industrial control systems, at an increasingly rapid pace. Ransomware attacks targeting operational technologies pose both a significant safety and economical threat to organizations and the general public.
The NSA warns in a recent alert:: "Without direct action to harden OT networks and control systems against vulnerabilities introduced through IT and business network intrusions, OT system owners and operators will remain at indefensible levels of risk."

THE CHALLENGE

Corporate leadership is faced with a dilemma of how to mitigate the exposure to ransomware attacks on OT control systems without impacting operations. Malicious cyber actors are attacking OT through compromised IT corporate networks or unprotected OT access points, as evidenced by the recent attacks on Colonial Pipeline and JBS. Hackers penetrate environments via phishing campaigns to gain access to user credentials and then deploy malware into the environment.

While many OT systems are segmented and not integrated with enterprise IT systems, segmentation alone is not a defense – hackers are finding open ports without proper access and protocol controls. Cyber experts recommend taking steps to mitigate attacks against OT, including:

1. Fully managing all IT-OT connections
2. Limiting access
3. Isolating protocols
4. Actively monitoring and logging all access attempts
5. Cryptographically protecting remote access vectors

XONA KEY BENEFITS:

- Secure "clientless" browser-based multifactor authentication (MFA) vendor asset management system
- Reduced cost through operational efficiency
- Role-based vendor technician to asset mapping
- Secure application access for monitoring and session logging
- Application screen recording for forensics and training
- Management, visibility and control of XONA user to system access
- Reduced cyber-attack surface
- NERC-CIP compliant

RECOMMENDATIONS TO REDUCE RISK OF RANSOMWARE ATTACKS

It is clear that the OT industry is not immune to cybersecurity risk. OT control systems have used segmentation as the main defense against attacks for years. However, the reality is that recent attacks have shown hackers are accessing internet-accessible industrial control assets including programmable logic controllers (PLCs) as well as finding and using open ports and back doors through OEM software and downloads.

A new paradigm for OT operators is to assume their networks have been compromised and implement encryption, authentication and granular authorization to at all OT network assets. **Effectively, OT systems need a Zero-Trust, secure operational gateway for user access with Multi-Factor Authentication (MFA), flexible role and time-based user and vendor access controls as well as full session logging, monitoring and recording.**

These security features should be extended to include any remote access connections. While hackers may penetrate a network with stolen credentials and passwords, a secure operational gateway with built-in hardware token- based MFA effectively blocks credential theft, reducing OT cybersecurity risk. OT operators need to create an asset and network map that includes identifying all known OT network communication and effectively integrate with the operational user access gateway to reduce cyber-attack surface.

THE SOLUTION

The XONA Critical System Gateway (CSG) was designed specifically to provide Zero-Trust secure user access for the OT environment. **The CSG directly addresses ransomware cyber risk through hardware token-based multi-factor authentication (MFA), user session recording, user-to-asset monitoring, OT protocol isolation, encrypted screen remoting and auditable connection logs.**

XONA CSG also enables secure remote operations for OT operators to access asset management software, HMI and PLCs to allow operations to manage remotely and communicate with control centers. The CSG was designed and built specifically for the OT environment.

THE RESULTS

REDUCTION OF CYBER RISK WITH STRONG USER AUTHORIZATION ON ACCESS POINTS

Remote access connections to OT assets are protected with complex ID/ password combinations coupled with MFA, OT protocol isolation, session logging, user access and recording and VDI with data-in-transit. XONA CSG is fully compliant with NERC-CIP elements for user access.

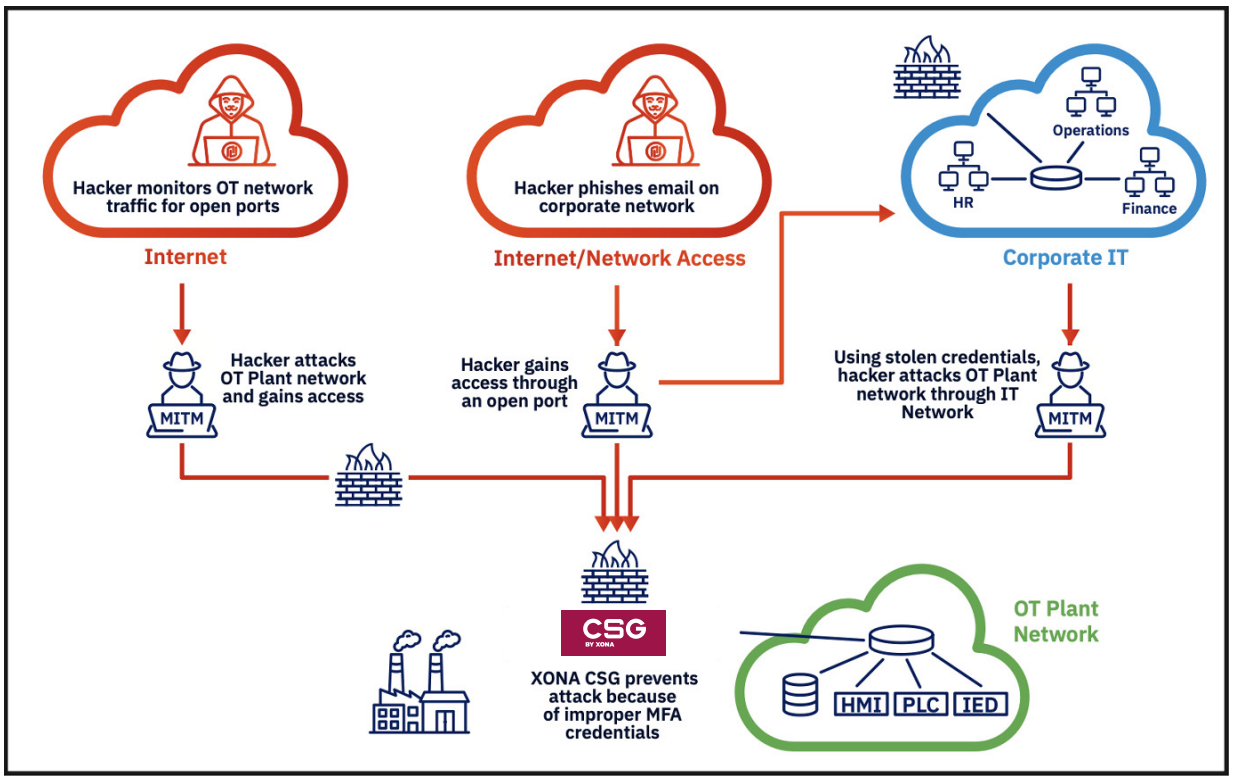
COST-EFFECTIVE, SIMPLE AND SECURE DEPLOYMENT OF A ZERO-TRUST, SECURE OPERATIONAL GATEWAY

The XONA CSG is a simple, secure and cost-effective solution for visibility and control to protect access to industrial control systems and plant operations. The CSG platform is a single appliance requiring no IT or cloud architecture to implement in the OT environment.

EFFECTIVE ACCESS MANAGEMENT FOR MITIGATION OF UNAUTHORIZED ACCESS

XONA CSG provides functionality for granular Zero-Trust-based user access by user role, time and specific system or application connection.

HOW XONA PROTECTS OT FROM RANSOMWARE ATTACKS



XONA ZERO-TRUST OT USER ACCESS PLATFORM

Whether as a remediation action within the first 72 hours of a cyber-attack or proactive securing of OT access connections, the XONA CSG can be deployed in hours and does not require multiple point access technologies. XONA understands the OT environment and what is required to operate securely in this specialized environment.

Let us show you our secure and cost-effective Zero-Trust solution.

Call or visit our website today to schedule a live demo

+1 866-849-6629 | info@xonasystems.com

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

+1 866-849-6629 | info@xonasystems.com