Highlights from the

2020 GLOBAL IoT/ICS RISK REPORT

A data-driven analysis of vulnerabilities in our Internet of Things (IoT) and industrial control system (ICS) infrastructure

Based on analysis of data collected from 1,821 real-world IoT/ICS networks using passive, non-invasive monitoring with patented deep packet inspection (DPI) and Network Traffic Analysis (NTA) algorithms.

CYBERX
BATTLE-TESTED CYBERSECURITY

Detailed in the CyberX Global 2020 IoT/ICS Risk Report, this analysis of real-world vulnerabilities from IoT/ICS network threats and unmanaged devices remains the only one of its kind.

Gaining visibility into IoT/ICS risk and mitigating these "hidden" vulnerabilities is critical to protecting organizations from costly production downtime, safety and environmental incidents, and theft of sensitive intellectual property.

Spanning diverse IoT/ICS systems — including robotics, refrigeration, chemical and pharmaceutical production, power generation and distribution, oil production,and building management systems (HVAC, CCTV, etc.) — the 2020 report is based on network data collected globally during the 12-month period spanning October 2018 to October 2019.

BROKEN WINDOWS: OUTDATED OPERATING SYSTEMS

62% **of sites have outdated and unsupported Microsoft Windows boxes such as Windows XP and Windows 2000**

Unsupported Windows boxes no longer receive regular security patches from Microsoft. The figure jumps to 71% if we include Windows 7, which reaches end-of-support status in January 2020.

HIDING IN PLAIN SIGHT: UNENCRYPTED PASSWORDS

64% **of sites have unencrypted (cleartext) passwords traversing their networks**

The reason cleartext is dangerous is because it makes gaining access to restricted systems easy — since these passwords are transmitted "in the clear" and can easily be sniffed. Legacy devices that don't support modern protocols such as SNMP v3 or SFTP are usually the culprits for leaving passwords in cleartext.

EXCESSIVE ACCESS: REMOTELY ACCESSIBLE DEVICES

54% **of sites have devices that can be remotely accessed using standard protocols such as RDP, SSH, and VN**

One of the primary attack vectors for ransomware is remote access protocols, which enable attackers to move laterally and expand their presence throughout networks.

CLEAR AND PRESENT DANGER: INDICATORS OF THREATS

22% **of sites exhibited indicators of threats**

CyberX's network traffic analysis flags suspicious activity such as scan traffic, malicious DNS queries, abnormal HTTP headers, excessive number of connections between devices, and known malware such as LockerGoga and EternalBlue.

NOT MINDING THE GAP: DIRECT INTERNET CONNECTIONS

27% **of sites analyzed have direct connections to the internet**

Security professionals and bad actors alike know that it takes only one internet-connected device to provide a gateway into IoT/ICS networks for malware and targeted attacks, enabling the subsequent compromise of many more systems across the enterprise.

STALE SIGNATURES: NO AUTOMATIC AV UPDATES

66% **of sites are not automatically updating their Windows systems with the latest antivirus definitions**

Antivirus is the very first layer of defense against known malware — and the lack of antivirus is one reason why CyberX still finds older malware such as WannaCry and Conficker in IoT/ICS networks.

Median Security Score Across All Industries: **69**

We recommend a minimum score of 80 to our clients. The scores across industries remained mostly consistent with our findings last year, with regulated industries such as energy utilities maintaining a slightly higher score than other industries.

74 Oil & Gas

70 Energy & Utilities

63 Manufacturing

62 Pharmaceuticals & Chemicals

62 Other

"Other" includes transportation, mining, data centers, and universities.

To download the full report, visit cyberX.io/risk-report-2020

CyberX performed this analysis on anonymized and aggregated metadata, with all customer-identifying information removed. Rigorous attention is paid to preserving the confidentiality of the customer information.

ABOUT CYBERX

We know what it takes.

CyberX delivers the only cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT/ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

Founded in 2013, CyberX is the only IoT/ICS security firm with a patent for M2M-aware threat analytics and machine learning technology. CyberX also delivers the only IoT/ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Partners include industry leaders such as IBM Security, Splunk, Palo Alto Networks, McAfee, Optiv Security, DXC Technology, Toshiba, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their IoT/ICS networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information, visit CyberX.io or follow @CyberX_Labs.

CYBERX
BATTLE-TESTED CYBERSECURITY