2023 CHEMICAL SECURITY SUMMIT BRIEFING

Cyber Threats Facing the Chemical Sector

Overview

SCOPE NOTE

Analyzed Chemical Sector and Chemical Facility Anti-Terrorism Standards (CFATS) voluntary-participating stakeholders using:

Cyber Hygiene-Vulnerability Scanning (CyHy-VS)

Web Application Scanning (WAS)

Assessment services

Open-Source Reporting

TIMEFRAME

July 1, 2022
to
June 30, 2023

CAVEAT

The entities depicted in this briefing **may not be considered statistically representative** of the complex and varied sector in the United States. However, **all entities are encouraged to adopt CISA's recommendations and best practices** as applicable.

The resulting analysis uses the MITRE ATT&CK® for Enterprise framework, Version 13.1

Notable Cyber Events in the Chemical Sector

Lazarus Advanced Persistent Threat (APT) likely targeted the Chemical Sector using job postings for defense contractors, employing (MITRE T1021) for network access. Post-compromise tools used were SiteShoter (MITRE T1513) and FastCopy (MITRE T1083).
Source: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

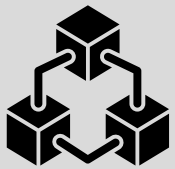
April 2022

October 2022

Lockbit 3.0 was the most prevalent ransomware group, making up 35% of the total ransomware attacks during the period of analysis and the only one to target the chemical sector, according to industry reporting. Lockbit 3.0 focused primarily on OT/ICS devices for initial access.
Source: https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q3-2022/

Key Findings for Chemical Sector Entities

CISA data showed Chemical Sector entities **exposed 19 known exploited vulnerabilities (KEVs)**.



CISA observed **exposure of industrial control system (ICS) assets** and **technologies used in OT environments.** Exploitation of these devices by a threat actor can lead to changes in chemical levels, disrupt normal operations, and cause physical harm to workers and customers alike.

Scanned entities **exposed one or more vulnerable services** (e.g., MS-Remote Procedure Call (MS-RPC) and Remote Desktop Protocol (RDP)) on internet-accessible hosts that, absent compensating or mitigating controls, can provide initial access into IT and OT infrastructure.

Key Findings for Chemical Sector Entities

Chemical Sector entities exposed **unsupported versions of FreeBSD, OpenBSD, and Windows operating systems (OS),** increasing exposure to vulnerabilities that can enable compromise.

Unsupported or insecure encryption, which threat actors are known to target, was observed across entities. This increases the risk of leaked credentials, sensitive information disclosure, and account enumeration.

Newly enrolled Chemical Sector entities in CISA's vulnerability scanning **reduced their exposed vulnerabilities by 42.3%** within the first three months of enrollment in CISA services, likely reducing opportunities for exploitation by threat actors.

Device Exposure Increases Risk to Physical and IT System Security

CISA observed that exposure of assets, without compensating or mitigating controls, put scanned Chemical Sector entities at risk of network exploitation. CISA data showed assets exposed to the internet:

- Printers, cameras, video game systems, and remote management interfaces (iLO devices) and Programmable Logic Controllers (PLCs).
- CISA advisories on PLC vulnerabilities include:
  - CVE-2016-2279 exploitation allows an attacker to inject arbitrary JavaScript into a user's web browser.
  - CVE-2020-12516 exploitation leads to denial-of-service (DOS) attack by sending a series of maliciously constructed packets to HTTP(S) ports, which may cause the device to crash.

Chemical Sector Remote Access Exposure Example

- Industry data revealed **exposure of remote access services**, such as the **Remote Desktop Protocol (RDP).**
- The RDP service is commonly used by threat actors to gain initial access, distribute ransomware, direct command and control, and exfiltrate data. When RDP services are internet-exposed, threat actors have visibility into the organization, location, domain name, and IP address (see Figure 2), which can lead to initial access to a network.

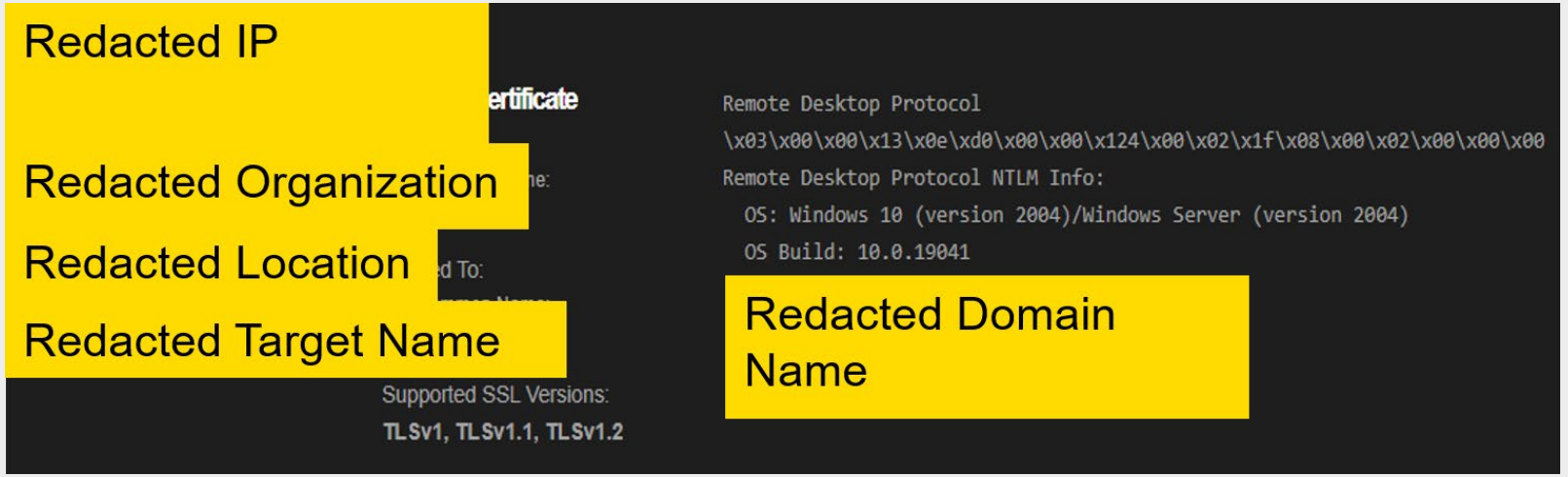


Figure 2: Industry data Screenshot of an exposed Remote Desktop Protocol (RDP) service Images by CISA | VM Insights during open-source research.

Cybersecurity Division | Vulnerability Management

Cyber Risk Summary Questions, Feedback and Mitigation Guide:

CSD_VM_Insights_Intake@cisa.dhs.gov

Cyber Hygiene Services

cisa.gov/cyber-hygiene-services

vulnerability@cisa.dhs.gov

Resource Guide

RESOURCE/SERVICE	DESCRIPTION
Cyber Hygiene Services	Scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.
CISA's Get Your Stuff off Search	CISA's guide to help entities identify their internet-accessible devices and protect their assets from potential harm.
CISA's Known Exploited Vulnerability (KEV) Catalog	CISA maintains a catalog of KEVs that carry significant risk to federal, public, and private sector entities.
CISA's ICS CERT Advisories	CISA alerts and advisories provide timely information about current security issues, vulnerabilities, and exploits.
Stopransomware.gov	StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.
Prioritizing Vulnerability Response (Stakeholder Specific Categorization)	System for prioritizing vulnerability management actions while avoiding one-size-fits-all solutions. Focused on a modular decision-making system with clearly defined and tested parts that vulnerability managers can select and use as appropriate to their context.
CISA's ICS Infographic	Recommended Cybersecurity practices for ICS implementation and management.
CISA Phishing Infographic	Summary of phishing methodology and recommended best practices.
Cross-Sector Cybersecurity Performance Goals (CPGs)	Version 1.01 published March 2023. Prioritized subset of IT and OT cybersecurity best practices aimed at reducing risk to both Critical Infrastructure (CI) operations and individuals. These are applicable across all CI sectors and incorporate the most common impactful threats and adversary tactics, techniques, and procedures (TTPs).

Appendix A: Data Collection Methods and Services

CyHy-VS tools are deployed to monitor internet-accessible systems of voluntary participants for known vulnerabilities, configuration errors, and suboptimal security practices. Using these tools, CISA can identify potential and known security issues and can then recommend mitigations to the impacted stakeholder. CISA scans IP addresses with the Nmap network scanner and probes responsive hosts with the Nessus vulnerability scanner to identify critical, high, medium, and low severity vulnerabilities based on the CVSS v2 scale of 0 to 10. Nessus references the National Vulnerability Database (NVD) for its vulnerability information. The NVD provides CVSS v2 base scores and corresponding severity levels for all Common Vulnerabilities and Exposures (CVEs). Scans use the range of IP addresses provided by the scanned entity.

CyHy WAS is "internet scanning-as-a-service." This service assesses the "health" of the publicly accessible web applications of voluntary participants by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.

Cybersecurity Assessments are one-on-one engagements between CISA and a voluntarily-participating entity that combine national threat information with the vulnerabilities CISA identifies through onsite or remote assessment activities. Assessments may include internet-accessible systems and internal systems. Assessment data derives from one or more of the various CISA offerings, including scenario-based network penetration testing, web application testing, social engineering testing, wireless network testing, configuration management reviews of servers and databases, phishing assessments, and network security architecture reviews. CISA uses security-engineering experts to conduct assessments over a fixed timeframe and defines the scope of each engagement by defining IP addresses, system names, and email addresses. At the assessment's conclusion, CISA provides an entity-specific risk analysis report that includes actionable remediation recommendations prioritized by risk. From July 1, 2022 to June 30, 2023, Chemical Sector entities participated in the following assessments: **Risk and Vulnerability Assessments (RVAs) and Validated Architecture Design Review (VADR).**