Food Ag ISAC

An IT ISAC Community

Built by industry *for industry.*

February 5, 2024

Food and Ag-ISAC Purpose

The Food and Ag-ISAC is a tailored forum for food and agriculture companies to:

- Engage with leading security experts and analysts from industry peers;
- Share cyber and physical threat intelligence and alerts;
- Drive effective security practices that help detect attacks, respond to incidents, and mitigate risks so they can better protect themselves and the sector; and
- Provide thought leadership to industry, government, and academia.

We are a cost-effective force multiplier for your security teams.

From a SIG to an ISAC

- IT-ISAC supported a Special Interest Group (SIG) for food and ag companies since 2013.
- SIG Members wanted an industry ISAC but did not want to lose the capabilities they had built through the IT-ISAC.
- The SIG launched the Food and Ag-ISAC in partnership with the IT-ISAC in May 2023.
  - Two ISACs, one low membership fee.
- The Food and Ag-ISAC leverages capabilities and analytic resources developed by the IT-ISAC over the past 20+ years.
- This structure also preserves the relationship between the technology industry that propels modern agriculture while providing the food and ag industry with a self-governing organization to engage in security issues specific to the industry.

Key Capabilities

- Mature capabilities - leveraging 23 years experience from the IT-ISAC.
- Adversary Attack Playbooks on dozens of threat actors.
- Ransomware tracker that contains thousands reports of ransomware, including those targeting the Food and Ag industry.
- Threat intelligence platform for automated sharing of indicators.
- Daily, weekly and incident specific, vendor neutral reporting.
- Bi-weekly meetings to discuss threats targeting the industry with peers.
- Engagement with other sectors, the National Council of ISACs, and government agencies.

Value to the Sector

> *Cyber experts have repeatedly cited the sector's lack of its own ISAC as a dangerous security gap in the industry's ability to get a full picture of the tremendous risks it faces. Backers of the ISAC, which includes major industry players like PepsiCo to Tyson Foods, expect it to fortify the defenses of its members.*

Tim Starks, The Washington Post Cybersecurity 202

May 25, 2023

Food Ag ISAC
An IT ISAC Community

Threat Environment Realities

- The attackers are already sharing with each other. They are well-organized, learning from each other, and actively collaborating.

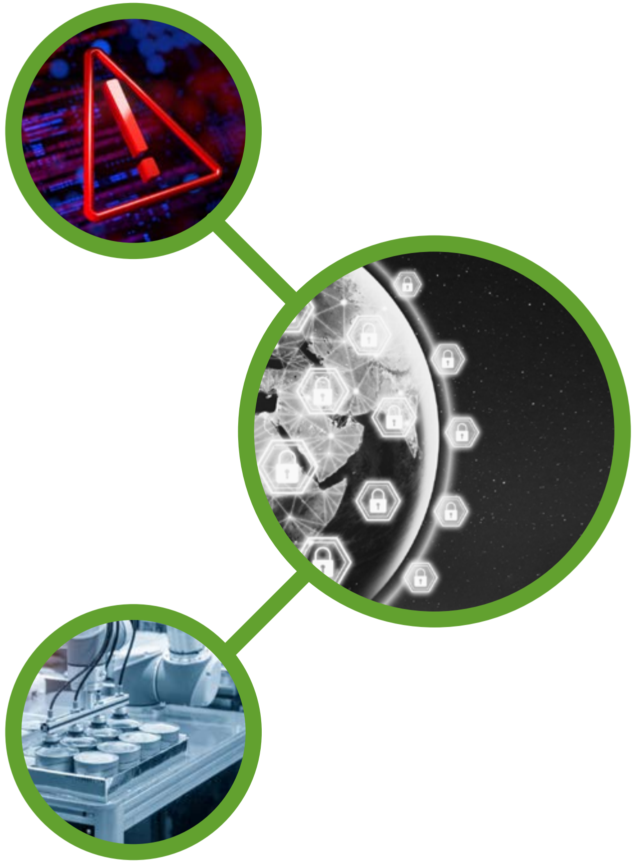
- The threat landscape is too complex for any one company to defend against alone. There are too many threat actors, too many vulnerabilities, and too few resources for any one company to adequately address the threat by itself.

- The economics of cybersecurity favor the attackers. It is more expensive to defend than it is to attack. Defenders need to maximize their resources.

Some Threats Facing the Sector

- **Advanced Persistent Threats (APT) Actors**
  Theft of intellectual property and economic data can help foreign nations shortcut their development process, which saves them time and resources.
  - *Groups that target the food and ag industry have existed since at least 2006.*

- **Ransomware**
  Attackers use malware to encrypt files on targeted servers, workstations, industrial controls systems and other essential technologies. Victims are given a ransom demand (typically paid in cryptocurrency) to unlock encrypted files and systems. Double extortion is also common, where threat actors may also leverage the leakage of stolen data to incentivize ransom payments.



Advanced Persistent Threat (APT) Actors

- Typically focused on data theft and espionage, especially of data involved in long term developmental intellectual property.

- There are a lot of wasted efforts in things like genetic development, and intellectual property can be especially valuable for specific nations.

- APT actors have been known to launch attacks with the goal of disrupting critical infrastructure.

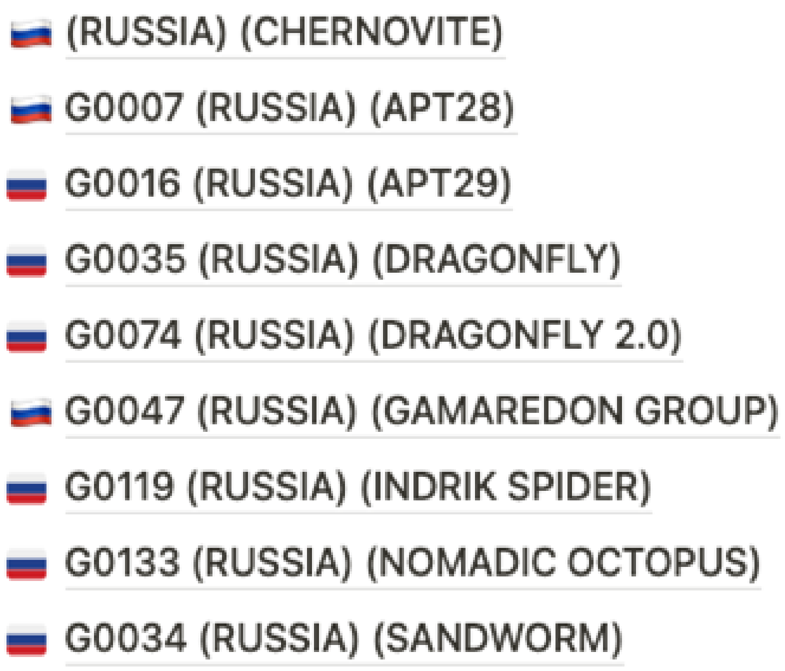
- Several nation states launch cyberattacks against the industry to gain economic advantage.

Adversary Attack Playbooks

- Offer over 175 playbooks that are mapped to the MITRE ATT&CK® Framework, on advanced persistent threat (APT) actors and cybercriminals groups.

- Each playbook enables our members to share tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs) of specific threat actors and their individual campaigns.

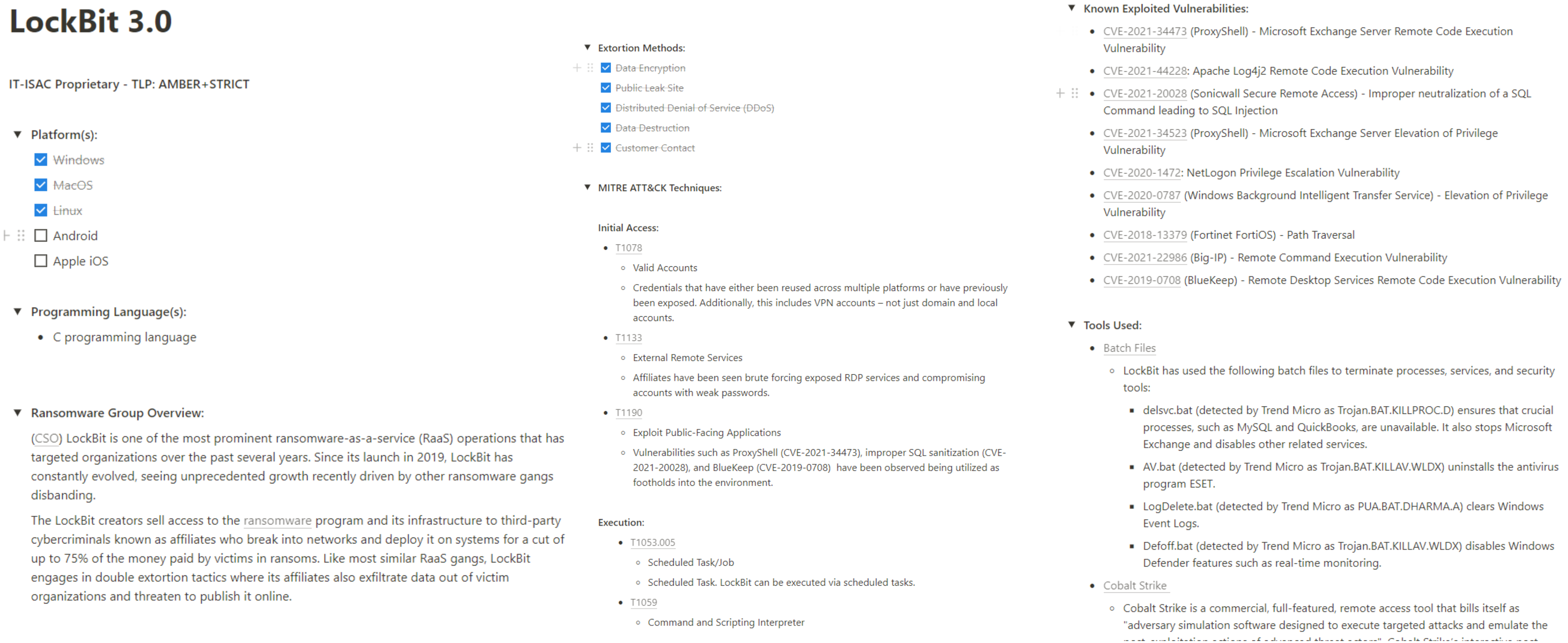
Russia Specific Playbook - Examples



- (RUSSIA) (CHERNOVITE)
- G0007 (RUSSIA) (APT28)
- G0016 (RUSSIA) (APT29)
- G0035 (RUSSIA) (DRAGONFLY)
- G0074 (RUSSIA) (DRAGONFLY 2.0)
- G0047 (RUSSIA) (GAMAREDON GROUP)
- G0119 (RUSSIA) (INDRIK SPIDER)
- G0133 (RUSSIA) (NOMADIC OCTOPUS)
- G0034 (RUSSIA) (SANDWORM)

Adversary Attack Playbooks

Example Playbook: LockBit Ransomware Group



LockBit 3.0

IT-ISAC Proprietary - TLP: AMBER+STRICT

▼ **Platform(s):**

☑ ~~Windows~~

☑ ~~MacOS~~

☑ ~~Linux~~

☐ Android

☐ Apple iOS

▼ **Programming Language(s):**

- C programming language

▼ **Ransomware Group Overview:**

(CSO) LockBit is one of the most prominent ransomware-as-a-service (RaaS) operations that has targeted organizations over the past several years. Since its launch in 2019, LockBit has constantly evolved, seeing unprecedented growth recently driven by other ransomware gangs disbanding.

The LockBit creators sell access to the ransomware program and its infrastructure to third-party cybercriminals known as affiliates who break into networks and deploy it on systems for a cut of up to 75% of the money paid by victims in ransoms. Like most similar RaaS gangs, LockBit engages in double extortion tactics where its affiliates also exfiltrate data out of victim organizations and threaten to publish it online.

▼ **Extortion Methods:**

☑ ~~Data Encryption~~

☑ ~~Public Leak Site~~

☑ ~~Distributed Denial of Service (DDoS)~~

☑ ~~Data Destruction~~

☑ ~~Customer Contact~~

▼ **MITRE ATT&CK Techniques:**

Initial Access:

- T1078
  - Valid Accounts
  - Credentials that have either been reused across multiple platforms or have previously been exposed. Additionally, this includes VPN accounts – not just domain and local accounts.
- T1133
  - External Remote Services
  - Affiliates have been seen brute forcing exposed RDP services and compromising accounts with weak passwords.
- T1190
  - Exploit Public-Facing Applications
  - Vulnerabilities such as ProxyShell (CVE-2021-34473), improper SQL sanitization (CVE-2021-20028), and BlueKeep (CVE-2019-0708) have been observed being utilized as footholds into the environment.

Execution:

- T1053.005
  - Scheduled Task/Job
  - Scheduled Task. LockBit can be executed via scheduled tasks.
- T1059
  - Command and Scripting Interpreter

▼ **Known Exploited Vulnerabilities:**

- CVE-2021-34473 (ProxyShell) - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-44228: Apache Log4j2 Remote Code Execution Vulnerability
- CVE-2021-20028 (Sonicwall Secure Remote Access) - Improper neutralization of a SQL Command leading to SQL Injection
- CVE-2021-34523 (ProxyShell) - Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2020-1472: NetLogon Privilege Escalation Vulnerability
- CVE-2020-0787 (Windows Background Intelligent Transfer Service) - Elevation of Privilege Vulnerability
- CVE-2018-13379 (Fortinet FortiOS) - Path Traversal
- CVE-2021-22986 (Big-IP) - Remote Command Execution Vulnerability
- CVE-2019-0708 (BlueKeep) - Remote Desktop Services Remote Code Execution Vulnerability

▼ **Tools Used:**

- Batch Files
  - LockBit has used the following batch files to terminate processes, services, and security tools:
    - delsvc.bat (detected by Trend Micro as Trojan.BAT.KILLPROC.D) ensures that crucial processes, such as MySQL and QuickBooks, are unavailable. It also stops Microsoft Exchange and disables other related services.
    - AV.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) uninstalls the antivirus program ESET.
    - LogDelete.bat (detected by Trend Micro as PUA.BAT.DHARMA.A) clears Windows Event Logs.
    - Defoff.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) disables Windows Defender features such as real-time monitoring.
- Cobalt Strike
  - Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post

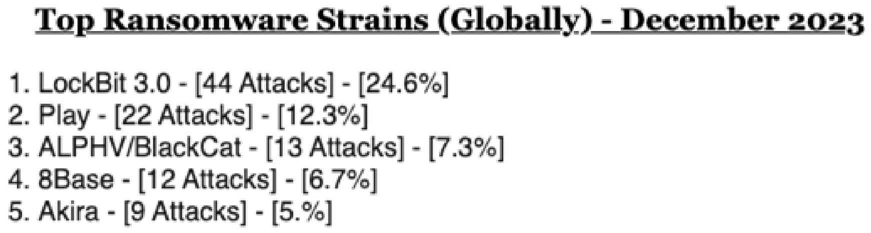
Ransomware

- 167 ransomware attacks against Food and Ag Sector in 2023 - (5.5%)
  - Ransomware is especially impactful for the food and ag sector
    - Just-in-time delivery of essential products
    - Impacts to human health and safety
    - Theft of sensitive intellectual property
    - Vulnerable to cross sector impacts (Water, Oil and Natural Gas, Transportation, Communications)
    - Vulnerable supply chain who may not have mature cybersecurity capabilities

Ransomware Tracker

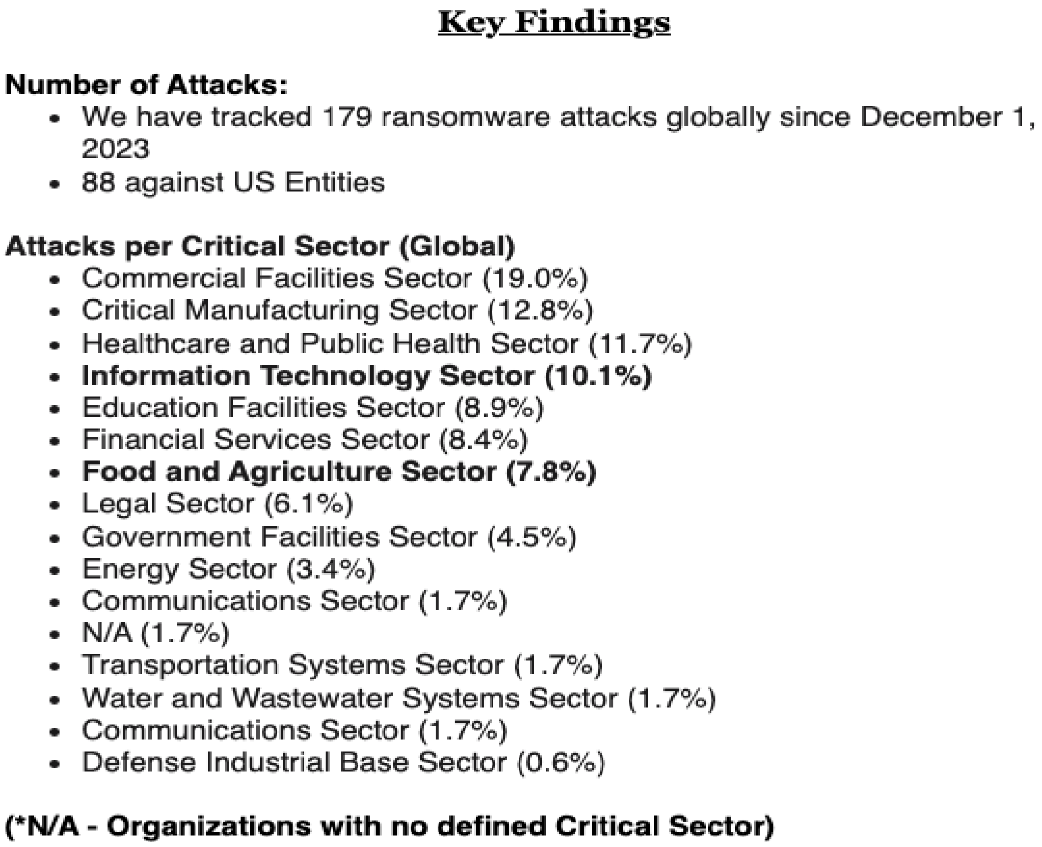
We have tracked 4,850 ransomware incidents since 2020 and provide monthly ransomware reports to our members. In 2023, we tracked 2,905 incidents.

December Report Excerpt



Top Ransomware Strains (Globally) - December 2023

1. LockBit 3.0 - [44 Attacks] - [24.6%]
2. Play - [22 Attacks] - [12.3%]
3. ALPHV/BlackCat - [13 Attacks] - [7.3%]
4. 8Base - [12 Attacks] - [6.7%]
5. Akira - [9 Attacks] - [5.%]



Key Findings

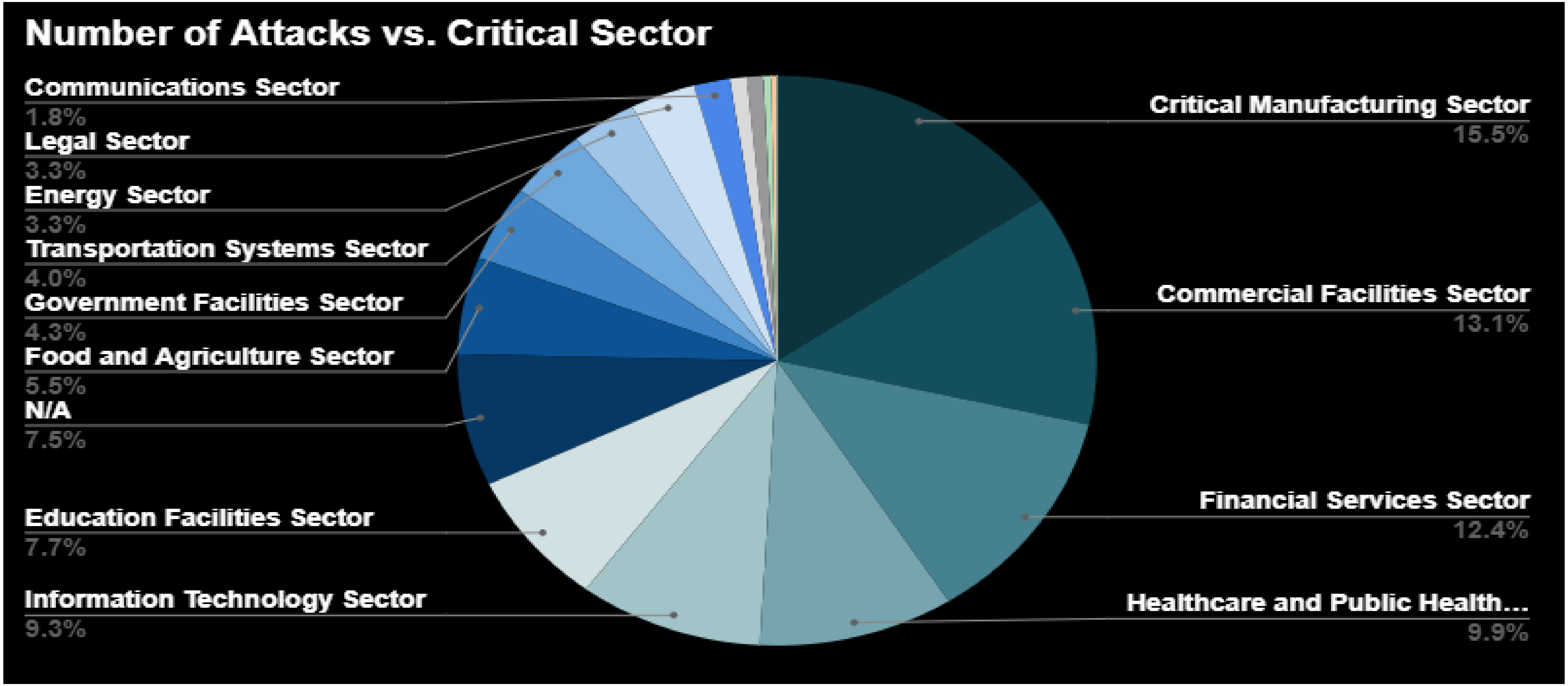
Number of Attacks:

- We have tracked 179 ransomware attacks globally since December 1, 2023
- 88 against US Entities

Attacks per Critical Sector (Global)

- Commercial Facilities Sector (19.0%)
- Critical Manufacturing Sector (12.8%)
- Healthcare and Public Health Sector (11.7%)
- **Information Technology Sector (10.1%)**
- Education Facilities Sector (8.9%)
- Financial Services Sector (8.4%)
- **Food and Agriculture Sector (7.8%)**
- Legal Sector (6.1%)
- Government Facilities Sector (4.5%)
- Energy Sector (3.4%)
- Communications Sector (1.7%)
- N/A (1.7%)
- Transportation Systems Sector (1.7%)
- Water and Wastewater Systems Sector (1.7%)
- Communications Sector (1.7%)
- Defense Industrial Base Sector (0.6%)

(*N/A - Organizations with no defined Critical Sector)

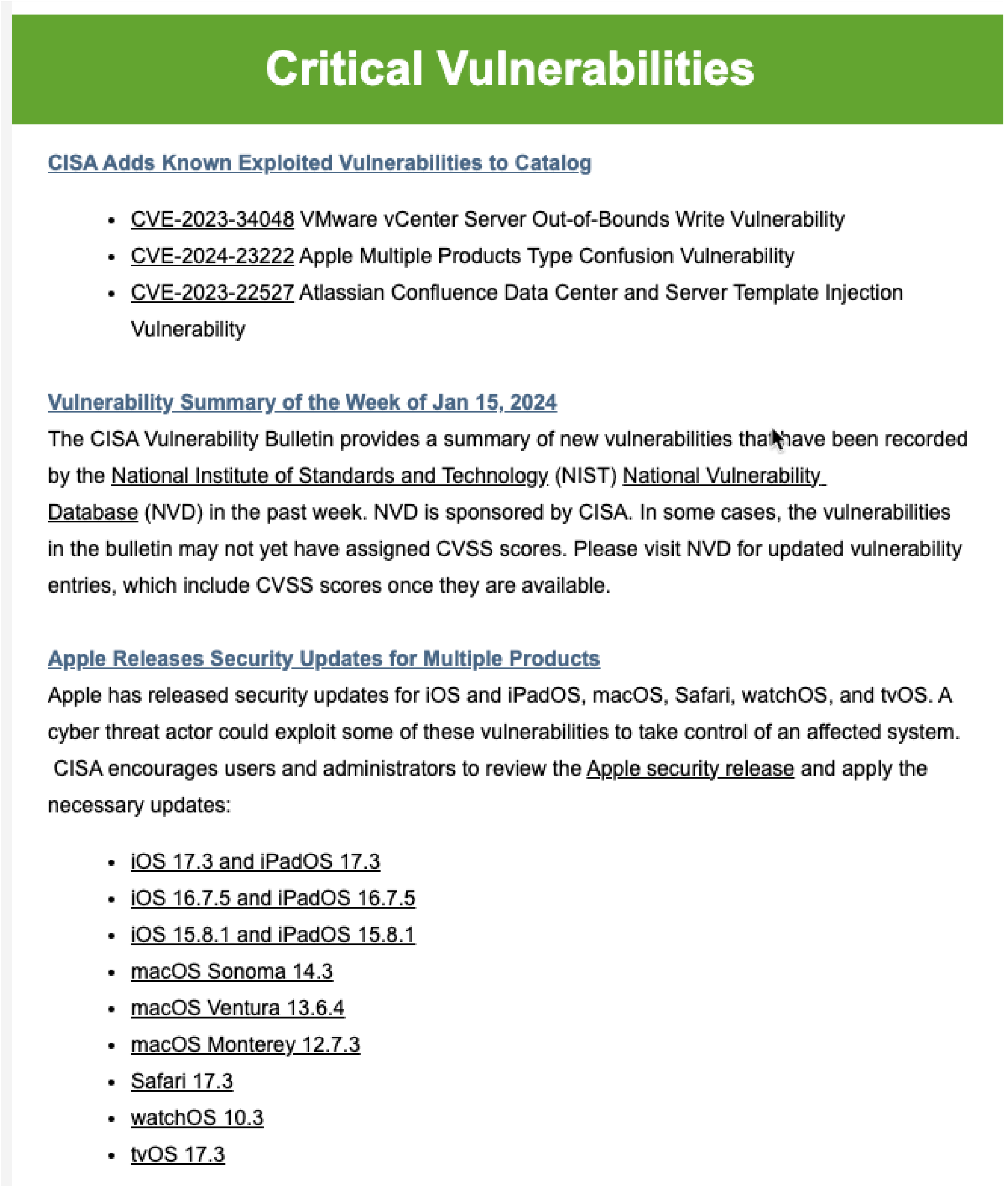


Number of Attacks vs. Critical Sector

Food Ag ISAC
An IT ISAC Community

Weekly Report

- Weekly summary of:
  - Critical Vulnerabilities
  - ICS/OT Vulnerabilities
  - Open Source Intelligence
  - Monthly Ransomware Update



Critical Vulnerabilities

CISA Adds Known Exploited Vulnerabilities to Catalog

- CVE-2023-34048 VMware vCenter Server Out-of-Bounds Write Vulnerability
- CVE-2024-23222 Apple Multiple Products Type Confusion Vulnerability
- CVE-2023-22527 Atlassian Confluence Data Center and Server Template Injection Vulnerability

Vulnerability Summary of the Week of Jan 15, 2024

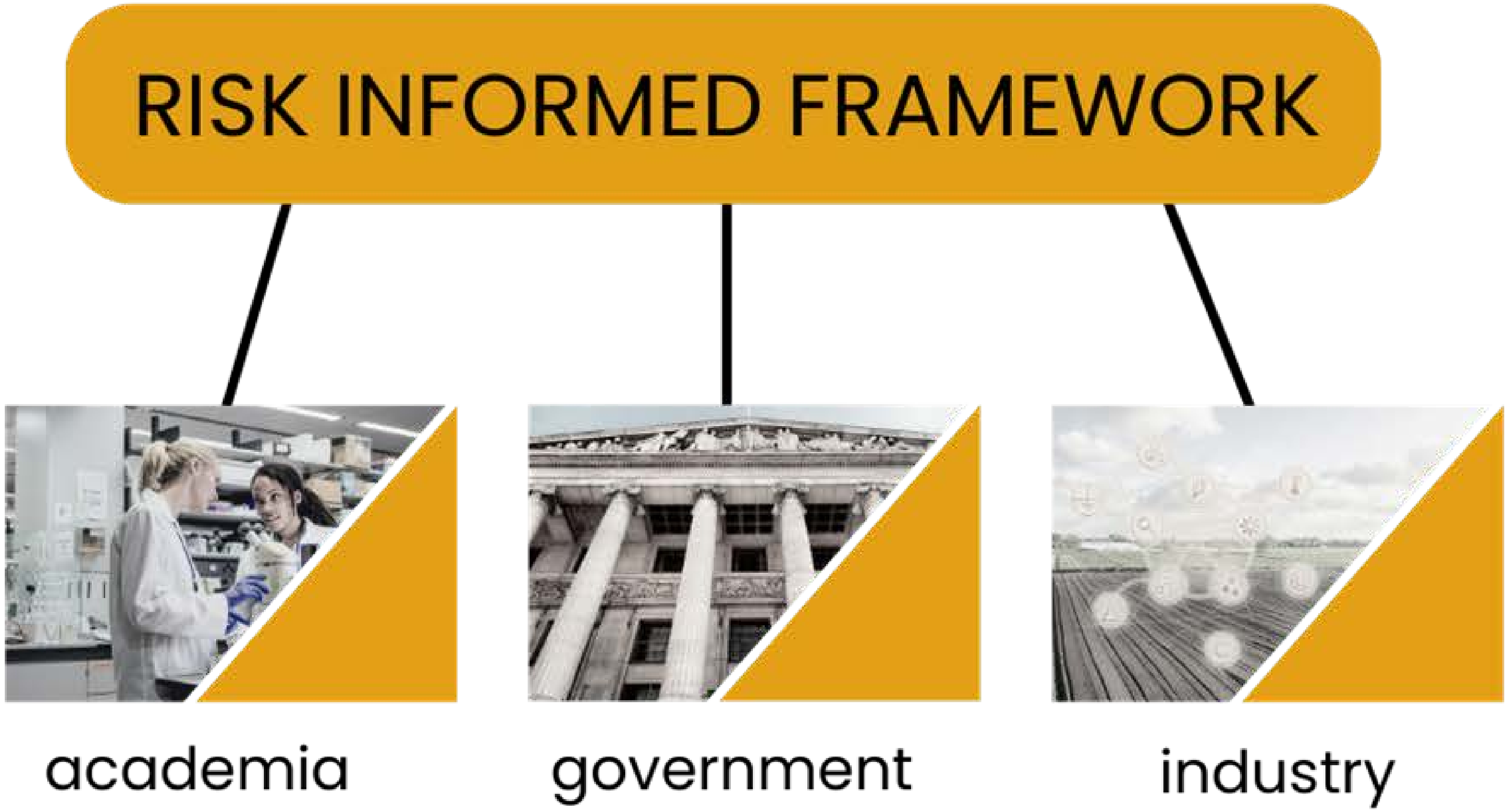
The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. NVD is sponsored by CISA. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Apple Releases Security Updates for Multiple Products

Apple has released security updates for iOS and iPadOS, macOS, Safari, watchOS, and tvOS. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the Apple security release and apply the necessary updates:

- iOS 17.3 and iPadOS 17.3
- iOS 16.7.5 and iPadOS 16.7.5
- iOS 15.8.1 and iPadOS 15.8.1
- macOS Sonoma 14.3
- macOS Ventura 13.6.4
- macOS Monterey 12.7.3
- Safari 17.3
- watchOS 10.3
- tvOS 17.3

Our Approach



RISK INFORMED FRAMEWORK

academia

government

industry

Sector Thought Leadership & Activities

- Cybersecurity Guide for Small and Medium Sized Enterprises.
- Leading industry participation in CISA’s CyberStorm IX.
- Ongoing speaking engagements and webinars.
- Engaging with CISA, FDA, and USDA.
- Outreach to key members of the House and Senate.
- Industry Association Partnership initiative.
- University Partnership program.

University Partnership Program

Establishes trusted communication channels to bolster collaboration between industry, academia, and the research community.

Benefits of Engagement

- Industry can better inform research and development efforts by ensuring the research reflects industry business realities and operating environments.
- Help researchers understand industry needs, to help prioritize research.
- Lead to improved public policy recommendations, since the research will reflect industry input and business realities.
- Provide opportunities for universities to inform industry of critical threats or vulnerabilities discovered in their research.
- Reduce risk and improve security - the more relevant and actionable the research, the more likely industry can leverage it. This can achieve the common goal of driving improved security throughout the industry.

Other Areas of Interest

- **Dependencies:** Understanding interconnections within the sector and how an incident or disruption in one critical function can cause disruptions across the sector.
- **Interdependencies:** Understanding how a failure or disruption in another sector can have cascading impacts on the food and agriculture sector.
- **Artificial Intelligence and Autonomous Technologies:** Understanding how AI and automation are used within the food and agriculture industry and risks they may pose.
- **Operational Technology:** Identifying and mitigating threats to operational technologies.
- **Incident Response:** Providing a voice for industry to government-led incident response activities.
- **Partnering, Partnering, Partnering:** There is plenty of work to be done.

How can we support your goals and mission?

Food Ag ISAC
An IT-ISAC Community

Board Members

Thank You!

Scott@FoodandAg-ISAC.org

FoodandAg-ISAC.org

Food Ag ISAC

An IT ISAC Community