Food Ag ISAC
An IT ISAC Community

Food and Ag Sector

Cyber Threat Report

2024

INTRODUCTION

The Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC) monitors cyber threats to the food and agriculture industry with the goal of sharing threat intelligence with member companies and partners to identify, prevent, and mitigate attacks on the sector. By collecting and sharing threat intelligence and effective security measures, we help companies manage risks to their enterprises. Individual risk management activities have the collective effect of increasing the overall security and resilience of the pre-farm-to-table supply chain.

This report provides a summary analysis of various threat actors facing the industry. Whereas previous reporting from the Food and Ag-ISAC was focused on Ransomware activity, this threat report looks at all threat actors. This summary is based on data collected by the Food and Ag-ISAC on over 200 threat actors. This data was collected in collaboration with our members and partners, including the IT-ISAC and other ISACs that are members of the National Council of ISACs. We leveraged a Predictive Adversary Scoring System to analyze the data from the 200-plus threat actors we are monitoring.

Members of the Food and Ag-ISAC gain access to collaborative adversary playbooks, where companies join the ISAC analysts in updating playbooks with recent tactics, techniques, and procedures, indicators of compromise, latest tools and exploits, and more.

PREDICTIVE ADVERSARY SCORING SYSTEM (PASS) OVERVIEW

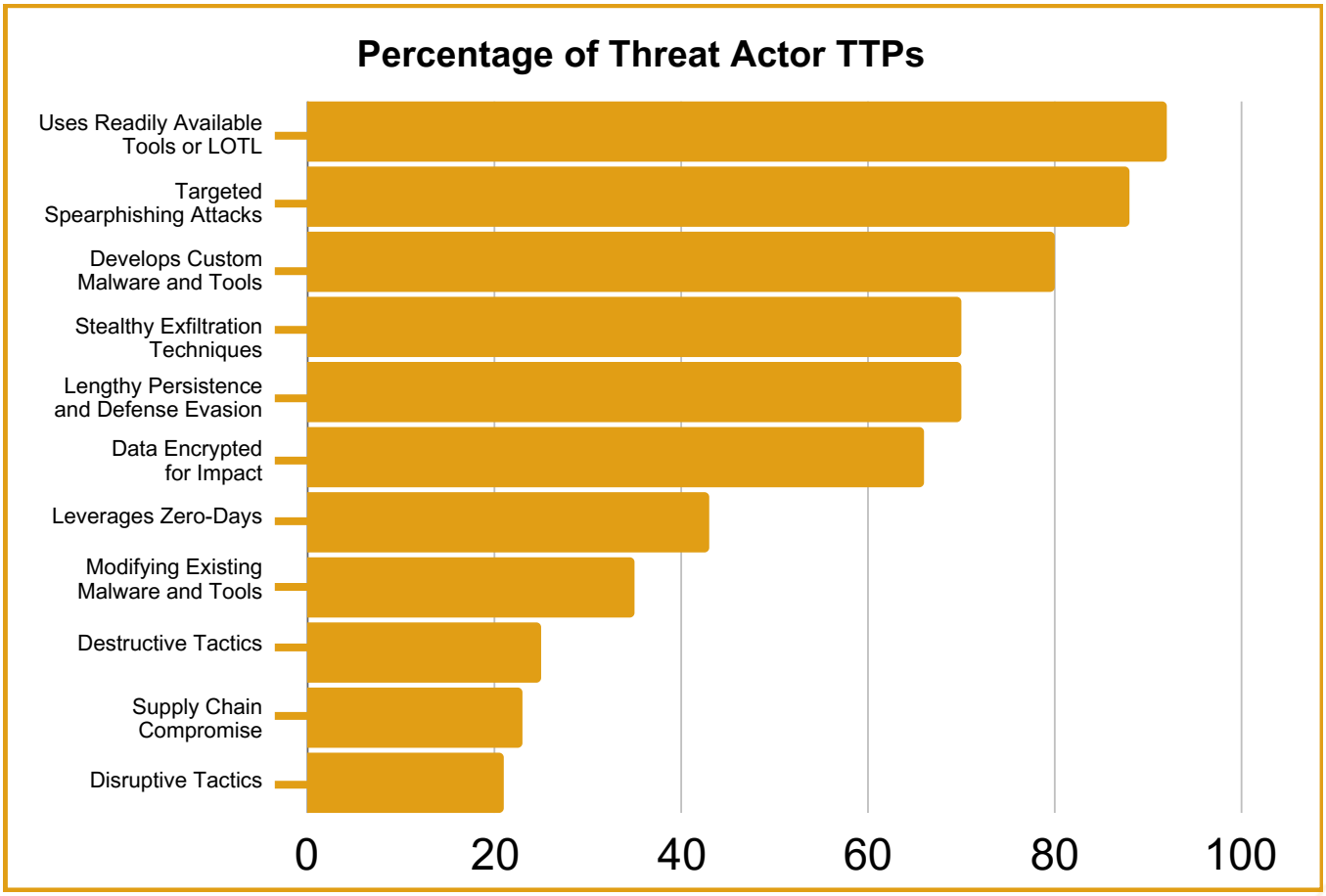
The Predictive Adversary Scoring System (PASS) was developed in collaboration by the Food and Ag-ISAC and the Information Technology - Information Sharing and Analysis Center (IT-ISAC) to help organizations prioritize their monitoring and analysis of known adversaries. The tool is used to identify which threat actors represent a significant danger to specific communities within the Food and Ag-ISAC and the IT-ISAC. The tool is available to members of both ISACs, who may use it to carry out a similar internal exercise against their own intelligence.

The tool focuses on several key metrics to determine a specific adversarial risk:

- **Level of Activity**
  How recently has the group been active
- **Frequency of Sector Targeting**
  How often has the adversary attacked the sector in the past
- **Sophistication/Impact**
  Set of tactics, techniques, and procedures that show a level of sophistication or impact
- **Motivation**
  Financial, Geopolitical, Ideological, Recognitional

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

After compiling a list of nearly 50 adversaries that have targeted the food and agriculture sector, we compared techniques used by these groups to breach organizations. Below we highlighted several tactics, techniques, and procedures that show a level of sophistication and/or impact to impacted organizations. We also provided a summary of the techniques and best practices organizations can use to defend themselves.



MITIGATIONS

Below are some effective practices to defend against observed adversaries. This list is not all-encompassing but these practices can bolster defenses against the tactics, techniques and procedures highlighted above.

- Apply and consult vendor-recommended guidance for security hardening.
- Implement application allowlisting and monitor the use of common LOLBins (Living-off-the-Land Binaries - trusted, pre-installed system tools used to spread malware and carry out their work).
- Review CISA Guidance on LOTL Mitigation - Identifying and Mitigating Living Off the Land Techniques.

- Enhance IT and OT network segmentation and monitoring.
- Implement authentication and authorization controls for all human-to-software and software-to-software interactions, regardless of network location.
- Employees should be trained to:
    - Not open emails or download software from untrusted sources – verify the domain even if it seems like a legitimate software hosting site.
    - Not click on links or attachments in emails that come from unknown senders.
    - Not provide passwords, personal information, or financial information via email to anyone (sensitive information is also used for double extortion).
    - Always verify the email sender's email address, name, and domain.
    - Report phishing emails to appropriate security or IT staff immediately.
- Back up important files frequently and store them separately from the main system.
- Protect devices using anti-malware, anti-spam, and anti-spyware software.
- Read and implement best practices from industry made cybersecurity guides. For example, the Food and Ag-ISAC's Cybersecurity Guide for Small & Medium Enterprises.

Joining an information-sharing forum, such as the Food and Ag-ISAC, is a good way to stay up-to-date on the latest malware strains and to collaborate with peer organizations and individuals who are facing the same challenges.

ABOUT THE FOOD AND AG-ISAC

The Information Technology - Information Sharing and Analysis Center (IT-ISAC), established the Food and Agriculture Special Interest Group (SIG) in 2013 to help companies in the industry protect their enterprises. In May 2023, the SIG launched the Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC) with the support of IT-ISAC.

The Food and Ag-ISAC provides threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share so they can better protect themselves and manage risks to their companies and the sector. The ISAC serves as a cost-effective force multiplier for security teams.

Visit us at FoodAndAg-ISAC.org or email us at membership@foodandag-isac.org.

Report published October 2024