Securing the Global Supply Chain through Red Team Analysis

Tues, Oct 27 11:30 AM – 1:25 PM CDT

Workshop Playbook

Table of Contents Page

High level description of the session

Join World Class expert Dr. Lynette Nusbacher in an "Observed Workshop" where supply chain and cyber security experts play an interactive role in identifying supply chain vulnerabilities. Dr. Amy Kircher will provide a realistic scenario using FPDI's CRISTAL supply chain simulator. Watch and listen as Team 1 assumes the role of cyber criminals focused on financial gain via ransomware. Team 2 will assume the role of corporate competitors searching for ways to adulterate the food supply chain. Rapporteurs will provide a play-by-play account and post your questions and comments in text commentary throughout the exercise. Move on to join the "Hot Wash" after action discussion. Participants will be able to see the entire session and witness both Red Team's analysis in live stream. Attendees will receive a report of the proceedings at the close of the Summit.

- Participants will be able to see the entire session and witness both Red Team's analysis in live stream.
- Team 1 assumes the role of cyber criminals focused on financial gain via ransomware.
- Team 2 will assume the role of corporate competitors searching for ways to adulterate the food supply chain.
- Six Rapporteurs will provide a play-by-play account and post your questions and comments in text commentary throughout the exercise.
- Move on to join the "Hot Wash" after action discussion.
- Attendees will receive a report of the proceedings at the close of the Summit.

Attendees/observers instructions

- Attendees may arrive late and join the session. The Rapporteurs will keep a play-by-play list on the Master text channel to enable the new arrivals to quickly get up to speed.
- The audience selects the Red Team they want to observe. They have ability to move between the two teams.
- They can provide suggestions or questions as the Red Teams are in play. The rapporteurs will integrate and prioritize the information and pass to the Red team for consideration.

Minute-by-minute description of the session

11:30-13:25 Role of the Rapporteur

Rapporteurs will collect, integrate, and prioritize e-comments from the Red Teams and observers. They will forward the e-comments to the lead person at the appropriate point in the

agenda. Questions will be incoming throughout the event. Rapporteurs will be reporting through text commentary visible on the public channel.

11:30-11:35 Michelle Greely (CWT) welcomes audience, thanks International Committee

11:35-11:40 Anne Bader introduces speakers, processes, red teams, and select observers from a displayed list which is also will be included in the Playbook. 5 minutes

11:40- 11:55 Dr. Lynette Nusbacher describes her work with scenarios, the analysis process, sets expectations, and describes underlying assumptions. 15 minutes

11:55-12:20 Dr. Amy Kircher provides overview of CRISTAL and runs the supply chain simulation. 25 minutes

- Dr. Kircher provides brief overview of FPDI, the CRISTAL simulator, and demonstrates the dynamic simulator which results in a graphical representation of an end-to-end international supply chain. The Red Teams will use the graphical representation in their analysis.
- All attendees and Red Team listen and watch this presentation.
- Rapporteurs will collect comments and questions.
- Red Teams listen and prepares for analysis.

12:20-12:35 Dr. Lynette Nusbacher and Brian Isle lead the security analysis discussion. 15 minutes

- Presentation with list of Red Team players, the seven-step process, and the simplifying assumptions. Set expectation for output from the Red Teams.
- Rapporteurs are collecting, integrating, and prioritizing clarifying questions to forward to segment leads. Priority on questions from Red Teams.

12:35-13:10 The Red Teams run a brief cyber security analysis of the food supply chain.

35 minutes

- Two Red Teams of seven people:
    - Team 1 will focus on financial gain via ransomware propagated by cyber criminals.
    - Team 2 will focus on food adulteration propagated by corporate competitors.
- Anticipated Red Team task/timing breakdown
    - 5 min. - Identify and discuss critical supply chain assets from standpoint of useful to meeting adversary's goal. Red Teams will start populating goggle sheets page during Dr. Kircher presentation on the supply chain. Select top 3 using voting.

- 10 min. - Identify attack surfaces for selected critical assets. Select top 3 using voting.
- 10 min. - Discuss probable vulnerabilities that are often associated with the selected attack surfaces. Select top 3 using voting.
- 10 min. - Brainstorm scenarios that exploit the top vulnerabilities. Capture the scenario in a headline (ex. Use phishing attack to bring in ransomware..).

Note: for this brief analysis we are using a simple voting decision making. With more time we would incorporate a richer set of decision-making metrics.

13:10-13:15 Team Leads will summarize the results of the analysis 5 minutes

13:15 – 13:24 Q&A live with Observers top 3-5 questions on that are posted from Observers 9 minutes

13:24 -13:25 Anne Bader narrates a Goodbye screen thanking and repeating info on report, survey if one is sent. 1 minute

Details of the virtual environment's communication features

We will have a robust text chat function that can handle four separate channels and international distributed participants. The rapporteurs will moderate the text chat channels. The four channels for the international session part B are:

- Master text chat and voice channel that goes to all attendees, Red Teams 1&2, and the speakers. The Rapporteurs' Play-by-Play goes out on this channel.
- Public text chat and voice channel for Team 1 - ex. The Team 1 analysis is on this channel.
- Public text chat and voice channel for Team 2 – ex. The Team 2 analysis in on this channel.
- Private text chat channel for the speakers and the Red Team – ex. "Bob, you have jelly on your tie".

In addition, the virtual environment will support the following:

- The Red Teams will use Google Sheets to capture the analysis results.
- We will document the identity of everybody in the session.
- The attendees will be in several countries and time zones.

Description of the roles and responsibilities

Rapporteurs:

- The six Rapporteurs will be collecting, integrating, and prioritizing clarifying questions to be forward to segment leads. Priority on questions from Red Team

- Questions will be incoming throughout the event. Rapporteurs will be reporting through text commentary visible on the public channel.
- The Rapporteurs will keep a play-by-play list on the Master text channel to enable the new arrivals to quickly get up to speed.
- There will be four separate text chat channels. One channel will be assigned to each of the Red Teams. There will be at least one Rapporteurs supporting each Red Team to act as moderator of the text chat channel, for information flowing into and out of the Red Team.

Red Team:

- Red Team members will review the Playbook prior to the 27th and start to formulate ideas on how their team will disrupt the supply chain.
- The Red Team will follow 4 of the 7-step analysis process. The goal is to show how the analysis process works, not to give a complete analysis of the supply chain.
- The results of the Red Team analysis will be captured on a formatted Google Sheets form. Each Red Team member will input their information directly in the sheets.

Analytical Red Team Process and Assignment

The goal of the exercise is to show the analysis process, not to produce a complete analysis. In this exercise we will take short cuts by pre-assigning the threat agents and their goals. We will simplify the decision making by using a simple vote, versus using a more sophisticated decision metrics. We will further simplify by not attempting steps 6 and 7.

The premise of this analysis is to have the team think like the threat agent. To adopt the goals and limitation of the threat agent. The limitation includes both technical capability and cost to undertake the attack. Cost is measured in both financial terms and risk to the threat agent.

The Red Team works best with a diverse group of people ranging from financial to technical to business. Insiders who know the business, may not be security experts, but make great Red Teamers.

Analytical Red Team process

The following is the seven step Analytical Red Team process annotated to describe how the process will be used in this exercise:

1. Define the assessment goals and threat agent – Given for this exercise
    a. Team 1 will focus on financial gain via ransomware propagated by cyber criminals.

   b. Team 2 will focus on food adulteration propagated by malicious corporate competitors.
2. Identify critical assets of the assessment target
   a. Supply chain: a critical asset is an entity in the chain that if taken down would greatly hinder the flow through the supply chain – and – difficult to quickly replace.
   b. Red Teamers will start to populate the critical assets page of the Google Sheets during Dr. Kircher presentation.
   c. We will discuss briefly and ask for additional critical assets.
   d. Individuals will vote to identify the top 3 to 5 critical assets.
3. Gather information on the critical asset to identify attack surfaces and vulnerabilities
   a. Brainstorm/discuss cyber/physical attack surfaces of the identified critical assets.
   b. Vote to select the top 3 to 5 attack surfaces as most likely
   c. Brainstorm the most probable vulnerabilities (based on OSINT) that would be present at the critical asset that would leverage the selected attack surfaces.
4. Develop attack scenarios that exploit vulnerabilities and attack surfaces
   a. Brainstorm scenarios that exploit the top vulnerabilities. Capture the scenario in a headline (ex. Use phishing attack to bring in ransomware..).
5. Prioritize vulnerabilities / targets in the supply chain
   a. Select the top 3 scenario by voting, using your best judgement that meets the adversary's goals and within their means (lowest cost).
   b. Identify the vulnerabilities exploited in the scenarios.
6. Identify shared vulnerabilities and common attack enablers – Not required for exercise
7. Develop mitigation strategy – Not required for exercise

Expected analysis results: The analysis provides insight into where an attack might occur (the most probable critical asset), possible attack surfaces at the location, probable vulnerabilities associated with the attack surface, and scenarios describing how the vulnerability might be exploited. With this information one can investigate the status of safeguards and security controls for each of the identified vulnerabilities.

Team 1 Assignment: Cyber criminals focused on financial gain via ransomware

Team lead: Brian Isle
Team 1 will assume the persona of cyber criminals focused on financial gain via ransomware by attacking an international multi-modal supply chain from source to consumer. Your team will be presented with a description of the supply chain and shown a graphical simulation as the food product moves through the supply chain. You will brainstorm supply chain attack surfaces, speculate on possible vulnerabilities that could be exploited, and prioritize the vulnerabilities based on the effectiveness of meeting your goal of damaging your competitor.

Team 2 Assignment: Malicious corporate competitors focused on adulterating the food supply chain

Team Lead: Todd Carpenter
Team 2 will assume the persona of a malicious corporation with the goal of damaging a fictitious company by adulterating their food product as it passes through an international multi-modal supply chain from source to consumer. Your team will be presented with a description of the supply chain and shown a graphical simulation as the food product moves through the supply chain. You will brainstorm supply chain attack surfaces, speculate on possible vulnerabilities that could be exploited, and prioritize the vulnerabilities based on the effectiveness of meeting your goal of damaging your competitor.

Definition of Attack Surfaces:

The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out.
www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet

- The sum of all paths for data/commands into and out of the application, and
- The code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding), and
- All valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII, and
- The code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls).

Graphical representation of the supply chain to be analyzed

The Red Teams will analyze an international supply chain for frozen breaded shrimp. The following images provide detail of the supply chain.

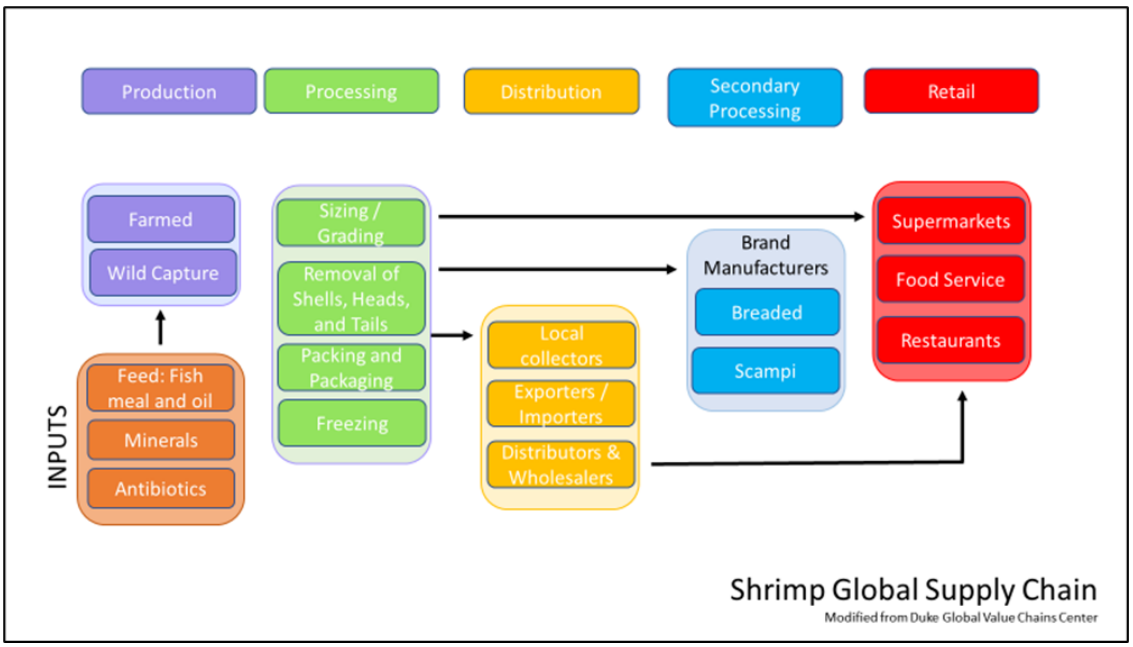

Figure 1: Shows the major components for the global supply chain for shrimp.

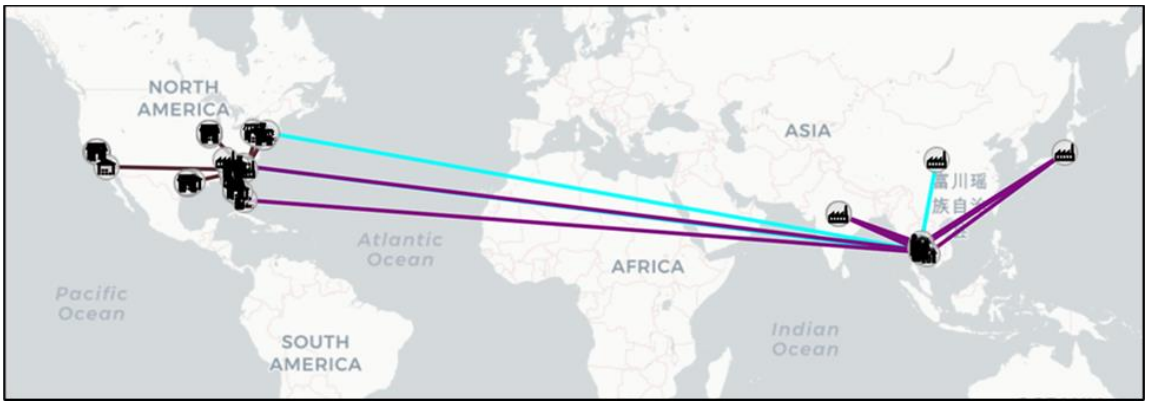

Figure 2: Shows production in Japan, China, India, and Thailand; with processing, distribution, and retail in the US.

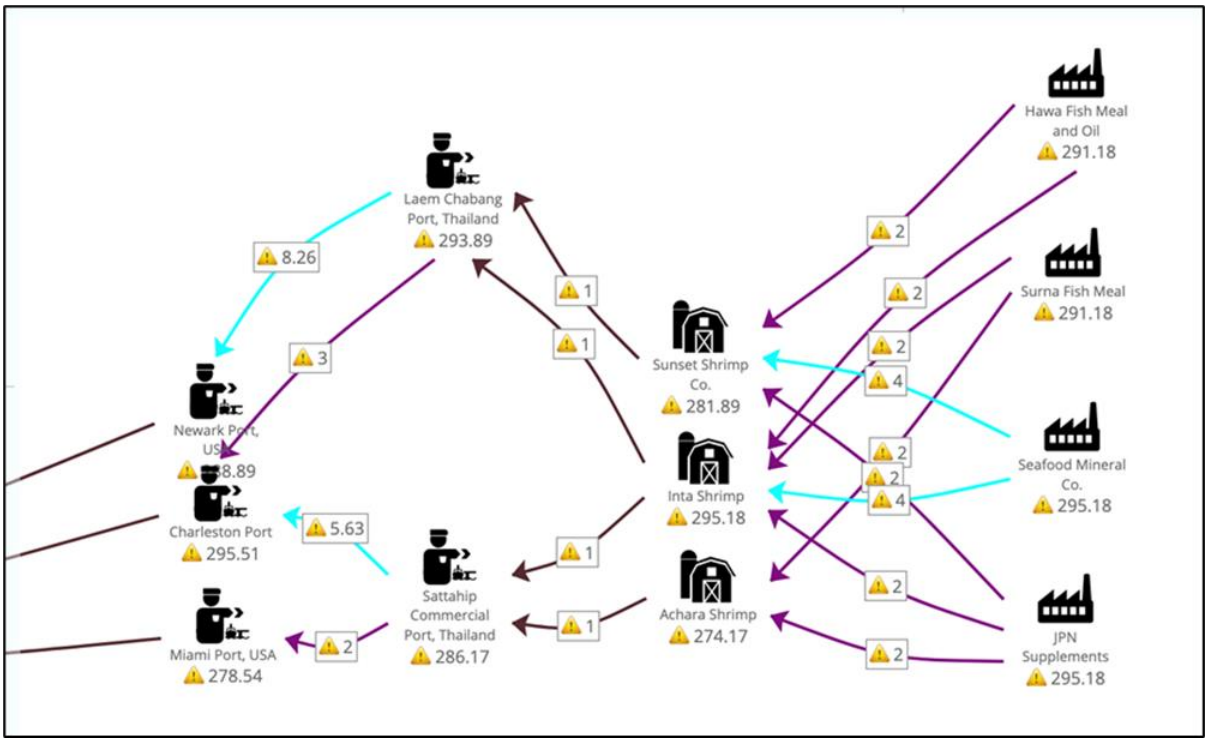

Figure 3: Shows the flow of product through the pre-production, production, and processing.

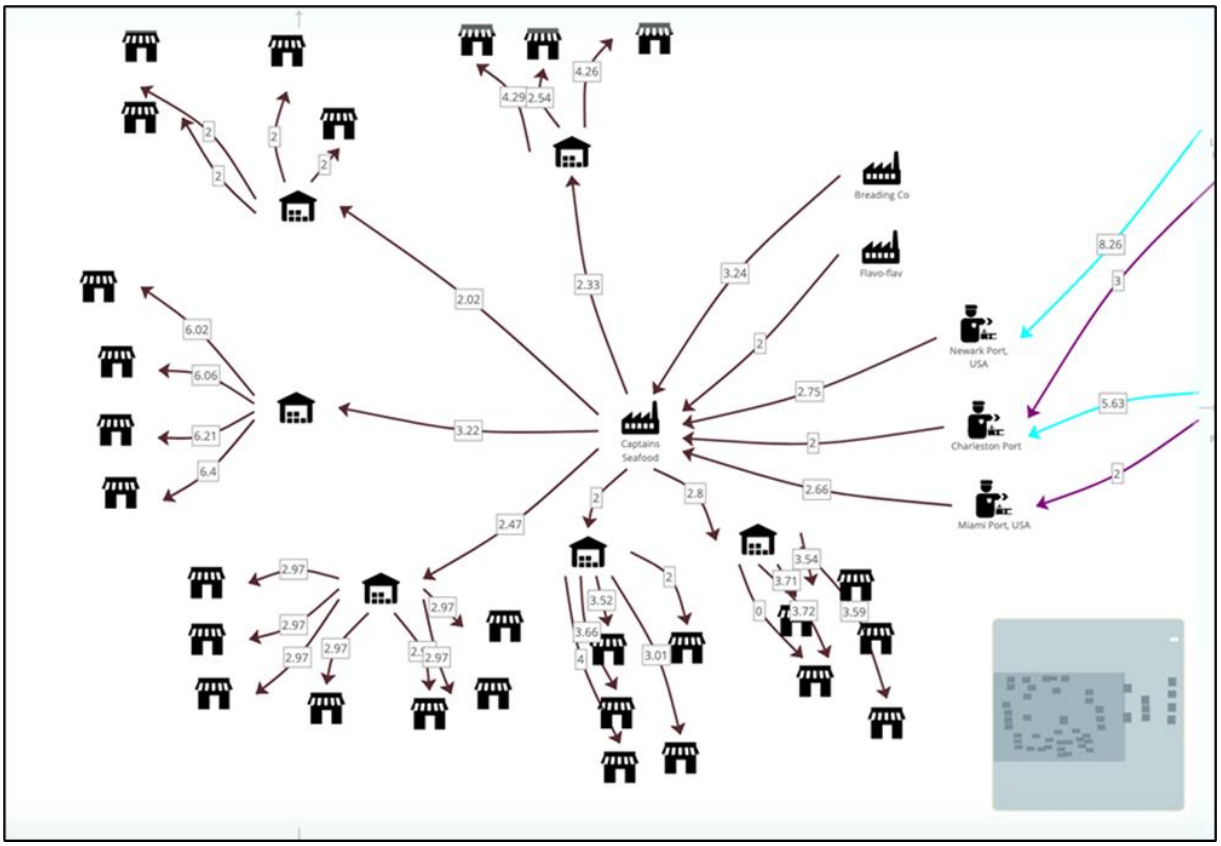

Figure 4: Shows the flow of product thru secondary processing, distribution, and retail.

Type	Name	City	State	Country
Farm	Achara Shrimp	Trat		Thailand
Farm	Inta Shrimp	Saraburi		Thailand
Farm	Sunset Shrimp Co.	Bangkok		Thailand
Storage - Warehouse	Hendrix Distributor	Peoria	IL	USA
Storage - Warehouse	Hendrix Distributor	Temecula	CA	USA
Storage - Warehouse	Hendrix Distributor	Augusta	GA	USA
Storage - Warehouse	J. Bon. J. Distribution	Harrisburg	PA	USA
Storage - Warehouse	J. Bon. J. Distribution	Beaumont	TX	USA
Storage - Warehouse	Jaggers Storage	Gainsville	FL	USA
Port of Entry - Sea	Charleston Port	Charleston	SC	USA
Port of Entry - Sea	Laem Chabang Port	Laem Chabang Port		Thailand
Port of Entry - Sea	Miami Port	Miami	FL	USA
Port of Entry - Sea	Newark Port	Newark	NJ	USA
Port of Entry - Sea	Sattahip Commercial Port	Sattahip		Thailand
Processing Plant	Breading Co	Chattanooga	TN	USA
Processing Plant	Flavo-flav	Valdosta	GA	USA
Processing Plant	Hawa Fish Meal and Oil	Longxi		China
Processing Plant	JPN Supplements	Toshima City		Japan
Processing Plant	Seafood Mineral Co.	Parasia		India
Processing Plant	Suma Fish Meal	Jamai		India
Processing Plant	Captains Seafood	Charleston	SC	USA

Table 1: Shows the locations of farms, storage, ports and processing.

Type	Name	City	State	Country
Retailer	A. Rose Grocery	Kerman	CA	USA
Retailer	A. Rose Grocery	Clovis	CA	USA
Retailer	A. Rose Grocery	Sanger	CA	USA
Retailer	A. Rose Grocery	Dinuba	CA	USA
Retailer	Slash Foods	Lincoln	IL	USA
Retailer	Slash Foods	Groveland	IL	USA
Retailer	Slash Foods	Peroia	IL	USA
Retailer	Slash Foods	Washintong IL	IL	USA
Retailer	E.V.H. Food Pride	Macon	GA	USA
Retailer	E.V.H. Food Pride	Macon	GA	USA
Retailer	E.V.H. Food Pride	Bonaire	GA	USA
Retailer	E.V.H. Food Pride	Milledgeville	GA	USA
Retailer	E.V.H. Food Pride	Dublin	GA	USA
Retailer	Sebastian B's Market	Lindenword	PA	USA
Retailer	Sebastian B's Market	Pine Hill	PA	USA
Retailer	Sebastian B's Market	Staton College	PA	USA
Retailer	Motley's	Pearsland	TX	USA
Retailer	Motley's	Brookside Village	TX	USA
Retailer	Motley's	Pasadena	TX	USA
Retailer	Motley's	Bellaire	TX	USA
Retailer	Motley's	Cypress	TX	USA
Retailer	Motley's	Sugarland	TX	USA
Retailer	Motley's	Humble	TX	USA
Retailer	Bob Plants Food and Eats	Spring Hill	FL	USA
Retailer	Bob Plants Food and Eats	Dade City	FL	USA
Retailer	Bob Plants Food and Eats	Lutz	FL	USA
Retailer	Bob Plants Food and Eats	Brandon	FL	USA

Table 2: Shows the location of retail organizations.

Open Source Information (OSINT) on ShrimpCo

Step 3 of the analysis process is to gather information on the critical asset to identify attack surfaces and vulnerabilities. This includes search on the web and dark, google earth, and various specialized information sources like WhoIs and Maltego. The following is an example of the types of information that can be assembled on a target. We will use this information as our baseline for the Red Team exercise analyzing our fictitious company ShrimpCo, LLC.

OSINT Reconnaissance - ShrimpCo LLC,
Business Intelligence:

- Recently acquired by StayPuff
- StayPuff earned $3.6B in annual Revenue last year.
- Top 100 largest privately held U.S. company in 2019.
- Warehouse location that has employed nearly 1k people for over 20 years has recently announced a physical relocation to the west coast. This will result in significant unemployment to the local area

Social Medial Presence of Leadership

- Professional headshots from company page used in each LinkedIn profile picture
- Email addresses with company domain found in both public and private data breaches included wide range of data that included mobile and office phone numbers. Including:
    - Each member's personal social media accounts, personal email addresses, value of personal property, etc.

Additional Findings

- New posting in Russian marketplace forum with [REVENGE] tag that is an apparent English-speaking person using a translator offering to sell network access.
- Plant Operations Engineer's email address found in data breach for popular third-party consumer hardware retail company.
- A post found in community discussion forum (~45 days ago) asking for assistance with configuration settings of a USB wireless adapter and remote access with a mobile phone. Community members asked for more details and engineer said it is a computer from inside the warehouse connected to guest wireless in order to monitor the HVAC system it's connected to. Screenshots were shared in post replies to ask more questions with settings. Pictures showed IP addresses and computer admin username. HVAC system confirmed at location of transport distribution warehouse.

Assessment of opportunities:

- Many opportunities to impersonate executives to introduce spear phish campaign.
- BEC admin to send financial records.
- SIM swap to bypass 2FA.
- xmas scans to HVAC computer and perform RCE attack.

Technical Recon

Information obtained from Maltego CE for CaptainsSeafood.com

Transform from DNS name

- 70-136-178-132.captainsseafood.com
- 70-136-178-133.captainsseafood.com
- 70-136-178-142.captainsseafood.com
- 70-136-178-151.captainsseafood.com
- 70-136-178-176.captainsseafood.com
- wildcard-in-use.cpatainsseafood.com
- ESA.cpatainsseafood.com
- hqmsex01.captainsseafood.com
- hqmsex02.captainsseafood.com
- www.captainsseafood.com

IP addresses link to domain

- 151.361. 201.24
- 107.992.123.122
- 54.243.222.632
- 54.243.222.880
- 54.243.222.892
- 192.52.241.9
- 192.52.241.255
- 192.52.241.2
- 192.52.241.6

Transform DNS to MX report

- Captainseafood-com.mail.protection.outlook.com
- Mail.captainsseafood.com
- mx1.captainsseafood.iphmx.com
- mx2.captainsseafood.iphmx.com

Transform from NS

- Ns0.dnsveryeasy.com
- NS1.dnsveryeasy.com
- Ns2.dnsveryeasy.com
- Ns3.dnsveryeasy.com

Transform SOA

- Ns0.dnsveryeasy.com
- DNS.DNSveryeasy.com

Transform other common dns names

- ftp.captainsseafood.com
- smtp.captainsseafood.com
- mail.captainsseafood.com

Transform other TDLs

- Captainsseafood.cn
- Captainsseafood.th
- Captainsseafood.info
- Captainsseafood.org

Other domains owned by company

- Captainphil.com
- Breadedshrimp.com
- Captainphilsshrimp.com

Whois Information for captiansseafood.com (website)

- IP Address 151.361. 201.24

Website

- Numerous email addresses found from various contact information found online
- Addresses of various buildings found using Whois and other online information via Maltego
- Other information available from Maltego search on Domain name Captainsseafood.com include:

  - Email addresses with @captainsseafood.com from various location on the internet including social media
  - Phone numbers used on registration requests via internet.
  - Any files uploaded to the internet that are searchable via search engines

Systems and Configurations

- Desktops
  - Windows 7
- Servers
  - Windows 2003
- Network Gear
  - Cisco routers running IOS 15.6(2)t
  - Cisco ASA 5505 firewall
- Email
  - Microsoft Exchange Server 2016 Update 17
- Building HVAC
  - Honeywell Controls
- Refrigeration plant
  - No network connectivity. Stand-alone unit.
  - Rooftop HVAC units and controllers were updated in 2015. Assume external facing webserver on HVAC.
- Logistics
  - Shipping dock scheduling platform. Custom front end to Access Database
  - Migrating to SaaS solution

Participants

Speakers:

1. Michelle Greeley , Sr. director, Global Risk Management, CWT
2. Dr. Lynette Nusbacher, Futurist, Strategist, Analyst, Facilitator, Advisor
3. Dr. Amy Kircher, Co-Director, Strategic Partnership and Research Collaborative, Senior Advisor, Food Protection and Defense Institute, UMN
4. Brian Isle, Senior Fellow UMN Technological Leadership Institute
5. Anne Bader, Founder, International Cybersecurity Dialogue

Rapporteurs:

1. Simon Bracey Lane, Chief Rapporteur, Cyber Security Summit
2. Sherwin Bothello (Minnesota State University, Mankato, Info Sec MA)
3. Alyssa Chetrick (New School, NYC, Global Studies & Violin)
4. Tanner Manley (Georgetown Qatar, IR)
5. Shelia Padre (Member of staff at the Institute for Statecraft)
6. Alex Gilbertson (UK contact. CV coming)

Red Teams

Team 1: cyber criminals focused on financial gain via ransomware

1. Brian Isle, Senior Fellow UMN Technological Leadership Institute
2. Mike Kearn, Director, Threat Informed Defense at U.S. Bank
3. Jennifer Reicherts, Threat Hunter and OSINT expert
4. Andrew Crocker, CEO, P2020ACADEMY
5. Pekka Vepsäläinen, CEO, Tikkasec Ltd.
6. Chad Svihel, Executive Director, Minnesota, PCs for People

Team 2: Malicious corporate competitors focused on adulterating the food supply chain

1. Todd Carpenter - Chief Engineer and Owner at Adventium Enterprises
2. Justin Opatrny - Sr. Manager, Cyber Security – Supply Chain
3. Richard Stiennon, Chief Research Analyst, IT-Harvest
4. Wendy Foslein, Lead Data Scientist, Thermo King
5. Stephen Streng, Food Defense Analyst, Food Protection and Defense Institute, UMN

Observers

1. Harshal Mehta Vice President, Chief Information Security Officer, Carlson Wagonlit Travel
2. Dr. Char Sample, Chief Research Scientist-Cybercore Division, INL

3. Dr. Roxanne Everetts DM, Chair Cyber Strategy and Infrastructure Department, College of Information and Cyberspace, National Defense University
4. Dr. Camino Kavanagh, Member, Advisory Support Team, UN OEWG and UN GGE on ICT and International Security **TBC**

Cyber Security Summit 2020 International Comittee

1. Michelle Greeley, Senior Director, Information Security Management, CWT, Chair
2. Jill Allison, Advisory CISO, Kudelski Security, Inc.
3. Anne Bader, Founder, The International Cybersecurity Dialogue LLC
4. Simon Bracey-Lane, Chief Rapporteur, The Cyber Security Summit
5. Sean Costigan, Director and Co-founder, ITL Security
6. Anita Finnegan, CEO, Nova Leah
7. Paul Hansen, Trade Commissioner, Consulate General of Canada in Minneapolis
8. Eileen Manning, Co-Founder, Executive Producer, The Cyber Security Summit
9. Mark Ritchie, CEO, Global MN
10. Natasha Shawver, Information Security Risk Analyst, University of Minnesota
11. Mohammed Suleh-Yusuf, Senior Manager, Legal & Regulatory Services, Nigerian Communications Commission
12. Chad Svihel, Executive Director, Minnesota, PCs for People
13. Pekka Vepsäläinen, CEO, Tikkasec Ltd.