gocyber

COLLECTIVE

July Announcements

- Capture the Flag Event – Hold the Date November 11 & 12
- GoCyber Signal Group

Honeypots

Fooling Hackers with Sweet Deception

TechSolve®

Resident Beekeeper

Joe Anderson
Senior Cybersecurity Analyst

25+ years of general IT and InfoSec experience

InfoSec Certifications

- Practical Network Penetration Tester (PNPT)
- Certified Information Systems Security Professional (CISSP)
- CompTIA Security+
- Certified Ethical Hacker (C|EH)
- EC-Council Certified Security Analyst (ECSA)
- CMMC Register Practitioner (CMMC-RP)
- Microsoft Certified Systems Engineer: Security

Areas of InfoSec experience include:

- Risk identification (pentesting/vulnerability scanning)
- Incident detection and response
- Cybersecurity consulting
- Governance, risk, and compliance

Who is TechSolve?

- We are a mission driven organization (501c3)
- Consultants to manufacturing
- We help manufacturers by providing:
  - IIoT \ OT Services
  - Continuous Improvement
  - Manufacturing Process Solutions
  - Cybersecurity Consulting & Services
  - We are proud member of the Ohio Manufacturing Extension Partnership (MEP)

Agenda

- Current challenges
- Attacker weaknesses
- Exploration of honeypots
- Adding honeypots to the threat landscape
- Demonstration
- Deployment Strategy
- Question & Answer

A Sticky Situation

Traditional security methods are good but…

- Can bring a false sense of security.
- Rely on the relative strength of the chosen technology.
- Depend on the experience of implementer.
- Require correlation from multiple sources.
- Need expertise from a seasoned incident responder.
- Alerts for false positives are common and create fatigue.
- There may still be “false negatives”.

A Sticky Situation

Honey-combing through the details

You have to know everything about everything!

- There are limited resources (time, money, people).
- The skillset demands are high.
- Working in an environment that is in constant flux.
- Vulnerabilities and risks are an everyday occurrence.
- Threats are constantly evolving.
- Even if you have all the information, you still might not know.

A Sticky Situation

Incident prevention is hard!!!

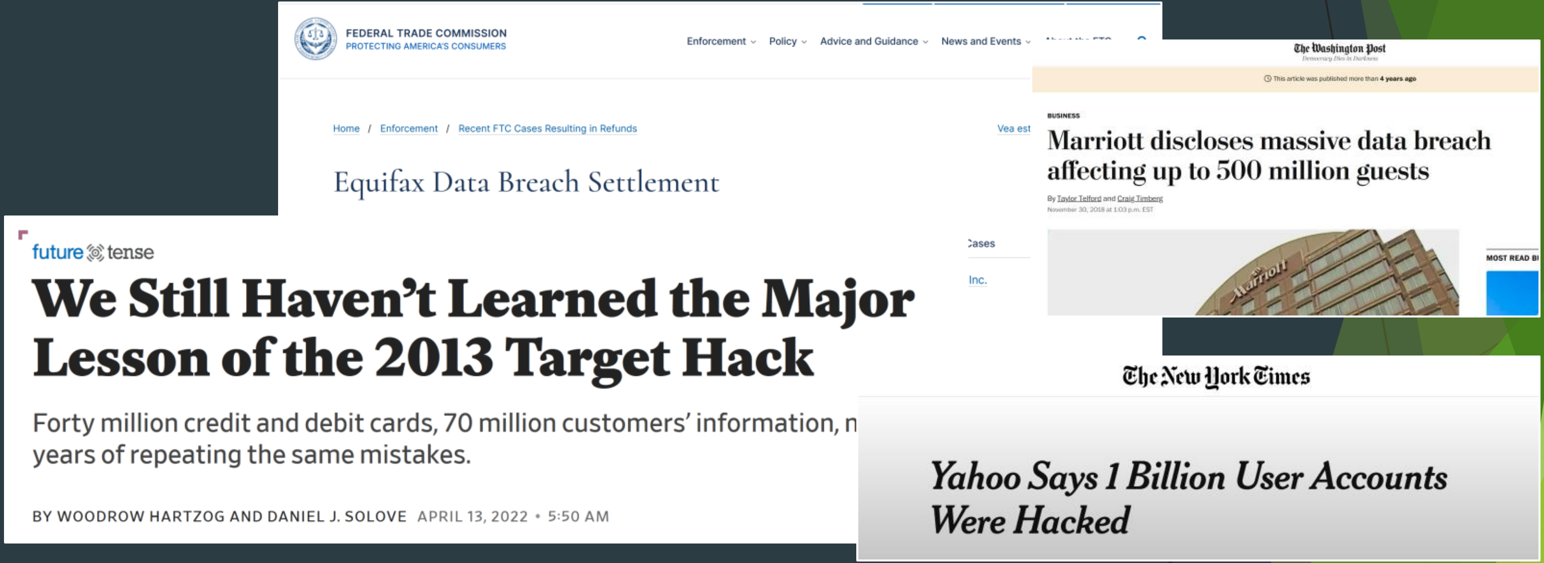
Incident detection is hard!!!

A “buzzing” need for an “if all else fails” approach

TechSolve®

A Sticky Situation

Average time to identify and report a breach is 9 months/277 days (IBM)



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Home / Enforcement / Recent FTC Cases Resulting in Refunds

Equifax Data Breach Settlement

The Washington Post
Democracy Dies in Darkness

This article was published more than **4 years ago**

BUSINESS

Marriott discloses massive data breach affecting up to 500 million guests

By Taylor Telford and Craig Timberg
November 30, 2018 at 1:03 p.m. EST

future tense

We Still Haven't Learned the Major Lesson of the 2013 Target Hack

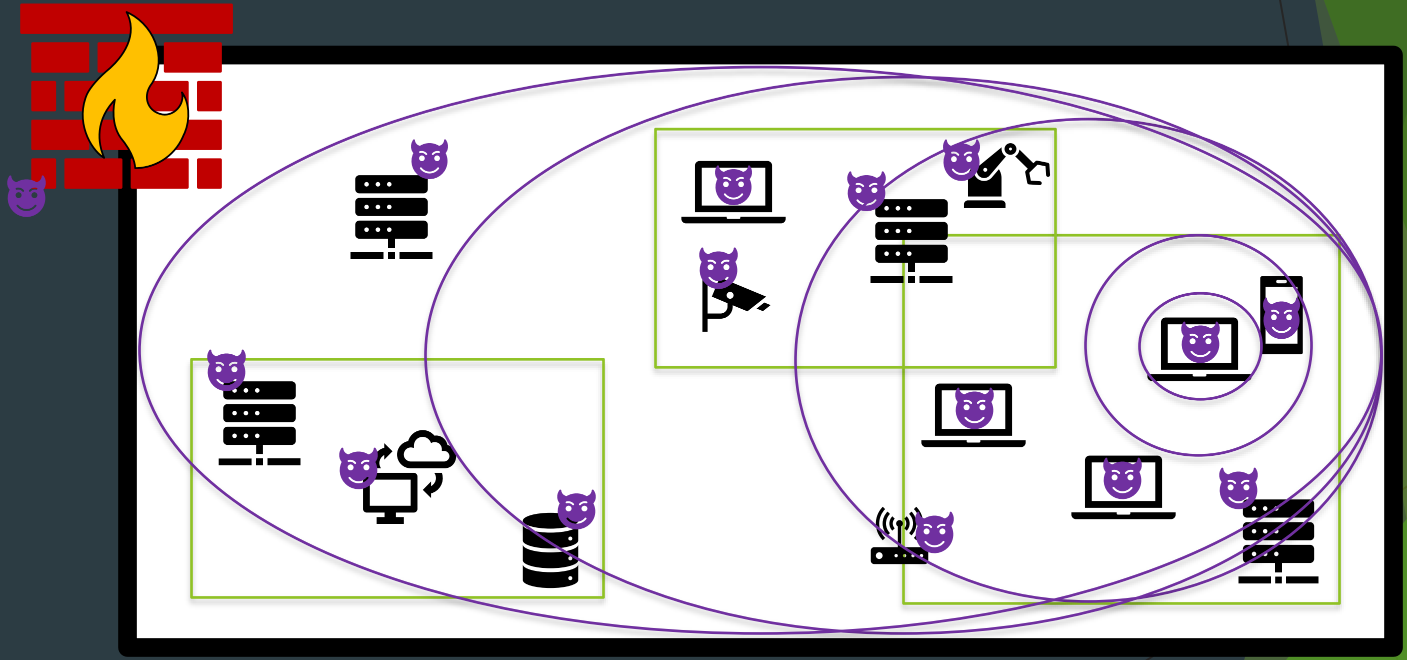
Forty million credit and debit cards, 70 million customers' information, n
years of repeating the same mistakes.

BY WOODROW HARTZOG AND DANIEL J. SOLOVE APRIL 13, 2022 • 5:50 AM

The New York Times

Yahoo Says 1 Billion User Accounts Were Hacked

A Sticky Situation



A Sticky Situation

It's not all roses for the attacker – they must:

1. Determine their position.
2. Find weaknesses.
3. Exploit weaknesses.
4. Find sensitive data.
5. Exfiltrate data.
6. Maintain persistence.
7. Remain stealthy.

Attackers look for the paths of least resistance;

While trying to avoid detection and prevention tools;

Move as quickly as possible to improve their position.

Can we sweeten the pot?

- Is there a way to have earlier threat detection?
- Is there a method to see what an attacker is trying to do?
- Is there a way improve the quality of alerts?
- Is there a way to deceive \ misdirect?
- Is there a way to record actions of an attacker?
- Do you have methods to detect indications of a “malicious insider”?
- Are there a solutions which requires minimal upkeep?
- Can we increase the overall likelihood of detection?

TechSolve®

Bit-O-Honey

Can we lead the bear to honey?

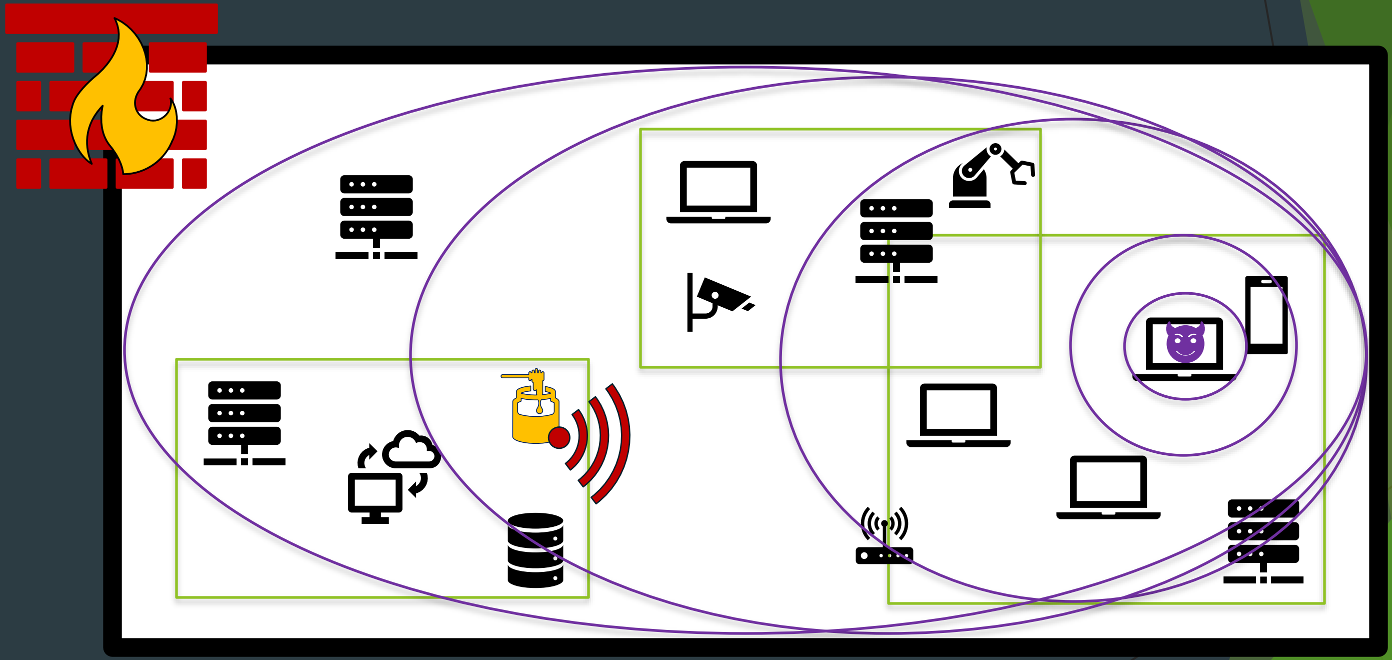
What is a honeypot?

- Decoy asset.
- Emulates a “real-world” organizational asset.
- Designed to attract, lure, and deceive attackers.
- Concept in Clifford Stoll’s book “The Cuckoo’s Egg” (1989).
- The Honeynet Project (1999) formalized the concept.
- Placed within a system.
- Where a users would not typically interact with the device.
- Designed to attract, lure, and deceive attackers.

Why are honeypots the bee’s knees?

- Increases detection capabilities.
- Low overhead and upkeep, if done correctly.
- Quality threat detection.
- Provide active attack intelligence.
- Improve \ enhance incident response and detection capabilities.
- Create a deception \ misdirection ability.
- Provide forensic logging for analysis.
- Indicates insider threats.
- An “if all else fails” complimenting security measure.

Protecting the Collective



All things honey

- Accounts
- Firewalls and networks
- Spam traps
- Tokens
  - Files
  - Folders
  - DNS Records
  - Authentication keys
  - QR Codes
  - Emails

Harvesting honey

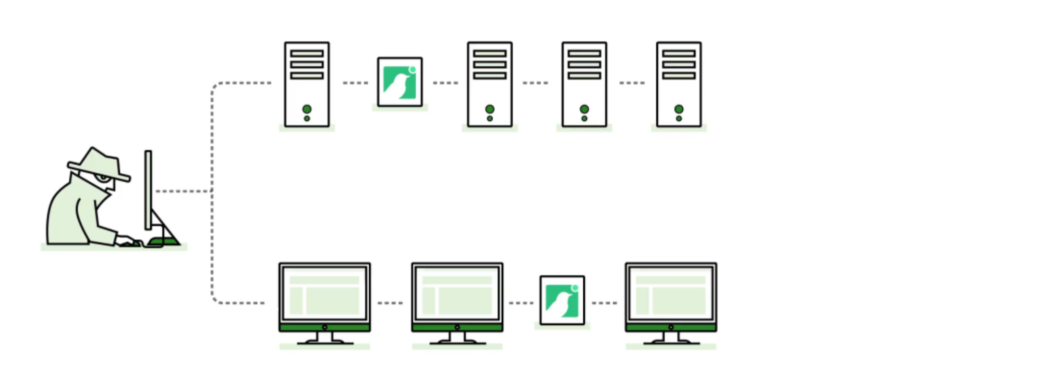
- Books
  - **Clifford Stoll's book "The Cuckoo's Egg" (1989)**
  - **Intrusion Detection Honeypots: Detection through Deception by Chris Sanders**
- Choose your own confection
  - Opensource vs. Commercial
    - Opensource
      - Build your own – Belt and suspenders \ higher barrier to entry
      - Honeynet Project (non-profit) https://www.honeynet.org
      - Honeypot List – https://github.com/parallax/awesome-honeypots
    - Commercial
      - Buy a device – Drop in and go \ higher costs

TechSolve®

Sweet Samples

THINKST CANARY

Live Demo



Deception-in-Depth

- Drop ‘em in your zones.
- Mix and match different honey “things”.
- Make them believable \ attractive.
- Limit or prevent ability for general user interactivity.
- Inventory and track placement.
- Provide clarity in alert messaging.
- Determine severity handling.
- Ensure ongoing alerting and effectiveness testing.

TechSolve®

Find the Hive

Joe Anderson
Senior Cybersecurity Analyst

✉ anderson@techsolve.org

in https://www.linkedin.com/in/joesec/

July Threat Briefing

July Threat Briefing

- Indiana County Files Disaster Declaration Following Ransomware Attack - Infosecurity Magazine
- TOP STORY! AT&T says criminals stole phone records of 'nearly all' customers in new data breach | TechCrunch
- October ransomware attack on Dallas County impacted over 200K people (securityaffairs.com)
- Why the Ticketmaster Breach is More Dangerous Than You Think - Security Boulevard
- Advance Auto Parts data breach impacts 2.3 million people (bleepingcomputer.com)
- New Ransomware Group Exploiting Veeam Backup Software Vulnerability (thehackernews.com)

Information

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register and download past presentations from the website.

- GoCyberCollective.org

Event Sponsors

SECURECYBER
DEFENSE

FORTINET®