(I do have slides)

You know, to support this rant on IR

$whoami

- **John Faria** - @Abjuri5t
- Incident Response & Malware Analysis ~5 years
  - Current host remediation engineer

- Hunt C2 servers in freetime
- Pursuing M.S. in Risk Management

$whoami

We **DESPERATELY** need help

Thank you for your interest in cyber-security.

China suspected of hacking diplomatic body for Pacific islands region

Data on nearly 1 million NHS patients leaked online following ransomware attack on London hospitals

Cyber-security problems that we face

Apple Drops Spyware Case Against NSO Group, Citing Risk of Threat Intelligence Exposure

Sep 16, 2024 Spyware / Threat Intelligence

Apple has filed a motion to "voluntarily" dismiss its lawsuit against commercial spyware vendor NSO Group, citing a shifting risk...

Top Skillz for Incident Response

1.
2.
3.
4.

Top Skillz for Incident Response

1. Communication - your ability to share ideas and relate to others
2. Critical Thinking
    - Questioning ‘Why?’ instead of just doing
    - Develop solutions to solve the real/underlying problem
3. Technical literacy
4. Understanding of business/organization/enterprise
    - IT exists to help business - need to understand how cyberattacks affect and harm a business

Incident A: Weird domain…

1. Junior analyst noticed 14 hosts querying a *random domain* every few minutes
2. Escalated to me for help investigating

Incident A: Weird domain…

1. Junior analyst noticed 14 hosts querying a *random domain* every few minutes
2. Escalated to me for help investigating

Findings:

- 14 (now 18) hosts all in manufacturing factory
- according to customer
- DNS lookup for **tcxuriyv[.]ws** (104.244.14[.]252)
- Also find apparent network scanning from hosts for TCP:445

Incident A: Weird domain…

1. Junior analyst noticed 14 hosts querying a *random domain* every few minutes
2. Escalated to me for help investigating

Findings:

- 14 (now 18) hosts all in manufacturing factory
- according to customer
- DNS lookup for **tcxuriyv[.]ws** (104.244.14[.]252)
- Also find apparent network scanning from hosts for TCP:445

3. Discovered Conficker Worm infection, told customer to format hosts and patch

Incident A: Weird domain…

1. Junior analyst noticed 14 hosts querying a *random domain* every few minutes
2. Escalated to me for help investigating

Findings:

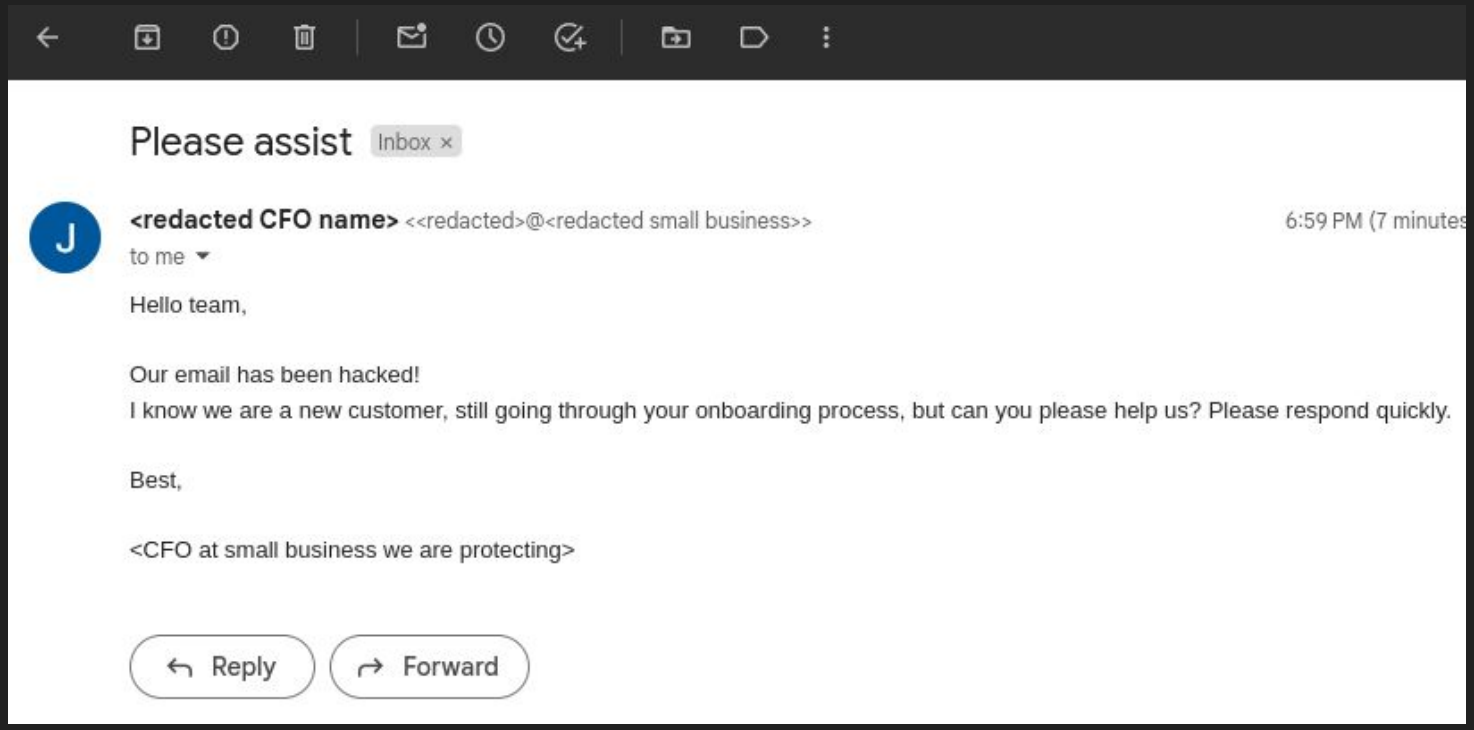
- 14 (now 18) hosts all in manufacturing factory
- according to customer
- DNS lookup for **tcxuriyv[.]ws** (104.244.14[.]252)
- Also find apparent network scanning from hosts for TCP:445

3. Discovered Conficker Worm infection, told customer to format hosts and patch
4. … junior analyst called me on Sunday

Top Skillz - What does this mean for students?

1. Communication - Writing and/or Comms classes (or practice giving talks)
2. Critical Thinking
3. Technical literacy - Ask questions & don't be afraid to not know everything
4. Understanding of business/organization/enterprise - Project Management, Finance, and/or Business Decision Making

Incident B: Email from a Customer:



Please assist Inbox ×

J **<redacted CFO name>** <<redacted>@<redacted small business>> 6:59 PM (7 minutes

to me

Hello team,

Our email has been hacked!
I know we are a new customer, still going through your onboarding process, but can you please help us? Please respond quickly.

Best,

<CFO at small business we are protecting>

Reply Forward

*I ran this incident approx 3 months after graduating

Incident B: Dialogue from Out-of-Band Comms.

Timeline*

1. C-suite received a number of emails from ‘Bob’** regarding an invoice
2. CFO replied to ‘Bob’ informing of invoice process - then received ‘strange’ response
3. Reset Bob’s password - but Bob unable to receive new emails

*the initial timeline for an incident should be based on **direct evidence** - not **attempted analysis**

**I do remember the victim’s name. It was not “Bob”, but that’s the name we’re going with for this talk