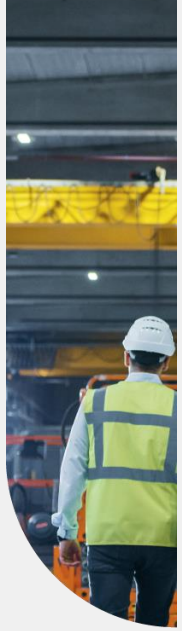
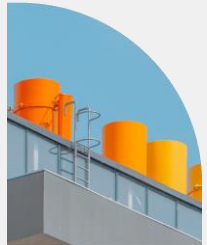


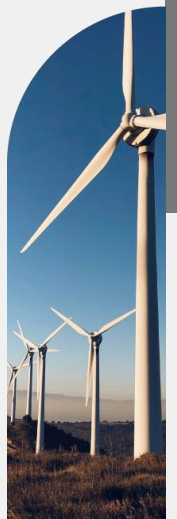
FORTINET

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Manufacturing is Both a Cybersecurity Target and a Vector

Robert M. Lee
CEO & Co-Founder
Dragos, Inc.
@RobertMlee

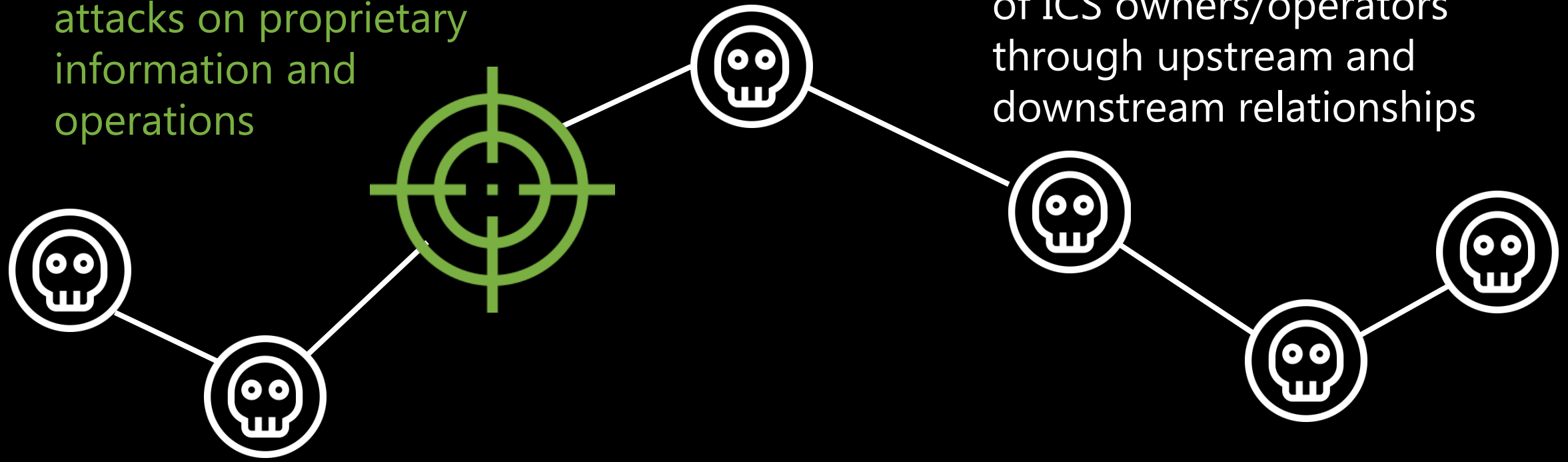




Manufacturing: A Cyber Target and Vector

TARGET: Targeted and ransomware attacks on proprietary information and operations

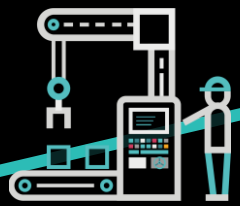
VECTOR: A method of compromising larger groups of ICS owners/operators through upstream and downstream relationships



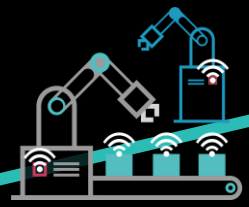
MANUFACTURING TRENDS

Growing investment in digital transformation and hyperconnectivity

STAND-ALONE



LOOSELY CONNECTED



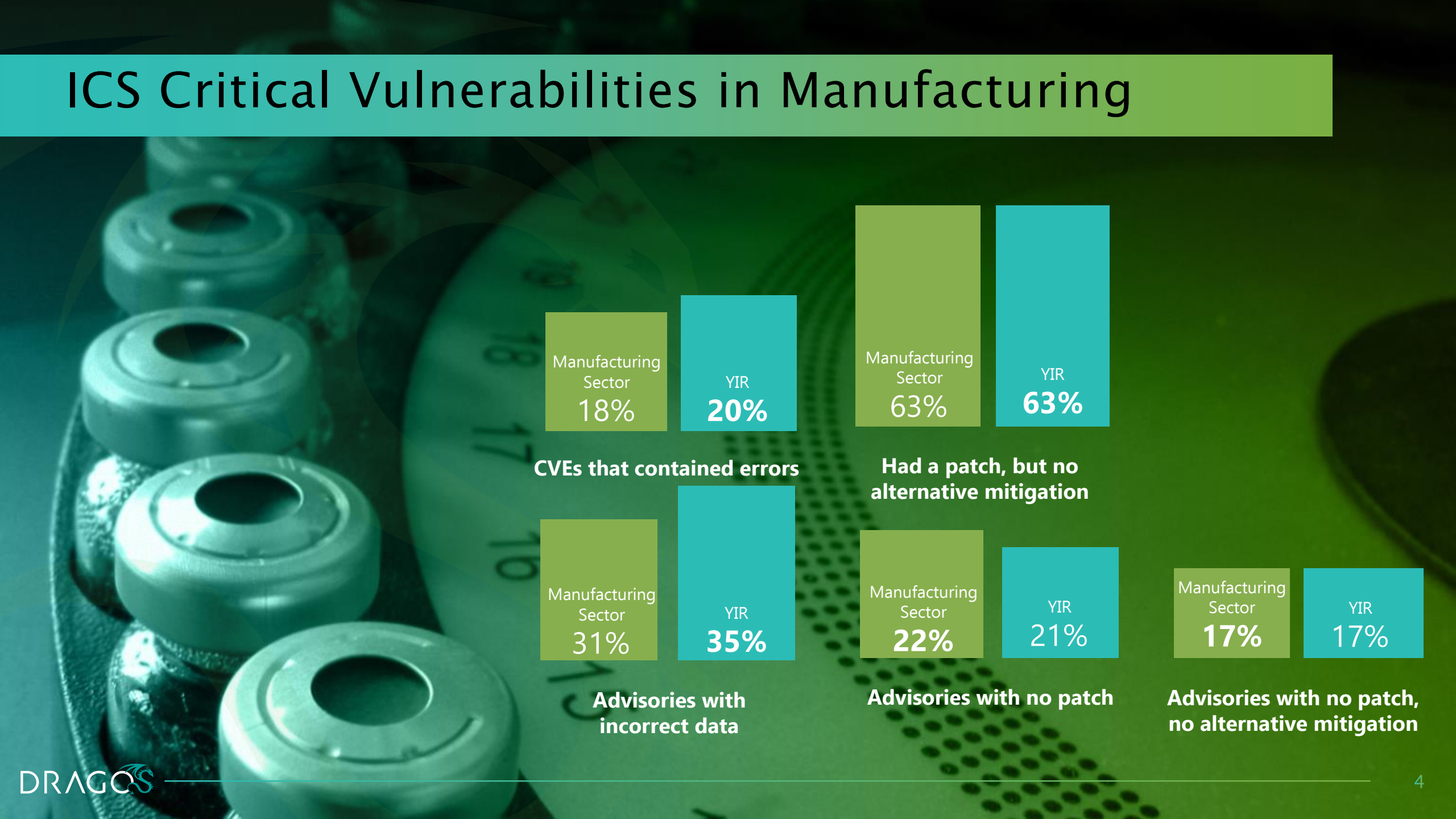
HIGHLY CONNECTED

Greater exposure to malicious cyberthreats

"Threat groups are rising 3X faster than they're declining…"

Source: Dragos 2020 YiR

ICS Critical Vulnerabilities in Manufacturing



OEM Equipment Vulnerability Example

Affected OEM devices include cellular gateways, cellular routers, wireless bridges, and access points. These devices facilitate network communication throughout ICS and OT networks. They can be found providing remote access[1], long distance wireless bridges, reliable automated guided vehicle (AGV) connectivity[3], rail monitoring[4], and even wireless access in space.

OEM Vulnerability Example

- Dragos researchers found new vulnerabilities in the OEM Service interface that allowed them to bypass authentication, leak plaintext credentials, enumerate users, and render the OEM Service interface unreachable until the device is rebooted
  - Additionally discovered authenticated command injection in the web interface
  - Unauthenticated stored Cross Site Scripting (XSS)6 via Secure Shell (SSH), Telnet, and Hypertext Transfer Protocol (HTTP(S)
  - Insufficient integrity verification on firmware upgrades
- Dragos reported these issues to the OEM, and requested the CVE, can take months on average sometimes into year+

```
albinolobster@ubuntu:~$ telnet 10.0.0.5
Trying 10.0.0.5...
Connected to 10.0.0.5.
Escape character is '^]'.

AWK-3131A_4F:84:B7 login: lol
Password:
~ # uname -a
Linux AWK-3131A_4F:84:B7 2.6.31--LSDK-WLAN-10.2.85 #1 PREEMPT Fri Mar 5 15:15:39 CST 2021 mips GNU/Linux
~ # id
uid=0(admin) gid=0(root) groups=0(root)
~ # cat /proc/cpuinfo
system type             : Atheros AR934x
processor               : 0
cpu model               : MIPS 74Kc V4.12
BogoMIPS                : 278.72
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : yes
hardware watchpoint     : yes, count: 4, address/irw mask: [0x0000, 0x0018, 0x0848, 0x0cc8]
ASEs implemented        : mips16 dsp
shadow register sets    : 1
core                    : 0
VCED exceptions         : not available
VCEI exceptions         : not available
```

Manufacturing as a Target

Threat Groups Targeting Manufacturing

- Of the 15 threat activity groups that Dragos tracks targeting the industrial sector, these 6 specifically target Manufacturing

WASSONITE

VANADINITE

COVELLITE

XENOTIME

TALONITE

KAMACITE

WASSONITE in Manufacturing

- Targeting the manufacturing sector since November 2019
- June 2020 - Dragos researchers identified WASSONITE activity targeting a component manufacturing firm
- The victim communicated with a WASSONITE command and control server associated with the Appleseed backdoor
- Appleseed is a multi-component backdoor that can take screenshots, log keystrokes, collect removable media information and upload, download and execute follow-on commands from the C2 server

Dragos Assessment: Dragos assesses with moderate confidence WASSONITE will continue to target the manufacturing sector for reconnaissance and data exfiltration operations.

Appleseed Code – Used by WASSONITE

```
  text "UTF-16LE", 'POST',0
  align 20h
8:                      ; DATA XREF: sub_180017560+AA↑o
                        ; sub_180017940+B1↑o ...
  text "UTF-16LE", '699c5345702a18d2c6c707a44bda5ad224d7fed2ce88f10cff1'
  text "UTF-16LE", '621a5c64b78c4c93a1e28781c50a255a28b1f6f959823248ee9'
  text "UTF-16LE", '97c795bb5db25513c7fc4a75f0fc021a3632371afb0ae3d7452'
  text "UTF-16LE", 'edccd576abba4cd9ddbaa13b05717d6fe4f7a81c8172c1b0443'
  text "UTF-16LE", '3ec332c1e87c19f09d7d2d9ffd8ec7cd86359533468bef00698'
  text "UTF-16LE", 'ccb6401',0
  align 10h
                        ; DATA XREF: sub_180017560+213↑o
                        ; sub_180017940+227↑o
  text "UTF-16LE", 'HTTP/1.1',0
  align 8
                        ; DATA XREF: sub_180017EB0+11C↑o
  text "UTF-16LE", '%06d',0
  align 4
  db 'end',0            ; DATA XREF: sub_180017EB0+442↑o
                        ; DATA XREF: sub_180017EB0+3A6↑o
  text "UTF-16LE", '-XXXXXX',0
  align 10h
b:                      ; DATA XREF: sub_1800184D0+7D↑o
                        ; sub_1800184D0+295↑o ...
  text "UTF-16LE", 'e1c26506e84acbfb26372a664979deadcc2371459be24b8594c'
  text "UTF-16LE", '7db8ca4be049b4debb789007e804f0f5b451b6628cf57d07722'
  text "UTF-16LE", '15cdb11ed0',0
  align 20h
l:                      ; DATA XREF: sub_1800184D0+A4↑o
  text "UTF-16LE", 'Content-Type: multipart/form-data; boundary=',0
  align 20h
p:                      ; DATA XREF: sub_1800184D0+376↑o
  text "UTF-16LE", '"',0Dh,0Ah
  text "UTF-16LE", 'Content-Type: application/octet-stream',0Dh,0Ah
  text "UTF-16LE", 0Dh,0Ah,0
  align 20h
i:                      ; DATA XREF: sub_1800184D0+2F8↑o
  text "UTF-16LE", 0Dh,0Ah
  text "UTF-16LE", 'Content-Disposition: form-data; name="binary"; file'
  text "UTF-16LE", 'name="',0
```

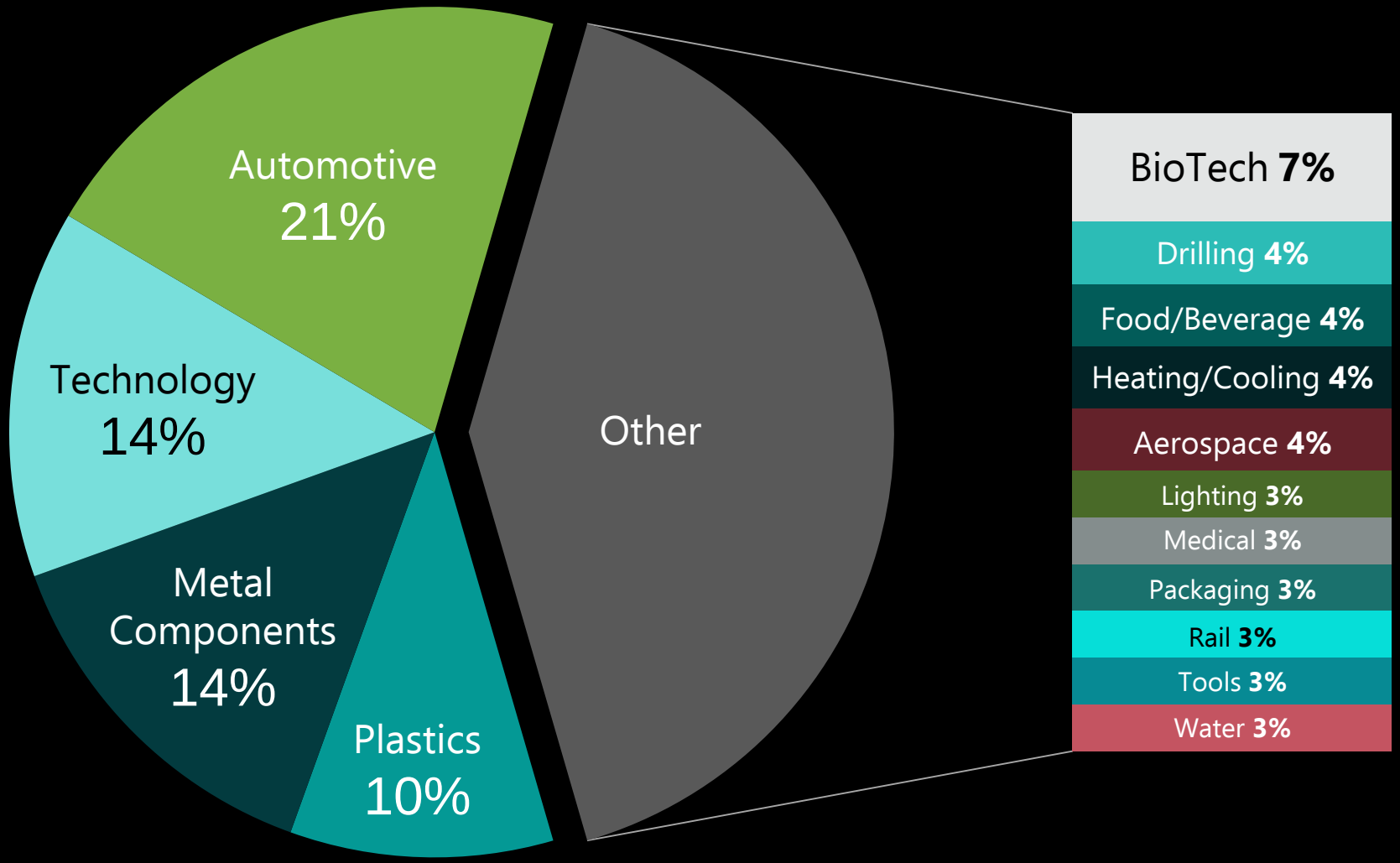
Appleseed

Identified two additional variants, in addition to the one mentioned in open-source reporting, of Appleseed shown below in Table 1.

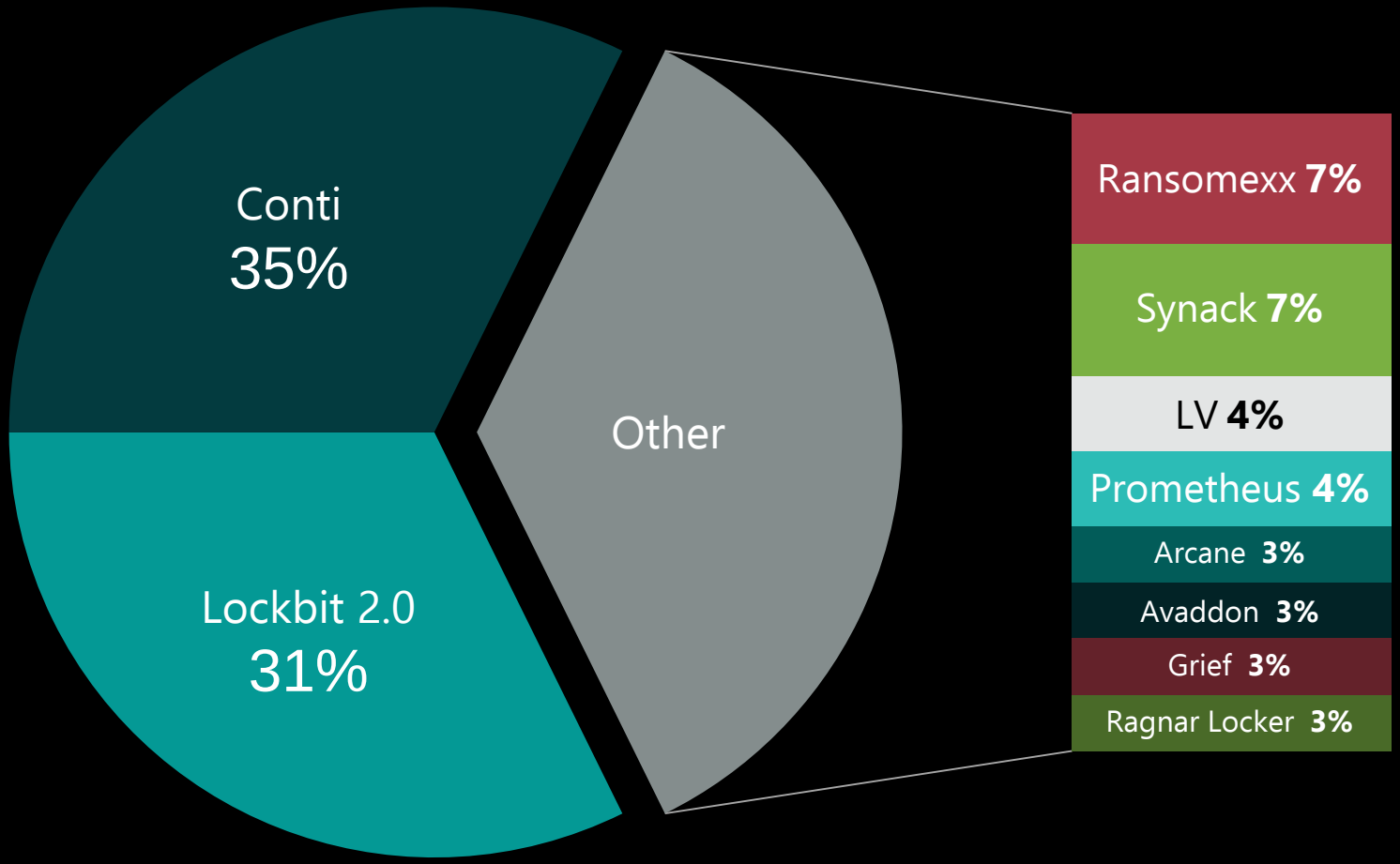
Appleseed is a multi-component backdoor that can take screenshots, log keystrokes, and collect removable media information and specific victim files. It can also upload, download and execute follow-on commands from the C2 server.

Routine functionality, over focusing on malware betrays people with adversary problems

Ransomware Attacks Against Manufacturing Firms



Ransomware Attacks Against Manufacturing by Group/Strain



Ransomware – JBS Foods

- JBS Foods is the largest meat processing company in the world
- May 30 - the day of the ransomware attack.
- Discovered chunks of data uploaded to the 'Mega' file sharing service from JBS dating back to March 4th
  - Uploads continued sporadically, ~40-60GB of data uploaded
- While this may have been the work of a JBS employee, Dragos assesses with high confidence the activity can be attributed to these ransomware actors, as Mega has been used to store information by ransomware actors in at least three other exfiltration campaigns

Assessment: Dragos assesses with moderate confidence ransomware groups will continue slow exfiltration of data, possibly to avoid activating security controls, in the months and weeks leading up to a ransomware extortion event.

Manufacturing as a Vector

Allowing Upstream and Downstream Intrusions

ICS OEM Nexus

- OEMs often have remote access to critical parts of customer networks
  - This means that hackers who breached an OEM could potentially use their credentials to control critical customer processes
- Compromising an OEM magnifies the potential risks to infrastructure
  - Infections in the critical infrastructure sector occurred on IT networks as well as on industrial control system networks that manage critical functions

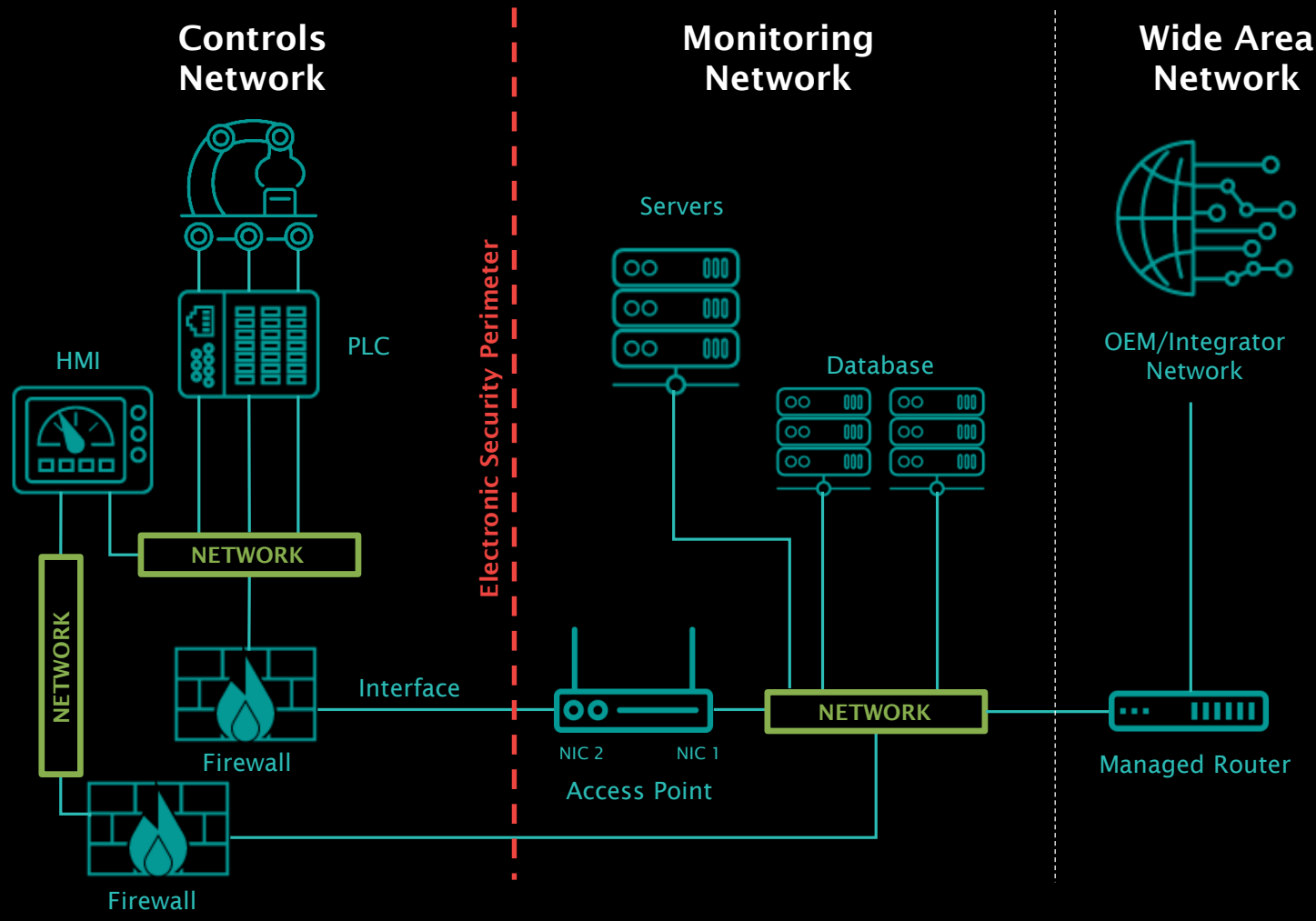
Manufacturing as a Vector: Remote Access

Use cases:

- Monitoring and troubleshooting
- Patch distribution
- Staff augmentation

Cases:

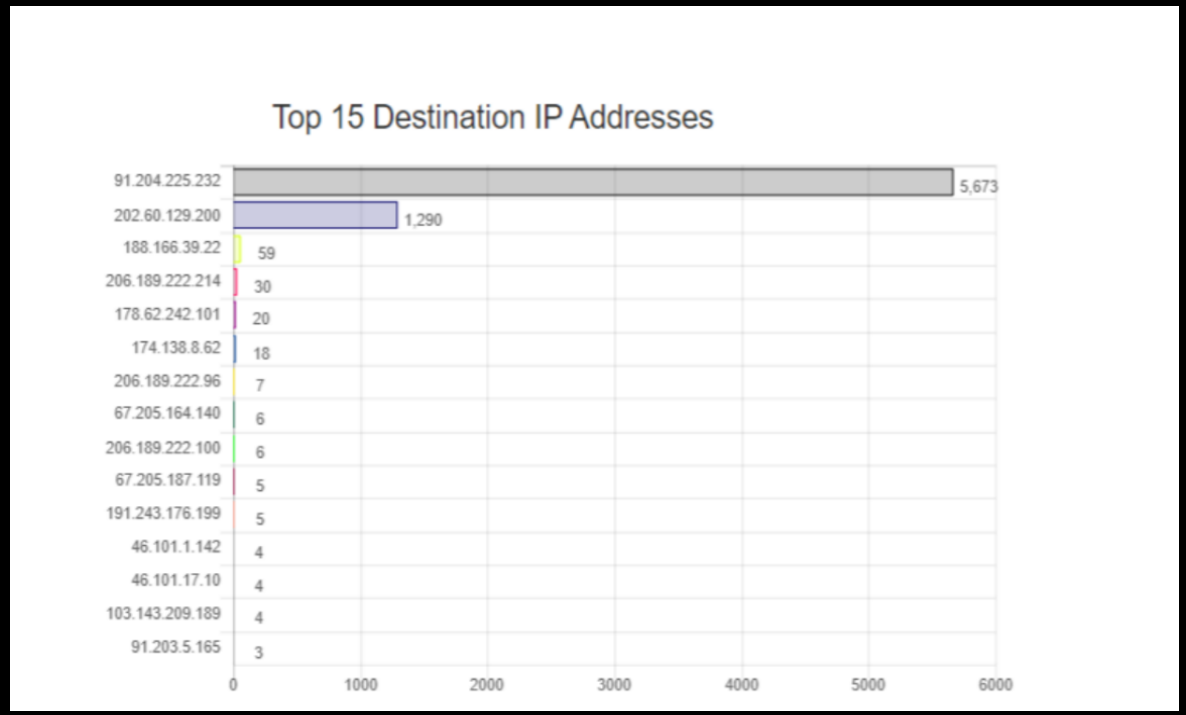
- SolarWinds
- Numerous manufacturer and OEM compromises direct into DCS/SCADA networks of industrial companies



South Asian OT and ICS Provider Targeted

- In late April 2021, Dragos discovered activity associated with an adversary targeting a south Asian based OT and ICS hardware manufacturer and service provider that has direct access to customer networks

- The OEM has customers across the Electric sector; OEM was notified, and response was inadequate



Summary Recommendations

- ACCESS RESTRICTIONS and ACCOUNT MANAGEMENT
  - Restrict administrative access within a domain, limit the number of domain administrators, and separate networking, server, workstation, and database administrators into separate Organizational Units (OUs)
- RESPONSE PLANS
  - Develop, review, and practice cyberattack response plans and integrate cyber investigations into root-cause analysis for all events specific to OT
- THIRD-PARTIES
  - Ensure that third-party connections and OT interactions are monitored and logged, from a “trust, but verify” mindset
- VISIBILITY
  - Take a comprehensive approach for visibility and threat detection into OT environments to ensure that there is no gap in monitoring

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Q&A

Thank you.

Robert M. Lee

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021