DARKTRACE
INDUSTRIAL

The Industrial Immune System

The World's Leading Cyber AI for OT, IT and IoT

Eleanor Weaver & Simon Fellows
Division Director, Darktrace Industrial

at 10th anniversary Cleanpower Smart Grids Conference 2019
www.cir-strategy.com/events

Company Background

DARKTRACE INDUSTRIAL

- World-leading artificial intelligence for cyber defence
- Founded by mathematicians in Cambridge
- Headquartered in San Francisco and Cambridge, UK
- 40 global offices
- 900 employees
- $1.65 billion valuation
- ‘Most Innovative ICS/SCADA Security’ InfoSec Award

THE QUEEN'S AWARDS FOR ENTERPRISE: INTERNATIONAL TRADE 2018

FT FINANCIAL TIMES 1000 Europe's Fastest Growing Companies 2019

statista

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD

50 Technology Fast 50 2018 UK WINNER Deloitte.

FAST COMPANY THE WORLD'S MOST INNOVATIVE COMPANIES 2018

CNBC DISRUPTOR 50

ROYAL ACADEMY OF ENGINEERING

MacRobert Award Finalist


Regina Airport Authority Inc.
SUNSWEET
avancial
BH GLOBAL
drax
energy saving trust
nord energi
PEUGEOT
The Royal Mint
apave
Harwich Haven Authority
Aqua Leisure
EPIC GROUP
Big West Oil
ASTON MARTIN
Westshore Terminals
open energi
Queensland Airports
Birmingham Airport
HUNT & PALMER
BESPOKE AIR CHARTER
MACOM
Steelcase
TREK
TRUCKEE DONNER PUBLIC UTILITY DISTRICT
H&M
Every Step of the Way
USPOWERGEN
Energy+
LOUDOUN WATER
The GLENMORANGIE COMPANY
DOLPHIN ENERGY
inmarsat
AIRLINK
Freedom of the African Sky
Portsmouth Water
RTM
AIG
Zpower
smarter grid solutions
SUZUKI
SANIFLO
A Group SFA Company
LOS ANGELES LGBT CENTER
THE CHURCH OF ENGLAND
SB Simply Business
Public Health England
TRJ TÉLÉCOM
ocado
IG
BT
RLC
TAQA
SingEx
Manchester Metropolitan University
SuMi TRUST
HUDSON PACIFIC PROPERTIES
SCIENCE MUSEUM GROUP
DENVER HEALTH
T-Mobile
IPREO
GROUP 1 AUTOMOTIVE
MetroPath
Belfast Harbour
Coca-Cola
MARITIME NEW ZEALAND
LEERINK
POOL RE
REINSURING TERRORISM RISK
JUMEIRAH GROUP
William HILL
CAMPARI
Johnson Matthey
MACROSYNERGY PARTNERS LLP
GEMFIELDS
DIRECTV
photobox
KOHL'S
Lanyon Bowdler SOLICITORS
Sackers
SHAWBROOK
EVERSHOLT RAIL GROUP
Penguin Random House
British Land
METRO BANK
International Baccalaureate
Bunim/Murray Productions
UST Global
elite insurance company
ebay
STARHOTELS
HUMAN LONGEVITY, INC.
COLONIAL GROUP INTERNATIONAL
Arsene
SLAUGHTER AND MAY
TeleChoice
TSB Bank
expect more
ShookLin & Bok
Kingston TECHNOLOGY
TruWest CREDIT UNION
Dædalus Books
Dreams
CenterParcs
make MY trip .com
CORDENPHARMA
TELSTRA
SAESL
BLACKHAWK NETWORK
32Red online casino
Moneris SOLUTIONS
AIR MALTA
charles river
spoor • fisher
APA NOVA
Allianz
sodexo
Zappos .com
DAC beachcroft
session m
EDISON MISSION ENERGY
neustar
nominet
ALMA BANK
JACKSON
OCEAN FIRST
DNK
Plextek
KEEN
paybay
StarTribune
ADDISON LEE
Teachers Building Society
QUICKPLAY
EPIC SCIENCES
Arbutus BIOPHARMA
TheCityUK
NORTHSIDE HOSPITAL FOUNDATION
bet365
AEGON Sony Life
BNP PARIBAS
Catholic Charities of Santa Clara County
K&L GATES
Wesco Aircraft
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Industrial Security Challenge

DARKTRACE INDUSTRIAL

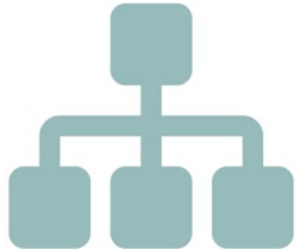
Critical Systems

- Safety critical
- High availability

Difficult to Secure

- Legacy devices
- Proprietary systems
- Lack of visibility

OT/IT Convergence



- Increased exposure
- Greater connectivity

Rising Threat

- Targeted attacks
- Accidental impact
- Insider threat

The Industrial Immune System

- **Passively learns ‘self’ in real time**
For every device no matter how unique or bespoke

- **Detects all forms of threat and vulnerability**
Including malware, malicious insiders, operator error and malfunction

- **100% coverage and visibility**
Full visualization across OT, IT, IoT, Cloud, SaaS

- **Protocol and technology agnostic**
Works with proprietary protocols and encrypted traffic

Why Self-learning?

DARKTRACE
INDUSTRIAL

- Needs to adapt to unique environments
- Needs to learn continuously without maintenance
- Baselining lacks context to tell good from bad
- Baselining can’t detect existing compromise
- Needs to correlate events to reduce number of alerts
- Needs to detect complex novel threat scenarios

THREAT CASE STUDY

Serpent Ransomware Infection

DARKTRACE INDUSTRIAL

Industry: Energy

Point of Entry: Corporate network

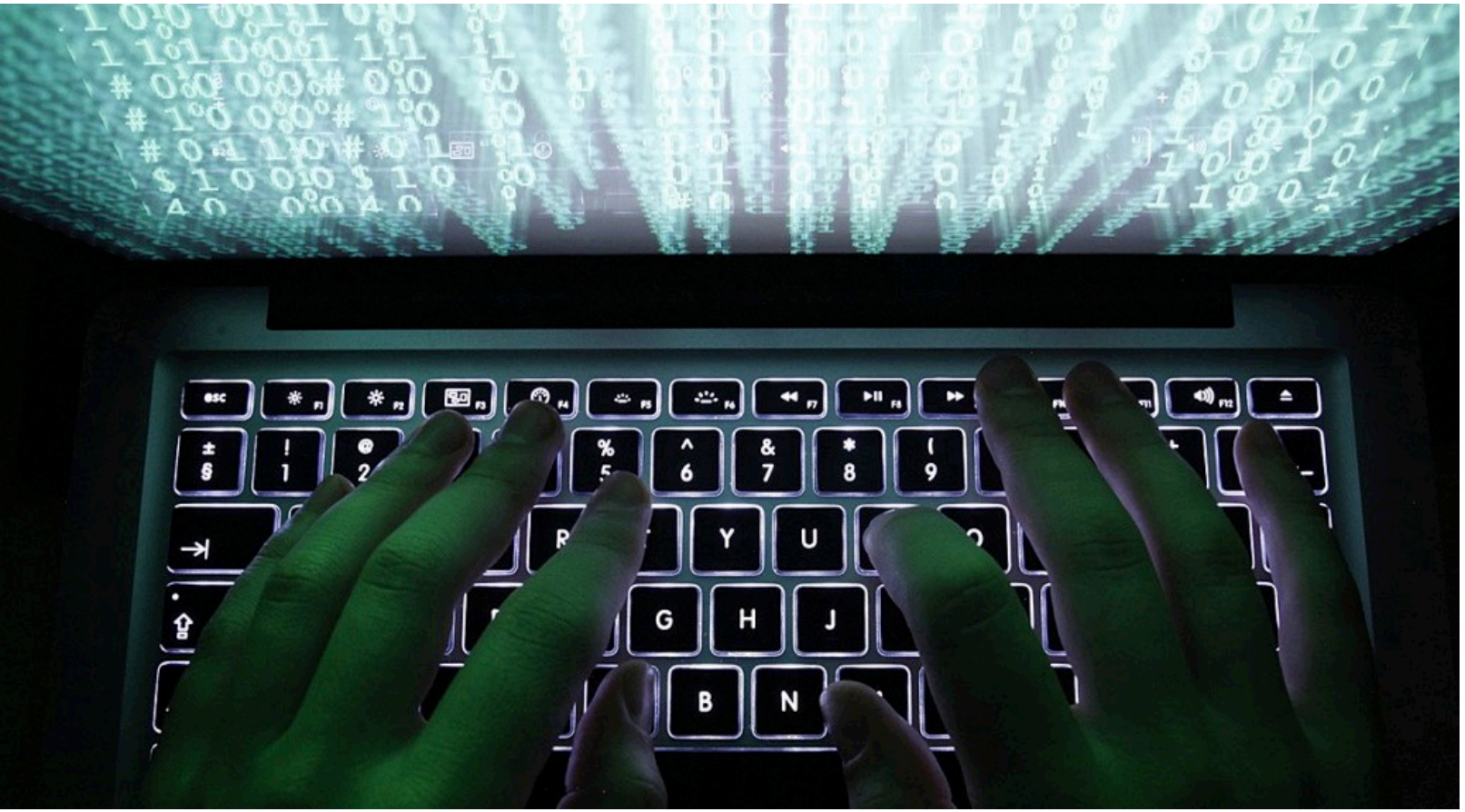
Apparent Objective: Infect OT and IT environments with ransomware

- Series of connections to rare destinations via internal proxy server
- Anomalous communications and downloads detected
- Pattern of behavior for Serpent infection identified

THREAT CASE STUDY

External Reconnaissance

DARKTRACE INDUSTRIAL



Industry: Oil & Gas

Point of Entry: Domain Controller

Apparent Objective: Infiltrate Network

- Blacklisted device with IP address in China discovered connecting to the network
- Connected to domain controller, an employee's computer and the mail server
- Tested for honeypot
- Serious security risk

THREAT CASE STUDY

Compromised Equipment on Assembly Line

DARKTRACE INDUSTRIAL

Industry: Food Manufacturing

Point of Entry: Connected manufacturing devices

Apparent Objective: Take control of Industrial IoT to infiltrate information

- Unknown attacker targeted devices on manufacturing assembly line to gain a foothold into the corporate network
- AI identified infected devices, even though security team was unaware they were connected to Internet
- Darktrace identified several issues with the firewall that were then remediated

Conclusion

DARKTRACE
INDUSTRIAL

- Threat against critical infrastructure and Industrial Internet of Things is growing
- Perimeter security approach is outdated – threat is inside
- Artificial intelligence delivers self-learning defence
- Protects whole infrastructure – operational technologies and traditional IT
- Real-time visibility
- Evolves as environment and threats evolve


DARKTRACE
INDUSTRIAL
Thank you