RANSOMWARE IN OT ENVIRONMENT

SANKET BHASIN | TECHNOLOGY STRATEGIS

HISTORY OF RANSOMWARE

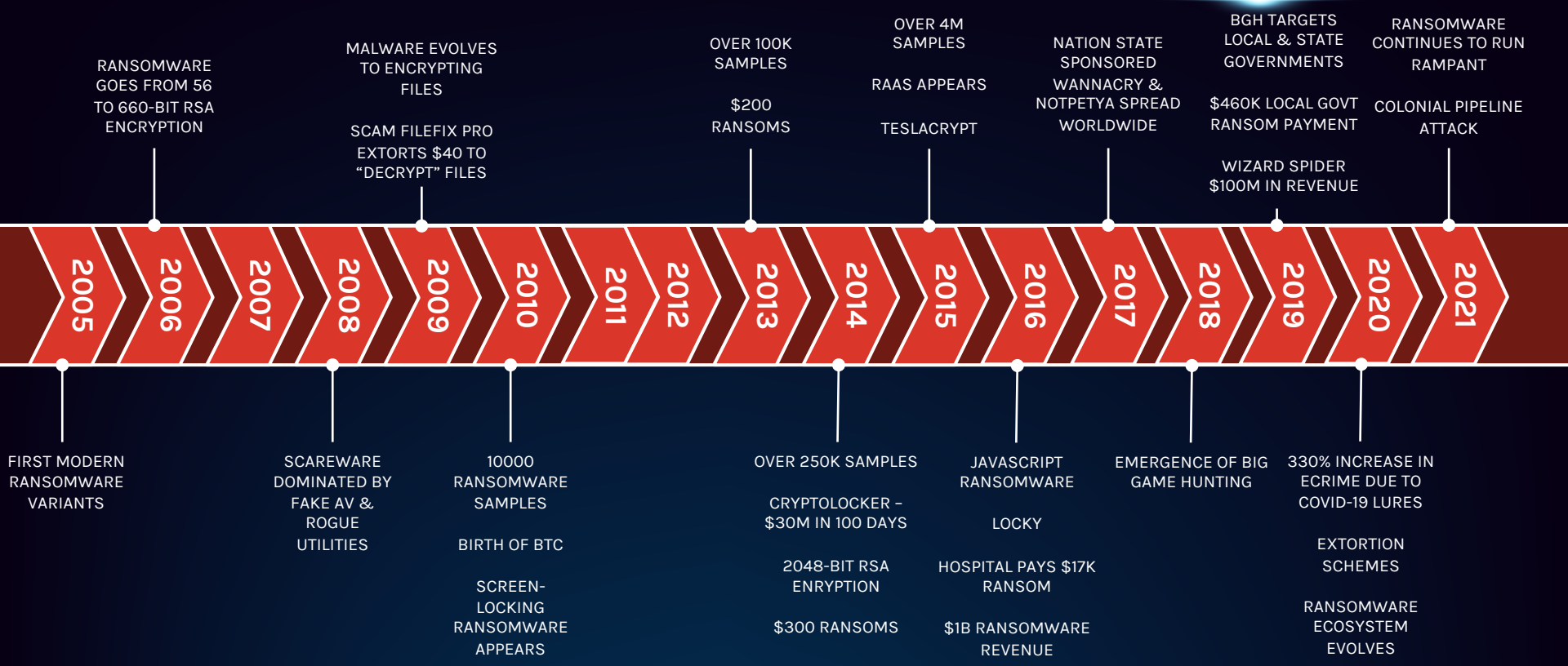
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BRIEF HISTORY OF RANSOMWARE

- DECEMBER 1989 FLOPPY DISKS MAILED TO VICTIMS
- 20,000 SENT TO ATTENDEES OF THE WORLD HEALTH ORGANIZATION'S AIDS CONFERENCE IN STOCKHOLM
- DEMANDED $189 BE MAILED TO A PO BOX IN PANAMA
- “AIDS TROJAN” AKA “PC CYBORG” RANSOMWARE

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BRIEF HISTORY OF RANSOMWARE



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

AGENDA

- COLONIAL PIPELINE ATTACK
- OPERATIONAL TECHNOLOGY THREATS
- WHO IS CARBON SPIDER?
- WHAT NEXT?
- CALL TO ACTION

COLONIAL PIPELINE

RANSOMWARE ATTACK


DID RANSOMWARE CAUSE A PIPELINE OUTAGE?

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHAT IS THE COLONIAL PIPELINE?

- LARGEST PIPELINE FOR REFINED OIL PRODUCTS IN THE UNITED STATES - 5,500 MILES (8,850 KM)
- PROVIDES GASOLINE, HOME HEATING OIL, AVIATION FUEL AND OTHER REFINED PETROLEUM PRODUCTS THE SOUTH AND EASTERN UNITED STATES
- CARRIES 3 MILLION BARRELS OF FUEL EACH DAY FROM TEXAS TO NEW YORK
- OPERATED BY COLONIAL PIPELINE COMPANY, HEADQUARTERED IN ALPHARETTA, GEORGIA

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

RANSOMWARE ATTACK & OPERATIONAL DISRUPTION

- ON MAY 7, DISCOVERED A NETWORK INTRUSION LEADING TO A RANSOMWARE ATTACK
- COLONIAL ACTIVELY SHUT DOWN PARTS OF THE PIPELINE'S OPERATION IN AN ATTEMPT TO CONTAIN THE THREAT
- ATTRIBUTED TO CARBON SPIDER – DARKSIDE RANSOMWARE RESPONSIBLE FOR THE ATTACK
- COLONIAL PAID ADVERSARY APPROXIMATELY $5M (75BTC) RANSOM

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CARBON SPIDER ADVERSARY PROFILE

- ACTIVE SINCE 2013 BUT EXPANDED THEIR TARGETING PROFILE IN DECEMBER 2015
- IN 2016, PART OF THE GROUP SPLIT OFF TO FORM COBALT SPIDER TO FOCUS ON THE FINANCIAL SECTOR
- PRIMARILY RELIES ON SPEAR PHISHING TO DELIVER THEIR CUSTOM HARPY BACKDOOR
- STARTED OUT BY PRIMARILY TARGETING POINT-OF-SALE TERMINALS USING SUPERSOFT TO HARVEST CARD DATA
- MONETIZED STOLEN CARD DATA BY SELLING ON THE CRIMINAL UNDERGROUND, SUCH AS JOKER'S STASH

BIG GAME HUNTING OPERATIONS

- APR 2020, STARTED BIG GAME HUNTING - INITIALLY PARTNERED W/PINCHY SPIDER USING REVIL
- AUG 2020, DARKSIDE RANSOMWARE DISCOVERED IN AT LEAST TWO RANSOMWARE ATTACKS TARGETING NA
- SEP 2020, RELEASED LINUX VARIANT TARGETING ESXI
- NOV 2020, RELEASED RANSOMWARE-AS-A-SERVICE VARIANT AND ANNOUNCED AFFILIATE PROGRAM
- MAY 2021, OSTENSIBLY CLOSED DARKSIDE OPERATIONS


“OT IMPACT OR AN OT OUTAGE,
CAUSED BY AN IT ACTIVITY”

OPERATIONAL TECHNOLOGY

THREATS TO OT, ICS, & SCADA

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BIG GAME HUNTING OPERATIONS

STUXNET

IRAN

BLACKENERGY

UKRAINE

NOTPETYA

MAERSK & MORE

EKANS

MULTIPLE VICTIMS

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

COMPROMISING OPERATIONAL TECHNOLOGY ENVIRONMENTS

- GENERALLY, REQUIRES FIRST COMPROMISING IT ASSETS
- POTENTIAL COLLUSION W/TRUSTED INSIDER(S)
- OT/ICS/SCADA ARE RARELY DIRECTLY ATTACKED
- PRIMARILY UTILIZED FOR DISRUPTION OR DESTRUCTIVE ACTIONS BY SOPHISTICATED NATION STATE ADVERSARIES

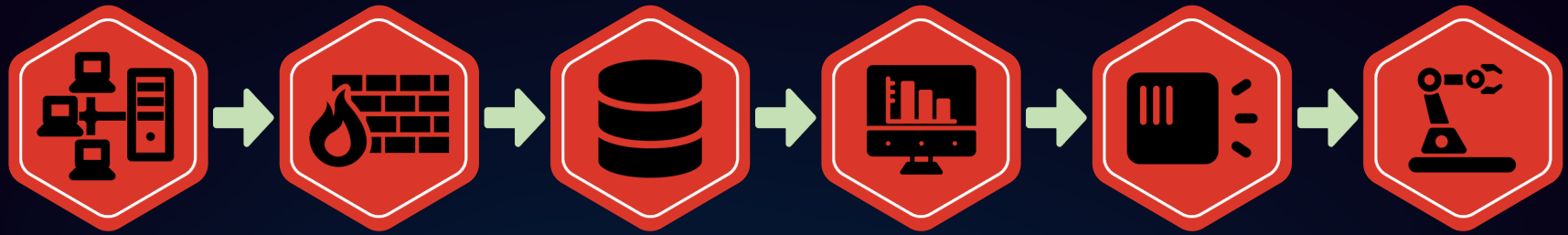
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

IT/OT CONVERGENCE : OVER-RELIANCE ON AUTOMATION?

- IT/OT CONVERGENCE HAS CAUSED ADVANCED NATIONS TO HEAVILY RELY ON AUTOMATION
- COUNTRIES W/LESS DIGITIZATION ARE AT LOWER RISK OF LONGER OUTAGES DUE TO MANUAL STARTUP EXPERIENCE
- USE OF REMOTE ACCESS TECH IN HUMAN MACHINE INTERFACES INCREASES RISK OF TRADITIONAL IT THREATS
- THIS IS NOT CONCEPTUAL – IT HAS HAPPENED

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

PURDUE MODEL FOR ICS SECURITY



LEVEL 4/5	LEVEL 3.5	LEVEL 3	LEVEL 2	LEVEL 1	LEVEL 0
ENTERPRISE (IT NETWORK)	DMZ	OPERATION & CONTROL	CONTROL SYSTEMS	INTELLIGENT DEVICES	PHYSICAL PROCESSES

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

UNDERSTANDING THE OPERATIONAL TECHNOLOGY ATTACK SEQUENCE

RECONNAISSANCE

ADVERSARY CONDUCTS RECONNAISSANCE TO IDENTIFY MULTIPLE METHODS OF GAINING ACCESS TO VICTIM NETWORK

EXPLOITATION

ADVERSARY PURCHASES ACCESS PACKAGE OR IDENTIFIES EXPLOITABLE VULNERABILITY FOR NETWORK ACCESS

COMPROMISE

VICTIM NETWORK IS COMPROMISED, AND ATTACKER IMPLANTS BACKDOORS, STAGES TOOLS, MAINTAINS PERSISTENCE, AND MORE ...

PIVOTING

ADVERSARY MOVES LATERALLY AROUND COMPROMISED NETWORK TO IDENTIFY ACCESS AND GATEWAY(S) TO OT SEGMENT(S)

OBJECTIVES

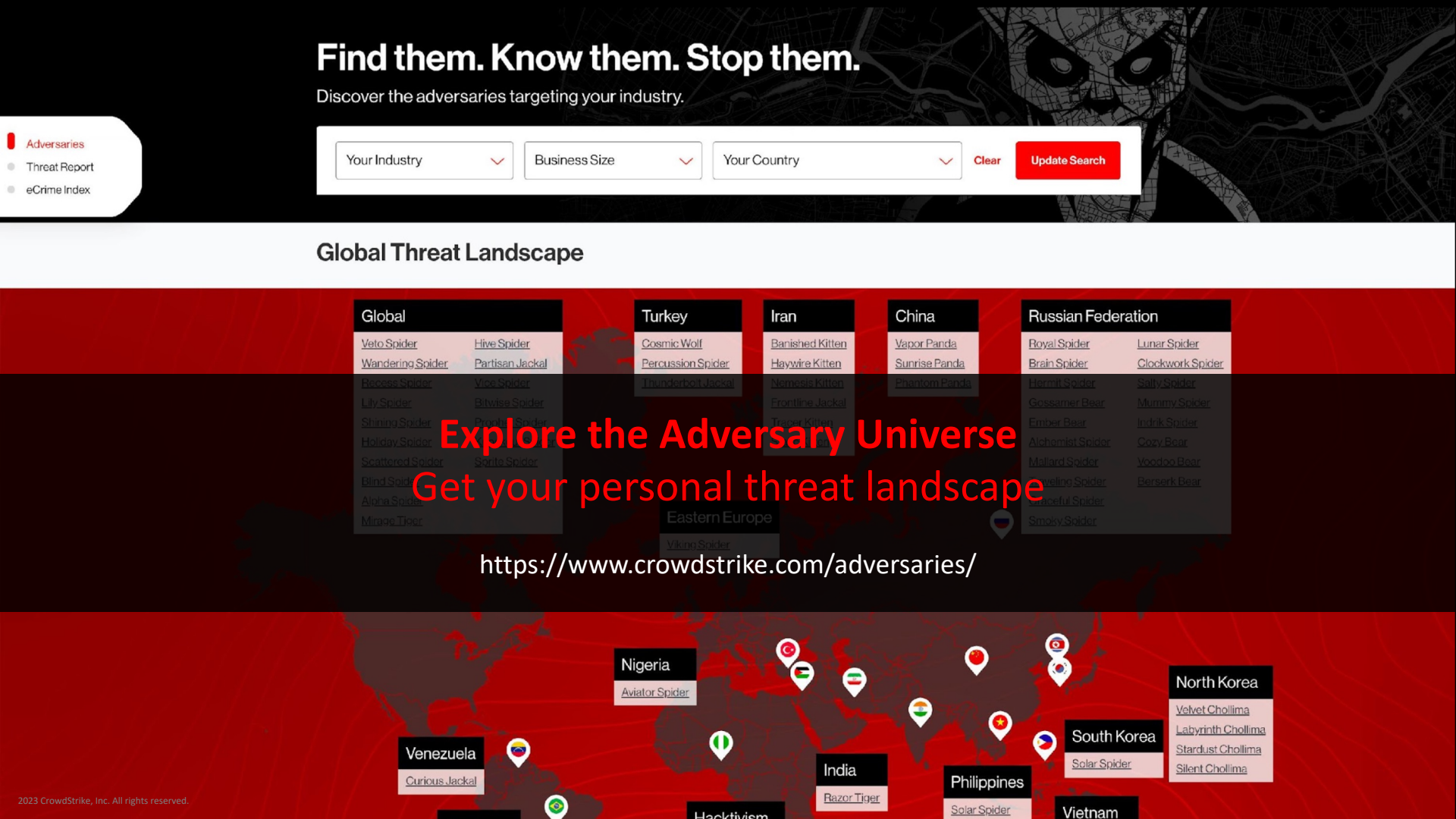
ADVERSARY LOCATES MISSION CRITICAL ASSETS, PERFORMING SOME FORM OF DISRUPTIVE OR DESTRUCTIVE OPERATIONS

WHAT

NEXT?

Stop The Bleed:
7 Steps To Be Prepared

1. Gain visibility into your security gaps
2. Implement separation of IT/OT network: Segment IT/OT
3. Protect Operational/Process Network
4. Reduce attack surface of Legacy devices
5. Prioritize identity protection
6. Know your adversary
7. Practice makes perfect



YOUR ABILITY TO DEFEAT ADVANCED CYBER THREATS RESTS ALMOST ENTIRELY ON YOUR UNDERSTANDING OF THE PROBLEM