

**Program Executive Office  
Command, Control, Communications,  
Computers and Intelligence (PEO C4I)**

**NDIA San Diego Fall Industry Event  
PMW 130 Information Assurance and  
Cybersecurity Program Office**

**27 October 2015**

**Statement A:** Approved for public release; distribution is unlimited (20 OCTOBER 2015)

***Integrated Information  
Dominance for the  
21<sup>st</sup> Century***





# Program Overview

## *Crypto & Key Management*



- Cryptography and Key Management: Acquire, install, and provide life cycle support for end cryptographic units for Navy, Marine Corps, and Coast Guard platforms
  - Data and Voice Cryptography (Modernization and Legacy)
  - Key Management (Electronic Key Management System (EKMS) and Key Management Infrastructure (KMI), Key Loaders)
  - Public Key Infrastructure (PKI)

***Navy's cybersecurity acquisition agent delivering cybersecurity products, capabilities, and services***



# Program Overview

## Computer Network Defense (CND)



- Protects against, monitors, analyzes, detects, and responds to unauthorized activity within Navy tactical networks and attacks against computer-network vulnerabilities, cyber threats, and critical assets
- Capabilities:
  - Shore: Firewalls, Host IPS/FW/Anti-virus, network IDS/IPS, event logging, security compliance scanning and assessment, spyware/malware & anti-virus protection, email scanning gateway, VPNs, Web content filtering, cross-domain solution, data-at-rest encryption, smart card logon (PKI)
  - Afloat: Host IPS/FW/Anti-virus, security compliance scanning and assessment, smart card logon (PKI), cross-domain solution, crypto secure voice/data, data-at-rest encryption

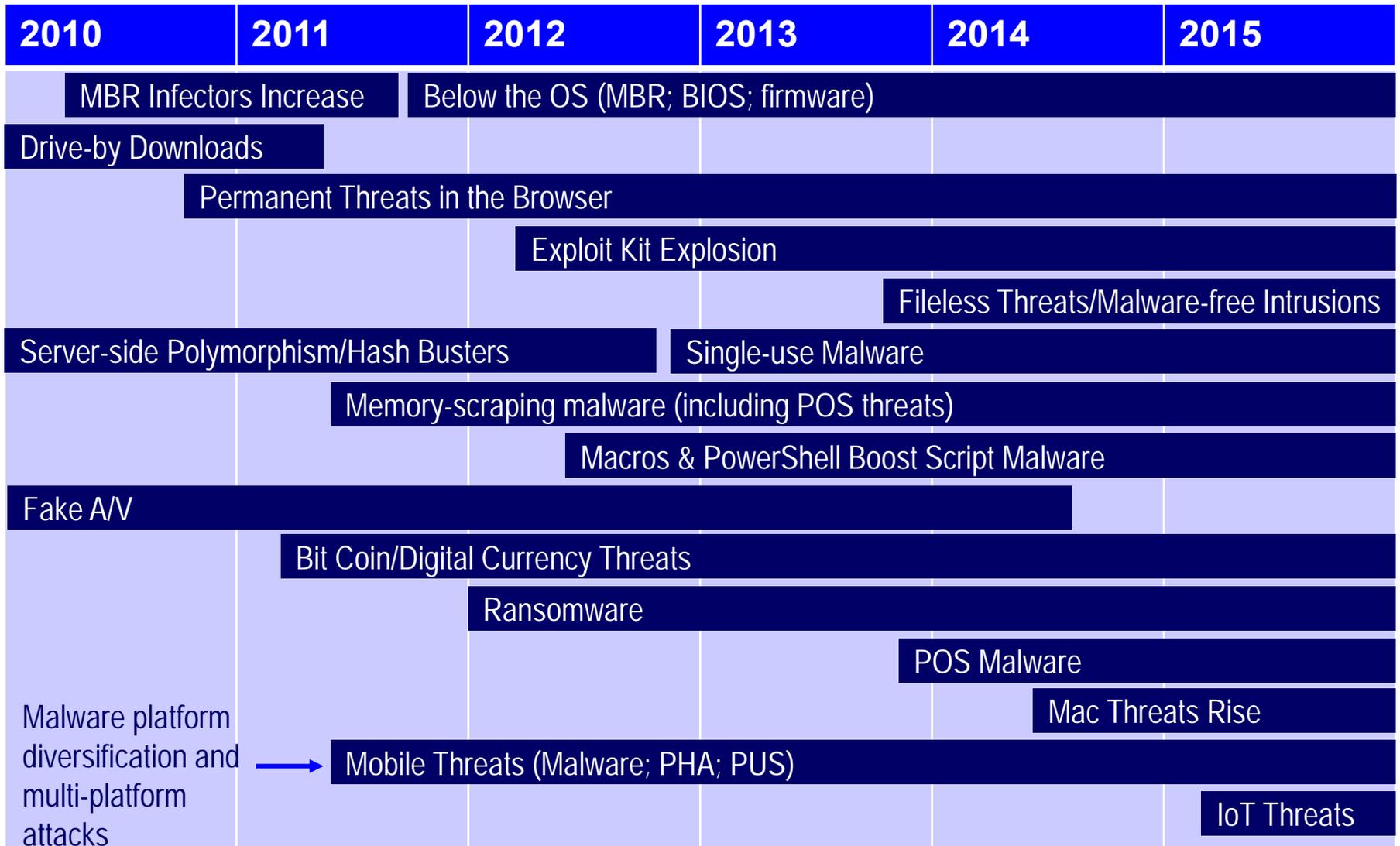


# The Threat Landscape

- 2014: Data breaches increased 23%; vulnerabilities such as Heartbleed, ShellShock, and Poodle had wide-spread prevalence across a number of OSs
- 2014 Trends
  - Attackers moving faster, defenses are not
  - All-time high of 24 discovered zero-day vulnerabilities
    - Took 204 days, 22 days, and 53 days, for vendors to provide a patch for top three most exploited zero-days
  - Attackers streamlining and upgrading techniques
    - 40% increase of highly targeted spear-phishing
    - Watering Hole attacks via legit websites; malware push
    - Trojanized software updates from spoofed websites

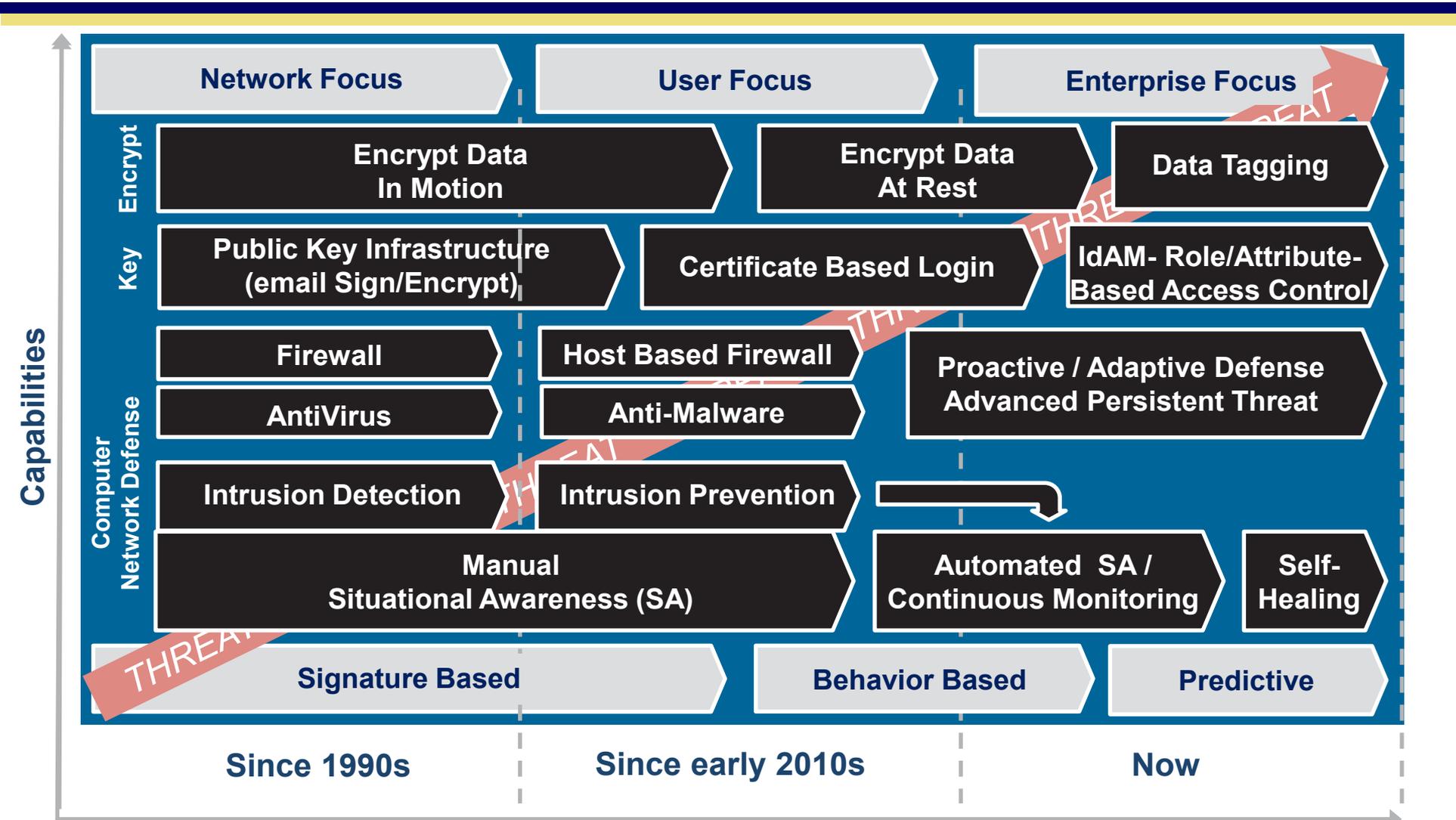


# Five Years of Threats





# Evolution of Cyber Protection Delivered to the Fleet





# Industry Trends

- Real-time Anomaly Detection & Response
- Reactive to Predictive
- Supply Chain Risk Management
- Social Engineering / Phishing
- Speed to Capability
- Industrial Control Systems
- Cyber SA / Continuous Monitoring
- Bring Your Own Device (BYOD)
- Education, Training, and Awareness
- Insider Threat/Data Loss Prevention
- Agile Configuration Management





# Industry Partnerships



Contract Number	SPAWAR HQ Contract Title	Contractor (Prime)	Contract Type	Ceiling Amount	POP
N00178-05-D-4180 NS04	PMW 130/160 Installation Support	ANSOL	CPFF	\$4,825,652	10/1/2012 - 9/30/2017
N00178-14-D-8006 NS01	PMW 120/130 Financial Support Services	Artemis	CPFF	\$13,122,450	6/1/2014 - 5/31/2019
N00178-05-D-4611 NS06	PMW 160/130 Integrated Logistics Support	TCI	CPFF	\$4,151,539	10/1/2012 - 9/30/2017
N00178-04-D-4024 NS41	PMW 130 Information Assurance, PM & Tech Spt	BoozAllen	CPFF	\$65,763,728	10/1/2012 - 8/31/2017

Note: light blue rows indicate small business

***Program Office teamed with Industry to support the Navy and PEO C4I's Cybersecurity mission***