PhishMe: Disrupting Cyber Attack Detection & Response

The PhishMe Ecosystem

January 2015

Spear Phishing: The Attack Vector of Choice

V3.co.uk All the latest UK technology news, reviews and analysis

Home | News | Features | Blogs | Video | Reviews | Downloads

IPad | Software | Internet | Security | Government | Social Networking | Mobile Phones

Home > News > Security

Governments warne
after Israel computer

by Alastair Stevenson 27 Jan 2014

ITPRO
IT ANALYSIS. BUSINESS INSIGHT.

Home | Security | Mobile | Server | Networking | Cloud | Strategy | Public Sector | Storage

News | Analysis & Insight | Reviews | Tutorials | Whitepapers | Cloud Re

Home » Security » News » Microsoft confirms law enforcement docs stolen during recent hacks

osoft confirms law
cement docs stolen
g recent hacks

27 Jan, 2014 | Caroline Donnelly

91 percent of cyberattacks that begin with spear phishing

The A

Data Center | Software | Networks

SECURITY

Hacker breaks into ThrustVPS, launches phishing attack from firm's own servers

Company confesses to cockup after Reddit thread surfaces

By Team Register, 21st January 2014

8

Virtual private server firm ThrustVPS has taken the unusual step of admitting it had suffered a phishing attack.

PHISHME

We Have a Detection Problem!

Median number of days that attackers were present on a victim network before detection[1]

229

Percentage of breaches that went undetected for “months or more”[2]

66

1 www.mandiant.com/resources/mandiant-reports/
2 http://www.verizonenterprise.com/DBIR/2013/

PHISHME

We Need to Cultivate Human Attack Sensors

2010 Times Square car bombing attempt

From Wikipedia, the free encyclopedia

The attempted car bombing of Times Square on May 1, 2010, was a planned terrorist attack which was foiled when two street vendors discovered a car bomb and alerted a New York Police Department (NYPD) patrolman to the threat after they spotted smoke coming from a vehicle.[1][2] The bomb had been ignited, but failed to explode, and was disarmed before it caused any casualties.[1][3][4]

Two days later federal agents arrested Faisal Shahzad, a 30-year-old Pakistan-born resident of Bridgeport, Connecticut, who had become a U.S. citizen in April 2009.[5] He was arrested after he had boarded Emirates Flight 202 to Dubai at John F. Kennedy International Airport.[5][6][7][8][9] He admitted attempting the car bombing and said that he had trained at a Pakistani terrorist training camp, according to U.S. officials.[10]

United States Attorney General Eric Holder said that Shahzad's intent had been "to kill Americans".[5] Shahzad was charged in federal court in Manhattan on May 4 with attempted use of a weapon of mass destruction and other federal crimes related to explosives.[5] More than a dozen people were arrested by Pakistani officials in connection with the plot. Holder said the Pakistani Taliban directed the attack and may have financed it.[11]

U.S. Secretary of State Hillary Clinton warned of "severe consequences" if an attack like this were to be successful and traced back to Pakistan.[12] The Obama administration saw a need for retaliatory options, including unilateral military strike in Pakistan, if a future successful attack was to be traced to Pakistan-based militants.[13]

On October 5, 2010, Shahzad was sentenced to life in prison after pleading guilty to a 10-count indictment in June, including charges of conspiracy to use a weapon of mass destruction and attempting an act of terrorism.[14]

PHISHME

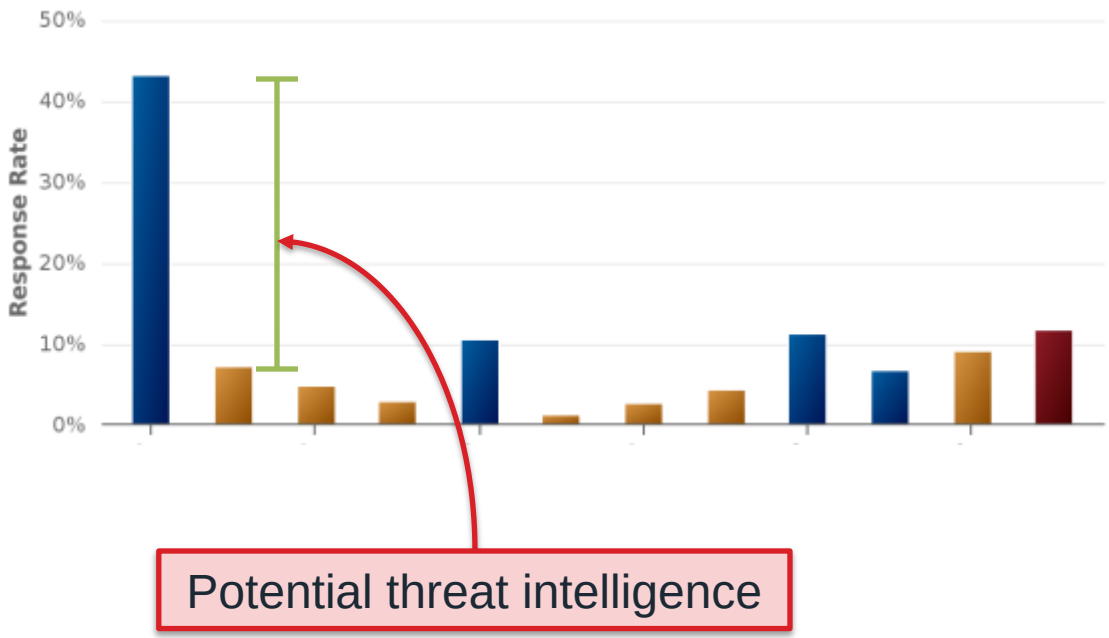
Mitigation is necessary

..but not sufficient

PHISHME

Can Employees Act as Attack Sensors?

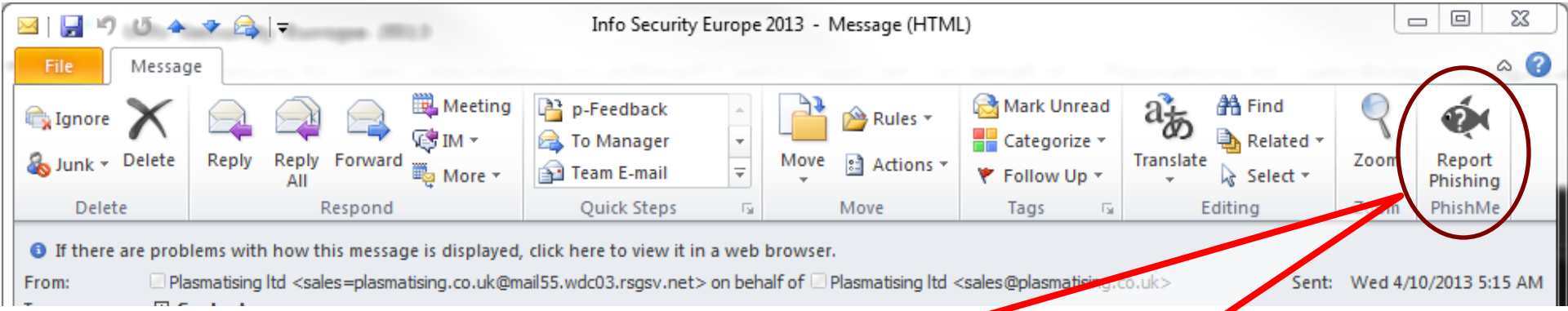
- People respond to emails quickly
- Empowered and encouraged users report
- IR & SOC teams get relevant and timely threat intelligence
- New source of “big data”



PHISHME

PHISHME

PhishMe Reporter: User-sourced Detection



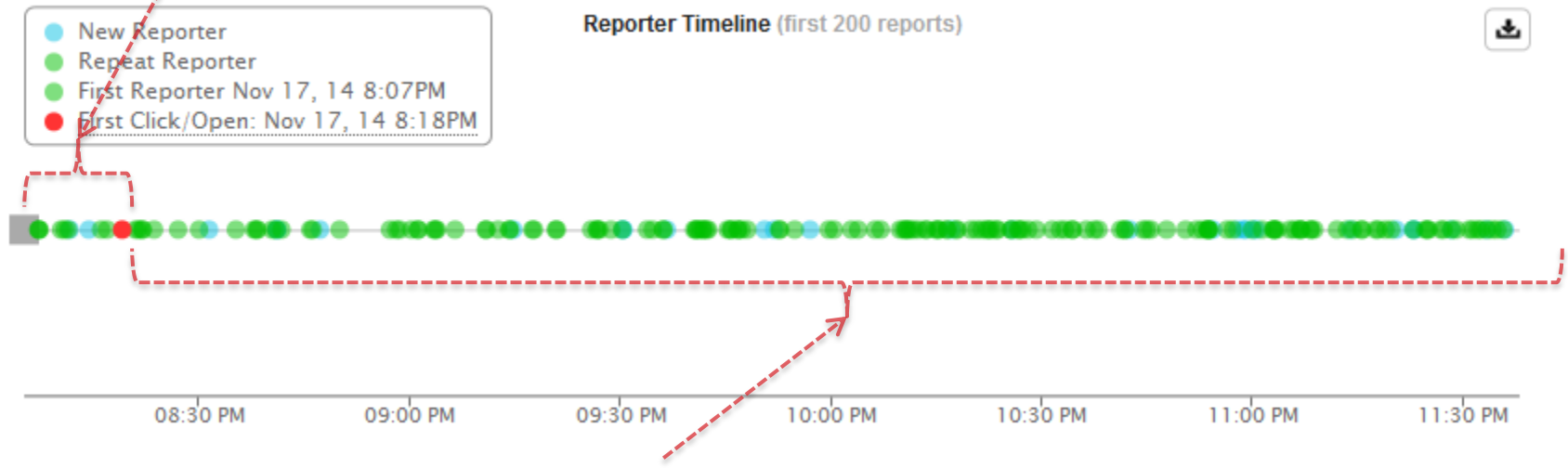
- Simplified single-click reporting for users
- Standardized submission format for IR/help desk
- Taps into human intelligence
- Generate a new source of threat data

PHISHME

Shrink Detection Time to Seconds

At 8:07 PM, **the first of several diligent users reported the attack – 11 minutes before the first compromised user clicked** on the fraudulent link (8:18 PM).

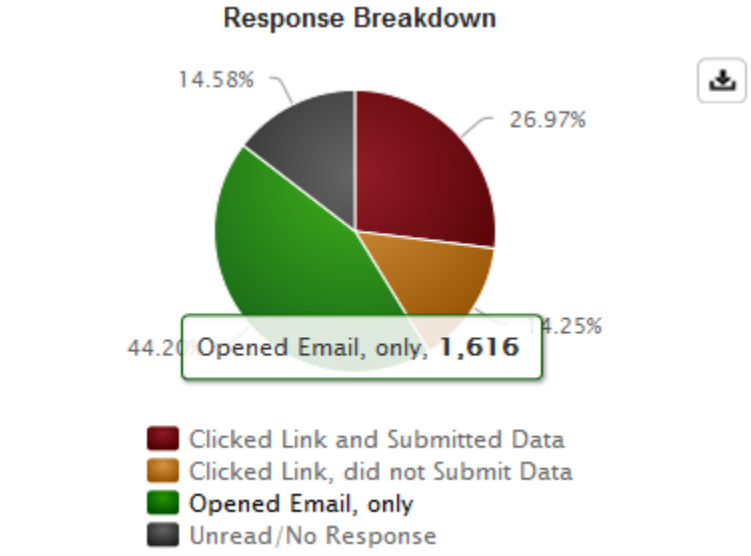
Customer deployed Reporter to 80,000 endpoints

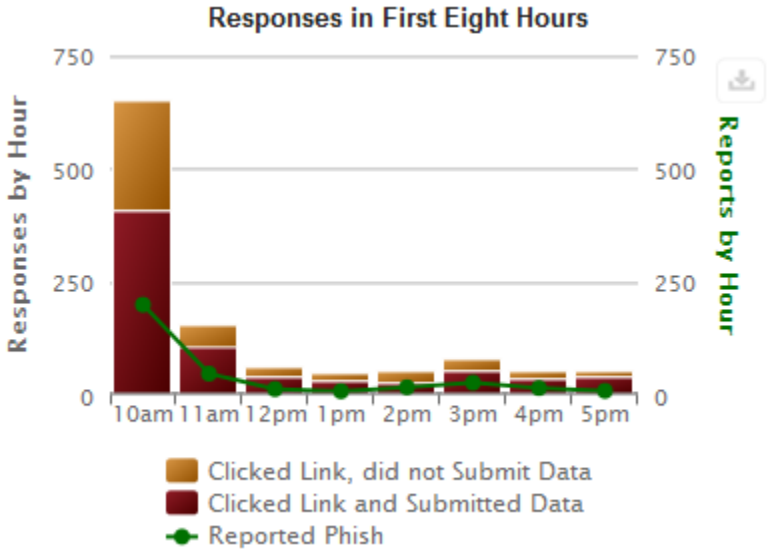


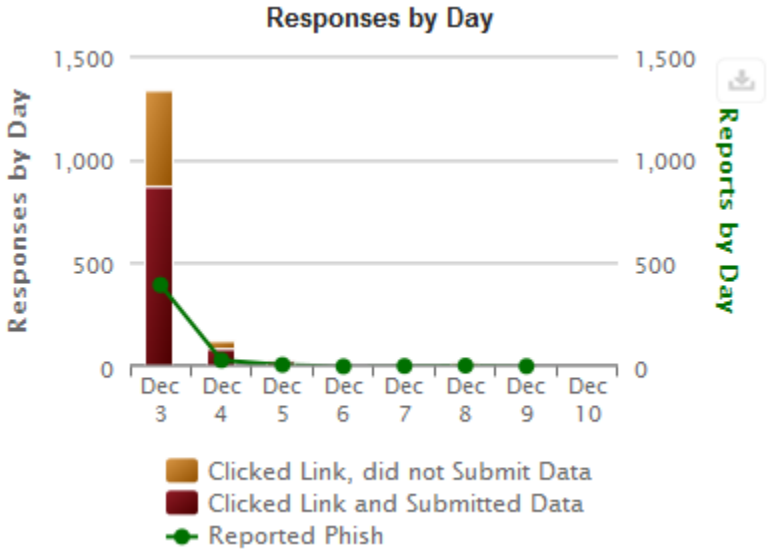
Next set of users correctly identified the attack

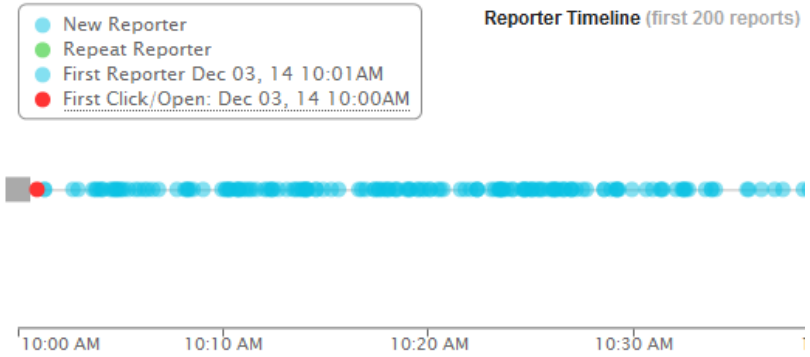
PHISHME

Recent deployment

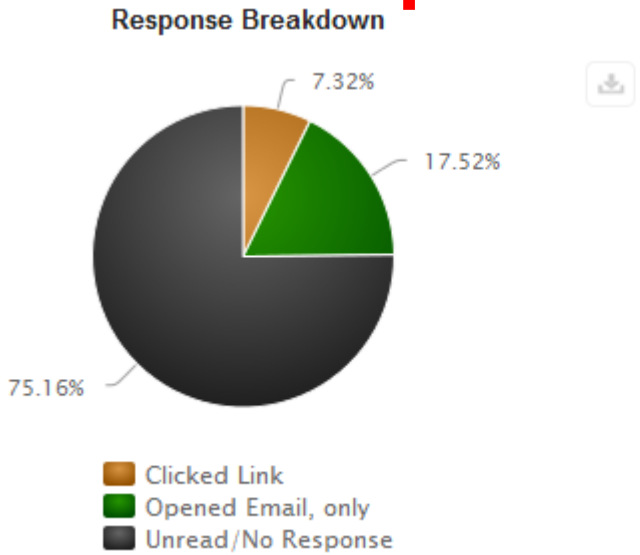


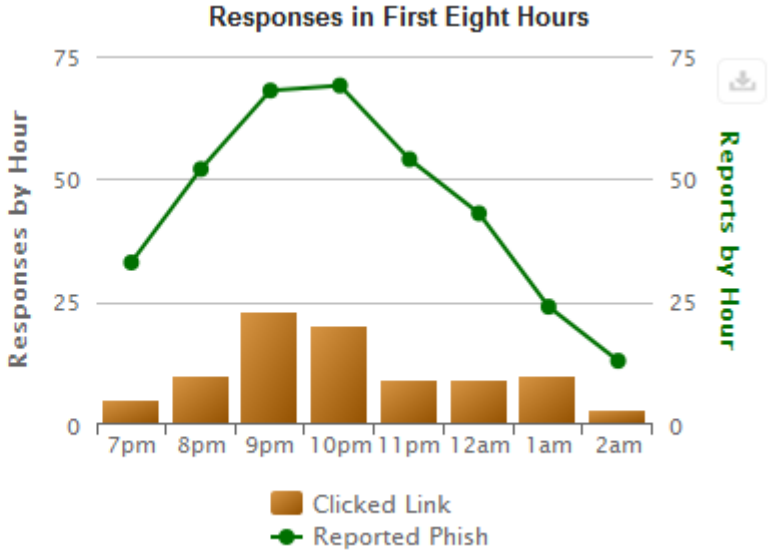


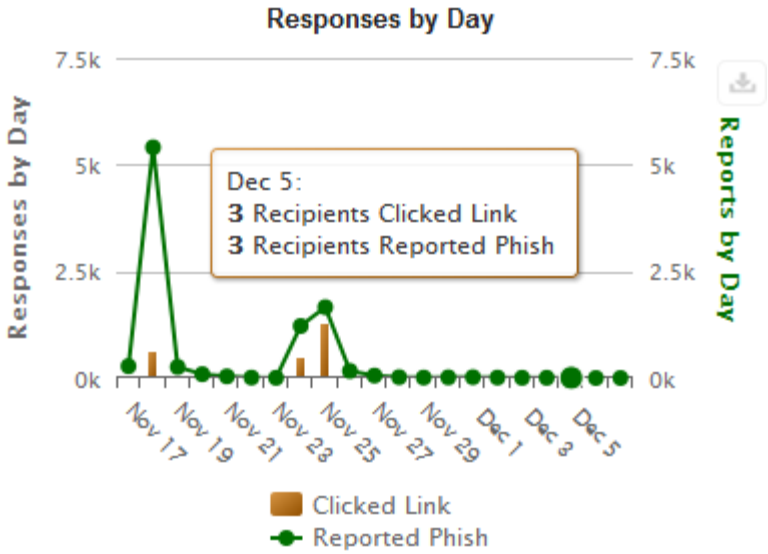


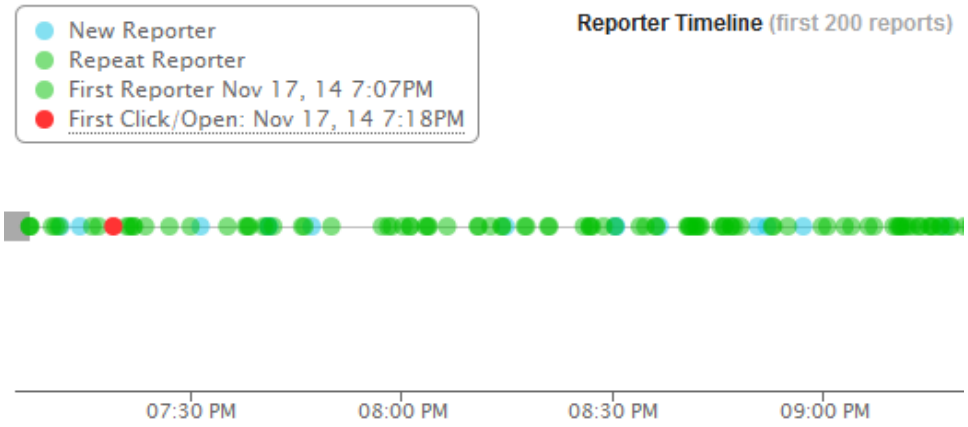


Established reporter install base

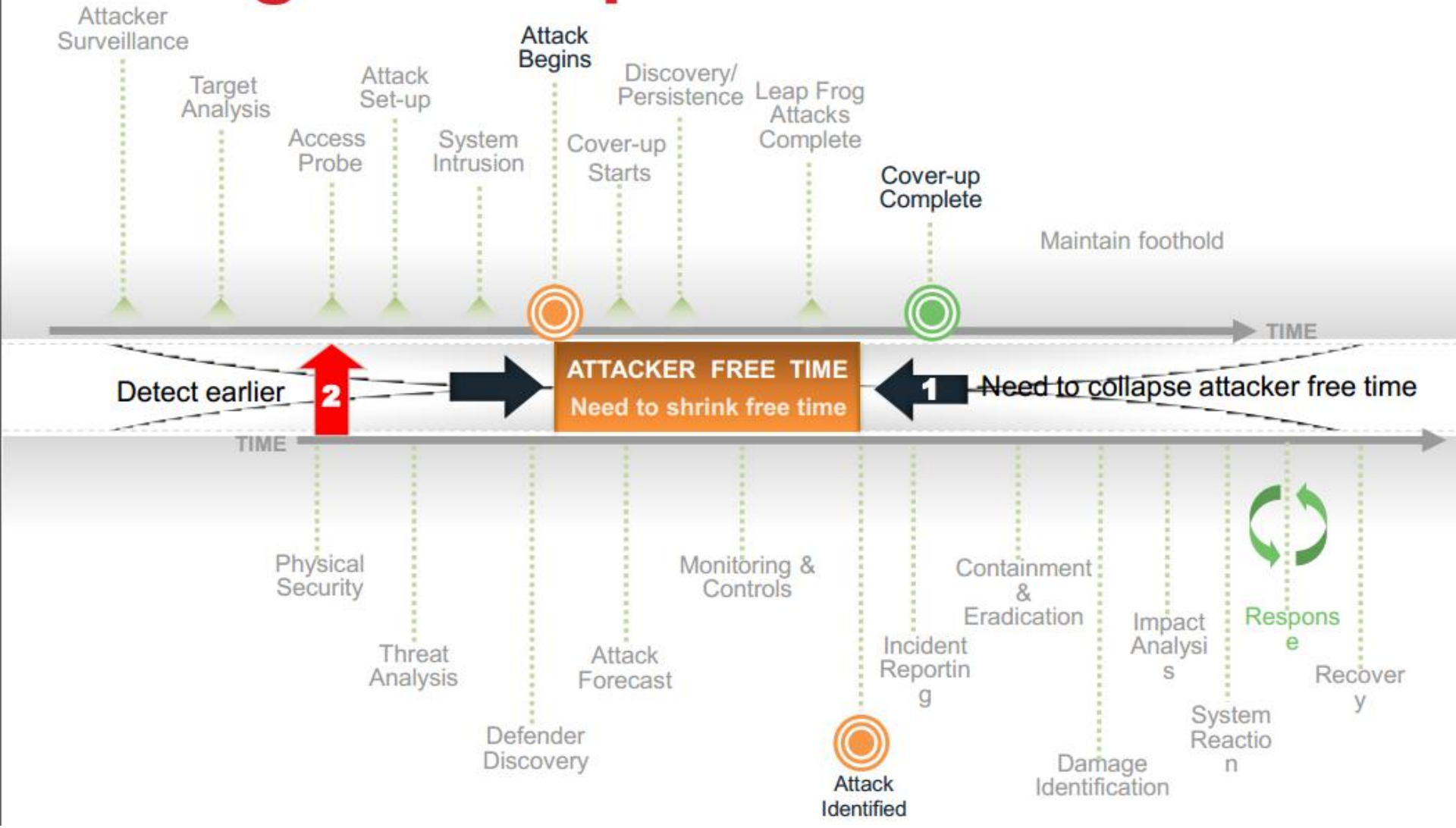








Intelligence Improves Detection



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

PHISHME

The new face of incident detection

VP, Finance and avid reporter of suspicious emails

Discovered Dyre malware

How many Sams do you have in your organization?

PHISHME

www.PhishMe.com

@PhishMe