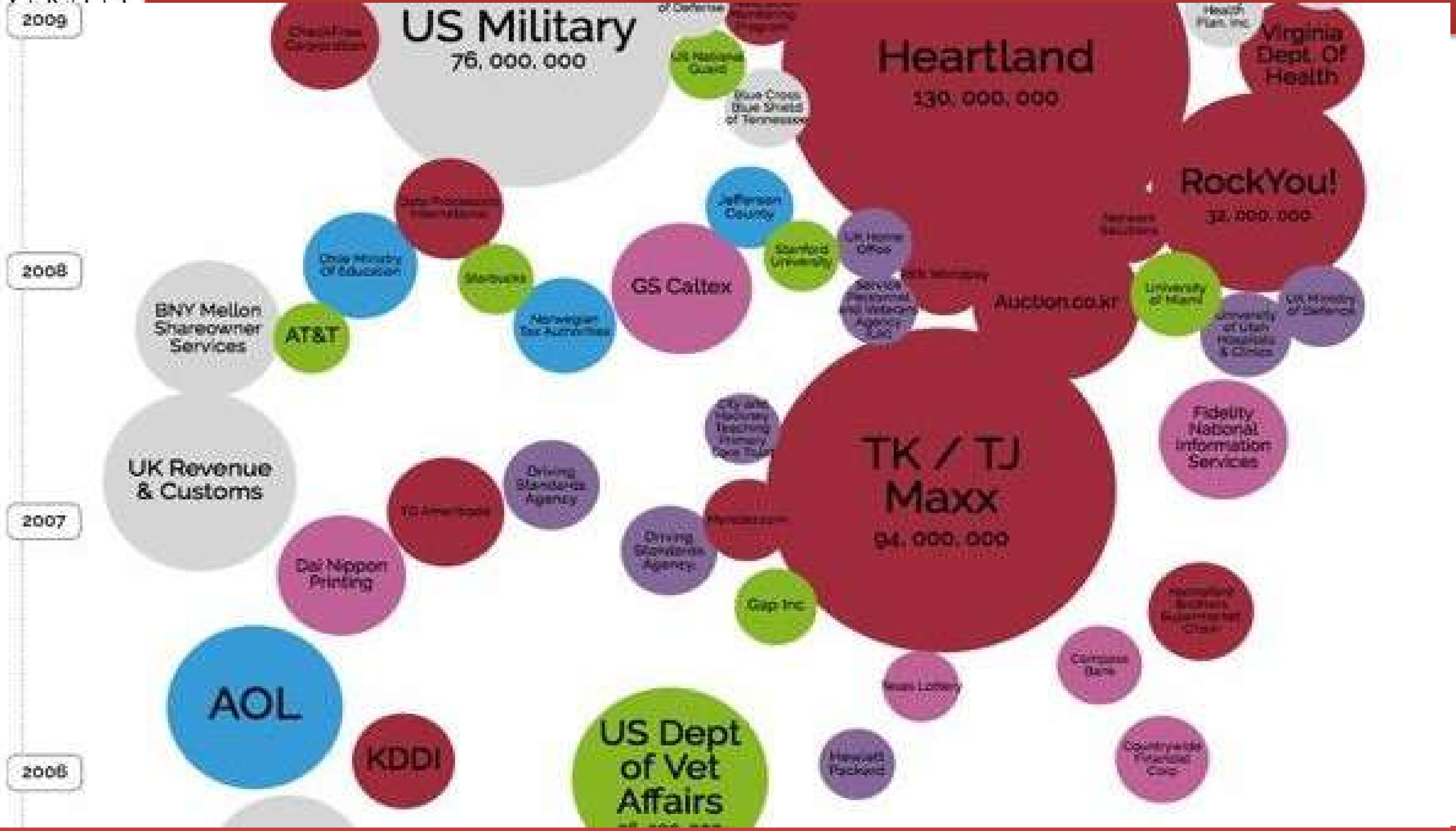
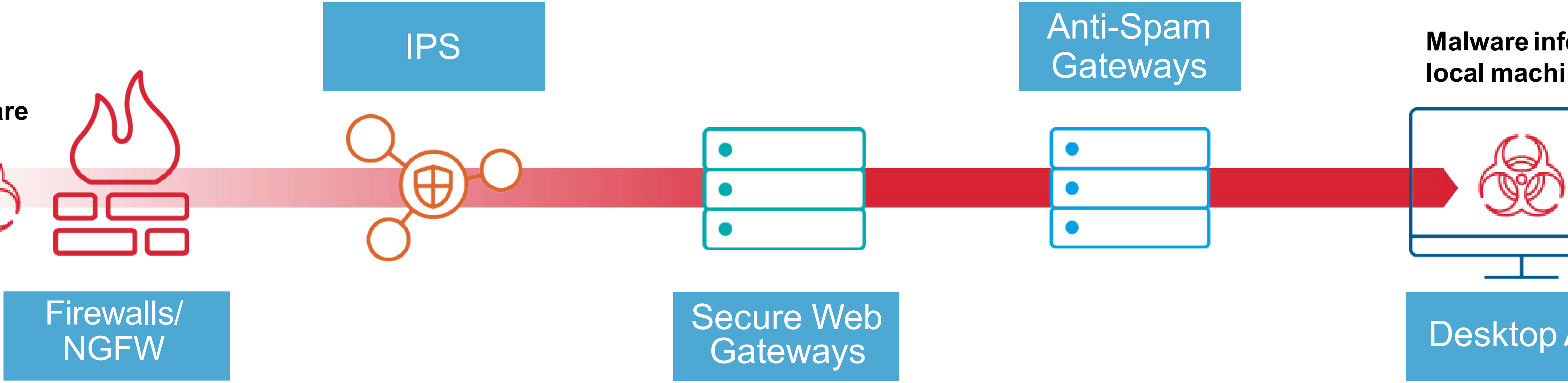
BREACHES ARE INEVITABLE, BUT THE OUTCOME IS NOT

O YOU HAVE A CYBER RESPONSE CAPABILITY?

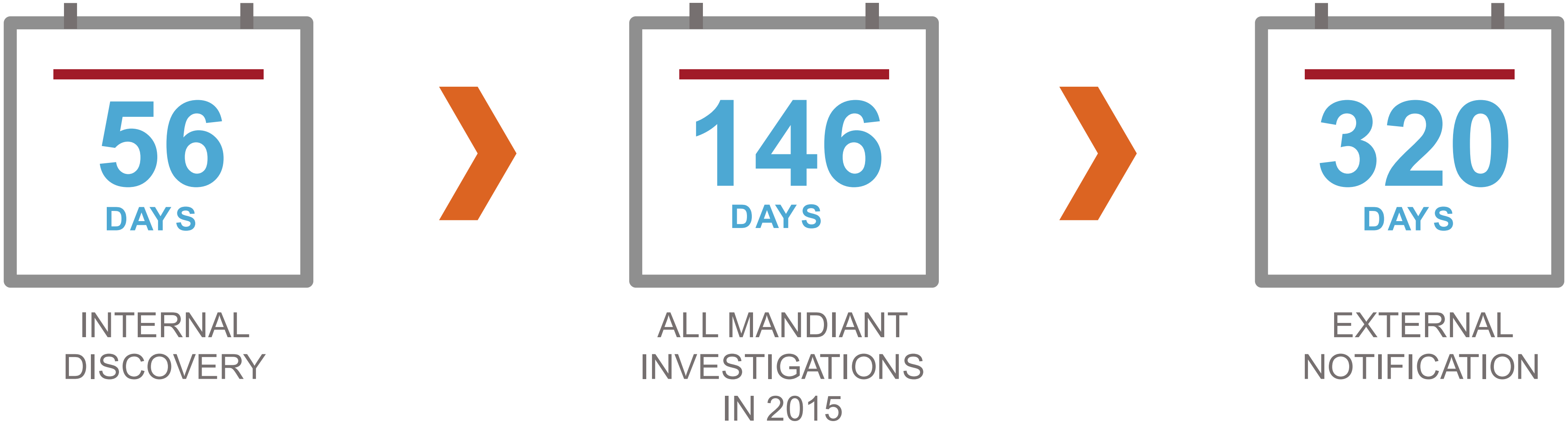
THREAT LANDSCAPE


2009
2008
2007
2006
US Military
76, 000, 000
CheckFree Corporation
of Defense
US National Guard
Blue Cross Blue Shield of Tennessee
Heartland
130, 000, 000
Health Plan, Inc
Virginia Dept. Of Health
RockYou!
32, 000, 000
Network Solutions
Data Processors International
Chile Ministry of Education
Starbucks
Norwegian Tax Authorities
GS Caltex
Jefferson County
Stanford University
UK Home Office
Service Personnel and Veterans Agency (UK)
Auction.co.kr
University of Miami
University of Utah Hospitals & Clinics
UK Ministry of Defence
BNY Mellon Shareowner Services
AT&T
UK Revenue & Customs
City and Hackney Teaching Primary Care Trust
TK / TJ Maxx
94, 000, 000
Fidelity National Information Services
Driving Standards Agency
TD Ameritrade
Monster.com
Driving Standards Agency
Dai Nippon Printing
Gap Inc
Hannaford Brothers Supermarket Chain
Compass Bank
Texas Lottery
AOL
KDDI
US Dept of Vet Affairs
Hewlett Packard
Countrywide Financial Corp

New Types of Attack Techniques Evade Traditional Defenses



Median time from breach to discovery is still too long



56 DAYS

INTERNAL DISCOVERY

146 DAYS

ALL MANDIANT INVESTIGATIONS IN 2015

320 DAYS

EXTERNAL NOTIFICATION

mpact of the current security model

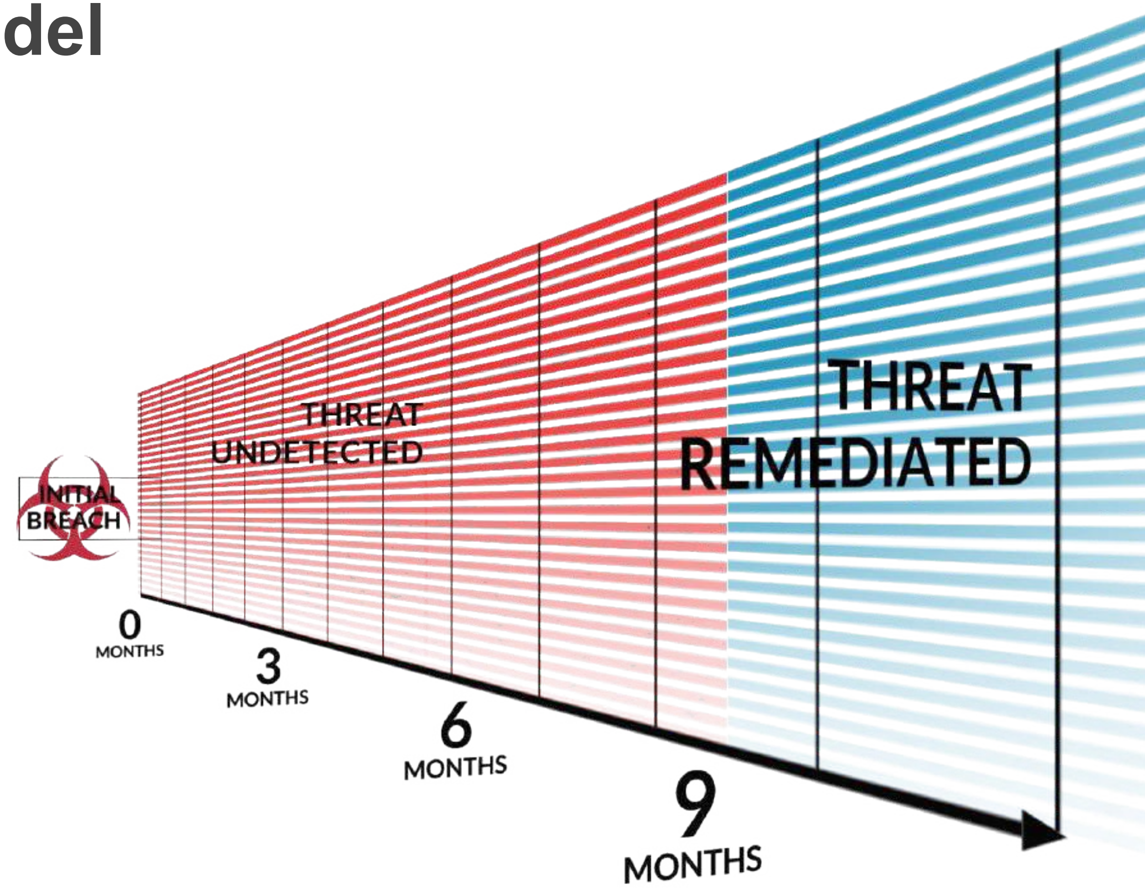
$$$ cost of breach

97% of organizations were breached
3/4 had active command and control communications

146 days median number of days before detection

32 days to respond to a breach

53% of companies learned they were breached from an external entity



SOURCE: MANDIANT M-TRENDS REPORT / PONEMON COST OF DATA BREACH STUDY
Cyber Security's Maginot line: A Real-World Assessment of the Defense-in-Depth Model

What are the challenges?

It's a "who," not a "what"

There is a human at a keyboard

Highly tailored and customized attacks

Targeted specifically at you

Professional, organized and well funded

Escalate sophistication of tactics as needed

Relentlessly focused on their objective

If you kick them out they will return

They have specific objectives

Their goal is long-term occupation

Persistence tools and tactics ensure ongoing access

ADVANCED ATTACK IS A HUMAN PROBLEM NOT A MALWARE PROBLEM

Key Mistakes

We have the proper protection in place

- Attackers use ‘Acceptable’ Risks to get to you

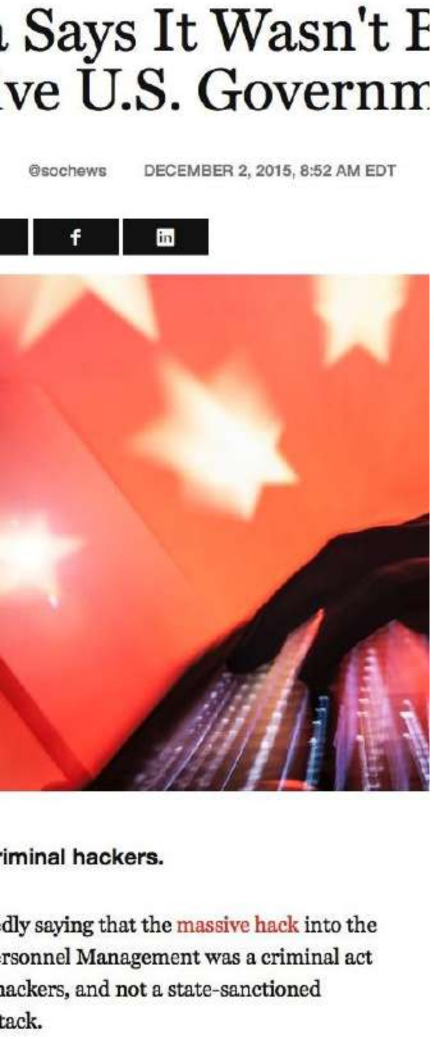
Up to date patches & signatures are enough to protect our crown jewelries

- Nowadays malware is highly obfuscated and customized to avoid detection based on signatures

Expecting large scale breaches to look large

- Big breaches are the hardest to detect

he Impact of an Attacker– “WHO”

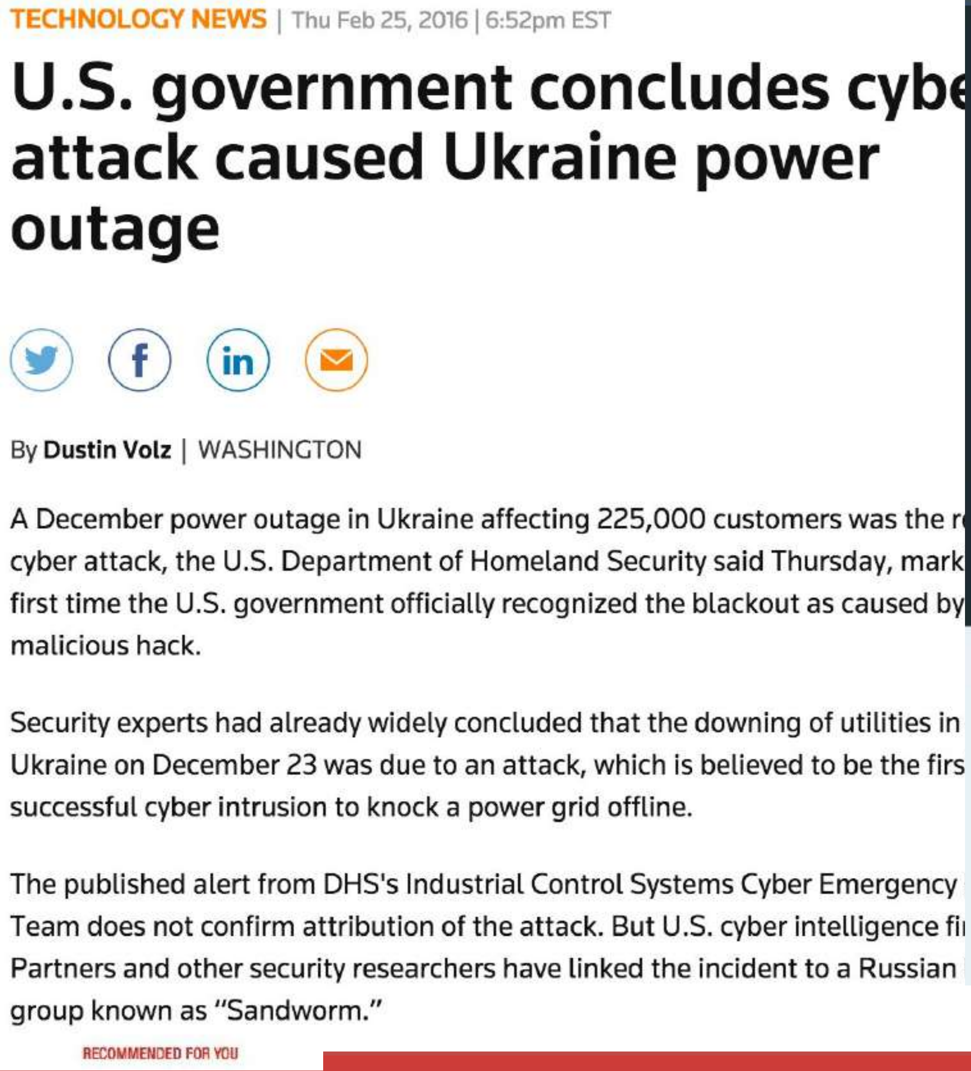


ı Says It Wasn't E
ıve U.S. Governm

@sochews DECEMBER 2, 2015, 8:52 AM EDT

riminal hackers.

edly saying that the massive hack into the
ersonnel Management was a criminal act
hackers, and not a state-sanctioned
tack.



TECHNOLOGY NEWS | Thu Feb 25, 2016 | 6:52pm EST

U.S. government concludes cybe attack caused Ukraine power outage

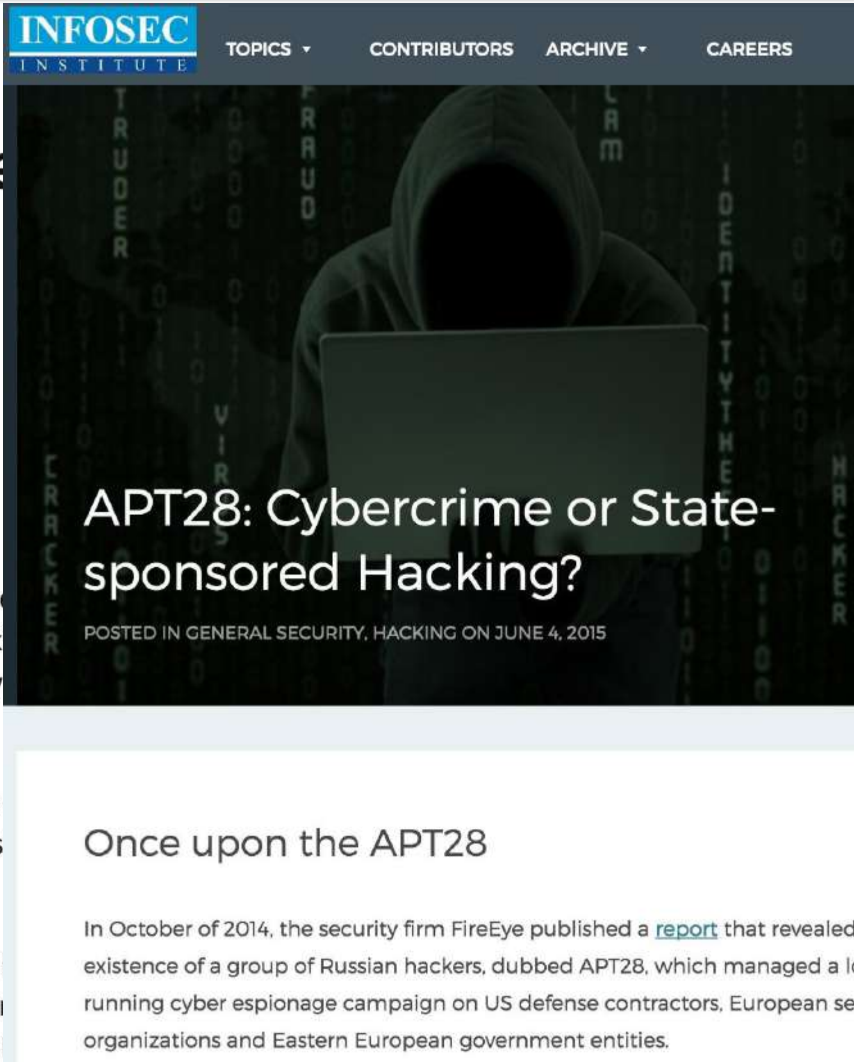
By Dustin Volz | WASHINGTON

A December power outage in Ukraine affecting 225,000 customers was the r cyber attack, the U.S. Department of Homeland Security said Thursday, mark first time the U.S. government officially recognized the blackout as caused by malicious hack.

Security experts had already widely concluded that the downing of utilities in Ukraine on December 23 was due to an attack, which is believed to be the firs successful cyber intrusion to knock a power grid offline.

The published alert from DHS's Industrial Control Systems Cyber Emergency Team does not confirm attribution of the attack. But U.S. cyber intelligence fi Partners and other security researchers have linked the incident to a Russian group known as "Sandworm."

RECOMMENDED FOR YOU



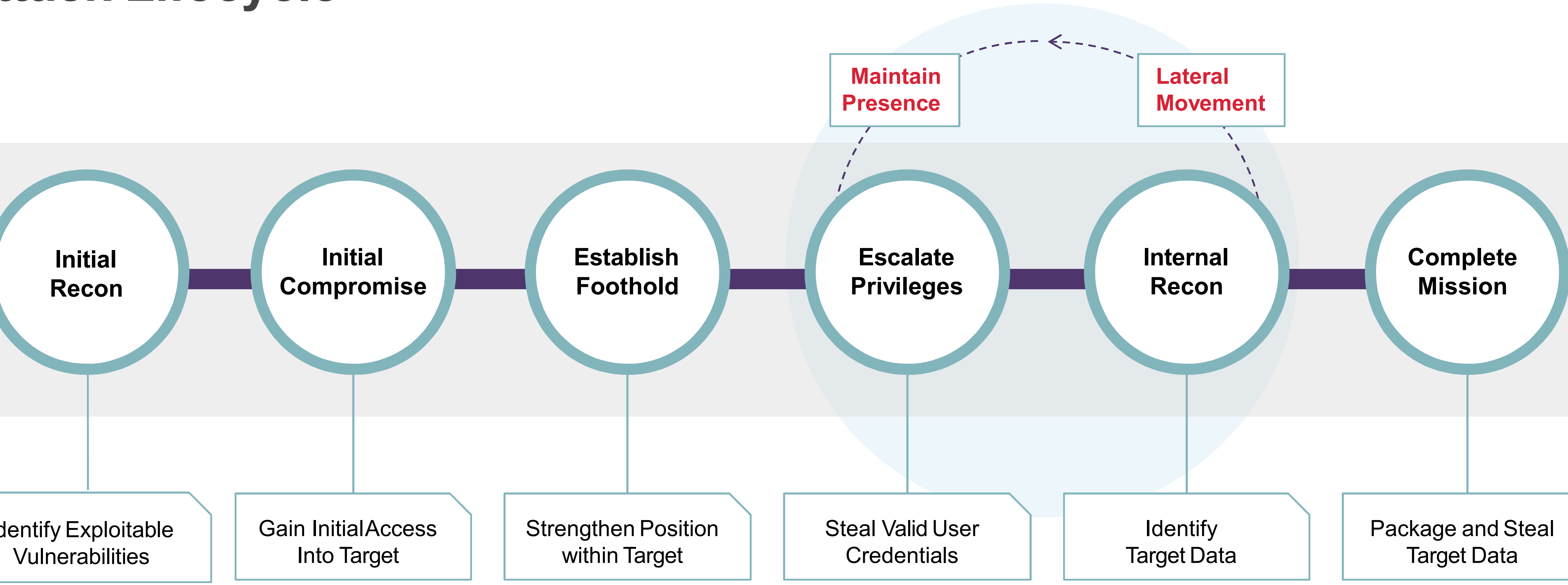
APT28: Cybercrime or State-sponsored Hacking?

POSTED IN GENERAL SECURITY, HACKING ON JUNE 4, 2015

Once upon the APT28

In October of 2014, the security firm FireEye published a report that revealed existence of a group of Russian hackers, dubbed APT28, which managed a l running cyber espionage campaign on US defense contractors, European se organizations and Eastern European government entities.

ttack Lifecycle



Maintain Presence

Lateral Movement

Initial Recon

Initial Compromise

Establish Foothold

Escalate Privileges

Internal Recon

Complete Mission

dentify Exploitable Vulnerabilities

Gain Initial Access Into Target

Strengthen Position within Target

Steal Valid User Credentials

Identify Target Data

Package and Steal Target Data

/hat is your security posture ?

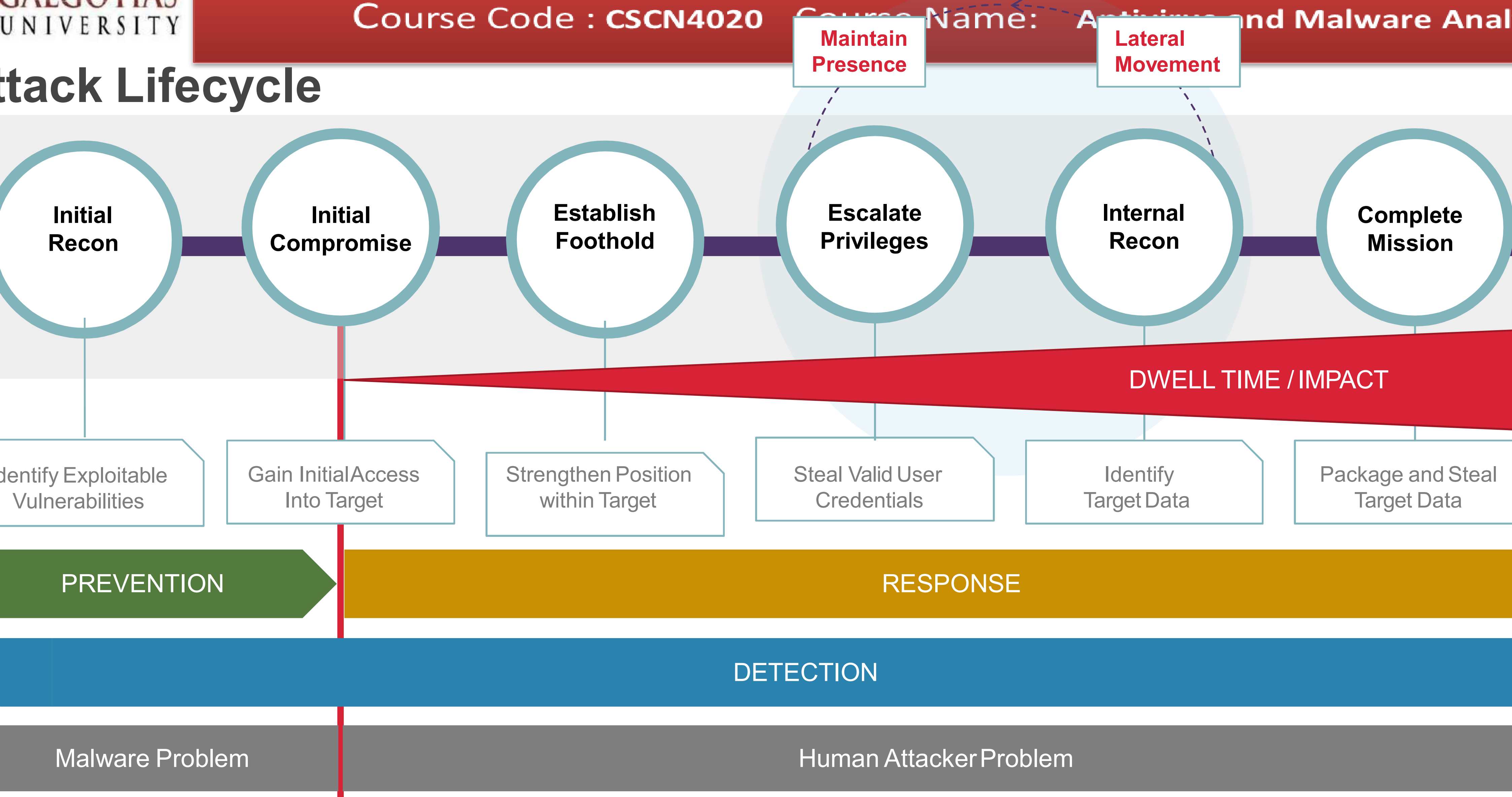
Breach Prevention

Breach Resilience

What are you doing to ANALYZE and RESPOND to threats when your PREVENTION fails?

MOVING FROM PURE PREVENTION TO BREACH RESILIENCE

ttack Lifecycle



Maintain Presence

Lateral Movement

Initial Recon — dentify Exploitable Vulnerabilities

Initial Compromise — Gain Initial Access Into Target

Establish Foothold — Strengthen Position within Target

Escalate Privileges — Steal Valid User Credentials

Internal Recon — Identify Target Data

Complete Mission — Package and Steal Target Data

DWELL TIME / IMPACT

PREVENTION

RESPONSE

DETECTION

Malware Problem

Human Attacker Problem

FireEye Supports Incident Response Workflow (IRW)

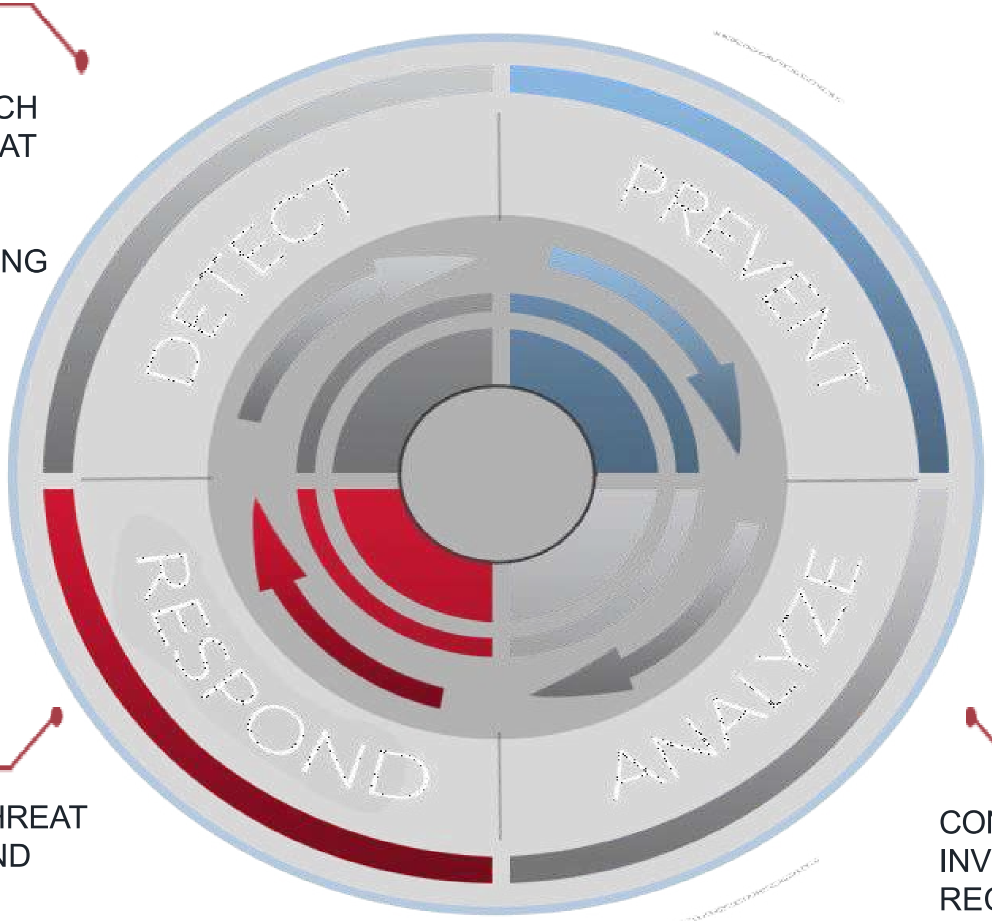
DETECT

SIGNATURE-LESS AND MULTI FLOW VIRTUAL MACHINE BASEDAPPROACH THAT LEVERAGES SUPERIOR THREAT INTELLIGENCE

TRIGER WHICH INITIATES FOLLOWING IRW STEPS

PREVENT

MULTI-VECTOR INLINE KNOWN AND UNKNOWN THREAT PREVENTION



RESPOND

REMEDIATION SUPPORT AND THREAT INTELLIGENCE TO RECOVER AND IMPROVE RISK POSTURE

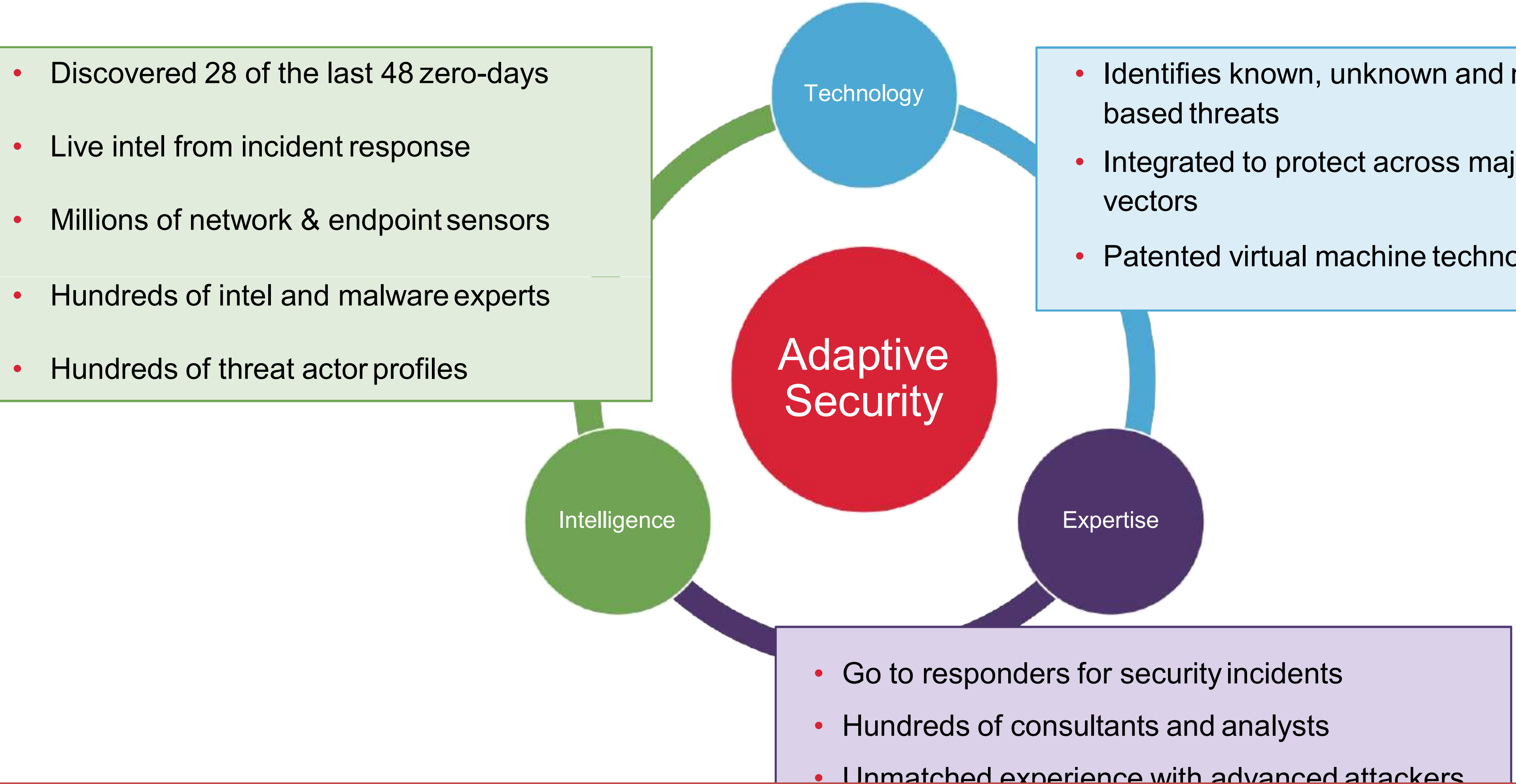
ANALYZE

CONTAINMENT, FORENSICS INVESTIGATION AND KILL CHAIN RECONSTRUCTION

DAYS/MONTHS → MINUTES

reEye platform: INTELLIGENCE-LED SECURITY

rovide ADAPTIVE solution to protect customers' most valuable assets



- Discovered 28 of the last 48 zero-days
- Live intel from incident response
- Millions of network & endpoint sensors
- Hundreds of intel and malware experts
- Hundreds of threat actor profiles

Technology

- Identifies known, unknown and non-malware based threats
- Integrated to protect across major attack vectors
- Patented virtual machine technology

Adaptive Security

Intelligence

Expertise

- Go to responders for security incidents
- Hundreds of consultants and analysts
- Unmatched experience with advanced attackers

reEye Platform – products and services

On-premise: Network

- CM – central management
- NX – network protection
- EX – email protection
- FX – file shares/SharePoint analysis
- AX – on-demand analysis
- PX/IA – network forensic (packet capturing)
- SSLi – HW SSL decryptor

On-premise: Endpoint

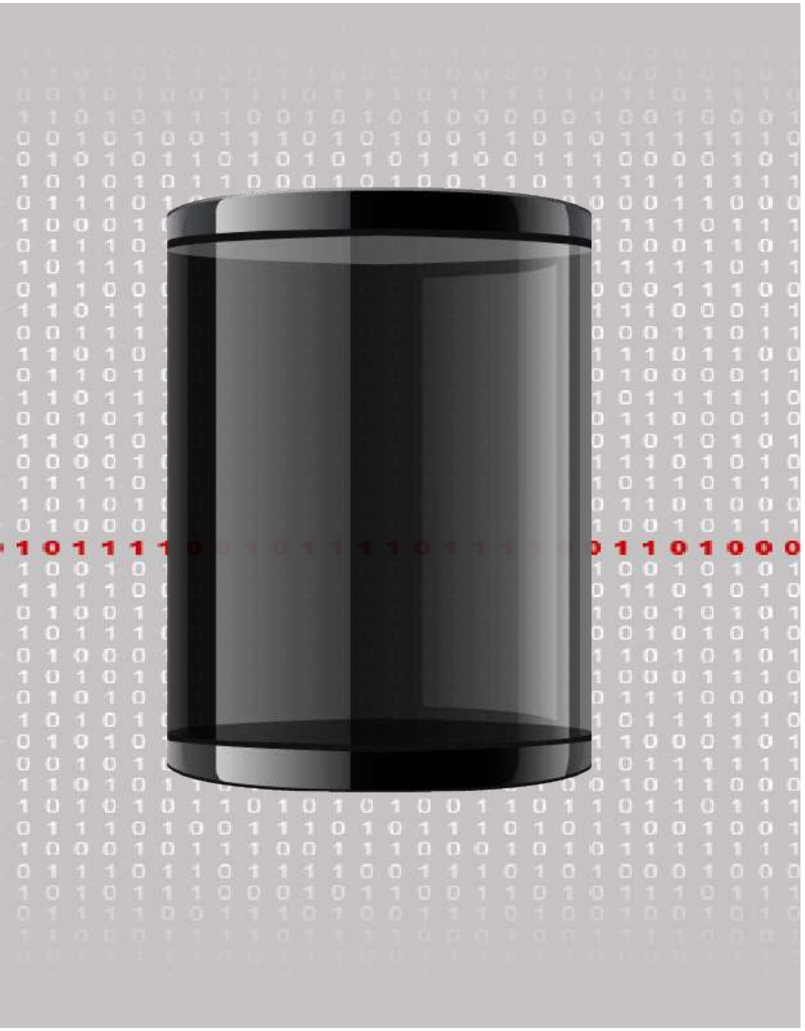
- HX – endpoint security (exploit detection, incident validation and analysis)
- MTA Agent – mobile protection (Android and iOS, MDM integration)

Cloud

- ETP – anti-spam + AV + "EX in the cloud"
- MTP Analysis – dynamic analysis of mobile apps
- TAP – cloud based "SIEM"

Services

- FaaS – FireEye as a Servic monitoring, alerting, huntin
- Mandiant Services
- iSight – access to Intelligen resources

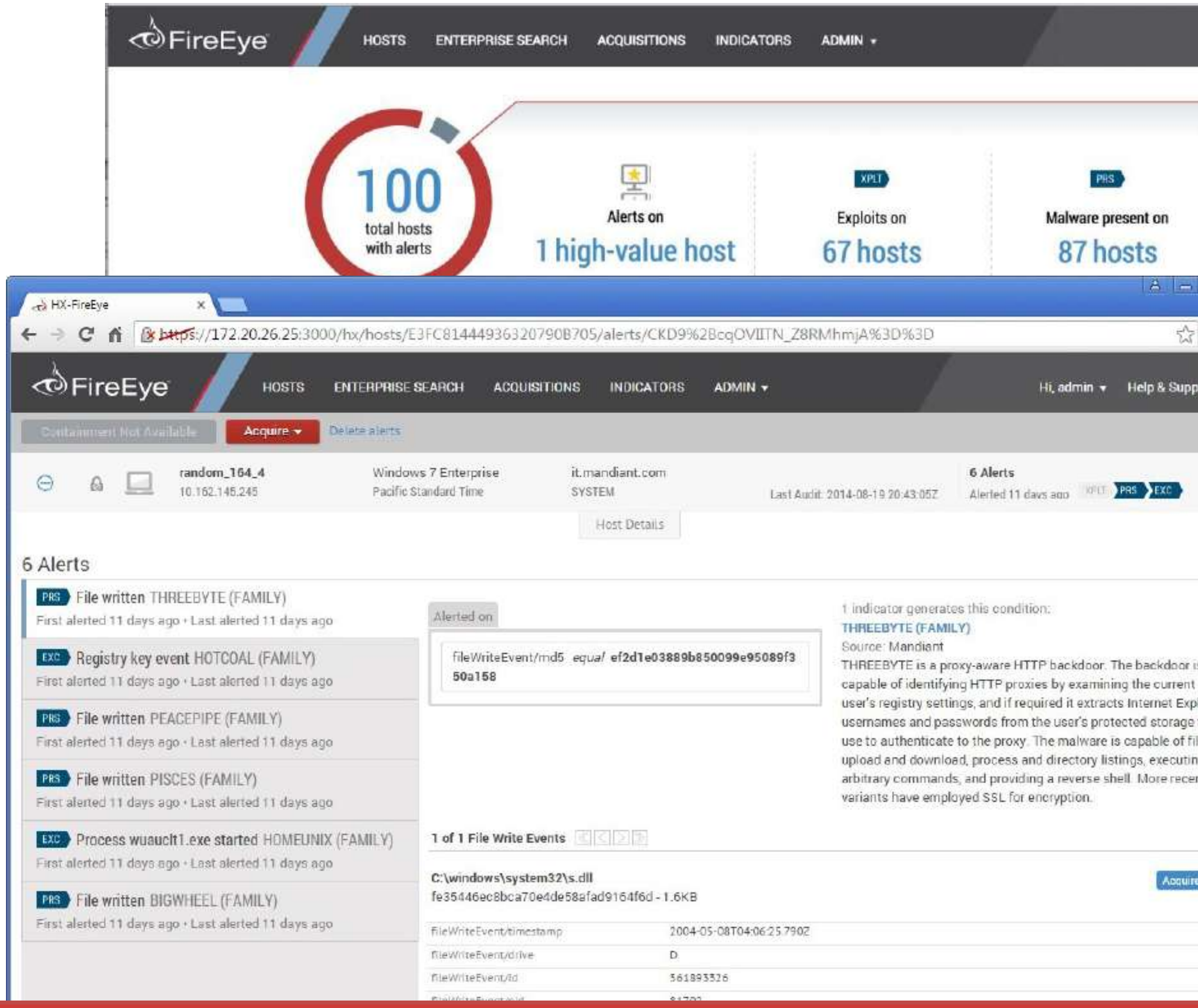


FireEye Multi-Vector Virtual Execution (MVX) Technology

- BASE OF ALL NETWORK DETECTION APPLIANCES
- PURPOSE-BUILT FOR SECURITY
- HARDENED HYPERVISOR
- SIGNATURE-LESS
- EXPLOIT-BASED DETECTION, NOT JUST FILES
- MULTI-VECTOR
- MULTI-PLATFORM, INCLUDING MAC OSX
- IMMEDIATE RULE CREATION AND ENFORCEMENT
- SCALABLE
- EFFICIENT

eEye Endpoint HX – Protection and Investigation Tool

- alidate compromised endpoints using reEye alerts
- each endpoints regardless of location
- ro-active detection and prevention of threat n every endpoint (generic *exploit detection*)
- uickly investigate all endpoints for IOC, or onduct robust search of all endpoints for otential threats.
- /hen compromised endpoints are found ontain them with a single click workflow
- ata acquisitions to continue analysis of the tack TTPs (tools, technics, procedures)
- eamless integration with SIEM



100 total hosts with alerts

Alerts on 1 high-value host

Exploits on 67 hosts

Malware present on 87 hosts

https://172.20.26.25:3000/hx/hosts/E3FC81444936320790B705/alerts/CKD9%2BcqOVIITN_Z8RMhmjA%3D%3D

random_164_4
10.162.145.245

Windows 7 Enterprise
Pacific Standard Time

it.mandiant.com
SYSTEM

Last Audit: 2014-08-19 20:43:05Z

6 Alerts
Alerted 11 days ago

6 Alerts

- PRS File written THREEBYTE (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago
- EXC Registry key event HOTCOAL (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago
- PRS File written PEACEPIPE (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago
- PRS File written PISCES (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago
- EXC Process wuauclt1.exe started HOMEUNIX (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago
- PRS File written BIGWHEEL (FAMILY)
  First alerted 11 days ago • Last alerted 11 days ago

fileWriteEvent/md5 *equal* **ef2d1e03889b850099e95089f350a158**

1 indicator generates this condition:
THREEBYTE (FAMILY)
Source: Mandiant
THREEBYTE is a proxy-aware HTTP backdoor. The backdoor i capable of identifying HTTP proxies by examining the current user's registry settings, and if required it extracts Internet Exp usernames and passwords from the user's protected storage use to authenticate to the proxy. The malware is capable of fi upload and download, process and directory listings, executin arbitrary commands, and providing a reverse shell. More recer variants have employed SSL for encryption.

1 of 1 File Write Events

C:\windows\system32\s.dll
fe35446ec8bca70e4de58afad9164f6d - 1.6KB

fileWriteEvent/timestamp	2004-05-08T04:06:25.790Z
fileWriteEvent/drive	D
fileWriteEvent/id	561893326

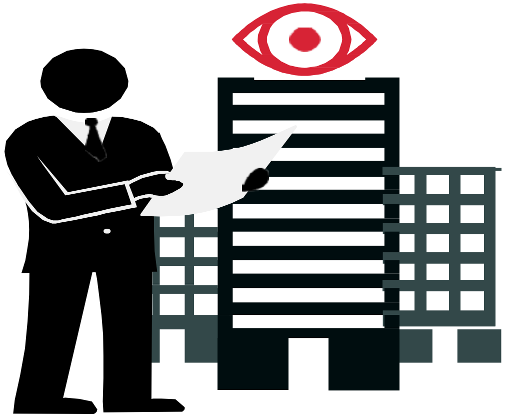
NOT SO FAR AGO…

Case Study

CUSTOMER - A

Signature based **TECHNOLOGY**
n-house **EXPERTISE**
No malware/threat actor **INTELLIGENCE**

CUSTOMER - B



FireEye **TECHNOLOGY**
FireEye **EXPERTISE**
FireEye **INTELLIGENCE**

Traditional in-house approach

CUSTOMER - A

TECHNOLOGY
AntiSpam and AV Filtering

Receives 50 thousands emails a day

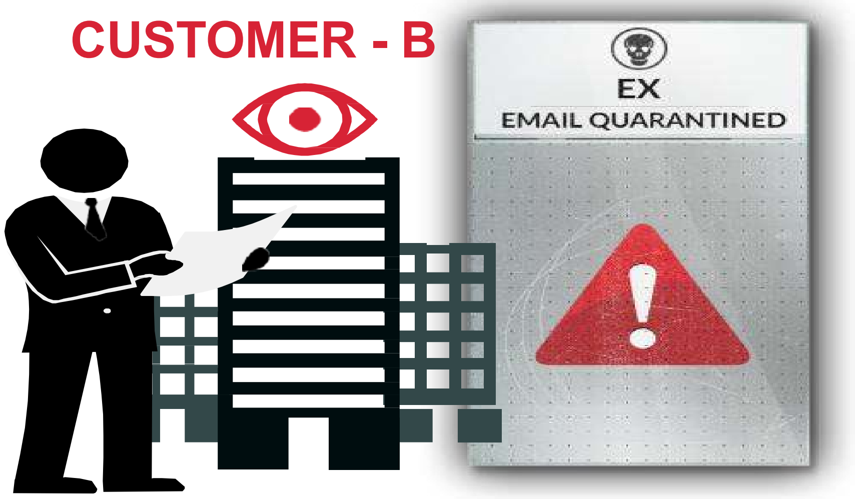
- AV updates slow
- Sometimes AV will only catch malware AFTER infection

When this happens

- Machine is reimaged
- Possibly send malware sample to their AV vendor

ssumption of the Breach

CUSTOMER - B



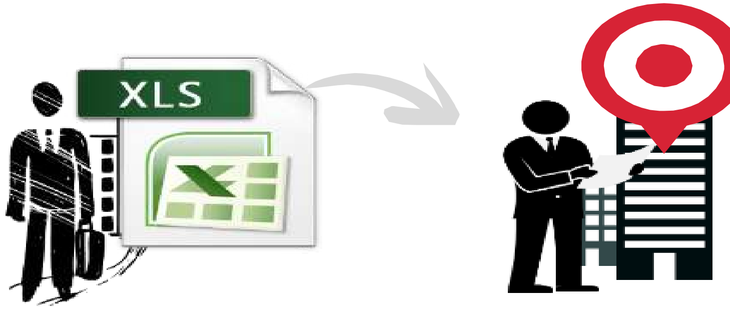
- FireEye **TECHNOLOGY** is not Signature based – and finds threats designed to bypass signatures – reducing time to detect
- FireEye EX finds the unknown threat "**Invoice.xls**" delivered by targeted email

TECHNOLOGY

1. AntiSpam and AV Filtering
2. **Malware Detonation – FireEye EX**

Receives 50 thousands emails a day

Unknown Threat: Invoice.xls



arget: CUSTOMER - B, and trying to appear legitimate

No signature

By passed existing defenses

reEye EX reveals:

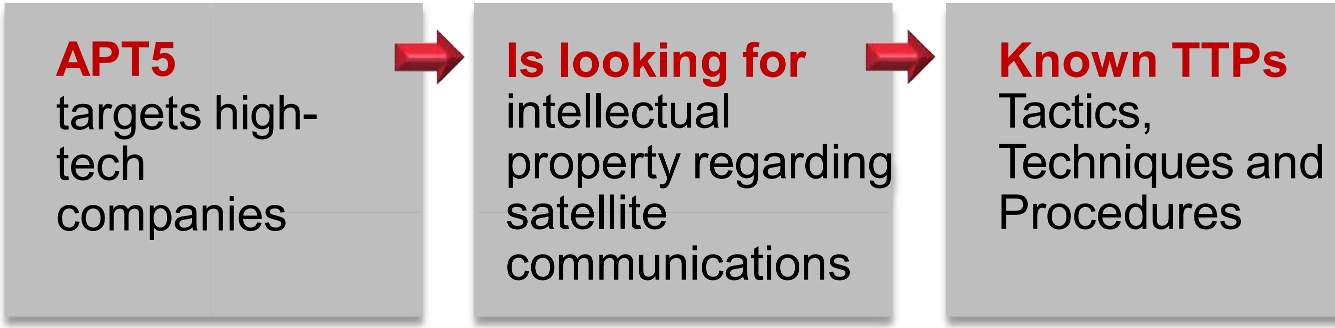
1. Invoice.xls designed to attack Excel 2013
2. Excel 2013 is the version CUSTOMER B has standardized on
3. Malware phones home to ServiceABC.skypetw.com
4. ServiceABC is the name of a VALID internal service in the CUSTOMER B network

Do you want to know more now that you have context and detail?

Who is attacking?

reEye **INTELLIGENCE** tells us:

Skypetw.com matches to known threat group: APT5



APT5 targets high-tech companies

Is looking for intellectual property regarding satellite communications

Known TTPs Tactics, Techniques and Procedures

FireEye Intel accessible directly by Customer through FireE Intelligence Center Portal or used by FireEye as a Service Te

APT5 - Tools Techniques and Procedures (TTPs)

1 Establish a Beachhead using malware

2 Move laterally using standard networking tools (no malware)

3 Find desired intellectual property

4 Exfiltrate stolen data using password protected zip files and FTP

Incident Scope

- APT 5 is behind the attack
- Looking for Satellite IP
- CUSTOMER B has Satellite Communication IP
- Alarm bells going off from this single alert

e need to find out

Did end user open email attachment?

Did other users get infected?

Did the attacker move laterally once inside the network?

FireEye HX Endpoint Agent Technology

ETECTS – INVESTIGATES – CONTAINS

n check endpoints both on and off the network

r Goal

tect and respond in the Network and on Endpoints

Validation on the Endpoint

Fully automated

IN UNDER **10 Minutes** NOT the **146 days** industry average

Detect and Respond

HX Agent

- Validates a Desktop on internal network is infected
- Validates a Laptop in home office is also infected

CUSTOMER B opts to 'stop the bleeding' and contain both machines

Escalate to a second level investigation

FireEye provides the **Endpoint Forensics** necessary for understanding the attack kill chain

Detect and Respond Process continues

Complete Host Based investigation, e.g. : Scraping Endpoint Memory

Reveal commands an attacker may have used on an endpoint

Look for APT5 TTP – Lateral movement using standard networking tools

Look for APT5 TTP – Exfiltration of password protected zip file

nvestigation using **FireEye HX** tells us

- “NETUSE” command was used to connect to 2 additional servers at CUSTOMER B
- Servers required Username and password - “BobAdmin” account was used by the attacker. This account is a Domain Admin at CUSTOMER B
- Our remediation now extends to this compromised admin account
- HX Agent tells us 7z (zip) command was used with a “password” option
- HX Agent tells us the password that was used to encrypt the file: *itsm9now*

Incident Scope

Scope of the attack

- Desktop
- Laptop
- 2 Servers
- Compromised Admin Account “BobAdmin”

What we need to know

- What was in those exfiltrated .zip files?
- Did they actually make it out?
- What is the business impact?

Network Forensics – FireEye PX/IA

FireEye **PX/IA** lets you “look back in time” on the network

Like Airplane black box

Store at high speed

Search at high speed

Every Email, Every web page, every network packet

Narrow search:

- 4 affected computers at CUSTOMER B
- FTP, exfiltration Protocol
- Destination “skypetw.com”

etwork Forensics – FireEye PX/IA

ireEye **PX/IA**

. Goes back in time and shows us the actual zip file “exfil.zip” that was sent to serviceABC.skypetw.com

. Lets us extract “exfil.zip” and save it to our computer…

. But it’s password protected
  - We use the password that we learned from endpoint forensic investigation
  - See what data was exfiltrated: new, secret satellite technology project…

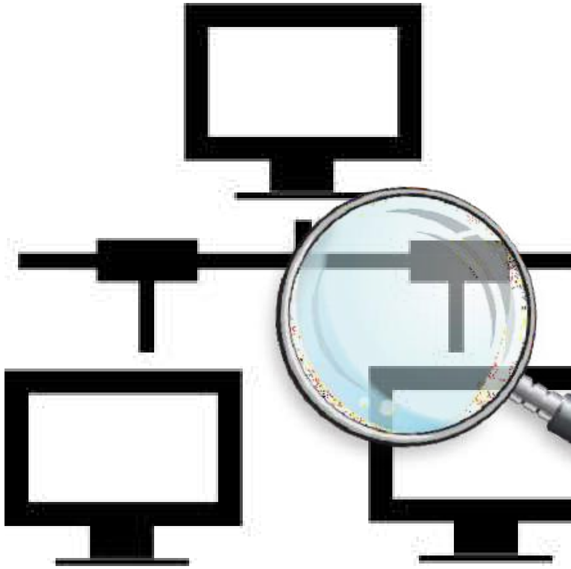
FireEye **PX/IA** provides the Network Forensics necessary for understanding the full attack

ummary

What would have happened if CUSTOMER B based their security model on "Pure Prevention" and did not have an "Assumption of the Breach" and performed a traditional in house response?

How long would it have taken before a signature arrived that caught the attack?

If their response was just to re-image the infected machine would it have helped? At all?



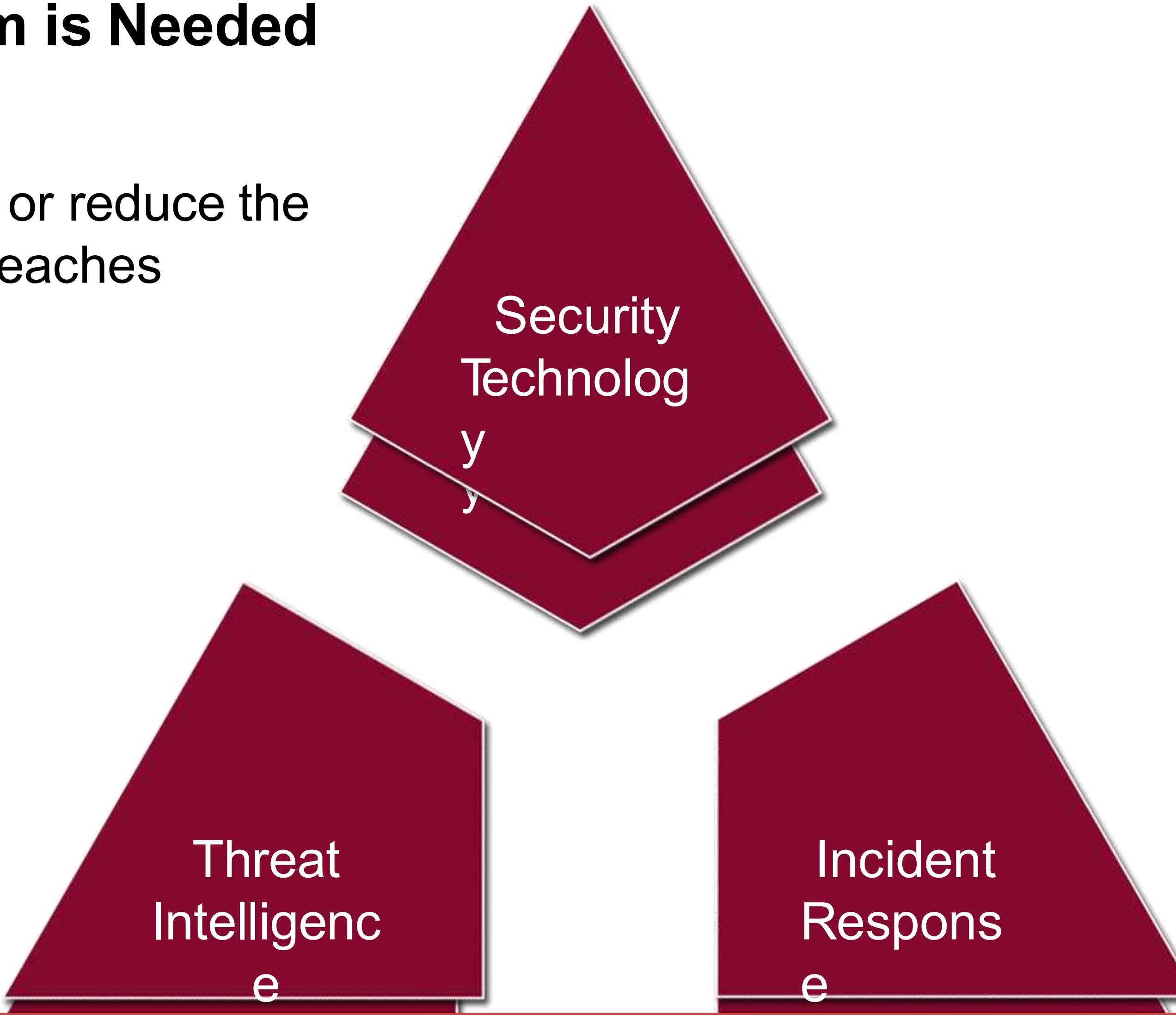
FireEye Platform supports Incident Response Workflow

- Minutes from detection to response vs days or months of professional services

nclusion - New Security Paradigm is Needed

Organizations need to seek to eliminate or reduce the consequences and impact of security breaches

- Ability to operate through compromise
- Holistic visibility (network & endpoint)
- Actionable threat intelligence
- Shift to threat centric security



Security Technolog y

Threat Intelligenc e

Incident Respons e