# Threats in Connected World

Bhavin Gandhi
Sr. Technical Consultant – Trend Micro India

# What was War - Earlier

Country A against Country B

- India - Pakistan
- US - Iraq
- Nato - Germany
- World War 1, 2... etc

That’s What War..... Was

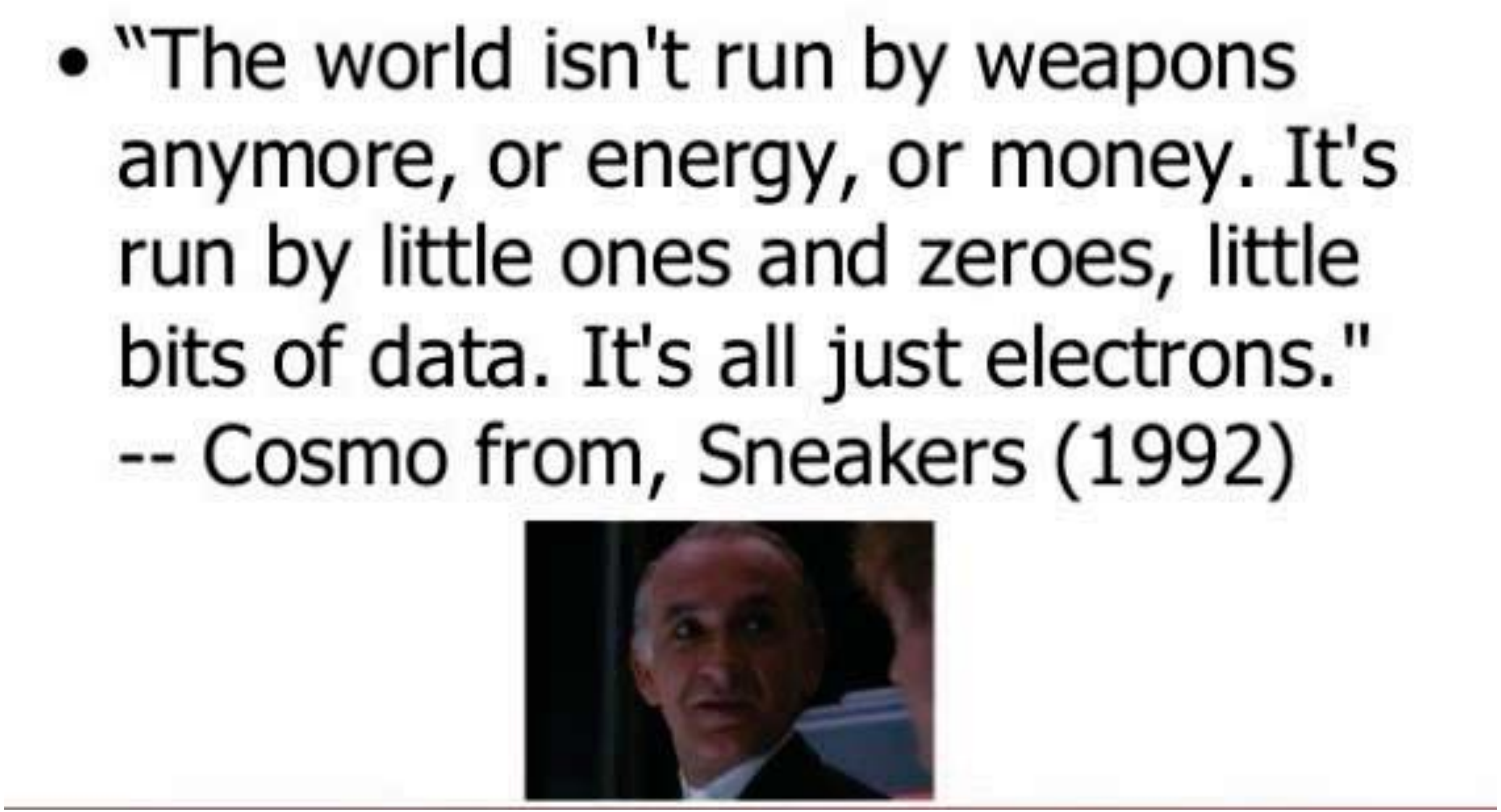
Dirty & Bloody with lots of noise, mayhem and blackouts

# But Now….

Time has changed and the definition as well

- No visible damage to Life & Property
- No Fires and Noise
- No supply chain management
- No Troops and Ammunitions
- Definition of heroes has changed since 9/11

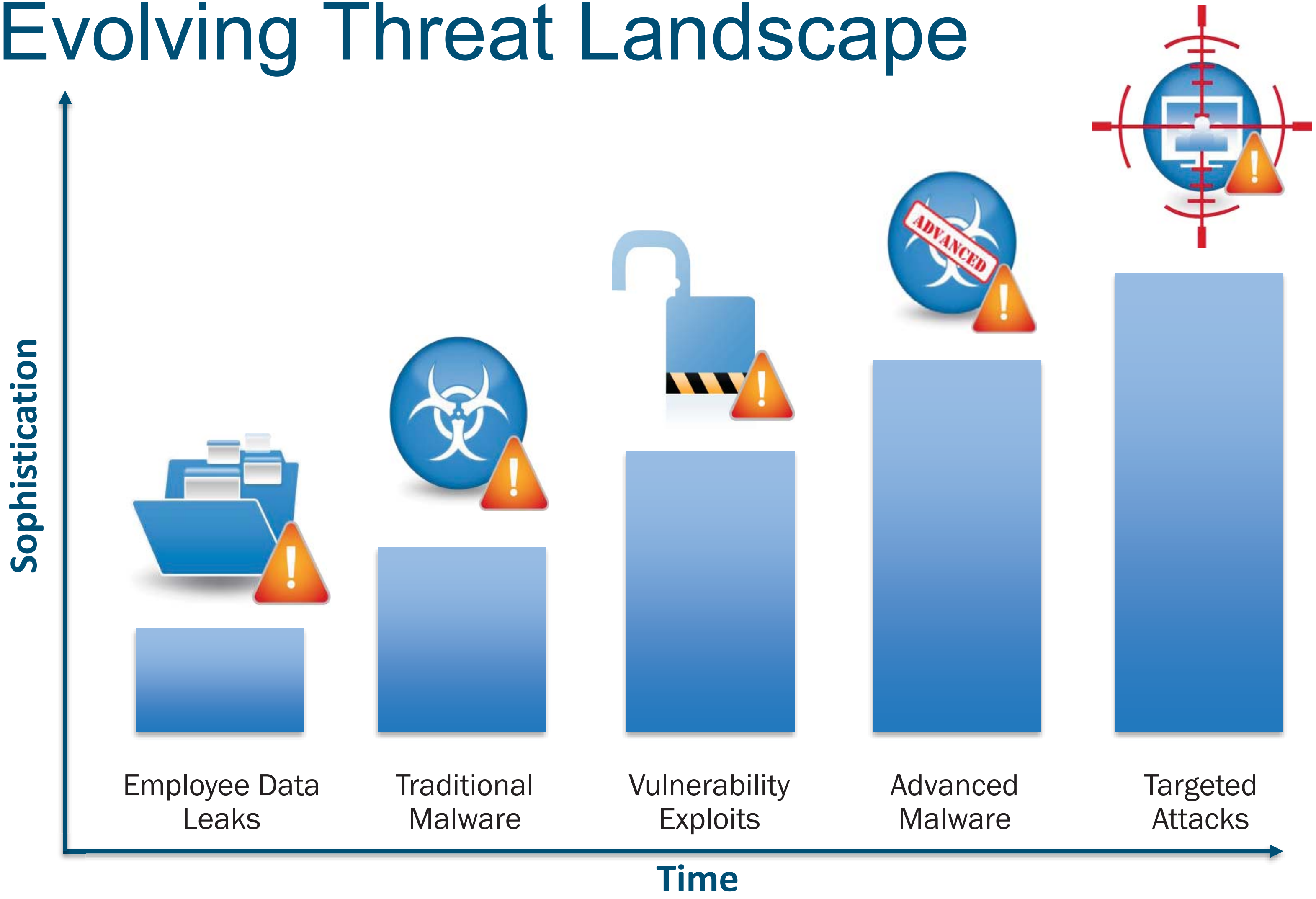
# It’s all about Little Ones and Zeroes



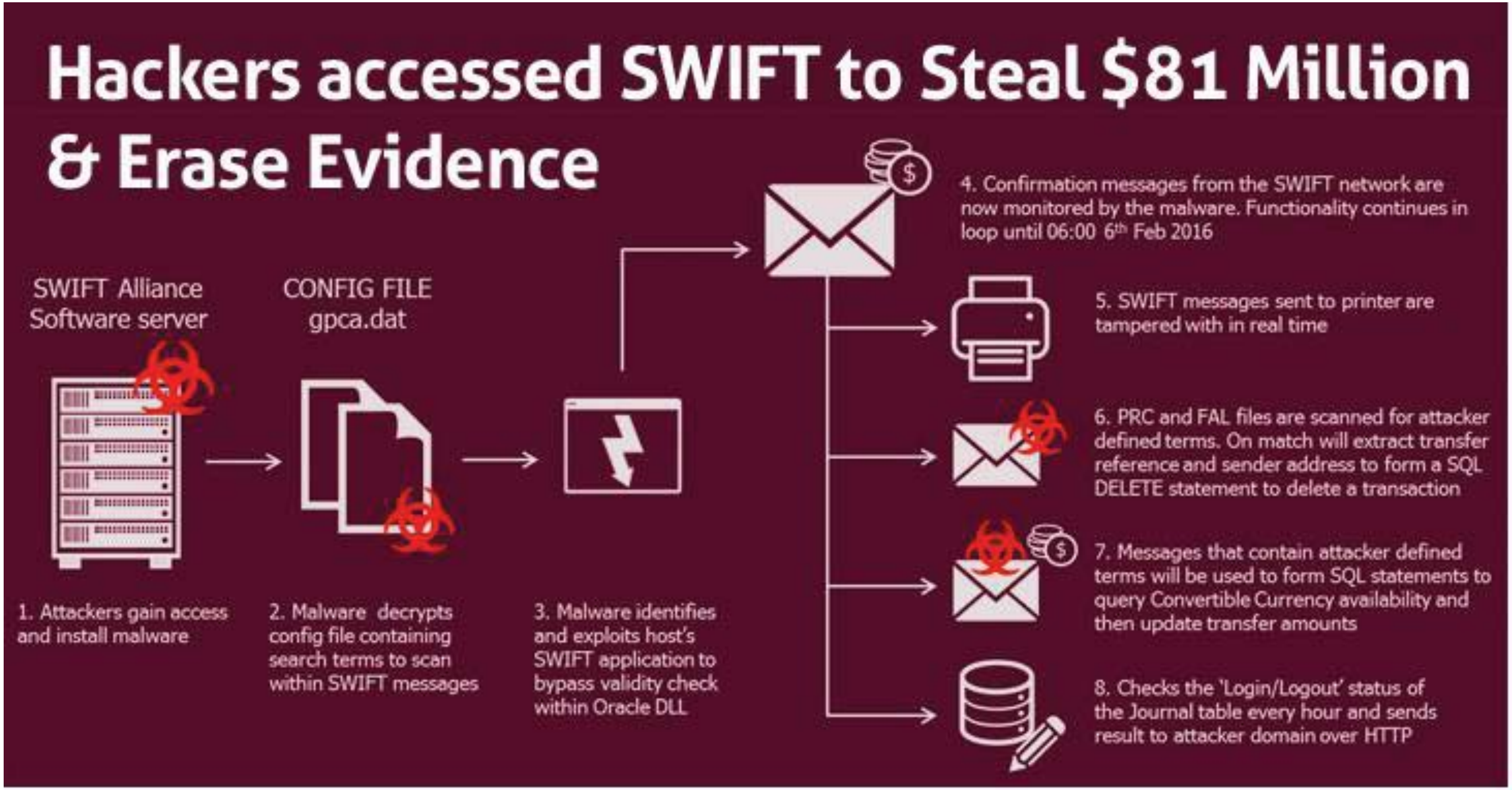
- "The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons." -- Cosmo from, Sneakers (1992)

# Advanced Persistent Threat (APT)

# Evolving Threat Landscape



# Hackers Stole $81M from Bangladesh Bank



## Hackers accessed SWIFT to Steal $81 Million & Erase Evidence

1. Attackers gain access and install malware

2. Malware decrypts config file containing search terms to scan within SWIFT messages

3. Malware identifies and exploits host's SWIFT application to bypass validity check within Oracle DLL

4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016

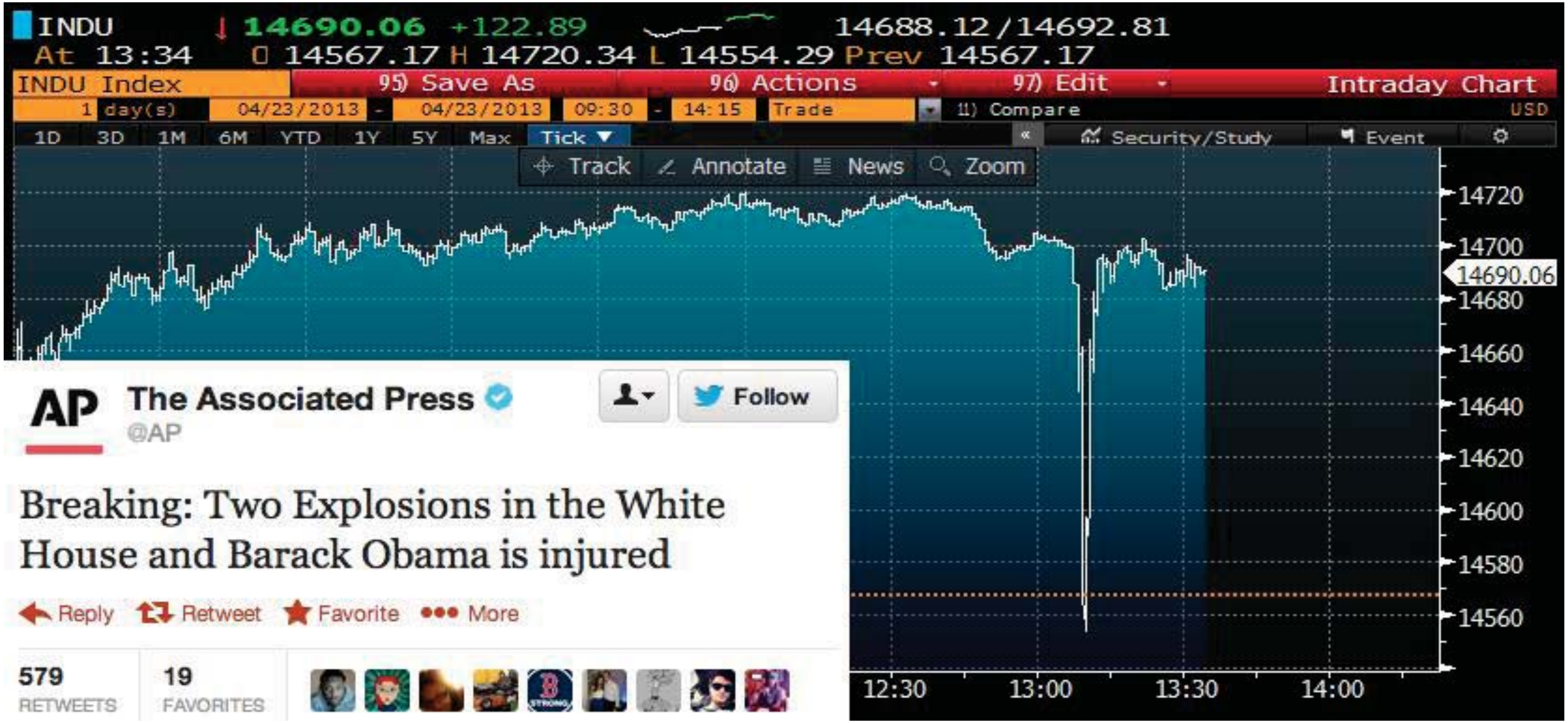
5. SWIFT messages sent to printer are tampered with in real time

6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction

7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts

8. Checks the 'Login/Logout' status of the Journal table every hour and sends result to attacker domain over HTTP

# Social Media Accounts



AP

**The Associated Press**

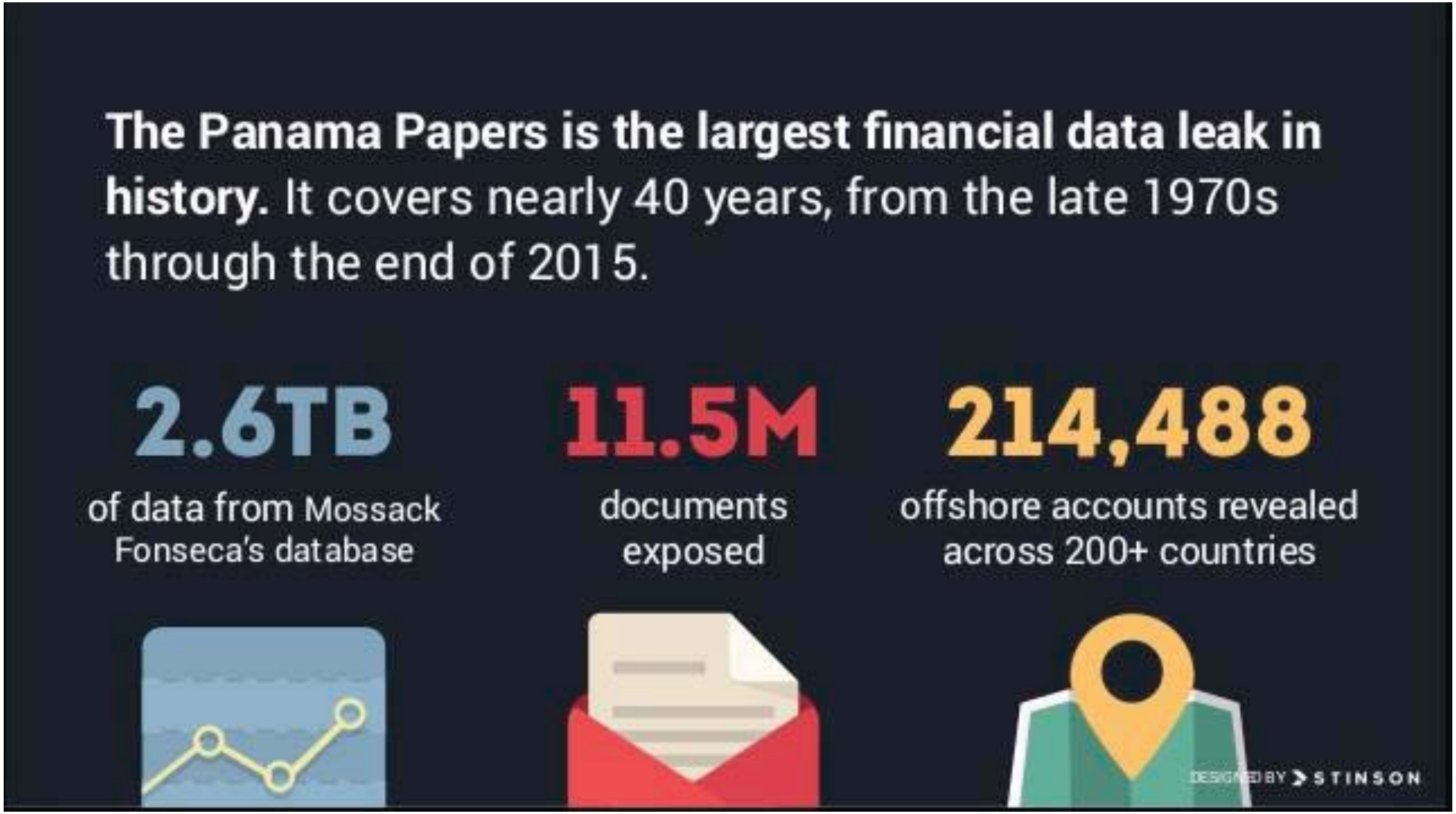
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

579 RETWEETS

19 FAVORITES

# Panama Papers Leak



**The Panama Papers is the largest financial data leak in history.** It covers nearly 40 years, from the late 1970s through the end of 2015.

**2.6TB** of data from Mossack Fonseca's database

**11.5M** documents exposed

**214,488** offshore accounts revealed across 200+ countries

DESIGNED BY STINSON

# We see the TIP of the APT ICEBERG

Attacks in the News

RSA The Security Division of EMC

Google

SONY make.believe

LOCKHEED MARTIN

HONDA The Power of Dreams

Adobe

ADP

citi

epsilon Marketing As Usual. Not A Chance.™

Most go unreported. 90% of companies found previously unknown Malware*

APTs
Cyber Espionage
Targeted Attacks
Cyber Threats

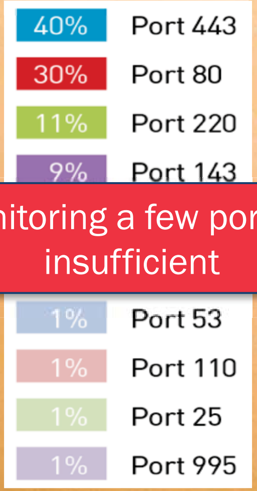
* Trend Micro Study

# Networks are becoming Cyber Swiss Cheese

Employees are often exploited

91% of targeted attacks begin with a spear-phishing email

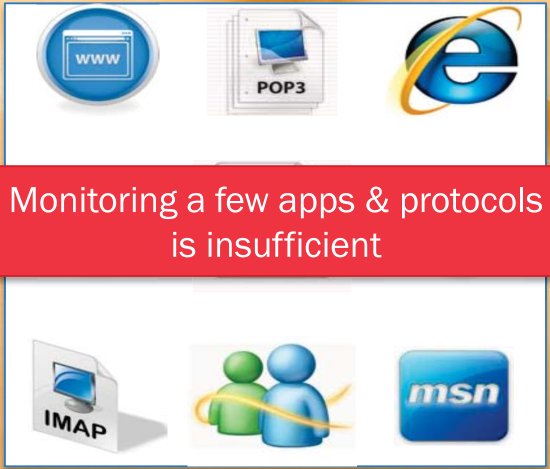
### Poison Ivy



| | |
|---|---|
| 40% | Port 443 |
| 30% | Port 80 |
| 11% | Port 220 |
| 9% | Port 143 |
| 1% | Port 53 |
| 1% | Port 110 |
| 1% | Port 25 |
| 1% | Port 995 |

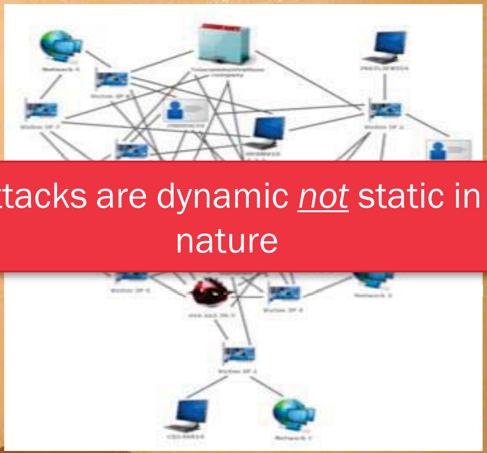
Monitoring a few ports is insufficient

### EvilGrab



Monitoring a few apps & protocols is insufficient

### IXESHE



Attacks are dynamic *not* static in nature

# Your adversaries have the advantage

**ADVERSARY**

Resources & expertise for hire

Target rich guerilla offense

Ease of execution

Focused objectives

**ENTERPRISE**

Resource & expertise constraints

Broad static defense

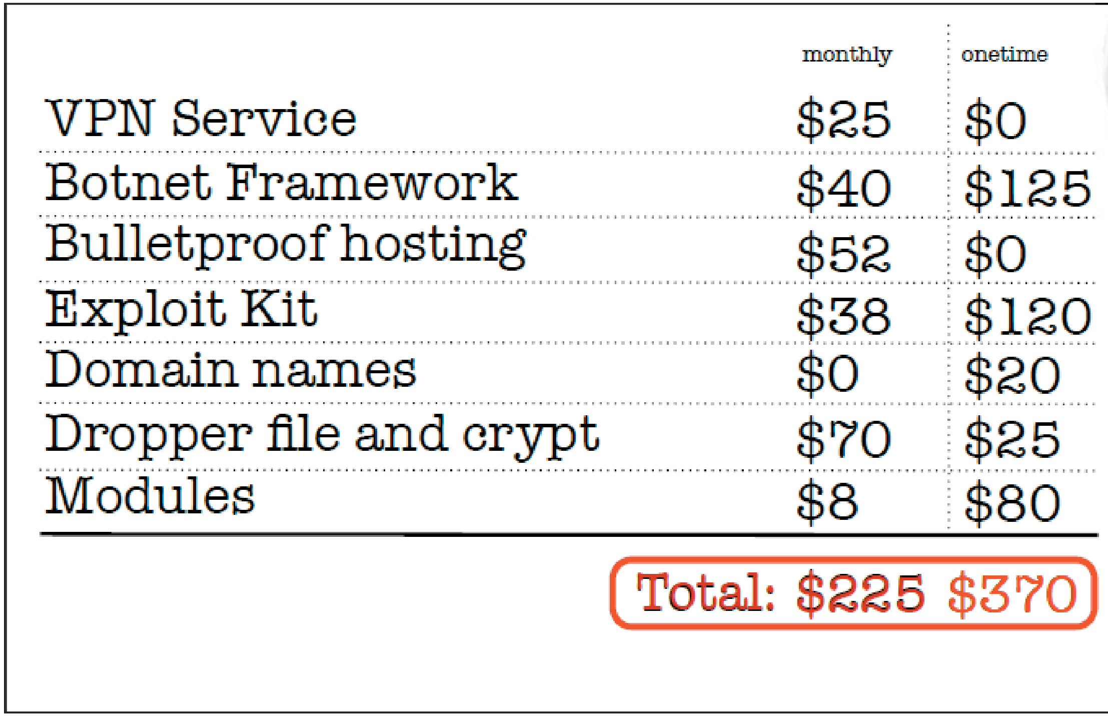
Detection complexity

Low signal to noise ratio

- **75%** of attacks require little skill to execute[1]……yet require advanced skills to detect and remediate
- **63%** of security professionals believe it is only a matter of time until their enterprise is targeted[2]
- **$5.9M** is average cost of targeted attack[3]

# Hackers Have an Unfair Advantage!

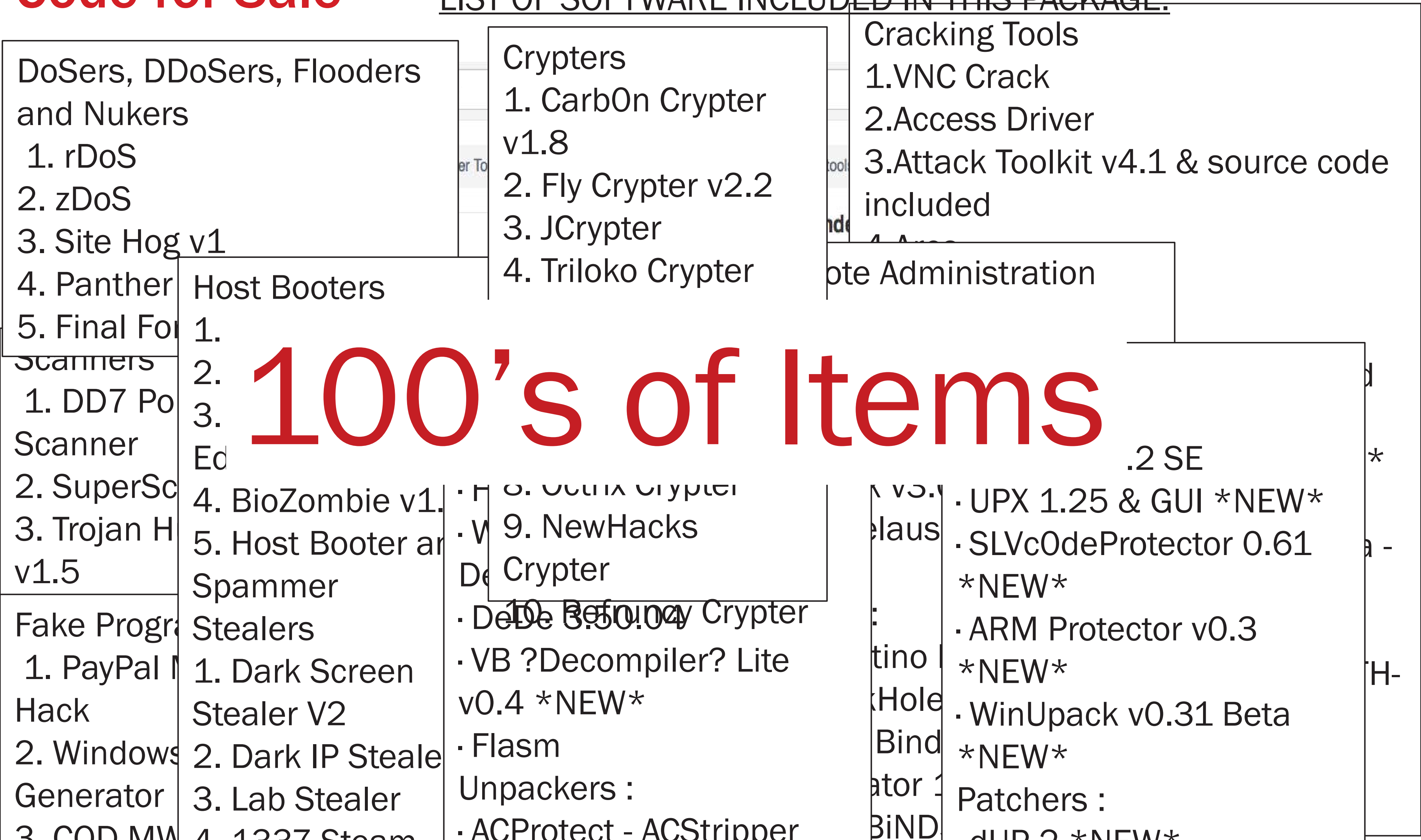
- All that's needed is a credit card and a mouse!



| | monthly | onetime |
|---|---|---|
| VPN Service | $25 | $0 |
| Botnet Framework | $40 | $125 |
| Bulletproof hosting | $52 | $0 |
| Exploit Kit | $38 | $120 |
| Domain names | $0 | $20 |
| Dropper file and crypt | $70 | $25 |
| Modules | $8 | $80 |
| Total: | $225 | $370 |

# Code for Sale

LIST OF SOFTWARE INCLUDED IN THIS PACKAGE:



DoSers, DDoSers, Flooders and Nukers
1. rDoS
2. zDoS
3. Site Hog v1
4. Panther
5. Final For

Scanners
1. DD7 Po
Scanner
2. SuperSc
3. Trojan H
v1.5

Fake Progra
1. PayPal M
Hack
2. Windows
Generator
3. COD MW

Host Booters
1.
2.
3.
Ed
4. BioZombie v1.
5. Host Booter ar
Spammer
Stealers
1. Dark Screen Stealer V2
2. Dark IP Steale
3. Lab Stealer
4. 1337 Steam

Crypters
1. Carb0n Crypter v1.8
2. Fly Crypter v2.2
3. JCrypter
4. Triloko Crypter
8. Octrix Crypter
9. NewHacks Crypter
10. Refuncy Crypter

· H
· W
De
· DeDe 3.50.04
· VB ?Decompiler? Lite v0.4 *NEW*
· Flasm
Unpackers :
· ACProtect - ACStripper

Cracking Tools
1.VNC Crack
2.Access Driver
3.Attack Toolkit v4.1 & source code included
4.Ares

ote Administration

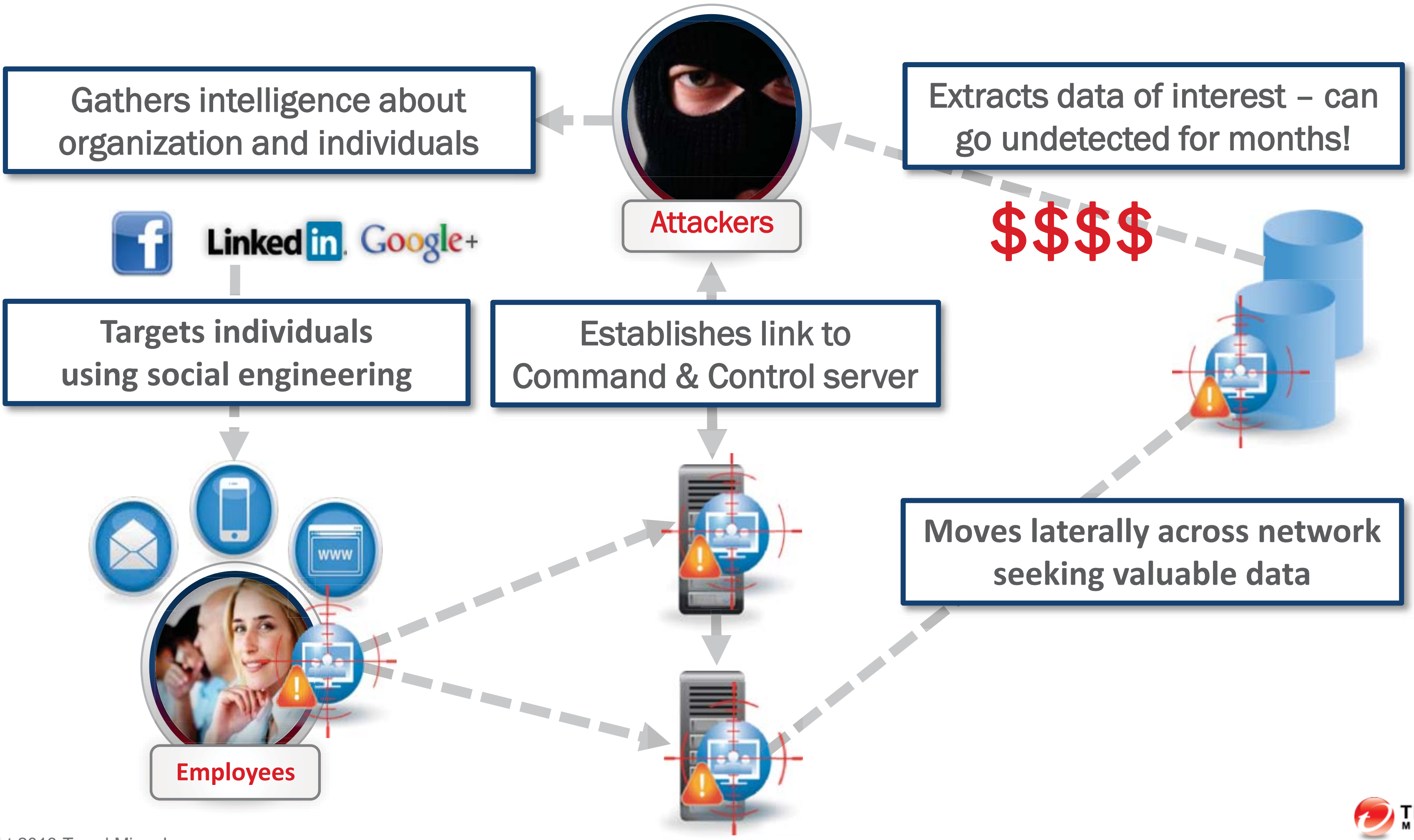
k v3.(
elaus
:
tino
kHole
Bind
ator 1
BiND

.2 SE
· UPX 1.25 & GUI *NEW*
· SLVc0deProtector 0.61 *NEW*
· ARM Protector v0.3 *NEW*
· WinUpack v0.31 Beta *NEW*
Patchers :
· dUP 2 *NEW*

d
*
a -
TH-

# 100's of Items

# A Targeted Attack in Action: Social, Stealthy



Gathers intelligence about organization and individuals

Extracts data of interest – can go undetected for months!

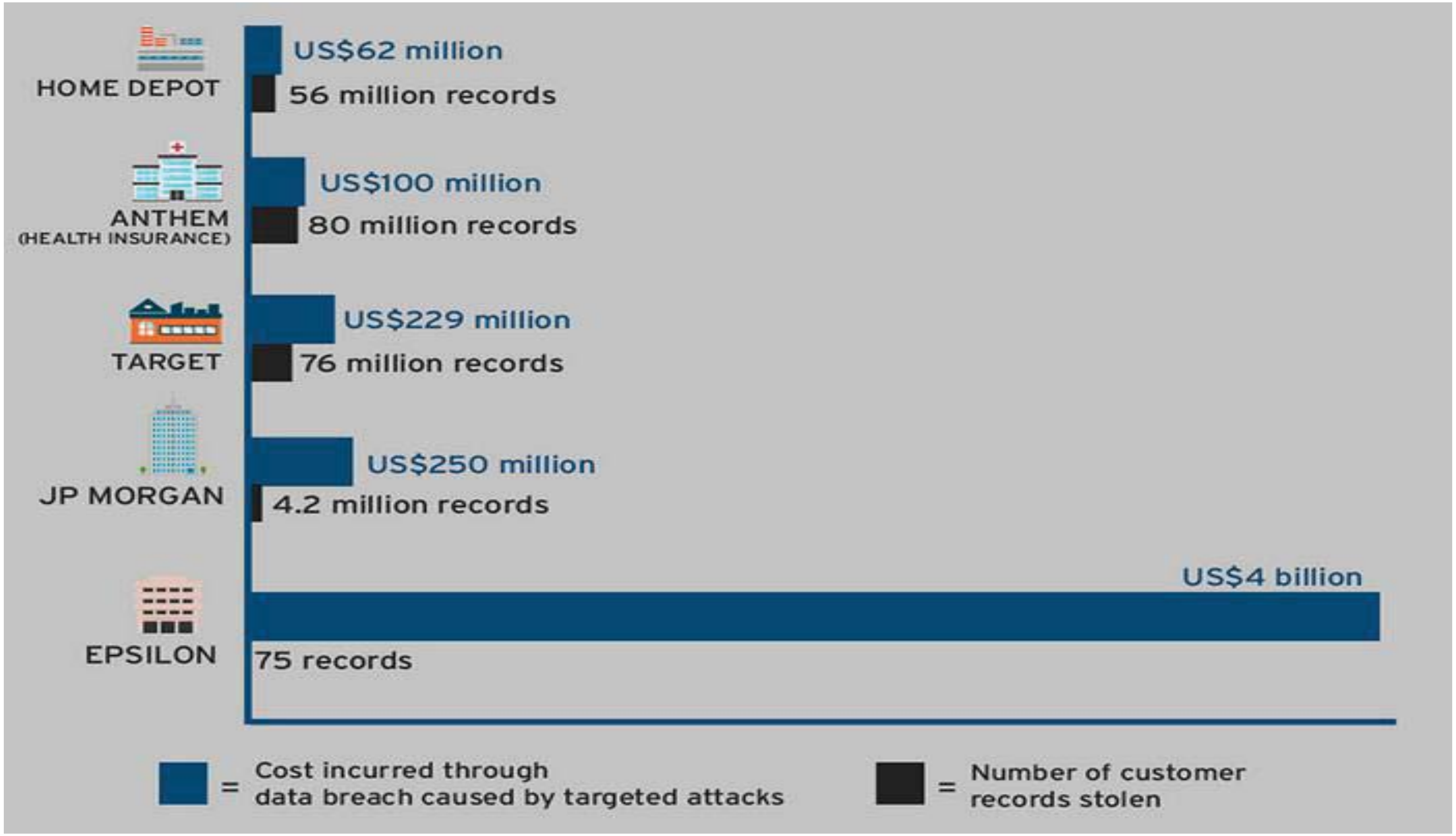
Targets individuals using social engineering

Establishes link to Command & Control server

Moves laterally across network seeking valuable data

# Large Spear-phishing Incidents

Most costly data breach incidents, all caused by spear-phishing:

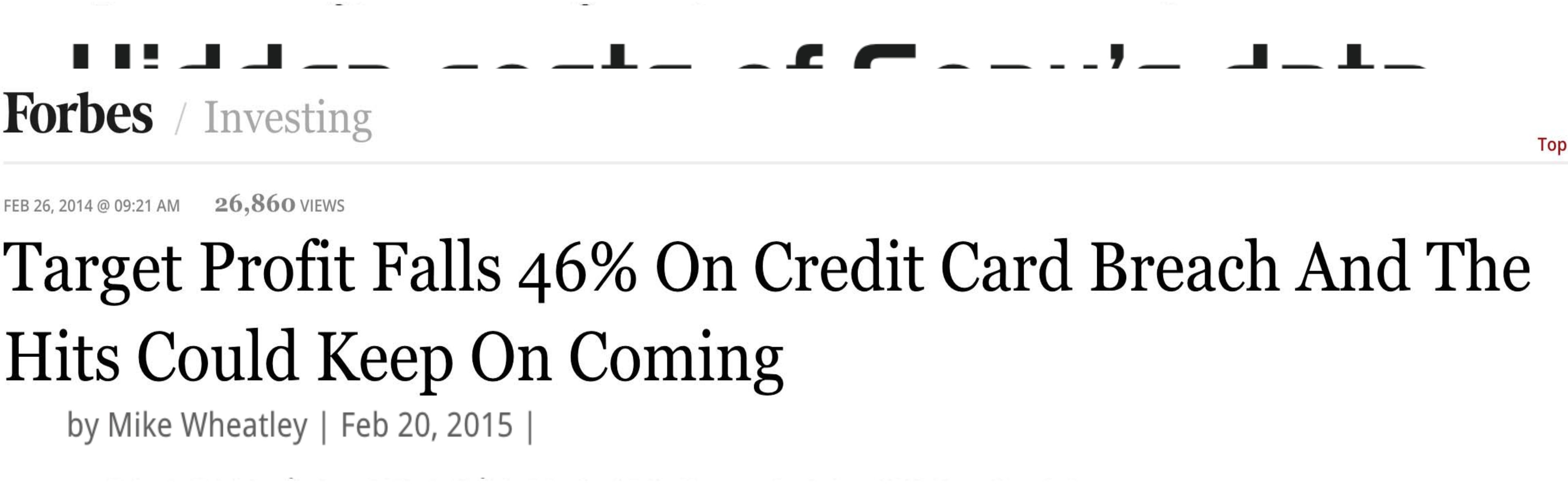


Source: Trend Labs

# Email: The dominant attack vector

- 91% of targeted attacks begin with a spear phishing attack
- The median time for the first user of to open a malicious spear phishing email is 1 minute, 40 seconds. Source
- It takes under a minute for an endpoint to be entirely encrypted by ransomware Source

# The Material Impacts of Targeted Attacks ….



Hidden costs of Sony's data

Forbes / Investing

Top

FEB 26, 2014 @ 09:21 AM 26,860 VIEWS

Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming

by Mike Wheatley | Feb 20, 2015 |

**Unexpected Costs**

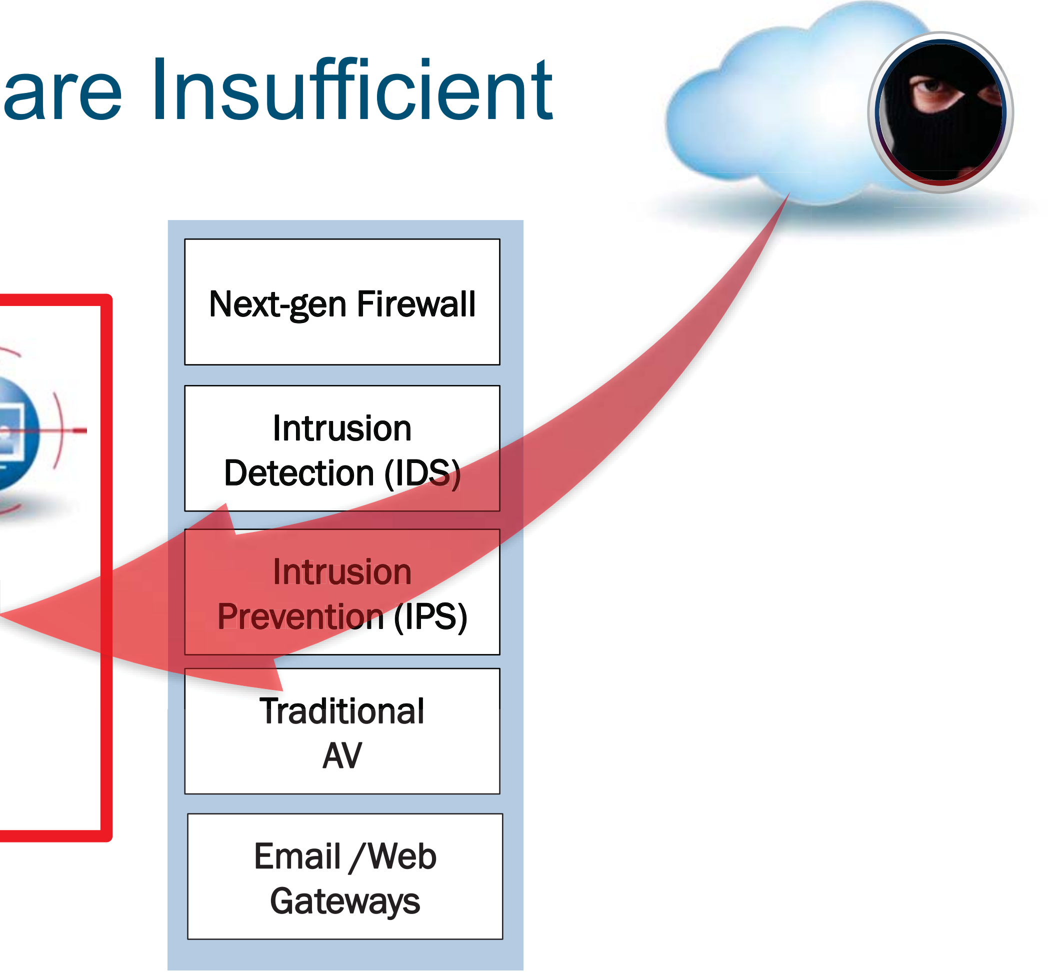
**Unexpected Strategic Impacts**

**Unexpected Risks**

**Unexpected Career Impacts**

# Standard Defenses are Insufficient

- Advanced reconnaissance
- Spear-phishing emails
- Embedded payloads
- Unknown malware & exploits
- Dynamic command and control (C&C) servers
- BYOD and remote employees create a broad attack surface



Next-gen Firewall

Intrusion Detection (IDS)

Intrusion Prevention (IPS)

Traditional AV

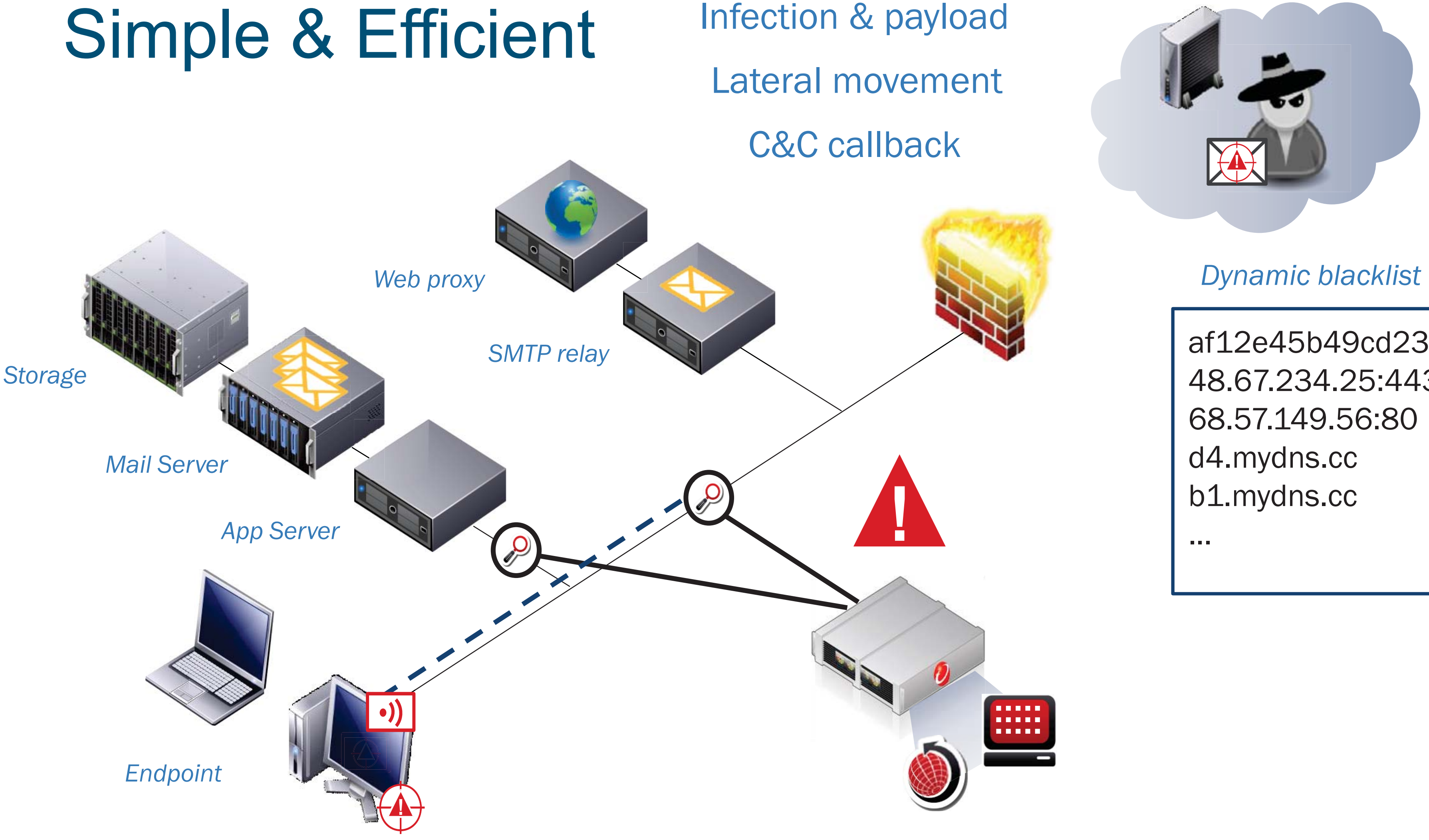
Email /Web Gateways

# Simple & Efficient

Infection & payload

Lateral movement

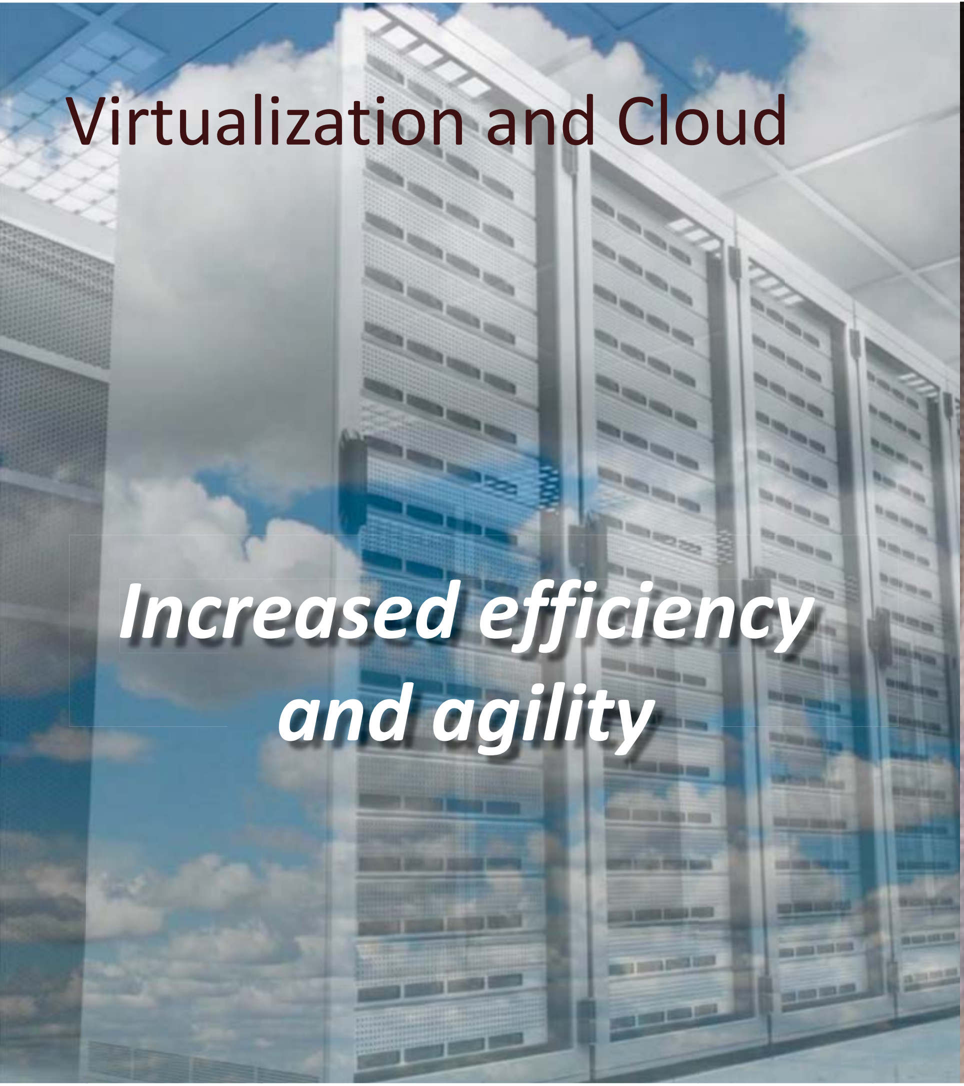
C&C callback



*Dynamic blacklist*

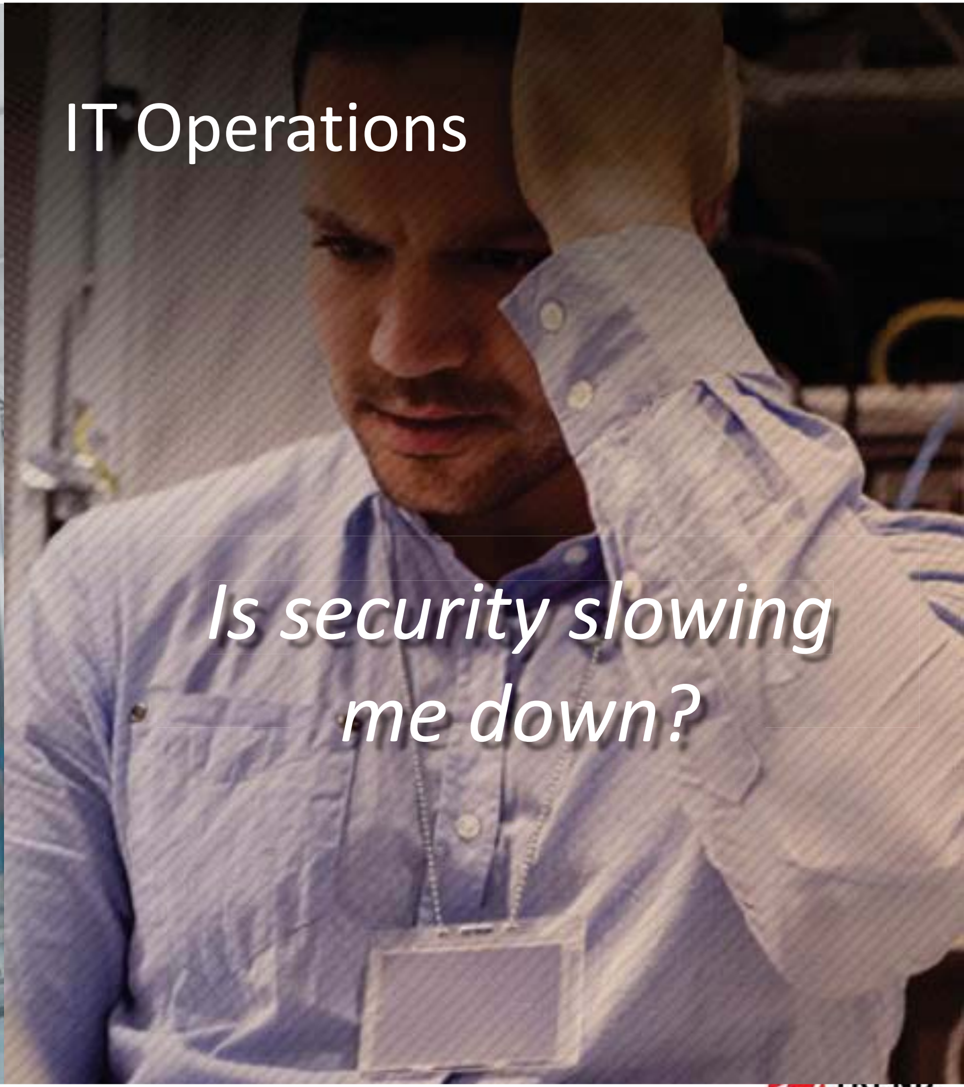
af12e45b49cd23…
48.67.234.25:443
68.57.149.56:80
d4.mydns.cc
b1.mydns.cc
…

# Data Center Security



## Virtualization and Cloud

***Increased efficiency and agility***

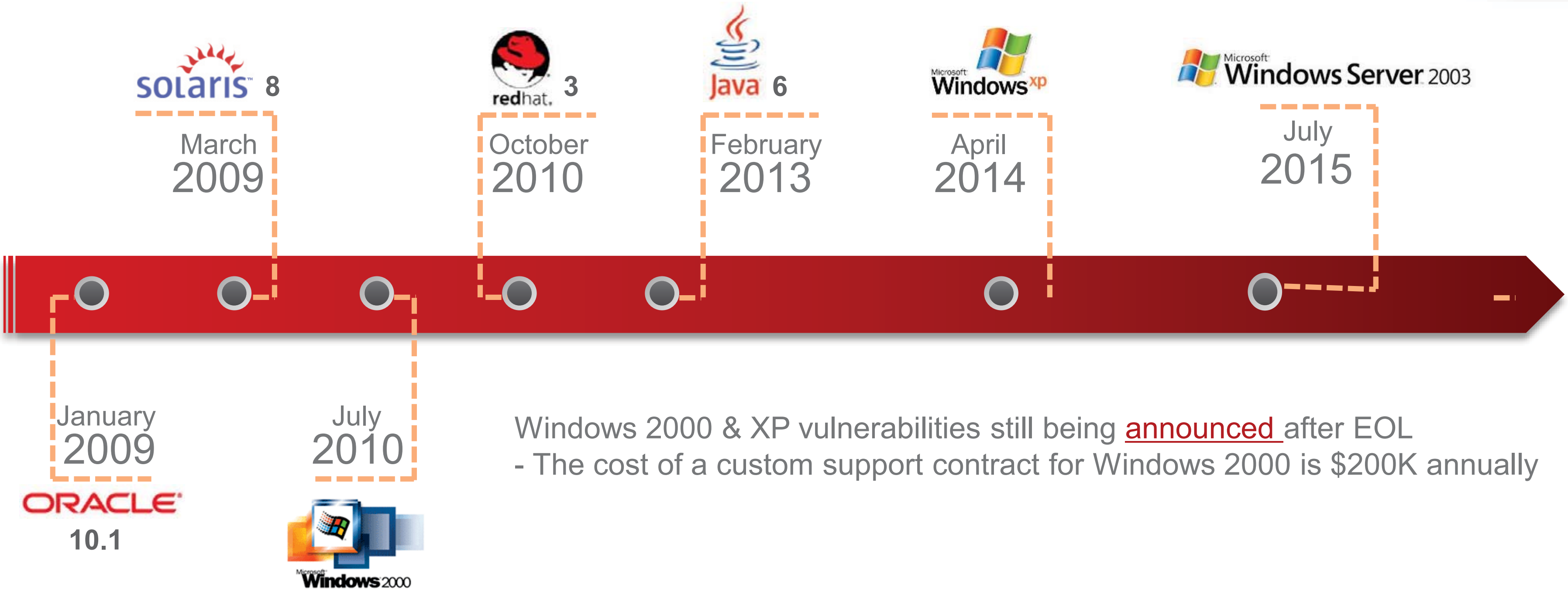


## IT Operations

*Is security slowing me down?*

# LEGACY APPLICATIONS
THAT DON'T GET PATCHED?

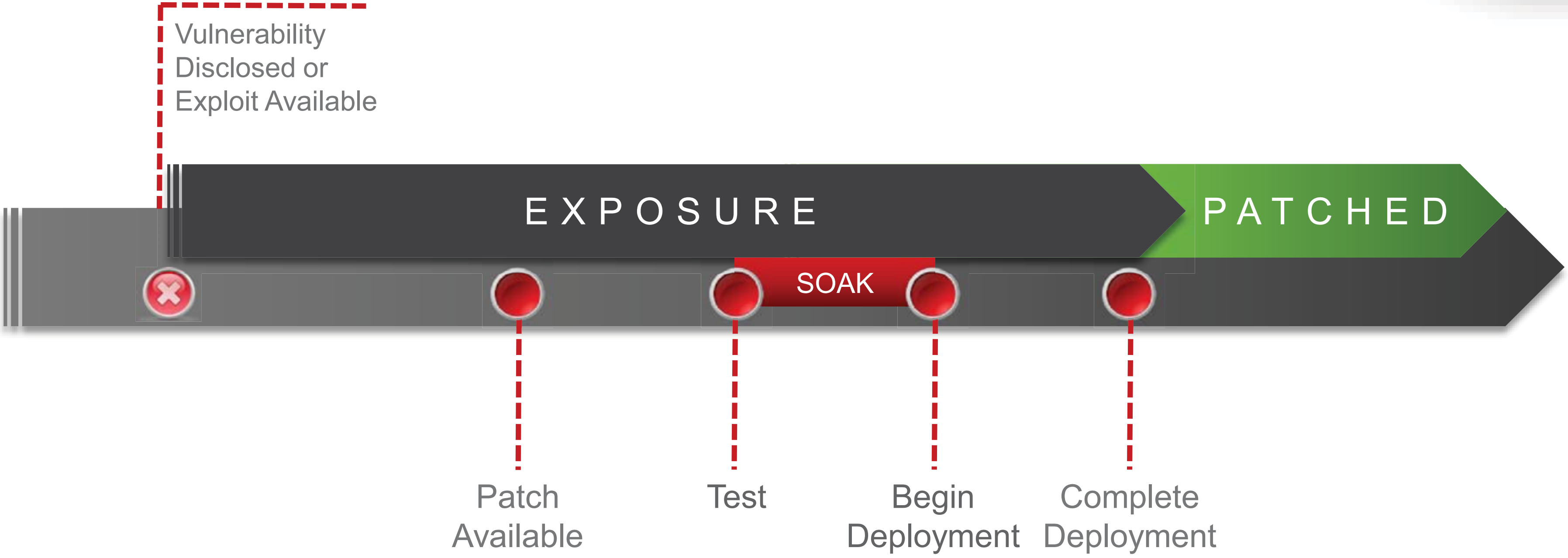
Security patches no longer issued for:



Windows 2000 & XP vulnerabilities still being announced after EOL
- The cost of a custom support contract for Windows 2000 is $200K annually

# PATCHING IS A NIGHTMARE

## HOW FAST DOES IT HAPPEN FOR YOU?



# Responsibility for Security is Shared in the Cloud

## Cloud Service Provider

Facilities

Physical security

Physical infrastructure

Network infrastructure

Virtualization infrastructure

## Customer

Operating System

Applications

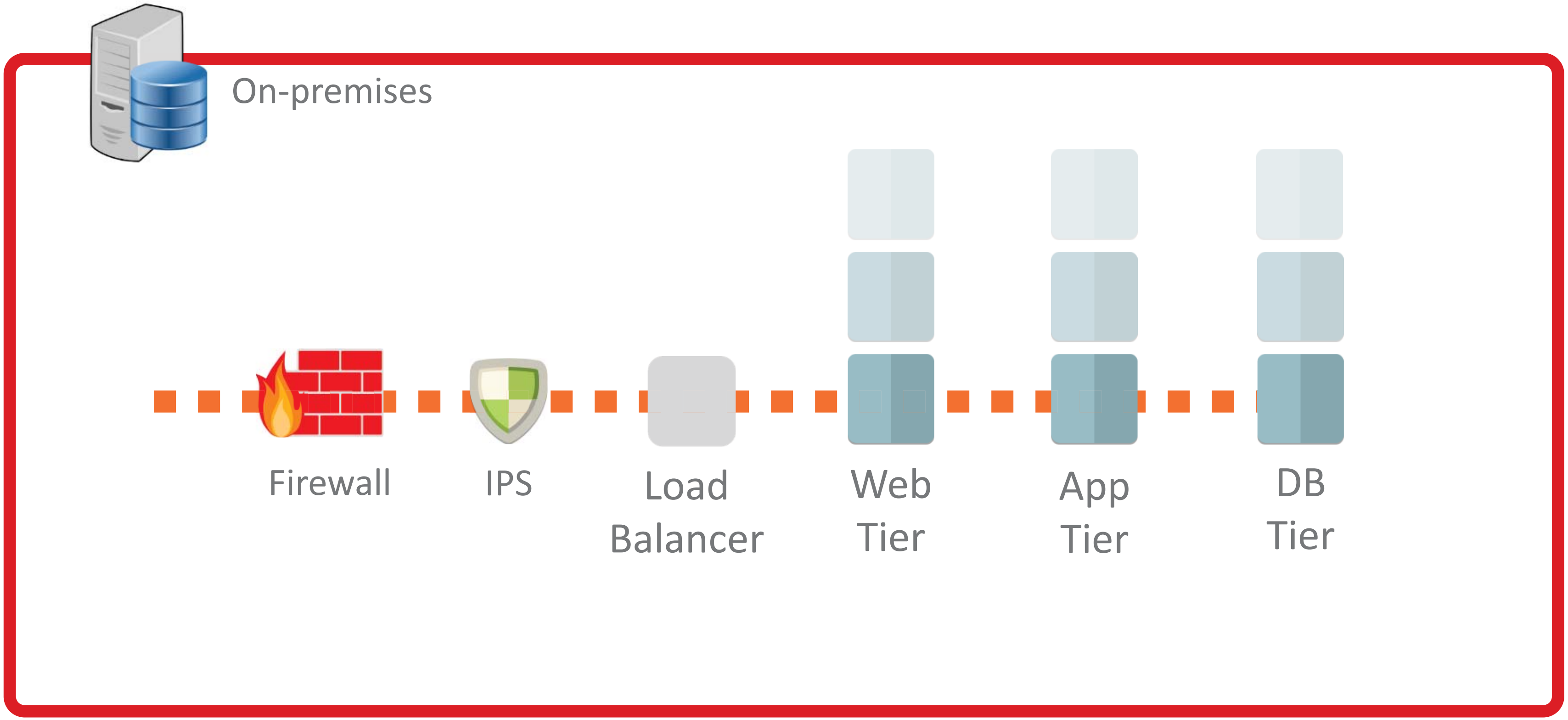
Data

Account / Security Groups

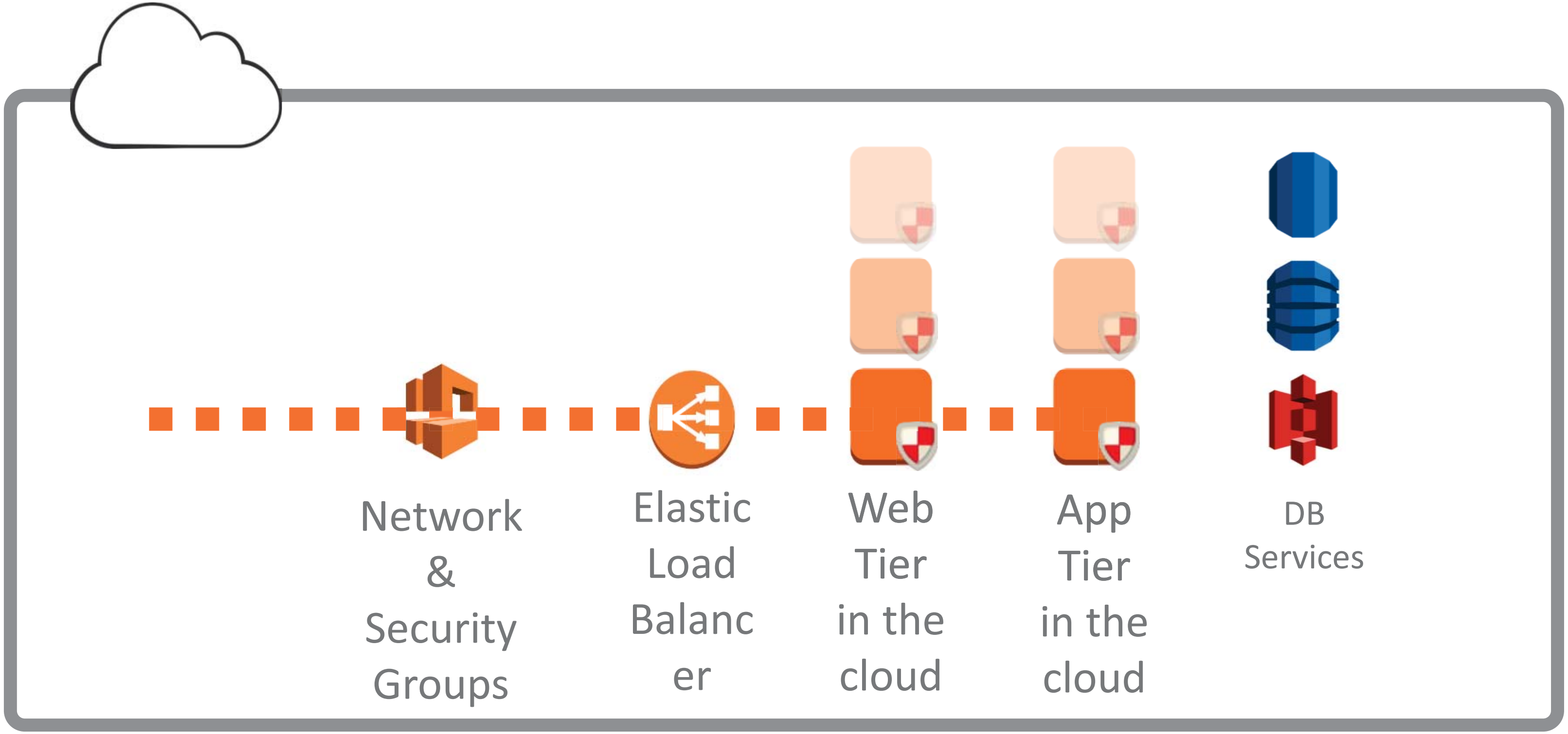
Network Configuration

# Traditional on-premise security

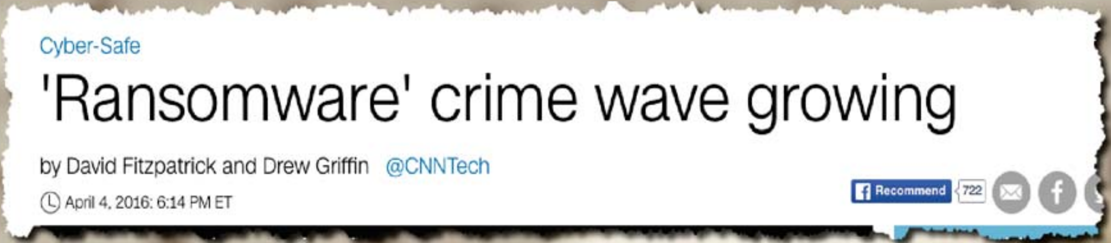
## Applied at the perimeter



# Build a workload-centric security strategy



# Ransomware

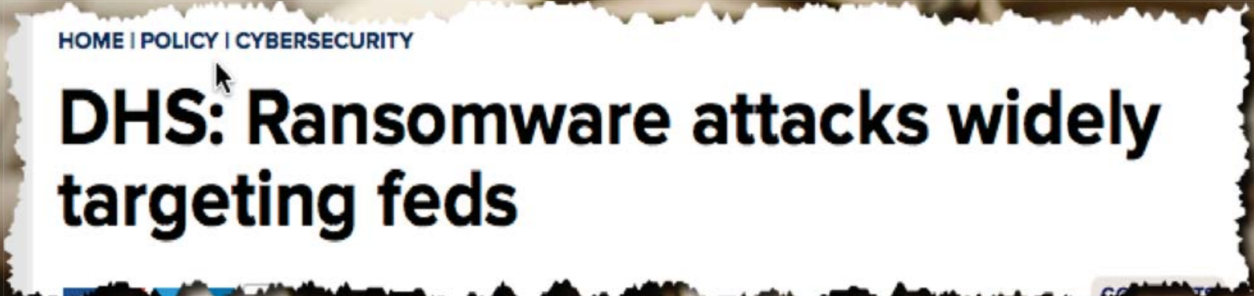


Cyber-Safe

'Ransomware' crime wave growing

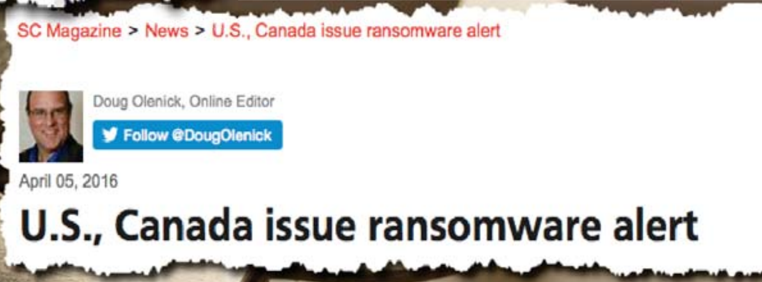
by David Fitzpatrick and Drew Griffin @CNNTech

April 4, 2016: 6:14 PM ET



HOME | POLICY | CYBERSECURITY

DHS: Ransomware attacks widely targeting feds

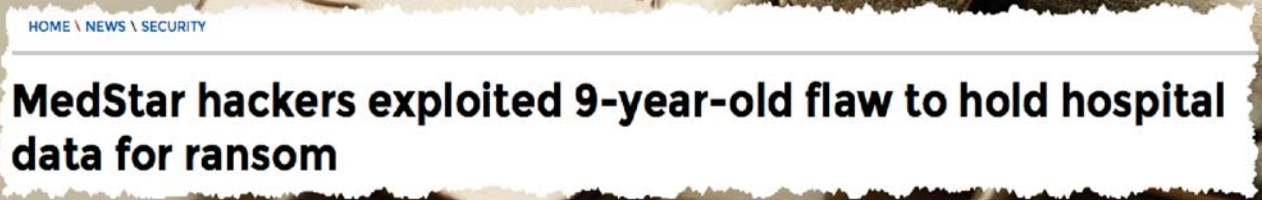


SC Magazine > News > U.S., Canada issue ransomware alert

Doug Olenick, Online Editor

April 05, 2016

U.S., Canada issue ransomware alert



HOME \ NEWS \ SECURITY

MedStar hackers exploited 9-year-old flaw to hold hospital data for ransom

# Ransomware by the Numbers

**$200-$10k**

Typical Ransom Paid

-FBI, April 2016

**>50%**

% of US Hospitals hit by Ransomware in 2015

-HIMSS Analytics, 2016

**90,000**

#of systems per day infected by Locky Ransomware

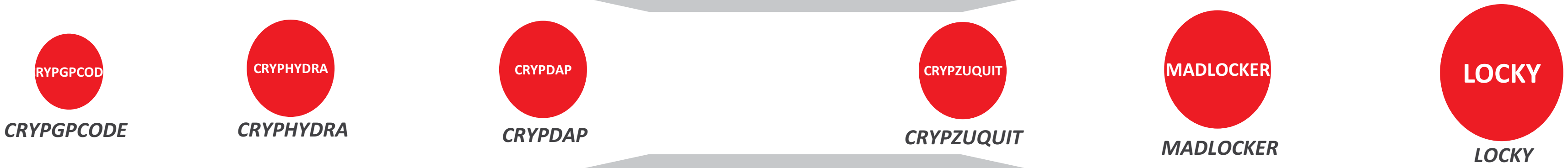
-Forbes, February 2016

# Jan 2016 - Ransomwares

| | LECTOOL | EMPER | CRYPRADAM | MEMEKAP | CRYPNISCA | CRYPJOKER | CRYPRITU |
|---|---|---|---|---|---|---|---|
| SPN DETECTION HITS | LECTOOL | EMPER | CRYPRADAM | MEMEKAP | CRYPNISCA | CRYPJOKER | CRYPRITU |
| INFECTION VECTOR | SPAM | SPAM | SPAM | SPAM | SPAM | PDF Adobe<br>DISGUISED AS PDF ATTACHMENT | SPAM |
| MODE OF PAYMENT | 2 BTC | 13 BTC | 0.5 BTC | 1 BTC | NO RANSOM NOTE | need to email malware author to get payment instructions | 0.1 BTC |
| ENCRYPTED DATA | SQL ZIP<br>DB FILES | ZIP | PERSONAL FILES<br>DB FILES + www. WEB PAGES | SQL ZIP<br>DB FILES | PERSONAL FILES<br>NO ADDITION TO PERSONAL FILES | DB FILES | DB FILES |
| ENCRYPTION | KEYS ARE GENERATED LOCALLY | PRIVATE KEY IN THE SERVER | KEYS ARE GENERATED LOCALLY | ENCRYPTION KEY IN THE SERVER | KEYS ARE GENERATED LOCALLY | KEYS ARE GENERATED LOCALLY AND DELETED | PUBLIC KEY FROM C&C |
| SELF-DESTRUCT | NO | NO | NO | NO | NO | NO | NO |

# Feb 2016 - Ransomwares

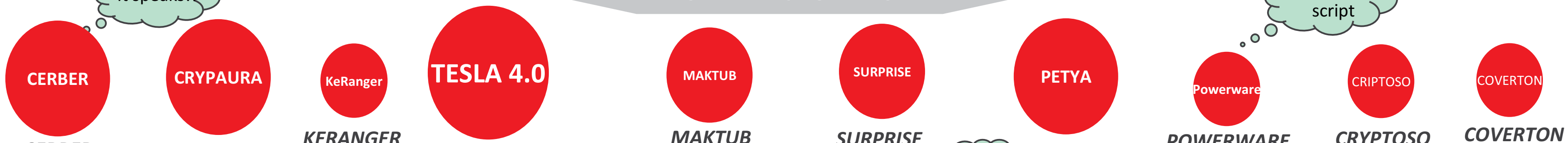
## SPN DETECTION HITS



| | CRYPGPCODE | CRYPHYDRA | CRYPDAP | CRYPZUQUIT | MADLOCKER | LOCKY |
|---|---|---|---|---|---|---|
| INFECTION VECTOR | INVOICE SPAM | EXPLOIT KIT | DISGUISED AS PDF ATTACHMENT | SPAM | SPAM | MACRO OR JS ATTACHMENT |
| MODE OF PAYMENT | 400 DOLLARS with instruction from author how to pay | 1 BTC | 0.8 BTC<br>$350 | 1.505 BTC | 2 BTC<br>536 GBP | 0.5 - 1 BTC |
| ENCRYPTED DATA (PERSONAL FILES + ) | DB FILES | SYNC MANGER LOGGER | NO ADDITION TO PERSONAL FILES | SQL + WEB PAGES | NO ADDITION TO PERSONAL FILES | WALLET<br>DB FILES<br>CODES |
| ENCRYPTION | KEYS ARE GENERATED LOCALLY | KEYS ARE GENERATED LOCALLY | PUBLIC KEY FROM C&C | PUBLIC KEY FROM C&C | KEYS ARE GENERATED LOCALLY | ENCRYPTION KEY FROM C&C |
| SELF-DESTRUCT | NO | NO | NO | NO | NO | |

# March 2016 - Ransomwares

## SPN DETECTION HITS



It speaks!!

Power shell script

| | CERBER | CRYPAURA | KERANGER | TESLA | MAKTUB | SURPRISE | PETYA | POWERWARE | CRYPTOSO | COVERTON |
|---|---|---|---|---|---|---|---|---|---|---|
| INFECTION VECTOR | EXPLOIT KIT | SPAM | APPSTORE | MACRO OR JS ATTACHMENT + EXPLOIT KIT | TERMS-OF_SERVICE (TOS) SPAM | TEAM VIEWER<br>unique | JOB APPLICATION WITH DROPBOX LINK | MACRO DOWNLOADER ATTACHMENT | | |
| MODE OF PAYMENT | 1.24-2.48 BTC | <TO BE UPDATED> | 1 BTC | 1.3 BTC | 1.4 – 3.9 BTC<br>$588 - $1638 | 0.5 to 25 BTC | 0.99 – 1.98 BTC<br>$431 - $862 | 1.18 – 2.37 BTC<br>$500 - $1000 | 1 BTC then increases by 1 BTC daily | 1 BTC |
| ENCRYPTED DATA | PERSONAL FILES<br>DB FILES | DB FILES<br>CODES | MACOS FILES | GAMES | GAMES<br>WALLET | ACCOUNTING/ FINANCE FILES | OVERWRITES MBR & BSOD<br>unique | US TAX RETURN FILES | | PERSONAL FILES<br>DB FILES |
| ENCRYPTION | PRIVATE KEY IS OBTAINED AFTER PAYMENT | PUBLIC KEY FROM C&C | PUBLIC KEY FROM C&C | 5 KEY PAIRS GENERATED LOCALLY<br>1 KEY REQUIRES RSA KEY | PRIVATE KEY IS OBTAINED AFTER PAYMENT | PRIVATE KEY IS OBTAINED AFTER PAYMENT | PRIVATE KEY IS OBTAINED AFTER PAYMENT | AES KEY GENERATED LOCALLY | | PRIVATE KEY IS OBTAINED AFTER PAYMENT |
| SELF-DESTRUCT | NO | NO | NO | NO | NO | NO | NO | ☑ | | NO |

# Protecting Against Ransomware

**Back-up and Restore**
Automated: 3 copies, 2 formats, 1 air-gapped from network

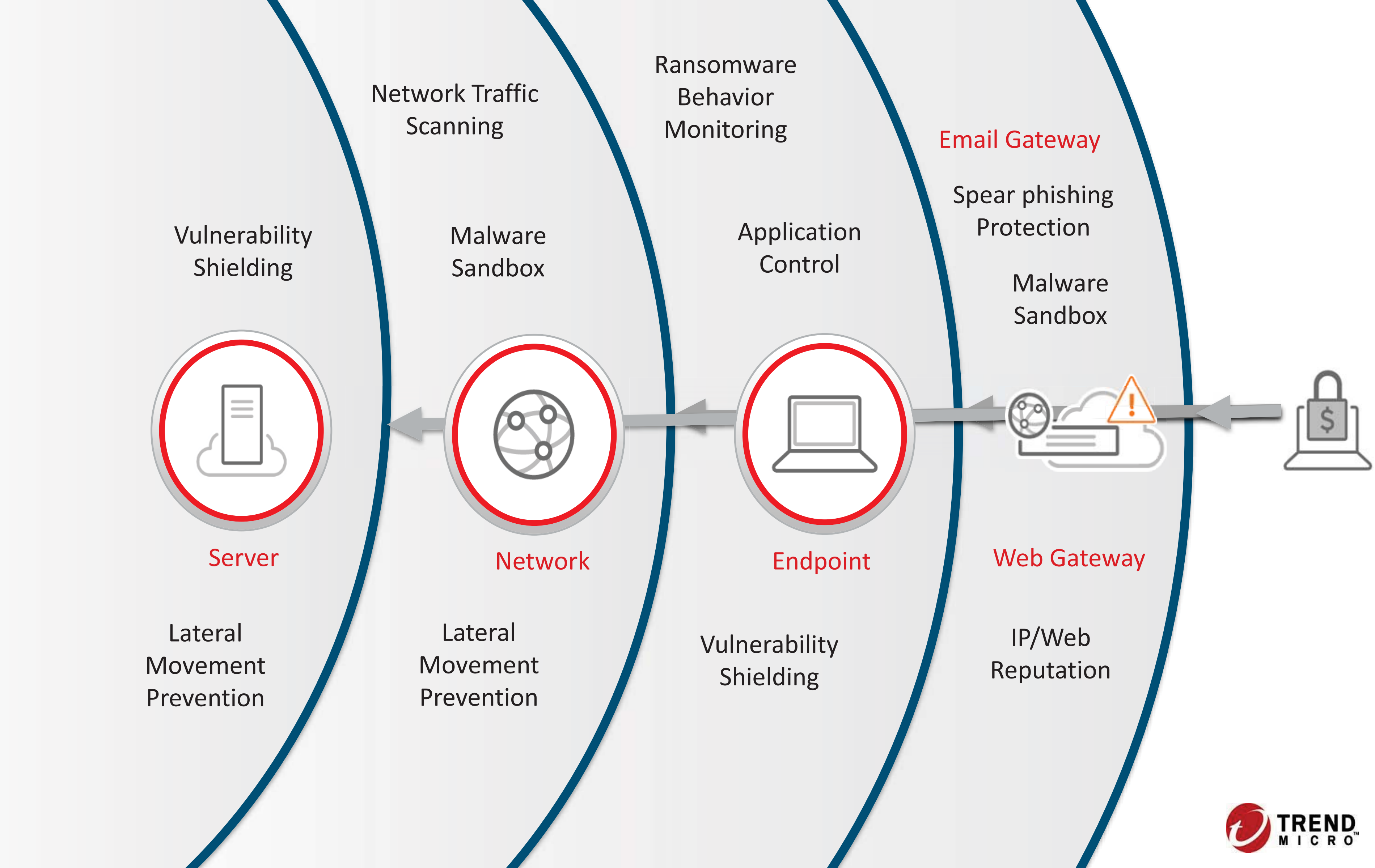
**Access Control**
Limit access to business critical data

**Keep Current with Patching**
Minimize exploits of vulnerabilities

**Don’t Pay the Ransom**
Pay-off encourages further attacks, no guarantee of data recovery

**Employee Education on Phishing**
Awareness, best practices, simulation testing

**Improve Security Posture**
Follow best practices for current solution, additional technology



Vulnerability Shielding

Server

Lateral Movement Prevention

Network Traffic Scanning

Malware Sandbox

Network

Lateral Movement Prevention

Ransomware Behavior Monitoring

Application Control

Endpoint

Vulnerability Shielding

Email Gateway

Spear phishing Protection

Malware Sandbox

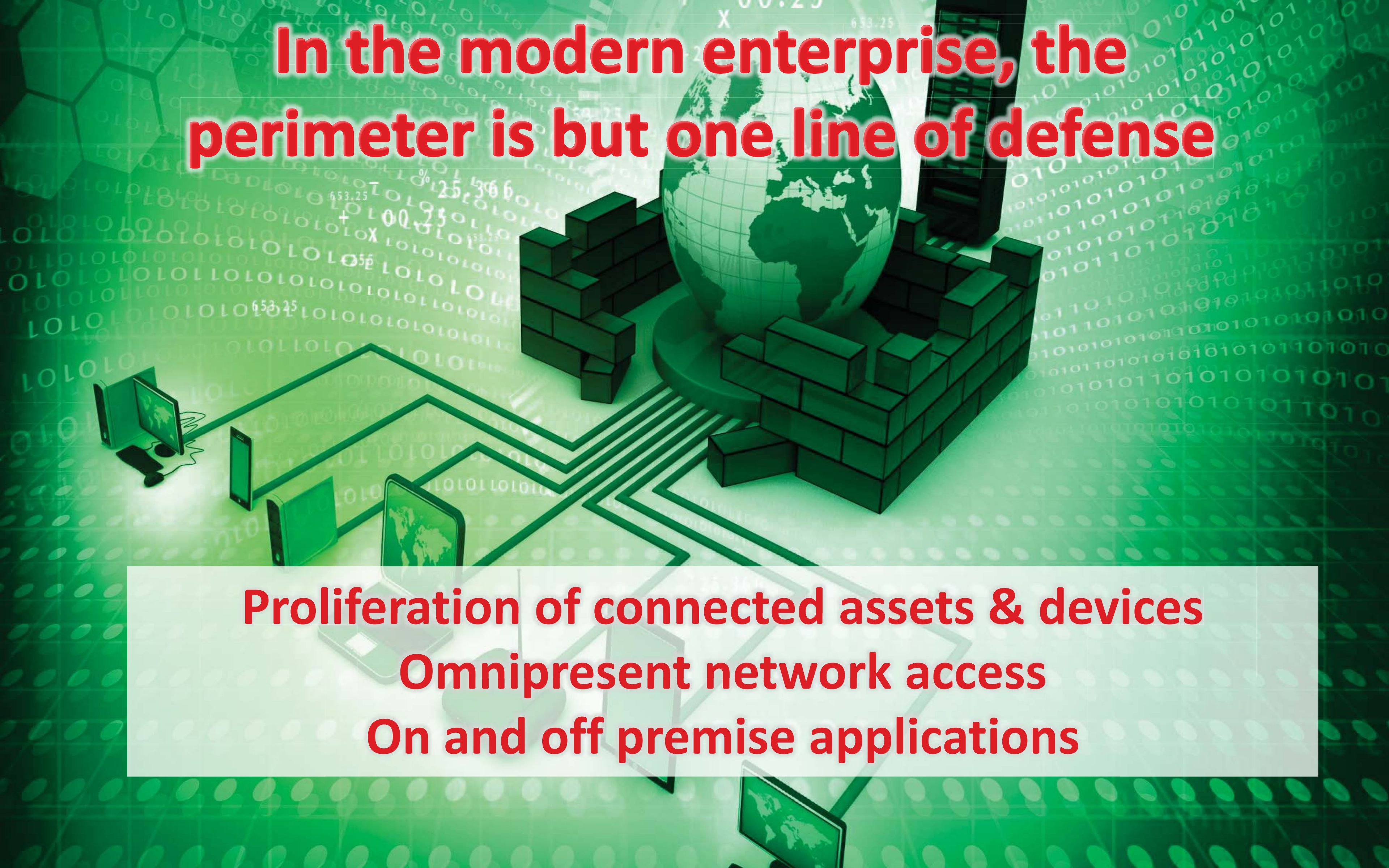
Web Gateway

IP/Web Reputation

TREND MICRO

# Throughout history adversaries have developed countermeasures to security

# In the modern enterprise, the perimeter is but one line of defense



Proliferation of connected assets & devices

Omnipresent network access

On and off premise applications

" THE TOASTER HAS BEEN HACKED INTO THINKING IT'S A BLENDER. "

*Source : www.darkreading.com*

# Thank you

Reach us on:

Srinivasan N.
Srinivasan_n@trendmicro.com

Bhavin Gandhi
Bhavin_g@trendmicro.com

www.trendmicro.com