Anatomy of the Compromised Insider

Terry Ray, Chief Product Strategist, Imperva

Agenda

- Insider Threat vs. ***Compromised*** Insider Threat
- Compromised Insiders in the News
- How Compromised Insider Attacks Happen
- How to Protect Your Organization
- Conclusion
- Q&A

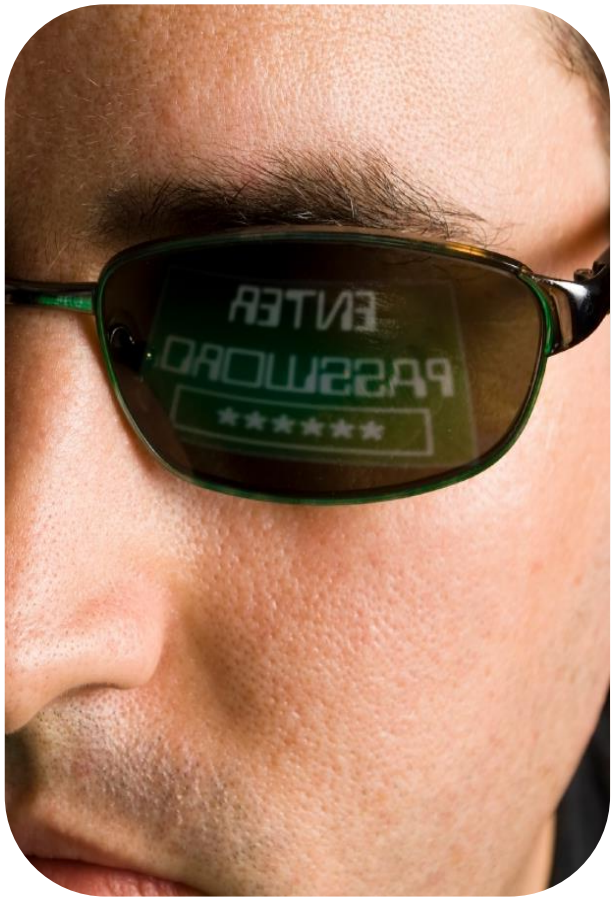
Insider Threat Defined

Insider Threat

Risk that the access rights of a trusted person will be used to view, take, or modify data or intellectual property.

Possible causes:

- Accident
- Malicious intent
- Compromised device



Compromised Insider Defined

Compromised Insider

A person with **no malicious motivation** who becomes an **unknowing accomplice** of third parties who gain access to their device and/or user credentials.

Putting Things in Perspective

"Less than 1% of your employees may be malicious insiders, but 100% of your employees have the potential to be compromised insiders."

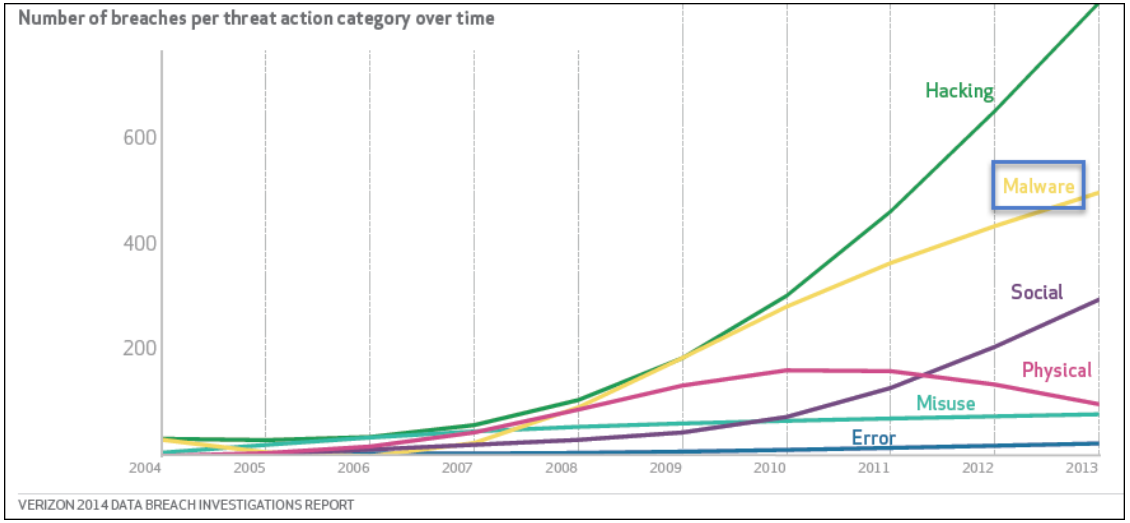
Source: http://edocumentsciences.com/defend-against-compromised-insiders

Malware: Compromised Insiders on the Rise

2012 Verizon Data Breach Report

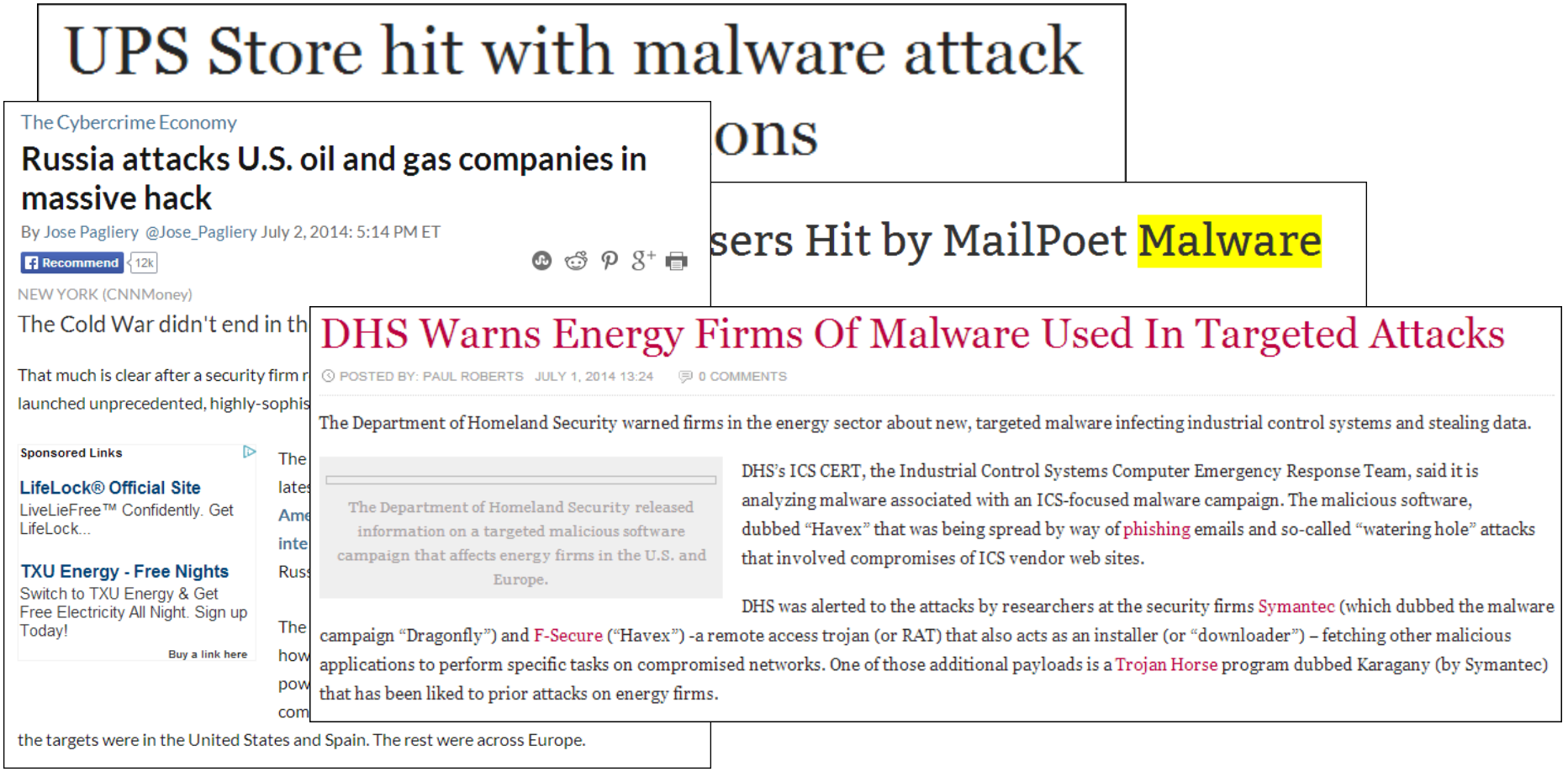
- Malware is on the rise:
  - “69% of all data breaches incorporated Malware” -- a 20% increase over 2011

2014 simply shows continued growth for Malware/compromised insiders



IMPERVA

Recent Major Enterprise Events



UPS Store hit with malware attack

ons

The Cybercrime Economy

Russia attacks U.S. oil and gas companies in massive hack

By Jose Pagliery @Jose_Pagliery July 2, 2014: 5:14 PM ET

Recommend 12k

NEW YORK (CNNMoney)

The Cold War didn't end in th

That much is clear after a security firm r

launched unprecedented, highly-sophis

Sponsored Links

LifeLock® Official Site

LiveLieFree™ Confidently. Get LifeLock...

TXU Energy - Free Nights

Switch to TXU Energy & Get Free Electricity All Night. Sign up Today!

Buy a link here

The

late

Ame

inte

Russ

The

how

pow

com

the targets were in the United States and Spain. The rest were across Europe.

sers Hit by MailPoet Malware

DHS Warns Energy Firms Of Malware Used In Targeted Attacks

POSTED BY: PAUL ROBERTS JULY 1, 2014 13:24 0 COMMENTS

The Department of Homeland Security warned firms in the energy sector about new, targeted malware infecting industrial control systems and stealing data.

The Department of Homeland Security released information on a targeted malicious software campaign that affects energy firms in the U.S. and Europe.

DHS's ICS CERT, the Industrial Control Systems Computer Emergency Response Team, said it is analyzing malware associated with an ICS-focused malware campaign. The malicious software, dubbed "Havex" that was being spread by way of phishing emails and so-called "watering hole" attacks that involved compromises of ICS vendor web sites.

DHS was alerted to the attacks by researchers at the security firms Symantec (which dubbed the malware campaign "Dragonfly") and F-Secure ("Havex") -a remote access trojan (or RAT) that also acts as an installer (or "downloader") – fetching other malicious applications to perform specific tasks on compromised networks. One of those additional payloads is a Trojan Horse program dubbed Karagany (by Symantec) that has been liked to prior attacks on energy firms.

* Sources: ZDNET 2014, InfoSecurity-Magazine 2014, CNN 2014, Security Legder.com

Where Do They Attack?

End-user devices and the user

Multimillion dollar datacenter

Not well protected

Both access the same data

Sometimes well protected

Shame Game

February 2013 – Research firm APT Report used as APT Infector

- **Mandiant** releases research paper on APT1 Chinese Hacking Group.
- Hackers create an **Infected APT1 report**.
- Hackers send **Spear Phishing** emails to lure security officers into opening the file


Home › Malware ›

February 21, 2013, 3:03PM

Spear Phishing Campaigns Use Fake Mandiant APT1 Report as Lure

by Dennis Fisher

Follow @DennisF

Share Like 13 +1 5

Comment

People looking to download and read the Mandiant report on Chinese government attacks on U.S. infrastructure should look carefully at the name of the file before opening it. Researchers say that there are at least two different spear-phishing attacks going on right now that are using rigged copies of the China APT1 report as lures.

IMPERVA

Ease of Infection Example:
Click Bait/Malvertizement – Malware Distribution

'Click bait' scams exploit Robin Williams' death

Thursday, Aug

This is a cons
Better Busin
appears Thu

Whenever a
scammers ta
with online
that claim t

This tactic is
the bait that
death of Robi

Rihanna replaces Taylor Swift as malware bait – the top 10 Facebook scam avoid them

Cyber Criminals Use
Crash News to Bait Us

Friday, July 18, 2014 Mohit Kumar

Any occasion that captures public
opportunity for spammers and hacke
the tragedy of the crashed Malaysia A

According to the U.S. intelligence off
283 passengers and 15 crew member
the missile was launched by the Ru
insurgents blamed each other.

Spammers and cybercriminals are qu
through the social media websites, ab

Ebola Content is Only Getting More Popular

October 6, 2014 Ildy Features & Tips 1 comment

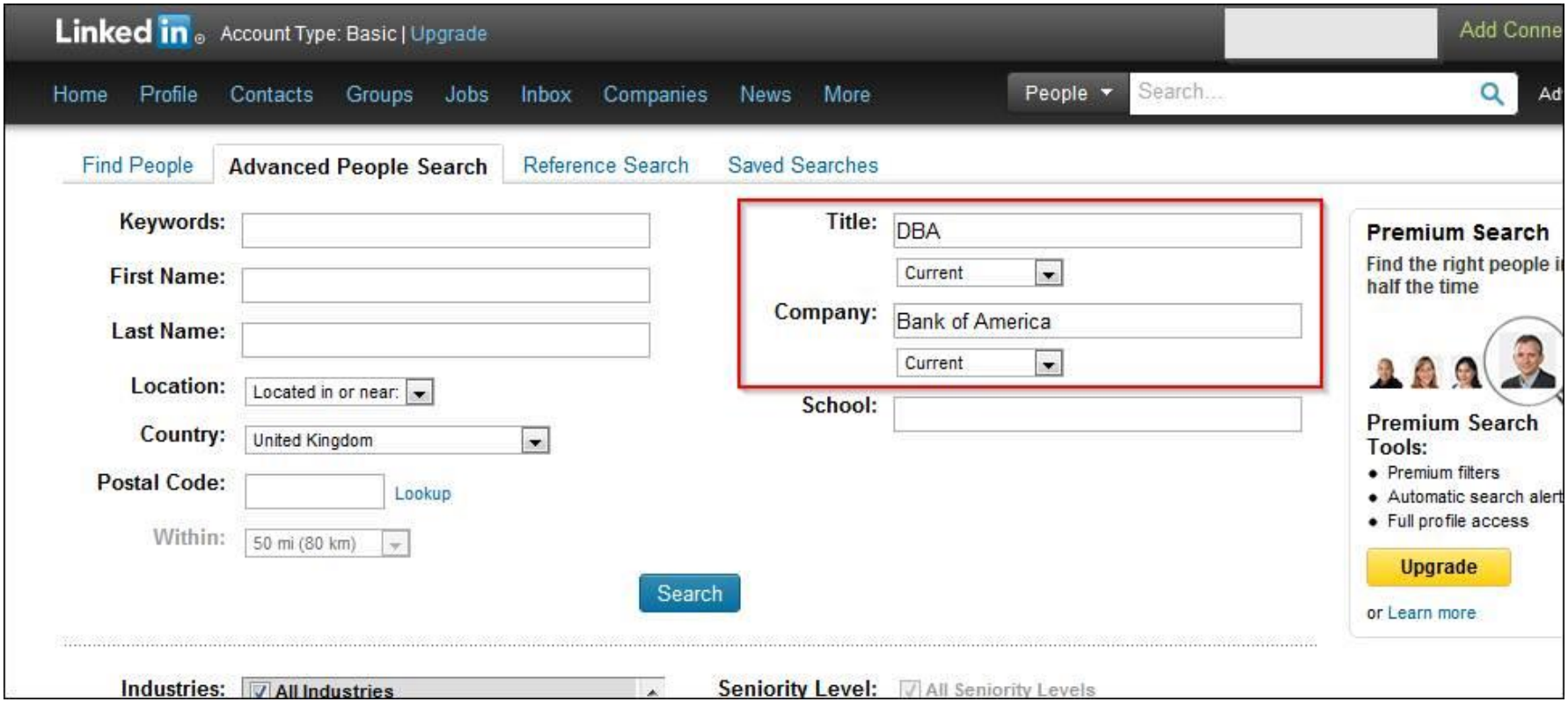
* Source: News-Sentinel, Venturebeat, thehackernews, addthis

IMPERVA

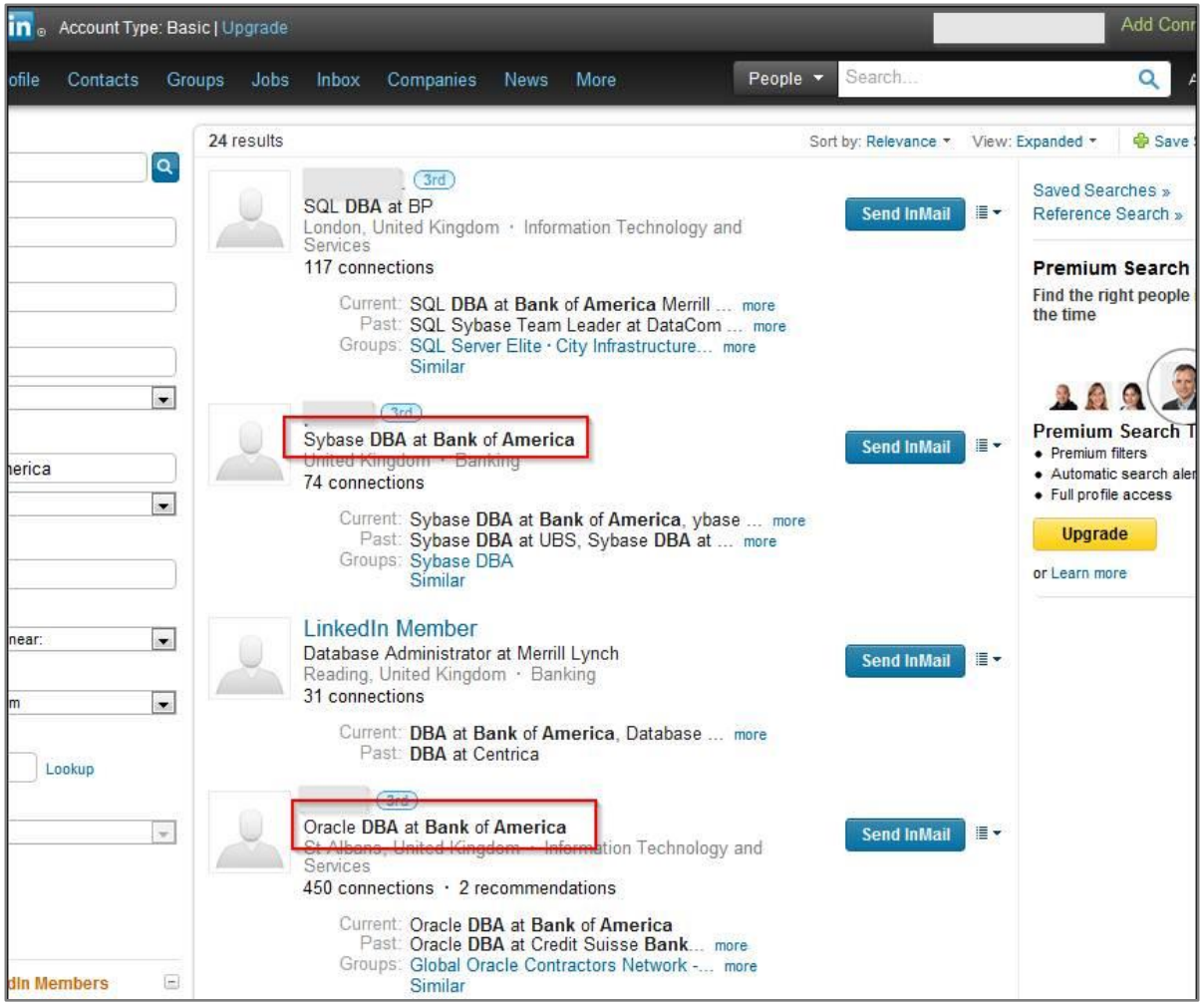
More Methods of Distribution

- Phishing / Spear Phishing
- Drive-by-download
- Malvertizement
- BlackHat SEO

Distribution –
The Unbearable Ease of Targeting



Distribution –
The Unbearable Ease of Targeting

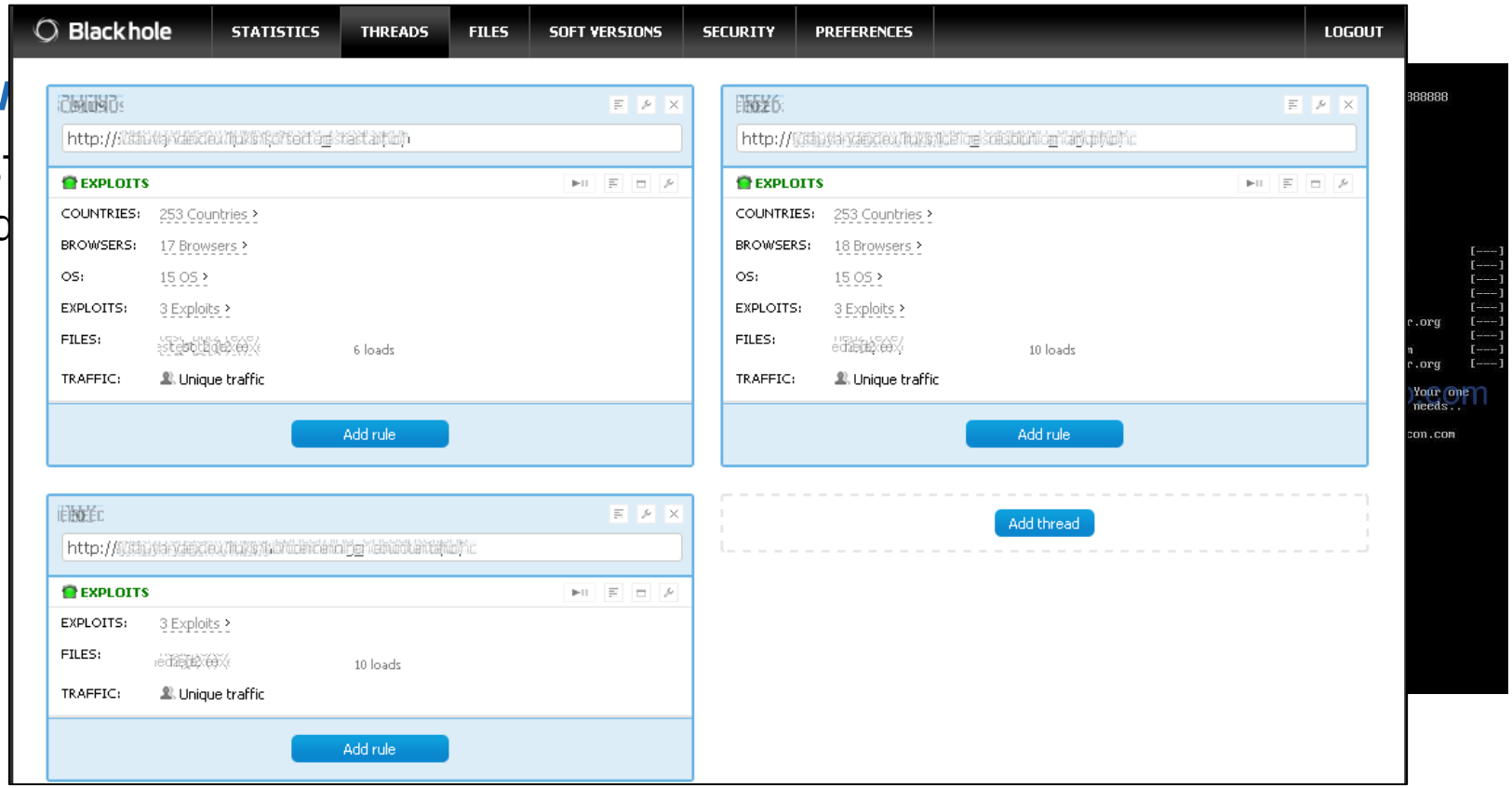


Industrialized Approach

Specialized Frameworks and Hacking tools such as BlackHole 2.0 and others, allow easy setup for Host Hijacking and Phishing

How

For $1
Includ



Persistent and Undetected

SAN FRANCISCO — For the last **four months**, Chinese hackers have **persistently** attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

The New York Times

Out of the 45 different pieces of malware planted on the Times' systems over the course of three months, **just one of those programs** was spotted by the Symantec antivirus software the Times used…

Remember this date

January 31, 2013

Symantec Response:

Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough… We encourage customers to be very aggressive in **deploying solutions that offer a combined approach to security**. **Anti-virus software alone is not enough…**

Source: The New York Times http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=1&_r=1, Symantec Corp

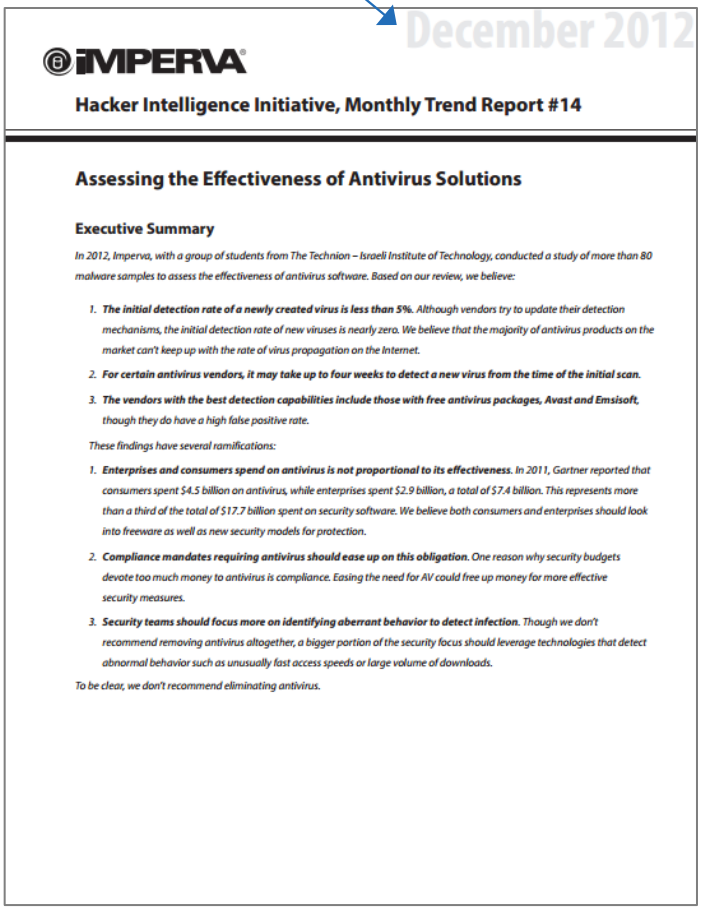
Some APT Stats

Malware	Type	Total Number of Infections	Operating Since (Estimated)	Discovered	Undetected Duration (Years)
Stuxnet 2009	Sabotage	?	June 2009	~June 2010	1
Stuxnet 2010	Sabotage	>300K	March-April 2010	June 2010	0.16
Duqu	Espionage	~50-60	April 2011	Oct 2011	0.5
Wiper	Sabotage	Tens		April 2012	
Flame	Espionage	~5000-6000	Aug 2008	May 2012	~4
Gauss	Espionage	~2500	Aug – Sep 2011	June 2012	~1
Narilam	Sabotage	?	2010	Nov 2012	3
GrooveMonitor	Sabotage	~10		Dec 2012	
Red October	Espionage	~200	May 2007	Jan 2013	5.5

Assessing Antivirus Solutions

- Imperva found that **less than 5%** of anti-virus solutions in the study were able to initially detect previously non-cataloged viruses
- For certain vendors, it may take **up to four weeks to detect** a new virus from the time of the initial scan

Note the Date



December 2012

IMPERVA

Hacker Intelligence Initiative, Monthly Trend Report #14

Assessing the Effectiveness of Antivirus Solutions

Executive Summary

In 2012, Imperva, with a group of students from The Technion – Israeli Institute of Technology, conducted a study of more than 80 malware samples to assess the effectiveness of antivirus software. Based on our review, we believe:

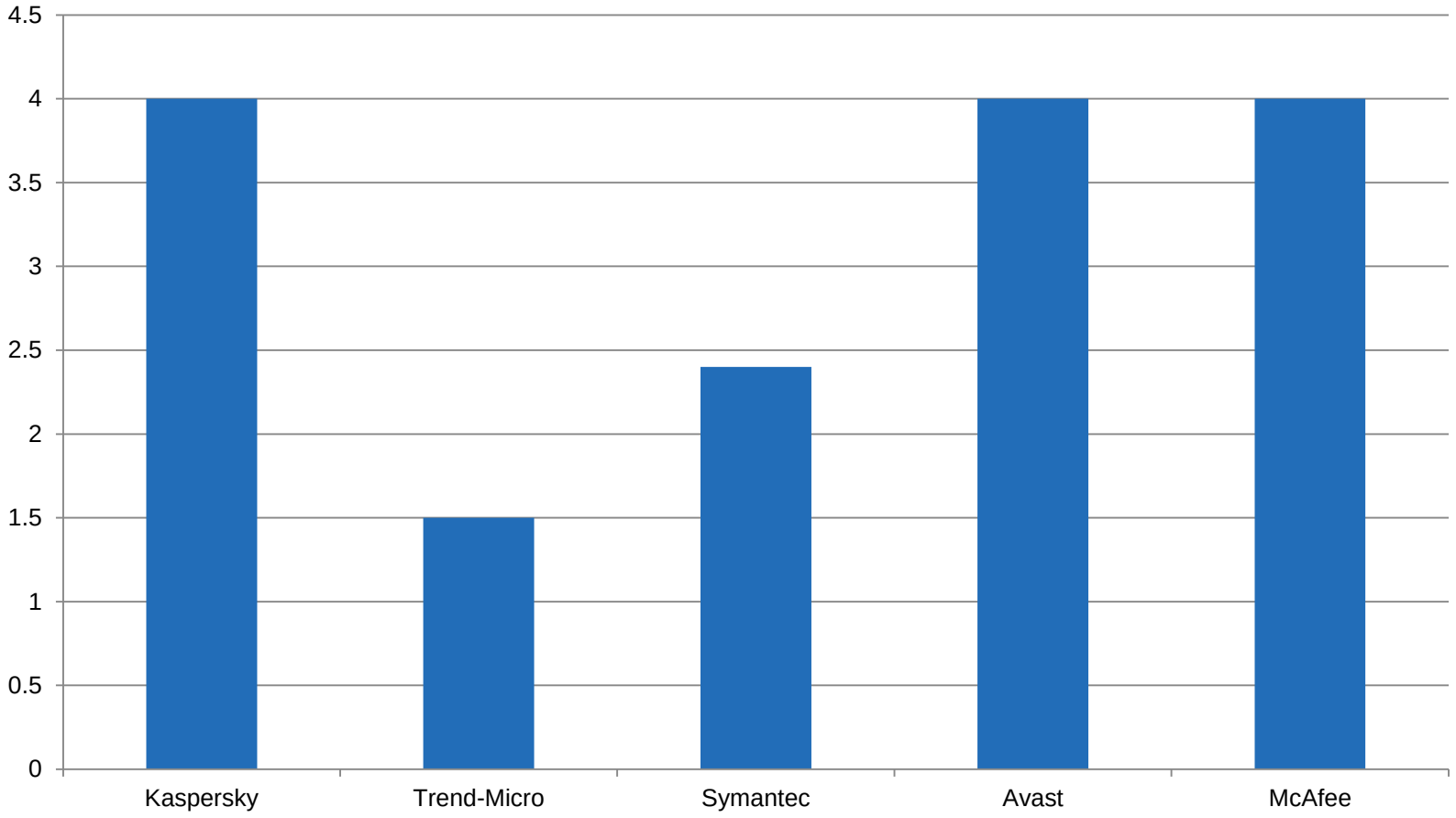
1. ***The initial detection rate of a newly created virus is less than 5%.*** *Although vendors try to update their detection mechanisms, the initial detection rate of new viruses is nearly zero. We believe that the majority of antivirus products on the market can't keep up with the rate of virus propagation on the Internet.*
2. ***For certain antivirus vendors, it may take up to four weeks to detect a new virus from the time of the initial scan.***
3. ***The vendors with the best detection capabilities include those with free antivirus packages, Avast and Emsisoft,*** *though they do have a high false positive rate.*

These findings have several ramifications:

1. ***Enterprises and consumers spend on antivirus is not proportional to its effectiveness.*** *In 2011, Gartner reported that consumers spent $4.5 billion on antivirus, while enterprises spent $2.9 billion, a total of $7.4 billion. This represents more than a third of the total of $17.7 billion spent on security software. We believe both consumers and enterprises should look into freeware as well as new security models for protection.*
2. ***Compliance mandates requiring antivirus should ease up on this obligation.*** *One reason why security budgets devote too much money to antivirus is compliance. Easing the need for AV could free up money for more effective security measures.*
3. ***Security teams should focus more on identifying aberrant behavior to detect infection.*** *Though we don't recommend removing antivirus altogether, a bigger portion of the security focus should leverage technologies that detect abnormal behavior such as unusually fast access speeds or large volume of downloads.*

To be clear, we don't recommend eliminating antivirus.

Number of Weeks Required to Identify Infected File Not identified in First Run



Bottom Line:
Security Threats Have Evolved

2001

- Script Kiddies
- “Digital Graffiti” artists
- Backdoors in open source

Nimda
Code Red
Klez
Anna Kournikova

2014

- Cyber-espionage
- Organized criminals
- Industrialized hackers

APT
Mobile phone attacks
Targeted malware attacks
200+ million identities stolen

Security Spend

- Anti-virus
- Firewall/VPN
- Content Filtering
- IDS/IPS

Security Spend

- Anti-virus
- Firewall/VPN
- Secure Email/Web
- IPS

…Security spending hasn’t

Sources: Gartner, Imperva analysis

What the Experts are Saying

Gartner

Is Antivirus Obsolete?

by **Neil MacDonald** | September 13, 2012 | Submit a Comment

technology review
Published by MIT

The Antivirus Era Is Over

Conventional security software is powerless against sophisticated attacks like Flame, but alternative approaches are only just getting started.

WIRED

"Flame was a failure for the antivirus industry. We really should have been able to do better. But we didn't. We were out of our league, in our own game."

Source: http://www.wired.com/threatlevel/2012/06/internet-security-fail/

Protect and Monitor the Cheese

- **Problem:** Most organizations chase the mice and don't focus enough on protecting the cheese

- Much of security budgets spent on:
  - NG-FW, IPS/IDS
  - Virus prevention

- Front-line/end-user defenses must be **100% accurate**, since if only 1 mouse gets past them the cheese is gone

Common Abnormal Activity to Review

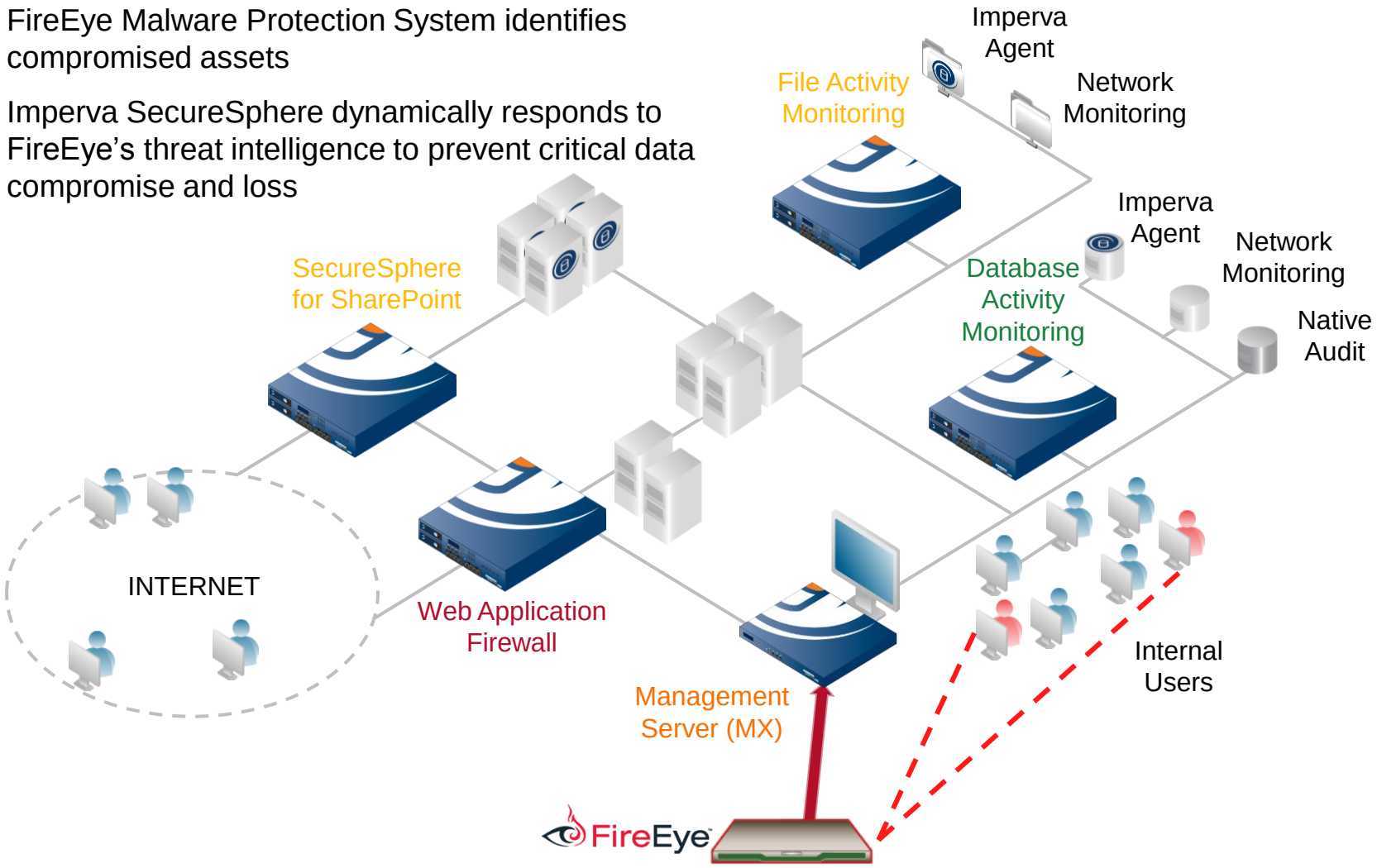
- Check the entry method
  Legitimate individuals should, typically, access data through a main door (web app, known client, etc)

- Monitor the activity of the individuals
  Malware typically causes unusual behavior and access patterns.

- Monitor the activity of privileged users
  Data controls should track the activity of the privileged users and monitor what are these privileged users accessing and how they access it.

Joint Imperva-FireEye Solution

- FireEye Malware Protection System identifies compromised assets
- Imperva SecureSphere dynamically responds to FireEye's threat intelligence to prevent critical data compromise and loss



Understand Data & What Users Do With It

Discover and Classify Sensitive Information

Build Security Policies

Review and rationalize access rights

Audit, Analyze, and Alert on Access Activity

Look for unusual behavior

Identify and Remediate Compromised Devices

Thank You