Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

3D SECURITY

"Security as part of Business Process"

Combining Policies, People and Enforcement

Derrick Ng
Regional Sales Manager

Recap: 2011 Information Technology Trends

Check Point

CLOUD COMPUTING: CONSOLIDATION, VIRTUALIZATION, CLOUDIZATION	MOBILITY: MOBILE APPLICATIONS & MEDIA TABLETS	WEB 2.0 APPLICATIONS & DATA LEAKAGE

* Gartner's Top Strategic Technologies For 2011

DATA IS EXPLODING

DATA – THE NEW OIL?

BUT IS IT LEAKING ?

Today's Threat Landscape

Check Point

Crime and Profit-Driven

Zeus
"The No. 1 financial Trojan—representing 44% of all financial malware infections today." Darkreading.com 2010

Ideology and State-Driven

Operation Aurora
"Cyber espionage attack on Google, Adobe, Yahoo and many others…"
The Washington Post 2010

Cyber War! HACTIVIST ANONYMOUS

Driven by Bot Attacks!

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 6
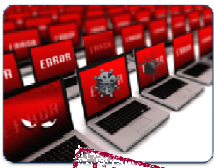
Organizations are at Risk!

Check Point

4.5 million computers were infected by TDL-4 botnet just in Q1/2011[1]

50% of Fortune 100 organizations were compromised by data stealing Mariposa botnet[2]

60% of IT security professionals consider APT attacks as #1 concern[3]

1 Kaspersky Labs, June 2011
2 http://securitywatch.pcmag.com/internet-crime/284377-botnet-reported-loose-in-fortune-100
3 B2B Endpoint Security Survey, August 2011

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 7

What Exactly Is APT?

Check Point

A dvanced attack capabilities and well-planned

P ersistent and have continuous access to the systems

T hreat to business, compromises the ability to operate

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 8

Victims of APT …

Check Point

Operation Shady RAT

Victim's Country of Origin		Victim Count
USA		49
Canada		4
South Korea		2
Taiwan		2
Japan		2
Switzerland		2
United Kingdom		2

Victim's Country of Origin		Victim Count
Indonesia		1
Vietnam		1
Denmark		1
Singapore		1
Hong Kong		1
Germany		1
India		1

The Breach: Facts

Check Point

- The formula of data breach: 1+1=2

Lack of:
(Integration + {Effective Legal + Policy Guidelines }) = data breach

- Malware is a **human** issue

- Attack surface is refocused on desktop content

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 10

IT Survey of Social Engineering Risk
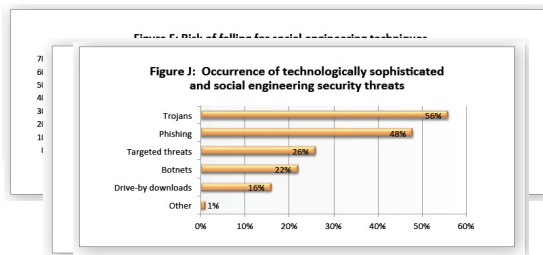
Check Point

Figure J: Occurrence of technologically sophisticated and social engineering security threats

Trojans	56%
Phishing	48%
Targeted threats	26%
Botnets	22%
Drive-by downloads	16%
Other	1%

THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY:
A SURVEY OF IT PROFESSIONALS

Dimensional Research | September 2011

Facebook in Asia – Quarter 3 2011

Check Point

Facebook in Asia, Estimated Total Users by Country – Quarter 3 2011

Current Rank (Previous Rank)	Country	September 30 2011	July 01 2011	% Growth
1 (1)	Indonesia	40,418,840	38,860,460	4%
2 (2)	India	36,422,980	29,475,740	24%
3 (3)	Philippines	26,721,920	25,307,780	6%
4 (5)	Thailand	12,076,740	10,612,360	14%
5 (4)	Malaysia	11,751,940	11,221,020	5%
6 (6)	Taiwan	10,976,580	9,932,720	11%
7 (7)	Pakistan	5,395,040	4,795,220	13%
8 (8)	Japan	4,819,200	3,812,480	26%
9 (10)	South Korea	4,081,460	3,697,040	10%
10 (9)	Hong Kong	3,829,760	3,748,580	2%
11 (11)	Singapore	2,590,000	2,489,020	4%
12 (13)	Vietnam	2,520,900	1,674,020	51%
13 (12)	Bangladesh	2,000,980	1,735,000	15%
14 (14)	Nepal	1,269,360	1,072,900	12%
15 (15)	Sri Lanka	1,093,400	973,740	12%
16 (16)	Cambodia	401,800	329,700	22%
17 (19)	Afghanistan	230,240	198,020	16%
18 (17)	Brunei	221,740	214,140	4%
19 (20)	Mongolia	214,360	182,620	17%
20 (18)	Macau	212,860	207,420	3%
21 (21)	Maldives	114,280	107,460	6%
22 (22)	Laos	96,560	70,440	37%
23 (23)	Bhutan	61,020	53,280	15%
	TOTAL	**167,521,560**	**150,771,020**	**11%**

Source: Facebook Ads estimator

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 12

Avoid All The Mess

- Is there something we can do ?
  - YES! But there are no magic bullets

- Can't rely on just layered protection, need to think beyond compliance.

- Invest in Education and Security awareness programs – immersive and realistic

- Invest in Security Controls to provide VISIBILITY so as to improve intelligence and response

- Implement Incident Response into daily practice. Involve People

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 13

Proven Security Strategies

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 14
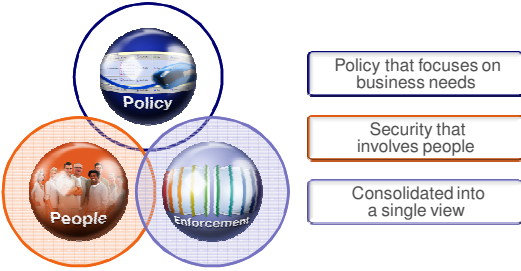
Check Point 3D Security Vision

Combine Policy, People and Enforcement for Better Security

Policy

People

Enforcement

Policy that focuses on business needs

Security that involves people

Consolidated into a single view

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 15

FIRST DEFINE THE
PROCESS & POLICIES

Security as a Business Process

Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURITY <u>POLICIES</u> & PROCESS

3D
SECURITY

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 17

ENFORCEMENT

POLICY

PEOPLE
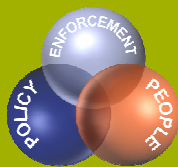
3D SECURITY:
DISCUSSION
EXAMPLE
SECURITY THAT INVOLVES PEOPLE

Policies, __People__ and Enforcement

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 19

Today's typical user 'involvement'

NO EXPLANATION

NO RESOLUTION

The website declined to show this webpage

Most likely causes:
• This website requires you to log in.

What you can try:
➔ Go back to the previous page.
⊕ More information

This error (HTTP 403 Forbidden) means that Internet Explorer website, but it does not have permission to view the web

For more information about HTTP errors, see Help.

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 20

People Taking Part in Security

EXPLANATION

RESOLUTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

Received: less than 1 min. ago

Data Loss Prevention Alert

An email that you have just sent has been quarantined.

Reason: You have sent an email suspected to contain **customer transactions disclosure** to an external recipient

The message is being **held** until further action.

__Send__ , __Discard__ or __Review Issue__

Close

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 21

People Are Part of Security

Check Point

PEOPLE — SHOULD BE **AWARE** OF THE CORPORATE SECURITY POLICY

PEOPLE — SECURITY SHOULD BE **SEAMLESS** AND **SIMPLE** TO PEOPLE

PEOPLE — ARE **PART** OF THE BEST SECURITY PROCESS

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 22

3D SECURITY:
GAIN CONTROL BY EFFECTIVE ENFORCEMENT
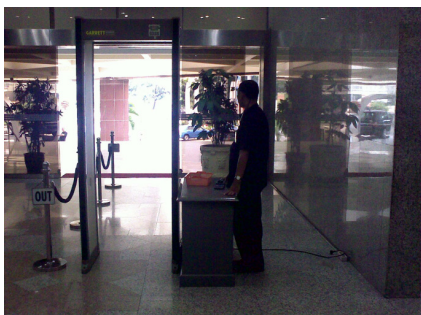
Policies, People and Enforcement

Check Point

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 24

Policies, People and <u>Enforcement</u>

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 25

Multiple Layers of Controls

MOBILITY	DATA	MALWARE
	VPN	FIREWALL
ACCESS CONTROL	DISK ENCRYPTION	ANTI VIRUS
AUTHORIZATION	DOCUMENTS	WEB ACCESS
DEVICE SECURITY	REMOVABLE MEDIA	IPS
VPN	DLP GATEWAYS	APP CONTROL

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 26
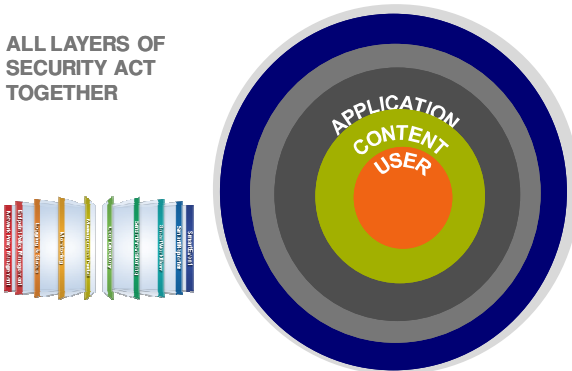
Consolidate Security

ALL LAYERS OF SECURITY ACT TOGETHER

APPLICATION
CONTENT
USER

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 27

Granular Control of all Security layers

- IPS — Network Threat Prevention
- Mobile Access — Mobile Access
- DLP — Sensitive Data
- Application Control & URL Filtering — Internet Applications Usage
- Identity Awareness — User Access

Granular Visibility

SmartEvent

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 28

Need to Control All Aspects of Web

Web Traffic
Websites   Applications

Websites
- www.poker.com
- www.hackthissite.org
- www.playboy.com
- www.fantasyfootball.com

Applications
- skype — Not URL-based
- Facebook Chat — Granularity beyond URLs

Unified Control Needed !

Introducing Check Point AppWiki

Unparalleled Application Control

Check Point AppWiki

Over **4,500** applications

Over **240,000** social-network widgets

Grouped in over **80** categories
(including Web 2.0, IM, P2P, Voice & Video, File Share)

http://appwiki.checkpoint.com/appwiki/applications.htm

World's largest Application Classification Library

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 30

SSL Encryption Inspection

Check Point | SECURITY TECHNOLOGIES LTD.

Check Point's New R75.20 Release

Check Point R75.20

Inspect SSL-encrypted traffic across all Software Blades

SSL-Encrypted Traffic

Check Point | SECURITY TECHNOLOGIES LTD.

More Traffic is Transmitted Through Secured Channels

Protecting commercial and private transactions

PayPal   Gmail by Google

ebaY   facebook   citibank

Check Point | SECURITY TECHNOLOGIES LTD.

Inspect SSL-Encrypted Traffic Across All Software Blades

| DLP | IPS | Application Control | Antivirus & Anti-Malware | URL Filtering |

Sensitive Data Leak Preventions

Check Point SOFTWARE TECHNOLOGIES LTD.

**Users need to be engaged
in the security process**

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 34

New Software Blade Takes on Botnets!

Check Point SOFTWARE TECHNOLOGIES LTD.

**Introducing Check Point
Anti-Bot Software Blade**

Anti-Bot

REVOLUTIONIZE BOT PREVENTION!

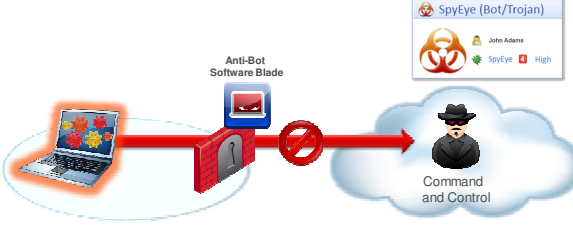softwareblades ©2011 Check Point Software Technologies Ltd. | [PROTECTED] – All rights reserved | 35

Check Point Anti-Bot Software Blade

Check Point SOFTWARE TECHNOLOGIES LTD.

| Discover infected machines | Prevent bot damages | Integrated Threat Prevention |

SpyEye (Bot/Trojan)

John Adams

SpyEye | High

**Anti-Bot
Software Blade**

Command
and Control

©2011 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 36

**Check Point Software Blades -
Integrated in a Single Gateway**

| Stop Bot and APT damages | Prevent exploit of vulnerabilities | Deny access to malicious Applications/Web | Protect Sensitive Data |

Anti-Bot · Application Control · URL Filtering · Data Leak Prevention

**Most Comprehensive
Threat Prevention Solution!**

©2011 Check Point Software Technologies Ltd.　|　[Unrestricted] For everyone　| 37

SmartEvent – Manage Visibility

**Identify critical security events from the
clutter with visual timelines**

Correlate events across all security systems

Stop attacks straight from the event screen

©2011 Check Point Software Technologies Ltd.　|　[Unrestricted] For everyone　| 38

Check Point 3D Security Can Help

1 Proven, Proactive Next-Generation Firewall

2 Comprehensive, Market-Leading Data Security

3 Engage and Train Users with UserCheck

4 Increase Visibility & Best Practices with SmartEvent

©2011 Check Point Software Technologies Ltd.　|　[Unrestricted] For everyone　| 39

A New Way to Address these Requirements

Introducing:

Check Point

3D Consulting Services

Architecture & Policy Review

Compliance Development & Assessment

Summary

Check Point

BECAUSE TODAY'S THREAT LANDSCAPE REQUIRES A PROACTIVE, UNIFIED APPROACH

THANK YOU

Stay Secured. Stay In Control

3D SECURITY
Policy. People. Enforcement.