2014 Security Report
Racing Against Time

SOFTWARE-DEFINED PROTECTION

JOIN THE **SECURITY REVOLUTION**

A recent report suggests that **victims lose around €290 billion** each year

worldwide as a result of cybercrime, making it more profitable than the global trade

in marijuana, cocaine and heroin combined (Europol)

About the 2014 Security Report

- Gateway event data from 9,240 organizations

- Meta-analysis of malware, application and DLP data from almost 1,000 organizations

- Data collected over course of 2013

softwareblades™

Key Findings of Check Point *2014 Security Report*

1 Use of unknown malware exploded in 2013

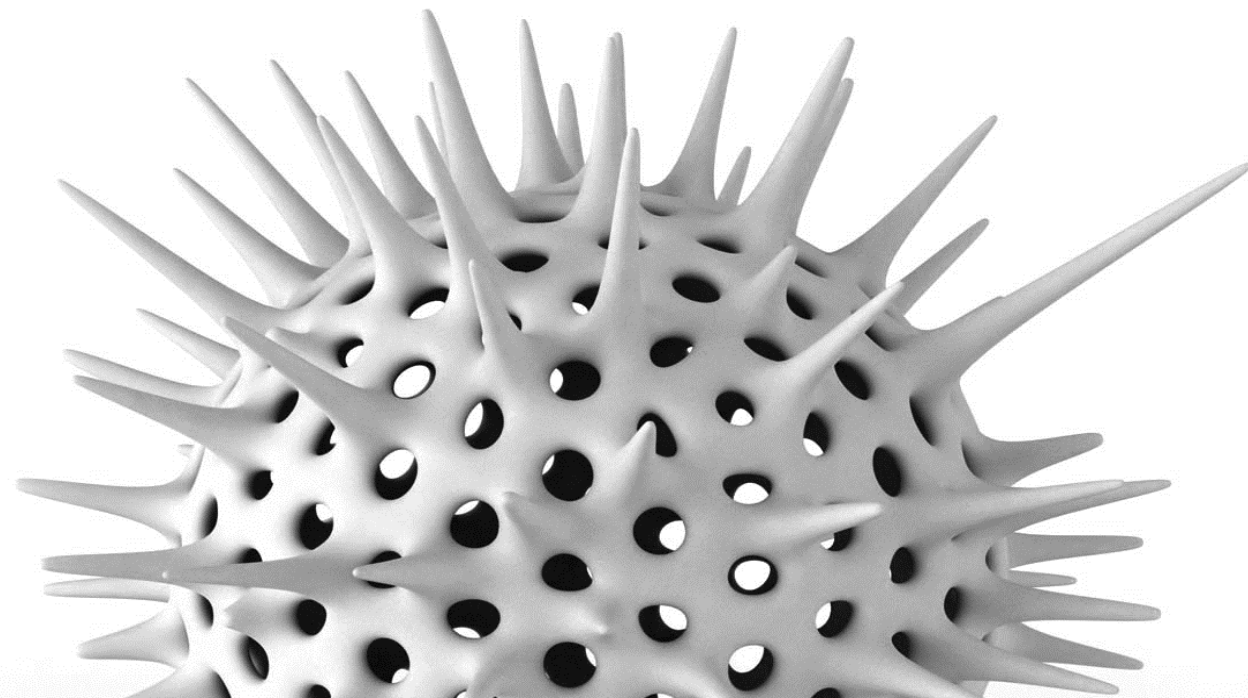**2** Malware exposure and infections increased

3 High-risk applications expanded in the enterprise

4 Data loss events grew across industries and data types

0/46

AV vendors who detected HIMAN when it was caught by Threat Emulation*

* Source: http://www.checkpoint.com/threatcloud-central/articles/2013-12-16-te-catches-new-sophisticated-malware-variant.html

©2014 Check Point Software Technologies Ltd.

53

UNKNOWN MALWARE files pass an organization's gateway EVERY DAY

New Unknown Malware Is Often Effective for *Days*

<10% of malware engines detected unknown malware when it was first caught in the wild

2-3 days for a majority of anti-malware engines to detect unknown malware after it is first caught in the wild

84%

OF ORGANIZATIONS DOWNLOADED A MALICIOUS FILE

Malware Exposure and Infections Increased in 2013

- ## A host accesses a malicious Web site every minute
  - In 2012, the *rate* was one host every 23 minute

- ## A host downloads malware every 10 minutes
  - 58% of organizations experienced a user downloading malware every 2 hours or less
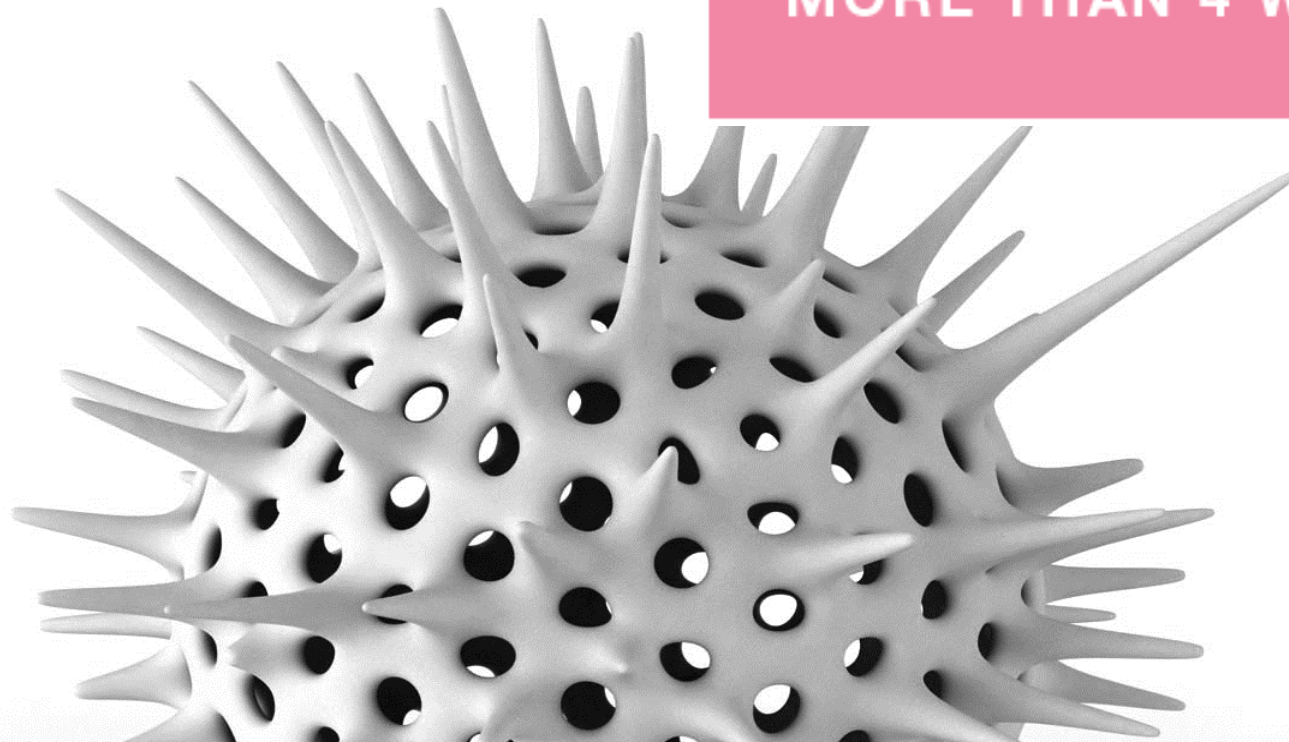
- ## 49% of organizations have 7 or more bot-infected hosts

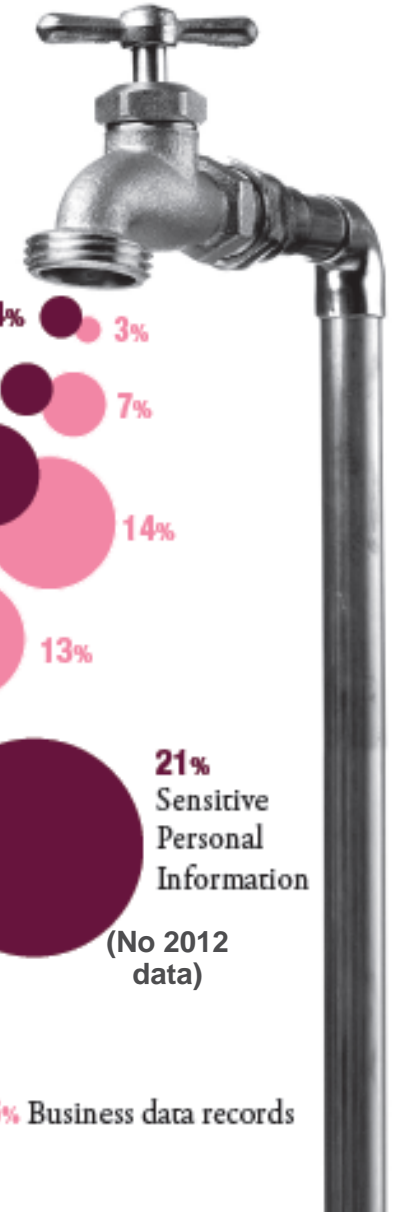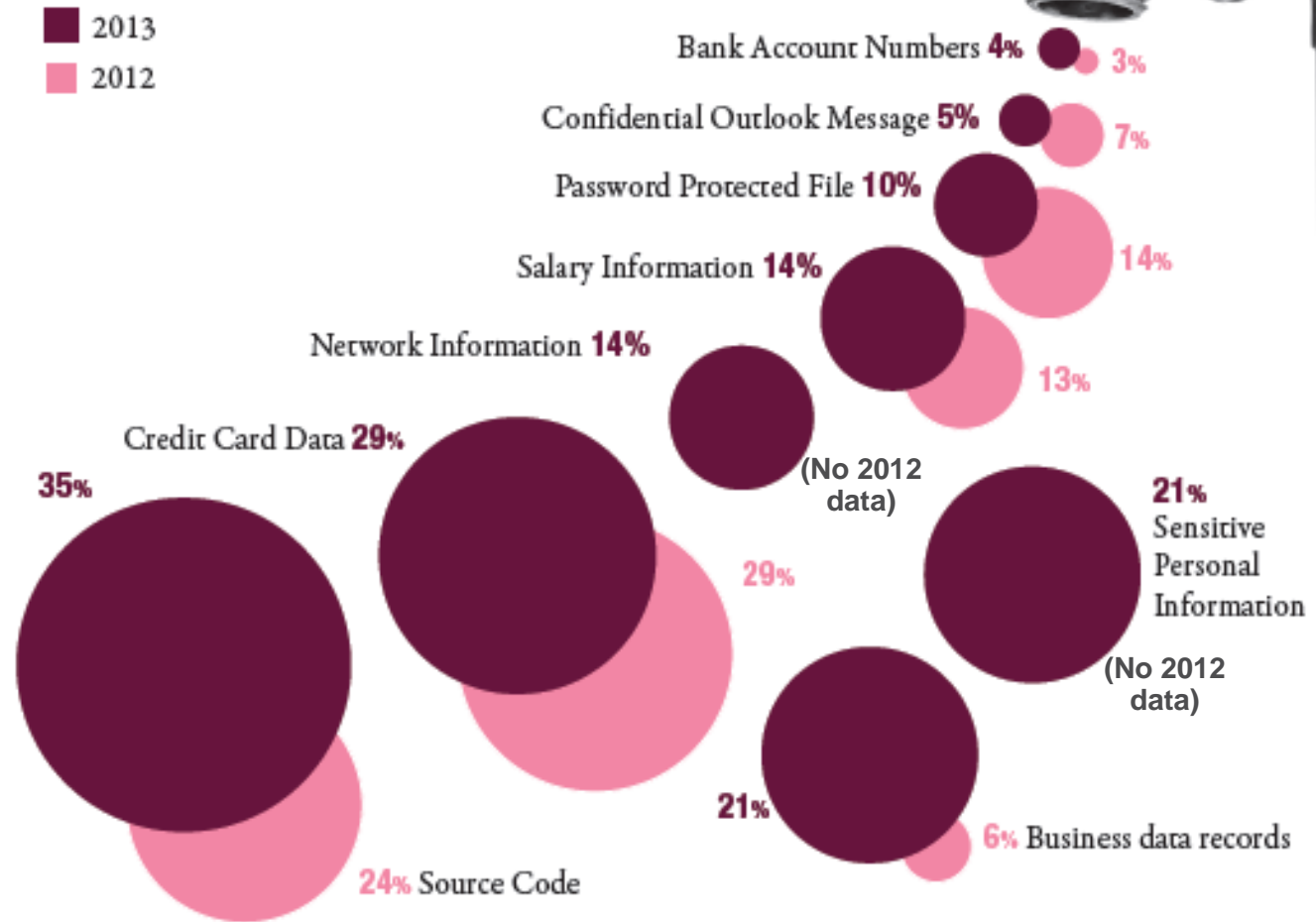- ## Every 3 minutes a bot is attempting to communicate with its C&C server

Bigger and More Entrenched Bot Infestations in 2013

77%
OF BOTS ARE ACTIVE FOR
MORE THAN 4 WEEKS

77% MORE THAN 4 WEEKS

LESS THAN 4 WEEKS **23%**

Data Loss Events Are Increasing

- 88% of organizations experienced at least one data loss event in 2013

- Economic espionage costs American companies $250-$500 million every year

MOST FREQUENTLY ATTACKED DATA TYPES

- 2013
- 2012

Bank Account Numbers **4%** **3%**

Confidential Outlook Message **5%** **7%**

Password Protected File **10%** **14%**

Salary Information **14%**

Network Information **14%** **13%**

Credit Card Data **29%**
35%

(No 2012 data)

29%

21% Sensitive Personal Information **(No 2012 data)**

21%

24% Source Code

6% Business data records

Every Hour, at the Average Organization

Sensitive data is sent outside the organization **every 49 minutes**

Unknown malware is downloaded **every 27 minutes**

Known malware is downloaded **every 10 minutes**

A high-risk application is used **every 9 minutes**

A bot communicates with its C&C server **every 3 minutes**

Hosts **access malicious web** sites **EVERY MINUTE**

ONE HOUR

Since the Start of This Talk…

At a single organization

- 12 hosts accessed a malicious Web site
- Every bot communicated with its C&C server 4 times
- Someone used a high-risk application
- At least one host downloaded a known malware

And in the next 24 hours

- 27 unknown malware files will be downloaded
- 1 more host will be infected by a bot

Take Action to Protect Your Organization in 2014

- A **free onsite network assessment** that will give you visibility into your network, uncovering incidents and risks.

- Within **as little as one hour**, we can provide a **comprehensive report** that identifies:
  - › Your current security status
  - › Active risks or security issues in your organization
  - › Suspicious activity or source of data leaks
  - › Recommendations on how to eliminate threats and resolve your security issues