



CHECK POINT 2013 SECURITY REPORT

JANUARY 2013



Check Point
SOFTWARE TECHNOLOGIES LTD.



About the research

Key findings

Security strategy

Summary

2012

2013 and beyond

Main **security threats & risks**

Security **architecture**
Recommendations



Multiple sources of data

Threat
Cloud

3D
Reports

SensorNet



A comprehensive survey

888 companies

1,494 gateways

120,000 Monitoring hours

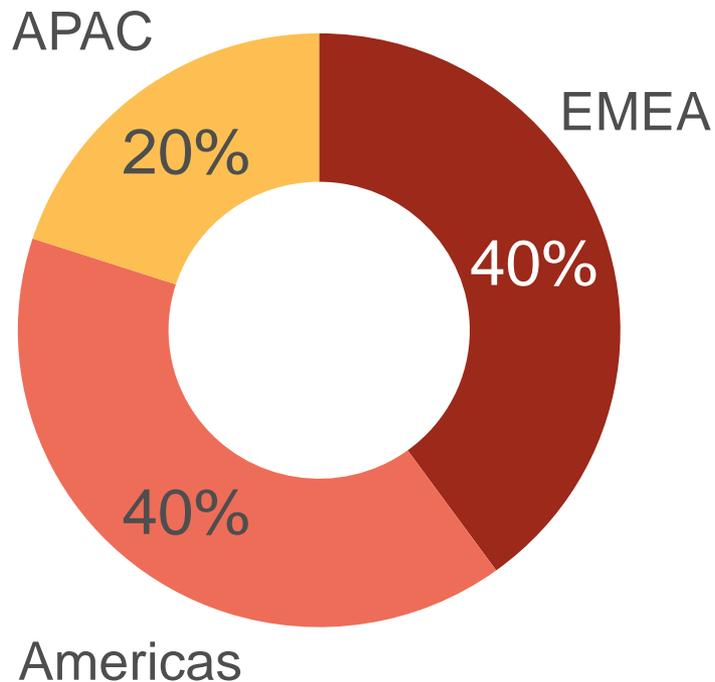
112,000,000 security events



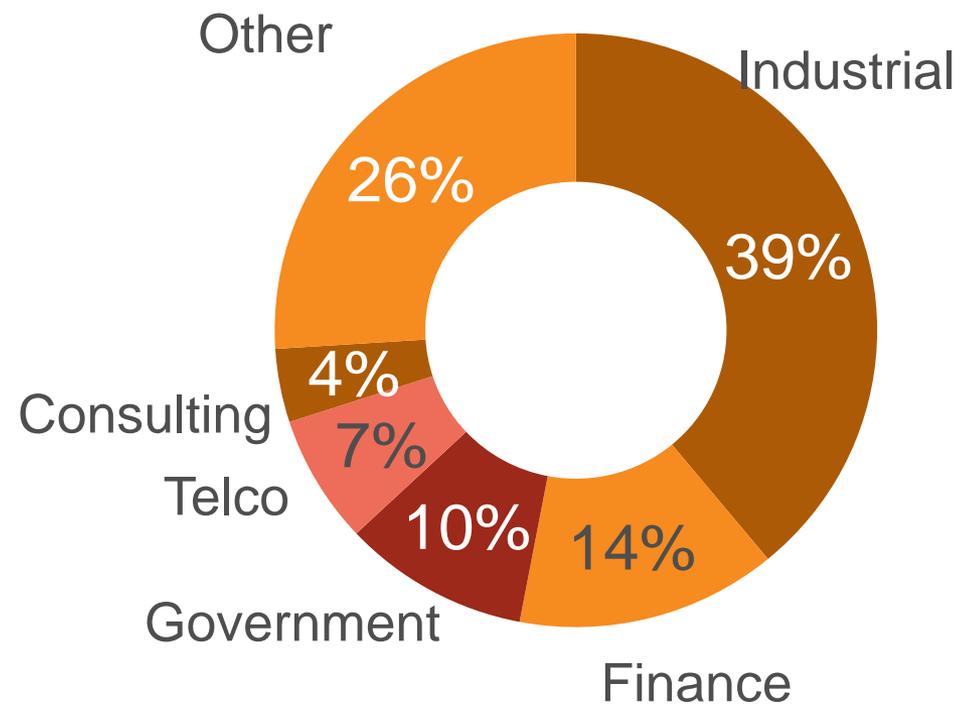
A comprehensive survey

% of companies

By geography



By sector





About the research

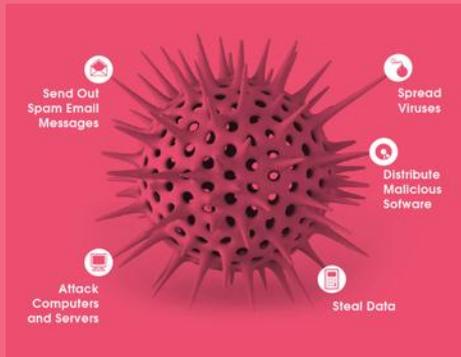
Key findings

Security strategy

Summary

We will talk about 3 issues

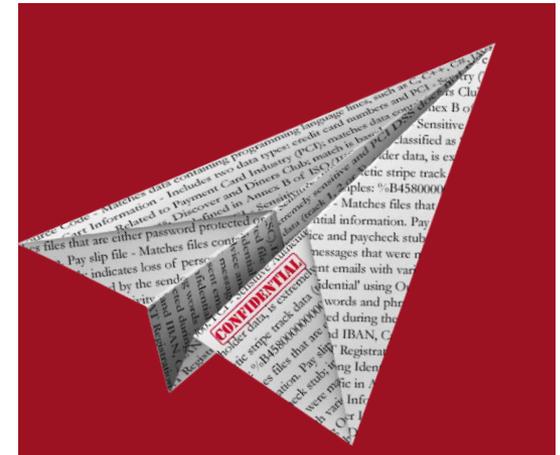
Threats to the organization



Risky enterprise applications



Data loss incidents in the network



Another day, another major hack



And then there's Anonymous





Arab Spring
Political freedom

Foxcon
Working conditions

Justice Department
Anti-corruption

Vatican
Unhealthy transmitters

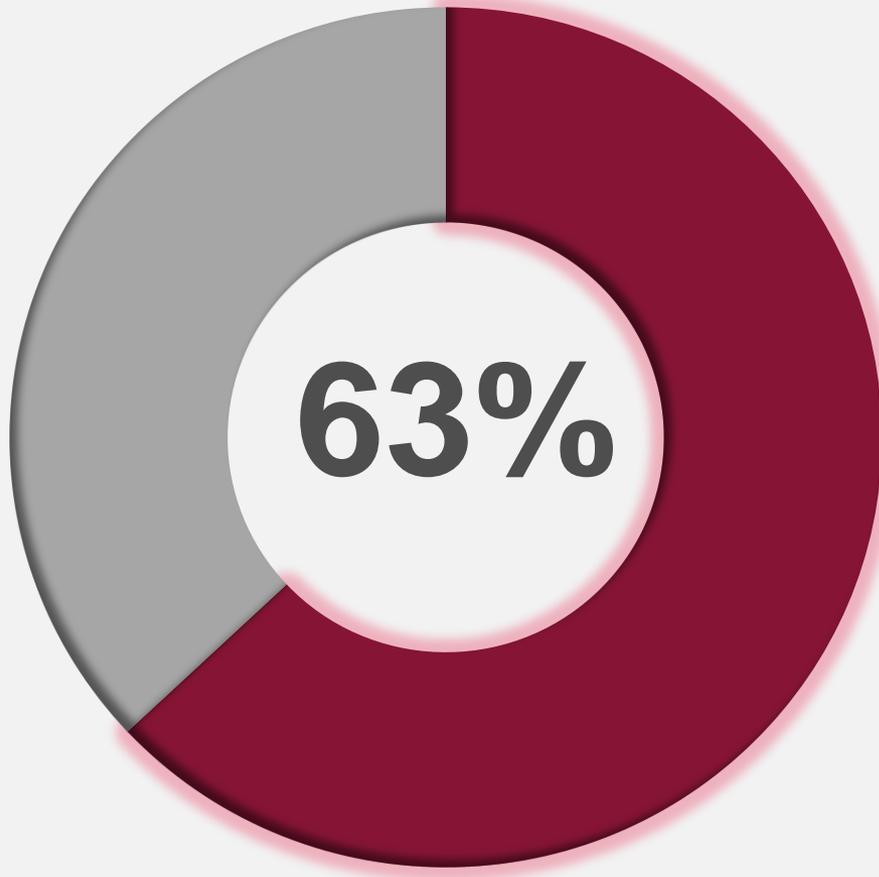
UN ITU
Internet deep packet inspection

This does not affect me, right?



The majority of companies are infected

100% = 888 companies



of the
organizations
in the
research
were infected
with bots

Once in ... always on



ZWANGI

Impose unwanted advertising

ZEUS

Steal online banking credentials

SALITY

Self-spreading virus

KULUOZ

Remote execution of malicious files

PAPRAS

Steal financial information,
gain remote access

JUASEK

Remote malicious actions
(search, delete files)



Exploit kits are easy to buy

Rental costs

One day – 50\$

Up to 1 month – 500\$

3 month – 700\$

Available
online



But there is more than Bots, right?

How does malware get to my network?





**Every 23 minutes,
a host
accesses a
malicious site**

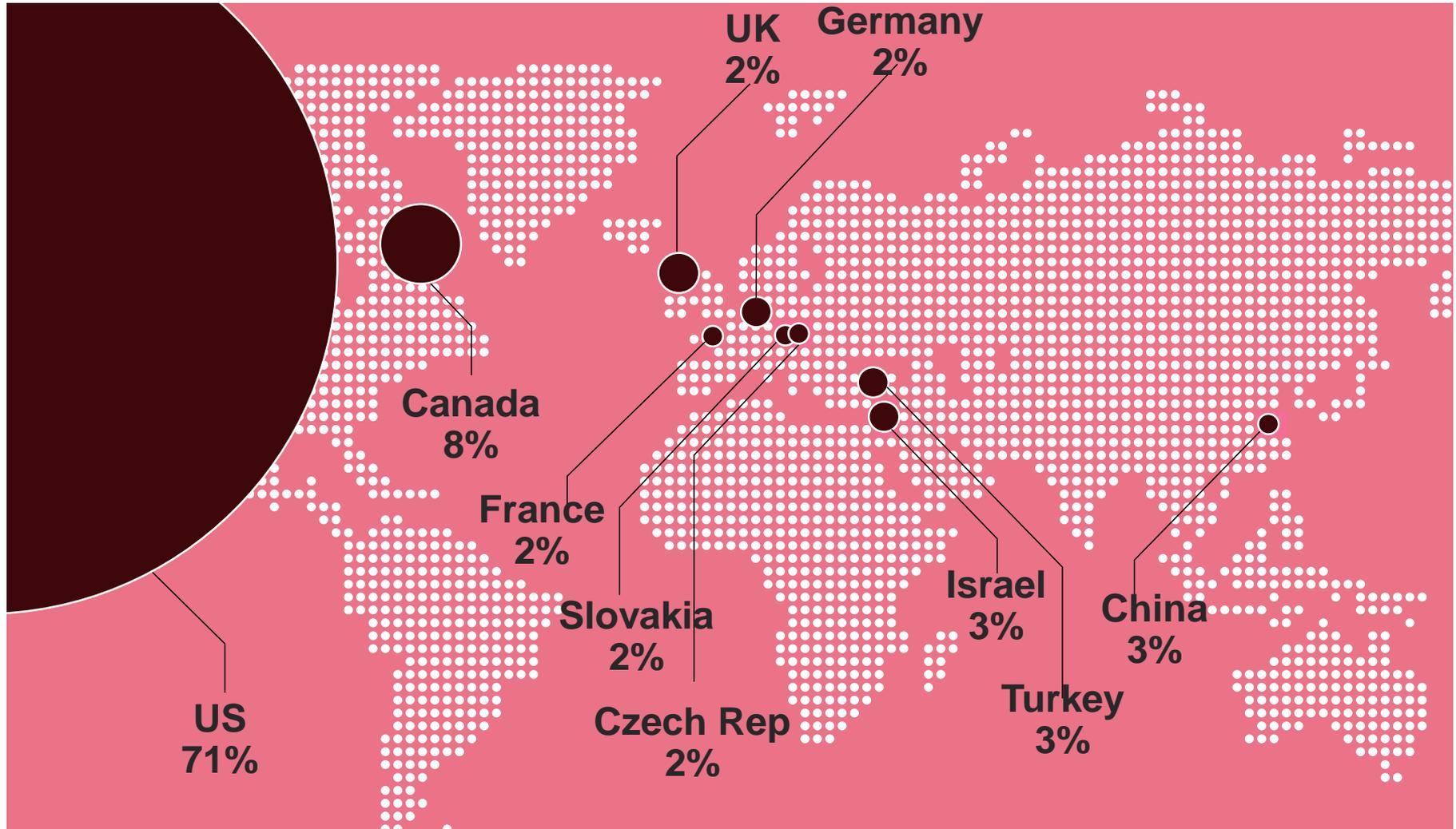


53%

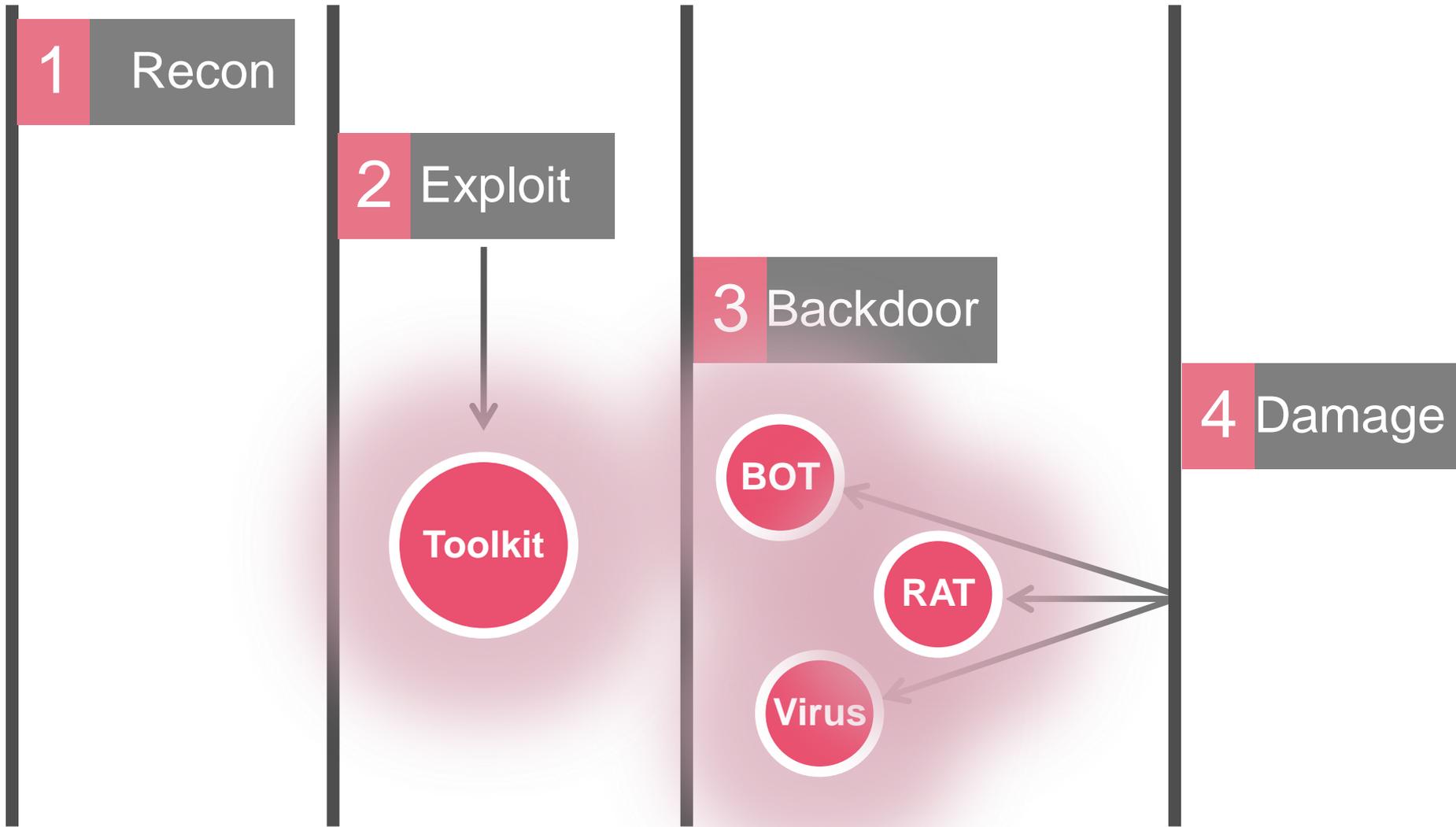
of organizations saw
malware downloads

Most attacks originate in the US

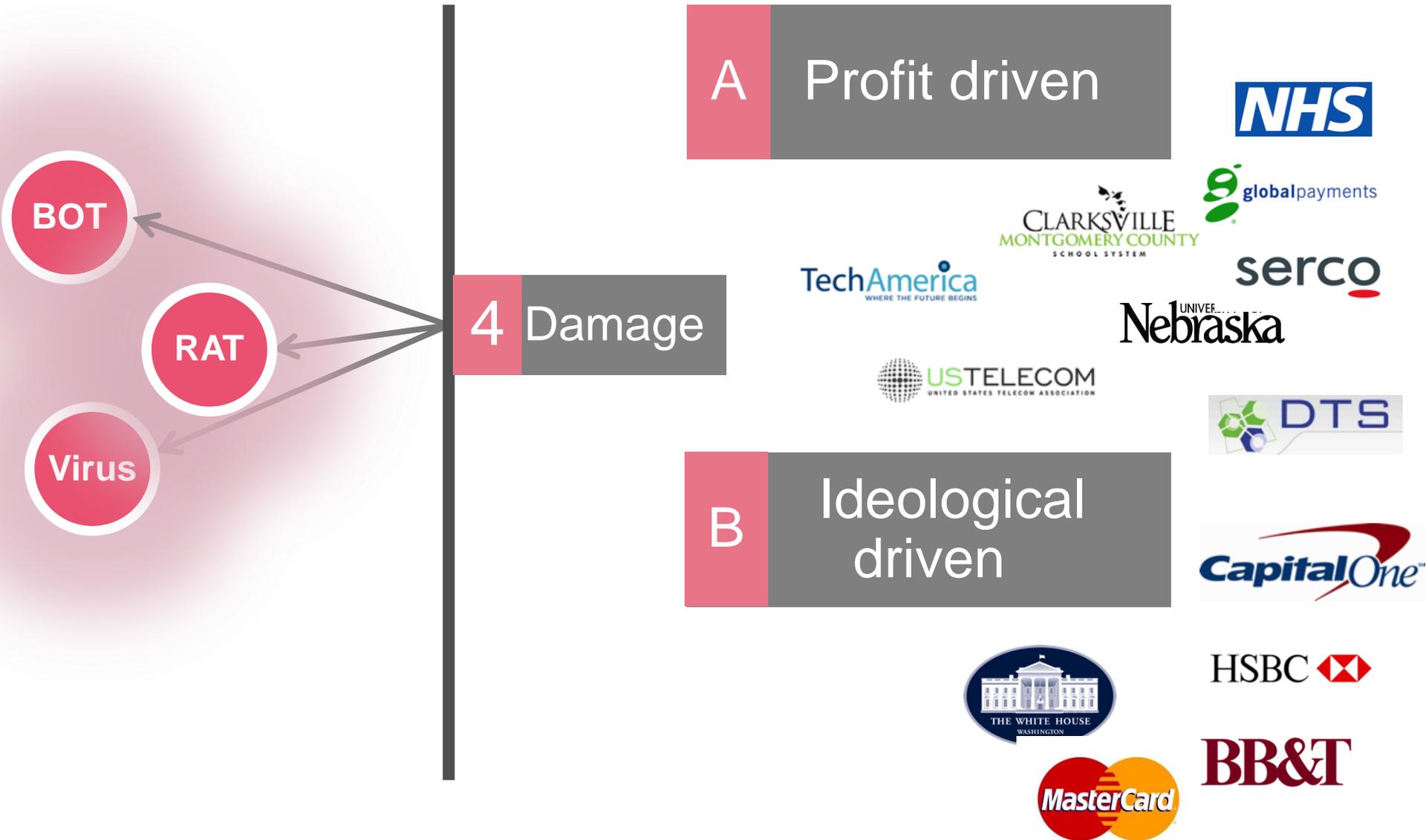
Top malware locations, %



Anatomy of an attack



Two major trends

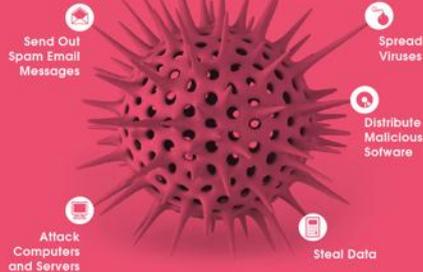


We will talk about 3 issues

Threats to the organization

Risky enterprise applications

Data loss incidents in the network



No longer a game



What are risky applications?

Bypassing security or
hiding identity

P2P file sharing

Anonymizers

Do harm without
the user knowing it

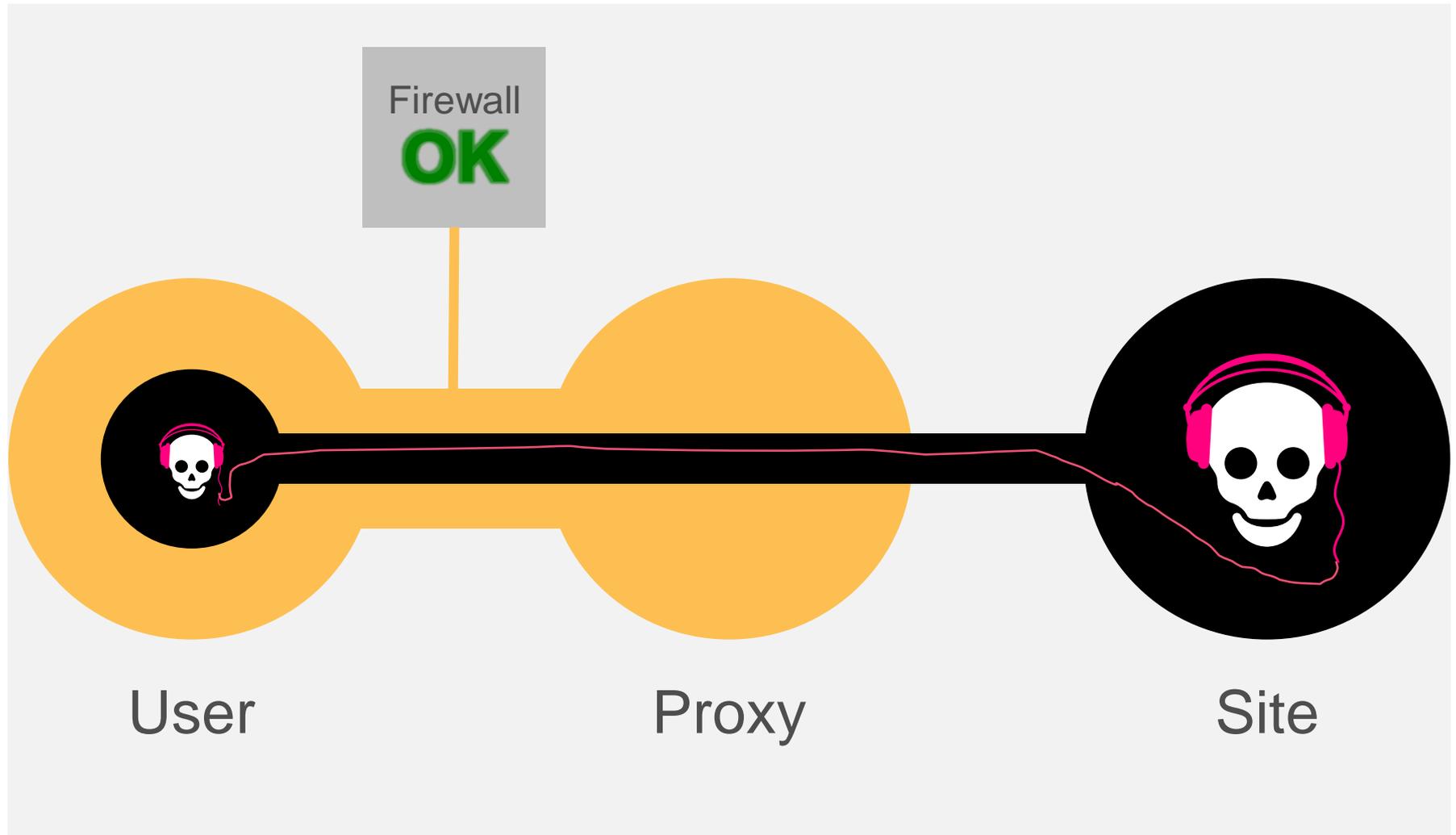
File sharing / storage

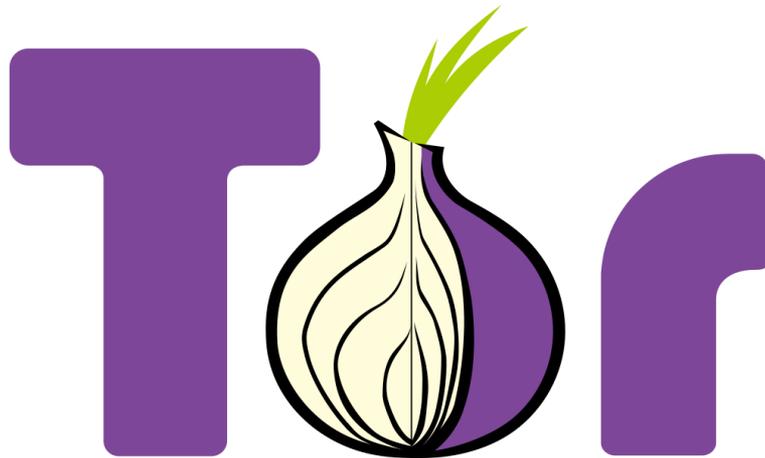
Social networks



Anonymizers

What is an anonymizer?





Began as “The Onion Router”

Officially sponsored by the US Navy

80% of 2012 budget from US Government

Used widely during Arab Spring

The risk of anonymizers



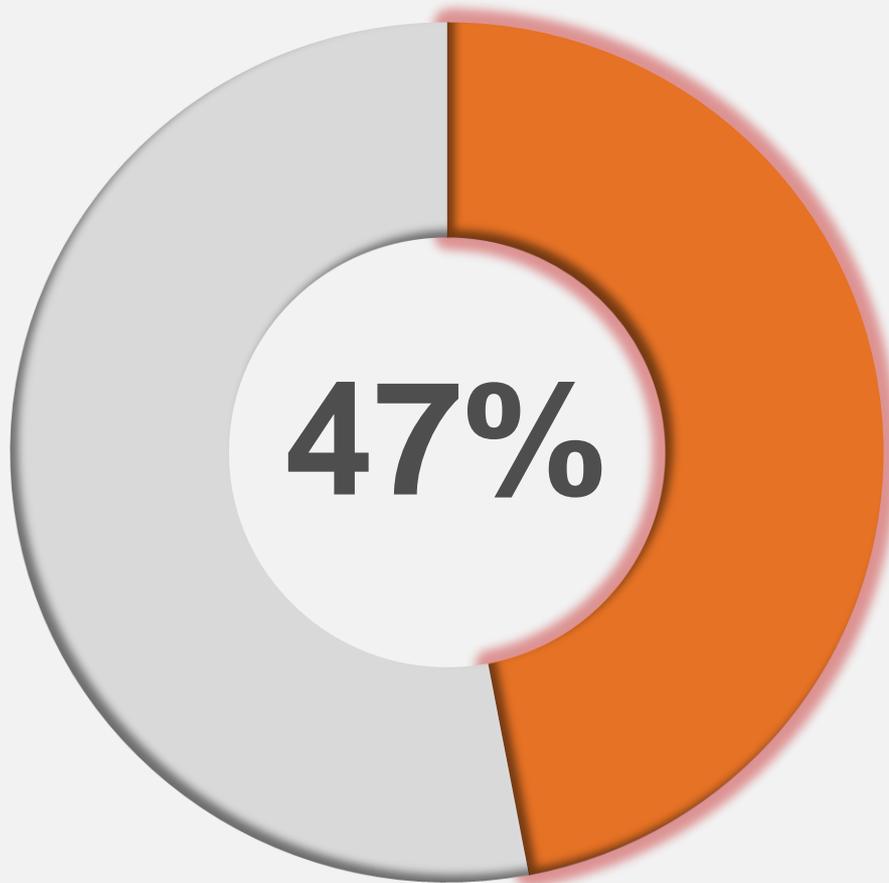
Bypasses security infrastructure

Used by botnets to communicate

Hide criminal, illegal activity

Anonymizers inside the corporation

100% = 888 companies



of organizations
had users of
Anonymizers

(80% were not aware that
their employees use
Anonymizers)

P2P file sharing

The Risk of P2P Applications

Downloading
the latest
“24” episode
right now 😊

“Back door” network access

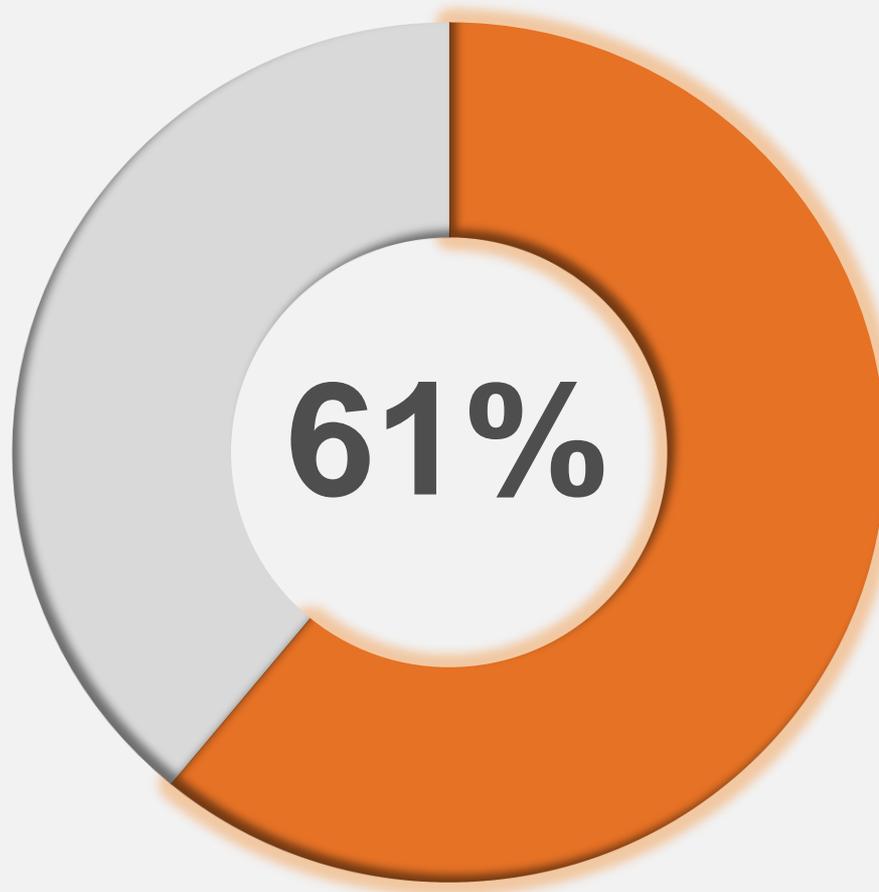
Pirated content liability

Malware downloads



P2P inside the corporation

100% = 888 companies



of organizations
had a P2P file
sharing app in
use



Fines for information disclosers



3,800
personal details shared
on P2P



95,000
personal details shared
on P2P

61%

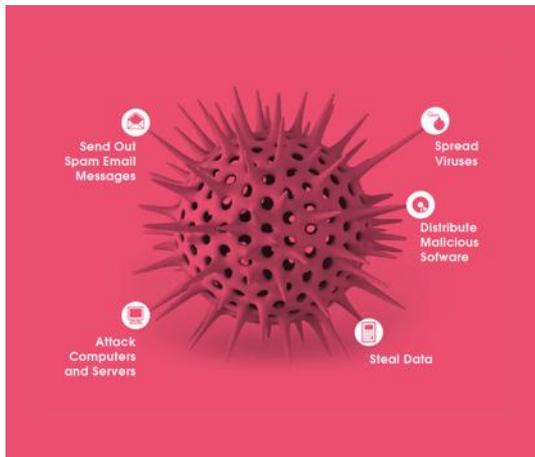
of organizations had a P2P
file sharing app in use

47%

of organizations had users of
anonymizers

We will talk about 3 issues

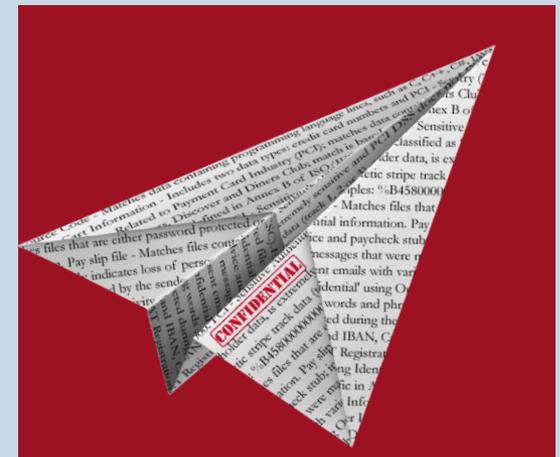
Threats to the organization



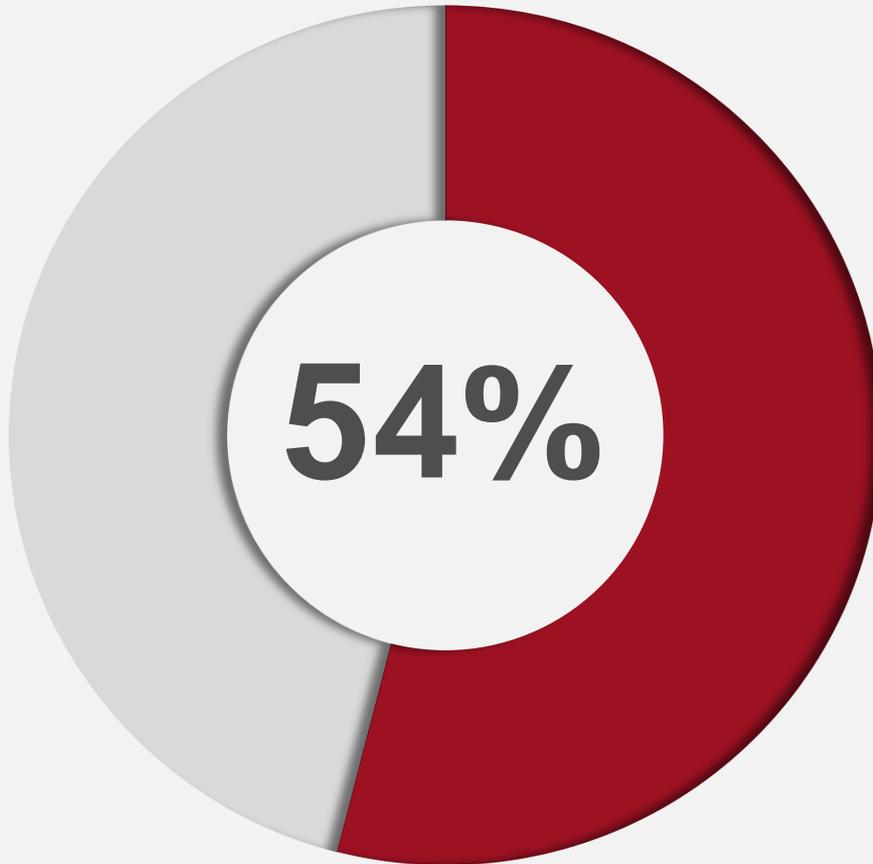
Risky enterprise applications



Data loss incidents in the network

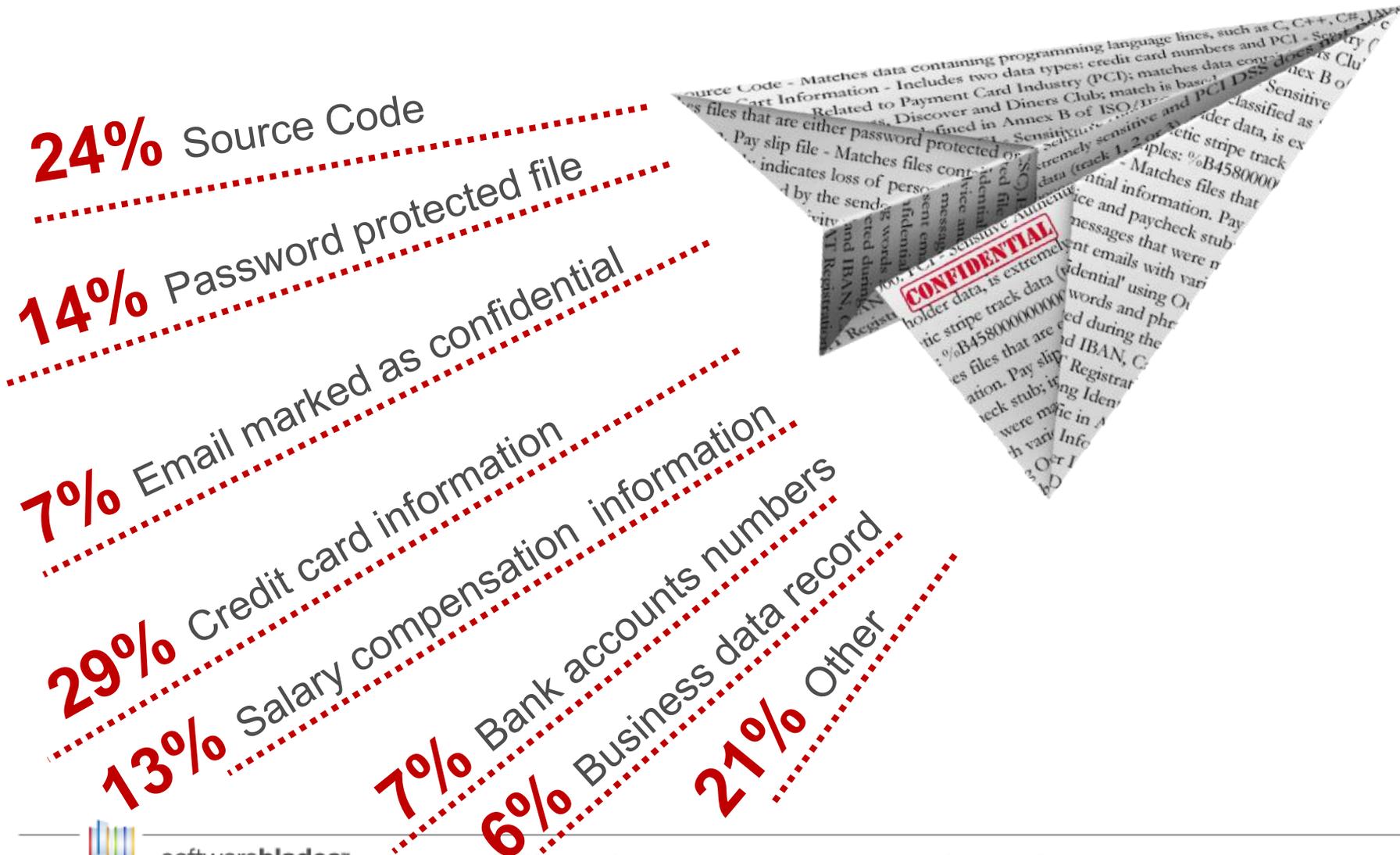


How common is it?



of organizations
experienced data
loss

Many types of data leaked



PCI compliance can be improved



36%

Of financial organizations sent credit card data outside the organization

Case examples: oops, wrong address



11 emails for a lawyer to the wrong address

**Oct
2012**

DAILY YOMIURI

Worker fired for sending sensitive information to the wrong people

**Oct
2012**



GPA's of all students leaked to hundreds of unintended recipients

**Apr
2012**



Accidentally leaked 4,000 student social security numbers

**Apr
2012**

We have all had this problem

Error 552: sorry, that message exceeds my maximum message size limit



Dropbox?



youSENDit

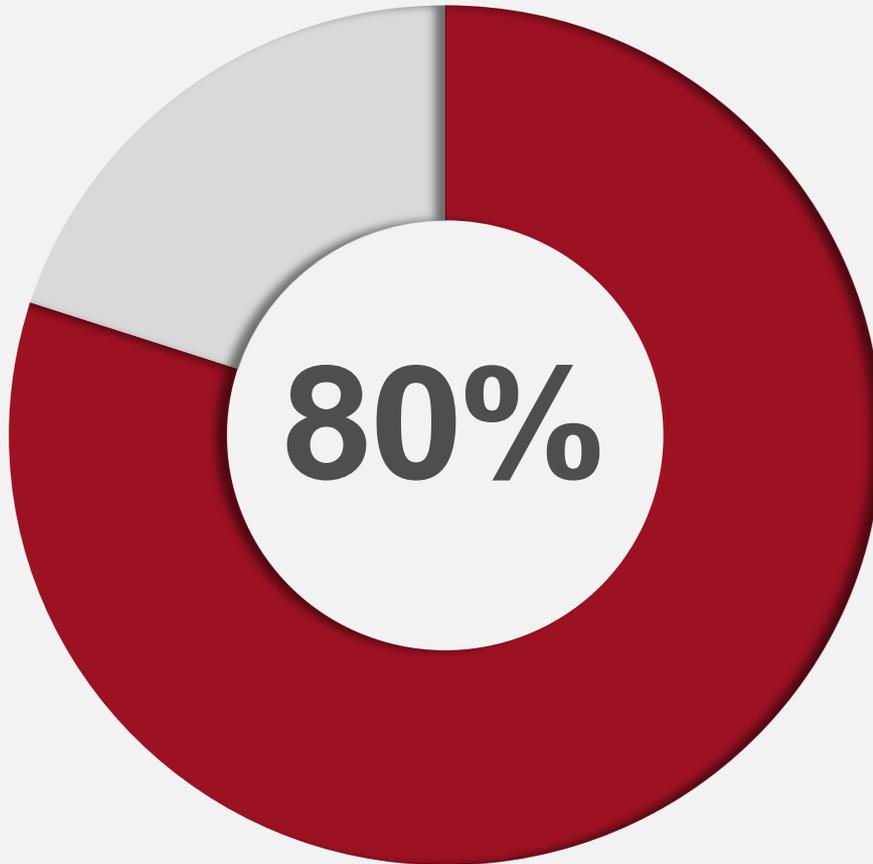
YouSendIt?



Windows Live?

Storing and Sharing applications

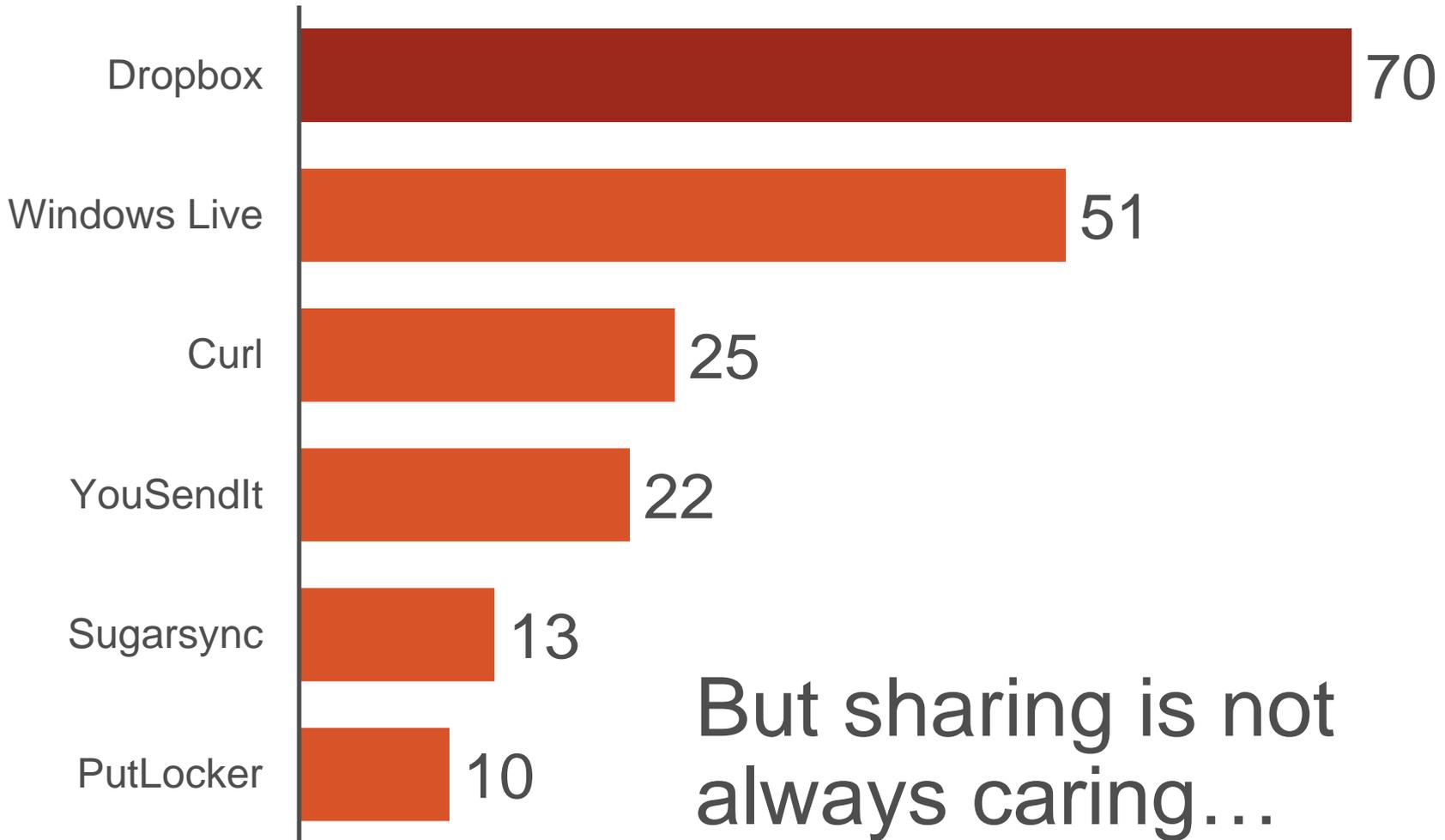
100% = 888 companies



of organizations
use file storage
and sharing
applications

Top sharing and storage apps

% of organizations





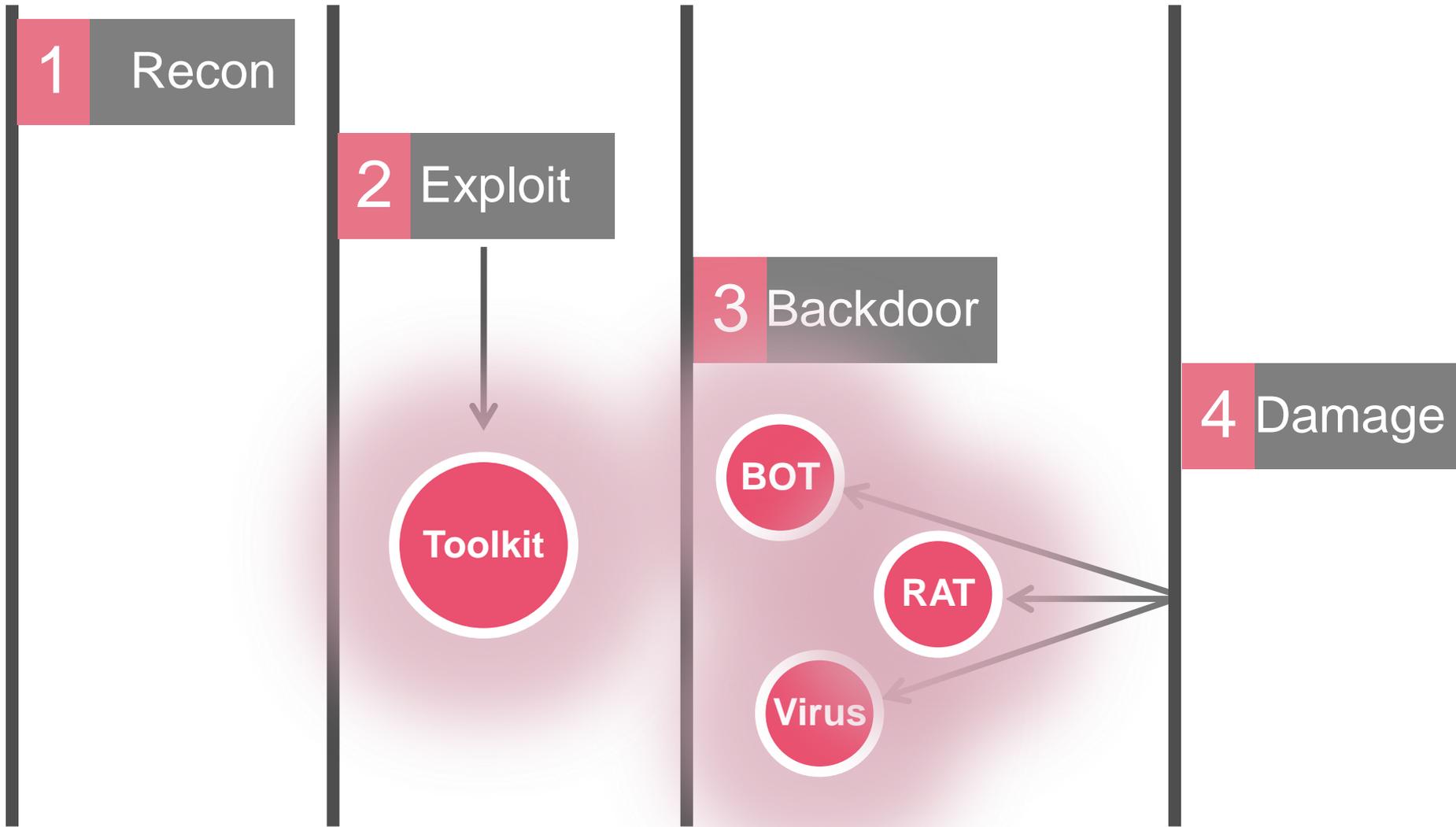
About the research

Key findings

Security strategy

Summary

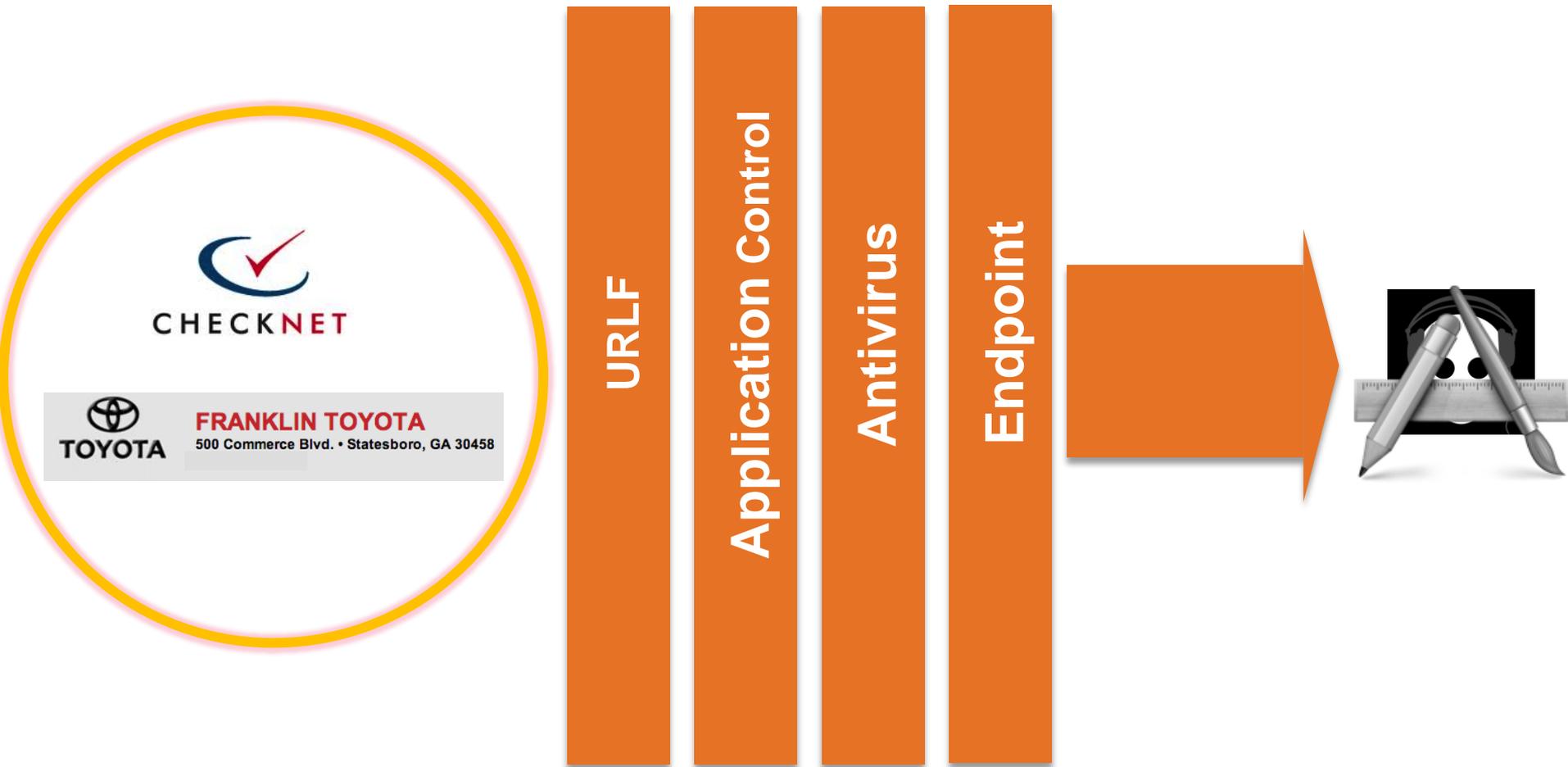
Anatomy of an attack



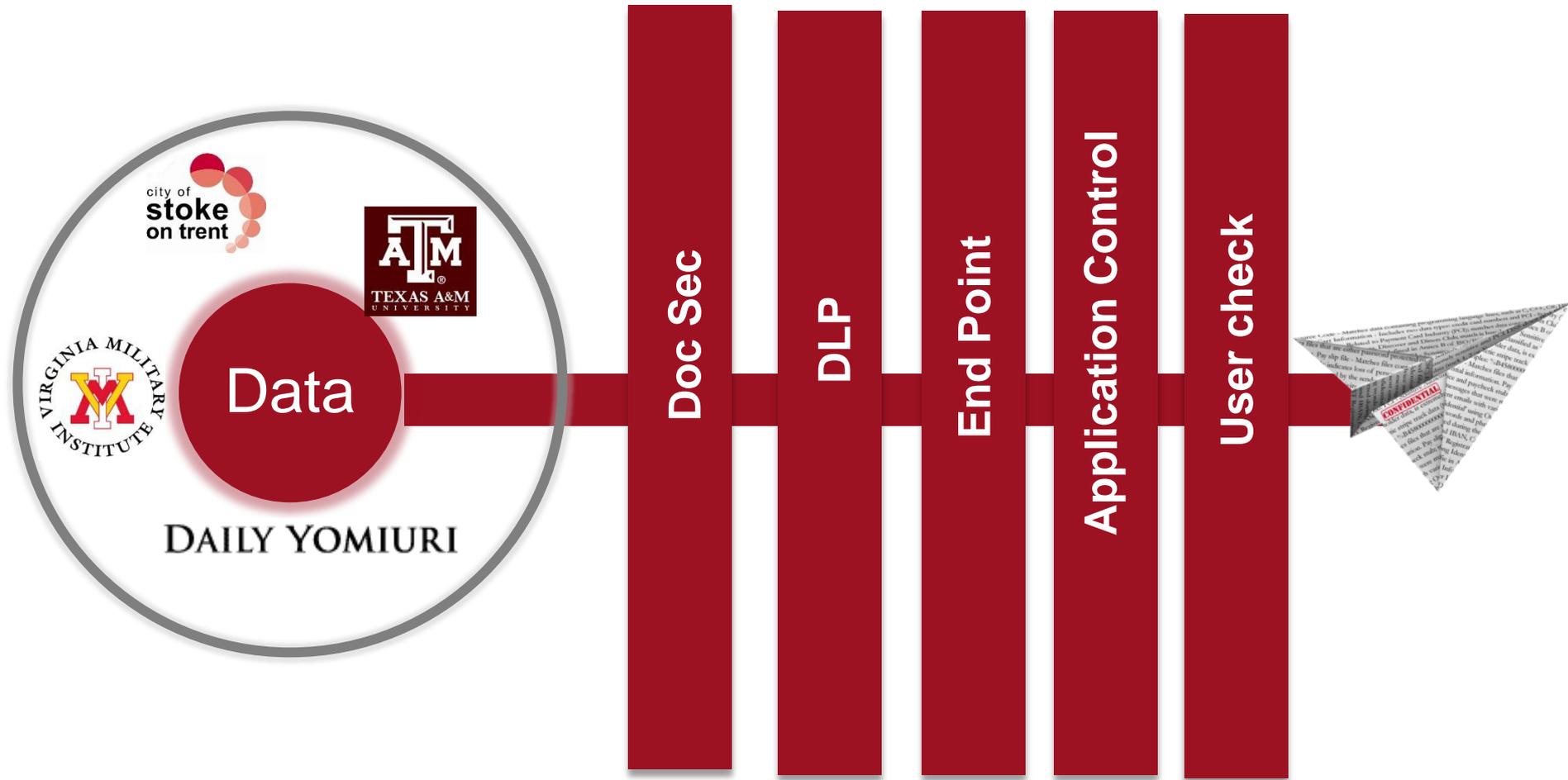
Addressing external threats



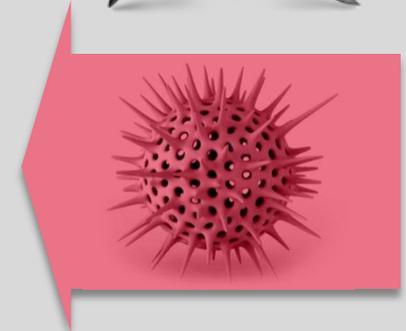
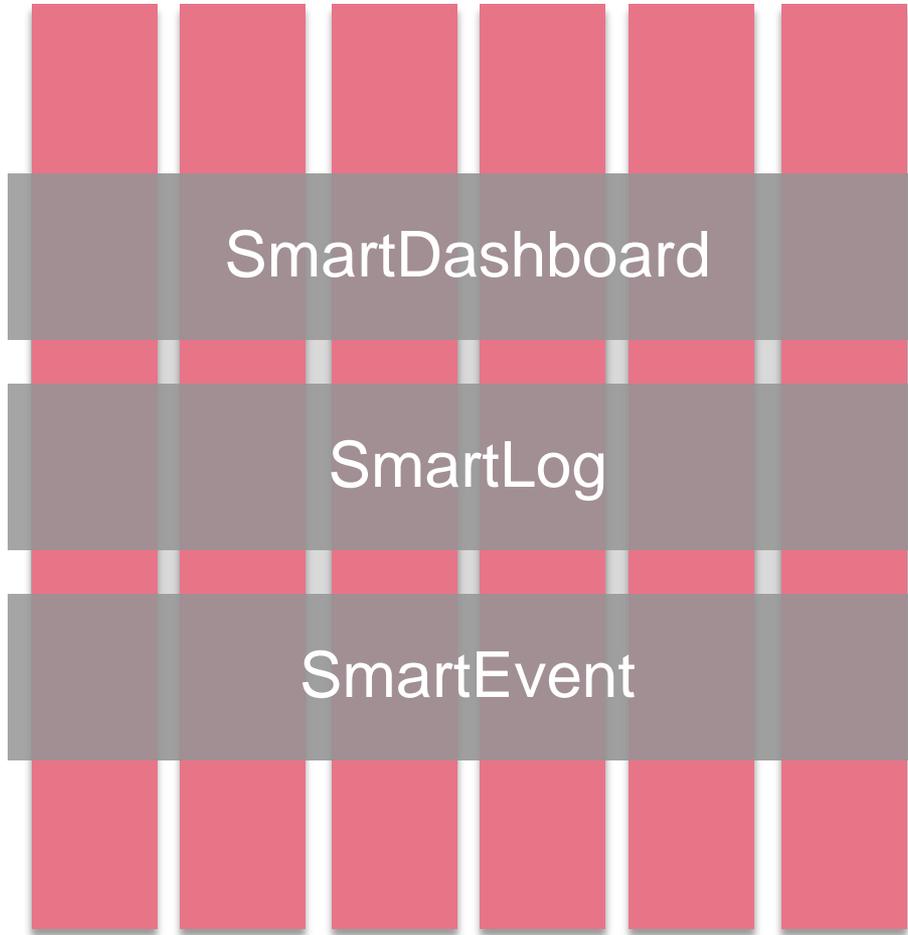
Enabling secure application use



Preventing data loss



Seeing attacks and protections



**Threats
to the
organization**

**Risky
enterprise
applications**

**Data loss
incidents in the
network**

63%

infected with
bots

47%

used
Anonymizers

54%

had a data
loss event



About the research

Key findings

Security strategy

Summary

Summary – Great Sales Tool

3 key Takeaways

63%

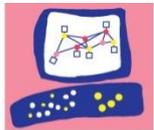
Infected with bots

47%

Used Anonymizer

54%

Experienced data leak



Check Point
SOFTWARE TECHNOLOGIES LTD.

Protect from external threats

Prevent access to bad sources

Keep the organization secured

Manage & Monitor

Multi Layer Security Central Management





CHECK POINT 2013 SECURITY REPORT

JANUARY 2013



Check Point
SOFTWARE TECHNOLOGIES LTD.