



# ISTR

Internet Security Threat Report

**Davor Kodrnja**  
Regional Sales Manager SEE



In 2009 there were  
**2,361,414**  
new piece of malware created.

---

In 2015 that number was  
**430,555,582**

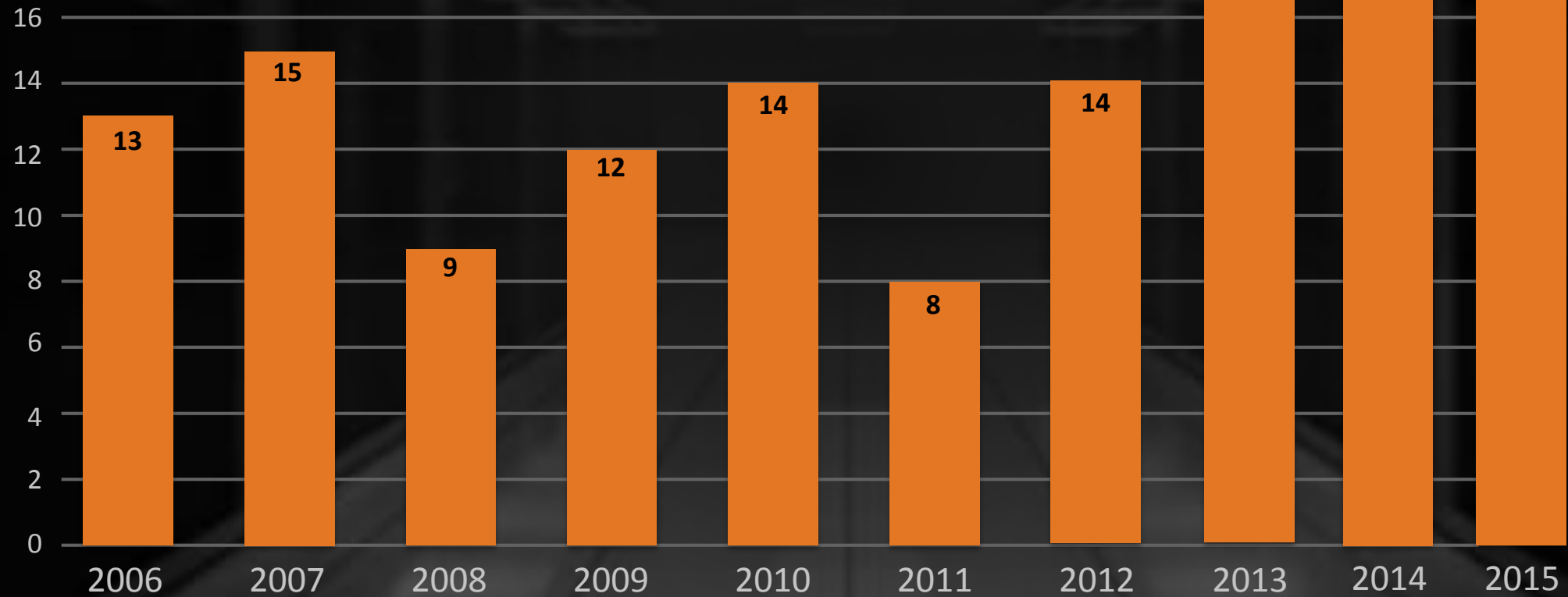
---

That's  
**1 Million 179 Thousand**  
a day.

---

# 1. Zero-Days

# Zero-Day Vulnerabilities



54

## Hackers Unleash Trove of Data from Hacking Team

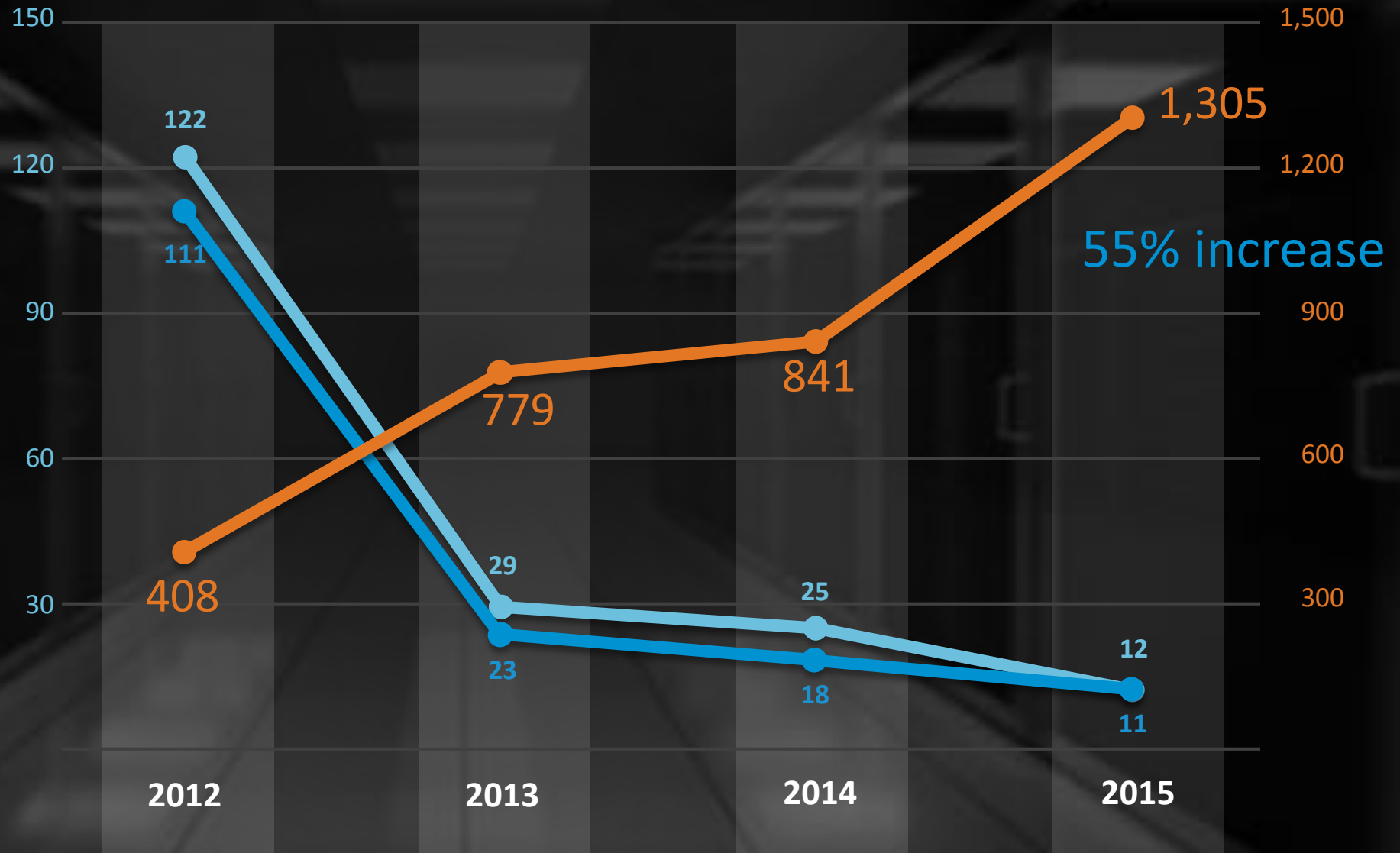
- HackingTeam (HT) had zero days in Adobe Flash, Internet Explorer and Microsoft Windows

CVE	Affected Product	First Notice	Patch Date
CVE-2015-5119	Adobe Flash	July 7	July 8
CVE-2015-5122	Adobe Flash	July 10	July 14
CVE-2015-5123	Adobe Flash	July 10	July 14
CVE-2015-2425	Internet Explorer	July 14	July 14
CVE-2015-2426	Microsoft Windows	July 20	July 20
CVE-2015-2387	Microsoft Windows	July 8	July 14

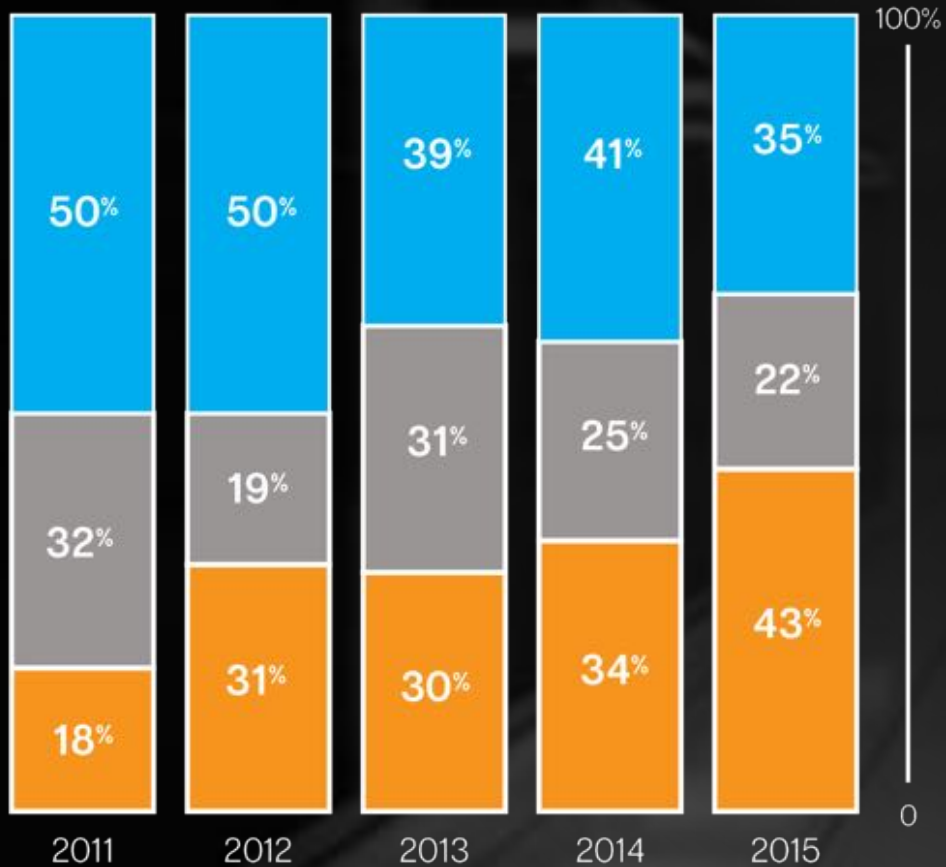
## 2. Targeted Attacks

# Targeted Attack Campaigns

- Average Number of Email Attacks Per Campaign
- Recipients per Campaign
- Campaigns



# Spear-Phishing Attacks by Size of Targeted Organization



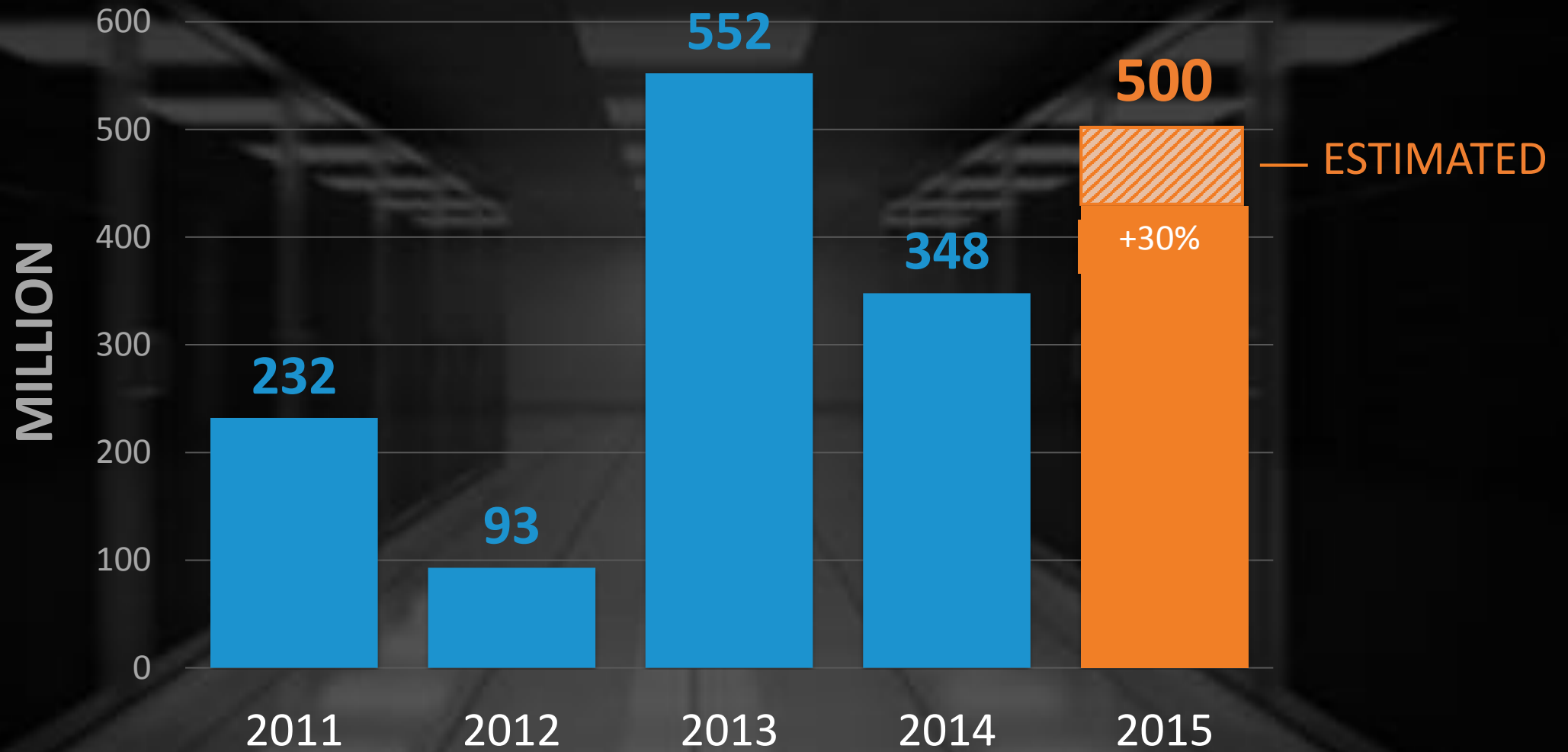
Org Size	2015 Risk Ratio	2015 Risk Ratio as Percentage	Attacks per Org
Large Enterprises 2,500+ Employees	<b>1 in 2.7</b>	<b>38%</b>	<b>3.6</b>
Medium Business 251-2,500 Employees	<b>1 in 6.8</b>	<b>15%</b>	<b>2.2</b>
Small Business (SMB) 1-250 Employees	<b>1 in 40.5</b>	<b>3%</b>	<b>2.1</b>





# 3. Breaches

# Total Identities Exposed



# Mega Breaches 2015





# 4. Vulnerabilities

## Scanned Websites with Vulnerabilities ...

2013  
**77%**  
–

2014  
**76%**  
-1% pts

2015  
**78%**  
+2% pts



## ... Percentage of Which Were Critical

2013  
**16%**  
–

2014  
**20%**  
+4% pts

2015  
**15%**  
-5% pts



# 5. Ransomware

# Evolution path

## MISLEADING APP



2005-2009

“FIX”

## FAKE AV



2010-2011

“CLEAN”

## LOCKER RANSOMWARE



2012-2013

“FINE”

## CRYPTO RANSOMWARE



2014-2015

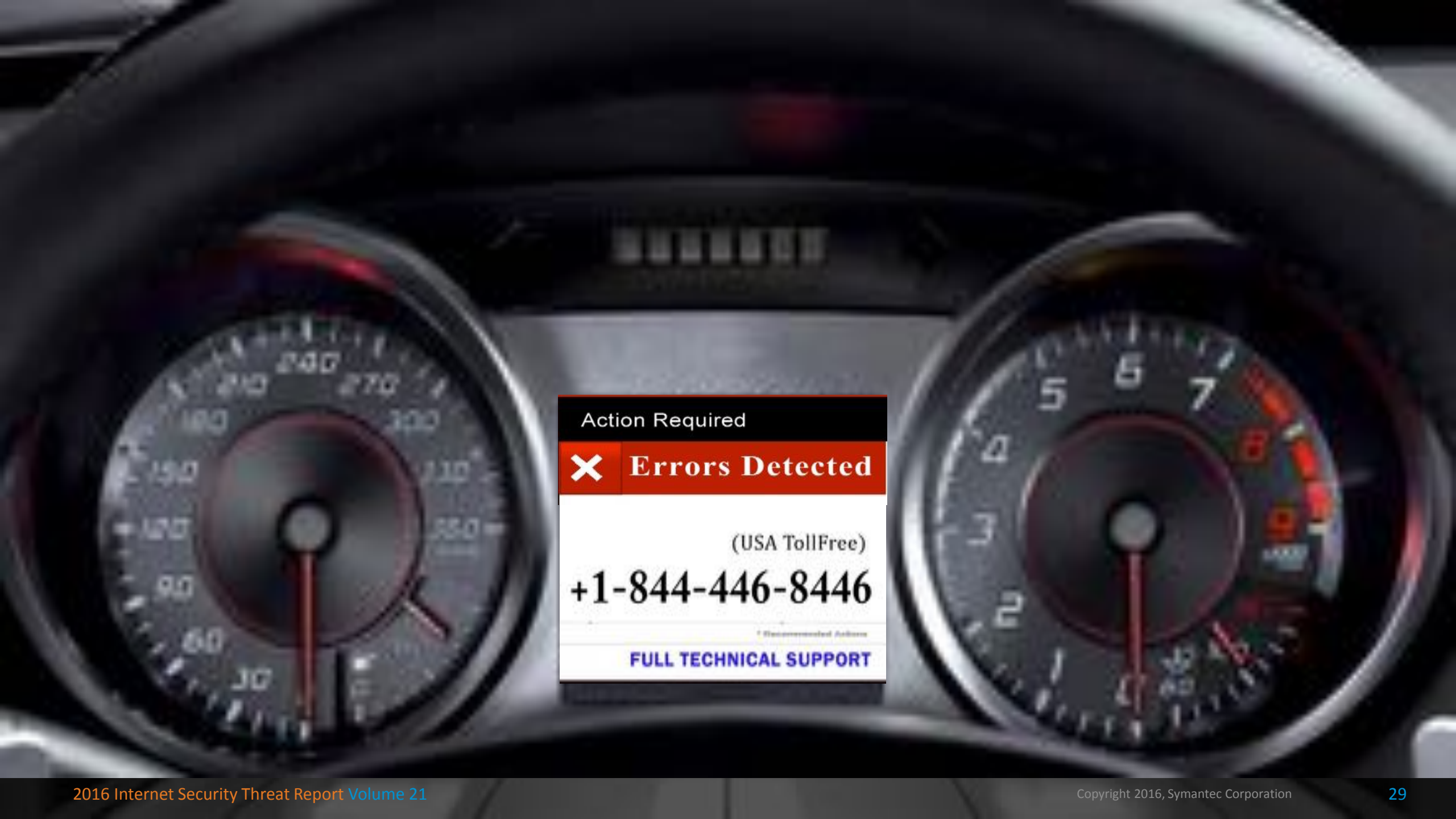
“FEE”

# 35% Increase in Crypto-Ransomware Attacks





# 6. Consumer Scams



Action Required

**✘ Errors Detected**

(USA TollFree)


**+1-844-446-8446**

\* Recommended Action

**FULL TECHNICAL SUPPORT**



# Security Response Blog

 Symantec Official Blog

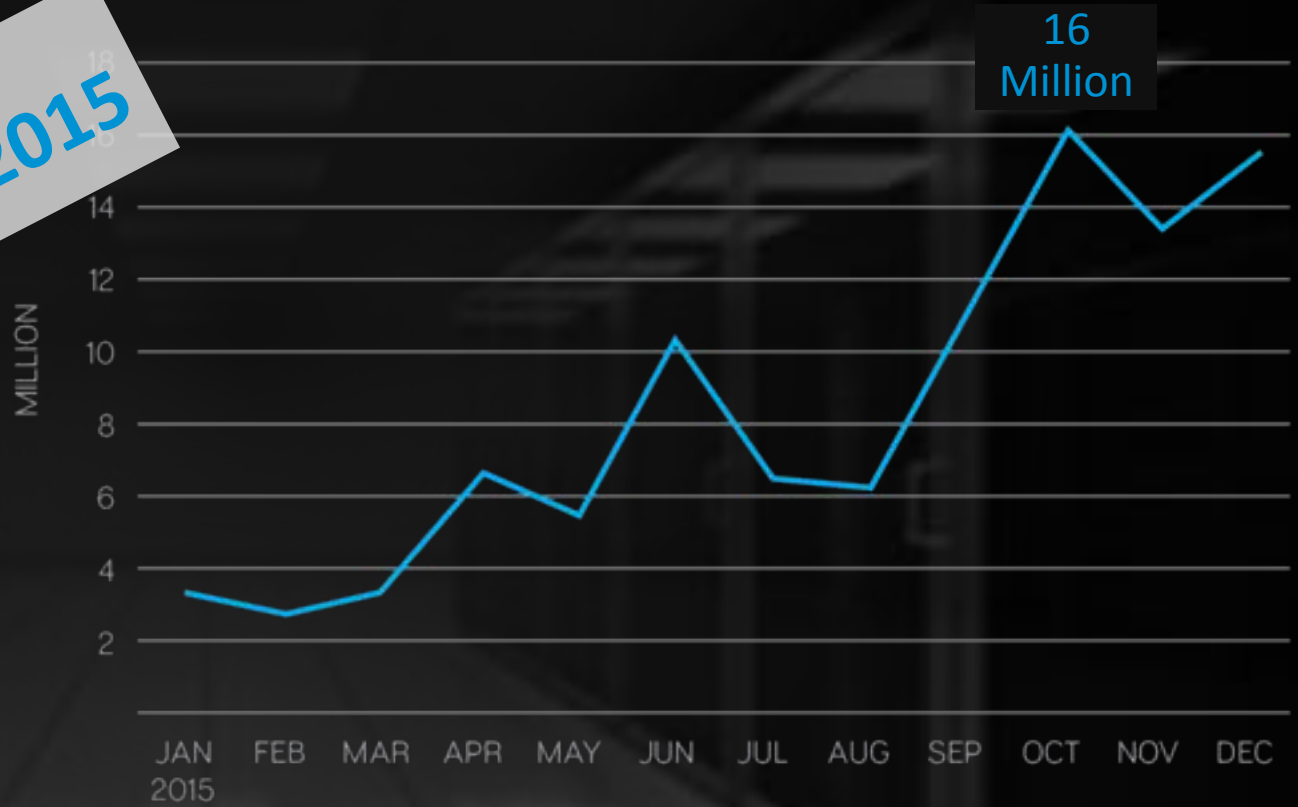
## Technical Support Phone Scams

By: **Orla Cox**  **SYMANTEC EMPLOYEE**

Created 22 Jun 2010

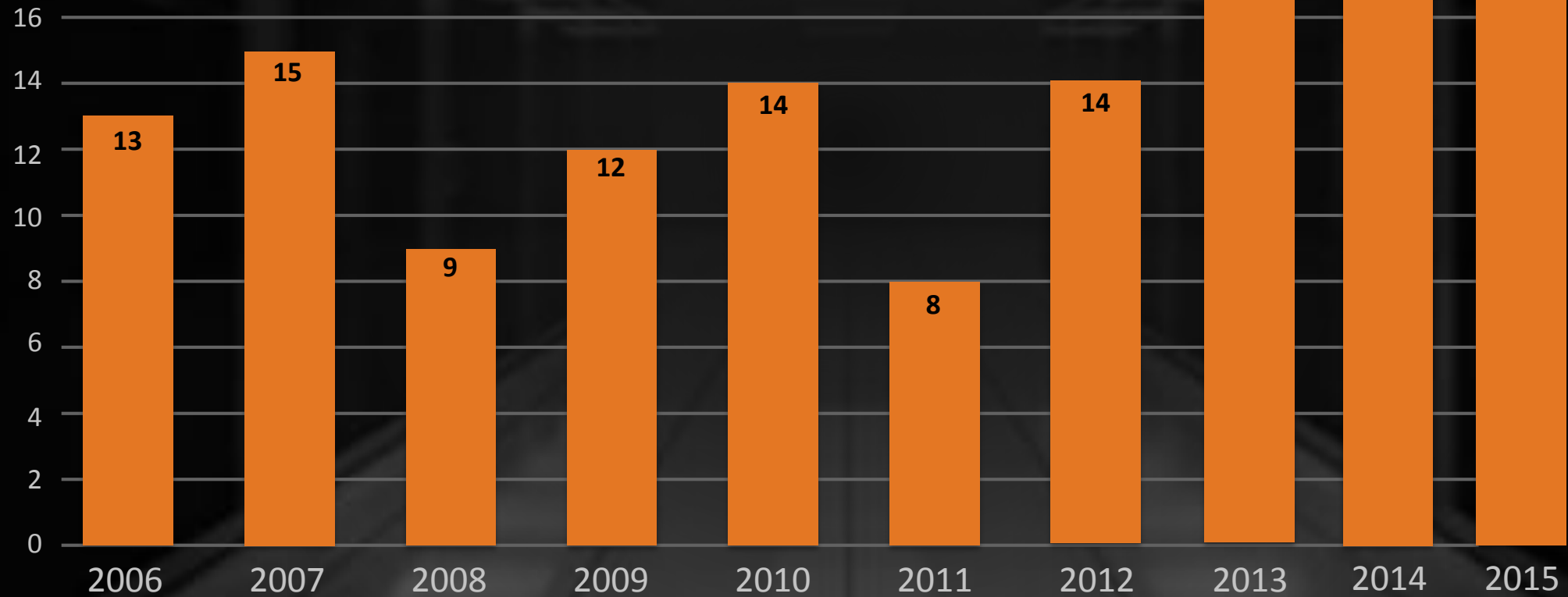
# Blocked Tech Support Scams

**100 MILLION BLOCKED in 2015**



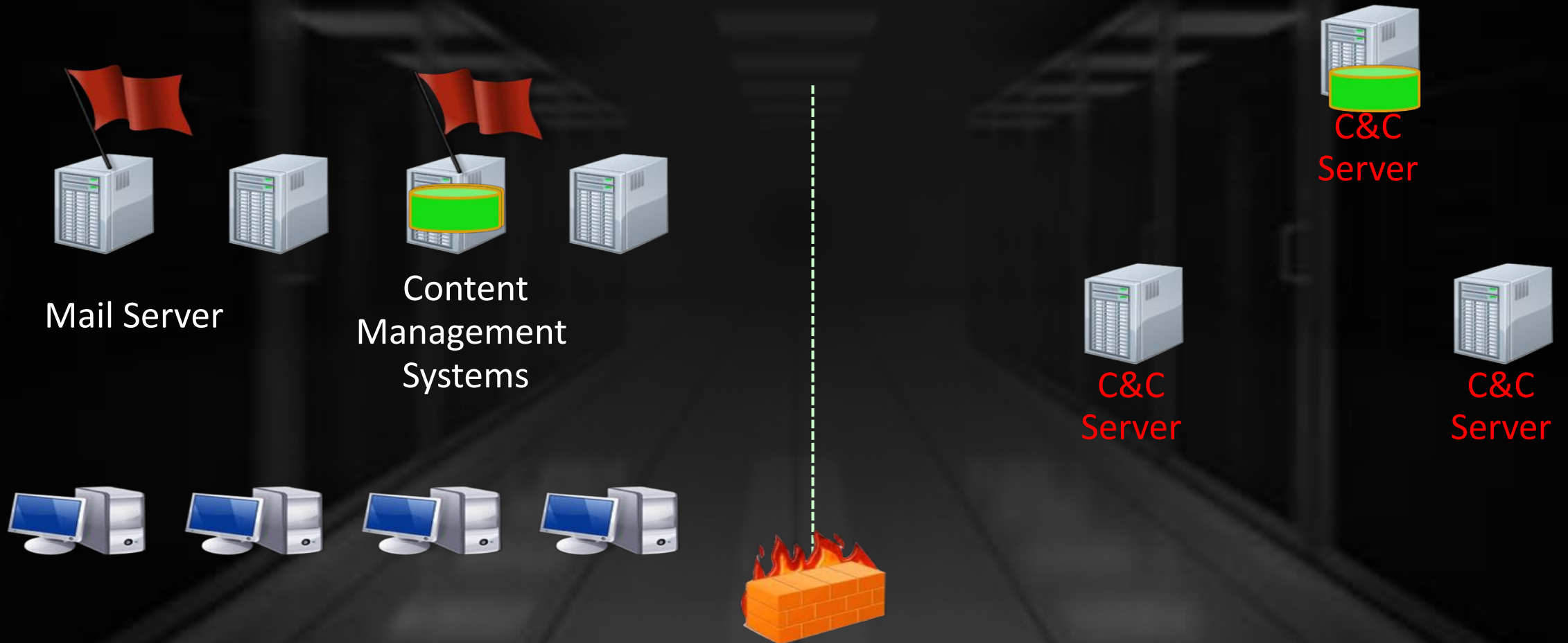
# 7. Professionalization of Cyber Crime

# Zero-Day Vulnerabilities



54

# Butterfly – Command & Control Operations





# Hacktool.MultiPurpose

## General options

\*\*\*\*\*

- install: install server on local host and load it
- host <host>: hostname or IP (local host if not set)
- password <password>: server password connection (mandatory)
- forcerload: load server on local host without test

## Server options


\*\*\*\*\*

--cmd: server command:

dump: dump stuff:

- sam: fetch LM/NTLM hashes
- machines: fetch machines hashes
- history: fetch history for LM/NTLM hashes
- sh: fetch logon sessions hashes
- sp: fetch security packages cleartext passwords
- accounts: <account list>: with --sam, specify accounts to dump  
(comma separated)
- lsa: fetch LSA secrets

# Tech Support Scams – Outbound Call Centers (Boiler Rooms) to Support the Scam



Hello sir,  
Your computer is infected.  
Please purchase a support  
plan for \$75 so we can help  
you...

# TeslaCrypt Ransomware – Technical Support Available

**TESLACRYPT**

## All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD.  
Your Bitcoin address for payment: 1LyjW5wyapoC3j9R6zDip6cDcZ7gM05

[PURCHASE PRIVATE KEY WITH BITCOIN](#)

You can also make a payment with PaysafeCard or Ukash

In case of payment with PaysafeCard or Ukash your total payment is € 400

[PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH](#)

Payment verification may take up to 12 hours.

**Support**  
[Message Center](#)

### Try to decrypt your file here

You can test the decryption service once for FREE.

# Dridex Gang - Number of Known Spam Runs Per Day



**When Cyber Criminals**

**Work in Call Centers, Write Documentation and Take  
the Weekends Off**

**You Know its a Profession**

**Davor Kodrnja**

davor\_kodrnja@symantec.com

**Hvala!**



**Copyright © 2016 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.