Check Point
SOFTWARE TECHNOLOGIES LTD.

ThreatCloud Emulation Service

LOCAL SOLUTION

Advanced Protection

Against The Unknown

Christof Jacques – Check Point
Strategic Account Manager Belgium/Luxembourg

The Luxembourg Slide - Disclaimer

Whenever you see the word “Cloud”

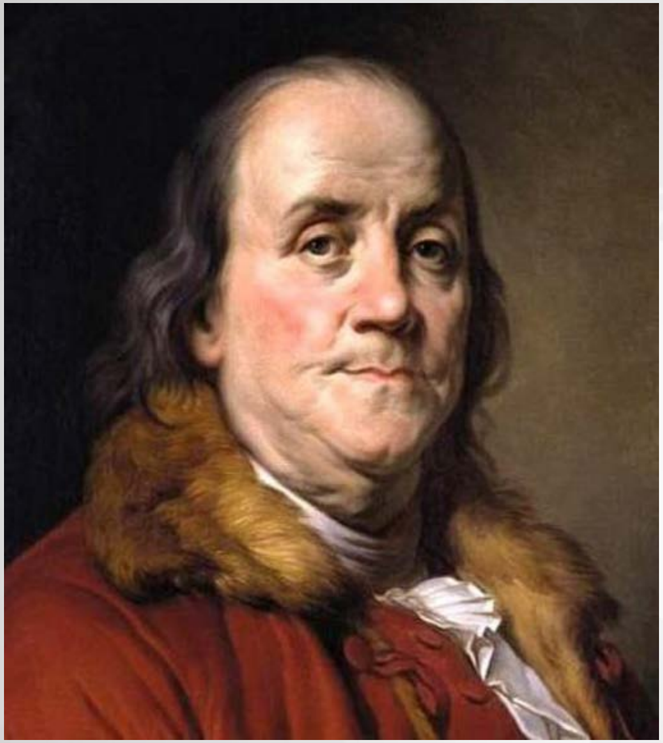
CHECK POINT
THREATCLOUD™

Please read it as “Local Solution”

LOCAL SOLUTION

(We offer every cloud service as a local solution too. That’s how cool we are.)

Benjamin Franklin



"One ounce of prevention is better than one pound of cure."*

*: in the metric system this means...

1 ounce ~= 28.35 grams

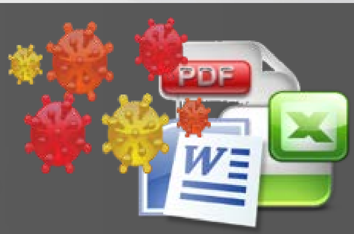
1 pound ~= 453.39 grams

Check Point Multi-Layered Threat Prevention

Check Point
SOFTWARE TECHNOLOGIES LTD.

IPS

Stops exploits of known vulnerabilities



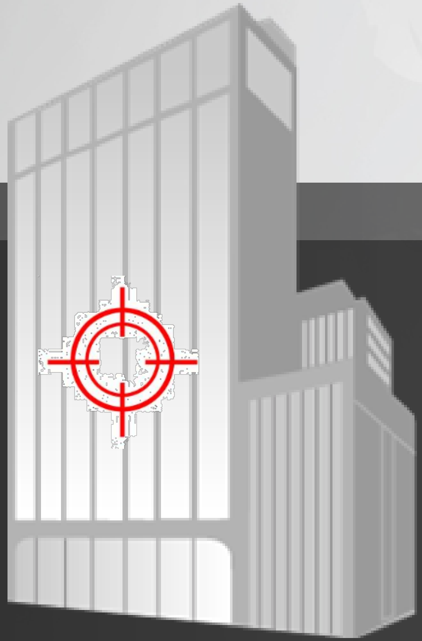
Antivirus

Block download of malware infested files

Anti-Bot

Detect and prevent bot damage

©2013 Check Point Software Technologies Ltd.



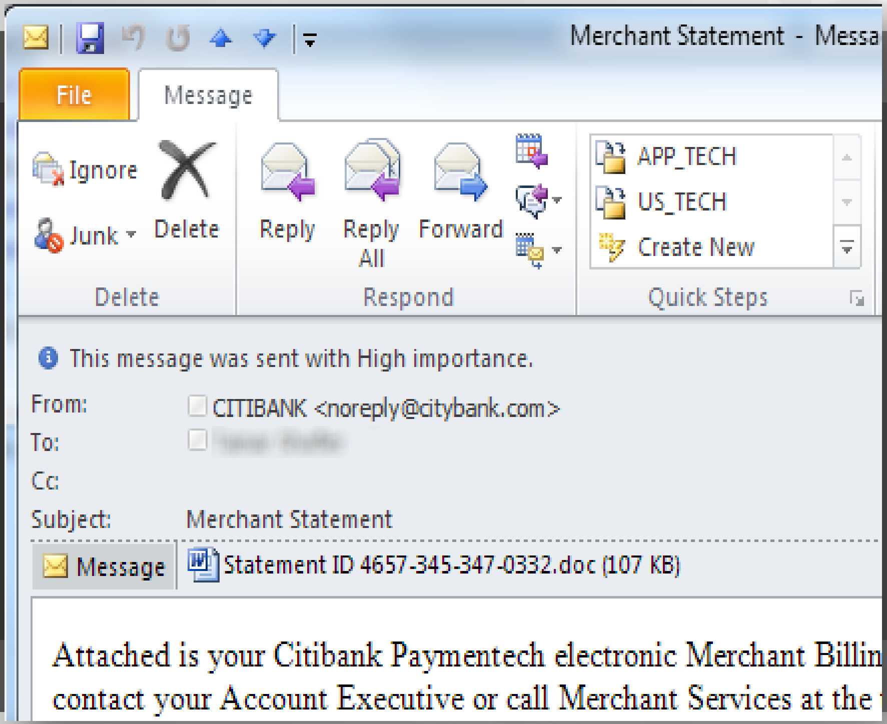
TARGETED ATTACKS BEGIN WITH ZERO-DAY EXPLOITS

Duqu Worm Causing Collateral Damage in a Silent Cyber-War

Worm exploiting zero-day vulnerabilities in a Word document

dark READING

©2013 Check Point Software Technologies Ltd.



This message was sent with High importance.

From: CITIBANK <noreply@citybank.com>

To: [redacted]

Cc:

Subject: Merchant Statement

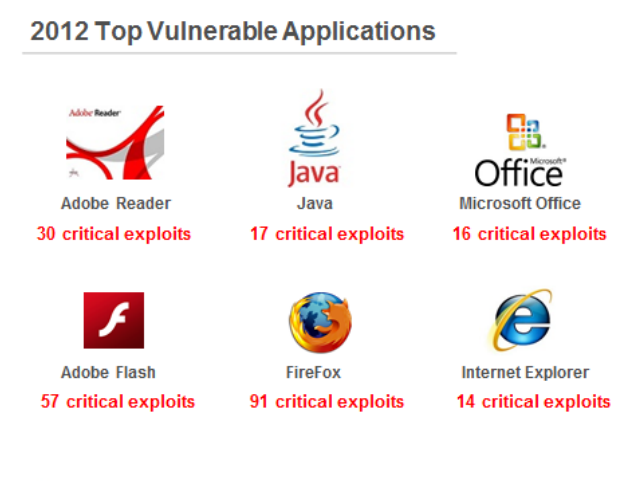
Statement ID 4657-345-347-0332.doc (107 KB)

Attached is your Citibank Paymentech electronic Merchant Billin
contact your Account Executive or call Merchant Services at the

WOULD YOU OPEN THIS ATTACHMENT?

©2013 Check Point Software Technologies Ltd.

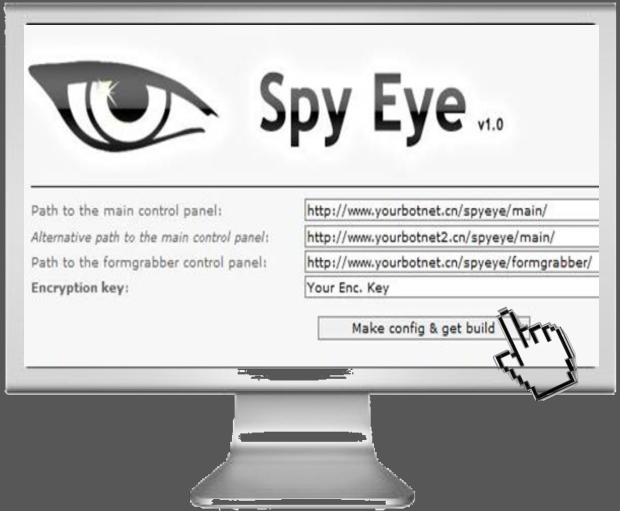
Exploiting Zero-day vulnerabilities



2012 Top Vulnerable Applications

Adobe Reader 30 critical exploits	Java 17 critical exploits	Microsoft Office 16 critical exploits
Adobe Flash 57 critical exploits	FireFox 91 critical exploits	Internet Explorer 14 critical exploits

New vulnerabilities



Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/
Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/
Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/
Encryption key: Your Enc. Key

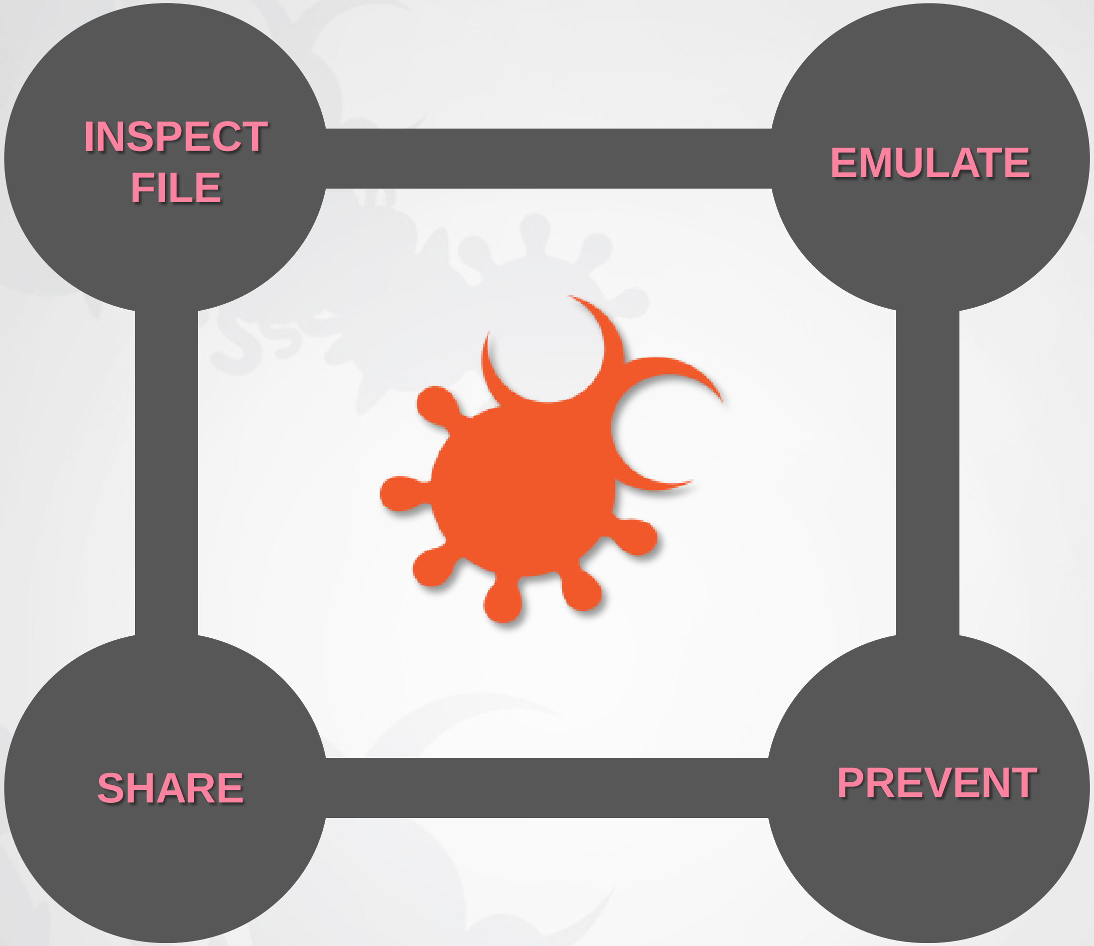
Countless new variants

> “nearly 200,000 new malware samples appear around the world each day”
>
> - net-security.org, June 2013

Introducing
Check Point Threat Emulation

PREVENTION OF ZERO-DAY ATTACKS !

©2013 Check Point Software Technologies Ltd.



Stop undiscovered attacks with

Check Point Threat Emulation

©2013 Check Point Software Technologies Ltd.

Identify files in email attachments and downloads over the web

Cloud service or On-Premise solution

Send file to virtual sandbox

INSPECT

Exe files, PDF and Office documents

Emulating Multi OS environments

WIN 7, 8, XP & user customized

Open file and monitor abnormal behavior

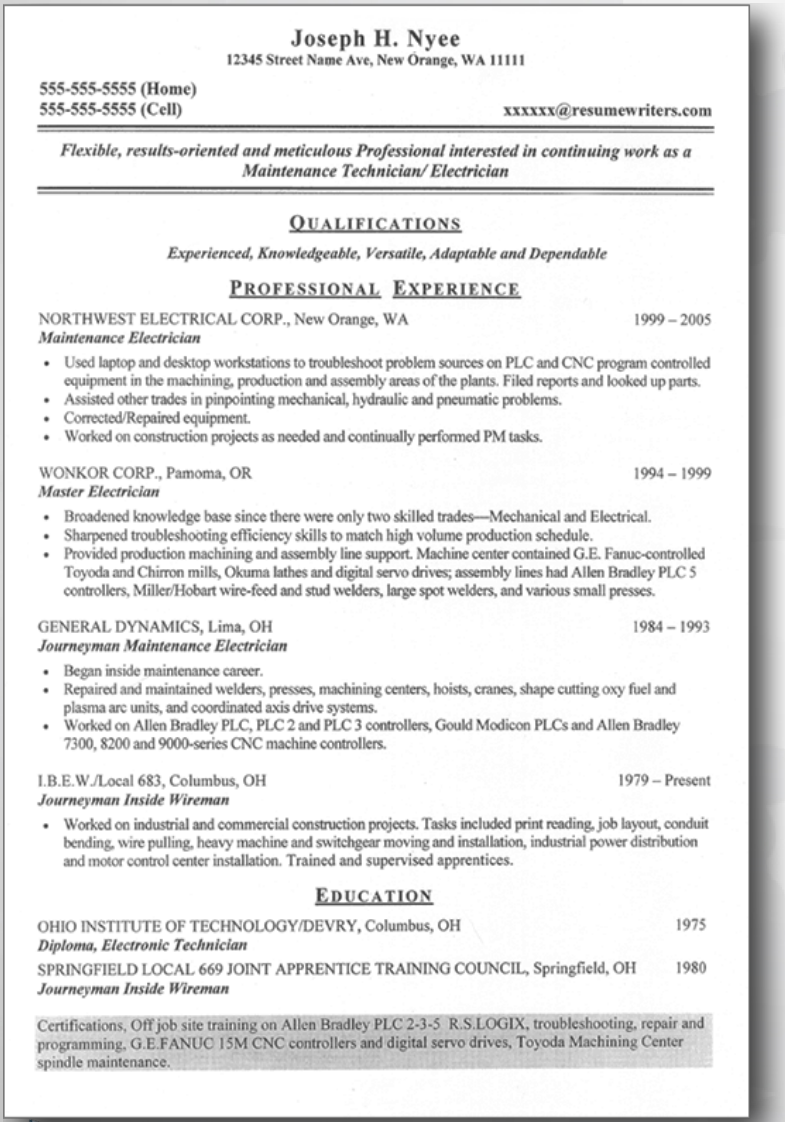
EMULATE

Monitored behavior:

- file system
- system registry
- network connections
- system processes

©2013 Check Point Software Technologies Ltd.

Emulation @ Work



Joseph H. Nyee
12345 Street Name Ave, New Orange, WA 11111

555-555-5555 (Home)
555-555-5555 (Cell)
xxxxxx@resumewriters.com

Flexible, results-oriented and meticulous Professional interested in continuing work as a Maintenance Technician/ Electrician

QUALIFICATIONS

Experienced, Knowledgeable, Versatile, Adaptable and Dependable

PROFESSIONAL EXPERIENCE

NORTHWEST ELECTRICAL CORP., New Orange, WA 1999 – 2005
Maintenance Electrician

- Used laptop and desktop workstations to troubleshoot problem sources on PLC and CNC program controlled equipment in the machining, production and assembly areas of the plants. Filed reports and looked up parts.
- Assisted other trades in pinpointing mechanical, hydraulic and pneumatic problems.
- Corrected/Repaired equipment.
- Worked on construction projects as needed and continually performed PM tasks.

WONKOR CORP., Pamoma, OR 1994 – 1999
Master Electrician

- Broadened knowledge base since there were only two skilled trades—Mechanical and Electrical.
- Sharpened troubleshooting efficiency skills to match high volume production schedule.
- Provided production machining and assembly line support. Machine center contained G.E. Fanuc-controlled Toyoda and Chirron mills, Okuma lathes and digital servo drives; assembly lines had Allen Bradley PLC 5 controllers, Miller/Hobart wire-feed and stud welders, large spot welders, and various small presses.

GENERAL DYNAMICS, Lima, OH 1984 – 1993
Journeyman Maintenance Electrician

- Began inside maintenance career.
- Repaired and maintained welders, presses, machining centers, hoists, cranes, shape cutting oxy fuel and plasma arc units, and coordinated axis drive systems.
- Worked on Allen Bradley PLC, PLC 2 and PLC 3 controllers, Gould Modicon PLCs and Allen Bradley 7300, 8200 and 9000-series CNC machine controllers.

I.B.E.W./Local 683, Columbus, OH 1979 – Present
Journeyman Inside Wireman

- Worked on industrial and commercial construction projects. Tasks included print reading, job layout, conduit bending, wire pulling, heavy machine and switchgear moving and installation, industrial power distribution and motor control center installation. Trained and supervised apprentices.

EDUCATION

OHIO INSTITUTE OF TECHNOLOGY/DEVRY, Columbus, OH 1975
Diploma, Electronic Technician

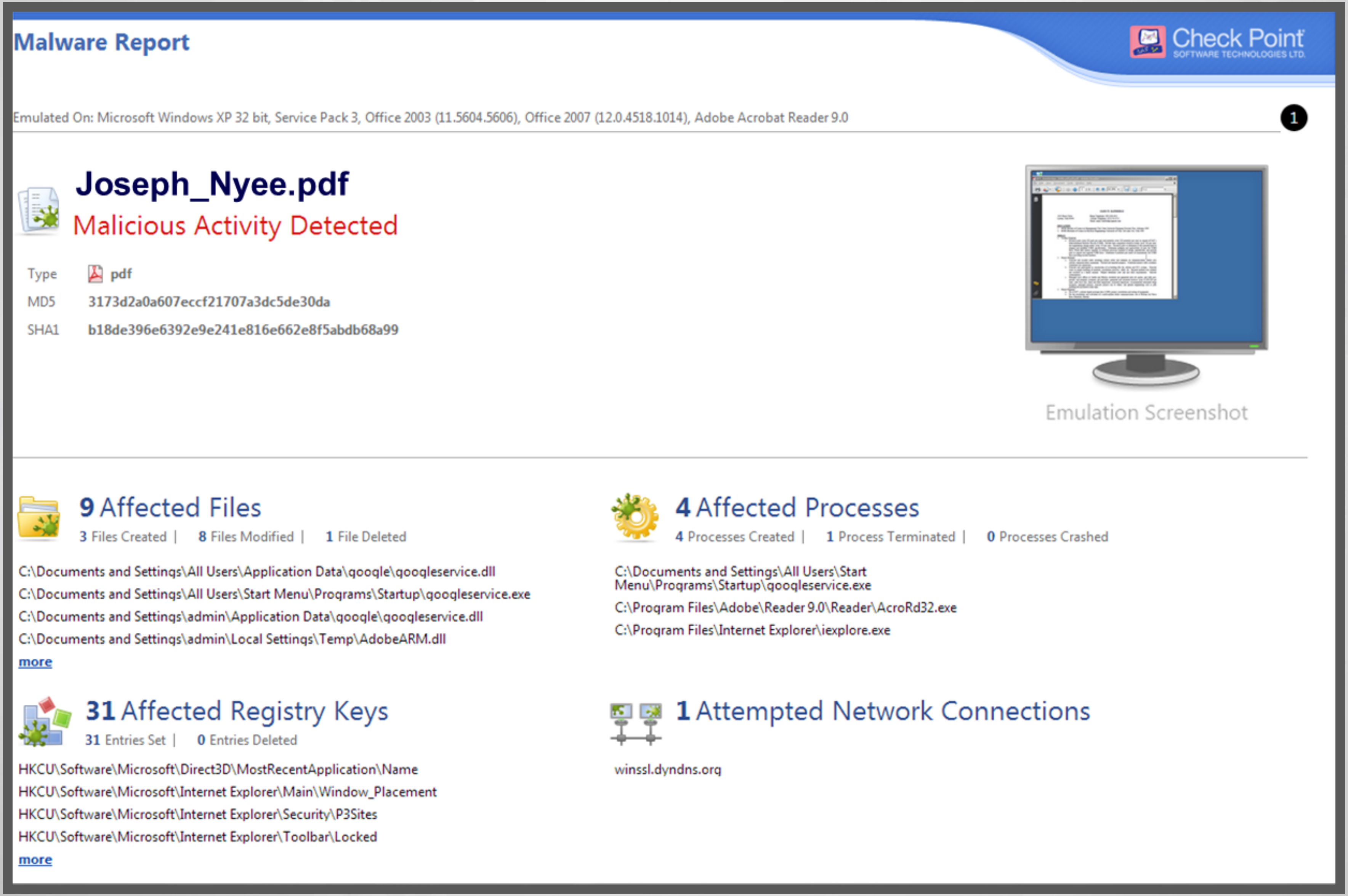
SPRINGFIELD LOCAL 669 JOINT APPRENTICE TRAINING COUNCIL, Springfield, OH 1980
Journeyman Inside Wireman

Certifications, Off job site training on Allen Bradley PLC 2-3-5 R.S.LOGIX, troubleshooting, repair and programming, G.E.FANUC 15M CNC controllers and digital servo drives, Toyoda Machining Center spindle maintenance.

A STANDARD CV?

©2013 Check Point Software Technologies Ltd.

Emulation @ Work



Malware Report

Check Point SOFTWARE TECHNOLOGIES LTD.

Emulated On: Microsoft Windows XP 32 bit, Service Pack 3, Office 2003 (11.5604.5606), Office 2007 (12.0.4518.1014), Adobe Acrobat Reader 9.0

1

Joseph_Nyee.pdf

Malicious Activity Detected

Type	pdf
MD5	3173d2a0a607eccf21707a3dc5de30da
SHA1	b18de396e6392e9e241e816e662e8f5abdb68a99

Emulation Screenshot

9 Affected Files

3 Files Created | 8 Files Modified | 1 File Deleted

C:\Documents and Settings\All Users\Application Data\google\googleservice.dll
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Documents and Settings\admin\Application Data\google\googleservice.dll
C:\Documents and Settings\admin\Local Settings\Temp\AdobeARM.dll
more

4 Affected Processes

4 Processes Created | 1 Process Terminated | 0 Processes Crashed

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files\Internet Explorer\iexplore.exe

31 Affected Registry Keys

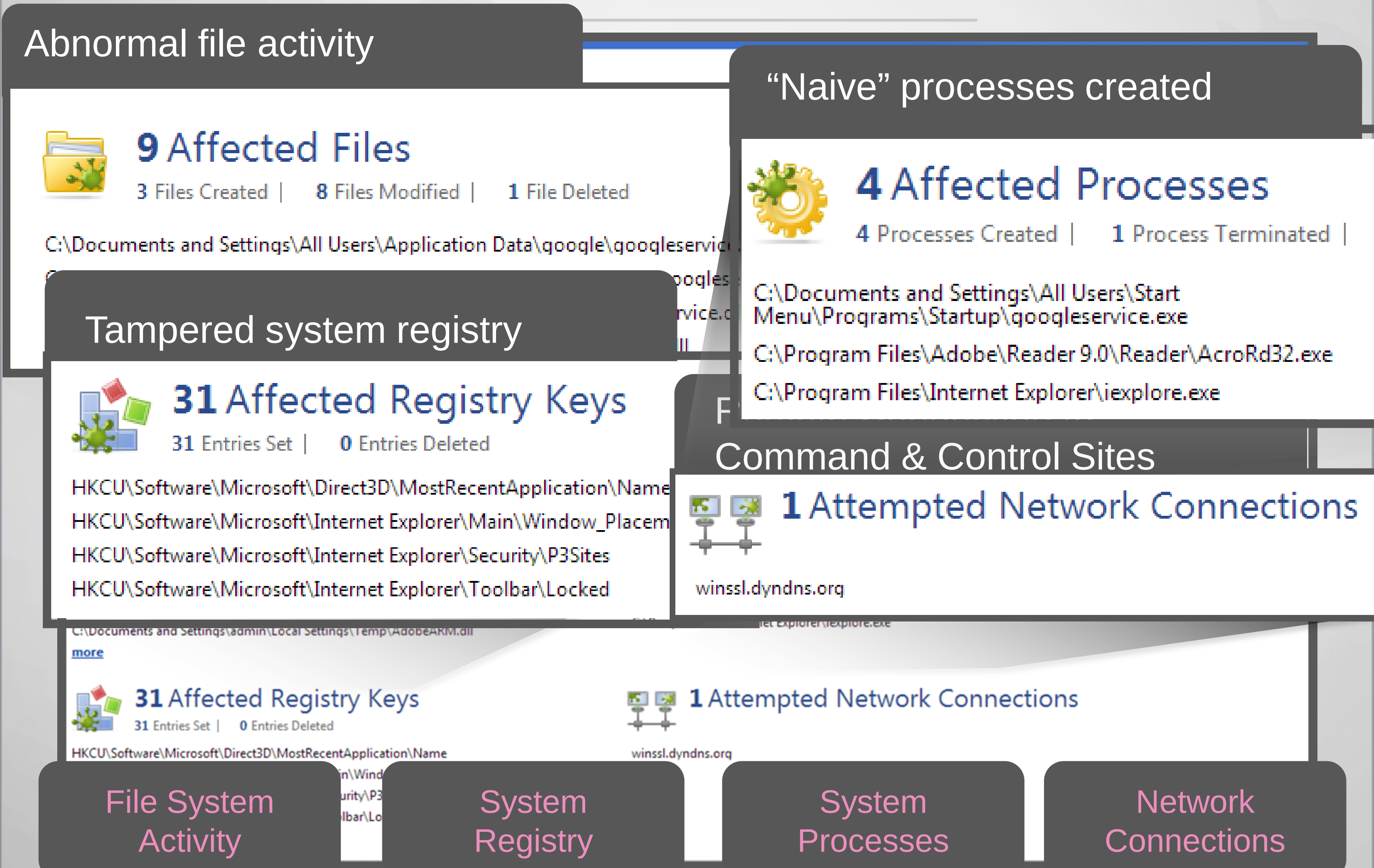
31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placement
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
HKCU\Software\Microsoft\Internet Explorer\Toolbar\Locked
more

1 Attempted Network Connections

winssl.dyndns.org

Emulation @ Work



Abnormal file activity

9 Affected Files

3 Files Created | 8 Files Modified | 1 File Deleted

C:\Documents and Settings\All Users\Application Data\google\googleservic

"Naive" processes created

4 Affected Processes

4 Processes Created | 1 Process Terminated |

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe

C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe

C:\Program Files\Internet Explorer\iexplore.exe

Tampered system registry

31 Affected Registry Keys

31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name

HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placem

HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites

HKCU\Software\Microsoft\Internet Explorer\Toolbar\Locked

Command & Control Sites

1 Attempted Network Connections

winssl.dyndns.org

C:\Documents and Settings\admin\Local Settings\Temp\AdobeARM.dll

more

31 Affected Registry Keys

31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name

1 Attempted Network Connections

winssl.dyndns.org

File System Activity

System Registry

System Processes

Network Connections

PREVENT

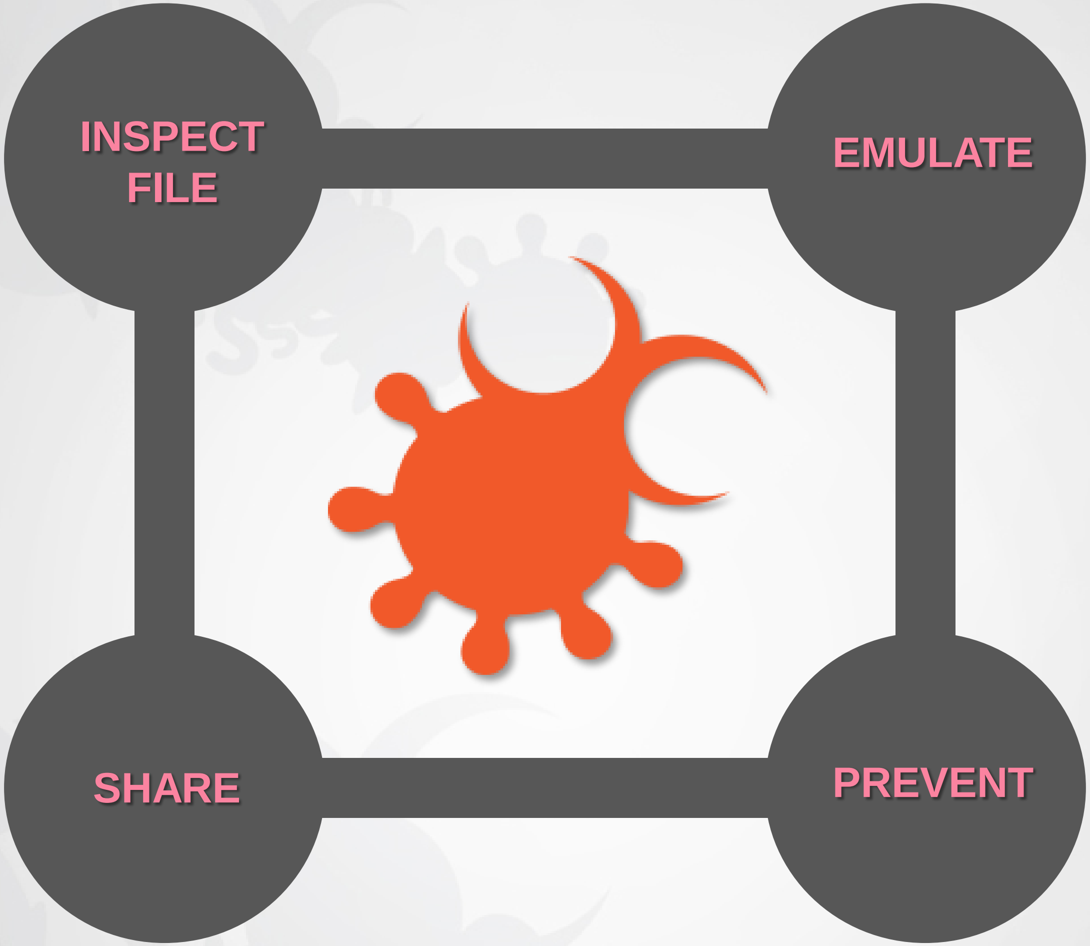
Security Gateway

Inline stopping of malicious files on any gateway

SHARE

Immediate update of all gateways

©2013 Check Point Software Technologies Ltd.



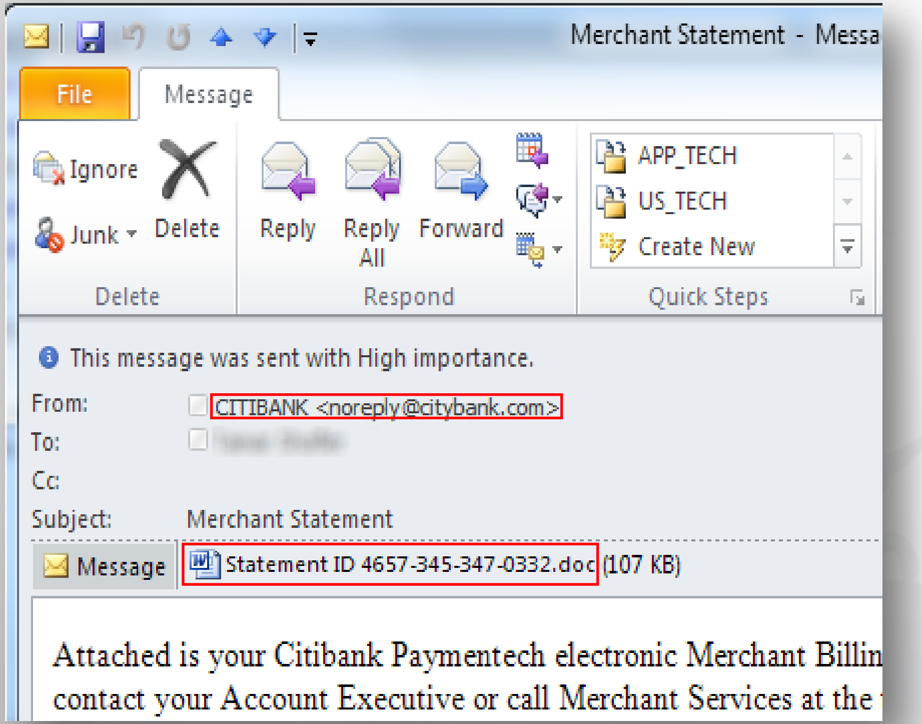
Stop undiscovered attacks with

ThreatCloud Emulation Service

©2013 Check Point Software Technologies Ltd.

Real Life Example

Prevented 140 phishing emails targeting 4 customers in 2 days!



This message was sent with High importance.

From: CITIBANK <noreply@citybank.com>

To: [redacted]

Cc:

Subject: Merchant Statement

Message | Statement ID 4657-345-347-0332.doc (107 KB)

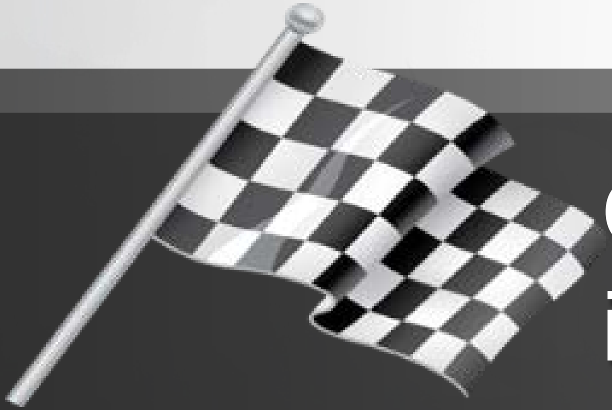
Attached is your Citibank Paymentech electronic Merchant Billin
contact your Account Executive or call Merchant Services at the

- New exploit variant of vulnerability (CVE-2012-0158)
- Installs a bot agent
- Opens network ports for bot communication
- Steals user credentials

©2013 Check Point Software Technologies Ltd.

Most Accurate and Fastest Prevention

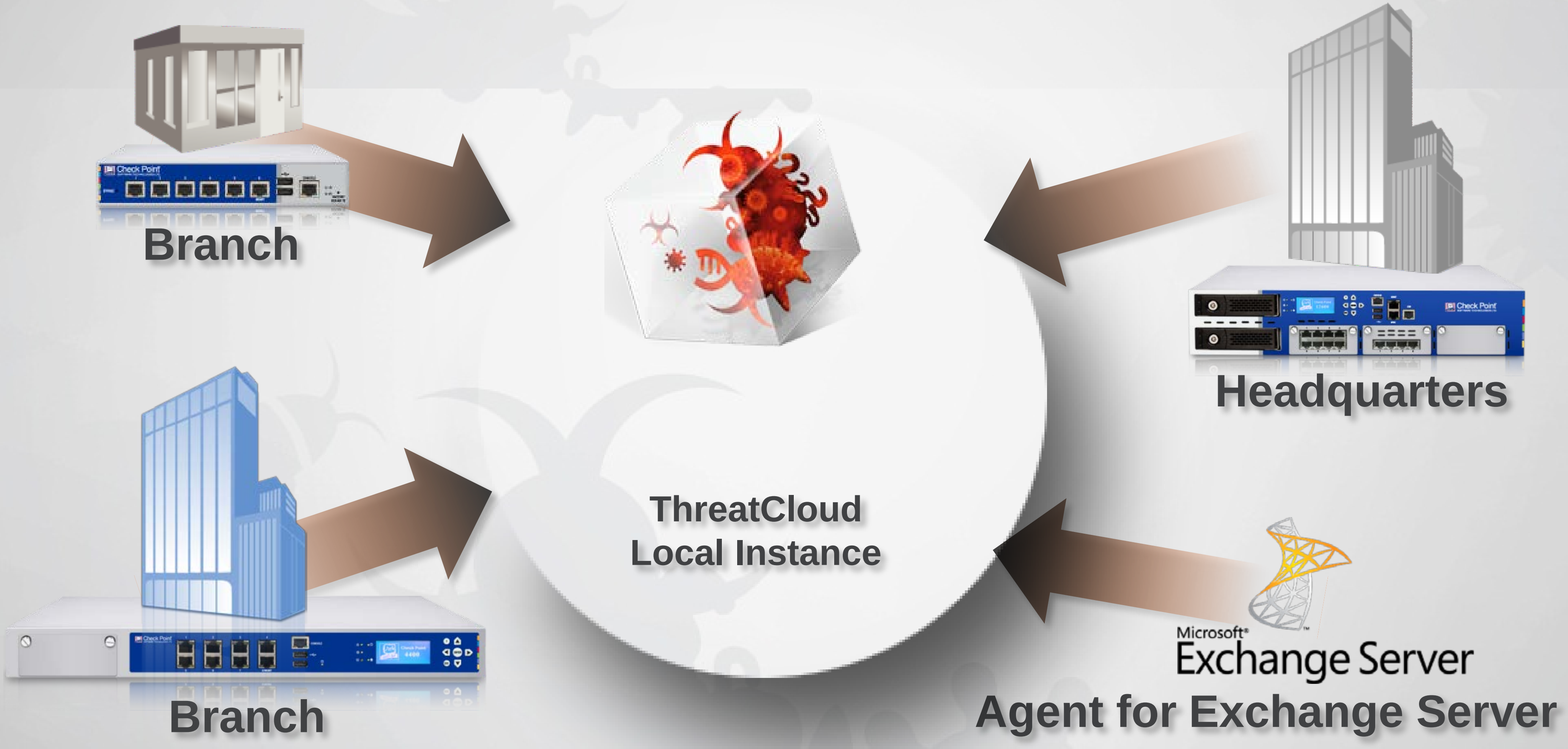
Zero false-positive in document emulation



Optimize analysis by inspecting only files at risk

THREAT EMULATION with ongoing innovation

ThreatCloud Emulation Architecture



Single Global Solution –
For the entire organization

ThreatCloud Emulation Service Advantages

LOCAL SOLUTION

Cloud based service—works with your existing infrastructure. No need to install new equipment

Control expenses with manageable lower monthly costs

LOCAL SOLUTION

Organizations can choose from 5 subscription options for global file inspections, starting at 10,000 files per month and up

©2013 Check Point Software Technologies Ltd.

ThreatCloud Local Cloud Appliances

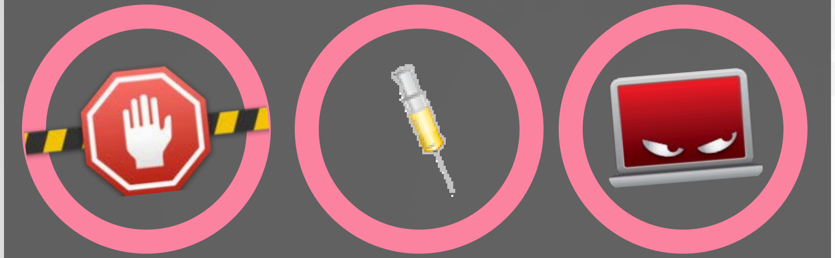
No need for Cloud connectivity.

©2013 Check Point Software Technologies Ltd.

Check Point Threat Prevention Solution

Multi-Layered Protection Against all Incoming Cyber Threats

Top Reasons customers pick Check Point Threat Emulation



A Complete Threat Prevention Solution for Known and Unknown threats

Choice between Cloud or On Premise solutions

Summary

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Prevents Zero-day Attacks

Stopping undiscovered malware

Prevent infections from malicious documents & executables

Simple deployment - requires no Infrastructure change

LOCAL SOLUTION

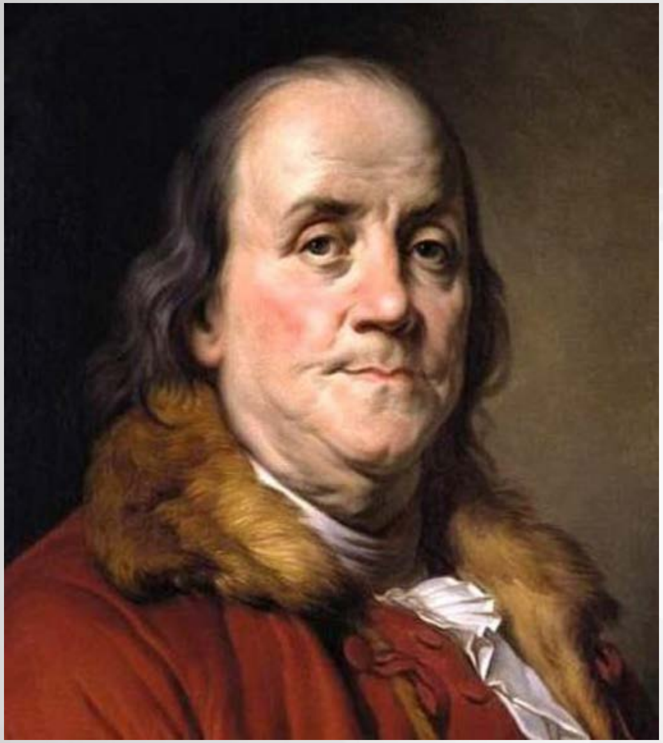
Part of Check Point multi-layered Threat Prevention

Always in motion, the future is.

- There is no silver bullet
- Better together in a multilayer security model
- Use each layer <u>correctly</u>
  - Threat Emulation: Zero Day
  - Anti-Virus: quick sorting of known bad
  - Anti-Bot: Post infection detection
  - Data Loss Prevention

©2013 Check Point Software Technologies Ltd.

Benjamin Franklin



“Well done is better than well said.”

Proof of concept!

©2013 Check Point Software Technologies Ltd.

Check Point SOFTWARE TECHNOLOGIES LTD.

Anyone can submit files for THREAT EMULATION

threats@checkpoint.com

threatemulation.checkpoint.com

©2013 Check Point Software Technologies Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD.

ThreatCloud Emulation Service

LOCAL SOLUTION

christof@checkpoint.com
+32 474 35 94 58

Christof Jacques – Check Point
Strategic Account Manager Belgium/Luxembourg