

版权说明

本内容均属e-works（中国制造业信息化门户网、武汉制造业信息化信息技术有限公司）会议论坛上所获取的资料，版权归e-works及演讲人单位及个人所有，严禁任何媒体、网站、个人或组织以任何形式或出于任何目的在未经本公司书面授权的情况下抄袭、转载、摘编、修改本会议资料内容，对有违上述行为而构成的版权侵权行为，e-works将依法追究其法律责任。如已是e-works授权合作伙伴，应在授权范围内使用。

e-works内容已是e-works授权合作伙伴，应在授权范围合作伙伴申请热线：wc@e-works.net.cn tel: 027-87592219/20/21-105

www.e-works.net.cn

中国制造业信息化门户网

武汉制造业信息化信息技术有限公司



2013 网络威胁应对： 建立企业安全信息共享平台

华东区高级安全顾问 孙捷

CCSE MCP

jsun@checkpoint.com

May 2013

领导者

- ▶ 全球防火墙/VPN与移动数据加密领域的领导者
- ▶ 为170,000家企业提供安全保护
- ▶ 6000万用户
- ▶ 100% 世界500强企业采用Check Point的解决方案
- ▶ 状态检测的发明者

100% 安全性

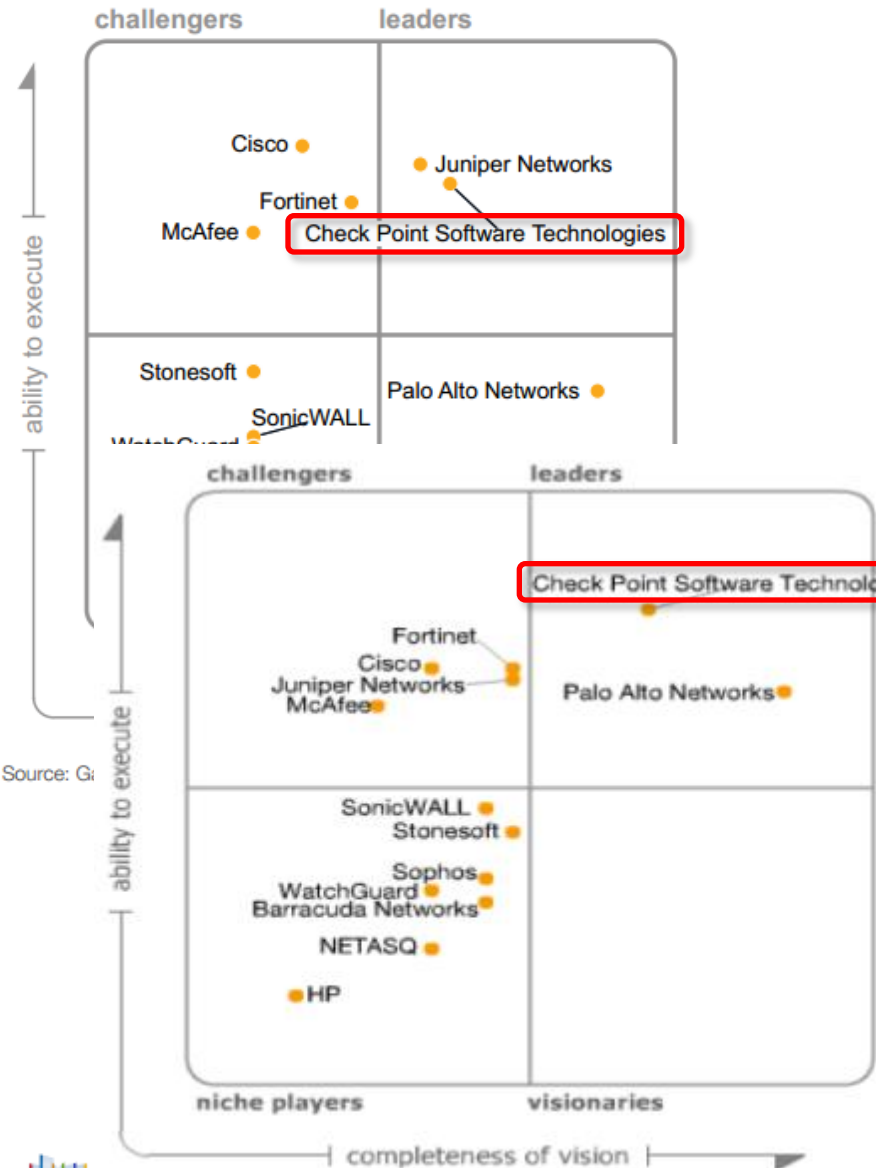
- ▶ 100% 专注于安全性
- ▶ 2300名安全专家
- ▶ 全球范围内有66,000名经过Check Point认证的专业人士
- ▶ 从Firewall-1到软件刀片

全球足迹

- ▶ 2,300名员工，总部位于以色列和美国，在30个国家拥有80个办事机构
- ▶ 在88个国家拥有3,000名合作伙伴
- ▶ 遍布全球250个备件库
- ▶ 120个授权培训中心



荣誉



Source: G



As of February 2013

Gartner

为何传统的防火墙防御已经不够了？ - 暗鼠行动为例



- 超过14个国家的70个受害企业
- 政府背景的黑客团队
- 2006年启动攻击，5年行动过程
- 2011第一次发现攻击

包括22个政府组织、6家能源企业、13家电子或媒体企业、13家国防承包商…其中，美国占了49个，居次的加拿大占了4个，而台湾和韩国各占3个… Shady RAT行动背后的操控者可能是一个国家…

3D SECURITY

人
People



政策
Policies



执行
Enforcement



3D SECURITY

下一代防火墙精确控制所有安全层次



合规性检查



SmartEvent

Unparalleled Application Control



超过 **4,800** 应用程序信息

超过 **310,000** 社交工具

提供 **150** 种应用分类

(包含 Web 2.0, Business, Anonymizer, IM, P2P, Voice & Video, File Share...)

<http://appwiki.checkpoint.com/appwikisdb/public.htm>

来自全球最早专注于应用程序控制的FaceTime
Check Point 拥有全球最大的应用程序识别云



云端网址库

- ✓ 64+ 分类
- ✓ 2亿+URLs

用户自定义网址、类别

99.2% 缓存查询利用率

从云端、缓存中自动移除误判信息

下一代威胁防御方案



Check Point
SOFTWARE TECHNOLOGIES LTD.

**Multi-Layered
Protection Against
all Incoming
Cyber Threats**

Check Point 安全云情报的信息共享





IPS

防止基于漏洞的网络攻击



Anti-Bot

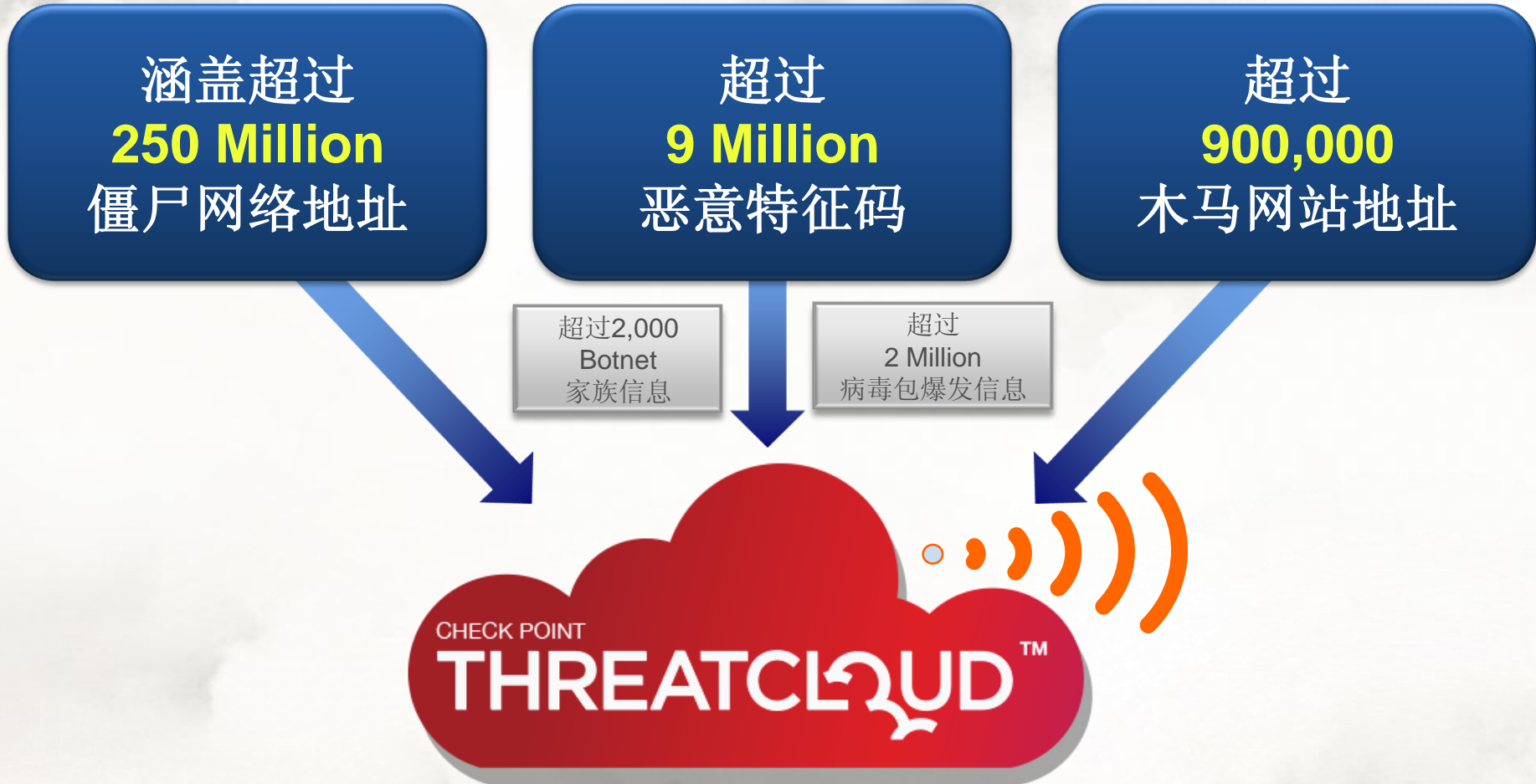
检测和阻止僵尸网络流量



Antivirus

阻止恶意软件的侵入





每天50,000新威胁情报的扩展



DISCOVER 发现和 阻止 僵尸网络攻击

发现僵尸行为

多维度识别

Command and Control
IP/URL/DNS



Communication patterns



Attack signs and types



阻止僵尸破坏

阻止远端黑客的控制



事后审计

提供调查工具





丰富的事件调查工具



感染的账号及设备



僵尸类型



僵尸行为



Bot Incident: Prevent

Copy Details Actions Anti-Bot

Summary Details

Frances Flash

Backdoor.WIN32.IRCBotg (Signature)

Prevented

Communication with C&C

High Severity

High Confidence

Today at 12:09:43

Event Description:

Malware Backdoor.WIN32.IRCBotg on 125.0.0.68 tried to locate its Command and Control server on 203.0.0.210 at 12:09:43 19 Mar 2012.

Additional Data:

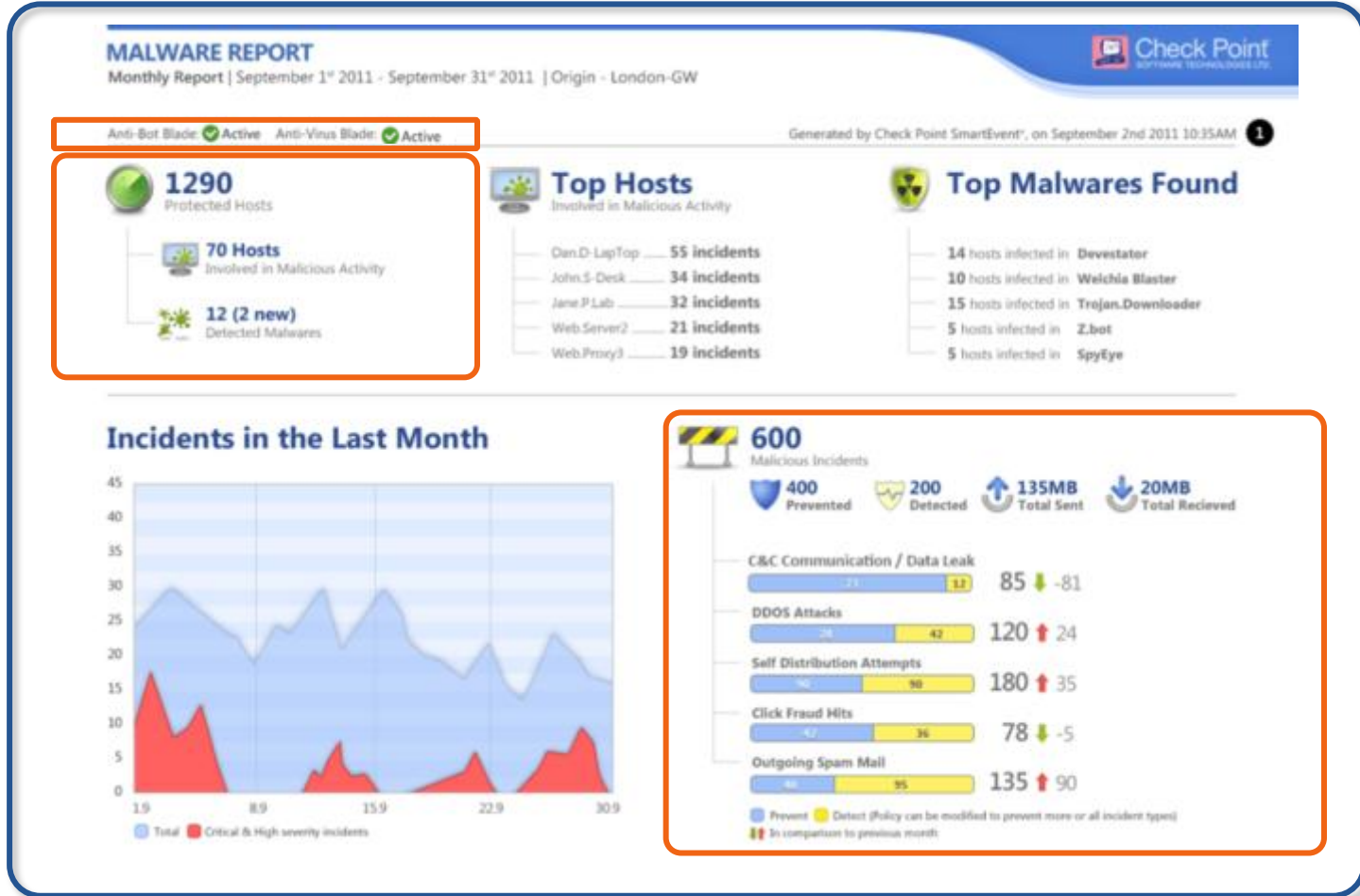
Destination: 203.0.0.210

Sent Bytes: 38 Bytes

Received Bytes: 112 Bytes



各维度的可视化统计数据



企业利用信息平台防御0Day



新爆发的漏洞



各类新变种

每天，超过70,000 - 100,000 恶意病毒样本更新到
ThreatCloud

darkREADING

郑重介绍

Check Point Threat Emulation 威胁仿真技术



阻止0Day未知攻击





Exe files, PDF and Office documents

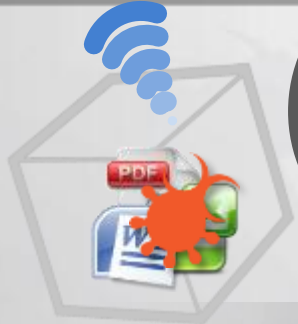
检测

威胁仿真



情报分析

阻止



阻截未知攻击
Check Point 威胁仿真技术

activity

“Naive” processes created



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

service.dll
ogleservice.exe

Connection to Control Sites

and Network Connections

9 Affected Files

- 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

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

1 Attempted Network Connections

winsl.dyndns.org

文件系统变化

系统注册表

系统进程

网络连接



任何人都可以提交文件检测
THREAT EMULATION

現在就能用！



threats@threats.checkpoint.com



threatemulation.checkpoint.com





IPS




Anti-Bot



Antivirus

MARKET LEADING AND MOST COMPREHENSIVE THREAT PREVENTION SOLUTION



Threat Emulation

行为分析及阻止
0Day攻击



基于情报平台的多层产品架构



下一代虚拟防火墙系统： Run any Software Blades on any Gateway

All Software Blades on
Every Virtual System



Simplify and Consolidate



- One-Click Virtual System Creation
- Dedicated Policy Per Virtual System
- Ease of Operation

Boosting Performance

VSLs



Check Point 保护企业私有云

Check Point
Security Gateway
Virtual Edition



Best Virtual Security
Gateway

Securing the Virtual
Machines

Unified Management for
Physical and Virtual

- 2200
- 4000
- 12000
- 21000
- 61000



- Power-1
- UTM-1
- Smart-1



GAiA

- IP Series



- Open Servers
- VMWare



Check Point 3D 下一代防火墙

防火墙、身份识别、VPN
软件刀片

应用程序控制、URL 过滤

移动设备安全接入
软件刀片

IPS 入侵
防御刀片

网络防毒
软件刀片

反僵尸网络
刀片

DLP 数据
防泄漏刀片

文档安全
软件刀片



2012 Model Series



SmartEvent
安全事件管理
统一事件关联分析



SmartWorkflow
工作流程管理
策略变更操作管理



SmartLog
海量日志分析系统
Turbo-search Log Analyzer



Smart-1

CHECK POINT 统一安全管理



我们认为：
数据泄露、恶意行为、病毒
感染、黑客攻击的长期存在

3D Security 报告贴近用户
环境进行安全评估

一键生成安全分析报告





Thank You



孙捷

jsun@checkpoint.com