




SACC 2015中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2015

互联网+ 重塑IT架构

应用筑基 “慧眼” 识魔

——下一代边界防御实践



网络空间的多事之秋

4000万信用卡



2014.01

5部



2014.11

2年, 100+个, \$1B

Carbanak

2015.02

3年, 29个省

“海莲花” APT

2015.05

400G+

]HackingTeam[

2015.07

2014.04



350万

2014.09



8300万

2015.03



8000万

2015.06



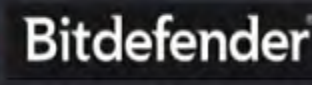
2150万

2015.06



> 6个月

2015.08



敲诈

缺资金？少技术？没意识？



悄悄的我走了，
正如我悄悄的来；
我挥一挥衣袖，
带走你全部钱财。

重新审视传统安全方法论

静态的、被动的、防御性的战略思维



假设前提

1. 信息系统蕴含的弱点可以被充分的评估和认识
2. 防护措施能够识别并阻断所有可能发生的攻击

告诉你一个真实的威胁环境

Wordpress Plugin CopySafe Web Protection Shell Upload (0day) Vulnerability

3337day-2018-23314

Verified ▲ Not verified yet

Warnings 0

Rating 0

20 Gold

Buy it!

地下黑市：The RealDeal Market

Full title Wordpress Plugin CopySafe Web Protection Shell Upload (0day) Vulnerability

Date add 2014-06-01

Category web applications

Platform php

Risk www

Vendor www.wordpress.org

Tested on

Tags

Comments 0

Views 4040

NSS Lab 2013: 每年供应量 85 个

0-Day漏洞

作者: Alucida

BusinessLevel [0/5]

Warnings 0

Exploits 19

Readers 0

请登录后再浏览

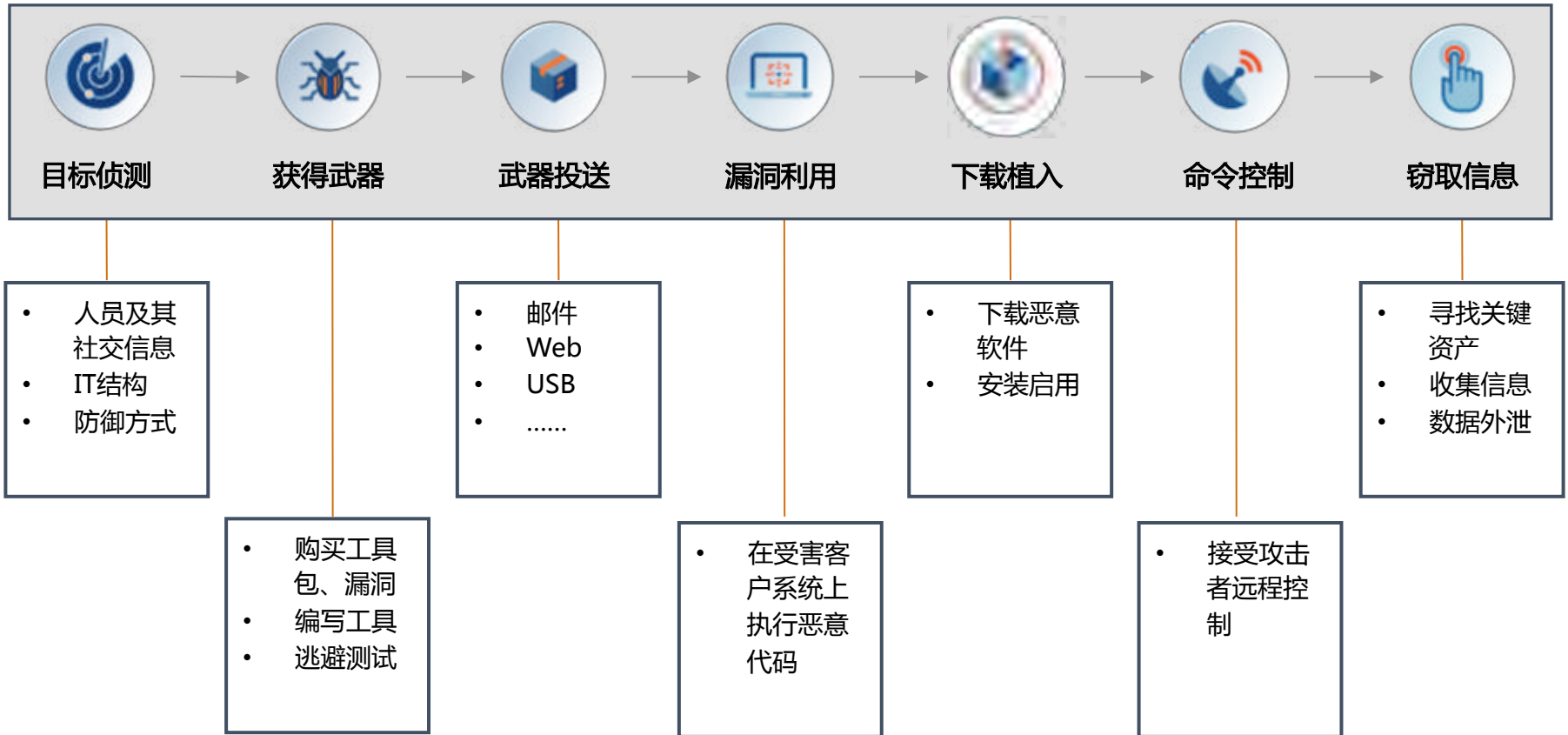
Please login or register to open this material.

APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
Desert_Falcon	3	2014/4/30	2015/3/3	3	教育	鱼叉邮件、水坑
GDATA_TooHash	4	2014/6/1	2014/8/31	3	科研	鱼叉邮件
DarkhoTel	134	2014/6/1	2015/3/19	29	教育、能源、电信	鱼叉邮件、网络劫持
DarkSeoul	4	2014/6/5	2015/1/5	3	电信	鱼叉邮件
Epic Turla	14	2014/6/12	2015/3/21	6	科研、教育	鱼叉邮件
NGO_Attack	6	2014/6/18	2015/3/13	6	非政府组织	鱼叉邮件
Dragonfly	2	2014/7/15	2014/8/19	1	能源	鱼叉邮件、水坑
APT28	1	2014/8/7	2014/8/7	1	航空	鱼叉邮件
Anunak	383	2014/9/28	2015/3/26	26	金融、电信、政府、科研	鱼叉邮件
CARETD	1	2014/10/28	2014/10/28	1	政府	鱼叉邮件
XSLCmd_O SX	1	2014/10/30	2014/10/30	1	金融	鱼叉邮件
Waterbug	1	2014/12/31	2014/12/31	1	政府	鱼叉邮件、水坑
Snake	1	2015/2/15	2015/2/15	1	金融	U盘
Equation	1	2015/4/16	2015/4/16	1	军工	U盘



定制木马、社交攻击、鱼叉钓鱼、水坑攻击.....

Cyber Kill Chain



被反复洞穿的边界防线

由外到内的防线

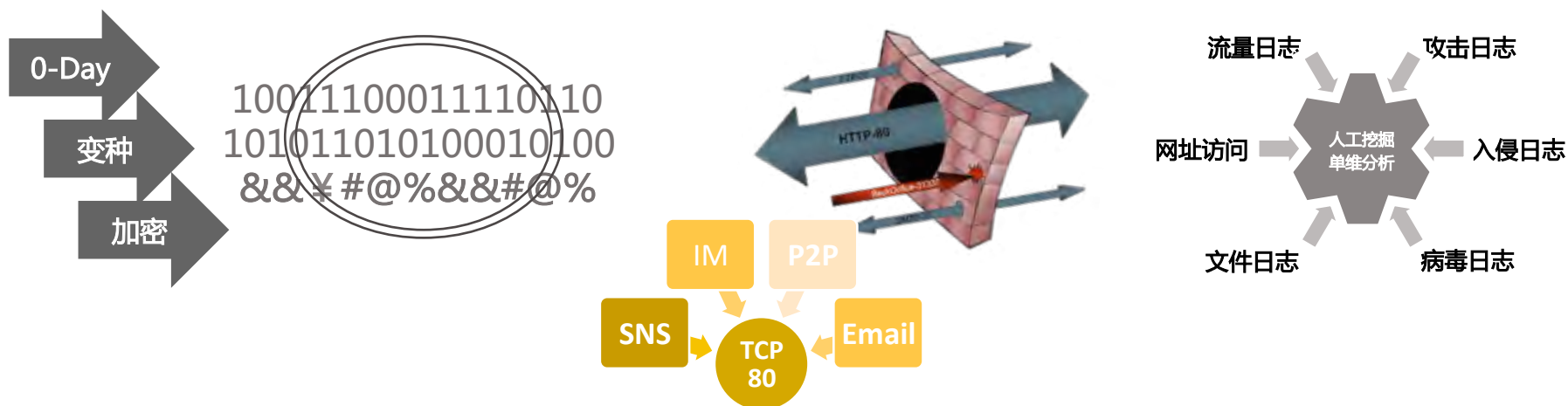
- 核心目标
 - 进入目标网络
- 主要手段
 - 钓鱼、恶意网址
 - 病毒、木马植入
 - 漏洞扫描和利用

由内到内的防线

- 核心目标
 - 获取更高权限
- 主要手段
 - 身份冒用、口令破解
 - 病毒、木马植入
 - 漏洞扫描和利用

由内到外的防线

- 核心目标
 - 核心资产暴露
- 主要手段
 - 建立C&C连接
 - 应用混淆逃逸
 - 机密数据上传



下一代安全方法论模型-PDFP

动态的、主动的、对抗性的战略思维



1. 未知威胁永远存在，系统已失陷
2. 借助威胁情报和大数据分析技术构建预测能力
3. 安全的起点从检测开始，通过安全情境和异常行为分析发现失陷点
4. 通过取证手段溯源攻击过程
5. 确定对抗措施，提升防御能力

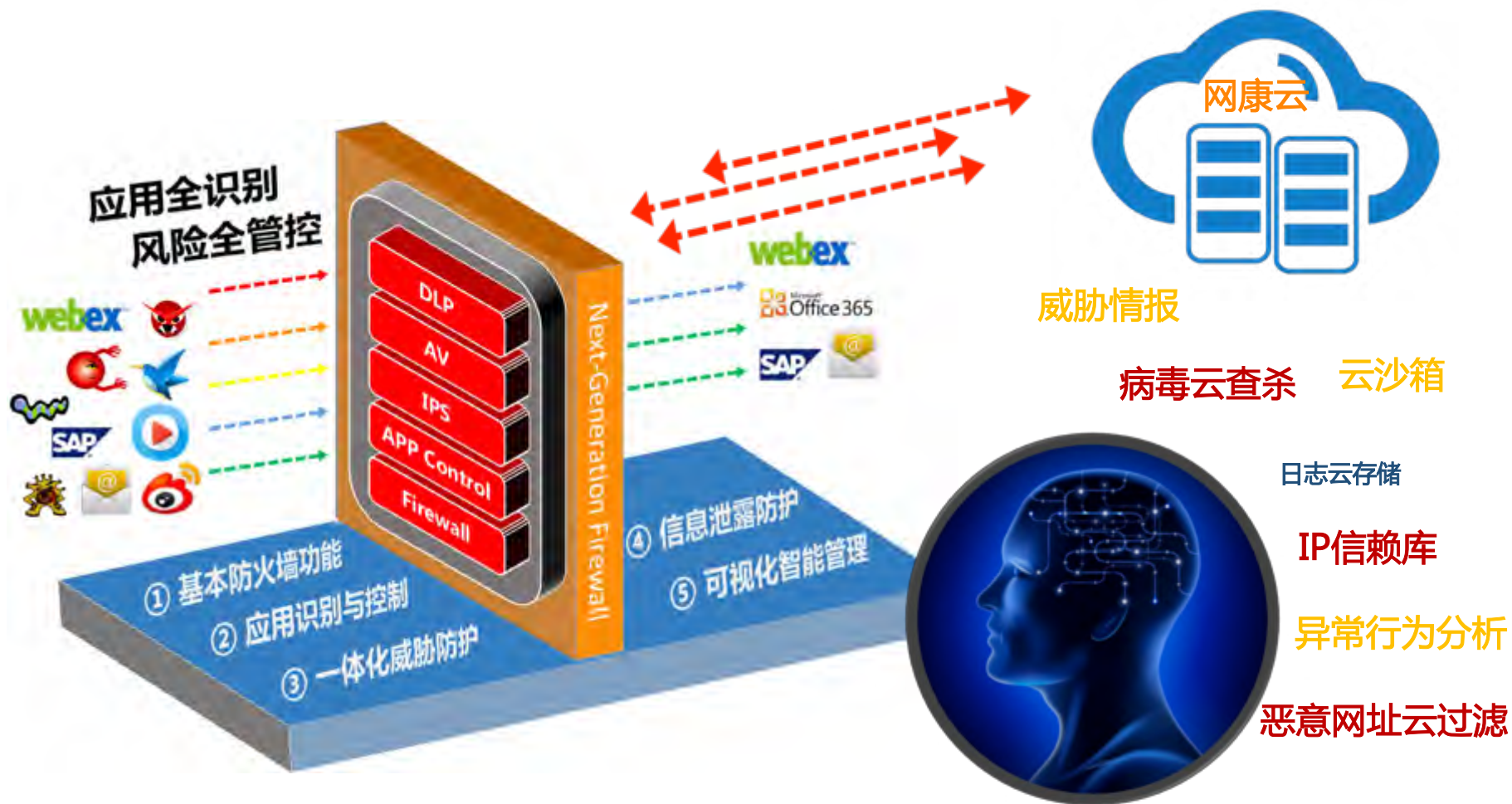
防护模式的变化和能力要求

- 从以“网络或系统”为中心的策略，转变为“**以信息或数据为中心**”的策略
- 从以“控制”为中心的安全演进至以“**人**”为核心的安全
- 安全能力从“防范”为主转向“**快速检测和响应能力**”的构建
- 安全防护从“个体或单个组织”的防护，转变为“**安全情报驱动**”的信息共享、集体协作方式

摘自：Gartner 《Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence》

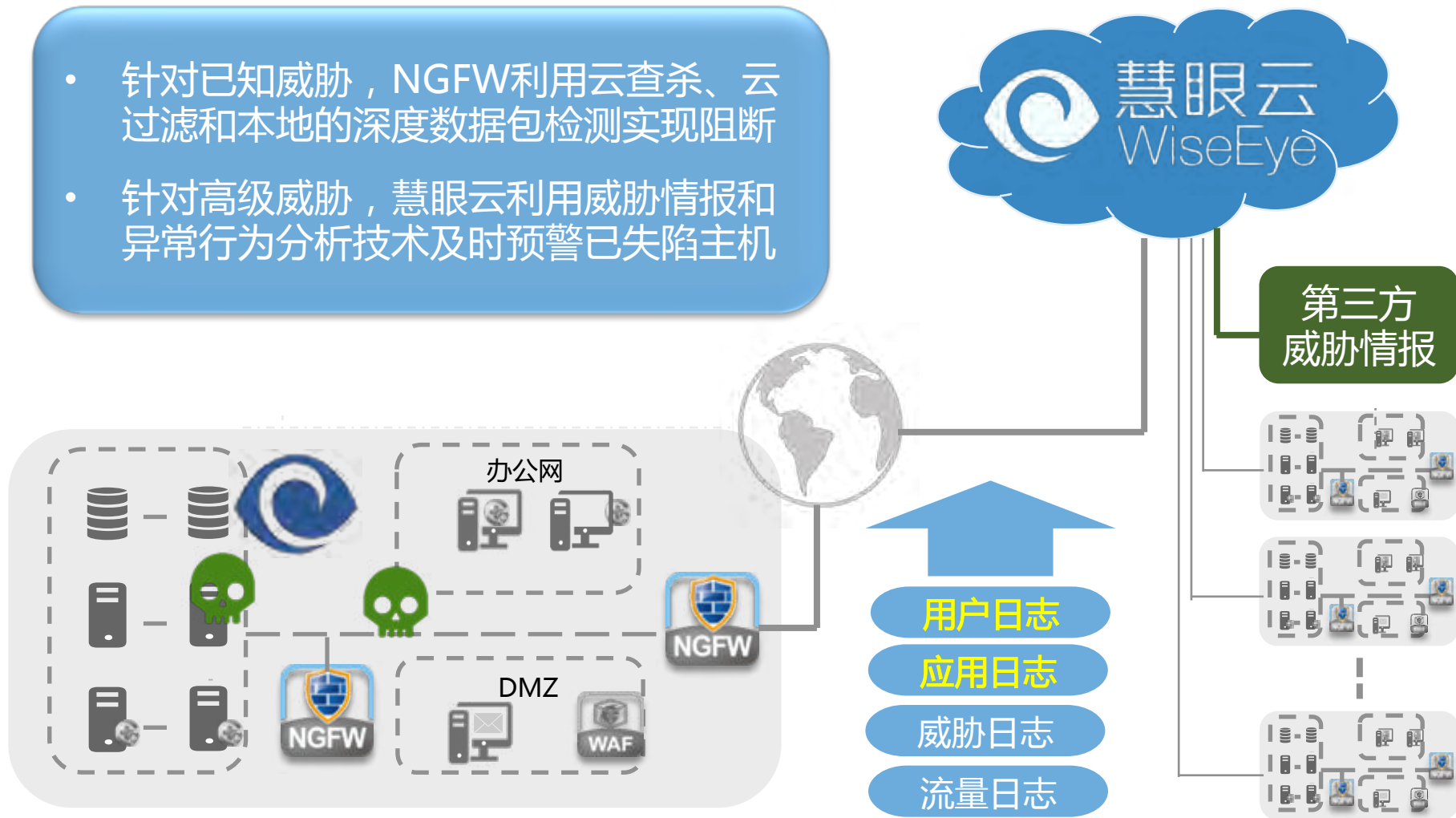


“云管协同” 的边界防御



网康下一代边界防御解决方案

- 针对已知威胁，NGFW利用云查杀、云过滤和本地的深度数据包检测实现阻断
- 针对高级威胁，慧眼云利用威胁情报和异常行为分析技术及时预警已失陷主机



Prediction

基于威胁情报的态势感知

24小时攻防情报

数据更新时间: 2015年9月27日

TOP攻击国家

IP数	#	国家
42254	1	中国
4139	2	美国
443	3	德国
400	4	荷兰
301	5	巴西
295	6	越南
266	7	俄罗斯
168	8	韩国
146	9	中国香港特区
145	10	乌克兰

TOP目标国家

IP数	#	国家
47291	1	中国
932	2	新加坡
621	3	美国
286	4	巴西
36	5	德国
35	6	中国香港特区
29	7	荷兰
28	8	日本
26	9	加拿大
25	10	印度

TOP攻击类型

IP数	#	攻击类型
18216	1	WEB-ATTACKS
7691	2	TROJAN
4978	3	DB-ATTACKS
2934	4	SPYWARE
2527	5	OTHER
2408	6	SQL-INJECTION
1988	7	POP
1754	8	WEB-SCAN
1727	9	XSS
1252	10	DNS

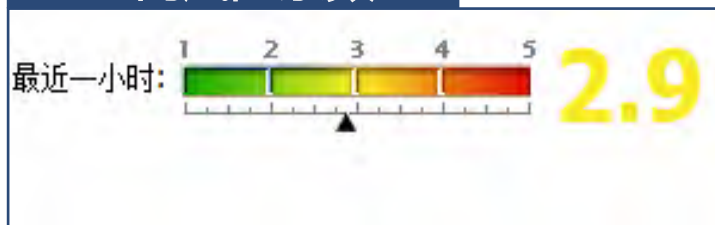
攻防日志

时间	发起方	攻击IP	受攻击地址	次数	应用	端口
09-27 00:00:15	China, Beijing	222.28.198.205	China, Beijing	87	ssh/ssh	80
09-27 00:00:16	Taiwan	118.163.194.184	China	4	POP3	110
09-27 00:00:17	China, Beijing	123.124.18.34	China, Guangzhou	150	Web P	80
09-27 00:00:17	China, Beijing	101.199.103.195	China, Beijing	23	Web/ssh	80
09-27 00:00:17	China, Zhengzhou	218.150.204.191	China, Zhengzhou	14	Web/ssh	80
09-27 00:00:18	China	117.158.137.92	France	14	Web/ssh	80

Detection

以风险为视角发现问题

全网风险系数



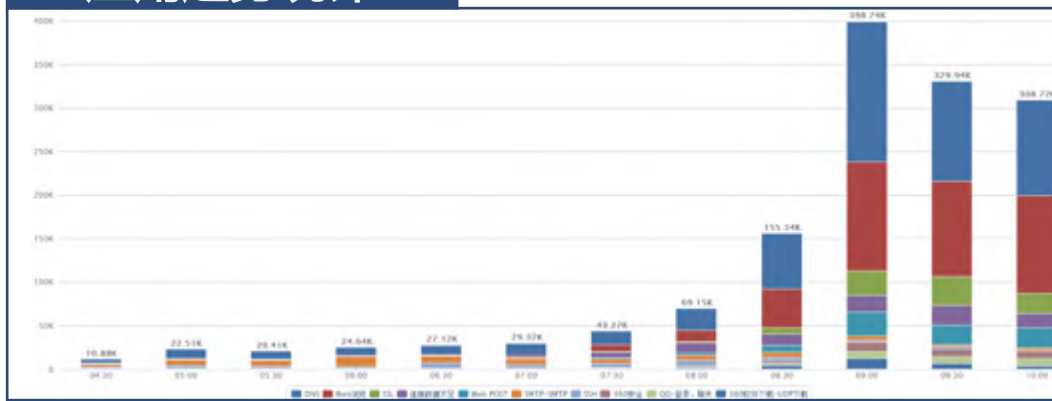
异常流量基线对比



高危应用统计



应用趋势统计



Detection

基于异常行为分析检测失陷主机



威胁情报

失陷主机

情境分析

日志搜索

安全报告

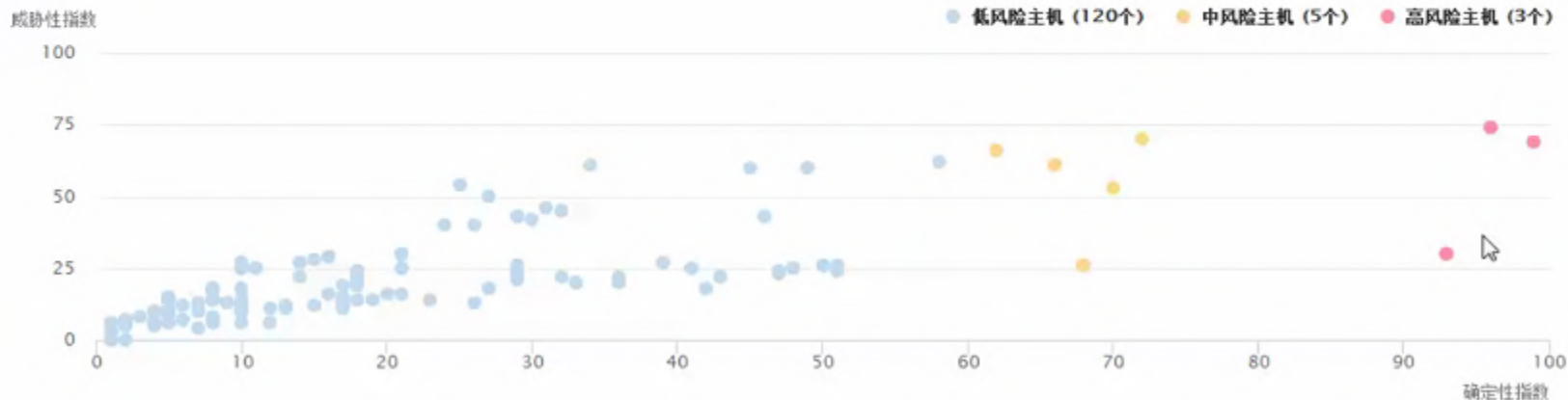
管理控制台 问题和帮助 netentsec 退出

主机总览

主机分析

失陷主机总览

当前失陷主机分布



Forensic

以应用为视角关联分析问题



Forensic

基于云存储的长周期溯源

The screenshot displays a forensic analysis tool interface. At the top, there is a navigation bar with the logo '网康科技 NGFW+' and a '日志搜索' (Log Search) button. Below this, there are tabs for '日志搜索' and '数据源管理'. The main area features a search bar with 'all' and a time range filter set to '最近24小时'. A search ID '1003238' is entered. The event count is '总事件: 1,156 (2015-05-26 20:30:00 — 2015-05-27 20:39:58)'. A timeline chart shows a significant spike in activity around 14:00 on May 27th. Below the chart, there are view options: '日志视图', '表格视图', and '图表视图'. A sidebar on the left lists various log fields, with a red dashed box highlighting the following items: IP协议, host, serialnumber, source, type, 严重性, 会话ID, 动作, 发起方, 威胁ID, 威胁分类, 威胁名称, 威胁类型, 应用, 源国家, 源地址, 源用户, 源端口, 目的国家, 目的地址, 目的用户, 目的端口, and 策略. The main log list shows several entries with details such as source IP, destination IP, port, application, and threat classification. The threat ID '1003238' is highlighted in yellow in several entries.

时间	原始日志
2015-05-27T13:37:16+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'379744328' 源地址:'202.206.3.30' 源端口:'22888' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'Web浏览' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'
2015-05-27T13:37:21+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'401621856' 源地址:'202.206.3.30' 源端口:'22844' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'QQ浏览器' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'
2015-05-27T08:32:44+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'1559384928' 源地址:'202.206.3.30' 源端口:'29766' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'QQ浏览器' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'
2015-05-27T08:35:02+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'4143458704' 源地址:'202.206.3.30' 源端口:'21341' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'Web浏览' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'
2015-05-27T13:38:20+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'4098119288' 源地址:'202.206.3.30' 源端口:'42943' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'Web浏览' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'
2015-05-27T10:41:18+...	源国家:'中国' 目的用户:'/undefined/undefined' 目的端口:'80' 会话ID:'1439462240' 源地址:'202.206.3.30' 源端口:'22093' 威胁名称:'HTTP 未认证的暴力破解尝试' localtime:'2015-05-27T14:30:16+08:00' 动作:'阻断' 应用:'Web浏览' IP协议:'TCP' 严重性:'高' 目的地址:'220.194.200.252' 威胁ID:'1003238' 策略:'日志转发1' 源用户:'/undefined/undefined' 威胁分类:'WEB-ATTACKS' 目的国家:'中国' 威胁类型:'漏洞' 发起方:'源'

Prevention 精细化应用控制

中国最大的应用识别库

全球最大的中文网页库

10余年应用层研究积累

安全提升

- 由数据流控制转向业务流控制
- 由黑名单控制转向白名单控制
- 由流量控制深入至内容级过滤



Prevention 融合的入侵防御



Certificate Of CVE Compatibility



MAPP Partners

海量特征库

ACTIVEX	IMAP	SQL-INJECTION
BACKDOOR	JAVA	TELNET
BAD-FILES	LDAP	VIRUS
DB-ATTACKS	MEDIA	VOIP
DDOS	NETBIOS	WEAKPASSWORD
DNS	OTHER	WEB-ATTACKS
DOS	POP	WEB-CLIENT
EXPLOIT	RPC	WEB-SCAN
FTP	SCADA-ATTACKS	WINDOWS
ICMP	SMTP	XSS

30类, 6300余种漏洞防护

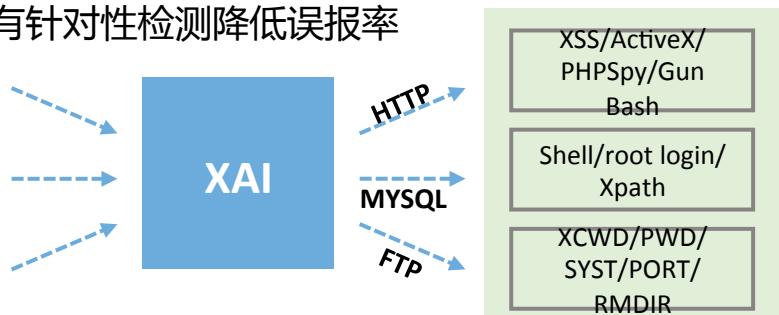
8类, 8600余种间谍软件防护

防逃逸机制

防逃逸机制	逃逸方法
分片重组	将攻击流量分散到多个协议分片中
单包多次解析	将分包传递的信息压缩在单包中
目录混淆防护	使用“..”或“.”等使路径复杂化
大小写互转	大小写字符混杂
特殊编码解码	使用UTF/Base64/gzip等编码伪装
特殊字符处理	使用无意义的字符填充流量

应用预识别

- 避免端口混淆导致的逃逸
- 有针对性检测降低误报率



高性能多模匹配算法

ACBM

基于状态机的带跳转的多模匹配算法



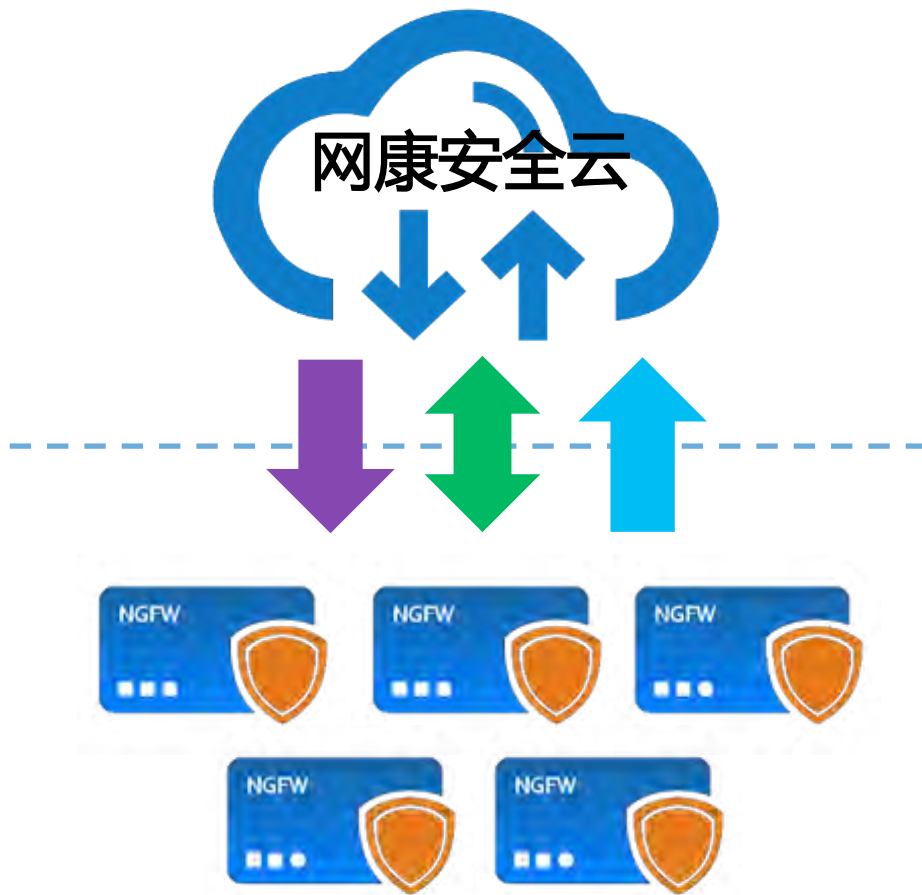
WMRSR

基于前后缀过滤快速跳转和字典树的接力跳转的多模匹配算法



Prevention

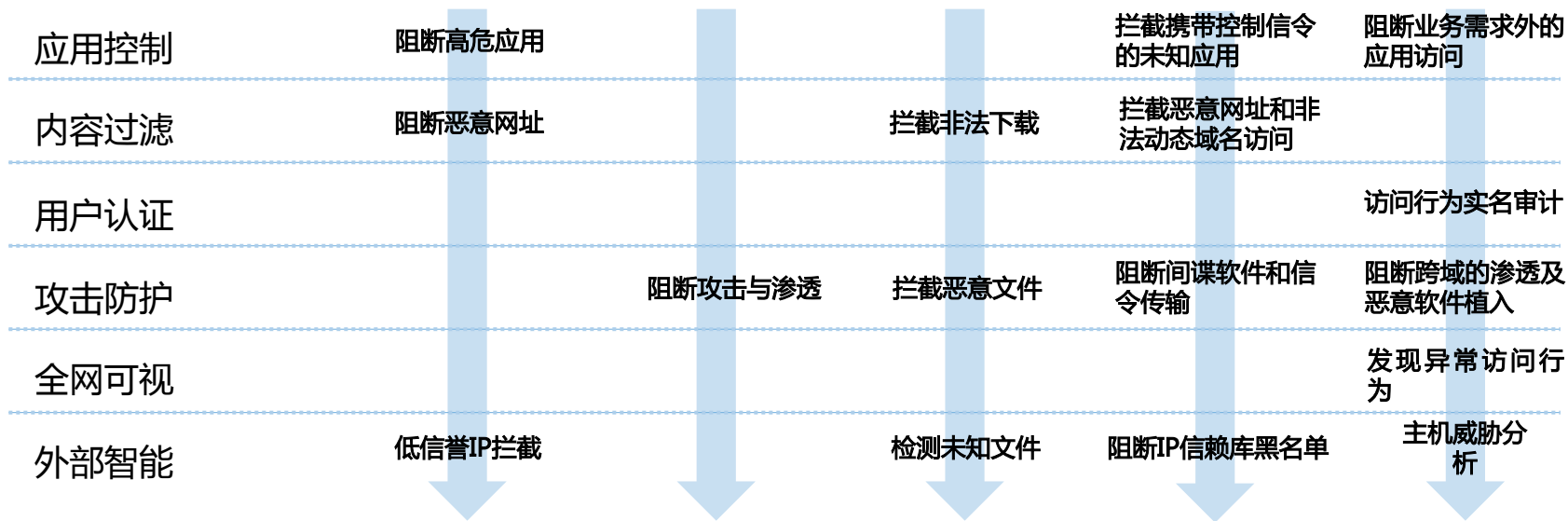
病毒云查杀 恶意网址云过滤



80亿 病毒文件样本 1亿 恶意网址

新威胁响应时间缩短至15分钟

在网络边界终止高级威胁



案例：XcodeGhost拦截及失陷手机检测



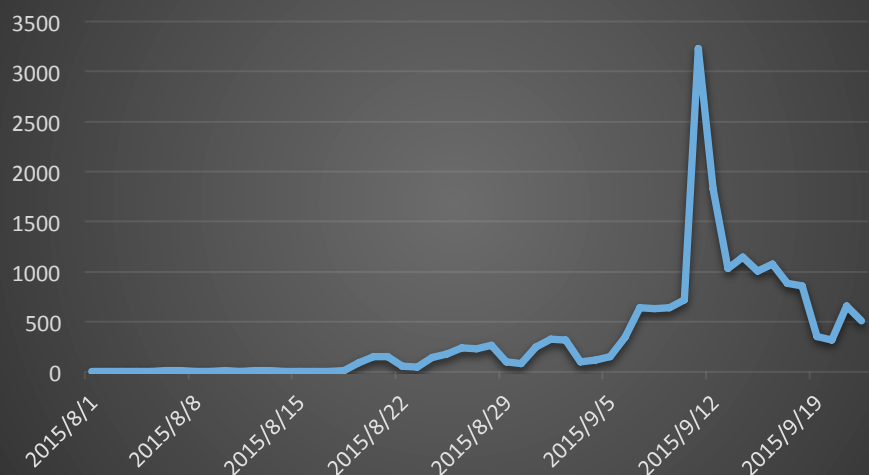
9月19日

威胁情报
推送完毕

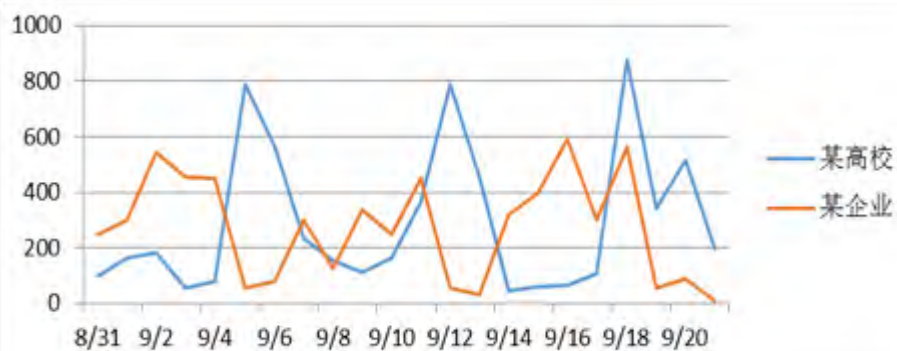
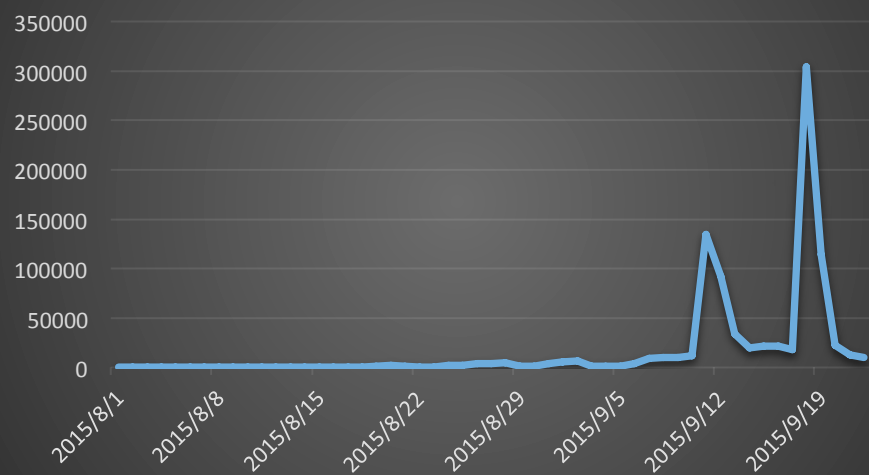
开始时间	结束时间	标识类型	IP地址	威胁源(IP或URL)	威胁源国家	威胁源城市	行为	动作	次数	查看详情
09-17 17:41:58	09-17 17:41:58	恶意URL	192.168.217.61	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情
09-17 16:15:40	09-17 16:15:40	恶意URL	192.168.217.9	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情
09-17 17:44:07	09-17 17:44:07	恶意URL	192.168.217.61	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情
09-17 10:59:54	09-17 10:59:54	恶意URL	192.168.219.139	v.admaster.com.cn/j/as/51			间谍软件	拦截	1	查看详情
09-17 17:37:45	09-17 17:37:45	恶意URL	192.168.217.61	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情
09-17 15:13:47	09-17 15:13:47	恶意URL	192.168.218.59	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情
09-17 14:58:17	09-17 14:58:17	恶意URL	192.168.217.88	init.icloud-analysis.com/			间谍软件	拦截	1	查看详情

XcodeGhost 风波仍未平息

失陷手机数量统计



失陷手机回连C&C服务器次数统计



网康慧眼云，
仍然可以监测到，
大量的XcodeGhost回连C&C成功，
直到今天。。。。。

IP地址已加入网康威胁情报库

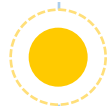
总结：方案的价值提升



边界安全性大幅提升



全局可见性大幅提升



投资回报率大幅提升

THANKS

SequeMedia
盛拓传媒

IT168
www.it168.com

ChinaUnix

ITPUB