ISC 2017

2017 中国互联网安全大会
China Internet Security Conference

数据驱动的大型央企应急响应实践

李超

石化盈科信息技术有限责任公司
信息安全实验室主任

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

- 大型央企新形势下的应急响应实践
- 数据驱动的安全运营响应体系建设

ISC 2017 中国互联网安全大会

360互联网安全中心

大型央企新形势下的应急响应实践

全球安全形势

2016-2017年，各国围绕互联网关键资源和网络空间国际规则的角逐将更加激烈，工业控制系统、智能技术应用、云计算等面临的网络安全风险进一步加大，黑客组织和网络恐怖组织等非国家行为发起的网络安全攻击持续增加，影响力和破坏性显著增强。

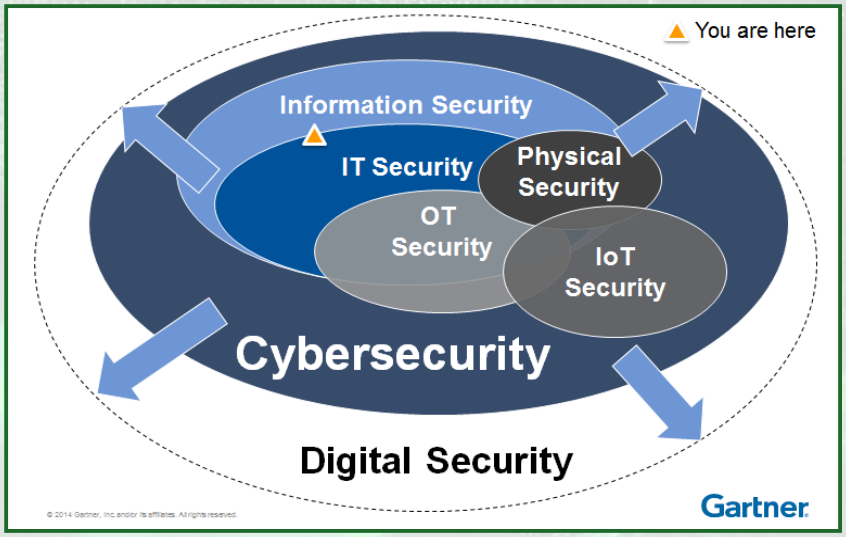
（一）全球网络空间军备竞赛风险加剧

（二）敌对势力和黑客组织的严重威胁

（三）关键信息基础设施安全隐患严重，影响国家安全

（四）新技术新应用带来了新的安全挑战

（五）互联网快速发展使网络犯罪升级



国家对于网络空间安全予以空前重视

《网络安全法》正式发布，对于安全监测、关键信息基础设施安全保护的特别要求。第二节关键信息基础设施的运行安全（31-36条，38条），第五章监测预警与应急处置（51，52，55，56）

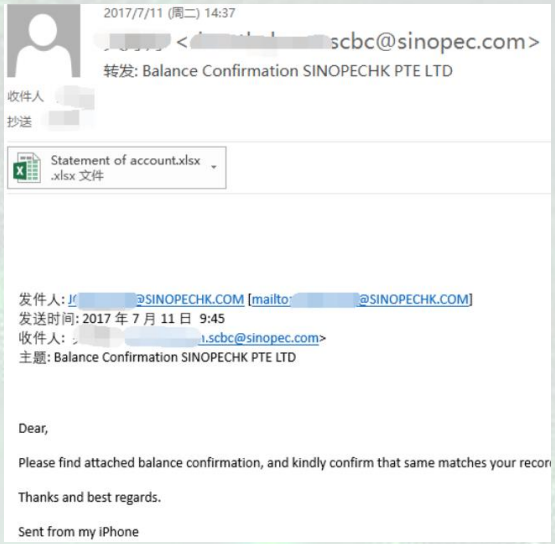
- 建立统一的监测预警、信息通报和应急处置制度和体系
- 建立健全网络安全风险评估和应急工作机制
- 建立各领域的网络安全监测预警、信息通报和应急处置制度和体系
- 网络安全信息的监测、分析和预警
- 网络安全事件的应急处置

习总书记 4.19讲话

第一次提出**“安全是发展的前提，发展是安全的保障”**，而以往都认为安全是发展的保障。

中国石化应急响应实战

“永恒之蓝”勒索病毒



邮件诈骗攻击

大规模突发事件

小范围持续APT攻击事件

勒索病毒防御战

1. 攻击思路的转变：勒索病毒的目标是数据！
2. 攻击方法的转变：网络武器民用化。
3. 攻击范围的转变：隔离网无法幸免。

勒索病毒防御战


7个数据中心


11个区域中心


数百家下属企业


上万台服务器


数十万PC终端

中国石化 零 台机器被勒索


2次下发正式通知


4期紧急通报


7份防护和修复建议


每日2次情况上报


自动化监测平台


秒级病毒告警


分钟级病毒处置

7X24小时监测

中国石化有效应对勒索病毒

领导重视，响应快速，处置得当

管理　技术

1. 集团党组紧急成立应急处置小组；

2. 信息化管理部立即启动网络安全应急预案，总部及数百家下属企业全面展开应急处置工作；

3. 启动病毒感染和处置情况“零报告”制度，企业每日10时和16时分2次向总部报告病毒感染和处置情况；

4. 通知、电话、短信、微信等多手段的应急通讯渠道快速通畅，建立了7×24小时值班制度和联络制度；

5. 面对5月15日（周一）上班电脑开机可能爆发病毒大面积感染的严峻形势，信息部14日夜和15日早连续召开两次会议，统一思想，分工负责，通过短信、邮件、公告等方式，通知总部及企业员工应对措施，“断网、备份、打补丁”等工作有序开展，有效控制了病毒的扩散。

中国石化有效应对勒索病毒

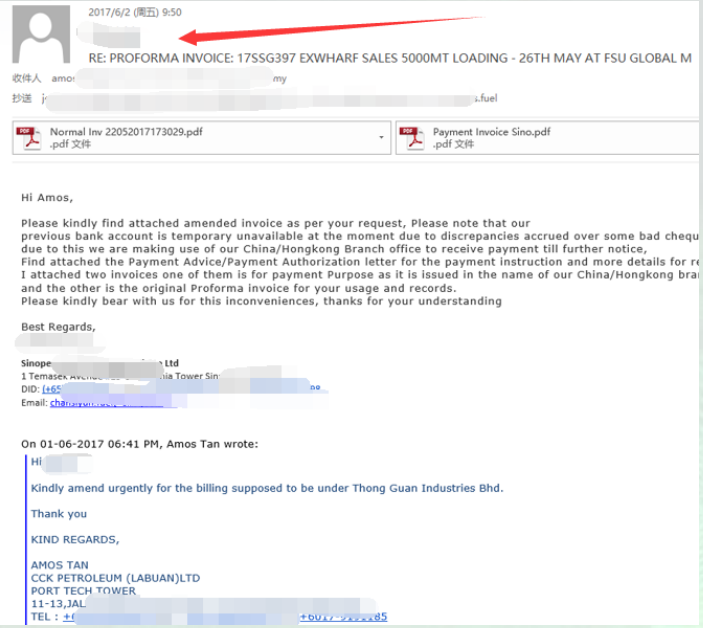
领导重视，响应快速，处置得当

管理 | **技术**

5月13日	01:00AM	获取病毒情报数据，并在一小时内完成逆向分析、通报预警工作；
5月13日	04:00AM	开始部署总部及各企业的病毒应急处置工作；
5月13日	07:00AM	向各企业下发“关于防范高危蠕虫病毒的紧急通报”；
5月13日	09:00AM	攻防团队自主设计并部署了勒索病毒监测系统，在国内率先实现了大型企业内网病毒的精准监测、告警及勒索免疫；
5月13日	至今	7X24小时不间断安全值守工作模式，邮件秒级告警。 全网445端口封锁、补丁及防病毒部署。

邮件诈骗攻击

伪造中石化员工邮箱



2017/6/2 (周五) 9:50

RE: PROFORMA INVOICE: 17SSG397 EXWHARF SALES 5000MT LOADING - 26TH MAY AT FSU GLOBAL M

收件人 amos my

抄送 j .fuel

Normal Inv 22052017173029.pdf
.pdf 文件

Payment Invoice Sino.pdf
.pdf 文件

Hi Amos,

Please kindly find attached amended invoice as per your request, Please note that our
previous bank account is temporary unavailable at the moment due to discrepancies accrued over some bad chequ
due to this we are making use of our China/Hongkong Branch office to receive payment till further notice,
Find attached the Payment Advice/Payment Authorization letter for the payment instruction and more details for r
I attached two invoices one of them is for payment Purpose as it is issued in the name of our China/Hongkong bra
and the other is the original Proforma invoice for your usage and records.
Please kindly bear with us for this inconveniences, thanks for your understanding

Best Regards,

Sinope Ltd
1 Temasek Avenue Tower Sin
DID: (+65 no
Email:

On 01-06-2017 06:41 PM, Amos Tan wrote:

Hi

Kindly amend urgently for the billing supposed to be under Thong Guan Industries Bhd.

Thank you

KIND REGARDS,

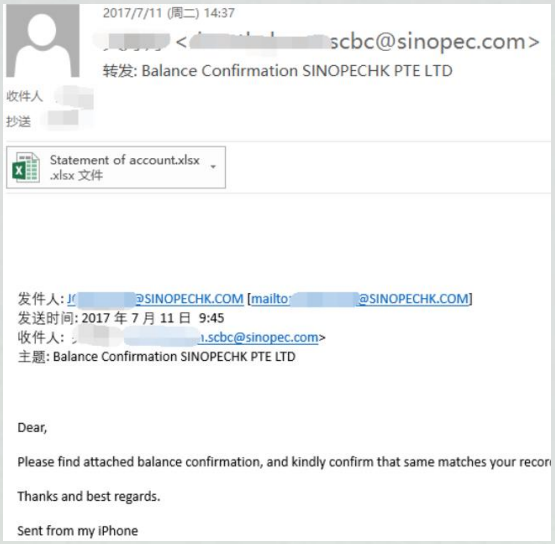
AMOS TAN
CCK PETROLEUM (LABUAN)LTD
PORT TECH TOWER
11-13,JAL
TEL : +6 +6017- d5

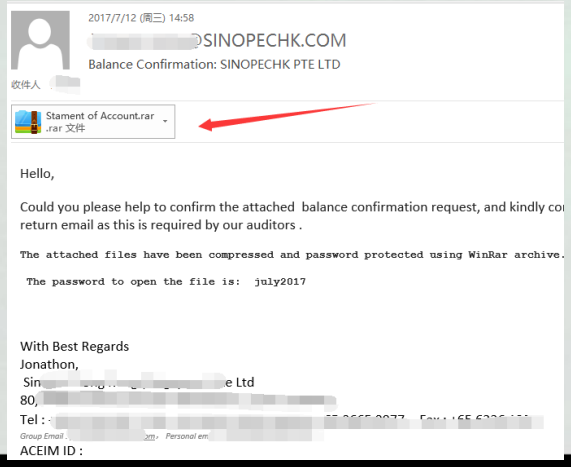
Return-Path: <info@mdxbiotech.com>
Reply-To: =?utf-8?B?5pu+5Lid6Z+1?=
<chansiyun.fuel@sin0pec.com>
From: =?utf-8?B?5pu+5Lid6Z+1?=
<[redacted]nopec.com>
To: <[redacted]m.my>,
<[redacted]cckgroup.com.my>
CC: <[redacted]gguan.com>,
<[redacted]gguan.com>,
<[redacted]ngguan.com>, g-sgops.fuel
<g-sgops.fuel@**sin0pec.com**>
Subject: RE: PROFORMA INVOICE: 17SSG397 EXWHARF SALES 5000MT LOADING - 26TH MAY AT FSU GLOBAL M
Date: Fri, 2 Jun 2017 09:50:15 +0800
Message-ID:
<20170601185015.e8d58a3387f65d48b7963e5e17cf65e8.96cf1deea4.wbe@email19.godaddy.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0025_01D2E427.C4ED4FF0"
X-Mailer: Microsoft Outlook 15.0
Thread-Index: AQJYPLrdcgznm4tBdNHcoADAJaddsQ==

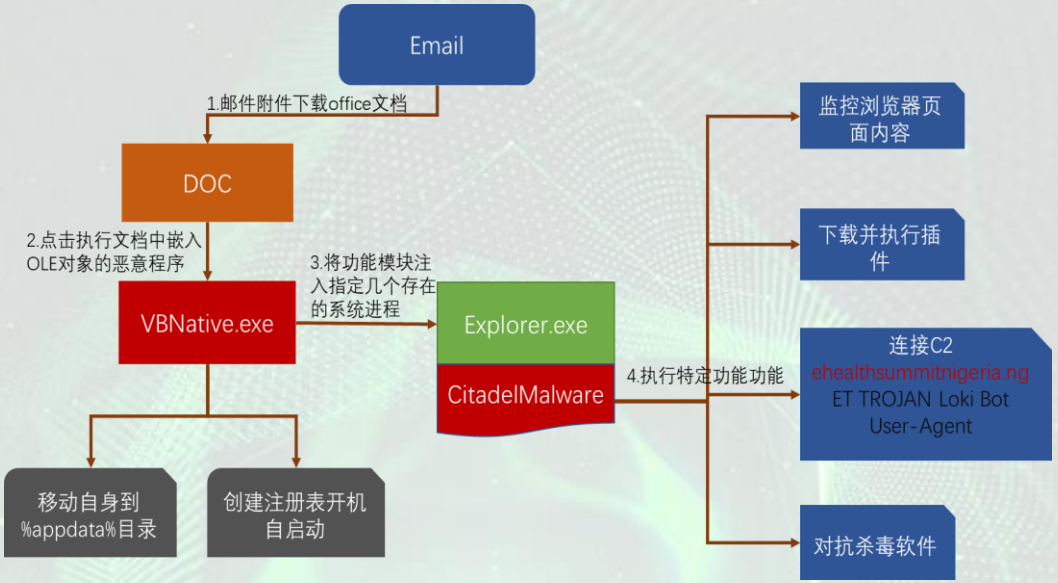
邮件头

邮件诈骗攻击

APT/社工方式窃取中石化员工邮件账户





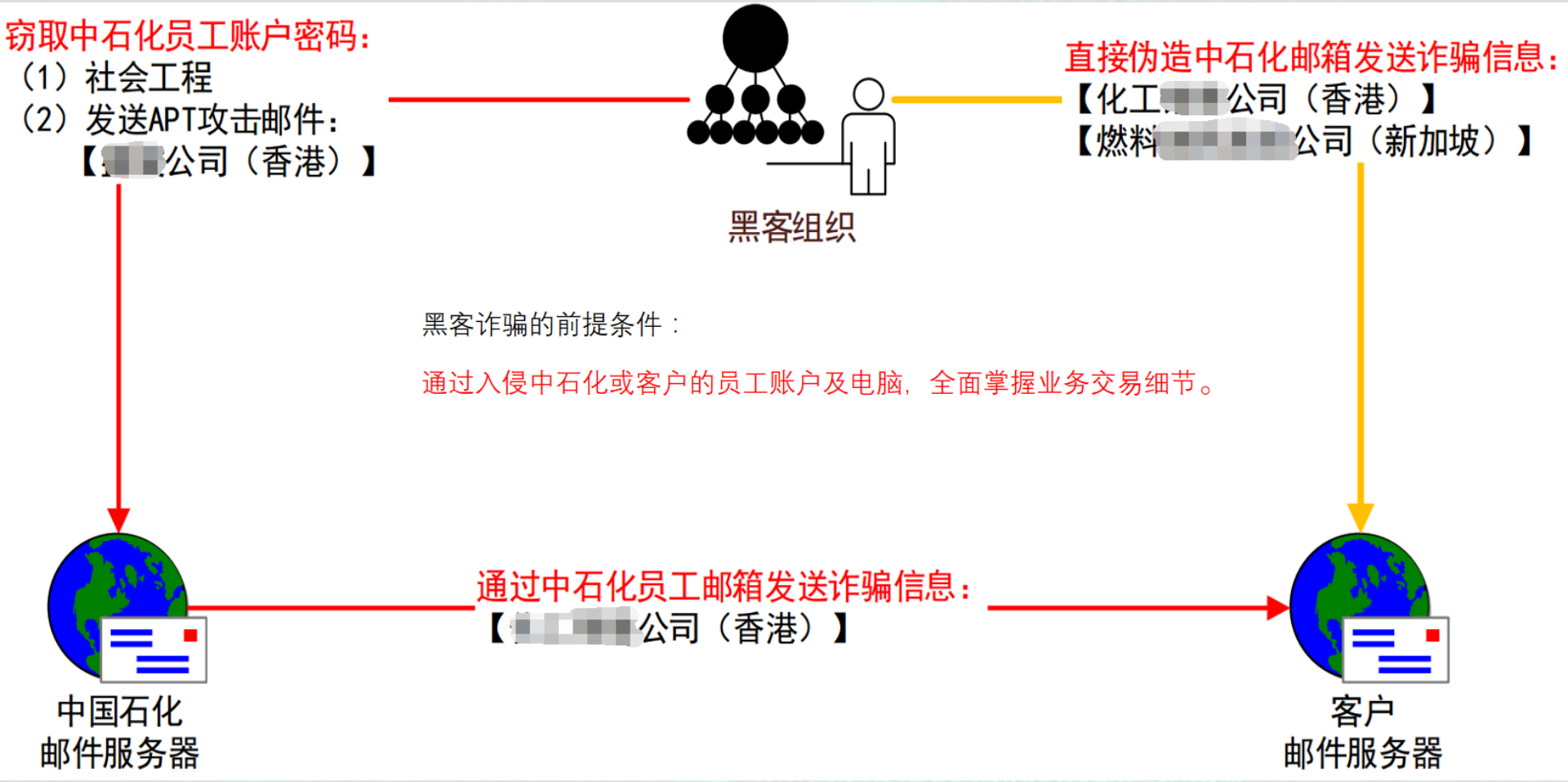


附件文件名	利用
scan-0712.doc.	CVE-2012-0158
scan-0715.doc	CVE-2012-0158
scan0717.doc	CVE-2017-0199
scan-0719.hta	HTML application（内嵌PowerShell）

- 从FTP客户端获取FTP/ HTTP密
- 窃取流行的WEB浏览器密码
- 窃取邮件(如：POP3, IMAP, SMTP)账号密码
- 窃取远程桌面账号密码信息
- 窃取比特币钱包账号密码
- 下载并执行其他木马程序

邮件诈骗攻击防御战

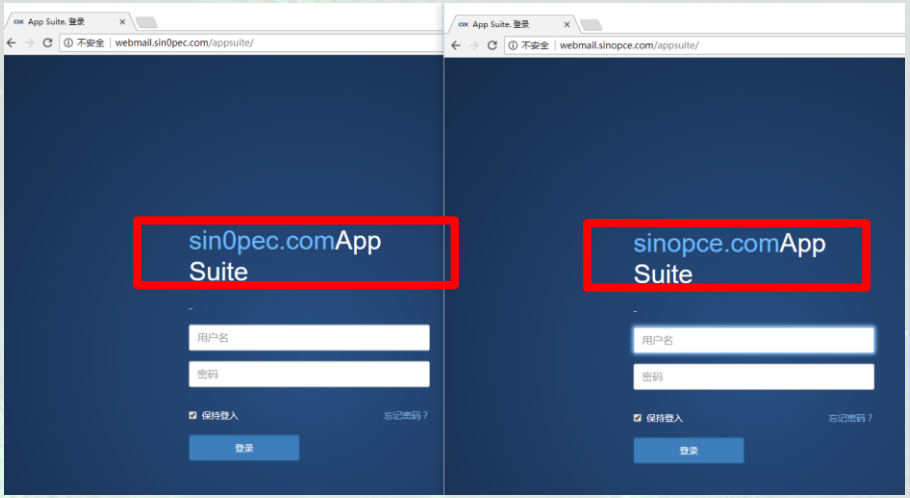
黑客组织长期攻击并潜伏企业内部，窃取业务交易细节，伺机实施诈骗！



邮件诈骗攻击组织画像

黑客注册诈骗域名用到的邮箱：

H——ng@gmail.com
S——0@yahoo.com



黑客诈骗邮件相关域名（截至目前共计116个）

黑客相关IP地址（截至目前共计24个）

webmail.*.*	pop.*.*	imap.*.*	smtp.*.*
199.79.63.241 199.79.63.243 199.79.63.227 199.79.63.110 199.79.63.239 199.79.62.248 199.79.62.62 199.79.63.206 198.251.83.215	208.91.198.215 208.91.199.246 208.91.199.6 208.91.199.116 198.251.83.215	208.91.198.215 208.91.199.246 208.91.199.6 208.91.199.116 198.251.83.215	208.91.199.225 208.91.199.224 208.91.198.143 208.91.199.223 198.251.83.215

黑客注册的所有诈骗域名都指向了同样的邮件发送系统。

邮件诈骗事件响应处置措施

1. 通过专业设备抓取区域中心网络流量，结合威胁情报进行深度安全分析，找出已经被攻陷的机器及账户，确定并封锁黑客窃取商业秘密的数据通路；
2. 持续开展追踪溯源工作，及时在全网封锁黑客相关域名及IP信息；
3. 提醒业务人员不轻易点击不明邮件附件，打好补丁，安装好防病毒，一旦发现异常及时上报总部攻防团队。
4. 海外业务交易需要经过多人电话确认后才可操作。

中国石化应急响应实战总结

大规模突发事件

快

- 组织协调快
- 情报传送快
- 决策处置快

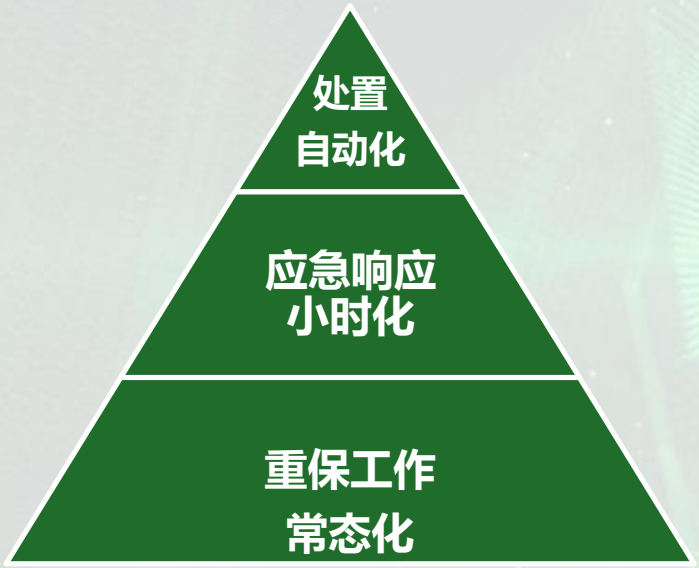
小范围持续APT攻击事件

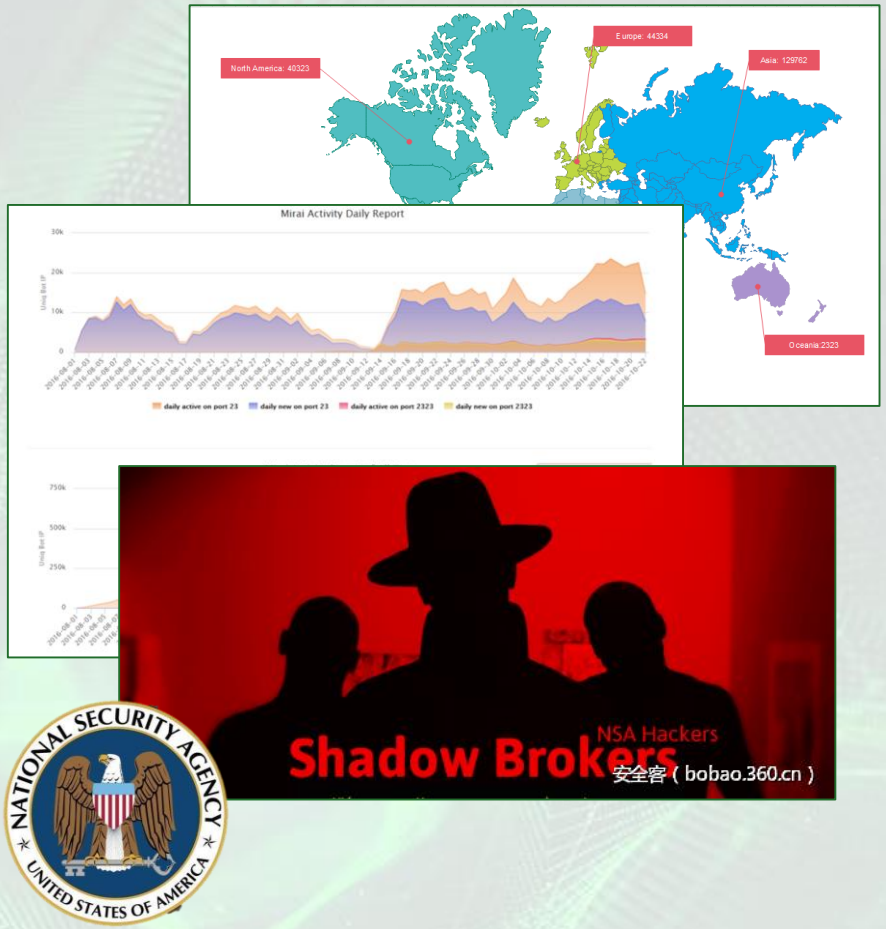
准

- 情报数据准
- 分析研判准
- 检测打击准

对抗一直在持续！

- 2017 - NSA 武器库泄漏，工具包括：永恒之蓝、永恒王者、永恒协作翡翠纤维等十多种工具
- 2017 - 多个APT在国内被发现：海莲花
- 2017，多次Strust2 高危漏洞爆发
- 2016-2017，Marai Botnet，IoT设备成为僵尸网络重要力
- 2016 - VENOM虚拟机毒液漏洞
- “反共黑客”组织





已经超越我们的传统被动防御能力！

ISC 2017 中国互联网安全大会

360互联网安全中心

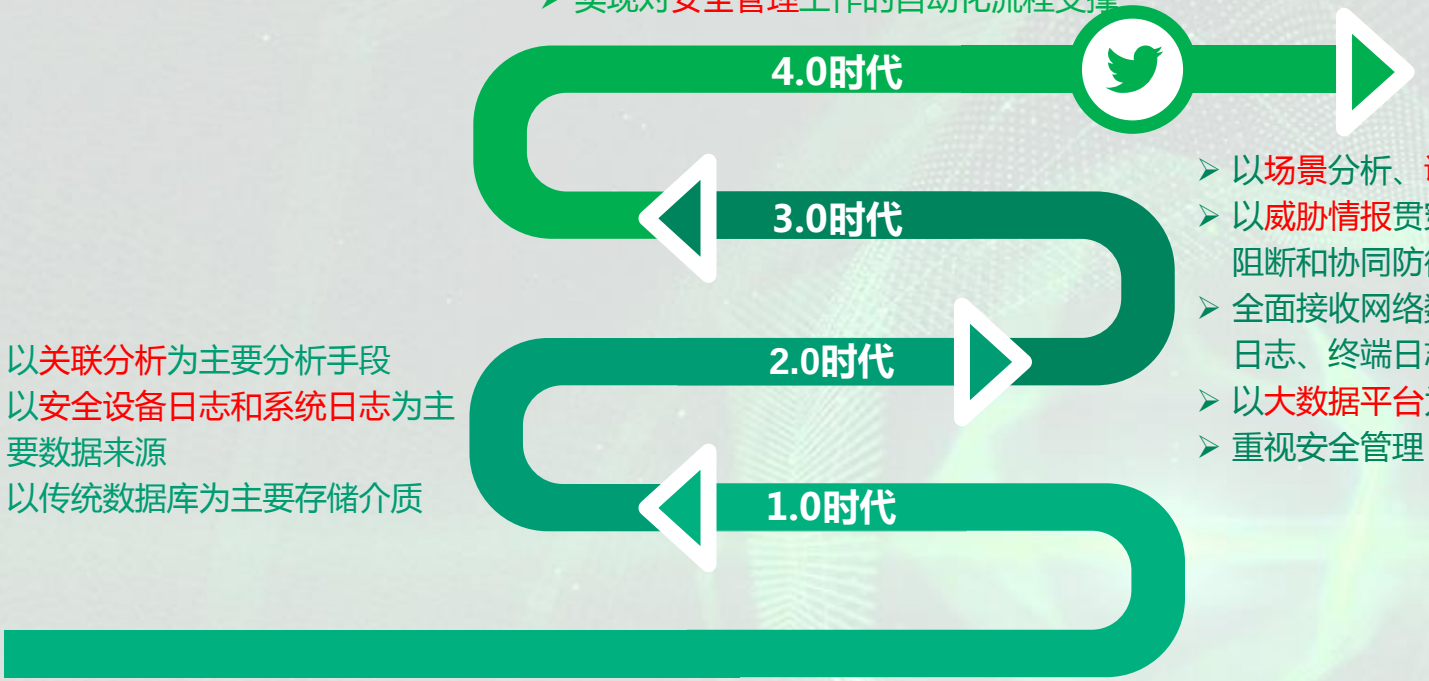
数据驱动的安全运营响应体系建设

过去20年，网络安全思想叠加演进

基础架构	被动防御	积极防御	威胁情报	威慑反制
ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
加强自身 强身健体	构筑工事 纵深防御	全面监测 快速响应	获取情报 准确预警	法律反制 威慑
✓ 安全管理体系 ✓ 安全域划分 ✓ 安全加固 ✓ 安全评估 ✓ 应用内建安全	✓ 传统安全防护 ✓ 纵深防御体系 ✓ 缩小攻击面 ✓ 消耗攻击资源 ✓ 迟滞攻击	✓ 安全大数据平台 ✓ 态势感知 ✓ 威胁情报 ✓ 自动化事件分析 ✓ 安全协同	✓ 信息收集 ✓ 情报生产 ✓ 情报分析验证 ✓ “狩猎”	✓ 法律手段 ✓ 自我防卫行为

安全响应监测与运营措施的发展

- 基于数据能力的安全运营平台
- 威胁情报成为平台的关键组成部分
- 融入自动化应急响应平台
- 建设有能力的安全运营与应急响应队伍
- 实现对安全管理工作的自动化流程支撑



- 以场景分析、调查分析为主要分析手段
- 以威胁情报贯穿拉通检测、分析、溯源、阻断和协同防御等环节
- 全面接收网络数据、安全设备日志、系统日志、终端日志和业务日志
- 以大数据平台为存储和分析平台
- 重视安全管理

- 以关联分析为主要分析手段
- 以安全设备日志和系统日志为主要数据来源
- 以传统数据库为主要存储介质

- 基于特征的单节点分析
- 全面接收安全设备日志
- 误报率、漏报率很高，被IDP告警淹没

中国石化安全运营与响应体系蓝图

威胁可知 应急可控 服务可靠 管控可视

服务支撑架构安全体系

主动防御体系

威胁情报平台为基石

大数据为安全分析基础

层次化构建被动防御体系

大数据 云计算 人工智能 互联网安全 移动互联网安全 工控物联网安全

以安全服务与应急响应平台为要点构建运营响应体系

以安全运营管控中心为核心构建主动防御体系

以自营威胁情报平台构建情报体系

以大数据分析平台为基础构建大数据整合分析能力

以先进技术平台为基础架构，层次化构建基础防御体系

应急响应体系建设

《网络安全法》第25条规定“网络运营者应当制定**网络安全事件应急预案**，**及时处置**系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，**立即启动应急预案**，采取相应的补救措施，并按照规定**向有关主管部门报告。**”

创建新的应急响应机制，**完善应急响应预案**

提升完善应急预案

建立**应急响应平台**，优化应急响应流程，借助自动化平台，大幅加快应急响应速度

建立应急响应平台

创新应急响应演练模式，提高演练的真实性和提高应急人员的技能水平

创新应急响应演练模式

应急响应平台建设

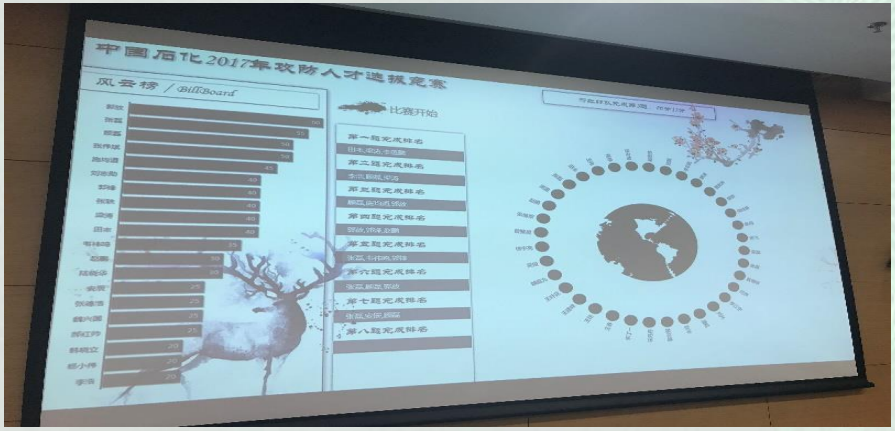
- 病毒监测
- 突发漏洞响应与检测
- 漏洞审核
- 漏洞复测
- 漏洞远程监控
- 应急经验与漏洞知识库
- 应急事件工单管理
- 应急公告管理
- 应急人员管理

应急响应队伍建设

2016年至2017年，总部组建了一支具有攻防对抗与响应处置能力的攻防团队。

能力建设

- 渗透测试能力
- 代码审计能力
- 漏洞挖掘能力
- 安全加固能力
- 安全扫描能力
- 应急响应能力
- 基线检查能力
- 调查取证能力



攻防团队**70人**

240个业务系统上线前安全评估

处理互联网通报的安全漏洞**290个**

调查处置各类重大安全事件**10起**

特殊时期**7X24小时**值守与安全保障

“反共黑客”“尼日利亚钓鱼诈骗”等重点黑客组织跟踪与对抗

有效开展勒索病毒应急处置任务

2017中央企业网络安全技术大赛团体赛**三等奖**

应急响应演练机制

信息化管理部

演练方案设计、演练过程的攻陷事件检测，收集演练过程的数据采集和分析，并完成最后的演练过程的推演和相关培训。

蓝军：负责外部攻击

进行真实攻击

- 组织攻防实验室与外部技术力量具体工作；
- 输出演习报告；
- 组织后期技术培训。

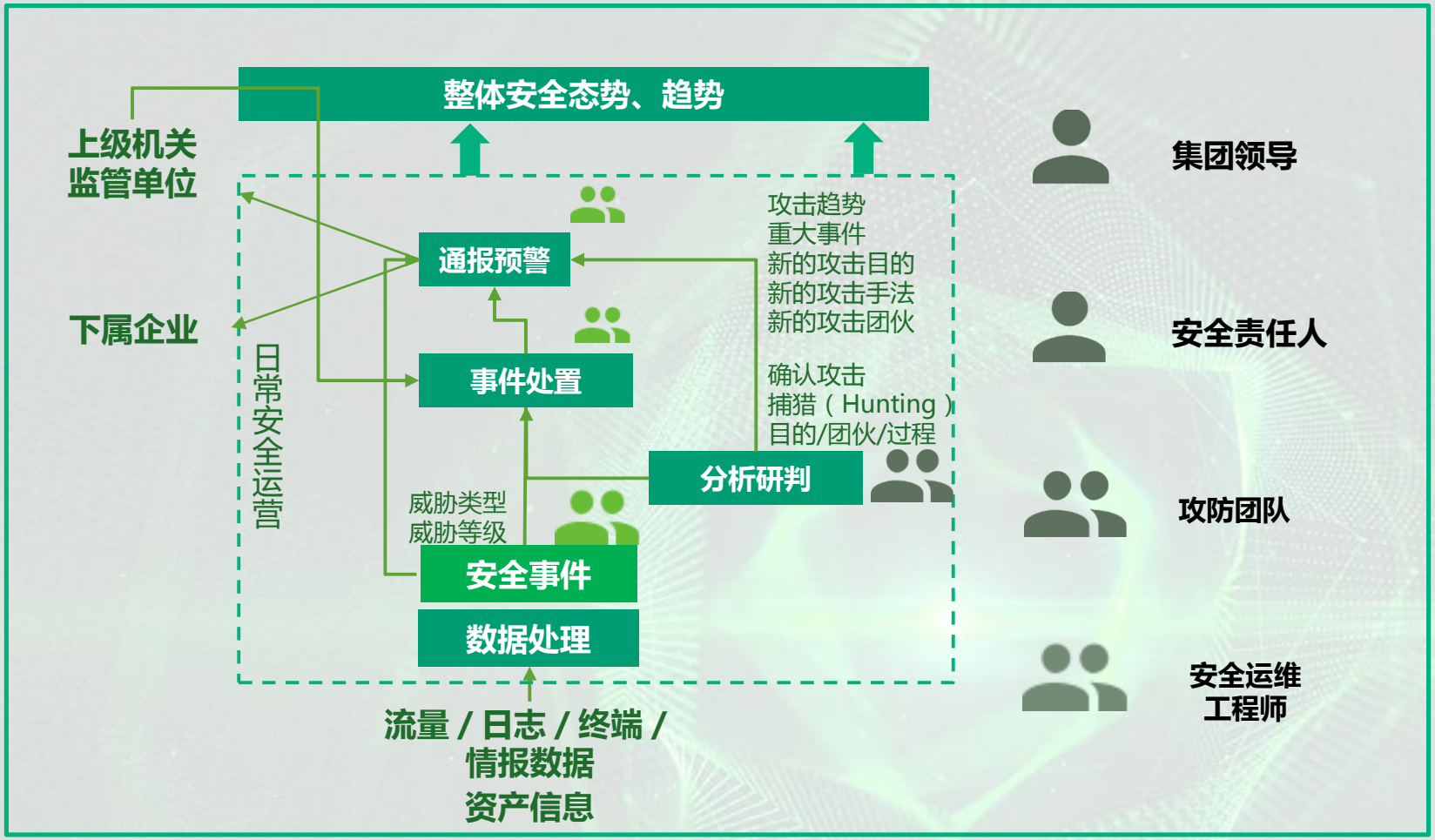
攻防团队

红军：负责内部防护

- 配合督导方面完成演练方案设计
- 基于现有防御体系开展红蓝演练的防护工作：
  - 安全设备防御策略优化
  - 安全事件监控/分析/处置
- 安全加固
- 事件追踪溯源

内部运维保障团队

“数据+平台+团队” 安全运营与应急响应体系的落地



谢谢!