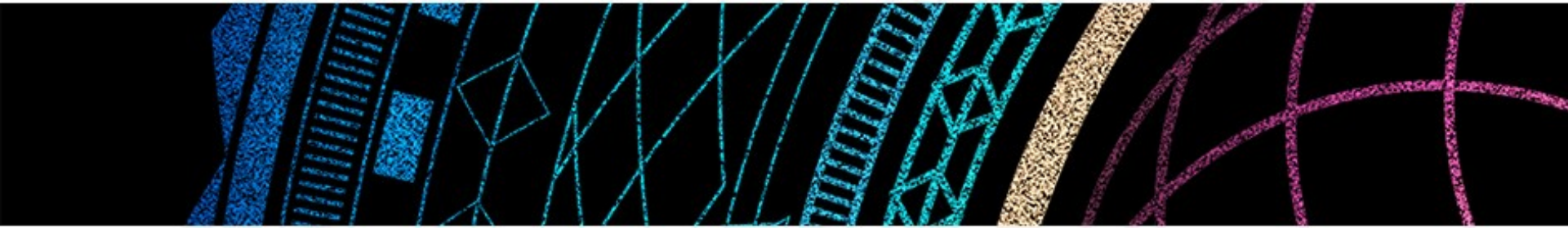
高级威胁的挑战与治理

蒋世琪，趋势科技资深产品经理



敏捷已来

Weaving The Future

Envision A Better Connected World

诺顿高管语出惊人：杀毒软件已死

2014-05-07 19:33:03 来源：新浪科技 [新闻 消费 服务 产品]

导读： 赛门铁克 信息安全高级副总裁布莱恩·代伊(Brian Dye)上周末接受《华尔街日报》采访时发表了一番令人意外的言论，他认为杀毒软件已死。 由于赛门铁克及其推出的诺顿杀毒软件多年来一直在PC安全市场处于...

赛门铁克 信息安全高级副总裁布莱恩·代伊(Brian Dye)上周末接受《华尔街日报》采访时发表了一番令人意外的言论，他认为杀毒软件已死。

由于赛门铁克及其推出的诺顿杀毒软件多年来一直在PC安全市场处于前列，因此这番言论似乎令人震惊。然而，不应被表面的言论蒙蔽：诺顿不会退休，代伊的言论只是反映了计算机防护领域的最新现状。

尽管扫描和防御电脑上的恶意软件仍然至关重要，但当今的很多复杂攻击手段仍然可以绕过杀毒软件，直接渗透到PC中。事实上，代伊对《华尔街日报》表示，他估计传统杀毒软件只能探测45%的攻击，所以效果不佳。

案例一：全球最大的动态密码锁公司研发数据外泄

RSA遭遇APT攻击 SecureID被偷

ZDNet 攻击防范 *来源：* TechTarget中国 2011年03月21日 评论(*0*)

关键词： APT RSA

本文摘要

RSA是EMC公司的安全部门，本周四，EMC公司表示，与其SecurID双因素认证产品有关的信息在"极其复杂的网络攻击"中被盗。这会带来什么影响？

RSA是EMC公司的安全部门，本周四，EMC公司表示，与其SecurID双因素认证产品有关的信息在"极其复杂的网络攻击"中被盗。

在公司网站上一封写给用户的公开信中，RSA执行董事Art Coviello表示，RSA最近检测到了该攻击。

"我们的调查告诉我们，该攻击属于先进持续威胁(Advanced Persistent Threat，ATP)的一种。调查还显示，该攻击可导致某些特定信息被从RSA系统中提取出来。这些信息有些是与RSA的SecurID双因素认证产品非常相关的。"Art Coviello这样解释道。

APT是用来描述有组织的入侵者所使用的攻击，通过该攻击，入侵者可以获得对网络的访问，其目的是在不被发现的情况下窃取信息。

RSA 承认 SecureID 令牌已被攻破

ugmbbc发布于 2011-06-08 13:12:07|8806 次阅读

感谢域名注册尽在思朴互联的投递

RSA终于公开承认，三月份进入系统的一个入侵已导致他们SecureID双因子认证的泄露。 该承认是发生在对美国军方合约商——Lockheed Martin（美国航空航天公司），L-3 Communications（技术与通讯系统制造商）以及Northrop Grumman——网络的网络攻击苏醒之后才发生的；其中一家公司已经对外确认遭受攻击，另外两家从它们内部的警报和非常规域名及密码重置进程可以推知。

RSA终于公开承认，三月份进入系统的一个入侵已导致他们SecureID双因子认证的泄露。 该承认是发生在对美国军方合约商——Lockheed Martin（美国航空航天公司），L-3 Communications（技术与通讯系统制造商）以及Northrop Grumman——网络的网络攻击苏醒之后才发生的；其中一家公司已经对外确认遭受攻击，另外两家从它们内部的警报和非常规域名及密码重置进程可以推知。

案例二：韩国多家企业业务中断

- 时间：2013年3月20日下午2时
- 韩国多家媒体与金融机构约48,700台计算机与服务器无法使用

媒体	银行
韩国广播公司（KBS） 韩国文化广播公司（MBC） 韩联社新闻台（YTN）	新韩银行 农协银行 济州银行

- 影响：
  - 业务运行中断
  - 受感染机器上的数据无法回复

这些都只是冰山一角...


Google
LOCKHEED MARTIN
RSA
The Security Division of EMC
International Monetary Fund
SONY
make.believe
PBS Be more
UNITED STATES SENATE
ADP
Adobe
citi
L3 communications
HONDA
The Power of Dreams
epsilon
还有许多攻击事件隐藏在水面之下
针对性攻击
高级持续性威胁
零日攻击
多形态攻击

国家互联网应急中心的关注

实施 APT 攻击的恶意程序频被披露，国家和企业的数据安全面临严重威胁

2012 年，“火焰（Flame）”病毒、“高斯（Gauss）”病毒、“红色十月”病毒等实施复杂 APT 攻击的恶意程序频现，其功能以窃取信息和收集情报为主，且均已隐蔽工作了数年。据 CNCERT 监测，2012 年我国境内至少有 4.1 万余台主机感染了具有 APT 特征的木马程序，涉及多个政府机构、重要信息系统部门以及高新技术企事业单位，且绝大多数这类木马的控制服务器位于境外。由于上述单位的网络信息系统中传输或存储的信息以及其自身的正常运行往往关系国家事务和经济社会运行，所以容易成为带有一定背景的组织或团体重点关注的目标，其数据安全面临严重威胁，需要各方高度重视。

2013 年值得关注的网络安全热点问题

在“宽带中国 2013 专项行动”稳步实施、移动互联网快速发展、应用终端不断丰富、信息系统云端化、资源大数据化以及国际政治经济新形势等环境因素的综合作用下，网络攻击将越来越呈现入侵渠道多、威力强度大、实施门槛低等特点，2013 年我国互联网面临的情况将更为复杂，网络安全形势将更加严峻。

恶意代码和漏洞技术不断演进，针对“高价值”目标的 APT 攻击风险持续加深，严重威胁我国网络空间安全

一是恶意代码将越来越多的具备零日漏洞攻击能力，黑客发现漏洞和利用漏洞进行攻击的时间间隔将越来越短。二是恶意代码的针对性、隐蔽性和复杂性将进一步提升，针对目标环境中特定配置的计算机可进行精准定位攻击。三是我国金融、能源、商贸、工控、国防等拥有高价值信息或对国家经济社会运行意义重大的信息系统将面临更多有组织或有国家支持背景的复杂 APT 攻击风险，轻则影响涉事企业的生存和发展，重则影响国家经济在全球的核心竞争力，甚至可能危及国家安全。

来源：CNCERT 2012年我国互联网网络安全态势综述

来自 Gartner 的建议

- 始终跟上威胁的发展变化
- 建构多层次防御体系
- 改进事件响应功能

Gartner

G00224682

Best Practices for Mitigating Advanced Persistent Threats

Published: 18 January 2012

Analyst(s): Lawrence Pingree, Neil MacDonald

Many security practitioners see the term "advanced persistent threat" (APT) as primarily a marketing term and do not acknowledge that there are advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems. Organizations face an evolving threat scenario that they are ill-prepared to deal with. They must respond to these threats with the proper techniques and technologies. This research will enable security practitioners to understand the new threats they face and the best-practice steps they must take in order to reduce the risk of compromise against the advanced adversaries taking direct aim at their organizations.

来自 Gartner 的建议

- **始终跟上威胁的发展变化**
- 建构多层次防御体系
- 改进事件响应功能

Gartner

G00224682

Best Practices for Mitigating Advanced Persistent Threats

Published: 18 January 2012

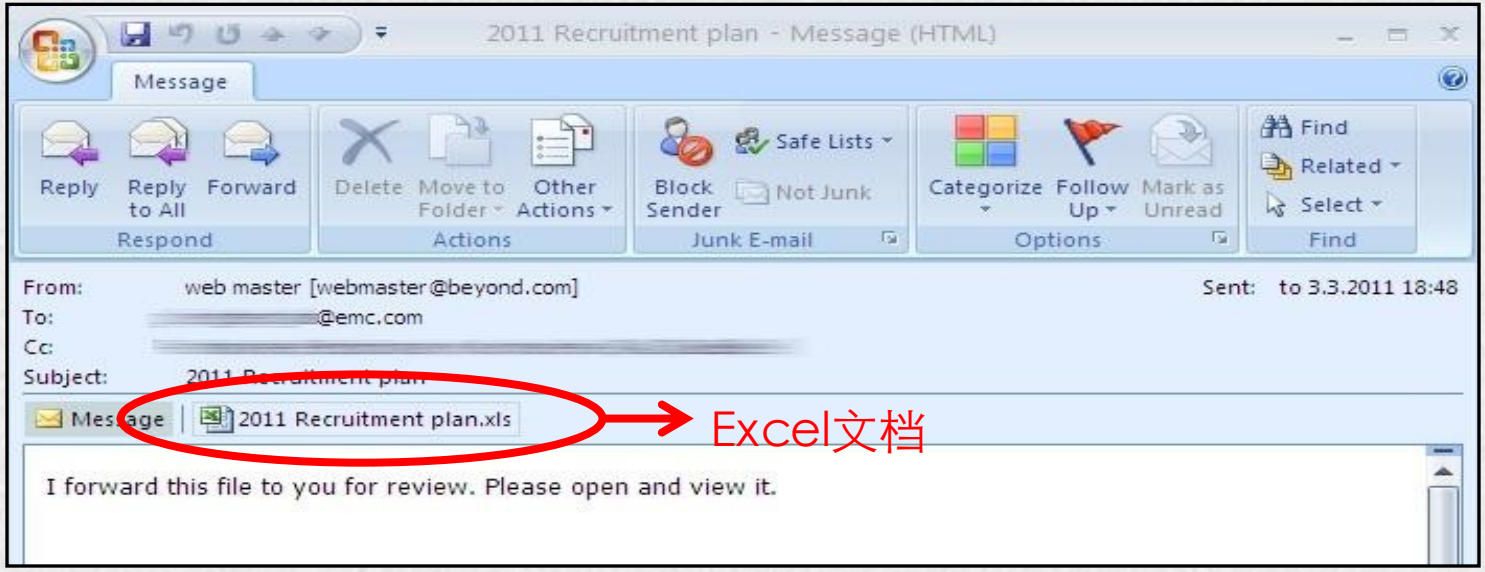
Analyst(s): Lawrence Pingree, Neil MacDonald

Many security practitioners see the term "advanced persistent threat" (APT) as primarily a marketing term and do not acknowledge that there are advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems. Organizations face an evolving threat scenario that they are ill-prepared to deal with. They must respond to these threats with the proper techniques and technologies. This research will enable security practitioners to understand the new threats they face and the best-practice steps they must take in order to reduce the risk of compromise against the advanced adversaries taking direct aim at their organizations.

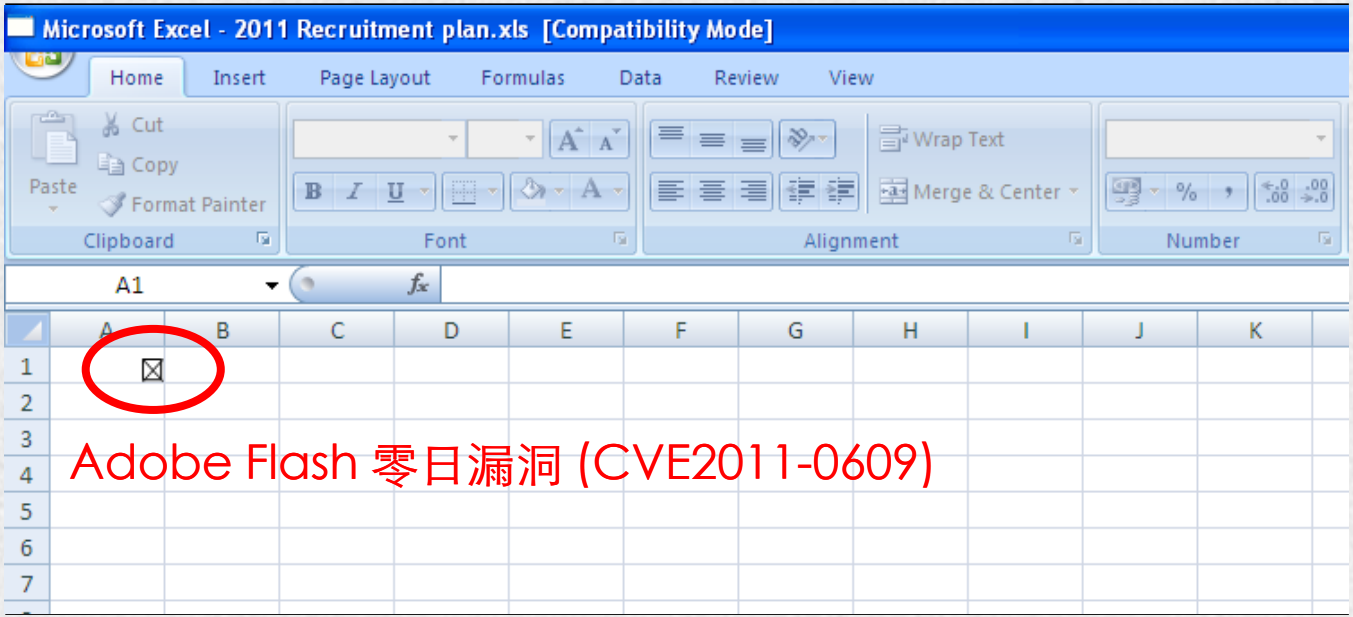
RSA攻击事件


RSA
EMC²
Speaking of Security
The Official RSA Blog and Podcast
Subscribe Here
Subscribe to the RSA blogs and podcasts for the latest posts and security updates!
Sign Me Up Now!
Home
About
Search
Topics
Authentication
Cloud Security
Compliance
Consumer Security
Cybercrime and Fraud
Anatomy of an Attack
Written on April 1, 2011 by Uri Rivner
Comments (42)
I was on a tour in Asia Pacific when I first heard the news about the attack. The investigation into this attack continues but I'm eager to share some information with you about it.
Let's first make sure everyone is on the same page. The number of enterprises hit by APTs grows by the month, and the range of APT targets includes just about every industry. Unofficial tallies number dozens of mega corporations attacked; examples are in the press regularly, and some examples are here, and here.
Speaking of Security Podcast
Tokenization: An Alternative Form of Data Protection – Podcast# 232
CyberShop 'til You Drop – Staying Safe Online this Holiday Season – Podcast #231
RSA Reaches Milestone of 500,000 Phishing Attacks Shut Down – Podcast #230

RSA攻击事件：由一封以假乱真的邮件开始



RSA攻击事件：由一封以假乱真的邮件开始



RSA攻击事件过程

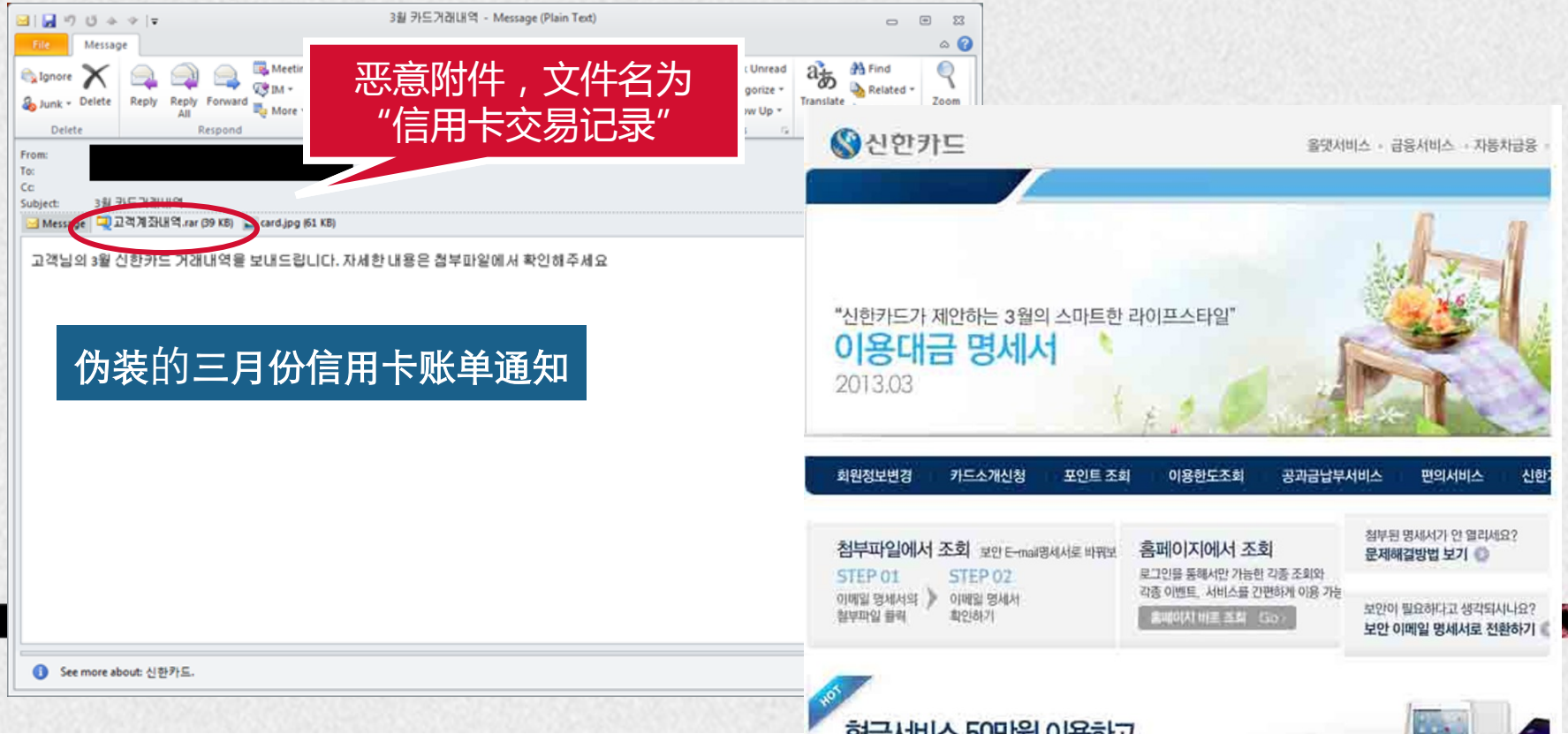
根据Uni Rivner的调查，这起造成RSA史上最重大损害的源头，是2封锁定RSA公司内两小群员工的网络钓鱼邮件。标题写着「2011年招募计划」，也夹带一个附加文档

这个Excel文档包含一个当时还没有发现、也还没有被修补的Adobe Flash零日漏洞

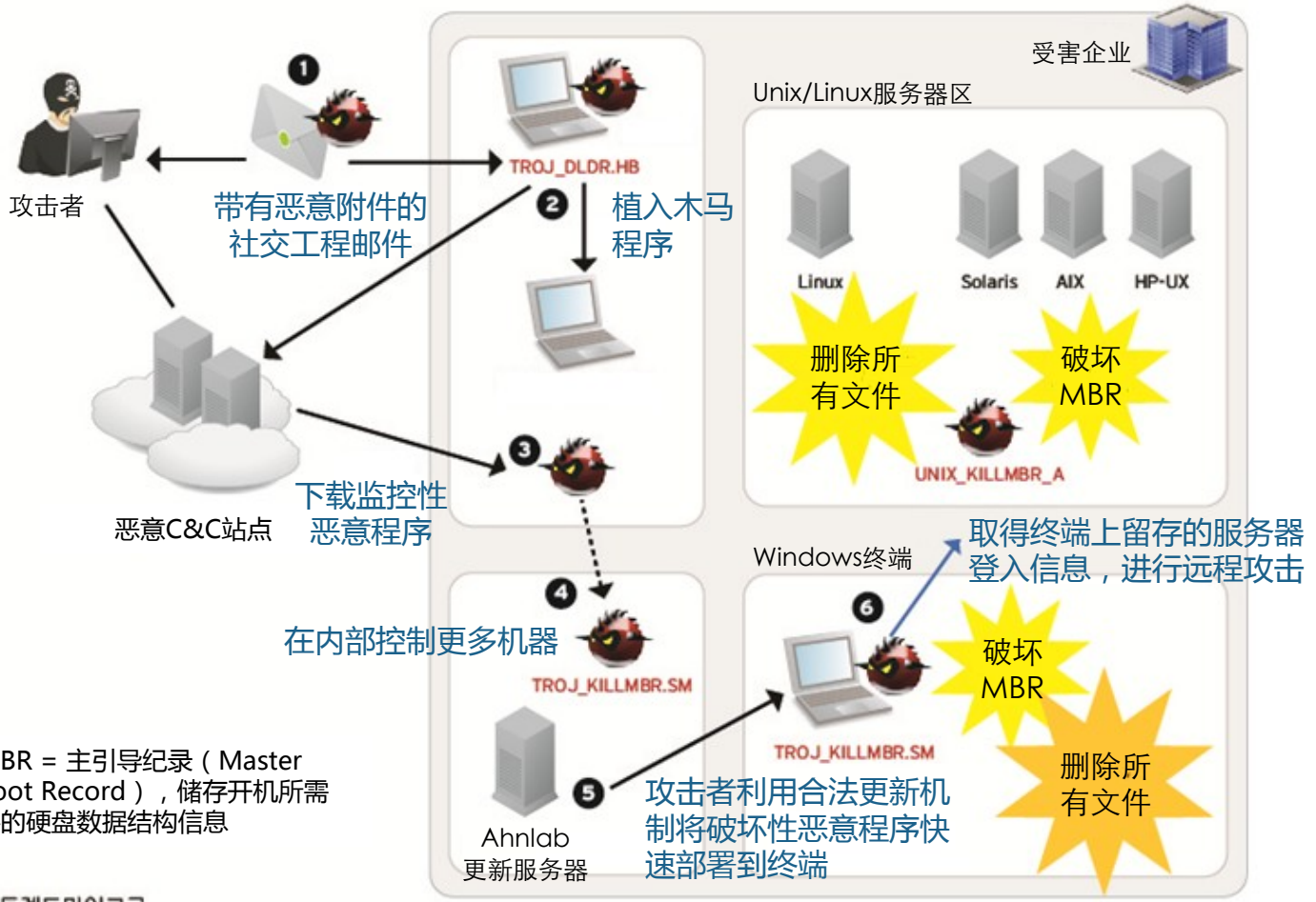
该员工计算机植入后门后，被远程遥控在内部做探测取得更高管理者权限

入侵开发用服务器，加密并压缩机密数据用FTP传到远程主机，清除入侵痕迹

320韩国攻击事件：伪装成银行通知的邮件



320
韩国攻击事件过程

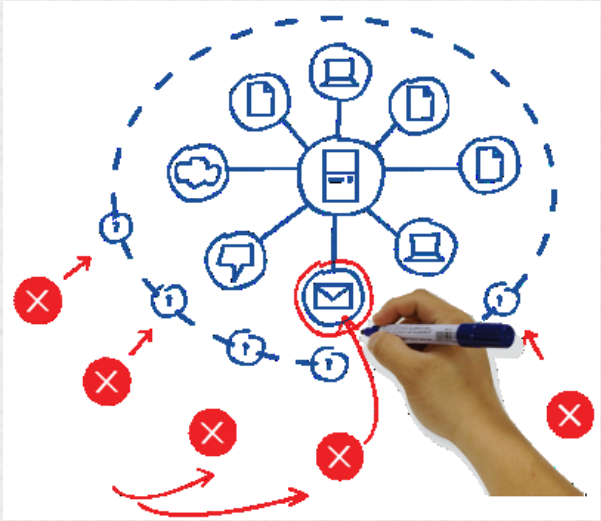


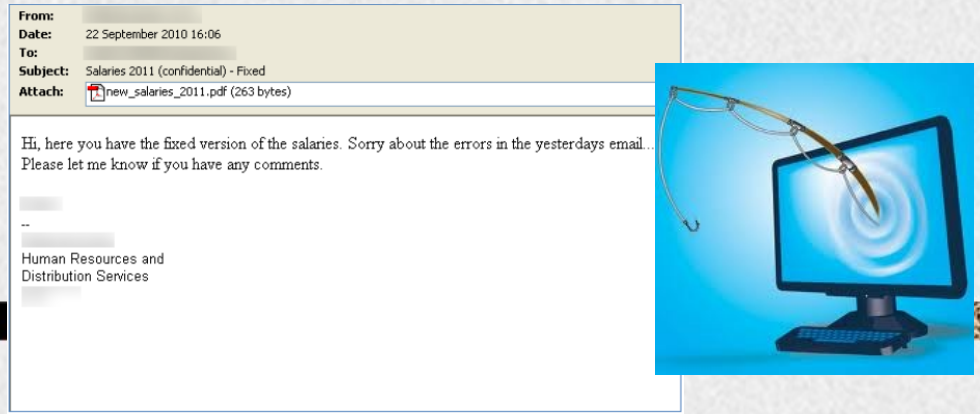
MBR = 主引导纪录（Master Boot Record），储存开机所需要的硬盘数据结构信息

출처 – 트렌드마이크로

APT攻击的序曲：社交工程邮件

95%的APT攻击利用了社交工程钓鱼邮件——即使是最针对性或最恶意的攻击，也经常仰赖简单的技巧。

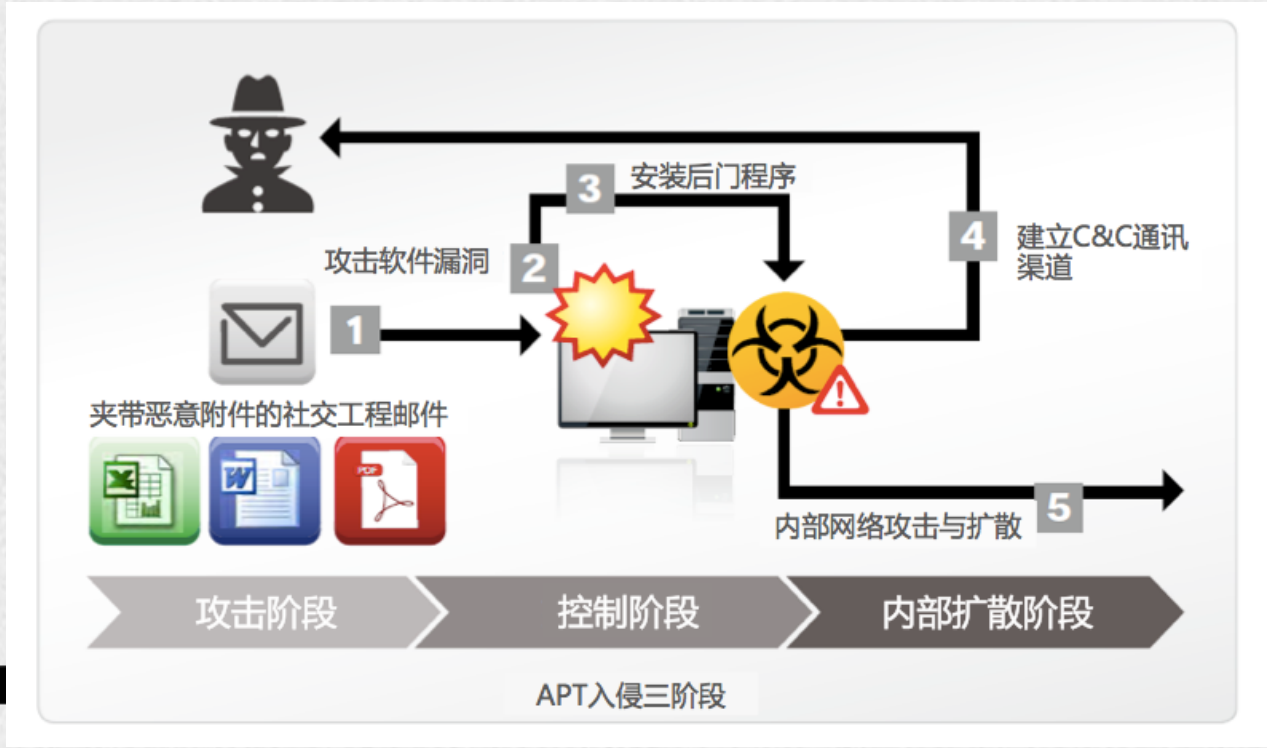



From:
Date: 22 September 2010 16:06
To:
Subject: Salaries 2011 (confidential) - Fixed
Attach: new_salaries_2011.pdf (263 bytes)

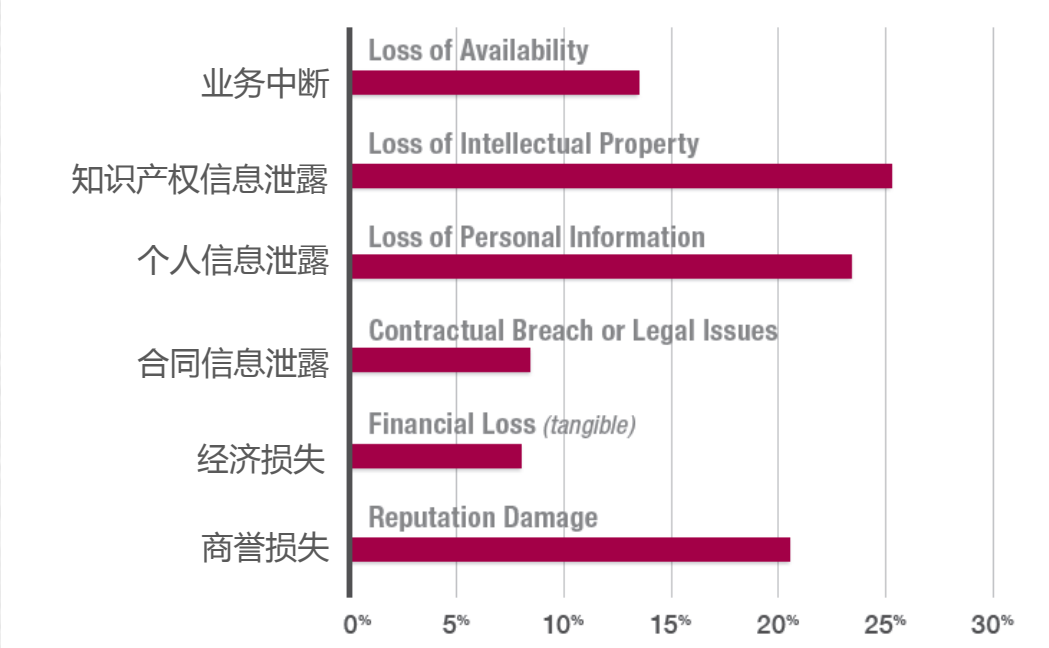
Hi, here you have the fixed version of the salaries. Sorry about the errors in the yesterdays email...
Please let me know if you have any comments.

--
Human Resources and
Distribution Services

APT攻击模型

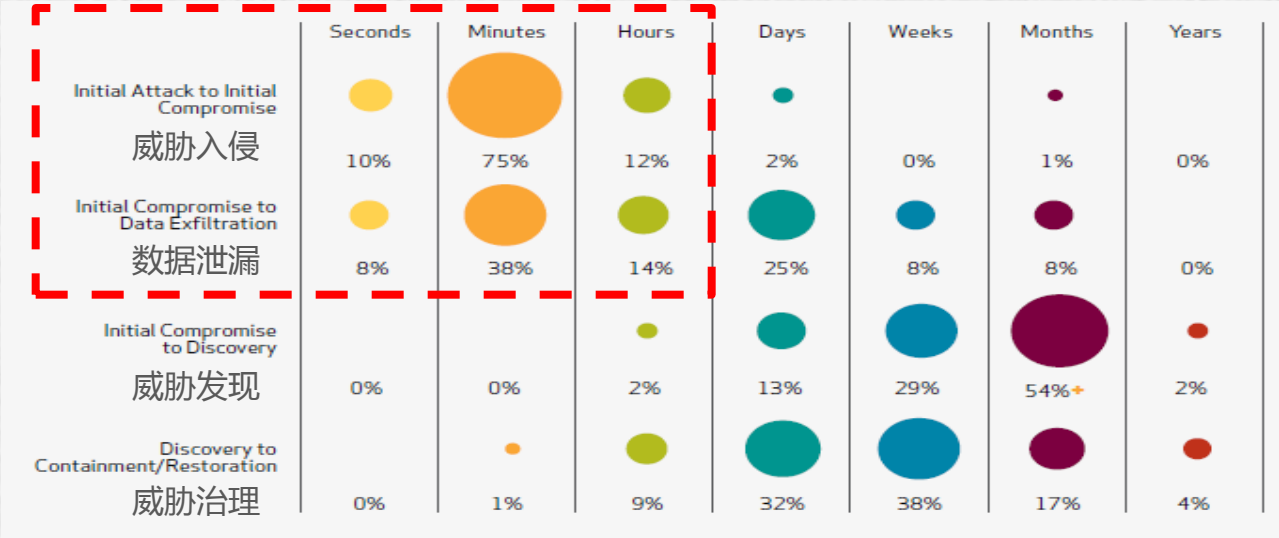

3
安装后门程序
4
建立C&C通讯渠道
攻击软件漏洞
2
1
夹带恶意附件的社交工程邮件
5
内部网络攻击与扩散
攻击阶段
控制阶段
内部扩散阶段
APT入侵三阶段

APT造成的后果



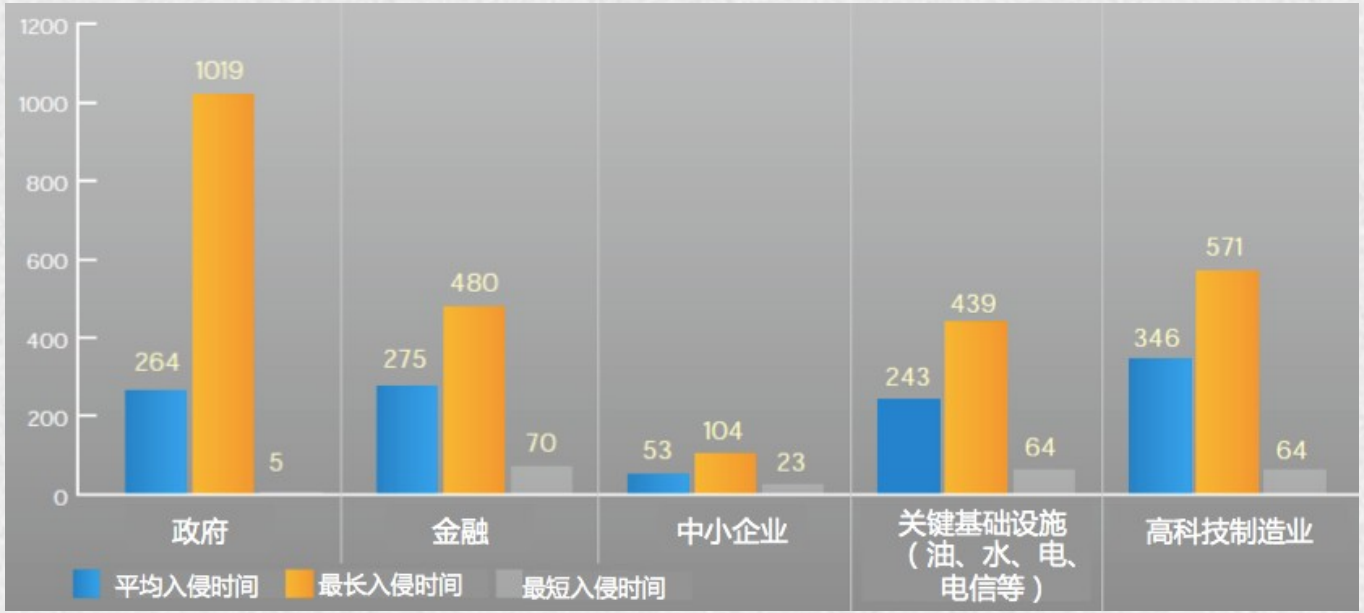
来源：ISACA APT Awareness Study

企业何时发现APT攻击？



来源：Verizon Data Breach Investigations Report 2012

企业何时发现APT攻击？



来源：趋势科技 2013 年 APT 调查

APT的防护困难点

- 针对性、客制化的攻击
  - 针对攻击目标环境
  - 针对攻击目标的防护机制
  - 客制化的恶意软件
- 高资源、高端技术的攻击
  - 零时差攻击
  - 黑客素质高
- 攻击范围小
  - 量小不易发觉
  - 攻击样本难以取得
- 长期、不间断的纠缠
  - 落叶扫不尽，秋风吹又堆

现有安全防护为何不足？

- **社交工程邮件**制作精巧，寄送数量少，甚至发送自信任的联络人，不会被认为是垃圾邮件
- 边界安全设备（如防火墙、IPS等）大多针对由外向内的攻击，**邮件、U盘、移动设备**等能够轻易绕过这些防御，直接进入企业网络内部
- 攻击者多使用**未知恶意程序**，以特征码比对为基础的安全产品无法辨识
- 恶意程序多**由内向外**发起恶意通讯，**频率低**，入侵防御设备难以发现异常
- 当攻击者取得内部员工账号密码，**合法登入服务器**原则上不会被记录

来自 Gartner 的建议

- 始终跟上威胁的发展变化
- **建构多层次防御体系**
- 改进事件响应功能

Gartner

G00224682

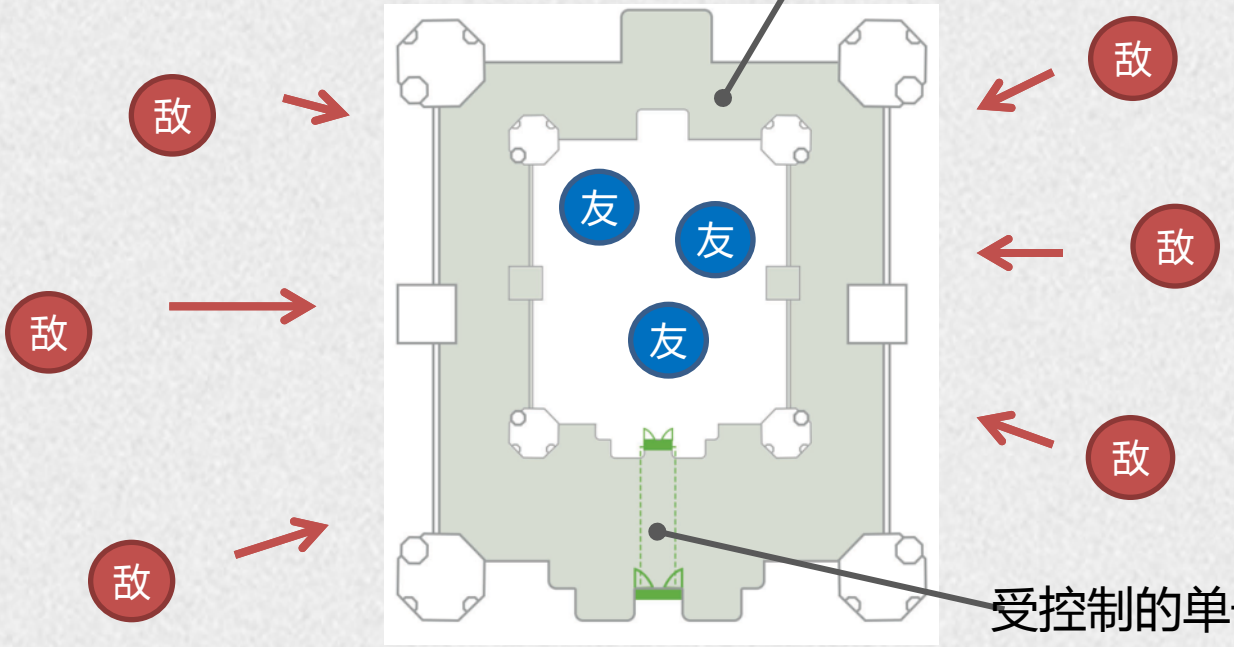
Best Practices for Mitigating Advanced Persistent Threats

Published: 18 January 2012

Analyst(s): Lawrence Pingree, Neil MacDonald

Many security practitioners see the term "advanced persistent threat" (APT) as primarily a marketing term and do not acknowledge that there are advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems. Organizations face an evolving threat scenario that they are ill-prepared to deal with. They must respond to these threats with the proper techniques and technologies. This research will enable security practitioners to understand the new threats they face and the best-practice steps they must take in order to reduce the risk of compromise against the advanced adversaries taking direct aim at their organizations.

传统安全防护思维



逐渐模糊的企业边界

针对性攻击
钓鱼邮件

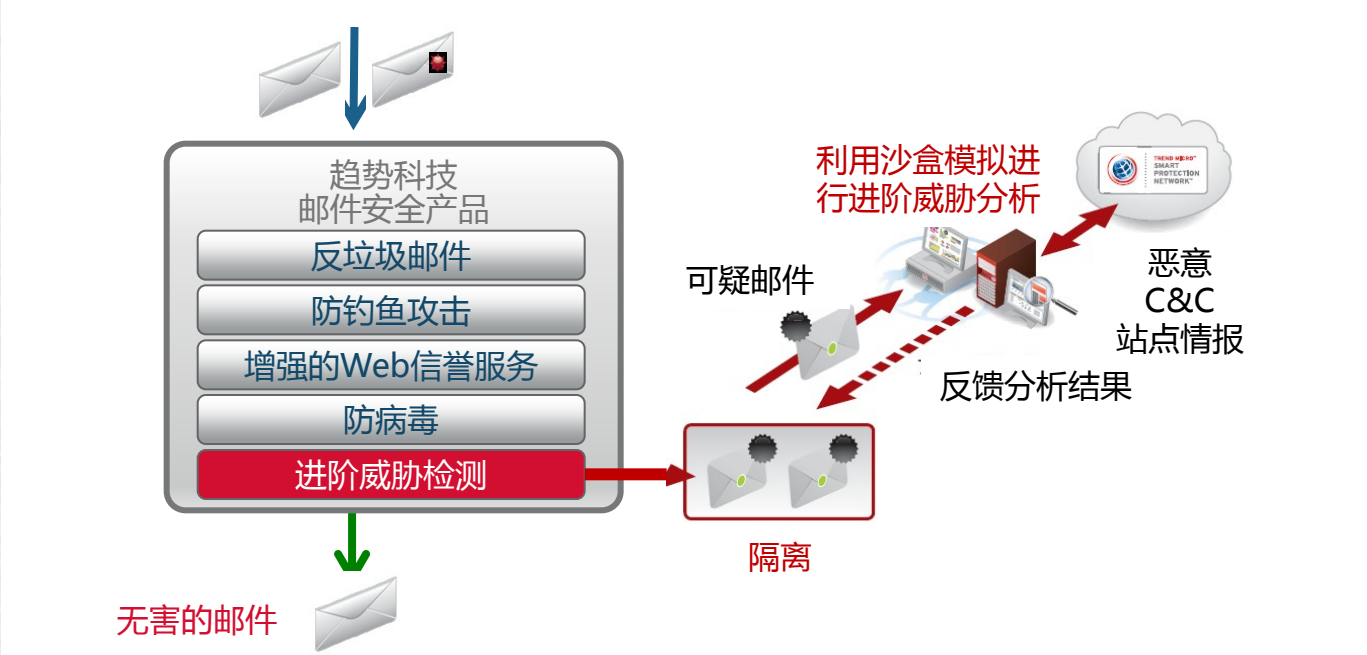
移动设备

云计算

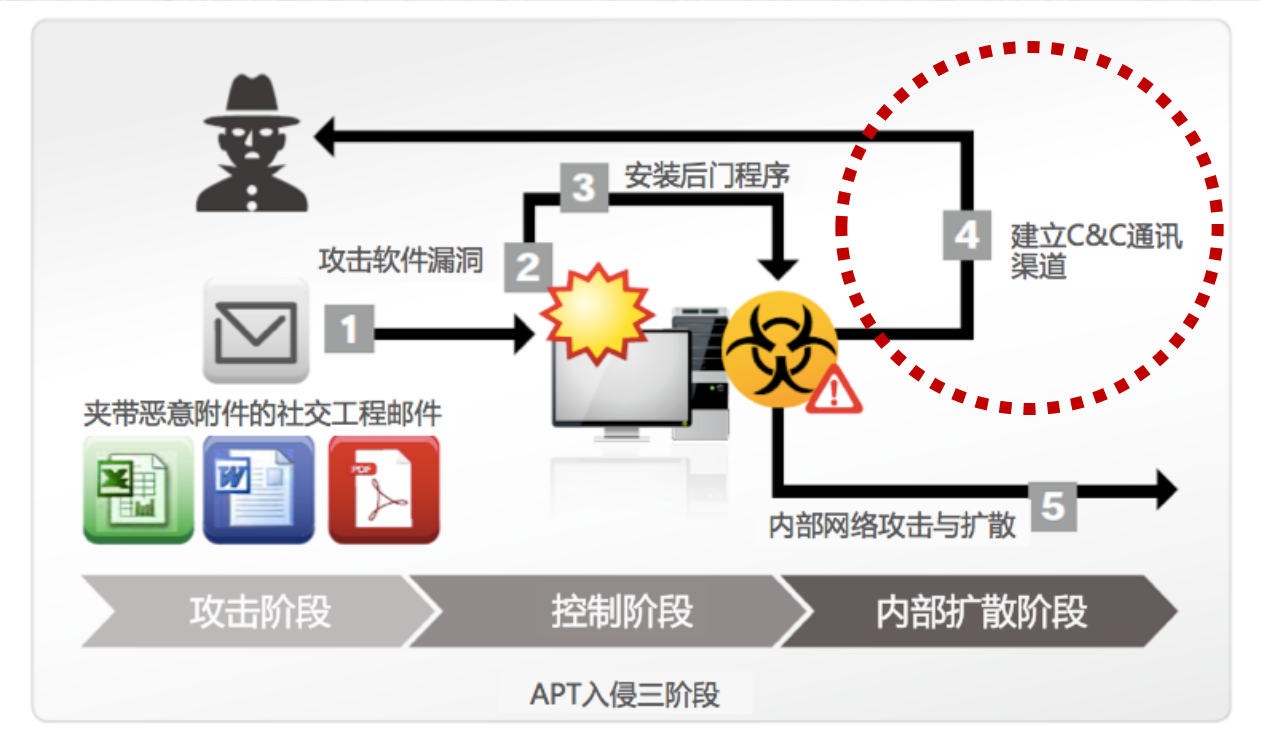
新的安全防护思维——多层次防御

攻击阶段：检测并阻挡社交工程邮件

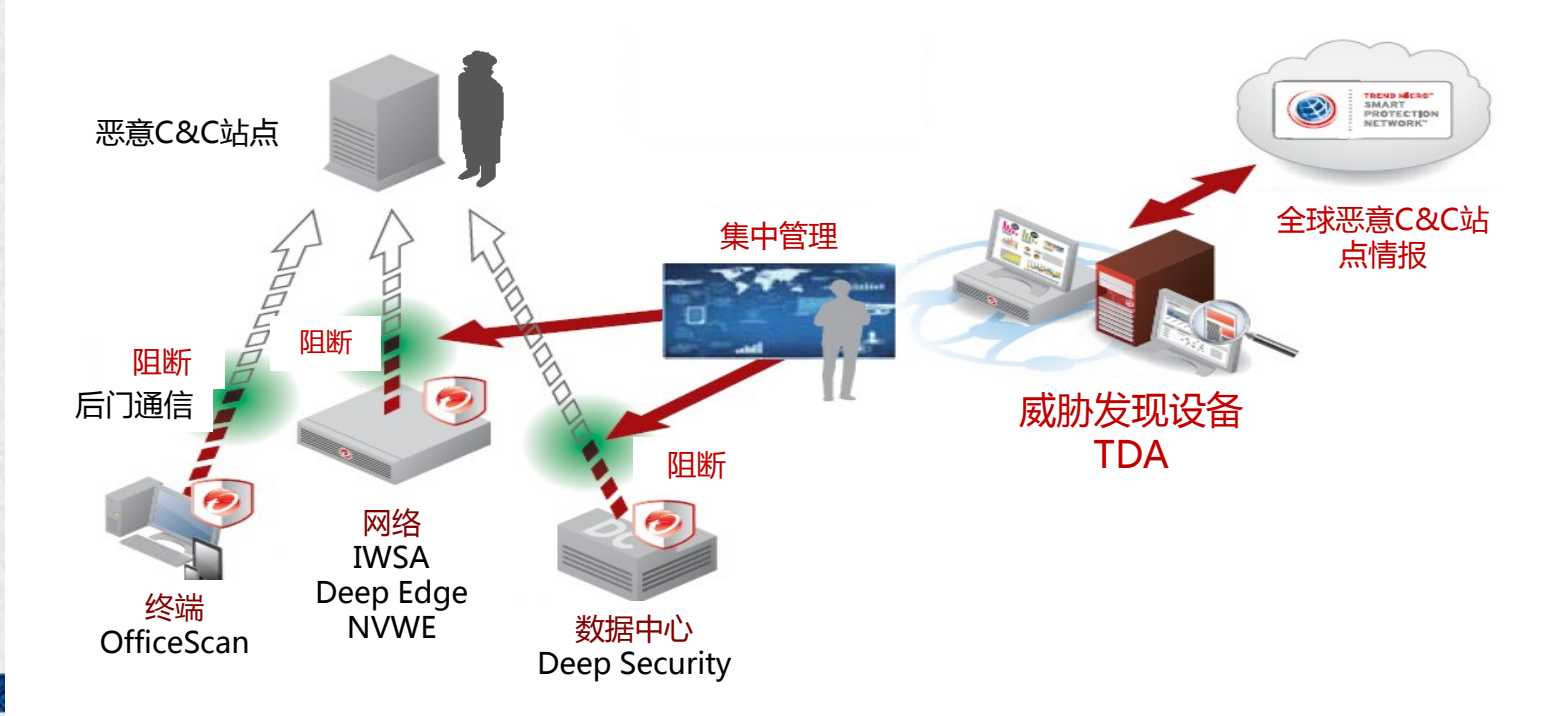
攻击阶段：检测并阻挡社交工程邮件



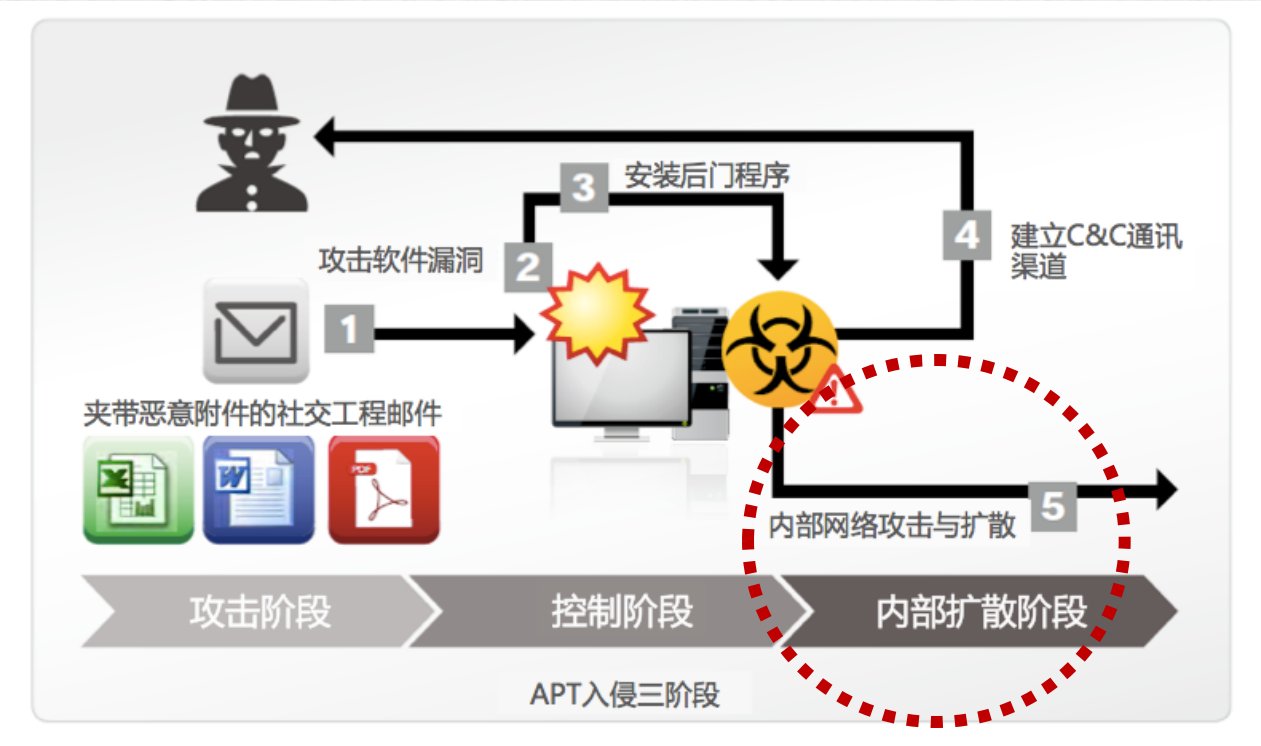
控制阶段：封阻C&C幕后操纵通讯



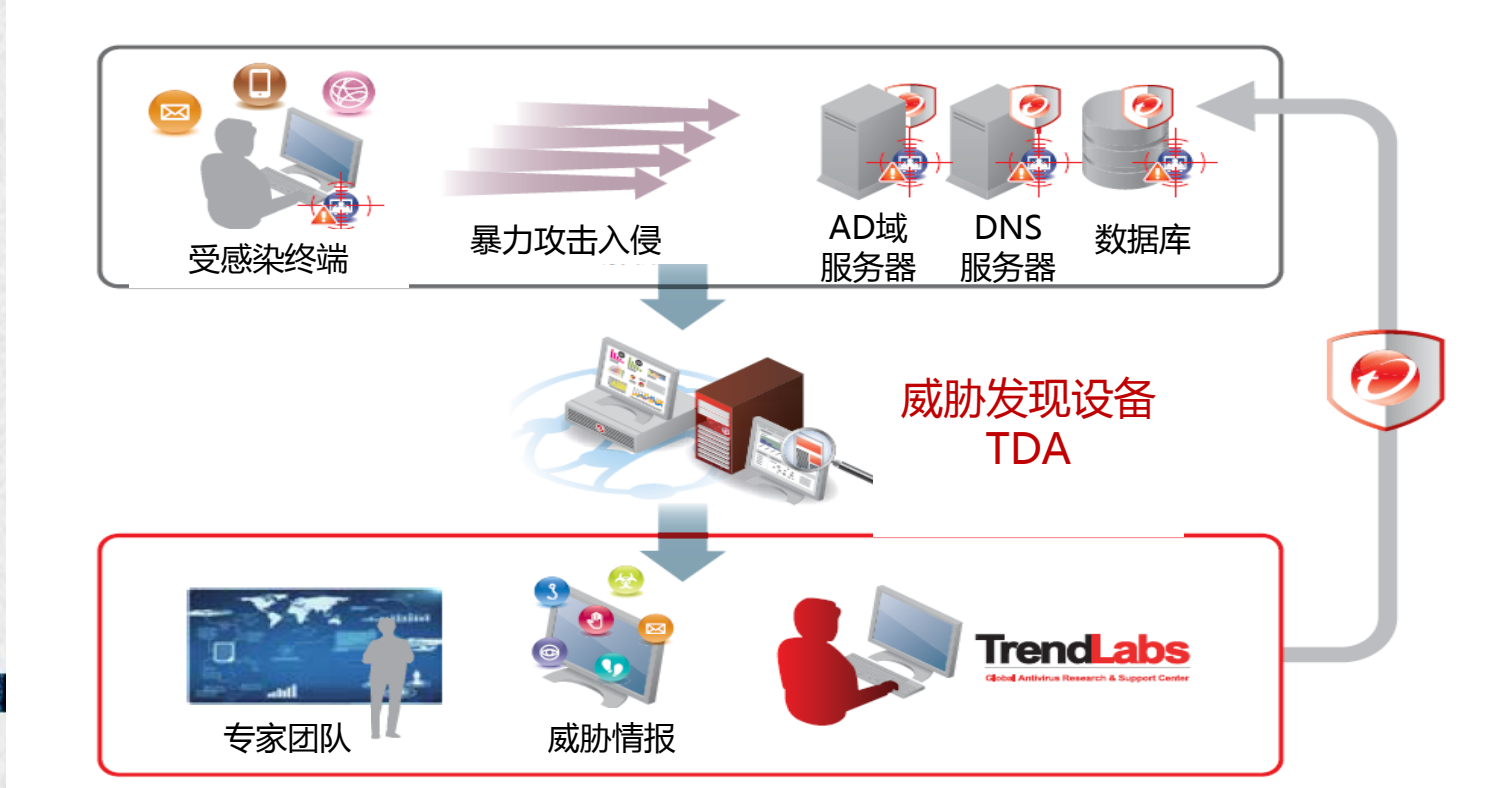
控制阶段：封阻C&C幕后操纵通讯



内部扩散阶段：监控内部访问与威胁活动



内部扩散阶段：监控内部访问与威胁活动



来自 Gartner 的建议

- 始终跟上威胁的发展变化
- 建构多层次防御体系
- **改进事件响应功能**

Gartner

G00224682

Best Practices for Mitigating Advanced Persistent Threats

Published: 18 January 2012

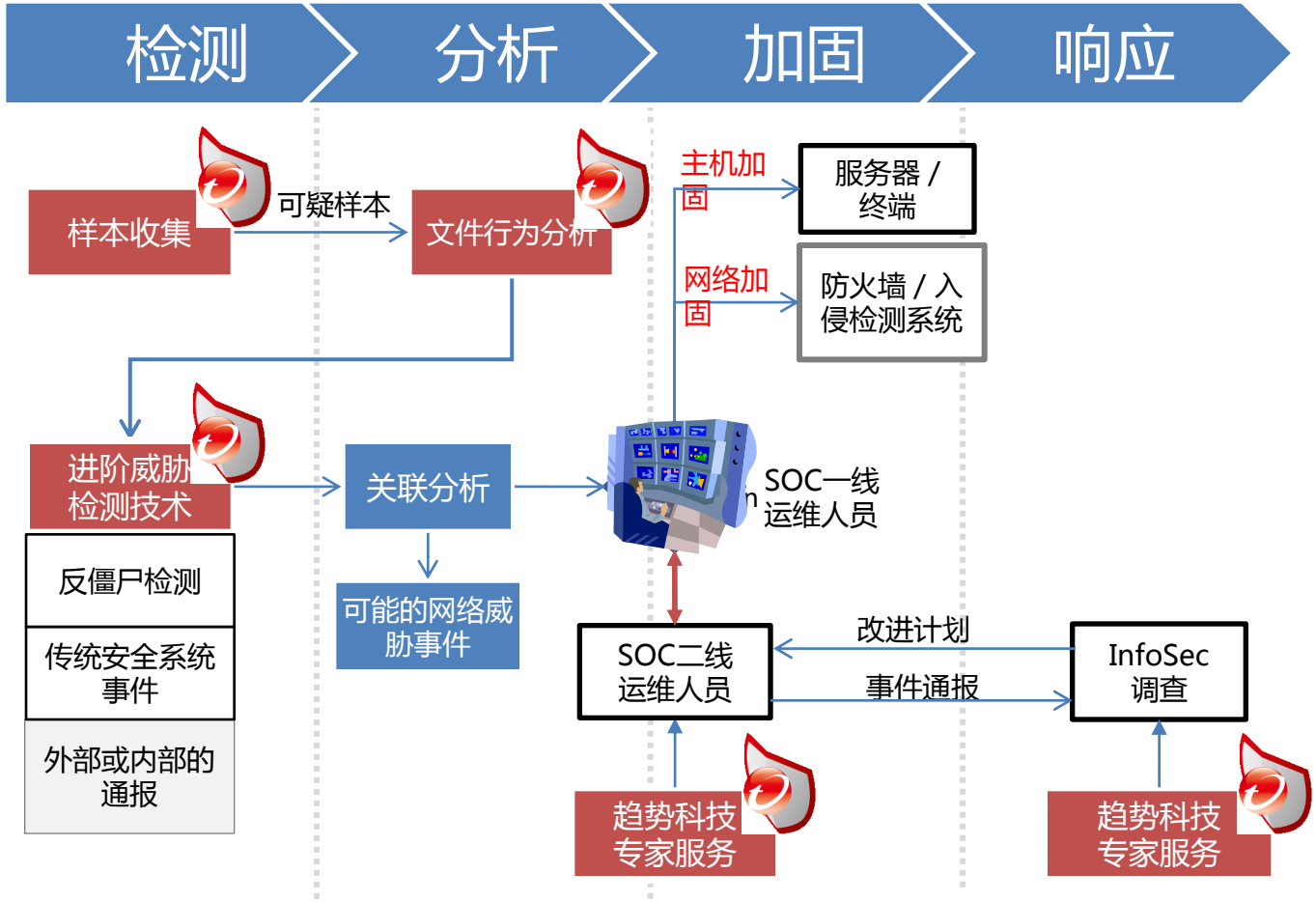
Analyst(s): Lawrence Pingree, Neil MacDonald

Many security practitioners see the term "advanced persistent threat" (APT) as primarily a marketing term and do not acknowledge that there are advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems. Organizations face an evolving threat scenario that they are ill-prepared to deal with. They must respond to these threats with the proper techniques and technologies. This research will enable security practitioners to understand the new threats they face and the best-practice steps they must take in order to reduce the risk of compromise against the advanced adversaries taking direct aim at their organizations.

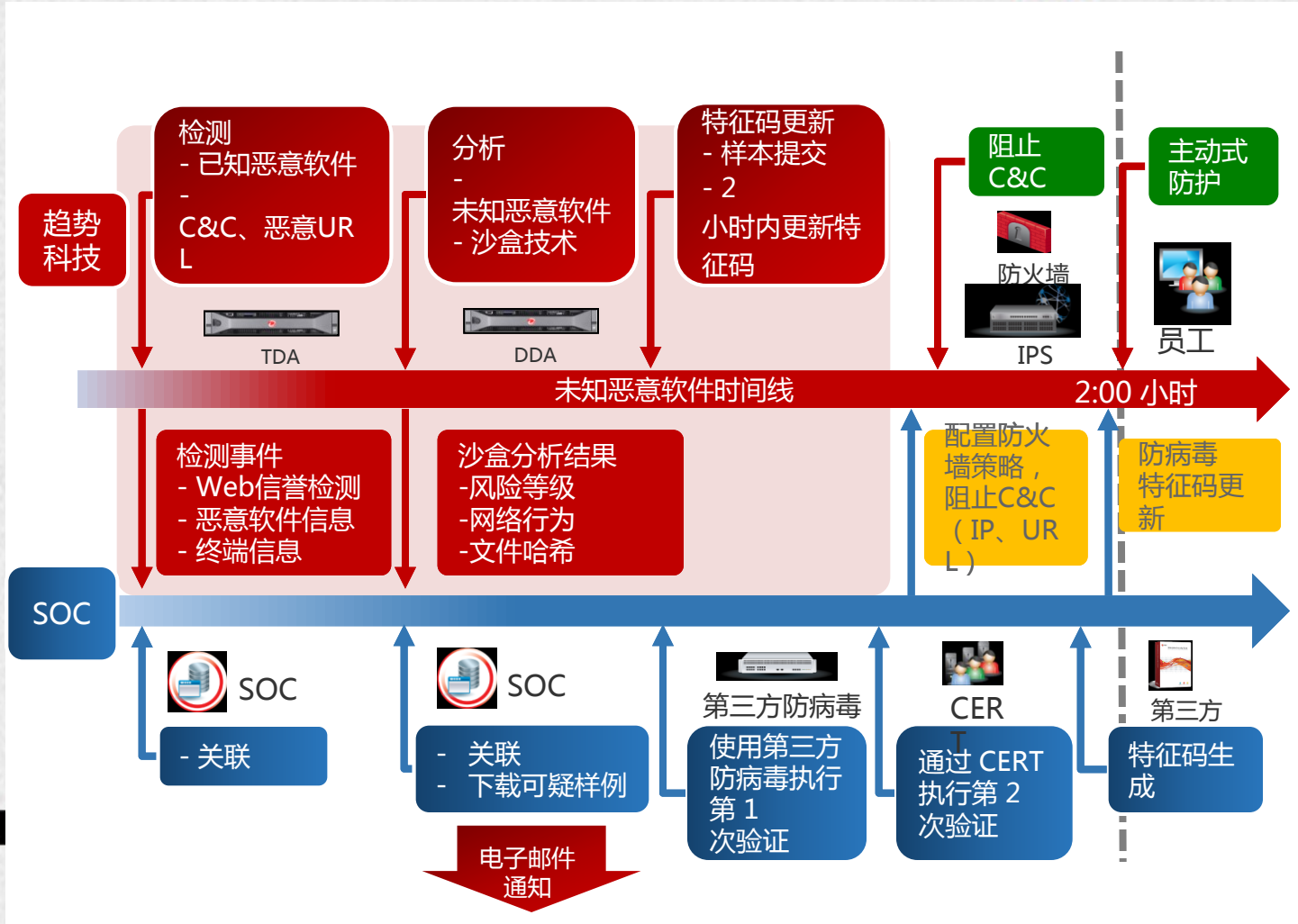
趋势科技定制化智能防御战略

侦测		无论在网络还是在其他端点，具备智能威胁侦测能力
分析		本地深度分析，搭配全球智能，完整分析恶意程序行为
加固		自定义安全黑名单与特征码，在各个端点阻断未来的攻击
响应		调查网络事件，侧写攻击者活动，提供治理解决方式

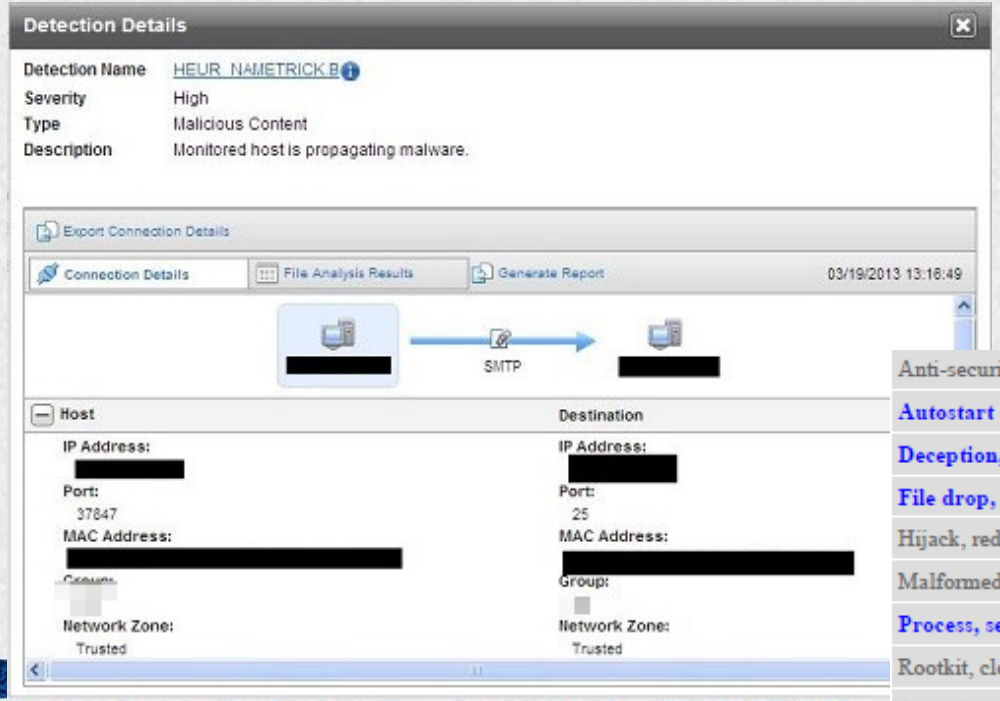
事件响应流程模型


检测
分析
加固
响应
样本收集
可疑样本
文件行为分析
主机加固
服务器 / 终端
网络加固
防火墙 / 入侵检测系统
进阶威胁检测技术
关联分析
SOC一线运维人员
反僵尸检测
传统安全系统事件
外部或内部的通报
可能的网络威胁事件
SOC二线运维人员
改进计划
事件通报
InfoSec 调查
趋势科技专家服务
趋势科技专家服务

实际应用案例：韩国银行客户



TDA成功截获社交工程邮件，提早告警



Anti-security, self-preservation	
Autostart or other system reconfiguration	✓
Deception, social engineering	✓
File drop, download, sharing, or replication	✓
Hijack, redirection, or data theft	
Malformed, defective, or with known malware traits	
Process, service, or memory object change	✓
Rootkit, cloaking	
Suspicious network or messaging activity	✓
Possible malware detected	

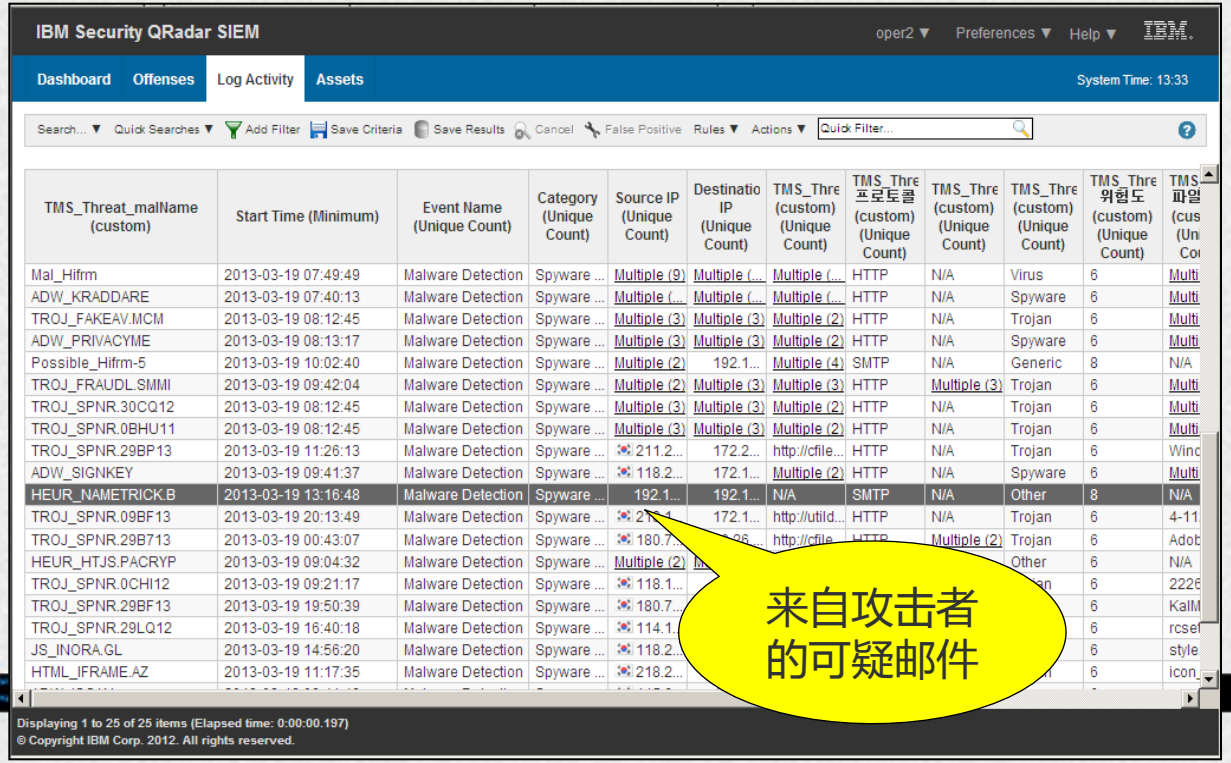
沙盒分析提供响应情报

Threat Behaviors by Category	
File drop, download, sharing, or replication	
Behavior	**Details**
Renames downloaded file	URL: http://wwwimages.adobe.com/www.adobe.com/ubi/template/identity/adobe/screen/gnav.css File: %windir%\system32\gscreem.exe
Renames downloaded file	URL: http://www.6885.com/uploads/fb9c6013f1b269b74c8cd139471b96fc/feng.jpg
Renames downloa	

Network Traffic

Remote Host	Protocol	Port	Requests
184.84.208.11 (wwwimages.adobe.com)	http	80	1
121.14.231.54 (www.6885.com)	http	80	1
174.35.3.29 (s1.daumcdn.net)	http	80	1
210.112.177.55 (cardimage.shinhancard.com)	http	80	1
116.125.220.28 (www.clickflower.net)	http	80	1

可疑事件集中到内部SOC平台监控管理



APT攻击治理成本

总结

攻击阶段

检测并隔离社交工程邮件，在第一时间防御APT攻击

控制阶段

发现并阻断恶意C&C通讯，阻止黑客进一步控制内部机器

内部扩散阶段

监控内部访问与威胁活动，发现黑客活动的蛛丝马迹并抑制其意图

HUAWEI

谢谢

敏捷已来

Weaving The Future

Envision A Better Connected World