第三届
全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

APT之特种木马检测

李薛

东巽科技（南京）有限公司

对话·交流·合作

目录

APT攻击事件频繁

APT（Advanced Persistent Threat）高级持续性威胁，是针对特定组织所作的复杂且多方位的高级渗透攻击。

2009：极光攻击

2010：震网攻击核电站

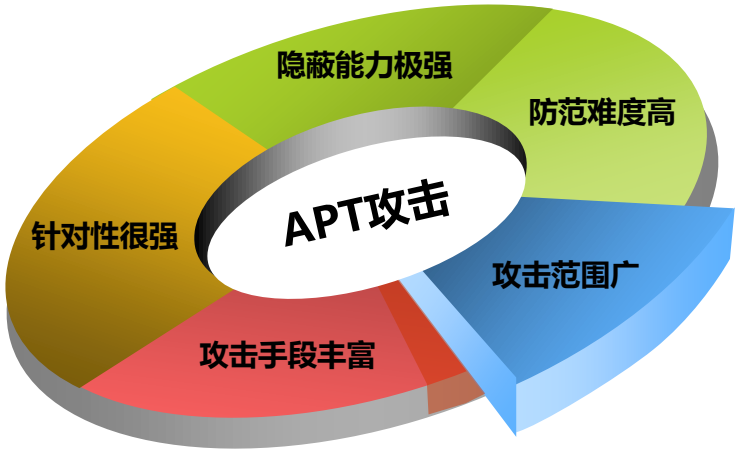
2011：窃取RSA令牌种子

2011：夜龙攻击

2011：三一 vs 中联

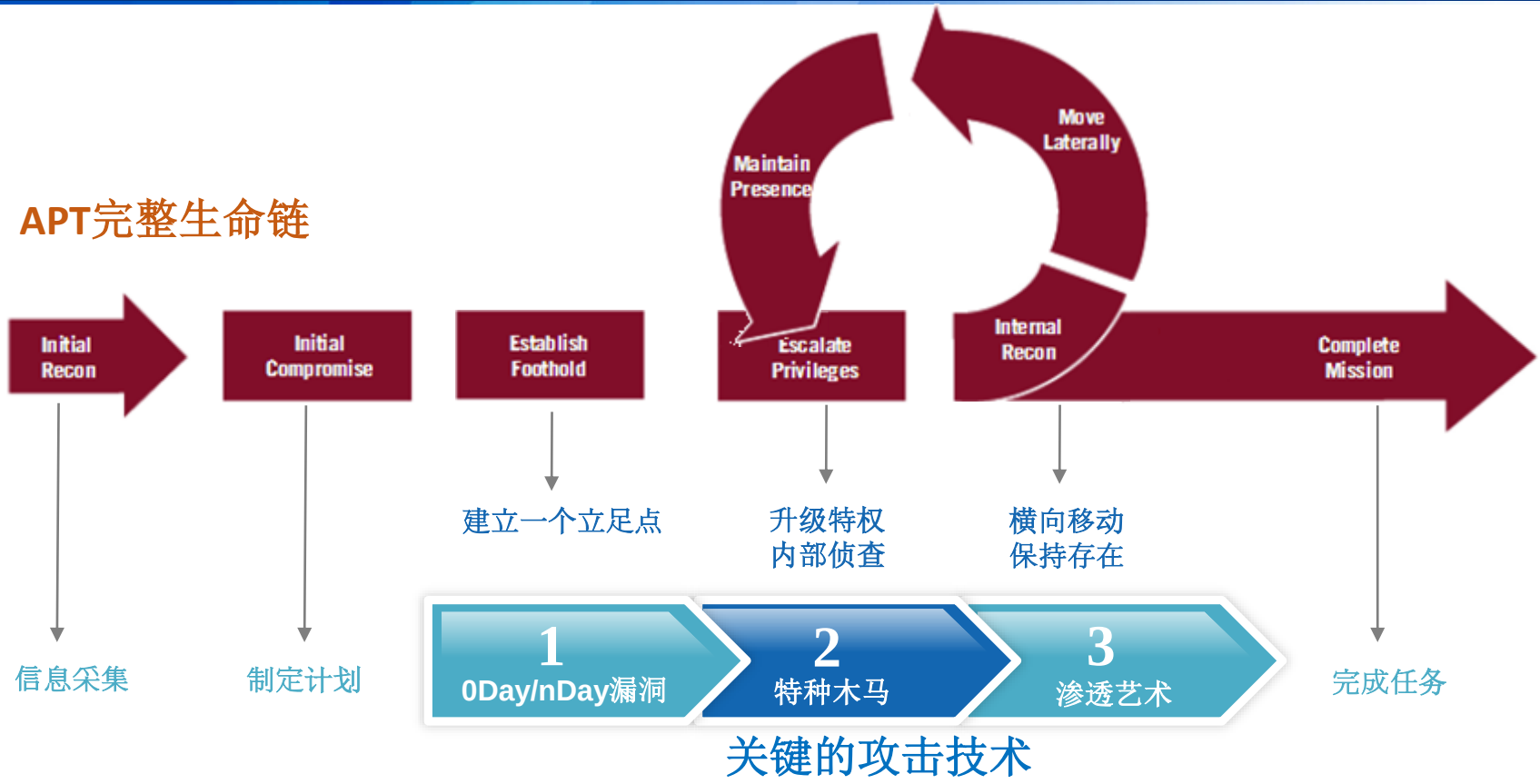
2013：媒体和银行瘫痪

2013:棱镜计划(PRISM)



APT三要素

APT完整生命链



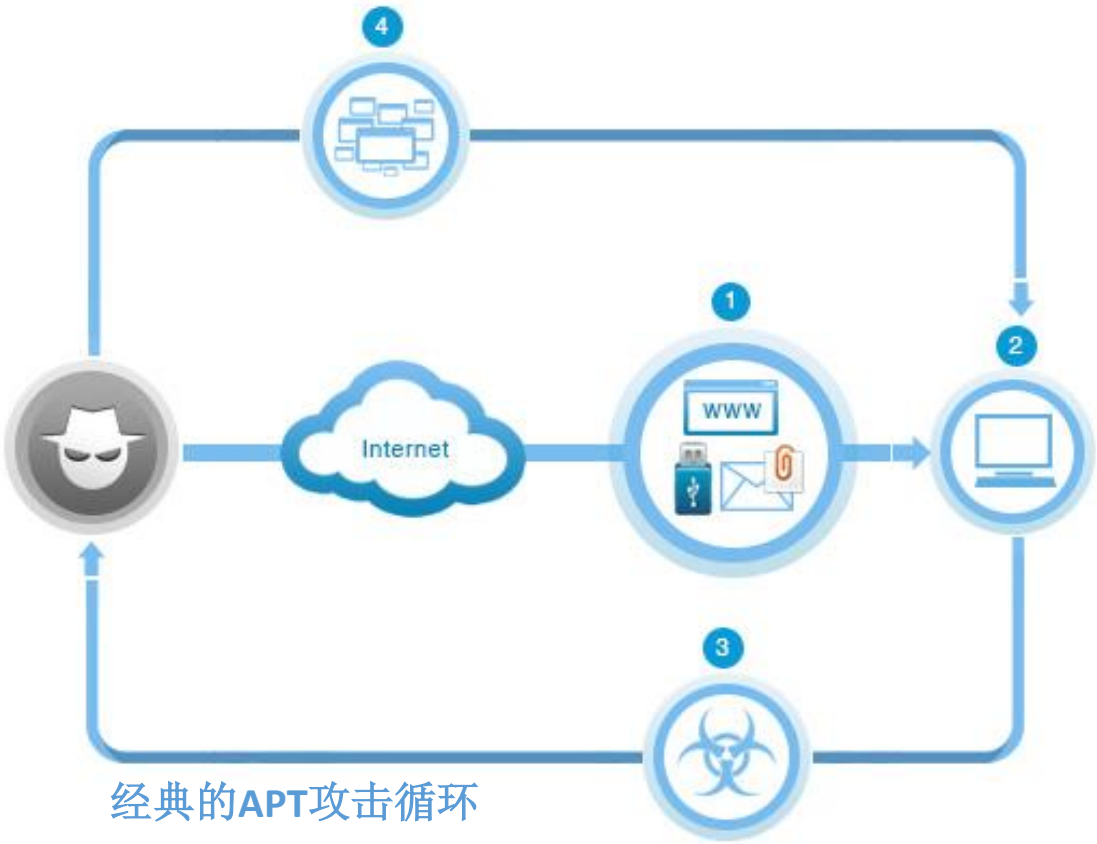
断链式防护理念

针对APT全生命周期链路上各关键环节进行截断式防御

全流量深入分析0Day/nDay漏洞、特种木马、渗透行为等技术手段及战法

典型APT过程

根据FireEye发布的2013年度APT攻击报告显示，通常情况下Web相关攻击发生次数是邮件攻击的五倍。



经典的APT攻击循环

事件剖析

极光攻击

木马植入

引诱企业内部人员访问**挂马**站点

发送**捆绑木马**的文档附件的邮件

木马控守

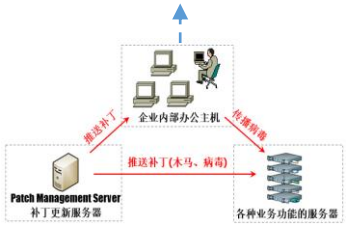
利用SSL加密通道访问C&C服务器，获取敏感信息

窃取

全球20多家高科技企业被波及，大量核心信息资产泄漏

韩国KBS事件

木马植入

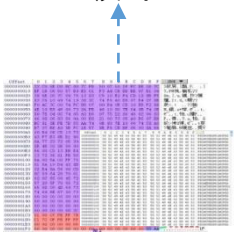


控制补丁服务器，向终端推送**木马程序**。

木马控守

从终端尝试连接到服务器，成功后执行破坏程序并执行。

破坏



定时激活数据毁灭功能，造成硬盘数据永久性毁坏。

根本停不下来

利用漏洞植入特种木马

依靠特种木马记录密码

使用特种木马进行渗透

依靠特种木马进行监控

家族分布Top10

1.UnitedStates(125)

2.Canada(52)

3.Germany(45)

4.United Kingdom(43)

5.Japan(37)

6.Taiwan(35)

7.South Korea(34)

8.Israel(31)

9.Switzerland(22)

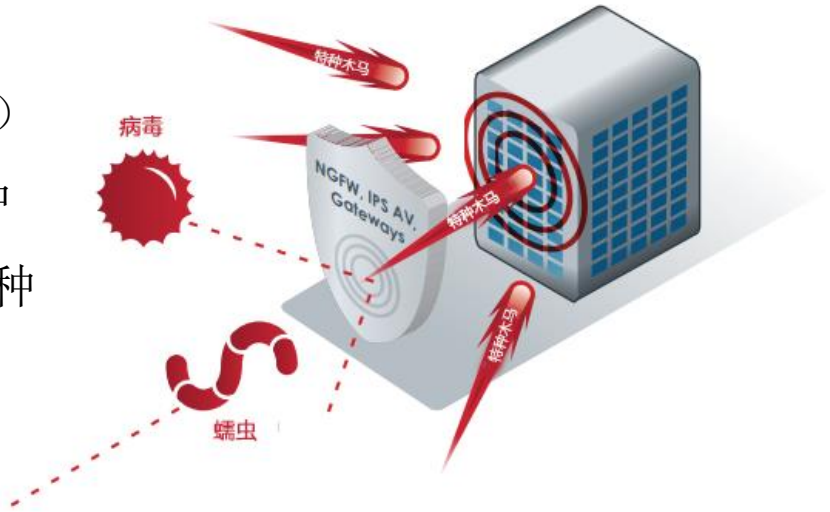
10.Turkey(21)

目录

特种木马的影响范围

- 2013年，国家应急中心监测发现我国境内1.5万台主机被特种木马控制，对我国关键基础设施和重要信息系统安全造成严重威胁。

- 国外知名反APT安全公司（FireEye）调查的结论：超过95%的企业网络中有主机遭受过特种木马入侵，且特种木马样本检测率低于10%。



- 赛门铁克高级副总裁:“杀毒软件已死。杀毒软件仅能拦截45%的网络攻击”。

防火墙、 IDS、 IPS、防毒等传统防御产品无法遏制特种木马攻击。

特种木马的定义

特种木马，一般理解的是为了某次攻击行为特别定制的，针对某个系统、行业的，免杀能力 、穿透性和隐藏性超强的远控木马。

从最近的APT事件中采集到的样本可以看出，特种木马多为各种漏洞和常见开源木马的结合。引用漏洞分类概念（从0Day到1Day再到nDay），可将特种木马定义为0RAT、1RAT、nRAT。

特种木马特点

在投放前就针对性的使用各种杀毒软件进行了测试，能够和杀毒软件“和平共处”

能够在使用了包过滤、应用网关、状态检测、复合型、ISA代理等防火墙的网络环境保证数据回传

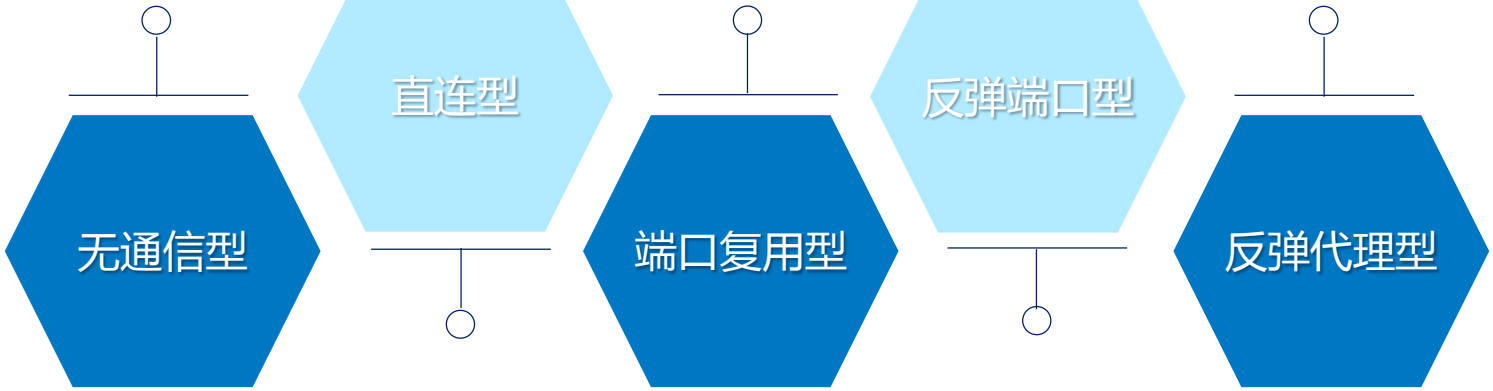
能够躲避一般管理员常用的检测工具，使之能够在系统中隐身

按通信方式分类

使用非网络通信方式进行通信，例如短波、高分贝音频信号、移动存储设备

劫持已经使用的通信端口，对正常连接进行重复利用

在反弹端口的基础上增加代理的使用，能够穿透ISA、Squid等代理网关

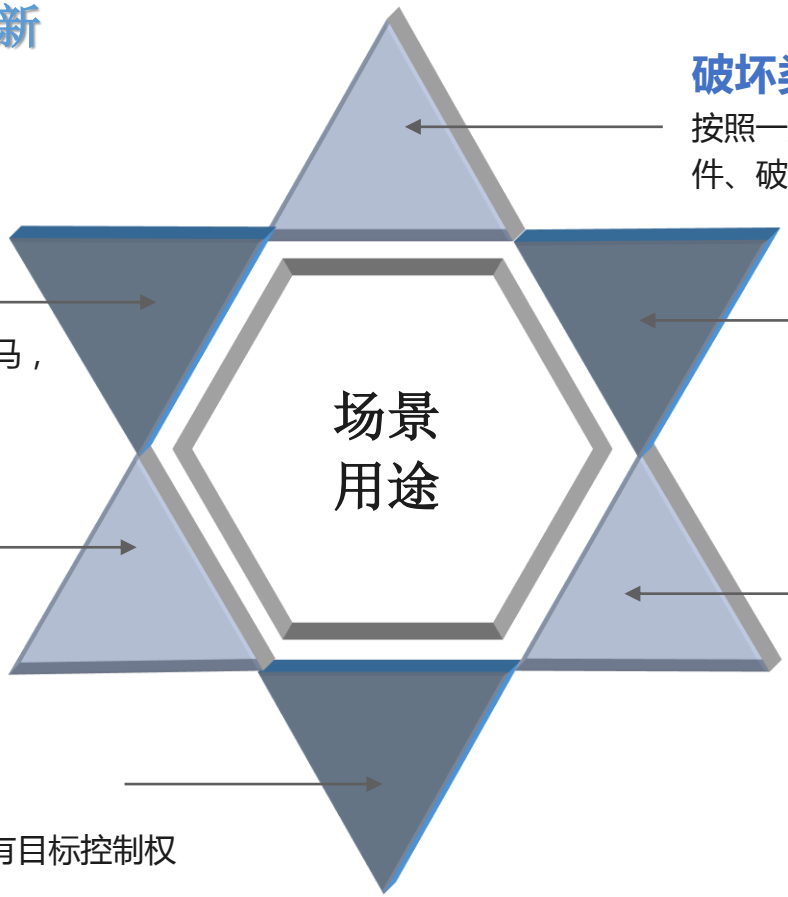


在目标本地绑定对外开放端口，攻击者可直接连接控制目标主机进行远程控制

由隐藏在目标主机上的木马服务端主动连接远程木马控制端。隐蔽性高，防火墙、IDS、IPS等难以防范

按功能分类

发散思考、不断创新



破坏类

按照一定机制触发执行破坏数据、破坏软件、破坏装置等毁坏功能

下载类

一般植入时使用自动下载木马，体积小便于下载并执行

窃密类

以定期获取目标各种常用帐号密码为目的，甚至定制针对专用系统的登入账户

控守类

隐秘控制远程目标资源的程序，搭建C&C网络实现远程管理

渗透类

提供各项辅助渗透攻击的常用功能，便于快速内网侦查和横向扩张

驻留类

深入隐藏以期更长时间拥有目标控制权

按需生产、谨慎使用

按寄宿方式分类

与蠕虫和病毒的技术相结合

1 操作系统

运行在Windows、Linux、Mac OS、Android、IOS等操作系统下，可以利用不同操作系统特性隐藏自身

2 应用程序

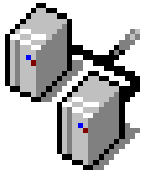
隐藏在浏览器、Java虚拟机、Ghost文件等应用程序的应用环境中，利用应用复杂性隐藏自身

3 硬件平台

隐藏在硬盘、主板、网卡、路由器、芯片等位置，这些地方的恶意代码检测手段极其匮乏

常见特种木马

Dark Comet，作者Lesueur， 2012年7月因发现工具被使用于叙利亚政府打击反政府分子的攻击中，故而宣布停止更新



Gh0st RAT，作者Cooldiyer， 2008年5月开源3.6版本后再无更新，但至今仍有无数修改版本在流传

PoisonIvy，2008年2月更新屏幕插件后再无跟新，主版本停滞在2.3.2，作者声称需要更多时间和动力来开发新版

Zeus/zbot，2011年3月2.0.8.9版本源代码泄露后，衍生出了诸多的变种和模仿者

Gh0st

Reset SSDT | **Install Service** | **Start Service** | **Connect Gh0st** | **Command Control**

Reset SSDT.
通过重新从系统文件中读取ntoskrnl内核信息，在驱动层重置SSDT表以屏蔽杀毒软件

Install Service.
搜索未被占用的服务名，并注册自身为系统服务，寄宿于svchost.exe服务进程

Start Service
启动工作线程初始化自身配置信息、模块插件等，获取并接管目标系统的各种计算机资源

Connect Gh0st.
使用TCP协议周期性期连接连接后台控制端程序，通过超时保活机制保持连接，使用Zlib解压/压缩并封装传递的真实数据

Command&Control
完成命令控制通道的搭建，远程控制端每次控制一种远程资源均建立一个新的Socket连接

PoisonIvy

Install

Add Regedit or Regsvr ActiveX , Inject Process

选择使用修改注册表或注册ActiveX控件的方式完成自启动，并通过注入远程线程完成功能代码的隐蔽执行，同时利用进程的白名单特性绕过防火墙的拦截

Work

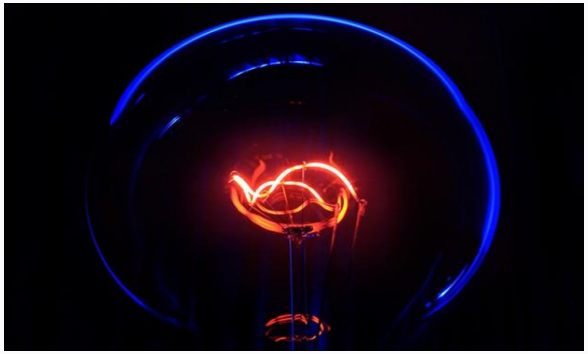
Connect PoisonIvy for Command&Control

使用自定义格式的TCP协议一直保持长时间连接，有周期性的心跳信号，使用LZNT1压缩算法对交互数据进行压缩，各种连接操作均使用1个Socket连接进行通信

近期热点特种木马

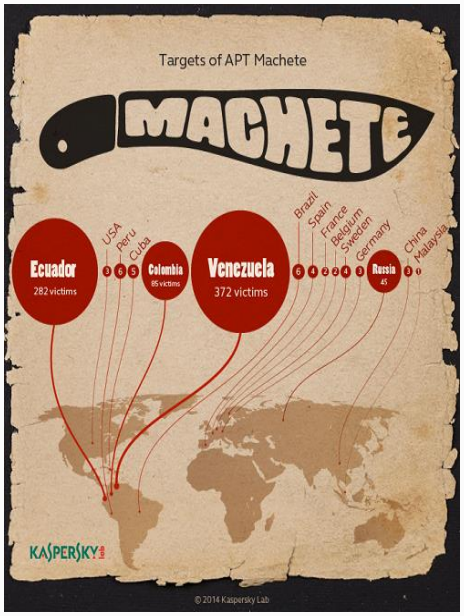
Citadel

被IBM的安全研究人员发现
攻击中东石化公司



BlackEnergy

融入Rootkit技术后进行APT攻击



Machete

攻击情报部门、军队、使馆等

SpyEye

俄罗斯黑客在美国服罪

Taidor和LStudio

广泛使用在CVE-2014-4114漏洞利用

美国国安局（NSA）工具库中的特种木马

2013年12月30日，德国《明镜周刊》发表题为《Shopping for Spy Gear: Catalog Advertises NSA Toolbox》的文章，揭秘NSA工具库已经攻破全球首屈一指的网络设备供应商、电脑供应商的安全防御设备或电子产品

BIOS木马

DEITYBOUNCE，提供一个软件应用利用主板的BIOS和利用系统管理模块（System Management Mode）的漏洞驻留在Dell的PowerEdge服务器上。

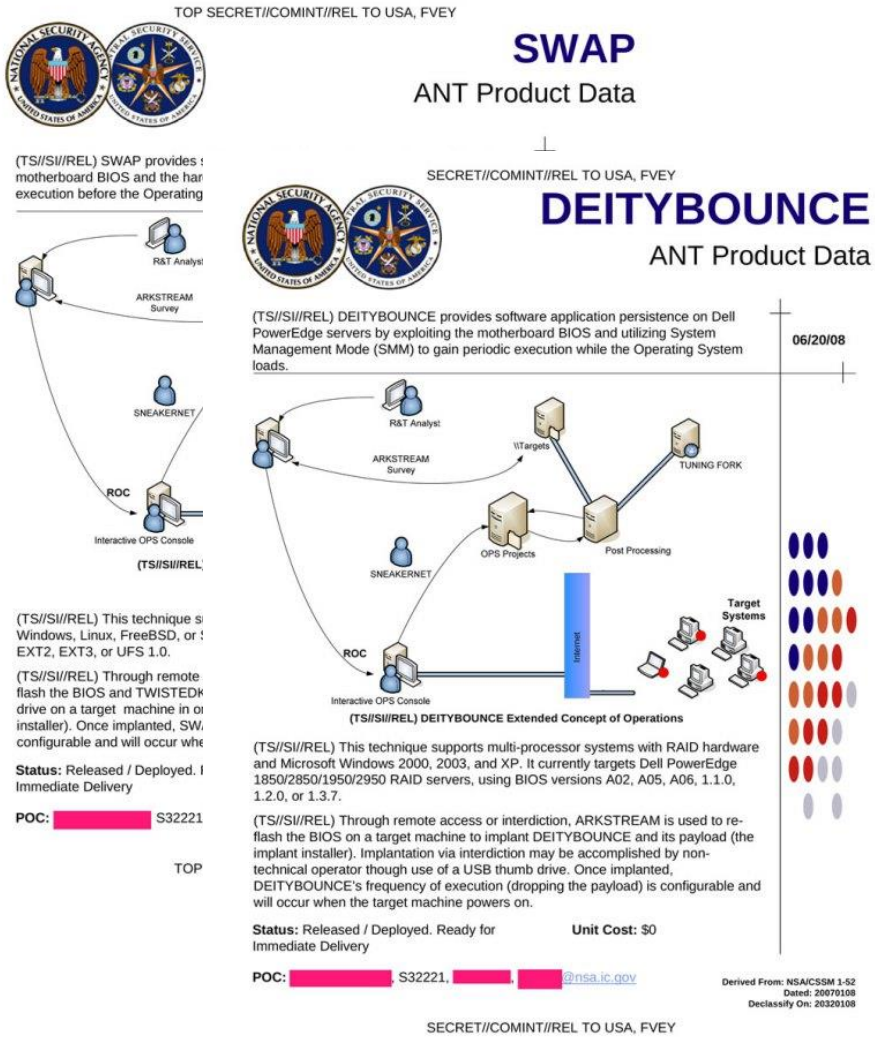
SWAP，可利用刷新BIOS的方法注入可执行代码到主板BIOS中去，在操作系统启动过程中激活并插入控制代码跟随运行。

受影响的包括Dell：
PowerEdge1850/2850/1950/2950

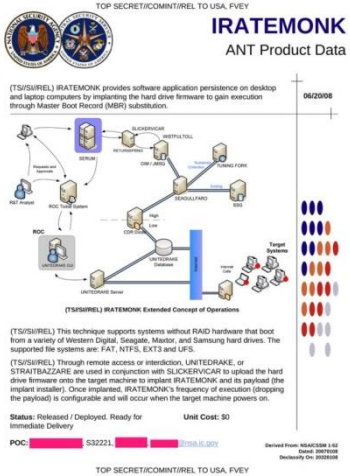
BIOS版本为：
A02、A05、A06的1.1.0、1.2.0或1.3.7

操作系统支持：
Windows、Linux、FreeBSD、Solaris

文件系统支持：
Fat32、NTFS、EXT2、EXT3、UFS 1.0



硬盘木马


TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

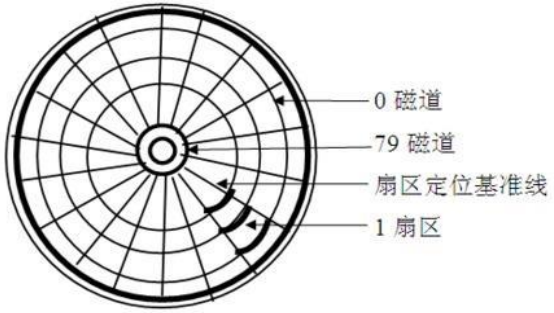
POC: [redacted] S32221, [redacted] @nsa.ic.gov

TOP SECRET//COMINT//REL TO USA, FVEY

IRATMONK，隐藏于硬盘Firmware固件中，通过MBR获取执行权限。能够对台式电脑、笔记本电脑进行持久性控制。

支持品牌：Seagate希捷、Maxtor迈拓、Samsung三星、Western Digital西部数码

硬盘Firmware固件除存放在硬盘EROM或EPROM（可编程只读存储器）中之外，还有部分数据保存在负磁道上，可用专业工具升级更新。



硬盘是从外向内数的，0号磁道在最外面

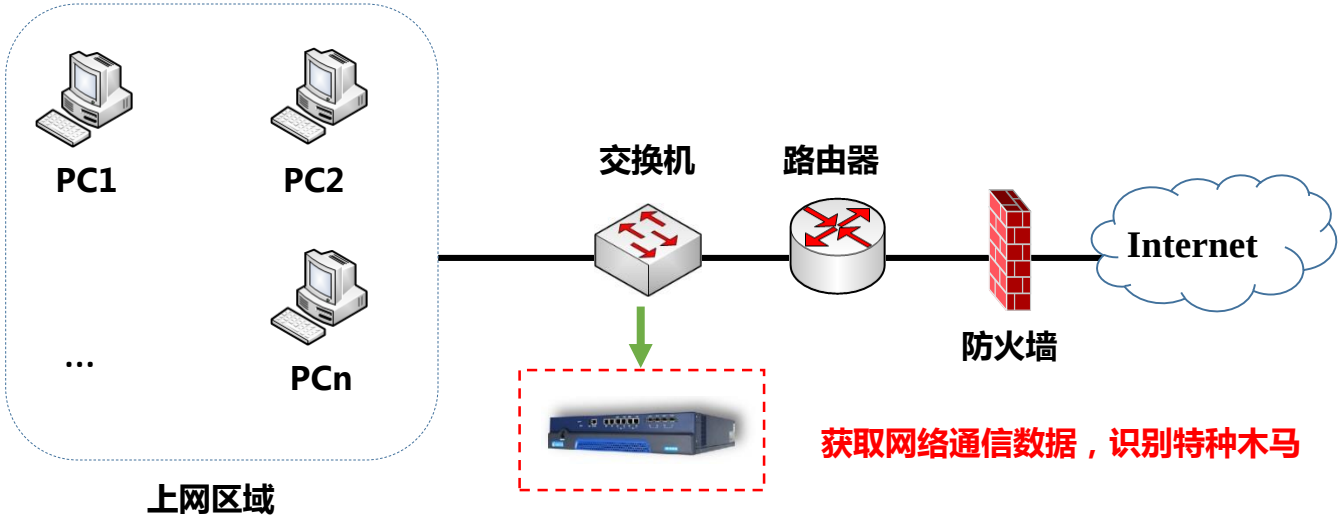
负磁道

- CI 硬件信息
- FI生产厂家信息
- WE写错误记录表
- RE读错误记录表
- SI容量设定
- ZP区域分配信息
- PL永久缺陷表
- TS缺陷磁道表
- HS实际物理磁头数及排列顺序
- SM最高级加密状态及密码
- SU用户级加密状态及密码

目录

从流量中挖掘特种木马

采用大数据分析技术来检测APT攻击行为的设备。该设备部署在网络出口处采集网络通信数据，分析通信数据中的木马通信痕迹，识别木马特征和行为，在网络层实现对全网范围内木马识别与追踪。



木马检测

已知木马

将访问黑IP、黑域名、黑URL，和匹配到木马流量特征的网络行为定性为已知木马，即木马。

已知/未知木马

具有挂马、钓鱼、扫描等恶意攻击行为的网页、IP、域名定义为威胁源。

未知木马

具有已知木马行为、威胁源特征以及网络攻击特征的事件发现过程定义为行为分析。

木马检测

已知木马通信行为特征→已知木马

- 木马程序分为控制端和被控端两个部分，其中被控端用来植入到用户的电脑中，控制端会在公网上提供一个IP地址、域名或URL让被控端连接完成木马上线。
- 从木马程序样本中提取的IP、域名、URL形成黑名单库，同时提取通信流量内容作为木马流量特征，通过黑名单和流量特征的检测，识别网络中的已知木马。

威胁分析

已知威胁源特征库→已知/未知的木马植入

- 网络中主动的或被动的通信行为，可能导致终端或服务器被植入木马、被黑客控制或信息泄露，包括访问挂马页面、钓鱼页面，黑客远程扫描、脆弱点测试等行为。
- 铁穹系统将具有挂马、钓鱼、扫描等恶意攻击行为的网页、IP、域名定义为威胁源。

威胁IP

主动访问威胁IP可能会致恶意代码下载到本地执行。

威胁域名

主动访问威胁域名可能会致恶意代码下载到本地执行。

威胁URL

主动访问威胁URL可能会致恶意代码下载到本地执行。

HTTP访问

HTML页面存在挂马代码，或存在Shellcode，用户点击访问之后会使页面中的恶意代码执行。

文件传输

具有恶意可执行文件、黑客工具、漏洞利用代码等网络流量和文件定性为文件传输威胁。

可疑邮件

利用冒名的方式发送邮件，或在邮件正文或附件中含有恶意代码的邮件。

行为分析

未知特征+未知通信行为→未知木马通信行为

- 以库特征的形式来识别木马通信行为，虽然精确性较高，但仅局限于已知木马的识别。
- 从已知木马行为、威胁源特征以及APT攻击事件总结出可用行为线索，用来发现未知木马和威胁。
- 铁穹系统将具有已知木马行为、威胁源特征以及APT特征的事件发现过程定义为行为分析。

动态域名

- 被木马利用作为连接地址的域名，通过该域名解析出实际的IP地址，动态域名一般没有固定的IP，但无论IP地址如何变化，都可以通过该动态域名解析出正确的连接地址。
- 通过动态域名后缀库的匹配，统计网络中活跃的动态域名。

协议异常

- 为了躲避安全监控，木马常会会采取利用正常的通信协议或端口来进行伪装，有部分伪装的内容与标准的协议不符。
- 统计协议和常见端口不匹配、HTTP协议、DNS协议、邮件类型协议等通信行为。

心跳

- 木马检测控制端是否存活的一种方式，通常会间隔相同或不同时间段与控制端进行通信。
- 间隔时间存在规律，且数据包内容的相同的数据报文定性为心跳数据。

行为分析

未知特征+未知通信行为→未知木马通信行为

- 以库特征的形式来识别木马通信行为，虽然精确性较高，但仅局限于已知木马的识别。
- 从已知木马行为、威胁源特征以及APT攻击事件总结出可用行为线索，用来发现未知木马和威胁。
- 铁穹系统将具有已知木马行为、威胁源特征以及APT特征的事件发现过程定义为行为分析。

非常见端口

- 木马一般会打开不常用的端口进行通信，或在获取系统权限进行远程控制时打开非常见端口进行控制。
- 统计所有通信端口，并利用端口白名单机制筛选出非常见端口。

规律域名统计

- 被木马利用作为连接地址的域名，通过该域名解析出实际的IP地址，访问次数会十分频繁，或仅有几次。
- 统计所有域名访问次数统计。

URL访问统计

- 被木马利用作为连接、配置获取等作用的URL，访问次数会十分频繁，或仅有几次。
- 内网所有IP地址访问URL的访问记录，并记录网页源码，提供下载分析。

流量异常

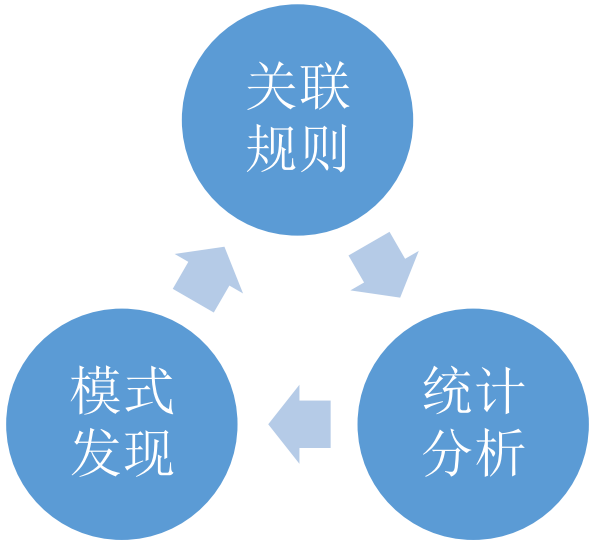
- 单个会话流量比超过X；
- 单个内网IP长期流量比曲线突变；
- 单个内网IP传输总流量超过5GB；
- 单个内网IP外联次数超过X；
- 单个内网IP外联时长超过X。

事件关联

诸如异常流量、心跳、连接动态域名等这些事件本身并不足以认定木马通信行为，一旦将这些事件通过其内在的联系进行关联，就能形成一整条证据链路，能够判定木马攻击行为。

铁穹系统将各种木马行为、威胁源特征以及典型行为线索等进行事件关联分析，识别未知木马和未知威胁。

关联规则	长期跟踪木马攻击行为，把攻击流程凝练为关联规则
统计分析	根据攻击方式、频率、周期、尺度来分析攻击者的身份、角色等
模式发现	利用木马攻击独有的行为模式，从事件中寻找、推测和预测事件关联性



目录

政策法规

公安部：《信息系统安全等级保护基本要求》《信息系统安全等级保护测评要求》		
第三级	网络安全-入侵防范（G3）	a）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、**木马后门攻击**、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； b）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
	网络安全-恶意代码防范（G3）	a）应在网络边界处对恶意代码进行检测和清除； b）应维护恶意代码库的升级和检测系统的更新。

工信部：《移动互联网恶意程序监测与处置机制》、关于印发《木马和僵尸网络监测与处置机制》通知		
关于印发《木马和僵尸网络监测与处置机制》的通知	事件通报内容	1、威胁较大的**木马和僵尸网络**IP地址、端口、发现时间、所属基础电信运营企业。 2、木马和僵尸网络使用的恶意域名。 3、木马和僵尸网络的规模和潜在危害。
《移动互联网恶意程序监测与处置机制》	第六条	移动通信运营企业、CNCERT应不断提高移动互联网恶意程序的样本捕获和监测处置能力，建设完善相关技术平台。移动通信运营企业应具备覆盖本企业网内的监测处置能力，CNCERT应具备跨不同企业移动互联网的监测能力。

中国人民银行：《网上银行系统信息安全通用规范》（JRT 0068-2012）		
服务器端安全：基本要求	网络安全-入侵防范	部署入侵检测系统/入侵防御系统（IDS/IPS），对网络异常流量进行监控，监控并记录以下攻击行为：端口扫描、强力攻击、**木马后门攻击**、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。
	网络安全-恶意代码防范	在网络边界部署入侵检测/防护系统、防病毒网关等防病毒设备，对恶意代码进行检测和消除。应定期对恶意代码防护设备进行代码库升级和系统更新。

检测的难点

- 即便不考虑检测隐藏在各种硬件设备中的特种木马，也同样是困难重重

网络复杂

因终端设备多且网络结构复杂，故人工上机检测和协调部门统一部署终端检测软件都不轻松

缺少工具

杀毒软件不可靠，特种木马都是已经经过免杀处理过的，已经具备绕过杀软的能力

任务量大

需分析的日志量巨大，需要专业人员使用专业工具进行针对性分析才能有成效

一种点面结合的解决方法

Discovery

01

网关出口处的网络检测

通过在网关处分析网络流量，以大数据的方法统计和识别特种木马的通信行为模型，判断可疑通信在内网的IP地址，从而定位到内网终端.

02 目标定位

可疑终端上机检测

使用各种ARK工具针对性挖掘可疑通信的发起源，逐项检查进程、注册表、服务、文件、网络、系统、日志等，并尝试分析感染源.

样本采集 03

取证和溯源

取证时先尽可能的保留环境避免触发自毁机制，还需注意被擦除、隐藏、加密的数据，采样完成后可进行溯源分析.

04 解决方案

处理方法及安全建议

分析清楚特种木马的存活机制之后，就可以针对性的提供处理方法了，不过大多时候都是建议先封存再更换终端设备.

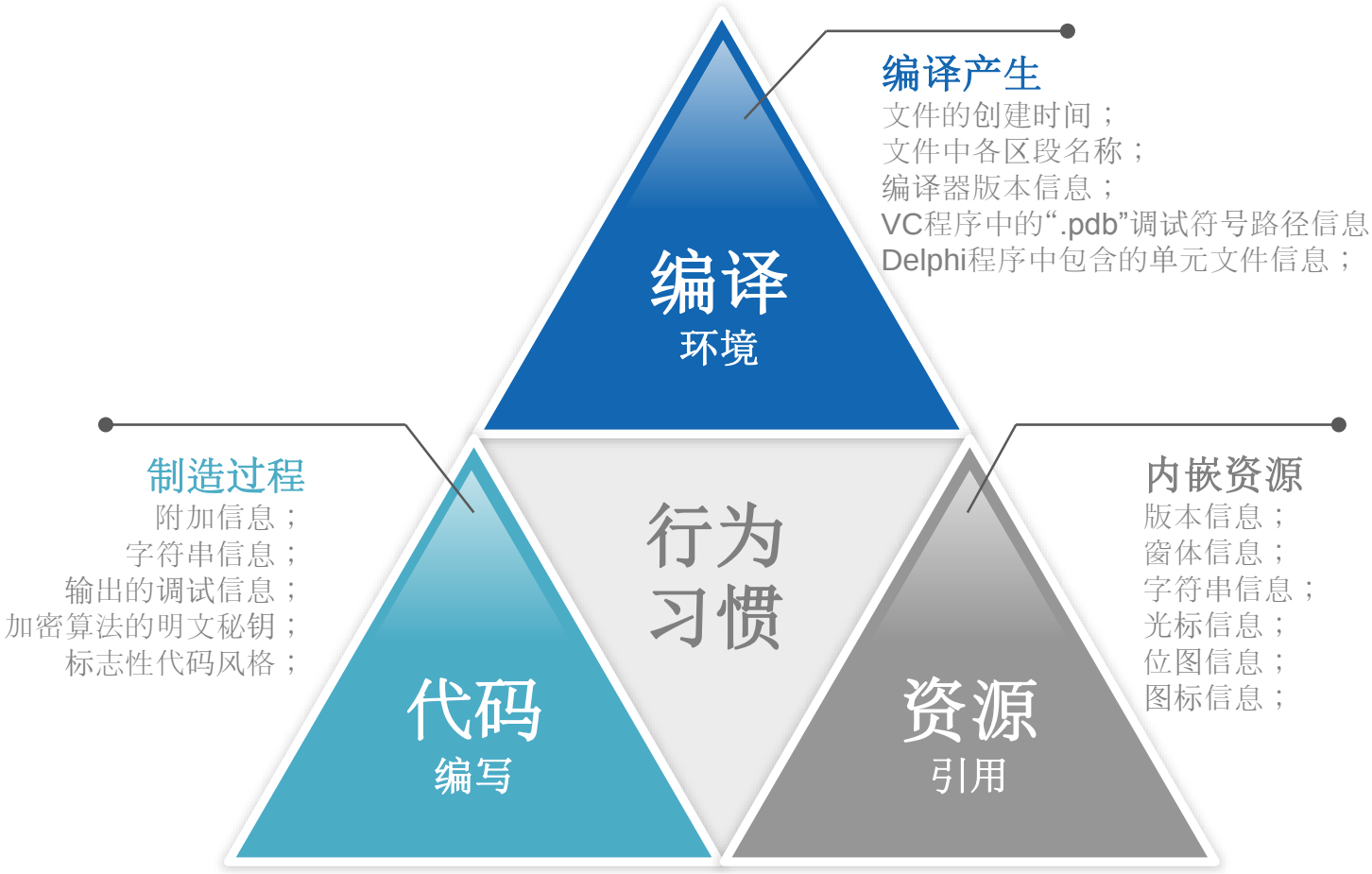
特种木马的溯源分析

触发难

取证难

逆向难

溯源线索



行为习惯也是用于辅助分辨特种木马家族产地的一个重要线索

寻找第一跳的背后


线索
人肉搜索
通过猜测特种木马的二进制文件中遗留的各种信息，再结合搜索引擎和各种互联网资源等对攻击者进行人肉搜索，确定攻击者或制造者身份。
灰网
陷阱钓鱼
在网络中或终端上布设陷阱，等待攻击者将陷阱取回查看。一旦攻击者未注意数据处理的环境安全性，就可以获取到攻击者的真实网络地址信息。
反制
主动攻击
通过口令猜解、网络攻击、溢出特种木马控制端程序等方法获得后台管理权后再进一步分析，或者尝试分析控制后台的交互IP和流量进出方向。
Luck
Outwit
Attack

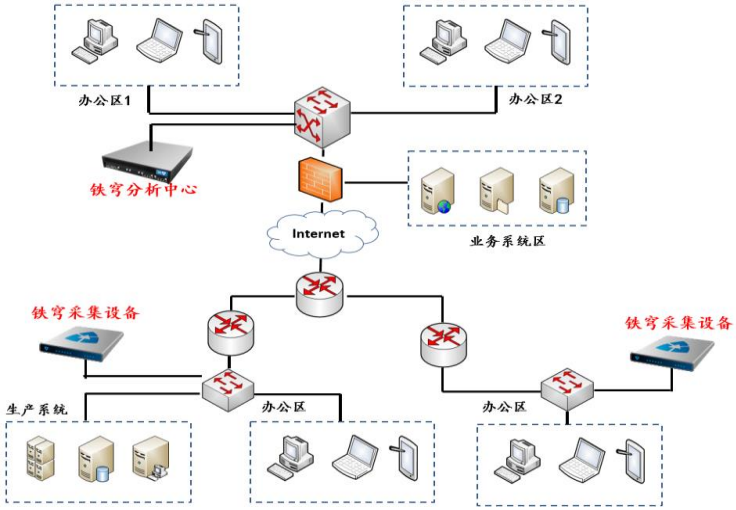
应用案例

用户需求：

检测集团总公司和子公司内网中可能存在网络安全威胁，降低信息泄密风险。

部署说明：

- 在集团分公司和总公司外网的网络出口交换机处旁路部署铁穹iDome采集设备；
- 在总公司部署分析设备和管控设备，完成对集团全网的安全威胁检测。



用户收益：

- 发现总公司核心服务器感染了两个后门程序，并被创建了hack和hacker两个用户。
- 一分公司业务应用服务器感染多个木马，严重的恶意LPK劫持程序将全盘感染，并发现多个黑客工具，此服务器被黑客控制并利用。
- 在提供详细的网络威胁检测报告，从报告中可了解到集团总公司和分公司的安全防御不足，报告中同时提出了网络安全防御系统的建设方案为用户提供参考。

Thank You!

谢　谢