关于系统化应对 NSA 网络军火装备的操作手册

安天安全研究与应急处理中心（安天 CERT）

报告初稿完成时间：2017 年 05 月 22 日 06 时 00 分

首次发布时间：2017 年 05 月 22 日 08 时 00 分

本版本更新时间：2017 年 05 月 22 日 19 时 00 分

1 概述

北京时间 2017 年 5 月 12 日 20 时左右，全球爆发大规模的 “WannaCry”（中文名称魔窟）勒索软件感染事件，我国各地的计算机网络（特别是一些内网）也受到不同程度的影响。该勒索软件迅速传播的原因是利用了基于 445 端口传播扩散的 SMB 漏洞——MS17-010。该漏洞利用工具原本是美国 NSA 下属的 Equation Group（方程式组织）使用的“网络军火”，在 2017 年 4 月 14 日的被黑客组织 Shadow Brokers（影子经纪人）曝光，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了此次全球性的大规模攻击事件。

关于本次事件需要注意的是，“WannaCry”（中文名称魔窟）勒索者蠕虫仅利用了被曝光“网络军火”中的“永恒之蓝”（Eternal Blue）漏洞，Shadow Brokers（影子经纪人）曝光的“网络军火”中还有系列的漏洞及其利用工具需要关注和防范。同时，Shadow Brokers（影子经纪人）在 2017 年 5 月 16 日再次发布声明，称其会在 6 月公布更多漏洞，鉴于以上原因，需要对当前已知的和未来将出现的威胁做好相应的防护和准备工作。

在面对各种严峻的安全风险时，除了通过有效的安全设计和使用安全产品形成防御能力之外，我们必须要做好合理的补丁策略、端口和应用的管理策略、边界的安全条件等基础安全工作。针对部分网络节点规模及数量较大的内网用户或部分对业务系统的稳定性及安全性要求较高的用户，有可能不能实施全面的系统的补丁策略，同时实时获取补丁的方法一定程度上受到网络隔离的相应影响或限制，因此，可能需要采用对严重漏洞进行单点补丁的策略。但是因为整个补丁系统的庞大和复杂性、补丁和业务系统的相关性，仅靠打补丁和关闭端口，并不能系统应对各种复杂情况。比如以下几种场景：

第一种情况，由于相应系统停止更新服务的原因，部分安全漏洞被发现时，原厂可能已经不再发布补丁，必须要使用升级相关的系统或应用的方式来解决，如本次受影响的 Windows XP 及 Windows Server 2003 系统，微软已经在多年前停止对这两个系统进行补丁更新及相关的升级，对于使用这两种系统的用户来说，无法获得官方的补丁进行修复漏洞，此时，我们就需要采用有效的安全设计和安全产品等策略进行防护。

第二种情况，实际上来看，每一个应用和它开放的端口都有其特定场景的业务价值，因此，在采用相应端口屏蔽策略之前，需要判断是不是系统中需要正常使用的应用或端口，以及这种应用或端口是否有其他的方式来替换。比如在用户的业务场景下，如果 80 端口是为了保证业务系统的正常运行时，不能够进行对其进行端口关闭、端口修改或停止相应的服务时，就需要采用有效的系统安全设计和使用安全产品形成对系统的整体性的综合防御来抵御其攻击。

第三种情况，如果补丁和业务系统的稳定性发生冲突的情况，对于多数情况下，可能需要保证业务系统的正常运行，这种不能更新补丁的情况，可能需要外部的安全检测方法或者替换现有操作系统版本等方式来解决，此时就需要引入特定的安全产品进行防护。

合理的补丁策略绝不只是针对重大事件的应急反应，而是要在日常的安全应用和维护中需要达成的一个规范工作及流程，仅靠打补丁和关闭端口是无法完整应对网络攻击的，必须借助安全设计、被动防御、积极防御和威胁情报的结合，依托具有有效防护能力的安全产品来形成防御的纵深能力。

微软补丁包机制是不安装基础补丁包则无法安装后续的部分补丁。因此安天建议普通的桌面系统和不重要的服务系统在内部无法安装在线补丁的情况下，先安装基础补丁包，然后再安装无法安装的补丁包。因为基础补丁包体积较大，一旦出现大型的安全事故，由于大量用户进行下载，可能造成下载不成功的情况，因此希望网络管理员提前储备基础补丁包及重要补丁包。

核心的安全风险在纵深地带，在内网纵深地带，整个的安全防御要做纵深展开。安天由几个安全产品所组成的安全防护体系，在安天态势感知和监控预警平台的统一协调下，能够形成真正有效具备全天候、全方位能力的态势感知，能够形成对信息资产的有效防护。

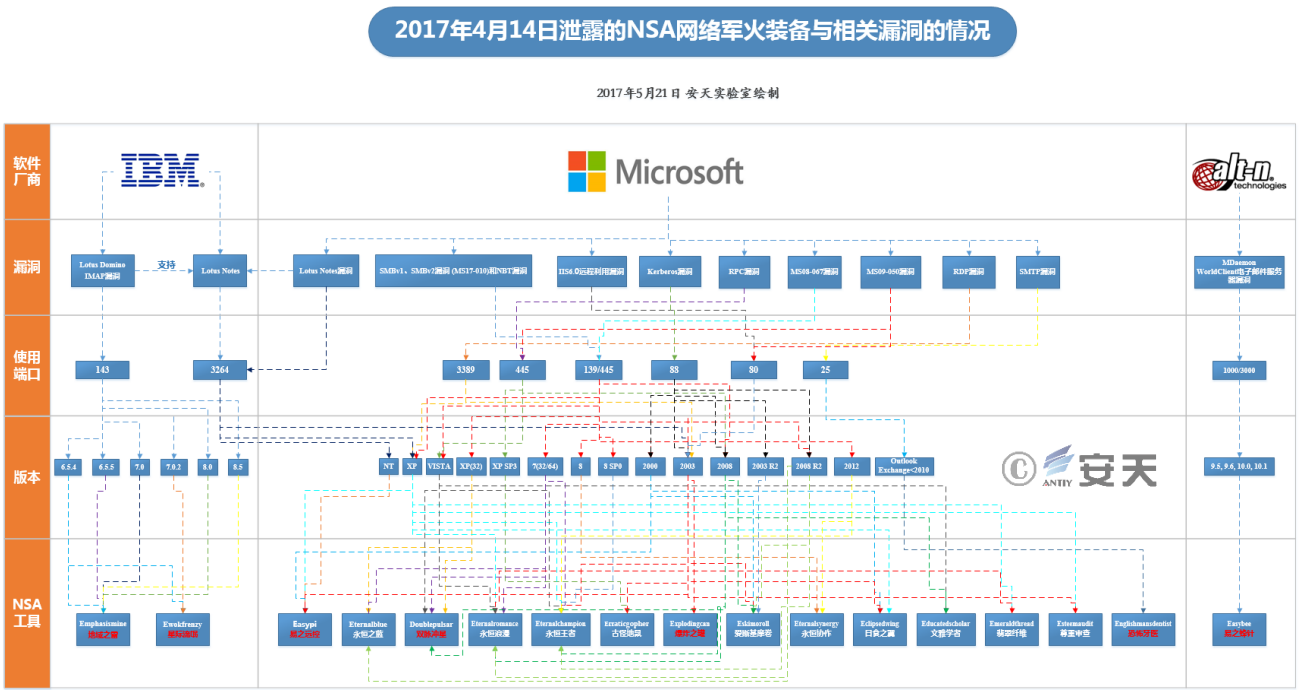


图 1 近期泄露的 NSA 网络军火装备与相关漏洞、系统版本关系图（详图）

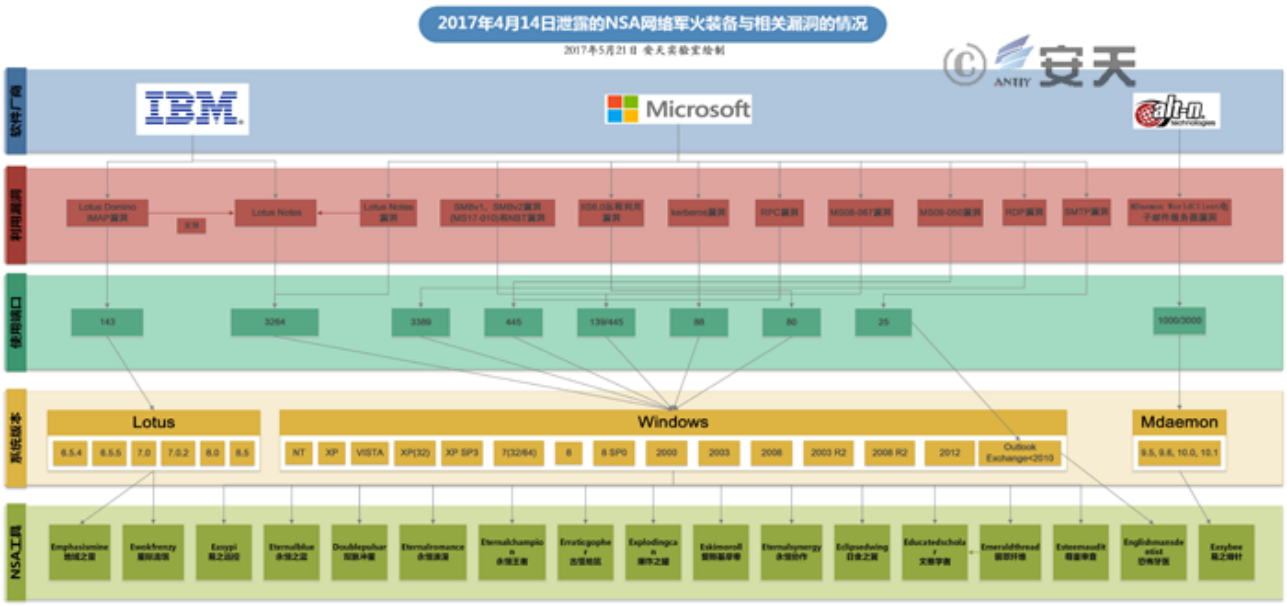


图 2 近期泄露的 NSA 网络军火装备与相关漏洞、系统版本关系图（简图）

2 基本处置流程

由于涉及的漏洞较多，影响的系统、应用版本复杂，且部分受影响系统官方已经不再更新补丁，因此在处置相关系统时需要对系统基本情况进行判断，选择对应处置方案。具体判断流程如下：

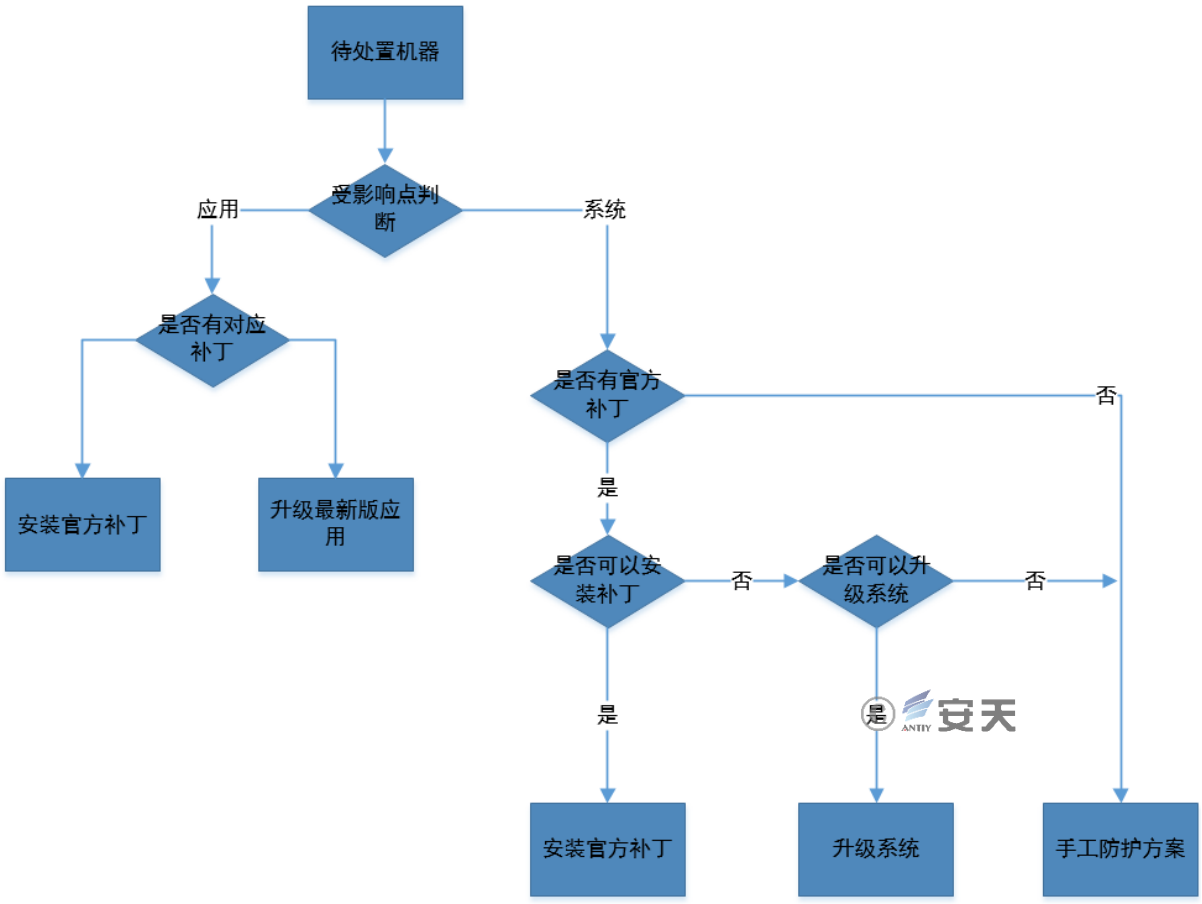


图 3 选择处置方案流程

选择处置方案后，如果系统可以安装补丁，可以根据下表安装更新补丁或升级系统、应用。补丁程序可以根据链接从官方下载，也可以使用提供的离线补丁包。

漏洞攻击模块名称	中文名	影响系统或应用名称	补丁或升级版本	影响端口	补丁或最新应用地址或手工处置建议
Easybee	易之蜂针	WorldClient 9.5, 9.6, 10.0, 10.1	升级最新版本 17.0.1	1000/3000	http://www.altn.com/Downloads/MDaemon-Mail-Server-Free-Trial/
Easypi	易之远控	IBM Lotus Notes (Windows NT, 2000 ,XP, 2003)	升级到 9.0.1 以上版本并安装最新补丁	3264	http://www-03.ibm.com/software/products/en/ibmnotes https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Notes&release=9.0.1.8&platform=Windows&function=all
Eclipsedwing	日食之翼	Windows 2000, XP, 2003	KB958644	139/445	https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
Educatedscholar	文雅学者	Windows vista, 2008	KB975517	445	https://technet.microsoft.com/en-us/library/security/ms09-050.aspx
Emeraldthread	翡翠纤维	Windows XP ,Vista ,7 , Windows Server 2003,2008	KB2347290	139/445	https://technet.microsoft.com/en-us/library/security/ms10-061.aspx
Emphasismine	地域之雷	IBM Lotus Domino 6.5.4, 6.5.5, 7.0, 8.0, 8.5	升级到 9.0.1 以上版本并安装最新补丁	143	http://www-03.ibm.com/software/products/en/ibmdomino https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Domino&release=9.0.1.8&platform=Windows&function=all
Englishmansdentist	恐怖牙医	Outlook Exchange	升级到 2010 以上版本	25	https://products.office.com/zh-cn/exchange/email
Erraticgopher	古怪地鼠	Windows XP SP3, Windows 2003	升级到 vista 以上版本	445	微软停止服务，暂无补丁，可禁用 SMB 服务，防火墙禁用 445 端口。
Eskimoroll	爱斯基摩卷	Windows 2000, 2003, 2003 R2, 2008, 2008 R2	KB3011780	88	https://technet.microsoft.com/en-us/library/security/ms14-068.aspx
Esteemaudit	尊重审查	Windows XP, Windows Server 2003	升级到 win7 以上系统	3389	微软停止服务，暂无补丁，可禁用远程桌面服务，关闭 3389 端口防护。
Eternalromance	永恒浪漫	Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2	KB4013389	139/445	https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Eternalsynergy	永恒协作	Windows 8, Windows Server 2012	KB4013389	139/445	https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

Ewokfrenzy	星际流氓	IBM Lotus Domino 6.5.4, 7.0.2	升级到 9.0.1 以上版本并安装最新补丁	143	http://www-03.ibm.com/software/products/en/ibmnotes https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=Collaboration%20Solutions&product=ibm/Lotus/Lotus+Domino&release=9.0.1.8&platform=Windows&function=all
Explodingcan	爆炸之罐	Windows Server 2003 WEBDAC	升级到 win7 以上系统	80	微软停止服务，暂无补丁，微软建议升级 WIN7 防护。
Zippybeer	夺命之酒	Windows Domain	升级系统	445	微软停止服务，暂无补丁，可禁用 SMB 服务，防火墙禁用 445 端口。
Eternalblue	永恒之蓝	Windows XP(32),Windows Server 2008 R2(32/64),Windows 7(32/64)	KB4013389	139/445	https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Doublepulsar	双脉冲星	Windows Vista, 7, Windows Server 2003, 2008, 2008 R2	KB4013389	139/445	https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx
Eternalchampion	永恒王者	Windows XP, Vista, 7, 10,Windows Server 2003, 2008, 2008 R2, 2012, 2016	KB4013389	139/445	https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

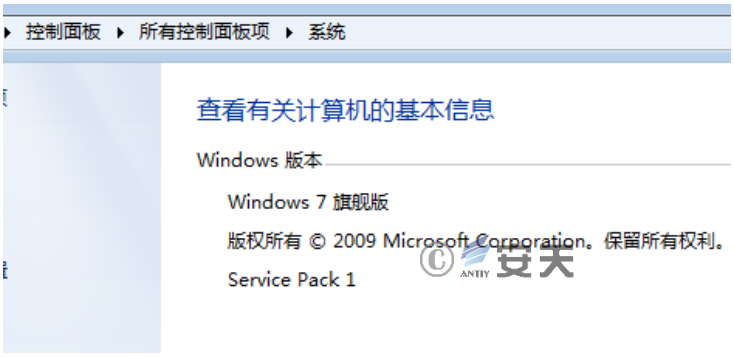
表格 1 漏洞对应的受影响系统、端口、补丁地址等信息

3 安装官方补丁或升级系统、应用版本

根据上表提供的漏洞对应的系统、软件及对应补丁等信息，可以根据各系统、软件厂商提供的补丁进行修补或升级最新系统或应用版本防御相关的漏洞攻击。下面以 Win XP、Win7 等系统为例，具体介绍安装补丁或相应的处理流程：

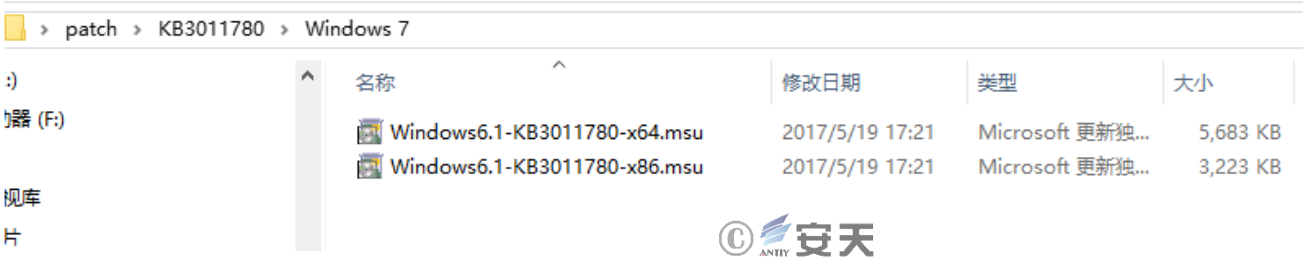
3.1 win7 安装系统补丁流程：

1) 查看系统信息，确定系统位数、版本、Service Pack（SP）版本。

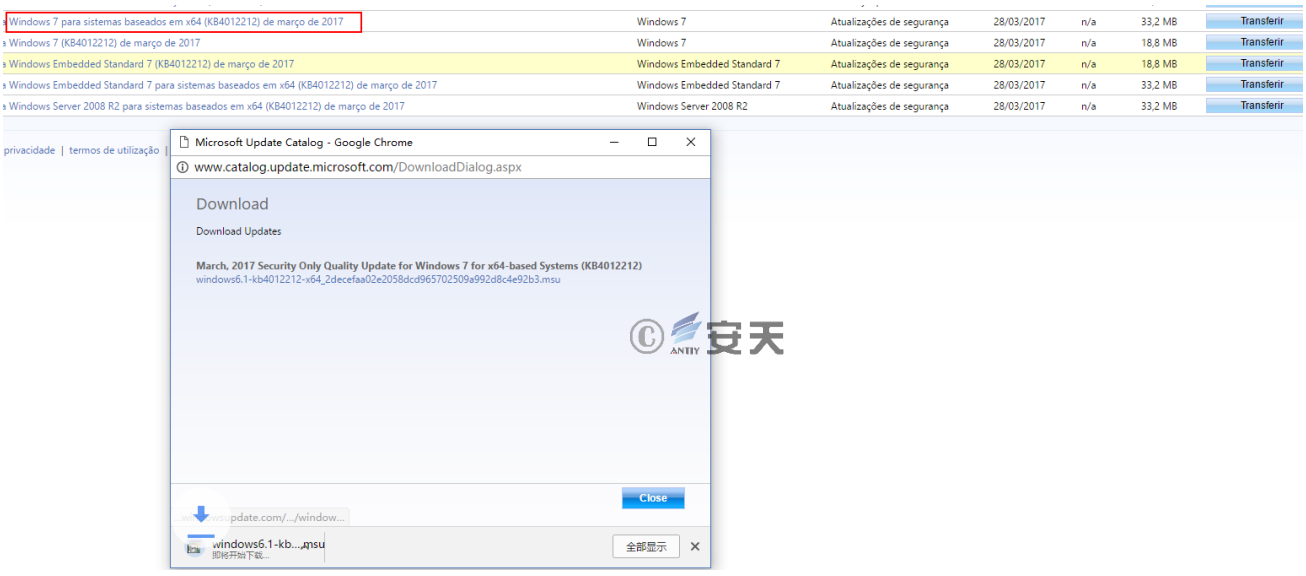


2) 根据表 1 提供的补丁地址、或者离线补丁包，找对应的补丁程序。

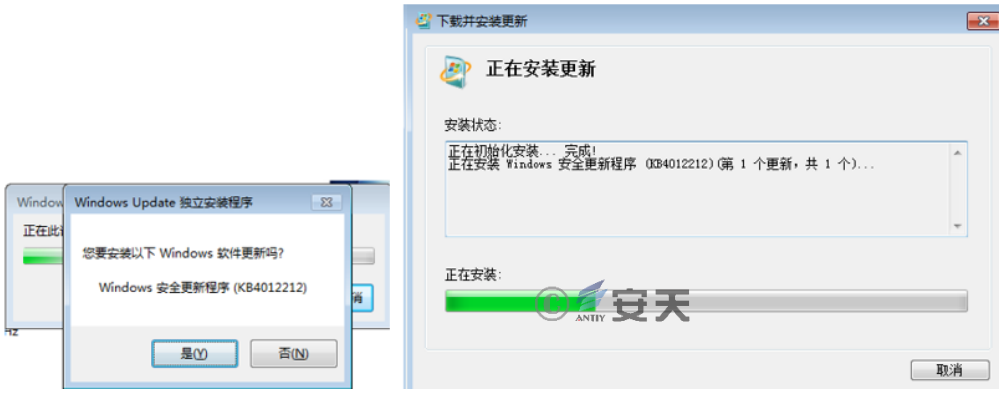
Windows 7							
Windows 7（用于 32 位系统）Service Pack 1 (4012212) 仅安全相关[1]	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	重要 信息泄漏	严重 远程代码执行	无
Windows 7（用于 32 位系统）Service Pack 1 (4012215) 月度汇总更新[1]	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	重要 信息泄漏	严重 远程代码执行	3212646
Windows 7（用于基于 x64 的系统）Service Pack 1 (4012212) 仅用于安全更新[1]	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	重要 信息泄漏	严重 远程代码执行	无
Windows 7（用于基于 x64 的系统）Service Pack 1 (4012215) 月度汇总更新[1]	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	严重 远程代码执行	重要 信息泄漏	严重 远程代码执行	3212646



3) 下载补丁或拷贝离线补丁

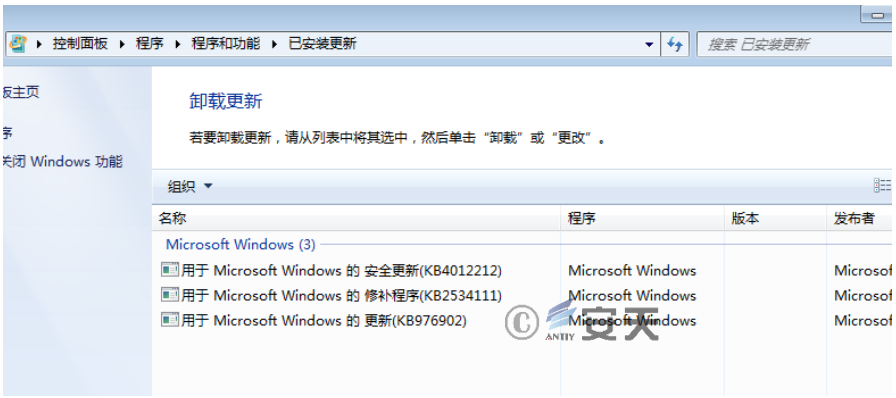


4) 在需打补丁系统内运行补丁程序，点击“是”安装补丁信息。



5) 安装完成，重新系统完成补丁更新。

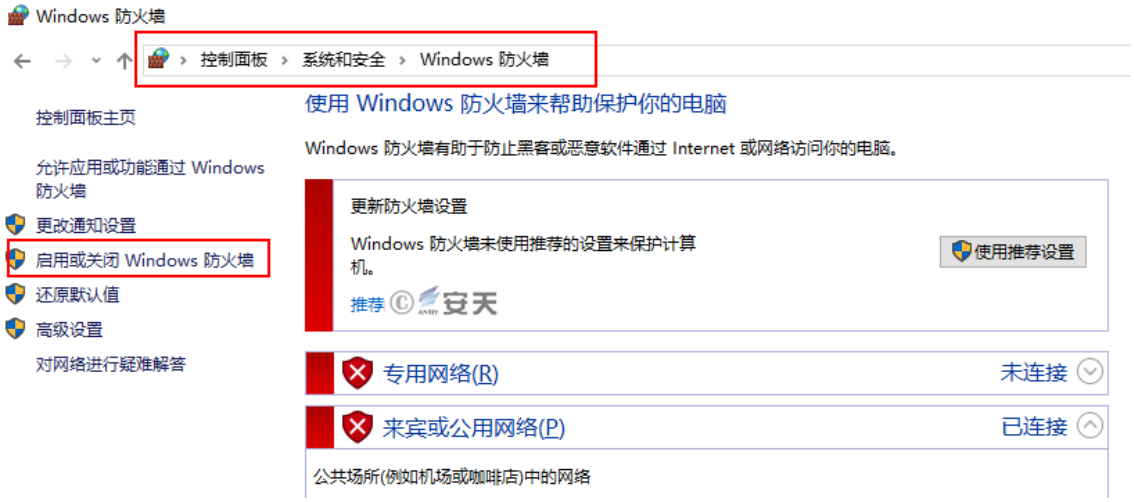
6) 进入系统，控制面板->程序和功能->查看已安装更新，如图出现安装的补丁号，表示补丁安装成功。



3.2 Win7、Win8、Win10 的安全配置处理流程

1) 关闭网络

2) 打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙



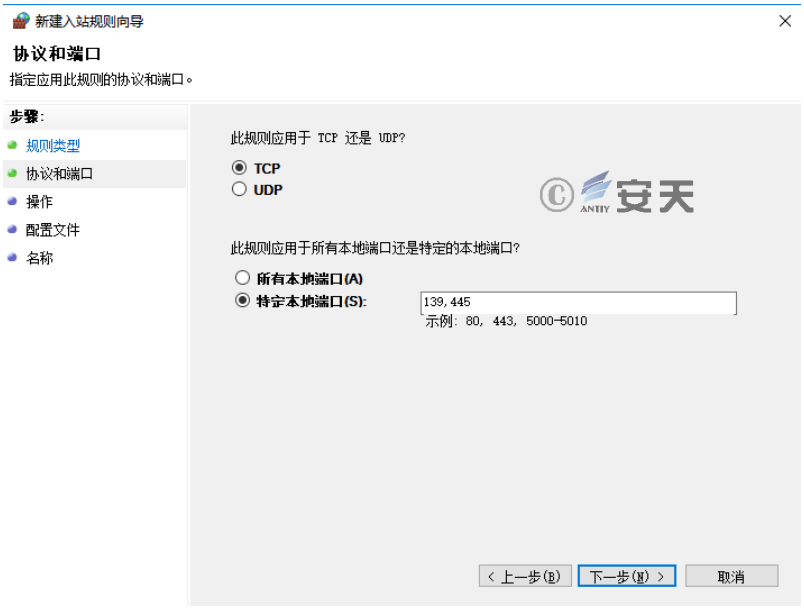
3) 选择启动防火墙，并点击确定

4) 点击高级设置

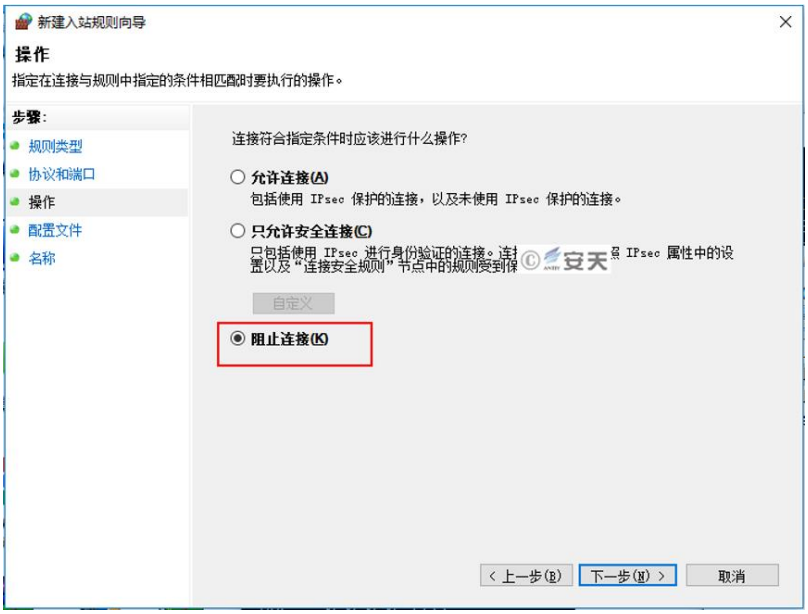
5) 点击入站规则，新建规则，以 445 端口为例

6) 选择端口、下一步

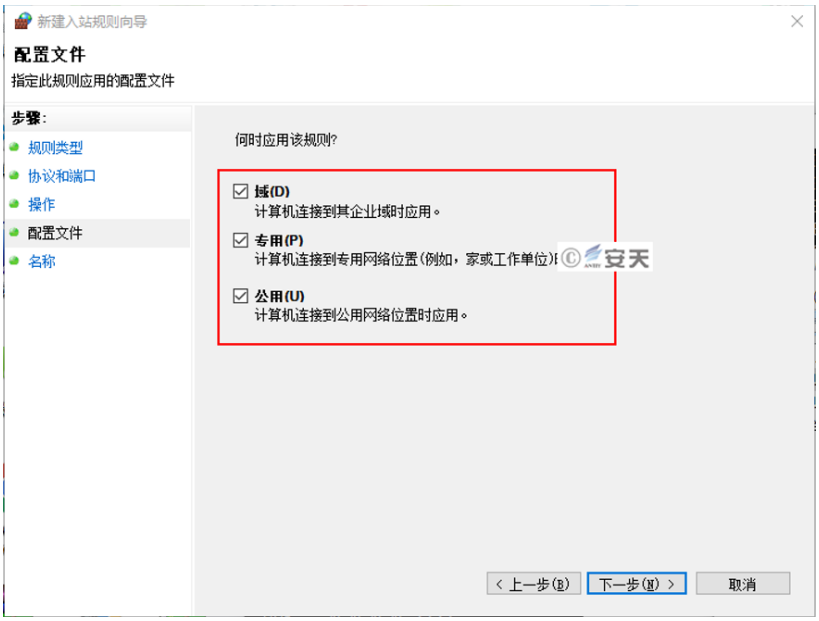
7) 选择特定本地端口，输入要防护的端口如 139、445，点击下一步



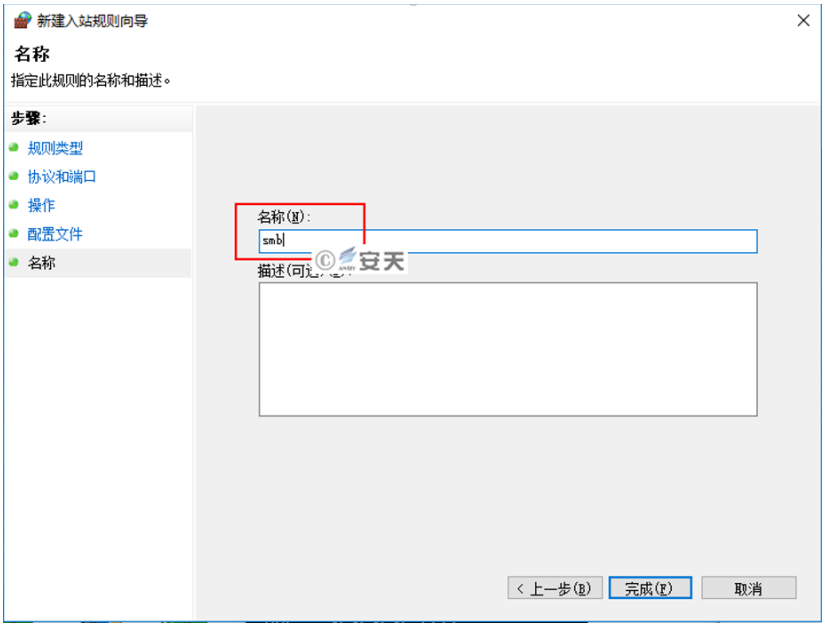
8) 选择阻止连接，下一步



9) 配置文件，全选，下一步

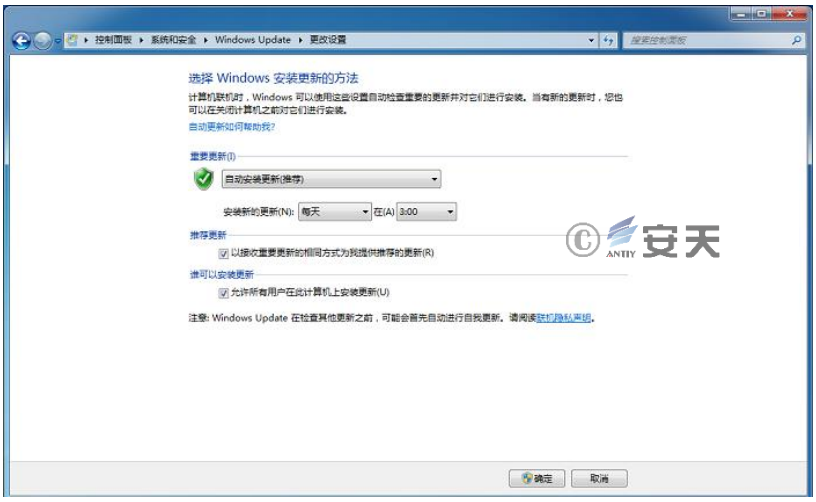


10) 名称，可以任意输入，完成即可。

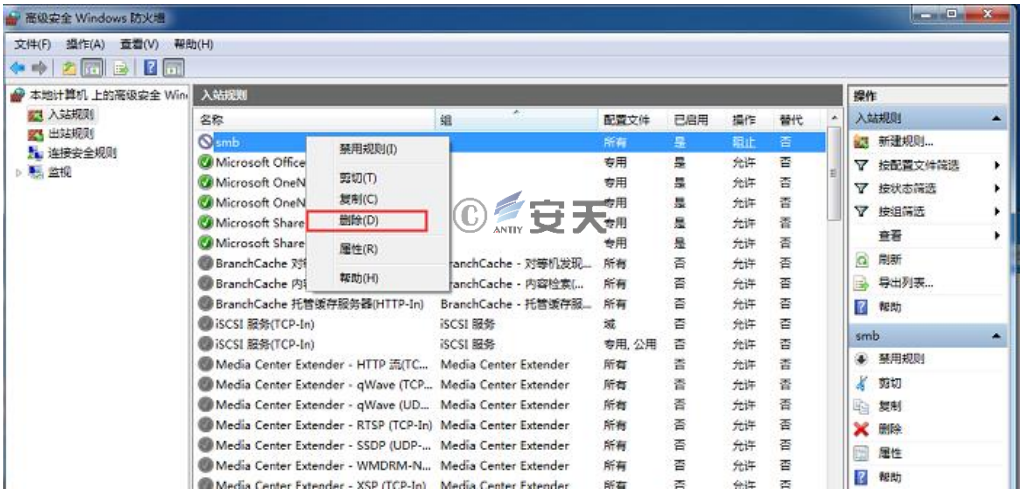


11) 恢复网络连接

12) 开启系统自动更新，并检测更新进行安装

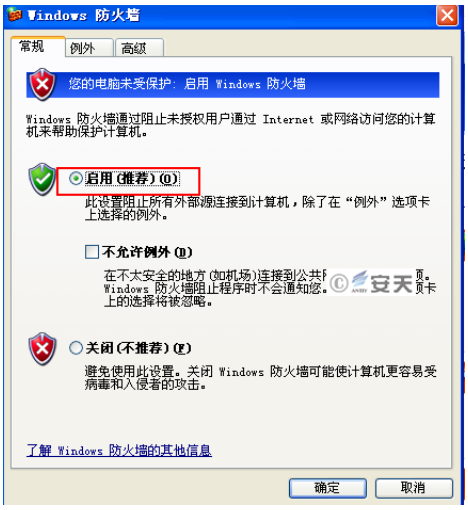


注：在系统更新完成后，如果业务需要使用 SMB 服务，将上面设置的防火墙入站规则删除即可。

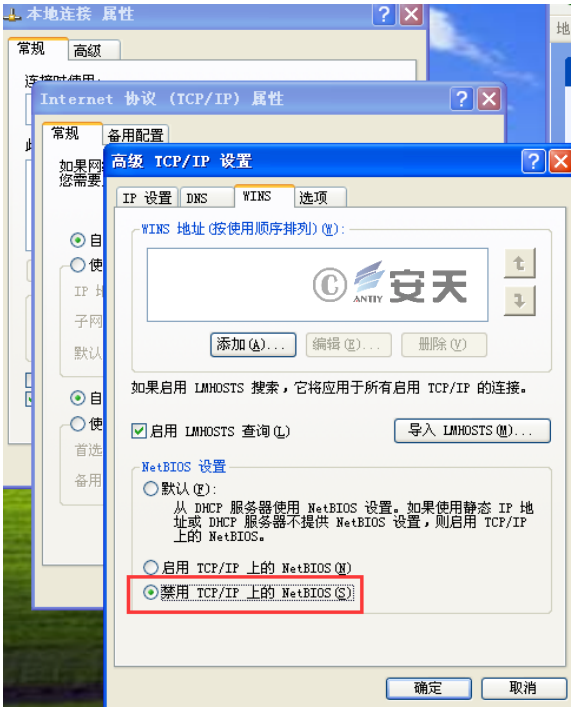


3.3 XP 系统的安全配置处理流程

1) 依次打开控制面板，安全中心，Windows 防火墙，选择启用。

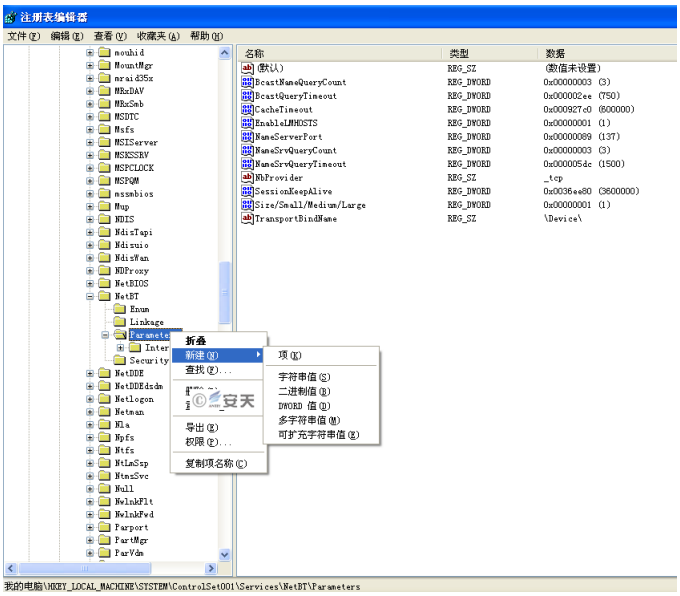


2) 关闭 139 端口，右击网上邻居－属性－右击本地连接－属性－internet 协议/(TCP/IP)－属性－高级－WINS－禁用 TCP/IP 上的 NETBIOS－确定。

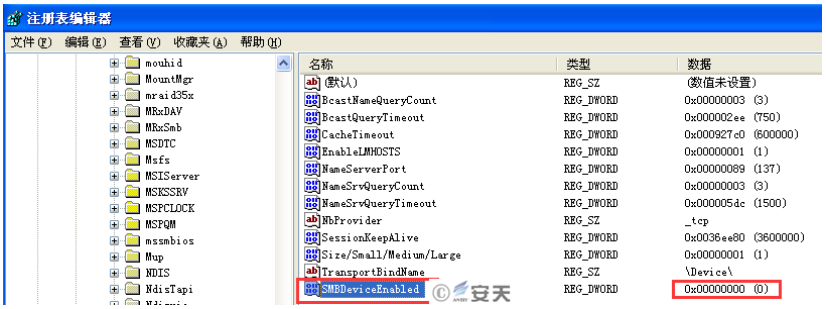


3) 通过注册表关闭 445 端口，单击“开始”——“运行”，输入“regedit”，单击“确定”按钮，打开注册表。

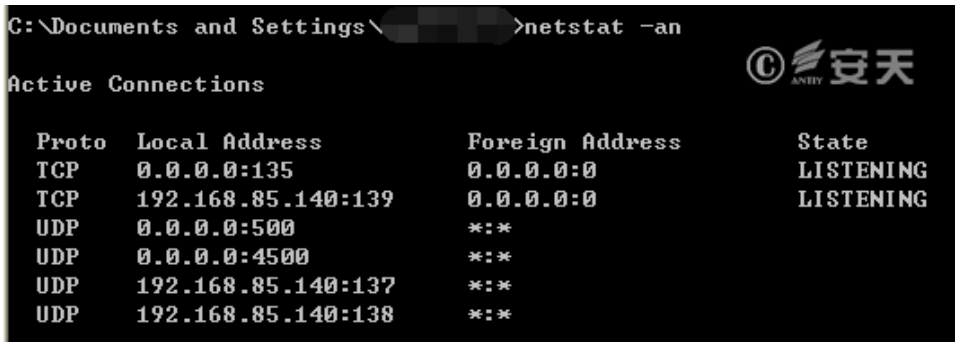
4) 找到 HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters，选择“Parameters”项，右键单击，选择“新建”——“DWORD 值”。



5) 将 DWORD 值命名为“SMBDeviceEnabled”，值修改为 0。



6) 重启机器，查看 445 端口连接已经关闭了。



4 总结

在较长一段时间以来，我国行业企业网络安全关注点，更多的在网站安全和暴露在互联网上的可感知业务节点上，其关注的更多的是网站篡改、DDoS 攻击等可感知度更高的风险。而对于感知度较低的秘密窃取、深度预制等 APT 攻击，特别是来自国家行为体的网络入侵预制，关注和投入不足。来自国家行为体、

特别是超级大国的网络攻击，通常具有极高的隐蔽性，难以捕获和发现。因此当武器级“永恒之蓝”漏洞被“魔窟”蠕虫非受控使用时，带来大面积影响也可想而知。

在 4.19 网信工作座谈会上，习近平总书记指出“网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是‘谁进来了不知道、是敌是友不知道、干了什么不知道’，长期‘潜伏’在里面，一旦有事就发作了。’”要求我们“聪者听于无声，明者见于未形”，“全天候、全方位感知网络安全态势”

因此，从整体来看，网络安全防御的重点应该从原来浅层次的网站安全和暴露在互联网上的一些业务节点入口安全转变为针对全面的信息系统节点，内网系统、业务系统和网络纵深展开，围绕着关键数据资产保障所展开。综合来看，从之前斯诺登爆料的 ANT 装备体系到“影子经纪人”所释放的与斯诺登的爆料相印证的材料，以及本批公开的漏洞利用工具和攻击平台，说明了超级大国在网络攻击方面，对整个内网体系，特别是对物理隔离系统的有效穿透能力。从这批漏洞来看，既说明了其取得“桥头堡”的能力，也说明了在穿透物理隔离防线后的全面横向移动能力。

面对这样一种综合性的能力，必须采用有效的产品和解决方案去应对。例如在端点安全上，传统反病毒的“非黑即白”模式，难以有效地应对远程端口植入、内存加载、浏览器劫持注入免杀恶意代码，而证书认证，虽然是供应链安全的保障，但对盗用软件厂商数字证书和深度的代码植入则又难以应对。因此需要采用黑白双控、信誉分析、行为建模等相应的端点防护手段，并结合强有力的安全配置策略和驱动层主防能力，才能改善端点防御情况。安天智甲终端防御系统基于上述机制设计，基于安天下一代威胁检测引擎所提供的黑白双项检测能力和向量分析能力，实现对可执行程序和内存对象的内容、行为、发布者和位置的综合授信判断，并给予生僻度、网内分布、场景连贯性等进行信誉分析。安天智甲支持更灵活的群组安全策略，在终端有效防护的基础上，可以实现全要素的感知分析和信息采集，以有效支撑用户态势感知系统的需求。安天智甲充分考虑到内网用户可能无法及时更新补丁的特点，提供了基础补丁+重点补丁的组合策略，通过热补丁、补丁动态策略期等来降低风险影响。针对勒索软件，安天智甲考虑到内网用户不可能按时更新病毒库的特点，通过检测引擎+主动防御+行为画像阻断的多重防御机制，即使经过深度加工伪装的勒索软件绕过引擎检测，其加密文件行为依然会被阻断。从而有效减低其带来的危害。

从流量监测来看，过去更多的是把边界侧的流量检测作为一个主要的检测点，采用的是单包的、轻量级的、实时化的检测方式，而从安天的研发部署探海威胁检测系统的安全实践来看，围绕着网络出口和重点网段的进行更细粒度基础流量解析（从五元组到十三元组）、载荷还原捕获、向量级的载荷分析，形成一个分析大数据，因此可以有效在获得威胁情报和分析成果时，建立起向前的追溯能力。在流量侧的全要素检测采集的基础上，可以完成对端点、链路和使用者的行为画像，从而有效呈现安全风险。

对于行业、企业网络每日进行着大量的运行维护、数据交换、文件分享等工作，而安全威胁也潜藏在这些行为之中，在这些可执行文件和文档文件之内。网内每日新增的载体文件，包括可执行程序以及相应的文档文件，不可能依靠用户本身的安全能力，或简单地凭借网络管理员的安全技能，去完成相关的判断，同时更不可能把文档文件传回给安全厂商做相应的分析支持，因此客户必须具备私有化的分析支撑能力。安天追影威胁检测系统是可以集群化部署于客户侧的分析系统，其不仅具备普通沙箱的动态分析能力，而且融合了安天深度的静态格式识别和解析能力，从而使分析可以寄托动态和静态向量的相互补充和验证来进行。除了对威胁的检测和解析，安天追影结合既有的黑白名单支持，可以直接进行威胁情报生产，使相关的安全网关、流量监测和终端侧能形成对 C2 等攻击方所使用资源的有效阻断。

安天的安全产品能够有效获得安天面向客户定向化的威胁情报同步和输送，用户亦可选择对接安天强大的云端分析能力和专家体系实现的有效支持。

在深度的防御对抗中，传统“地图炮”式的态势感知虽然可以展示部分威胁状况，但对于改善网络资产的实际安全保障水平，价值低微。安天的态势感知系统是围绕着资产和威胁视角展开的，实现资产信誉评价和威胁认知，充分了解资产和威胁的关联，评价威胁对资产所造成的后果和风险。

在 2 月 17 国家安全工作座谈会上，习近平总书记再次要求我们“加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护”。安天多年所做的基础工作和产品解决方案，正是围绕防护的有效性、感知的全面性和持续性而展开。防御武装到牙齿的网络攻击者，不能期望持续会有类似“斯诺登”或“影子经济人”的爆料，更不可能期望攻击者会留下开关域名式的可发现中止条件。协助客户感知、呈现、削弱和阻断最隐蔽、最高级的威胁，达成有效防护，实现价值输出，是安天产品的核心要义，是安天人的使命所系。

附录一：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近六亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*