安全的复杂与复杂的安全

肖新光 安天集团 首席技术架构师

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）

目录

从超级大国的一次攻击行动的复盘谈起

安天对超级大国网空攻击能力的分析轨迹

2010 分析起点

日期	题目
<网信军民融合>杂志2017年12月刊	美国网络空间攻击与主动防御能力解析（一）——概述篇
<网信军民融合>杂志2018年1月刊	美国网络空间攻击与主动防御能力解析（二）——美国大型信号情报获取项目
<网信军民融合>杂志2018年2月刊	美国网络空间攻击与主动防御能力解析（三）——美国网络空间安全主动防御体系
<网信军民融合>杂志2018年3月刊	美国网络空间攻击与主动防御能力解析（四）——美国网络空间进攻性能力支撑体系
<网信军民融合>杂志2018年4月刊	美国网络空间攻击与主动防御能力解析（五）——美国网络空间攻击装备体系
<网信军民融合>杂志2018年5月刊	美国网络空间攻击与主动防御能力解析（六）——用于突破物理隔离的网空攻击装备
……	……

超级大国一次攻击行动的完整可视化复盘

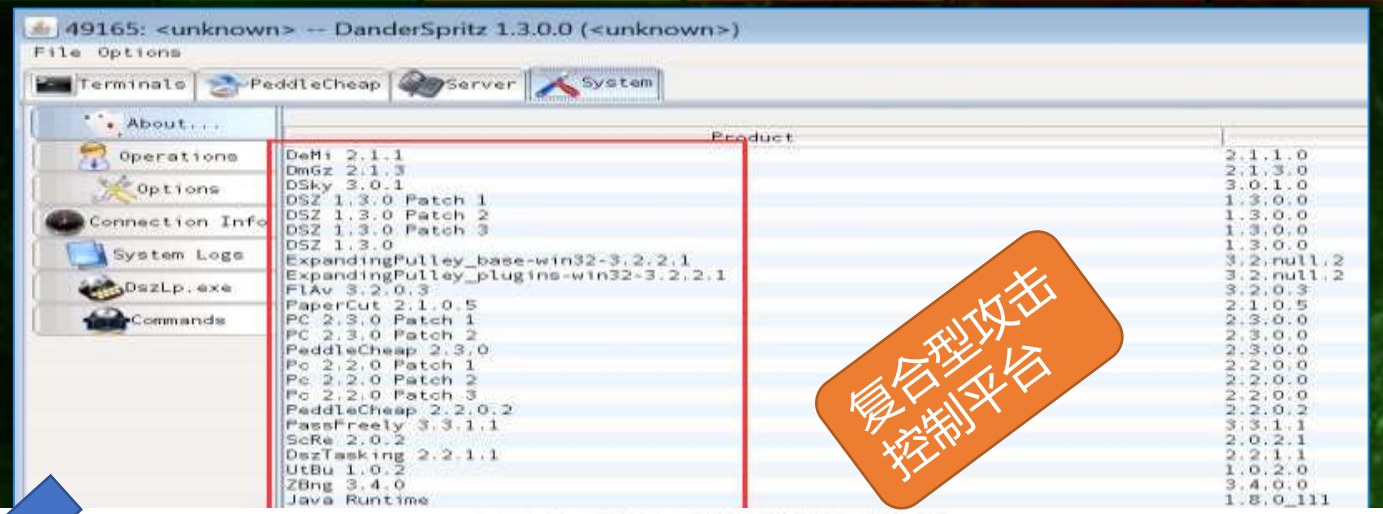
攻击EastNets所使用的网络攻击工具

装备名称	针对产品
ZESTYLEAK	针对Juniper防火墙的攻击工具
BARGLEE	针对Juniper防火墙的攻击工具
BANANAGLEE	一个用于植入CISCO ASA和PIX系列设备的非持续控制工具集合（只驻留于内存中，重启后失效），目的是在获取防火墙权限后，能够实现对设备的控制。
PITCHIMPAIR	Unix后门工具
INCISION	具有Rootkit功能的后门工具
FuzzBunch	FB平台是漏洞利用工具，可植入后门。
DanderSpritz	DS平台是远程控制程序的客户端，可在被植入后门的机器上执行各种操作。
ETERNALROMANCE	永恒系列攻击工具，ETERNALROMANCE (永恒浪漫) 是影响Windows全平台的SMBv1远程代码执行漏洞攻击工具，受影响的系统为Windows XP, Vista, 7, Windows Server 2003/2008/ 2008 R2等
ETERNALCHAMPION	永恒系列攻击工具，ETERNALCHAMPION（永恒冠军）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows Server 2008 SP1 x86等
ETERNALSYNERGY	永恒系列攻击工具，ETERNALSYNERGY（永恒协作）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows 8等
ETERNALBLUE	永恒系列攻击工具，ETERNALSYNERGY（永恒之蓝）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows 7/8/XP等
EXPLODINGCAN	EXPLODINGCAN（爆炸之罐）是IIS6.0 webDAV漏洞的攻击工具。

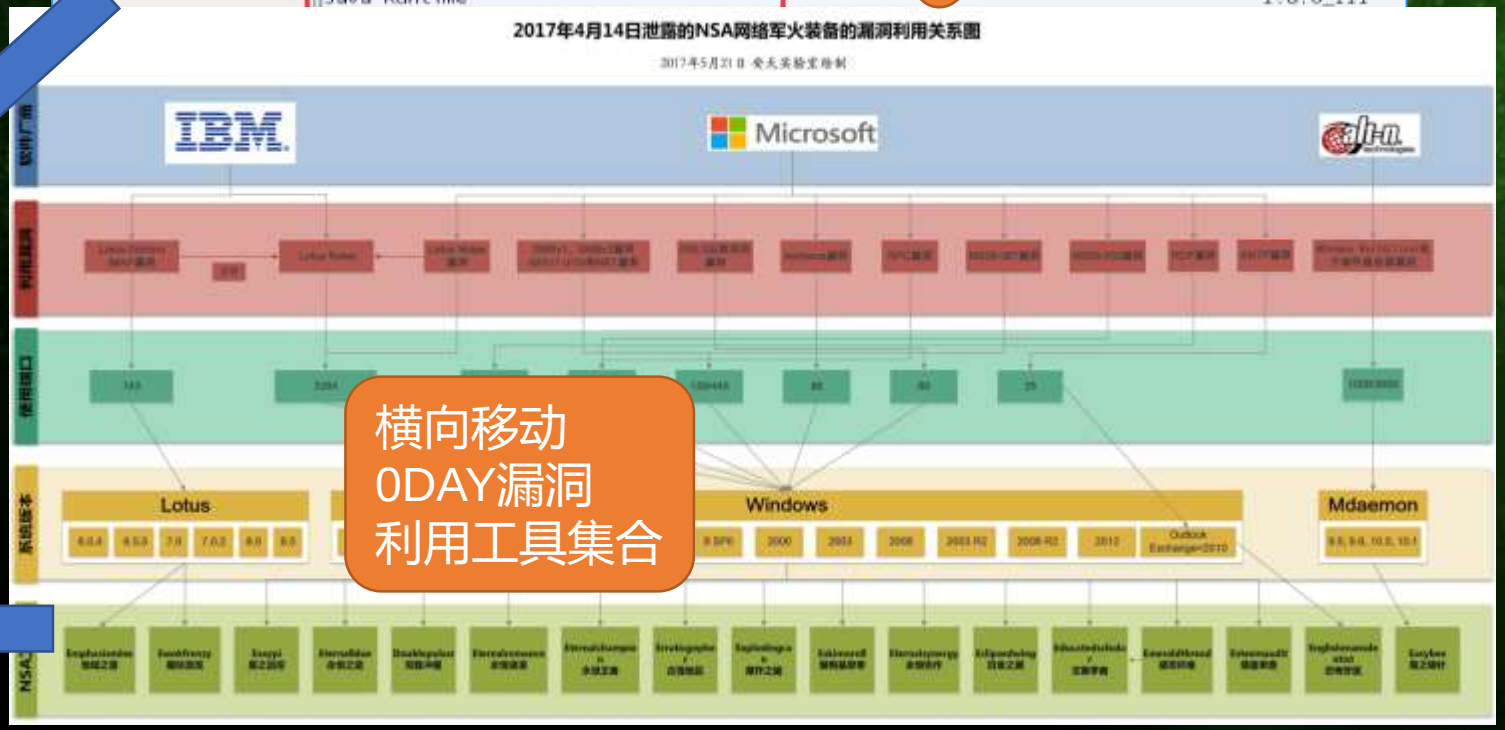
超级大国攻击EastNets所使用的网络攻击工具及漏洞

针对性场景植入和持久化工具

装备名称	针对产品
ZESTYLEAK	针对Juniper防火墙的攻击工具
BARGLEE	针对Juniper防火墙的攻击工具
BANANAGLEE	一个用于植入CISCO ASA和PIX系列设备的非持续控制工具集合（只驻留于内存[illegible]后失效），目的是在获取防火墙权限后，能够实现对设备的控制。
PITCHIMPAIR	Unix后门工具
INCISION	具有Rootkit功能的后门工具
FuzzBunch	FB平台是漏洞利用工具，可植入后门。
DanderSpritz	DS平台是远程控制程序的作业端，可在被植入后门的机器上执行各种操作。
ETERNALROMANCE	永恒系列攻击工具，ETERNALROMANCE (永恒浪漫) 是影响Windows全平台的SMBv1远程代码执行漏洞攻击工具，受影响的系统为Windows XP, Vista, 7, Windows Server 2003/2008/ 2008 R2等
ETERNALCHAMPION	永恒系列攻击工具，ETERNALCHAMPION（永恒冠军）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows Server 2008 SP1 x86等
ETERNALSYNERGY	永恒系列攻击工具，ETERNALSYNERGY（永恒协作）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows 8等
ETERNALBLUE	永恒系列攻击工具，ETERNALSYNERGY（永恒之蓝）是影响Windows的SMB[illegible]执行漏洞攻击工具.受影响的系统为Windows 7/8/XP等
EXPLODINGCAN	EXPLODINGCAN（爆炸之罐）是IIS6.0 webDAV漏洞的攻击工具。

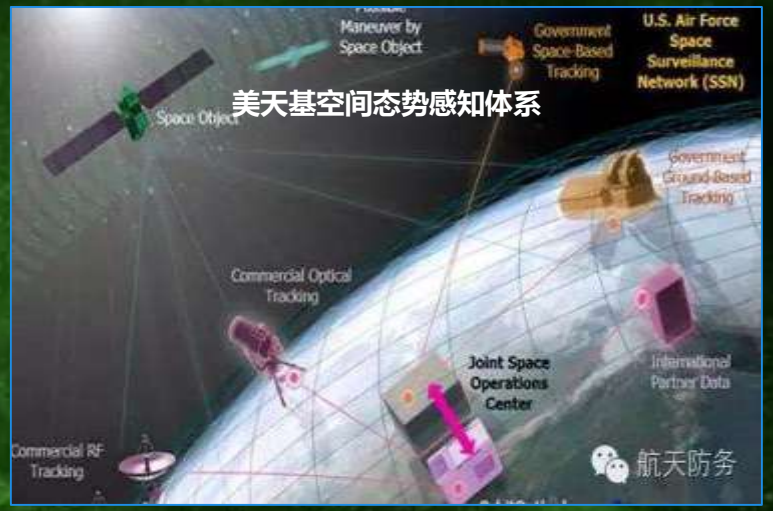


复合型攻击控制平台



横向移动
0DAY漏洞
利用工具集合

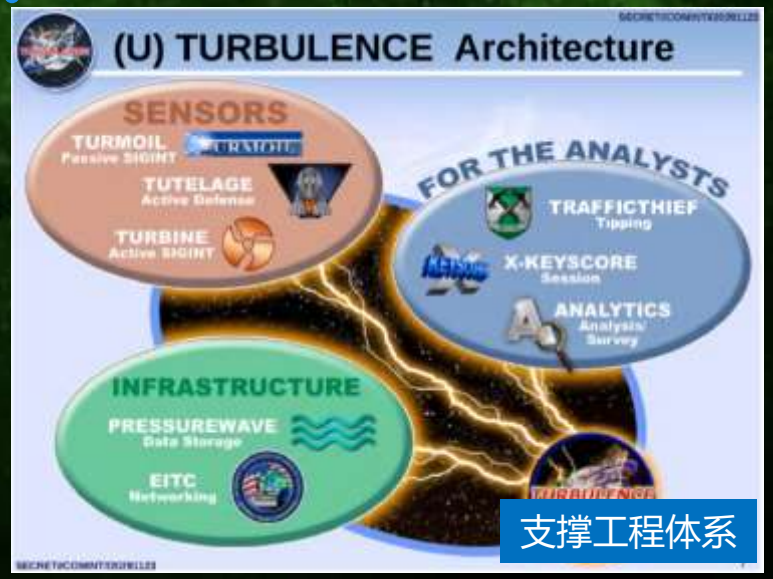
在大工程系统的支持下形成攻击作业能力



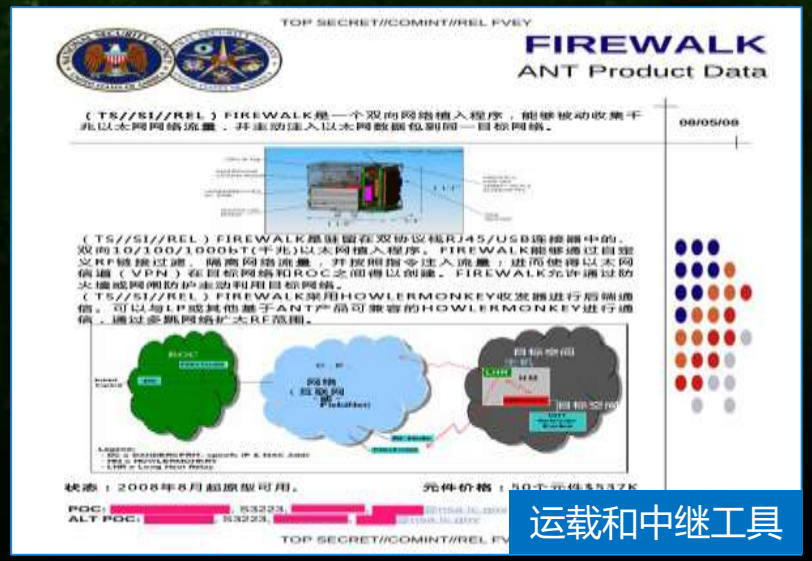
美天基空间态势感知体系

美B2隐形轰炸机

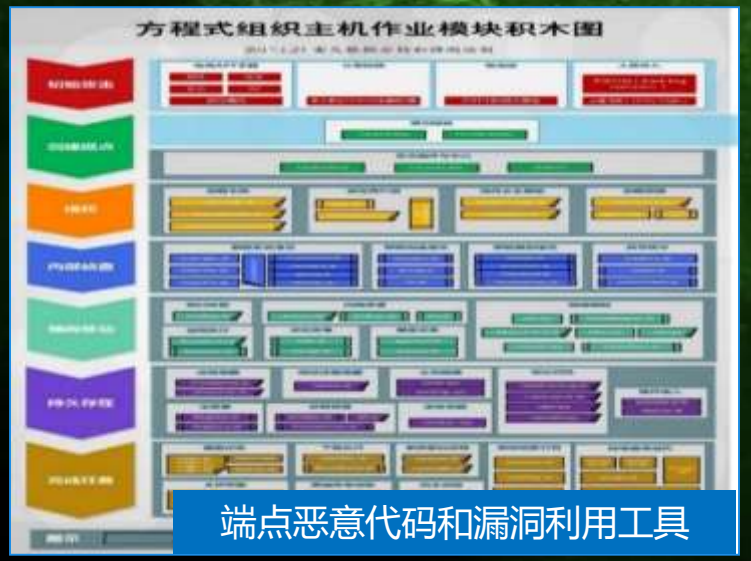
美军防区外空地导弹



支撑工程体系



运载和中继工具



端点恶意代码和漏洞利用工具

超级大国全球监控项目（工程体系）支撑网空作业能力

NSA全球监视项目/工程体系（部分）

名称	监视对象	作业方式	主要系统
“棱镜” PRISM	网络数据，与境外人士通信的美国公民的全球即时通信和资料	供应链感染 (与互联网软硬件供应商合作)	XKEYSCORE
“溯流” UPSTREAM	通过骨干网络光缆和交换机直接复制光信号，网络数据	供应链感染	TUMULT
“梯队” ECHELON	通信卫星传输的个人和商业通信（大规模监视）		XKEYSCORE
BLARNEY	网络内容数据（核扩散、反恐、经济、军事、政治等）及元数据	全面收集&监视	XKEYSCORE MAINWAY
SKIDROWE	卫星通信内容监视	卫星通信	TURNWEALTHY(信号获取) XKEYSCORE
“奔牛” BULLRUN	加密通信数据	利用超级计算机，破解各种网络安全协议	GALLANTWAVE XKEYSCORE TURMOIL
FAIRVIEW	移动电话监视	“商业合作” 疑为AT&T	
MAINCORE	针对外国手机用户的大众监视		
MYSTIC	以反恐（阿富汗）为目标的语音拦截		XKEYSCORE
MUSCULAR	海外窃听	谷歌和雅虎未加密的内部网络	Turmoil
SENTRY EAGLE	对手信号情报收集		

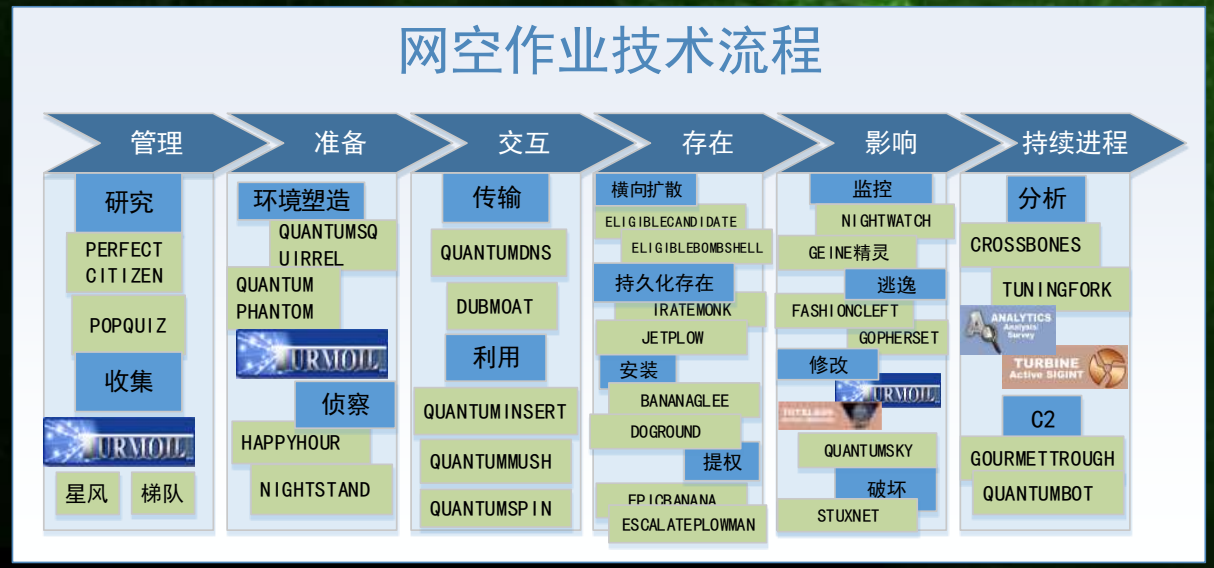
NSA网络作业框架“湍流”及其子系统

子系统名称	功能
TUMULT	中点主动采集系统. 分流装置（硬件）。不影响/作用于流量本身，仅仅是复制-转发 。
TURMOIL	全球信号情报（包括卫星、微波、有线通信信号 ）的被动收集机制，TURMOIL系统部署于互联网骨干结点（路由器、服务器），对数据包进行拦截和分析。
TURBINE	任务逻辑（C2 结点）。深度包注入技术，用于植入自动 C2 软件，有效创建由“政府控制的 botnet”。 该系统位居被动采集系统TURMOIL 与 Quantum 的主动攻击机制之间，是二者之转接器。
QUANTUM	网络作业管理系统，即向互联网侧目标部署作业工具，或操纵已部署工具。部署于NSA内网，由TAO(定制访问办公室)远程作业人员操纵，其作业能力覆盖广泛，包括域名系统（DNS）和HTTP注入式攻击等多种网络攻击工具、数据库注入工具、僵尸网络控制工具等。
TUTELAGE	情报驱动的积极防御系统，采用深度包监测技术，能够对恶意流量报警、阻断、重定向等，部署于国防部网络。
XKEYSCORE	能够检索数据库中的信息，用于关键目标的定位
LONGHAUL	密码服务系统，支持情报分析
PRESSUREWAVE	数据仓库系统
TRAFFICTHIEF	针对高价值目标的近实时流量分析系统

超级大国网络空间进攻性能力体系

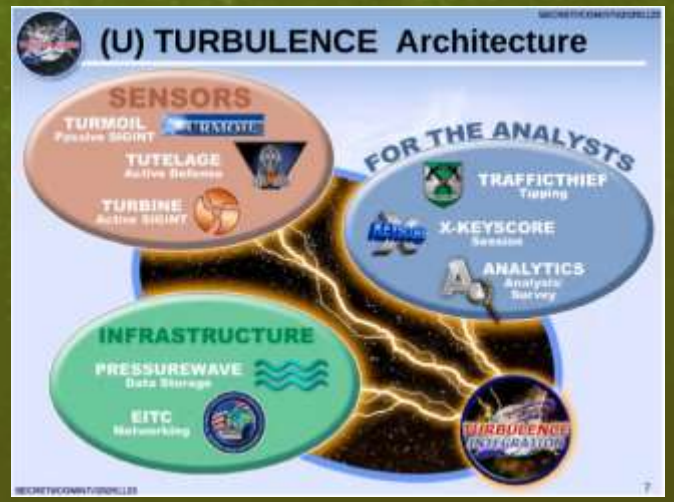
NSA-TAO装备表（部分）

ANT	待确定			
DEITYBOUNCE	GECKO II	QUANTUMINSERT	SHOTGIANT	FOGGYBOTTOM
IRATEMONK	GODSURGE	QUANTUMMUSH	TUTELAGE	QUANTUMSKY
IRONCHEF	ROGUESAMURAI	QUANTUMSPIN	VIEWPLATE	QUANTUMDIRK
JETPLOW	PERFECT CITIZEN	SENTRY HAWK	VOYEUR	QUANTUMDNS
SWAP	POPQUIZ	SHORTSHEET	DUBMOAT	HAPPYHOUR
NIGHTSTAND (NS)	CROSSBONES	TEFLONDOOR	HANGARSURPLUS	MIRROR
GOPHERSET	TUNINGFORK	BANANAGLEE	FESTIVEWRAPPER	NIGHTSTAND (NS)
MONKEYCALENDAR	BLINDDATE (BD)	DOGROUND	QUANTUMBOT	WICKEDVICAR
NIGHTWATCH	CRYPTICSENTINEL	MISTYVEAL (MV)	QUANTUMBOT2	FLOCKFORWARD
RAGEMASTER	CUTEBOY	ODDJOB	STORMPIG	QUANTUMSQUIRREL
GOURMETTROUGH	DARKHELMET	WICKEDVICAR	SURPLUSHANGAR (SH)	QUANTUMPHANTOM
	DEAD SEA	ZESTYLEAK	WARNVULCANO	FLASHHANDLE Mission Management (FMM)
DNT	HAMMERCHANT	EPICBANANA (EPBA)	ELIGIBLEBOMBSHELL	
FASHIONCLEFT	HAMMERSTEIN	ESCALATEPLOWMAN	ELIGIBLECANDIDATE	
FOGYNULL	HAPPYHOUR	STUXNET	ELIGIBLECONTESTANT	
CASTLECRASHER	NOPEN	RETURNSPRING	EGREGIOUSBLUNDER	



完备的网络空间进攻性能力支撑框架

- “湍流”是美国国家安全局（NSA）是NSA在21世纪信号情报（SIGINT）任务的核心作业框架，具有进攻性的网络战能力；
- 其综合考虑了感知获取、作业层面和后端分析，构成了对可精确打点、具有较好隐蔽性和反溯源性的支撑。



全球网络地形绘制和目标寻址能力

- 通过全球部署的被动收集系统Turmoil进行全球信号情报采集；
- 利用主动收集系统Turbine对互联网流量进行过滤，筛选出感兴趣的流量信息，并触发指挥控制模块；
- 指挥控制模块会将相关信息发送给TAO的节点，由TAO执行网络攻击。

- 通过情报分析定位目标，使用“量子”对目标进行网络攻击；
- 其中“量子之手”（QUANTUMHAND）主要针对的Facebook等可以识别身份的社交网站用户，当目标访问社交网站时，TURBINE系统可以先于真实的Facebook服务器给出反馈，发送诱骗数据包，将目标重定向至TAO的服务器，之后进行恶意代码植入等攻击。

针对Facebook用户的Man-on-the-side攻击

全球网络地形绘制、目标寻址和目标行为采集分析能力

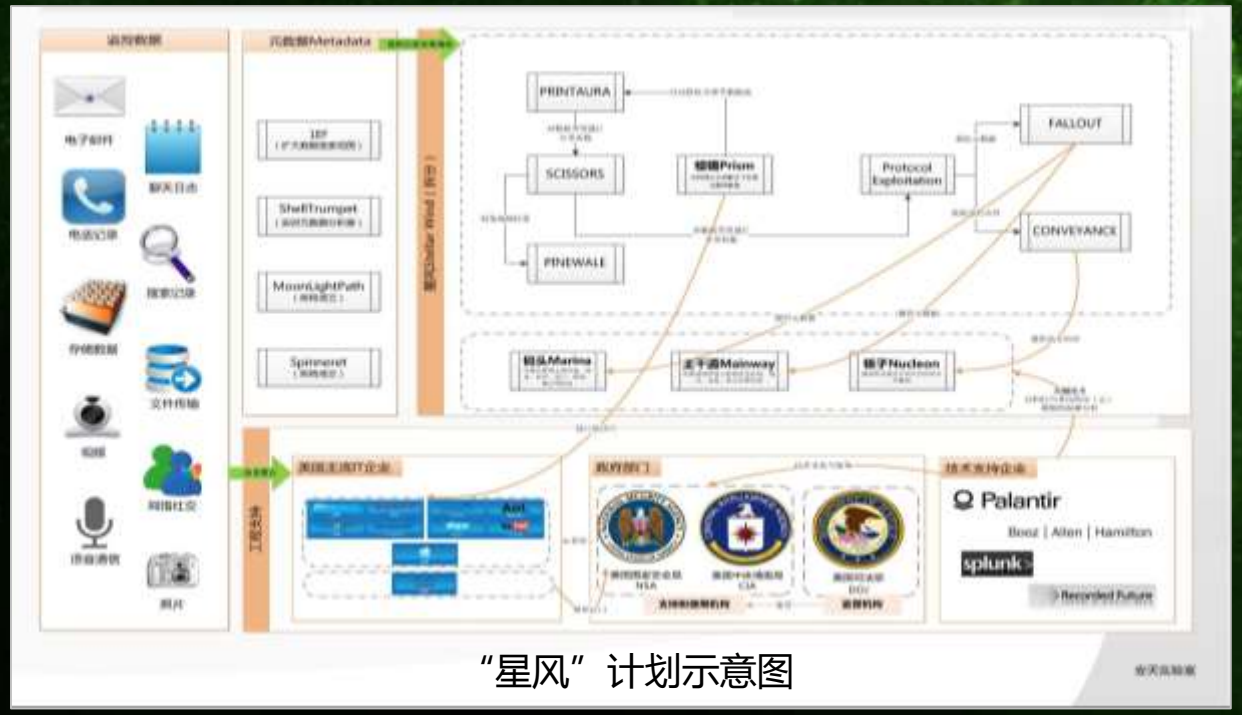
- “星风计划”启动于2004年，是美国政府秘密开展的大规模搜集情报监控信息的计划。由于法律程序等敏感问题星风计划被拆分为“棱镜”(PRISM)、“主干道”(MAINWAY)、“码头”(MARINA)以及“核子”(NUCLEON)四大项目交由NSA掌管。

“棱镜”(PRISM) 利用美国主要互联网企业所提供的接口进行情报作业

“主干道”(MAINWAY) 对通信元数据进行搜集和分析

“码头”(MARINA) 对互联网元数据进行搜集和分析

“核子”(NUCLEON) 截获电话通话者对话内容及关键词



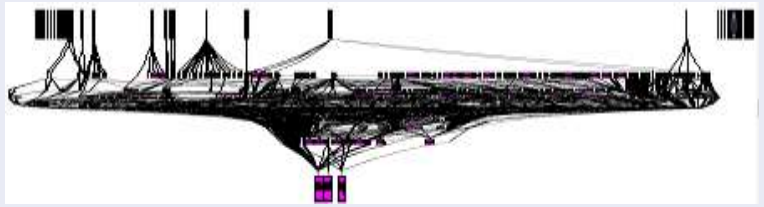
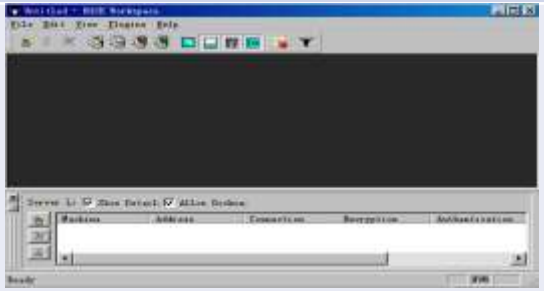
“星风”计划示意图

面对类似的网络安全威胁我们必须考虑到的因素

- 高级威胁行为体有突破目标的坚定意志、充足资源、成本准备。并进行体系化的作业。
- 任何单点环节均可能失陷或失效，包括网络安全环节本身。
- 信息系统规划、实施、运维的全过程，都是攻击者的攻击时点。
- 防御者所使用的所有产品和环节同样是攻击方可以获得并测试的。
- 攻击者所使用的攻击装备有极大可能是“未知”的，这种未知是指其因在局部和全局条件下，对于防御方、和防御方的维护支撑力量（如网络安全厂商）来说，是一个尚未获取或至少不能辨识的威胁。

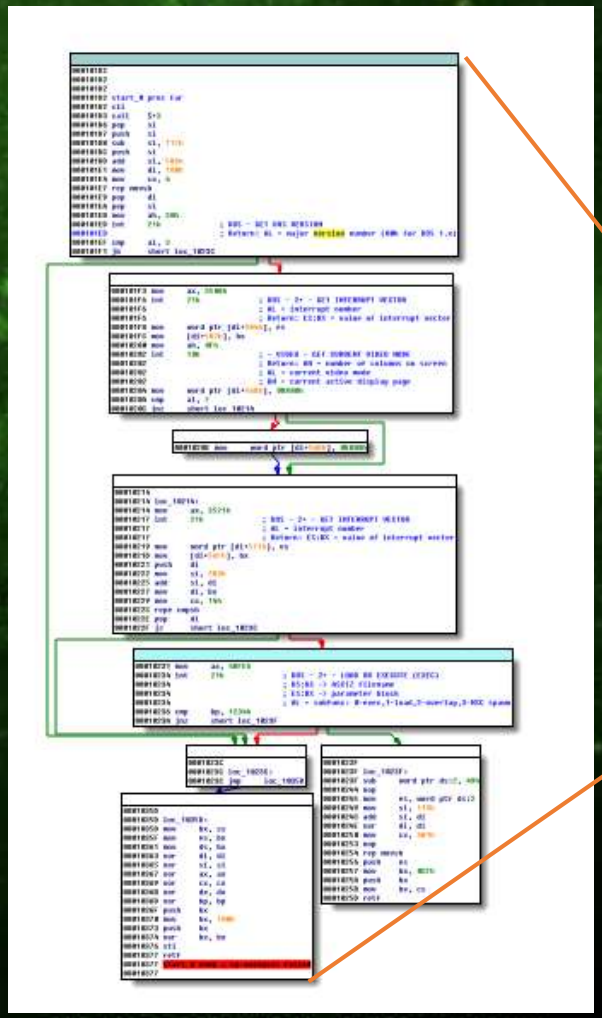
从复杂的威胁到敌情想定

恶意代码的复杂度增长

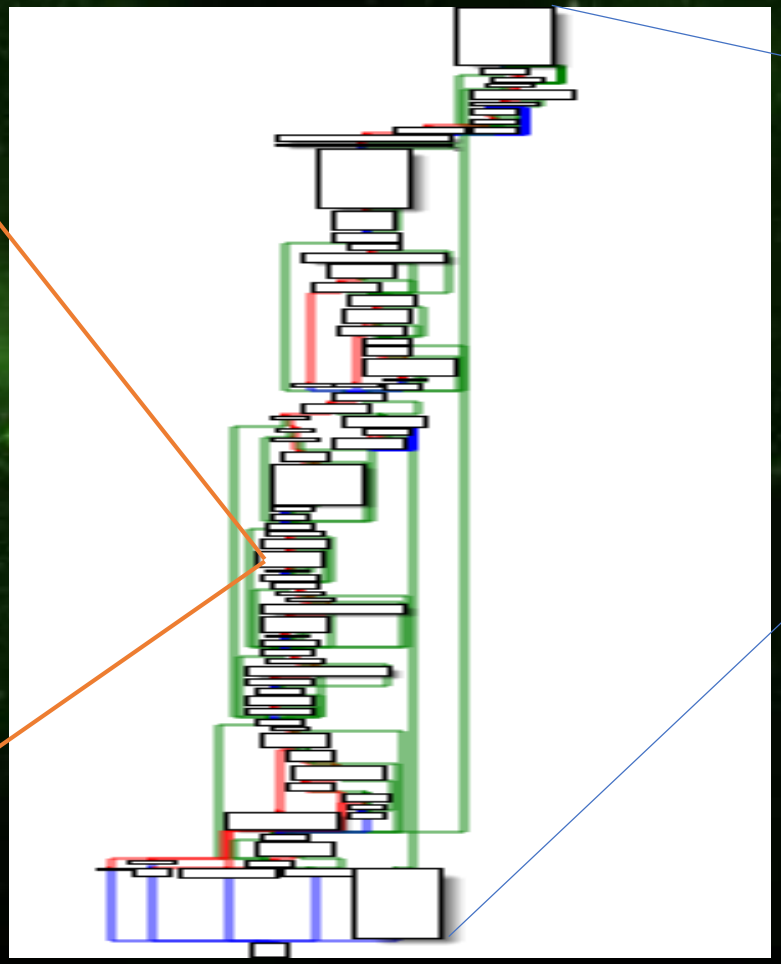
	DOS样本	早期木马（以Back Orifice ）	APT样本（以方程式攻击组织的DS为例）
运行平台	DOS平台	Windows平台	全平台
样本数量	单一样本	单一样本（少数带有插件）	样本集合（集成化、模块化）
代码行数	几十到几百行	5W-7W行左右	百万行
函数调用			
网络通信	无	多数为无加密通信	多种方式加密通信
开发者	个人	个人或民间小规模组织	有充足成本支持的规模型组织
命令与控制	无	简单	复杂
操作界面	无		
回连地址	无	需要感染节点能够被控制端访问到	大量地址
生命周期	短	几周	隐匿，长期控制
控制方式	无	正向连接	正向、反向、激活、近场控制等
使用漏洞	无	几乎没有	0day
抗分析能力	无	相对比较简单，易于分析	高强度的本地加密，复杂的调用机制

恶意代码的复杂度增长（续）

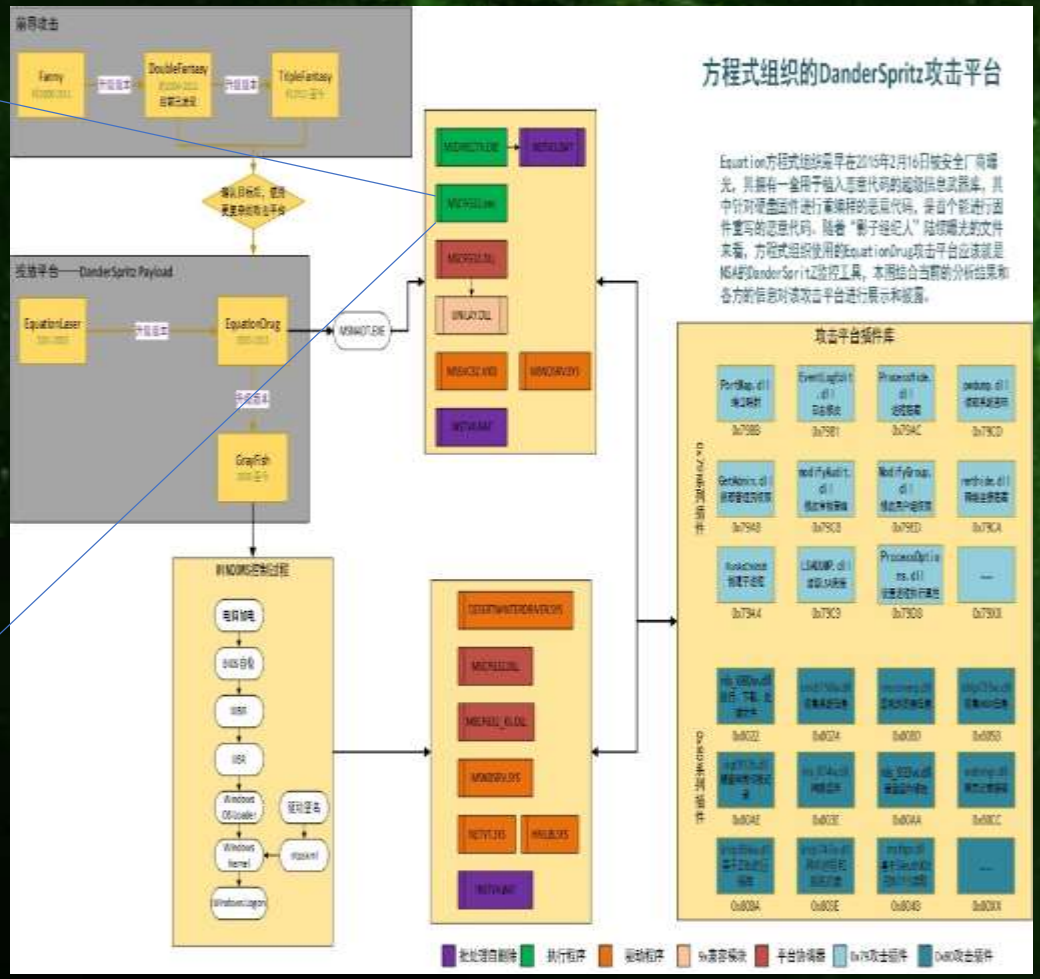
DOS病毒（ Storm）



Back_Orifice_2000

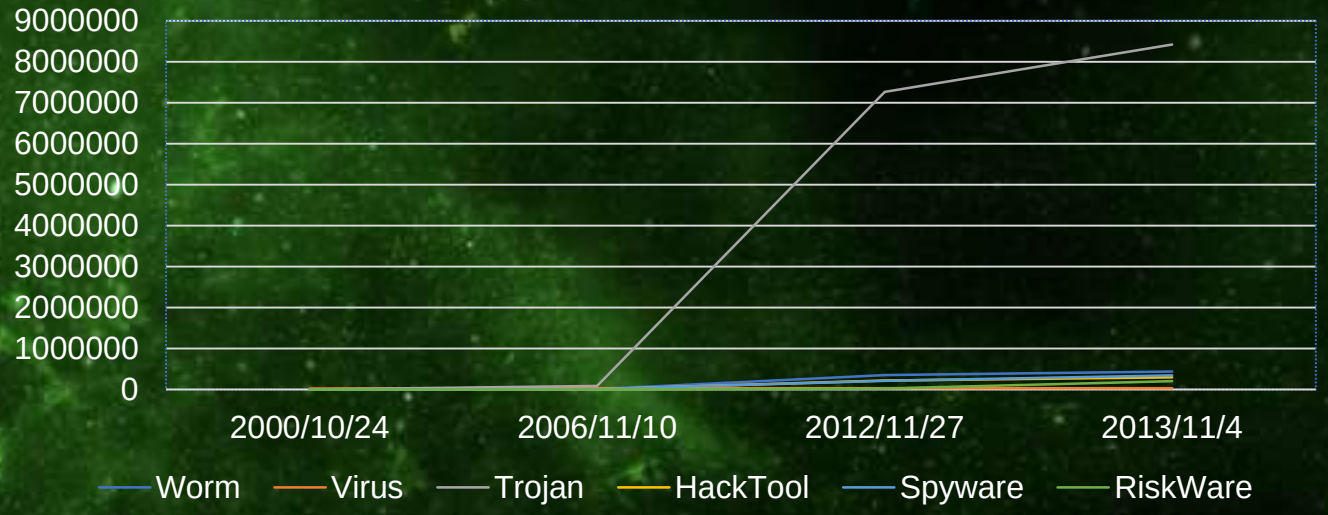


APT（方程式DS攻击平台）



恶意代码种类的发展变化

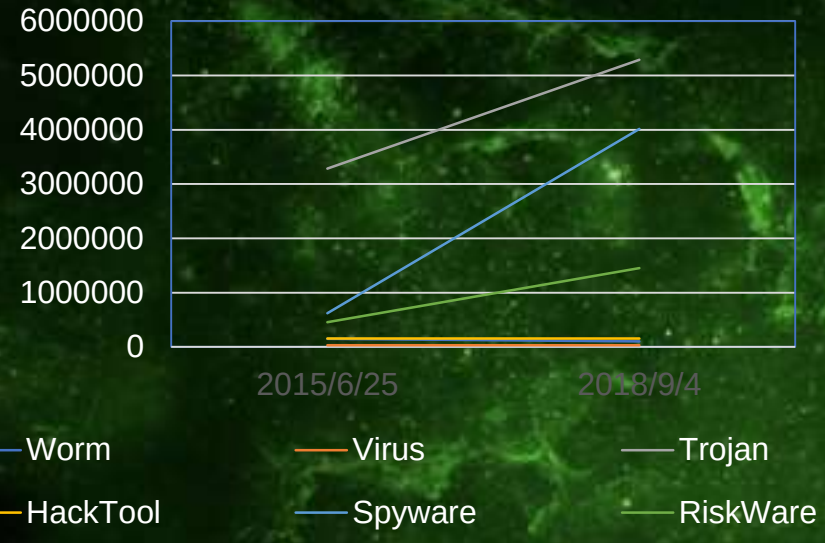
2000-2013恶意代码的变种总量统计



分类/日期	2000/10/24	2006/11/10	2012/11/27	2013/11/04
Worm	512	8109	354049	435247
Virus	21006	27760	29940	30060
Trojan	3066	84811	7262094	8423751
HackTool	260	4968	217502	301076
Spyware	37	4899	214570	340751
RiskWare	0	88	25800	201401

从观测来看2014年，由于卡巴后台分析与同源合并能力的增强，导致此后的数据度量衡发生了变化。因此无法连续统计。

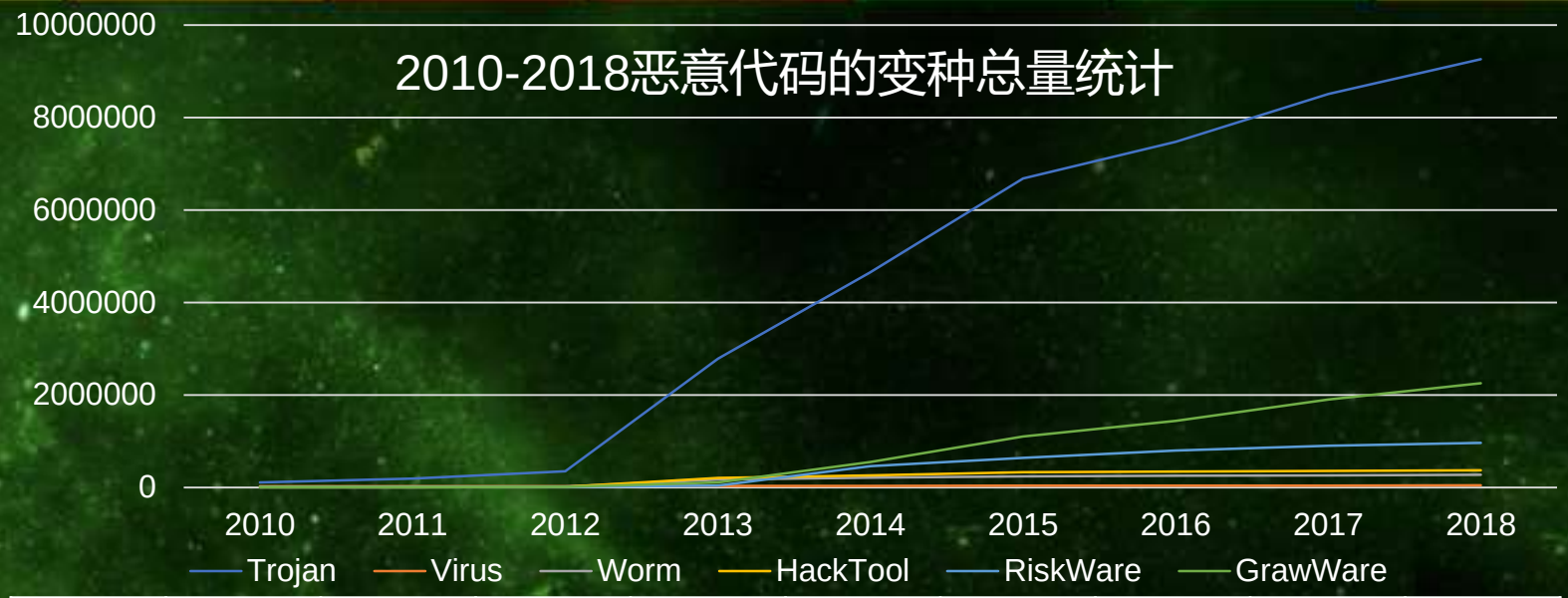
2015-2018恶意代码的变种总量统计



2015/06/25	2018/09/04
149137	101674
29397	29980
3283882	5289006
153493	154800
622344	4013384
458035	1451458

来源：Kapersky对应日期病毒名列表

恶意代码持续增长带来的影响



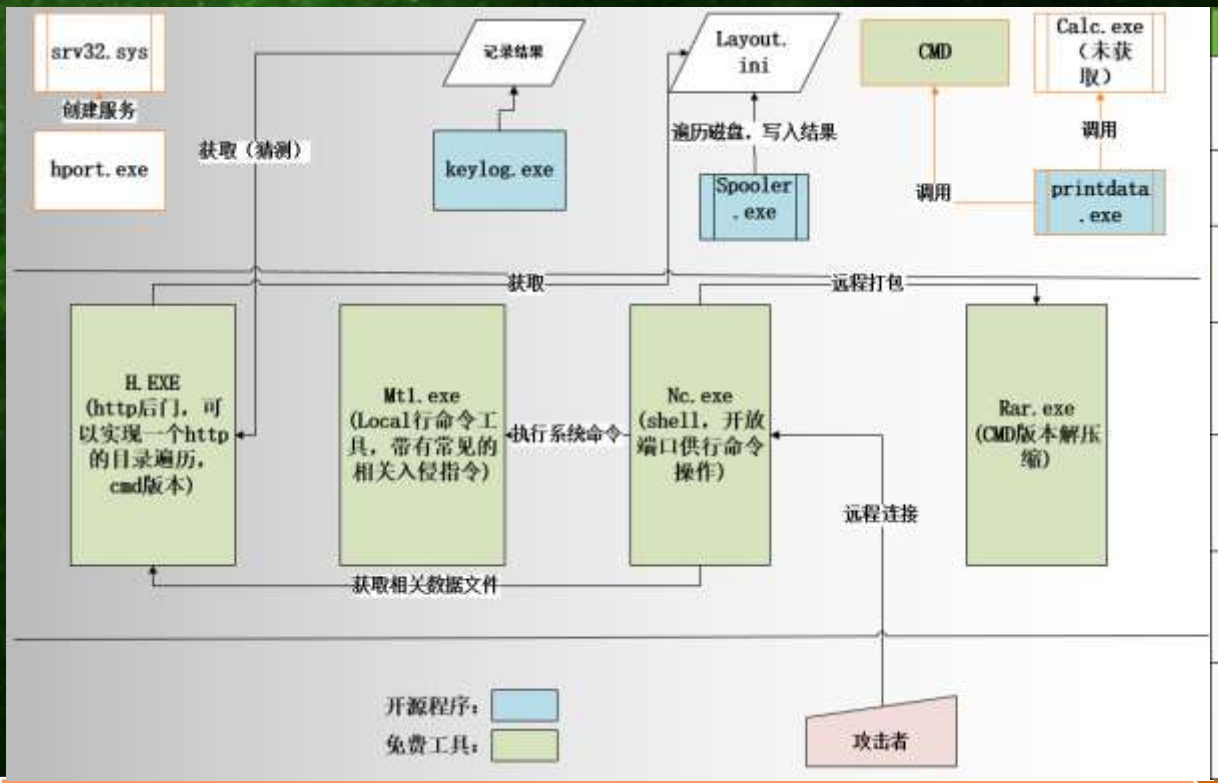
分类/年份	2010	2011	2012	2013	2014	2015	2016	2017	2018
Trojan	105856	191344	351168	2781524	4654026	6679871	7473987	8508125	9260840
Virus	24688	25090	25927	30496	34915	37658	39567	40623	48065
Worm	10473	14914	20335	172832	208851	240974	255247	261843	271410
HackTool	5043	7690	10323	207639	257627	328041	342796	356414	372576
RiskWare	3887	6868	9705	38226	457698	641942	795007	902246	965398
GrawWare	3874	5739	12736	105309	548852	1102948	1436328	1898963	2249846

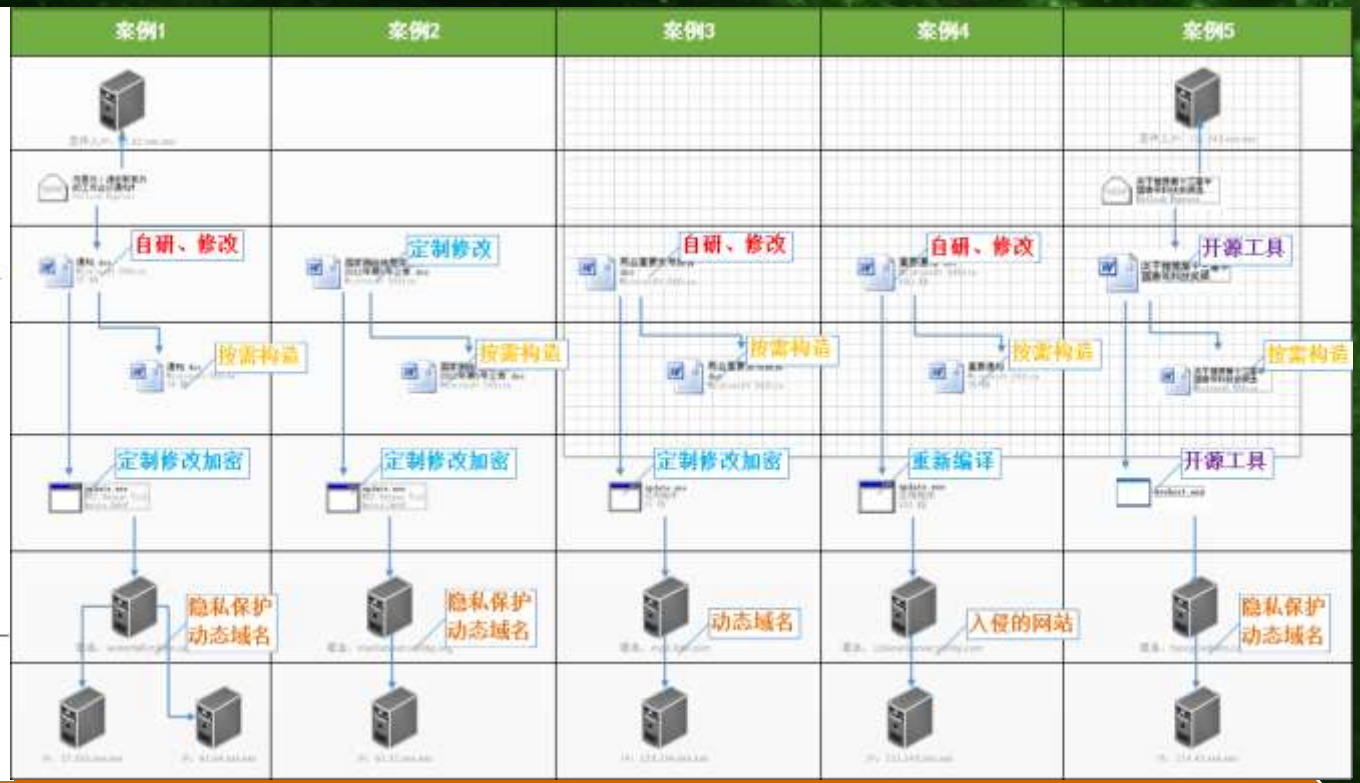
- 军火级恶意代码失窃流失、商业军火销售、恶意代码开源、对正常开源和免费工具的改造和利用。导致现有恶意代码的威胁图谱高度复杂。
- 样本自动化分析技术尽快已经十分普及，但分析大数据即是追踪溯源的助力，也带入大量干扰项。
- 僵尸网络为高级威胁带来更多的可用资源，高级攻击者可以直接劫持利用现有僵尸网络。

来源：安天基础样本流水线的处理结果

研发投入驱动绿斑组织的攻击装备的演进

- 绿斑组织在2007年前后自研能力有限，对开源和免费工具比较依赖，作业风格受到早期网络渗透攻击的风格影响较大。自2010年以后，该地区组织攻击能力已经有所提升，善于改良1day利用，能够对公开的网络攻击程序进行定制修改，也出现了自研的网络攻击武器。





2007-2010

2011-2017

加速度：商业军火带来的演进

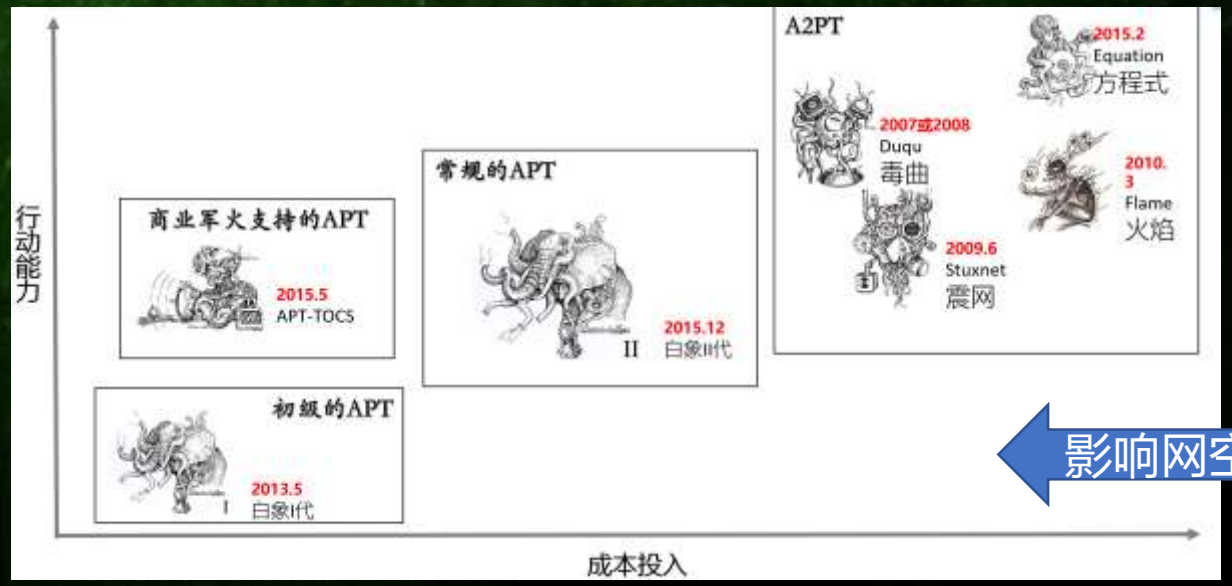
公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

旋转门型开发者 → 研发“全栈”攻击平台

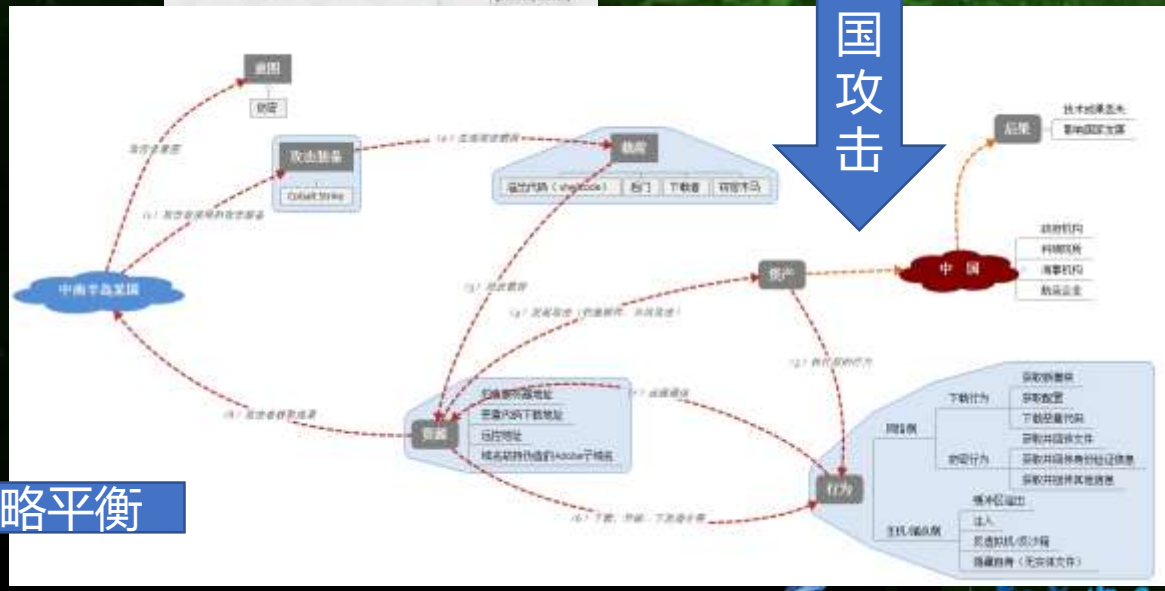
Packages
- HTML Application
- Java Application
- MS Office Macro
- Payload Generator
- USB/CD AutoPlay
- Windows Dropper
- Windows Executable
- Windows Executable(S)

Web Drive-by
- Manage
- Auto-Explo
- Client-side
- Clone Site
- Firefox Ad
- Attack

用于对中国攻击



影响网空战略平衡



中南半岛某国的攻击行为图谱

没有敌情想定的网络安全是注定无效的

国家/政经集团行为体

民间复合行为体

传统民间行为体

对手：层次化的攻击行为能力
具有其自身战略/利益意图的作业方向

外部信息环境

基础电磁（信号）环境处于对手广泛监听

关键链路设备被入侵和控制

互联网服务者、云和其他公共互联网基础设施供应商存在不可靠性

社会关系

所有关键系统的用户多数都是互联网用户。

所有社会关系可以从互联网定位摸底。

全民数据已经泄露。

敌已在内

内网已（将）被渗透，人员已（将）被策反，这是最基础和核心的想定

供应链

上游研发、生产、场景均可被控制和入侵。

物流仓储不能保证可靠。

运维、升级、更换等均不能保证可靠

对外信息交换

广泛的信息交换必须发生

威胁针对性的跟随信息交换

敌情：真实极限化/的敌情想定

（平时）
持续性对抗
隐蔽性对抗
（战时）
高烈度对抗
（平战）
无底线对抗
高成本对抗

网空斗争的特点

从IAD的防御五条规则看美方的敌情想定

IAD(Information Assurance Directorate，**信息保护办公室**)——NSA之盾。

- 负责引导各部门设计最先进的信息保障和网络安全解决方案，以确保国家的核心任务环境免受任何以及所有不断演变的威胁。
- “既然网络空间是我们保护信息的主要舞台，我们正在努力塑造一个敏捷而安全的运营网络环境，**在那里我们可以成功地超越任何对手。**”（IAD官网）

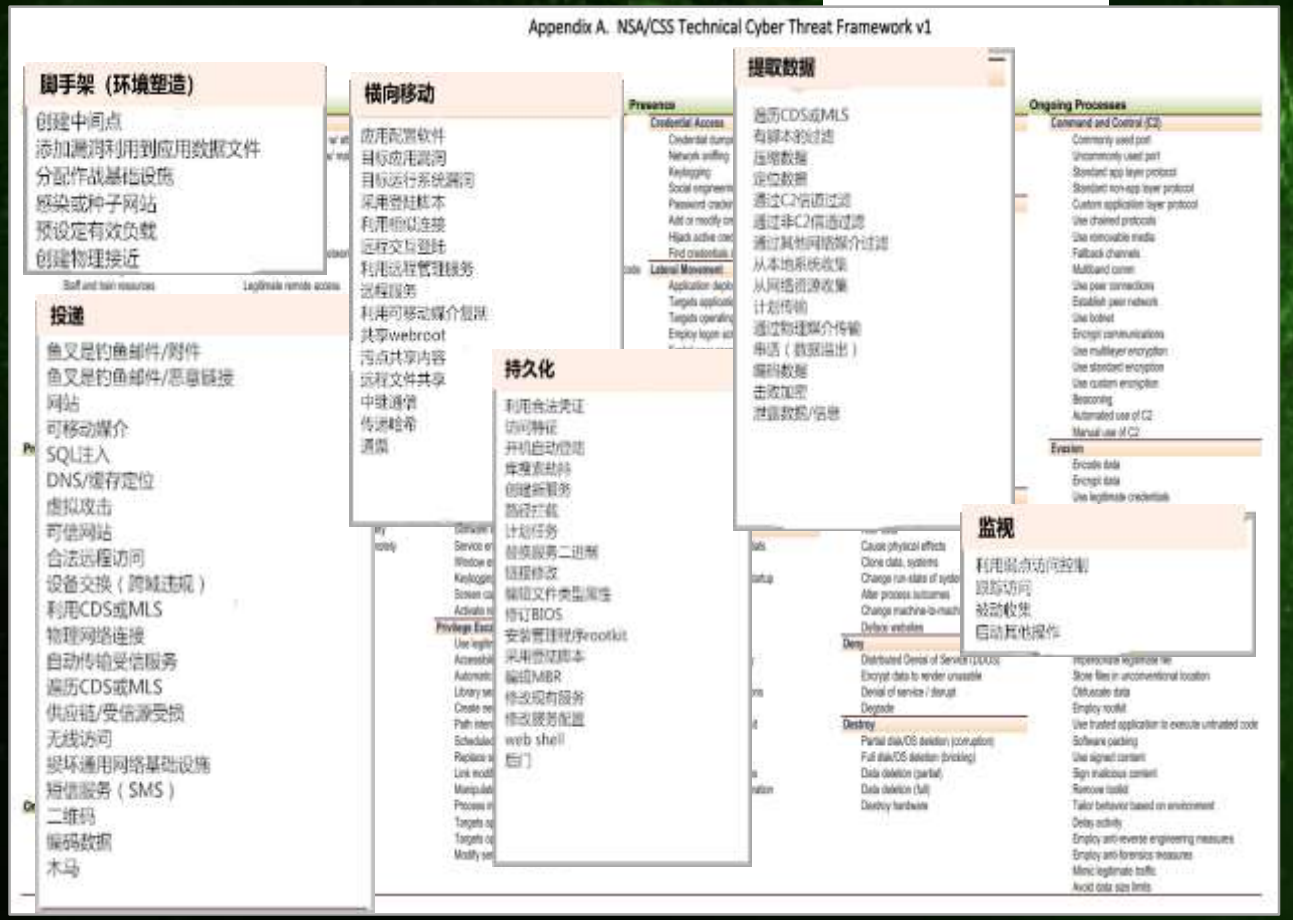
Rule #1: They are going to get in.
敌方将要进入我方内网

Rule #2: Network defenders cannot change rule #1.
网络防御者不能改变第一条。

Rule #3: They are already in.
敌方已经进入我方内网

Rule #4: Attacks will continue.
攻击将会持续进行

Rule #5: It's going to get worse.
情况会越来越糟



敌情想定是针对性的、具象的

我方机构和行业领域	敌方攻击意图	攻击目标和入口	目前场景特点和缺陷
***网	窃取我方核心机密、干扰战略性决策、长期持久化和预制、战时毁瘫	供应链污染、物流劫持、组合攻击、人员派驻发展、摆渡攻击	缺少系统性敌情分析，单点防护依然为主导，反特、保密和安全工作没有有效整合。
政务内网	窃取我方秘密信息、干扰决策、长期持久化和预制、向更高目标摆渡、战时毁瘫	供应链污染、物流劫持、组合攻击、人员派驻发展、摆渡攻击	检测深度和防御纵深需要进一步提升，单点防护依然为主导
政务外网	窃取我方敏感信息、长期持久化和预制、向更高价值目标摆渡	邮件、网站（水坑）等。	检测深度和防御纵深需要进一步提升，电子邮件威胁相对离散
关键基础设施	获取核心运行数据，干扰系统运行、破坏社会稳定	外网暴露接口、离散战、运行维护支撑环节、内部人员扩展等。	主要依靠隔离防护，规划体系不清晰，安全防护不足，大量核心节点裸奔。

几个典型场景的基本敌情想定对比

敌情想定是针对性的、具象的（续）

几个典型的需要梳理敌情想定的攻击场景

我方机构和行业领域	敌方攻击意图	攻击目标和入口	目前场景特点和缺陷
自主产品企业	植入漏洞弱化我产品安全性;获取我方代码和产品进行漏洞分析挖掘;窃取产品证书绕过白名单	环境入侵、跳板攻击、人员带入等	开发人员自身的安全能力和经验不足；缺少有效的安全开发方法引入；缺少场景安全保障
高科技企业	获取我方技术成果进行抄袭模仿；在商业竞争中获取谈判等优势；在产品进行预制弱化下游环节安全	互联网侧直接攻击、基于上游供应链入口的攻击等	人员高度依赖互联网，容易被从网上定位摸底，
军工企业、民参军企业	获取装备信息参数；借鉴模仿；弱化干扰我方武器能力，进行针对性对抗	针对关键人员摸底的间接攻击、人员带入等	较大比例是制造、电子、精密加工企业，网络安全意识和投入不足
高等院校、科研院所	窃取我方科技成果；获取我方重大工程项目进展；了解国防和其他关联领域情报	互联网入口；学术交流活动和等	缺少持续性的安全防御投入和能力；依赖阶段性的保密检查推动安全改进；人员流动性较大。
遥感测绘部门	获取我方基础数据、干扰篡改测绘数据	监听还原信息传输、入侵存储数据等	以发展和效率为主导的思路，缺少总体安全观的指导
智囊机构	获取我方决策支持思路、	社会工程；基于互联网以邮件等入口直接攻击等	个人单点目标价值大、人员安全意识差、

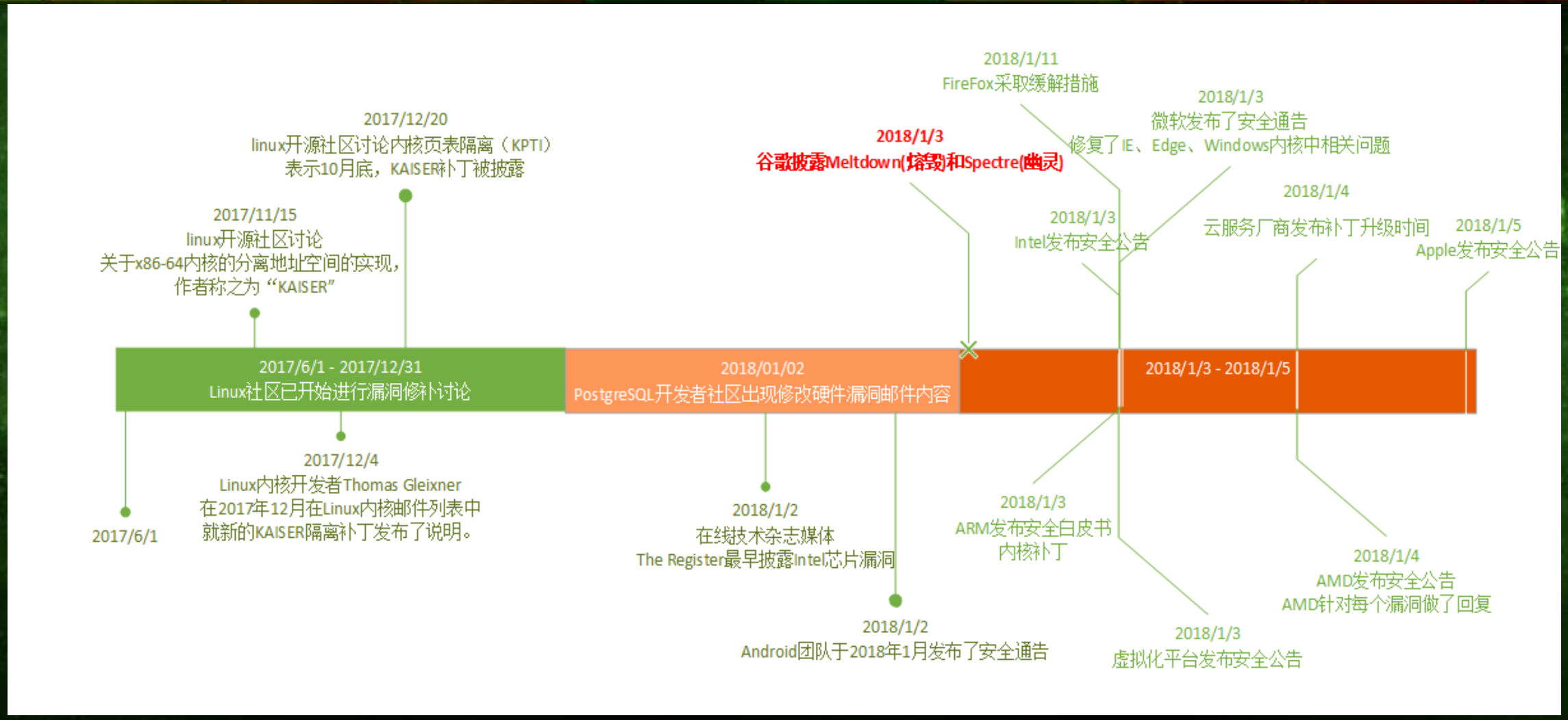
几个典型场景的基本敌情想定对比

敌情想定是基于对手作业能力和机会窗口期的对位

	白象一代（2012）	白象二代（2015）
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	以中国的大面积目标为主，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC 、 VB 、 DEV C++ 、 AutoIT	Visual C#、AutoIT
二进制攻击载荷加壳情况	少数使用UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

- 我们不只面临风险，而是面临后果。
- 对手作业窗口遭遇未修复漏洞，要以对手已经利用漏洞完成植入为想定，形成深入排查和重新布防，而非简单的漏洞修补。
- 恶意代码、僵尸网络感染未及时处理，不是简单的消杀，而是要基于已经被对手劫持控制利用来进行应对。

信息化现状的复杂性与攻击机会窗口叠加是一个复杂问题



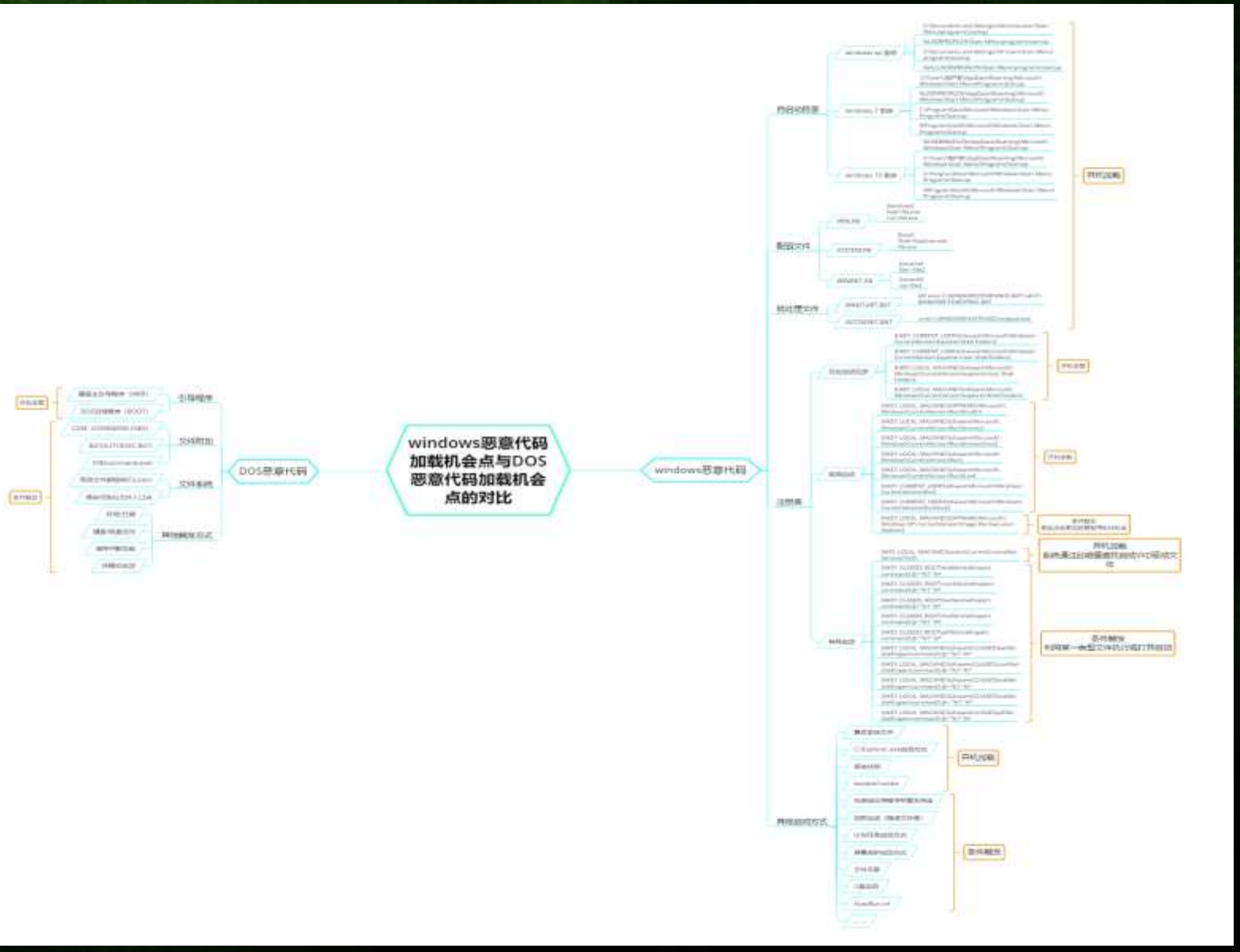
A级漏洞Meltdown(熔毁)和Spectre(幽灵)的处置分析说明重大漏洞补丁处置极为复杂
而攻击时间窗口需要深入分析推演

网络安全防御是复杂的系统性工作

信息系统复杂性的沧海一粟：以PC发展为例

年代	CPU						内存					操作系统		
	具体年份	型号	CPU主频	CPU位数	晶体管数量	制造工艺	具体年份	型号	针脚	单条容量	运行频率	具体年份	型号	代码行数
1970-1980	1978	8086	5MHz-10MHZ	16位	2.9万	3微米								
	1979	8088	4.77MHz-8MHZ	内部16位，外部8位	2.9万	3微米								
1980-1990												1981	DOS 1.0	数千行（猜测）
	1982	80286	6MHz-25MHz	16位	13.4万	1.5微米						1984	DOS 3.0	N/A
							1982	SIMM内存	30pin	256k	N/A	1985	Win1.0	N/A
	1985	80386	12MHz-40MHz	32位	27.5万	1微米-1.5微米	1988	SIMM内存	72pin	512KB-2MB	N/A	1987	Win2.0	N/A
	1989	80486	16MHz-100MHz	32位	90万/118.5万	0.6微米-1微米								
1990-2000	1993	Intel Pentium	50MHz-200MHz	32位	320万	0.6微米	1991	EDO DRAM	72pin	6M-16M	N/A	1990	Win3.0	N/A
	1995	Pentium Pro	150MHz-200MHz	32位	220万	0.355微米-0.5微米						1992	Win4.0	N/A
	1997	Intel Pentium MMX	166MHz-300MHz	32位	450万	0.35微米						1993	DOS 6.0	N/A
	1997	Intel PentiumII	233MHz-450MHz	32位	750万	0.18微米-0.35微米						1995	Win95	N/A
	1999	Intel PentiumIII	450MHz-1.4GMHz	32位	950万	0.13微米-0.25微米						1998	Win98	1500万
2000-2010	2000	Intel Pentium4	3.06GHz	32位/64位	5500万	0.18微米、0.13微米、0.09微米.65纳米	2000	DDR1	180pin	128M-1G	400MHz	2000	Win2000	N/A
	2002	Intel Pentium 4 HT	3.2GHz-3.5GHz	32位/64位	N/A	90纳米						2002	WinXP	4000万
	2003	Intel Pentium M	1.3GHz-1.6GHz	32位	7700万	90纳米	2003	DDR2	240pin	256M-4G	1066MHz			
	2005	Intel Pentium D	2.8GHz-3.2GHz	32位/64位	2.3亿	90纳米								
	2006	Intel Core 2 Duo	2.2GHz	32位/64位	2.91亿	65纳米、45纳米						2006	Vista	5000万
	2008	Intel Core i3/i5/i7	2.8GHz/3.46GHz	32位/64位	5.82亿	32纳米、45纳米	2007	DDR3	240Pin	512M-8G、16G	1066MHz	2009	Win7	5000万
2010-2018	2010	第二代处理器 （Sandy Bridge架构）	2.4GHz-3.8GHz	32位/64位	11.6亿	32纳米								
	2012	第三代处理器 （Ivy Bridge架构）	2.6GHz-3.9GHz	32位/64位	18.6亿	22纳米						2012	Win8	>5000万
	2014	第四代处理器 （Haswell架构）	2.8GHz-4.0GHz	32位/64位	14亿+	22纳米	2014	DDR4	284Pin	4G、8G、16	2133MHz-4200MHz			
	2015	第五代处理器（ Broadwell架构）	3.1GHz-3.6GHz	32位/64位	19亿	14纳米						2015	Win10	>1亿
	2016	第六代处理器 （Skylake架构）	2.8GHz-4.0GHz	32位/64位	N/A	14纳米								
	2017	第七代处理器（ Kaby Lake 、Skylake-X架构）	3.5GHz-4.2GHz	32位/64位	80亿+	14纳米								
	2018	第八代处理器 （CoffeeLake架构）	2.8GHz-4.0GHz	32位/64位	N/A	14纳米								

复杂为攻击攻击带来更多的机会



安天的工程师在这里只列举了恶意代码的加载机会，尚不包括主机系统的完整的可攻击点。

端点系统的复杂为攻击者带来了更多的机会，操作系统的代码不只必然带来更多的漏洞攻击点，由于系统一方面需要提供更多便利性，同时需要兼容原有的应用、协议等，因此同样带来了大量可以被非法利用“合法”入口。而安全需要在达成安全效果的同时，确保资产的可用性和可靠性

信息化建设是通过大量的充满了“不确定性”和“隐形质量”的复杂端点系统和连接关系组成的。对于规模化的信息系统来说，确保每个节点都绝对不失陷，显然是不可能的。

从习近平总书记4.19讲话到4.20讲话—工作要求在不断提升

419

树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，**全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力**

217

要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，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。**

420

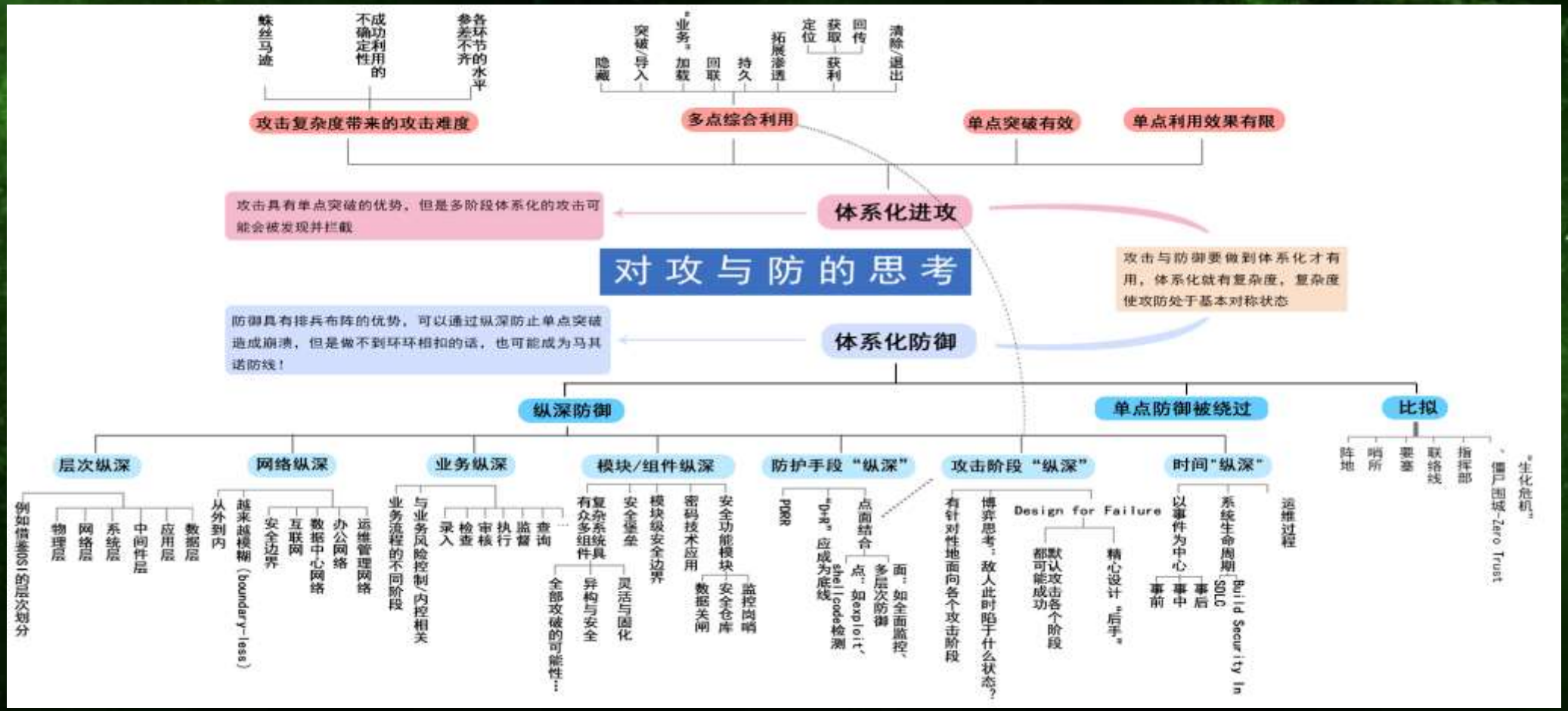
要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息系统统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，**做到关口前移，防患于未然。**

反对网络防御的虚无主义

- 习近平总书记指出：“**增强网络安全防御能力和威慑能力。网络安全的本质在对抗，对抗的本质在攻防两端能力较量。**”
- **防御提升对手攻击成本，制约对手能力展开，干扰对手攻击决策，削弱对手攻击效果。**
- **国产信息化产品**自主、先进、可控是网络强国的基础支撑，但其**和网络安全防护应是共同发展，相互促进关系。**将供应链自主视为网络安全工作前提的观点，不符合客观规律，导致了防御的虚无主义。
- 防御工作需要**直面当前全球信息技术供应链**这一基本情况展开。
- 鉴于超级大国强大的场景预制能力和攻击装备的场景覆盖能力，基础信息化产品的研发、生产过程需要有高度的网络安全防护保障，需要严格的遵循安全的规划、设计框架进行设计，严格执行代码安全的相关规范，**系统建立其安全保障机制，实现全生命周期的安全管理。**
- **网空攻击无核弹，防御无银弹。** 我们需要避免防御上的虚无主义，避免神化对手和庸俗化对手，避免寻找永动机和银弹。

以体系化防御对决体系化的进攻

- 需要以体系化防御对决体系化的进攻是一个最基本的认识，防御无银弹。



本图引自黄晟《关于网络纵深防御的思考》

从基础结构安全到超越威胁情报的叠加演进

基础结构安全
Architecture

纵深防御
Defense in Depth

态势感知与积极防御
SA & Active Defense

威胁情报
Intelligence

攻击与反制
Counter

在信息系统建成后，进行的外挂式防御已经不能满足需求，而是必须将网络规划为一个**可防御网络**，而可防御网络的前提是**可管理网络**。要实现一个可管理网网络，就必须在系统全生命周期遵从“三同步”原则，即在

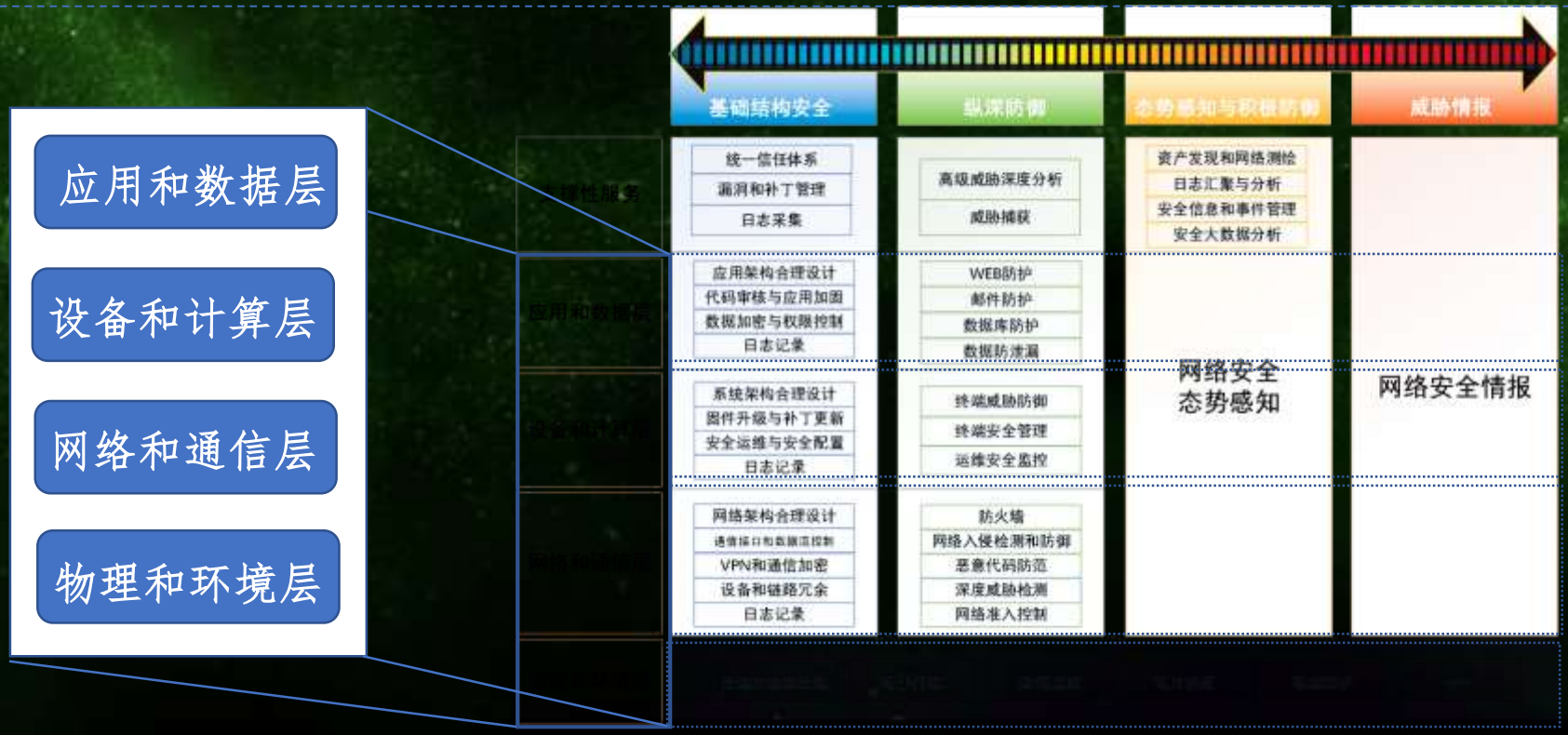
- 网络的规划设计阶段
- 建设实施阶段
- 运行维护阶段

都要考虑安全问题。

叠加演进是安天从能力型安全厂商的公共安全模型滑动标尺演绎发展的一套模型，滑动标尺模型由SANS提出，由安天翻译引入国内，并与国内能力型厂商约定为公共安全模型，参见：《网络安全滑动标尺模型—从架构安全到超越威胁情报的叠加演进》中文译本，安天公益翻译组翻译。

动态综合网络安全防御体系框架-结合面

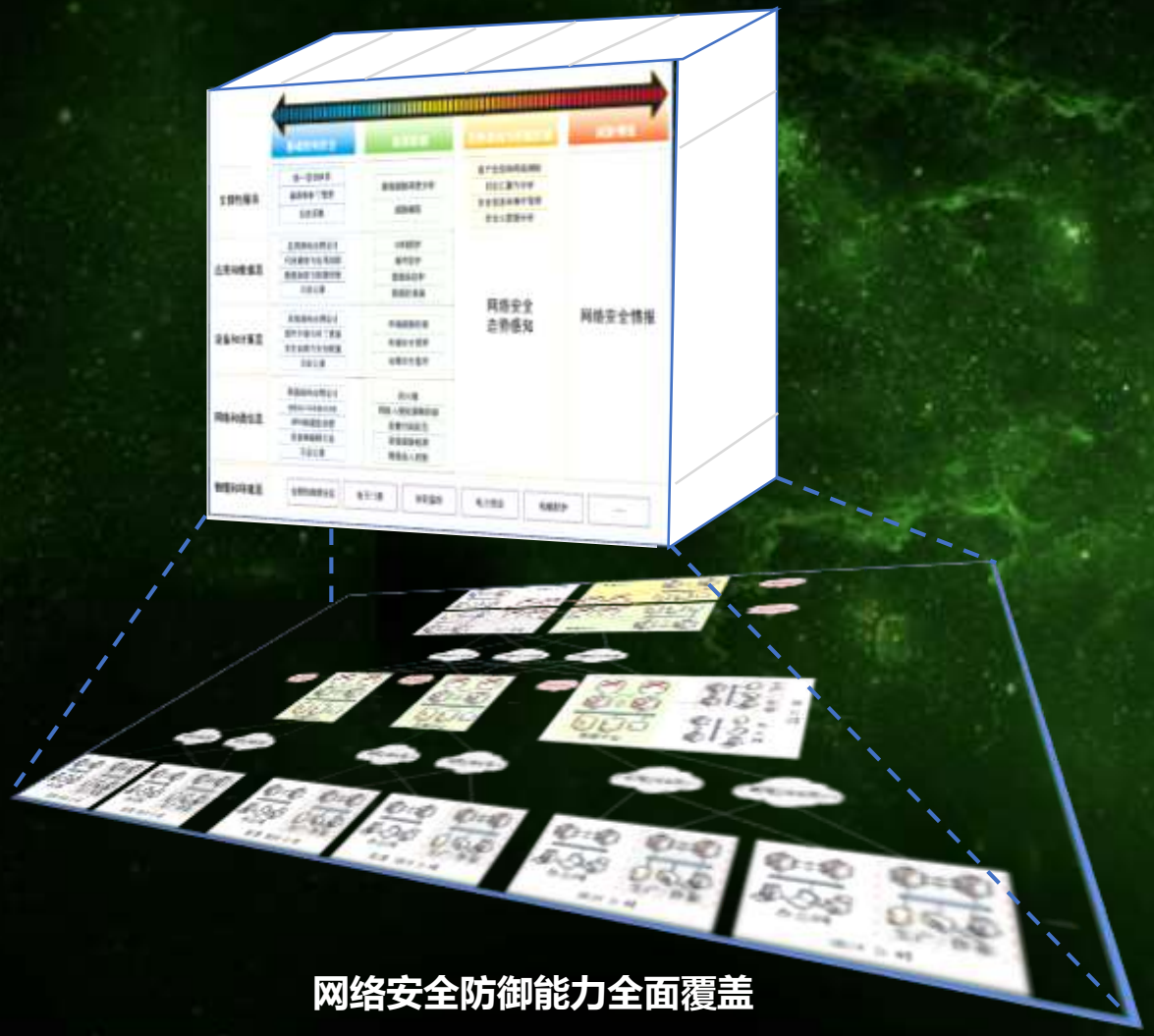
在规划以及后续项目方案设计的过程中，需要基于“面向失效的设计”原则，在构成信息系统的物理和环境、网络和通信、设备和计算、应用和数据等各个层面实现与网络安全防御能力的深度结合。



网络安全防御能力深度结合

动态综合网络安全防御体系框架-覆盖面

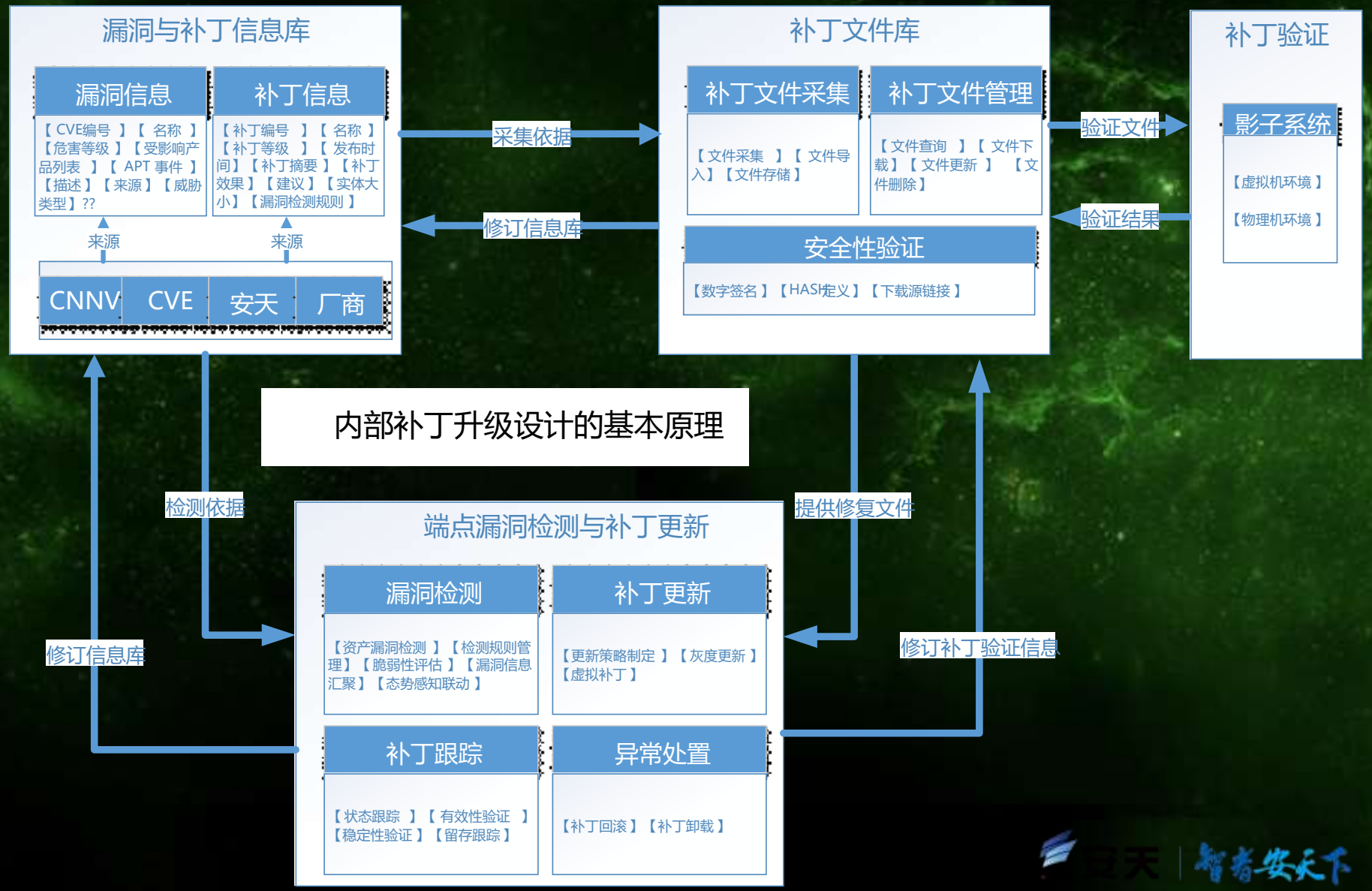
要将网络安全防御能力部署到信息基础设施和信息系统的“每一个角落”，力求**全面覆盖构成信息网络的各个组成实体**，包括桌面终端、服务器系统、通信链路、网络设备、安全设备乃至人员等等，**避免由于存在局部的安全盲区或者安全短板**，而导致整个网络安全防御体系的失效。



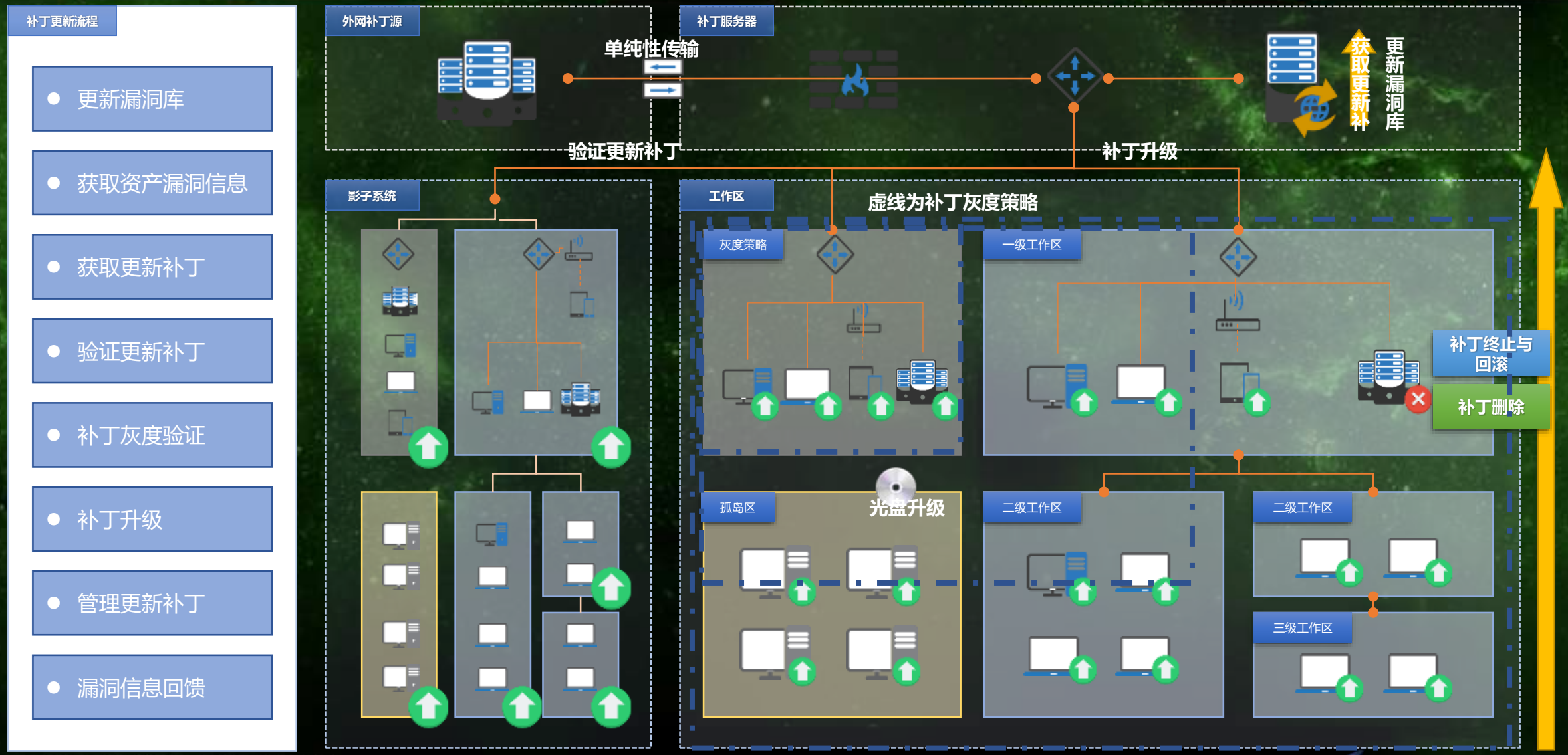
网络安全防御能力全面覆盖

复杂的基础工作：以补丁升级为例（1）

补丁升级不是所有节点连接到原厂自动下载升级。
其必须考虑到。
内部节点不能连接外网的情况。
大量内部节点不能通过用户交互打补丁的情况。
一些补丁在安装过程中必须操作交互的情况。
部分节点为了保证业务连续性、系统的稳定性不能打补丁、或不能打所有补丁的情况。
一些打补丁必须通过管理接口进行连接的情况。
……



复杂的基础工作：以补丁升级为例（续）



灰度策略：1%->10%->30%->10%%

复杂的基础工作：以系统加固（STIG标准）为例（1）

操作系统加固项共**15685**个，覆盖8大类系统，168个版本操作系统。

操作系统	类别及版本数量	版本详细情况	加固项
Windows	Windows 2003(2)	Windows 2003 Domain Controller Windows 2003 Member Server	286
	Windows 2008(2)	Windows 2008 Domain Controller Windows 2008 Member Server	457
	Windows Vista (1)	Windows Vista	251
	Windows XP (1)	Windows XP	147
	Windows 7 (1)	Windows 7	295
	Win2003、2008、7 审计(4)	Win2k3 Audit Win2k8 Audit Win2k8 R2 Audit Win7 Audit	839
	Windows 8/8.1(2)	Windows 8 Windows 8/8.1	773
	Windows 10 (1)	Windows 10 Windows Server 2008 R2 Domain Controller	280
	Windows Server 2008 R2(2)	Windows Server 2008 R2 Member Server	612
	Windows Server 2012 / 2012 R2(6)	Windows Server 2012 / 2012 R2 Domain Controller Windows Server 2012 / 2012 R2 Member Server Windows Server 2012 Domain Controller Windows Server 2012 Member Server Windows Server 2012/2012 R2 Domain Controller Windows Server 2012/2012 R2 Member Server	2212
	Windows Server 2016(1)	Windows Server 2016	275
Linux	SUSE(1)	SUSE Linux Enterprise Server v11 for System z	550
	Red Hat Enterprise Linux(3)	Red Hat Enterprise Linux 5/6/7	1070
SOLARIS	SOLARIS(6)	SOLARIS 10 SPARC SECURITY TECHNICAL IMPLEMENTATION GUIDE…	2451
AIX	AIX(3)	AIX 5.3 SECURITY TECHNICAL IMPLEMENTATION GUIDE…	1602
Mac OS X	Apple OS X(7)	Apple OS X 10.10 (Yosemite) Workstation …	1154
z/OS	z/OS(88)	z/OS ACF2 …	1132
移动	Android 2.2(1)	Android 2.2 (Dell) …	50
	Apple iOS(10)	Apple iOS 11 …	453
	Windows Phone(1)	Windows Phone 6.5 (with Good Mobility Suite)	9
	BlackBerry(23)	BlackBerry 10 OS	700
设备	Cisco 网际操作系统(2)	Cisco IOS XE Release 3 NDM	87

应用和服务加固项主要有**4245**个，主要覆盖5大类应用和服务。

厂商	类别和版本数量	版本详细情况	加固项
Microsoft	Windows DNS(1)	Windows DNS	29
	Windows Defender Antivirus(1)	Windows Defender Antivirus	38
	Windows Firewall(1)	Windows Firewall with Advanced Security	21
	Windows PAW (1)	Windows Firewall with Advanced Security	24
	IIS(5)	IIS 7.0 WEB SERVER IIS 7.0 WEB SITE IIS 8.5 Server IIS 8.5 Site IIS6 Server	24
	Microsoft Dot Net Framework(1)	Microsoft Dot Net Framework 4.0	15
	Microsoft IE(5)	Internet Explorer 6/7/8/9/10	98
	Microsoft Outlook(5)	Microsoft Outlook 2003/2007/2010/2013/2016	9
	Microsoft PowerPoint(5)	Microsoft PowerPoint 2003/2007/2010/2013/2016	6
	Microsoft Visio(2)	Microsoft Visio 2013/2016	13
	Microsoft Word(5)	Microsoft Word 2003/2007/2010/2013/2016	6
	Microsoft Excel(5)	Microsoft Excel 2003/2007/2010/2013/2016	6
	Microsoft SQL Server(8)	MS SQL Server 2014 Database …	42
	Microsoft Exchange(13)	Microsoft Exchange 2010 Client Access Server Role …	33
	Microsoft Access(5)	Microsoft Access 2003/2007/2010/2013/2016	6
	Microsoft Groove(1)	Microsoft Groove 2013	10
	Microsoft InfoPath(4)	Microsoft InfoPath 2003/2007/2010/2013	5
	Microsoft Lync(1)	Microsoft Lync 2013	3
	Microsoft Office System(4)	Microsoft Office System 2007/2010/2013/2016	35
	Microsoft OneDrive(1)	Microsoft OneDrive for Business 2016	13
	Microsoft OneNote(3)	Microsoft OneNote 2010/2013/2016	11
	Microsoft Skype(1)	Microsoft Skype for Business 2016	3
	Microsoft Publisher(3)	Microsoft Publisher 2010/2013/2016	16
	Microsoft Project(3)	Microsoft Project 2010/2013/2016	12
Java	Java Runtime Environment (JRE)(15)	Java Runtime Environment (JRE) 6 for Win7…	9
Google	Google Chrome(6)	Google Chrome Browser …	33
APACHE	APACHE(10)	APACHE 2.2 SERVER for Windows …	56
Adobe	Adobe Acrobat(3)	Adobe Acrobat Pro XI …	26

复杂的基础工作：以系统加固为例（2）

配置要求	相关属性	启用后系统和应用获得的安全增益	对系统和应用稳定性或可用性的影响
必须禁用Windows安装程序总是安装具有提升权限性质的程序。	版本：WINCC-000001 规则ID：SV-46220r1_rule 重要程度：高	标准用户帐号不被授予特权。安装应用程序时如果不禁用Windows特权可以允许恶意人员和应用程序获得系统的全部控制权。	禁用默认以高特权进行安装策略时，在安装一些应用服务时，可能会出现安装失败或者安装完成时一些服务无法启动的情况。
禁止关闭资源管理器的数据执行保护->对所有程序应用数据执行保护（DEP） 。	版本：5.285 规则ID：SV-32465r1_rule 重要程度：中	防止一些恶意程序通过溢出等手段对系统进行攻击，当出现缓冲区溢出的时候，DEP将被自动激活并对系统起保护作用。	导致一些没有通过DEP兼容性测试的正常软件无法执行，尤其是一些用户自研的业务系统（应用范围窄，测试不充分）。
提升LAN管理器身份验证级别，仅发送NTLMv2响应。	版本：3.031 规则ID：SV-32300r1_rule 重要程度：高	限定了协议来源，提升了系统安全性，该验证级别一共6级，包括LM、 NTLM和NTLMv2等组合。用户需要根据自己的系统情况选择对应级别。	贸然按照STIG给定的级别进行设置，会导致不支持 NTLMv2 身份验证的客户端设备无法在域中进行身份验证，并且无法使用 LM 和 NTLM 访问域资源。
必须对必要的服务持续维护记录，以确定系统是否具有额外的、不必要的服务，以SMB服务为例。	版本：WN12-GE-000021 规则ID：SV-52218r2_rule 重要程度：中	不必要的服务增加了系统的攻击面。关闭服务可以阻止入侵者获得系统许可，关闭SMB服务，可防范类似魔窟（WannaCry）这样的恶意代码通过永恒之蓝漏洞进行大面积传播。	关闭SMB服务会导致依赖共享服务以及远程打印服务的业务系统无法正常运行，例如无法使用企业文件存储、网络打印机等，造成用户日常工作的不便，。

总结

- 信息系统是复杂系统：1995年，钱学森院士指出“**信息网络加用户将构成一个开放的复杂巨系统。**”钱老当时并未说明“信息网络”是指整个的全球网络体系，还是单一信息网络。从目前的情况来看，对于达到一定规模的重要信息系统和关键信息基础设施来说，其都已经是一个复杂巨系统。将信息系统的复杂性作为网络安全防御工作必须深入研究和考虑前提，总体上是网络安全界的一个共性认知，但在一些具体的工作中我们往往缺少应有的严谨与敬畏。
- 网络空间敌情是高度严峻复杂的，认知敌情是复杂艰巨的工作。通过单点风险防控环节和产品堆砌方式形成的防护，无法应对敌情，导致无效投入。在大国博弈和地缘安全的背景下，细化、具象化每个重要信息系统和关键信息设施面临的敌情想定，是必须完成的工作；并应将有效应对“敌情想定”作为重要信息系统和关键基础设施的的能力要求。
- 网络安全防御工作是高度复杂的工作，也是需要由大量扎实演进的基础环节、基础能力支撑的工作，网络安全企业、网络安全工作者，需要融入到信息系统的规划、建设和运维中去，在可管理网络的基础上，建设可防御的网络，推动从基础结构安全、纵深防御、态势感知与主动防御到威胁情报的整体叠加演进。在网络安全体系建设实施的过程中，必须在投资预算和资源配备等方面予以充分保障，以确保将“关口前移”要求落到实处，在此基础上进一步建设实现有效的态势感知体系。

谢 谢

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）

谢 谢

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）