



以《网空威胁框架》 构建全流量监测

林榆坚
安赛CEO

议题简介

ABOUT: 安赛CEO 林榆坚

攻方: 参与多届攻防演练

防护: 参与G20峰会、金砖国家峰会、一带一路、十九大、全运会等活动防护

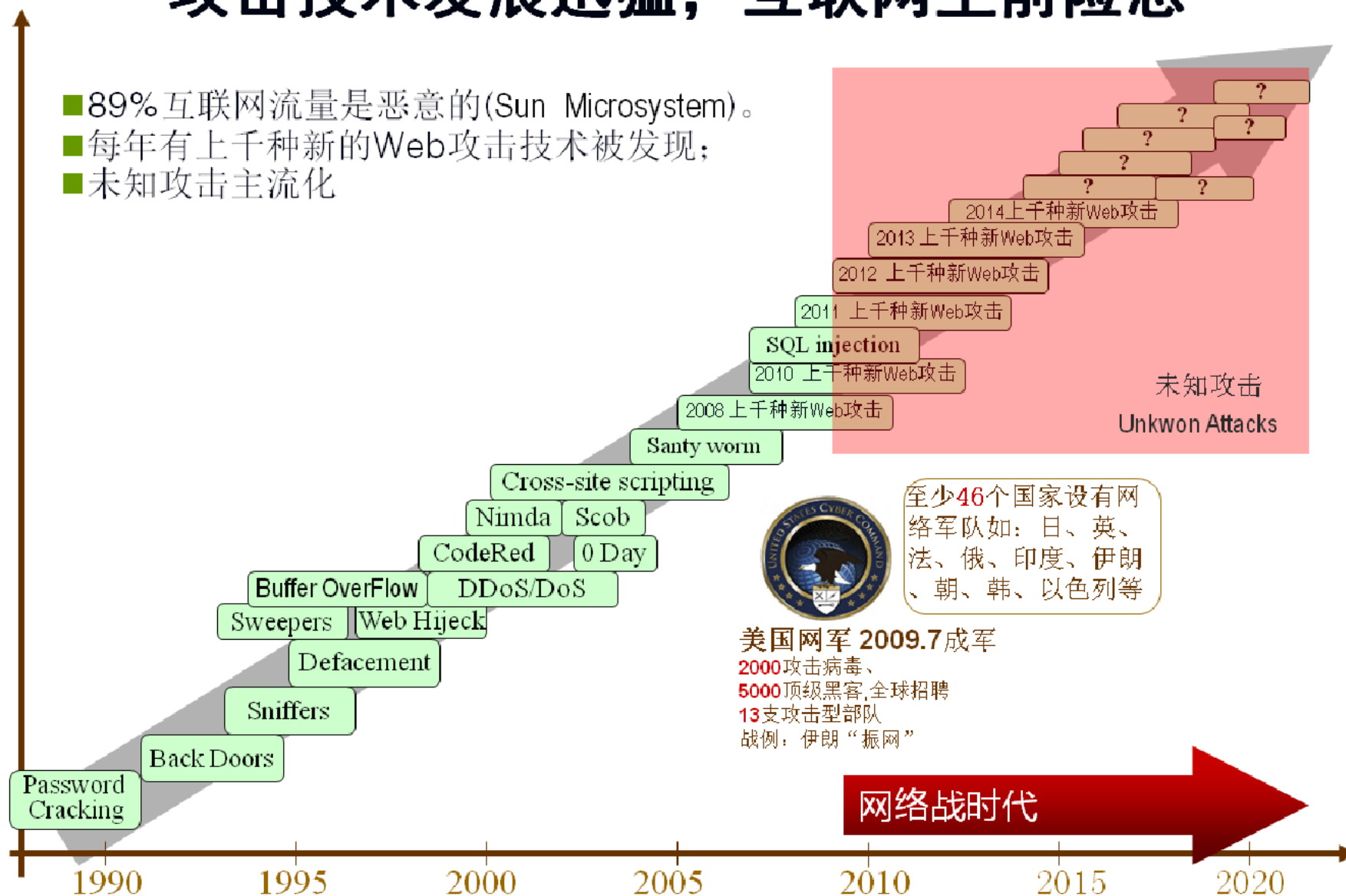
信息化 > 合规 > 攻防

选择系统化模型: 用三大模型, 细化事前、事中、事后的防护策略

纵深防御: 构造多层防线, 即时某一防线失效也能被其他防线弥补、纠正; 不同源

攻击技术发展迅猛，互联网空前险恶

- 89%互联网流量是恶意的(Sun Microsystem)。
- 每年有上千种新的Web攻击技术被发现；
- 未知攻击主流化



业务越复杂：问题越多（银行[信用卡等]、学校）、WEB是主要突破口之一

通用防护手段失效：应用安全时代，企事业的业务千变万化，需要纵深防护

木桶理论的应对：识别攻击链的任何一个链条，就能实现发现、瓦解

防火墙&IDS：阻断设备&分析设备；作用于攻击链的不同位置；不同源

明处&暗处：没有开不了的锁，防护终究是被绕过[必有痕迹]。拔网线是好方法

防护永远落后与攻击：0DAY各不一样，却有共性特征

协议安全&应用安全：HTTPS保证协议安全，应用安全却成了盲点（可视）

成本对抗：封锁IP仍然是有效模式（任务多，挑简单的）

目录

三大模型：对事前、事中、事后的细化

1

攻击者视角：杀伤链模型KILL CHAIN

2

防护视角：ATT&CK模型（ACK模型）

3

管理视角：NSA/CSS网空威胁框架

4

系统化的应对方案

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

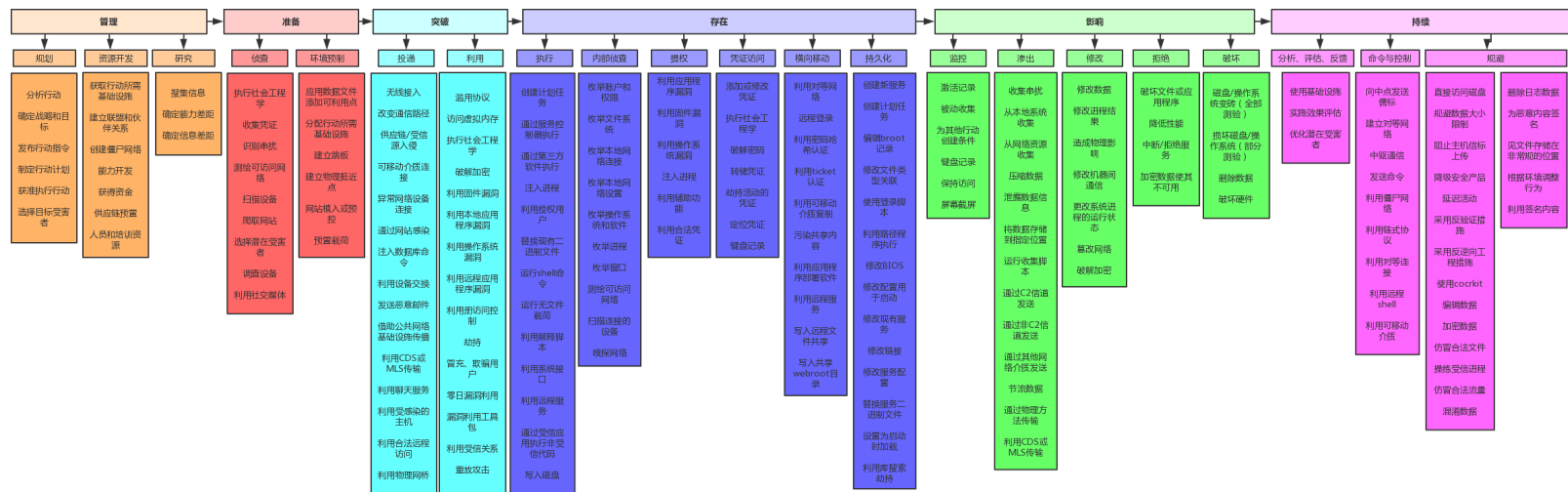
ATT&CK (ACK) 模型:12个阶段, 240多种攻击方式

目标达成

在攻陷系统后，攻击者具有像直接操作目标主机的高级权限，进一步执行和达成攻击者最终的目标。

[illegible]

网空模型： 6个阶段， 21个目标， 188多种攻击方式



目录

三大模型：对事前、事中、事后的细化

1

攻击者视角：杀伤链模型KILL CHAIN

2

防护视角：ATT&CK模型（ACK模型）

3

管理视角：NSA/CSS网空威胁框架

4

系统化的应对方案

网络杀伤链 Kill Chain



阶段	检测	拒绝	中断	降级	欺骗	毁坏/反制
侦查跟踪	WebIDS/NIDS	WAF/NIPS/旁路阻断/ACL				
武器构建	WebIDS/NIDS	WAF/NIPS/旁路阻断/ACL				
载荷投递	WebIDS/NIDS	WAF/NIPS/旁路阻断/ACL	In-line AV			
漏洞利用	WebIDS/NIDS	WAF/NIPS/旁路阻断	DEP			
安装植入	WebIDS/NIDS/HIDS	WAF/NIPS/旁路阻断/ACL	AV			
命令与控制	WebIDS/NIDS/HIDS	Firewall/旁路阻断/ACL	Firewall ACL		DNS	
目标达成	WebIDS/NIDS/HIDS/审计				蜜罐	

目录

三大模型：对事前、事中、事后的细化

1

攻击者视角：杀伤链模型KILL CHAIN

2

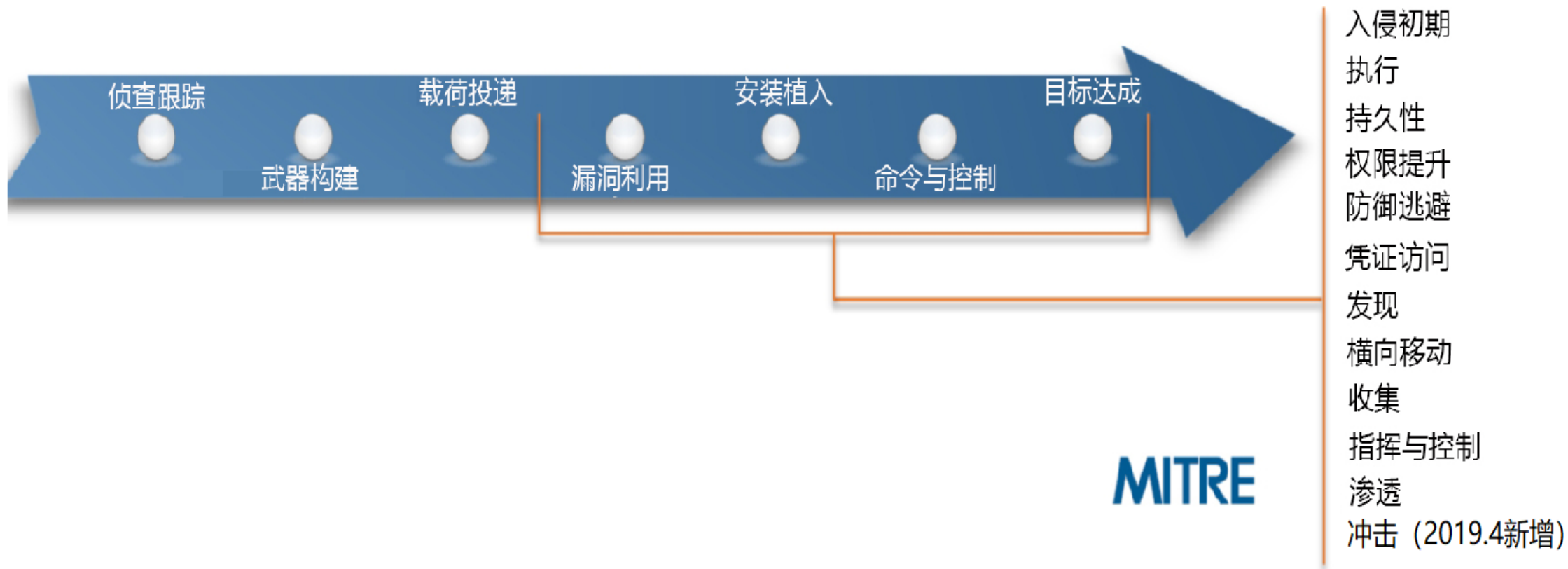
防护视角：ATT&CK模型（ACK模型）

3

管理视角：NSA/CSS网空威胁框架

4

系统化的应对方案



ATT&CK (ACK模型：ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE) 即对抗战术、技术和通用知识库。是一个反映各个攻击生命周期的模型和知识库。ATT&CK的12个战术类别是对杀伤链后C2阶段后的细化，对攻击者获取权限后的行为提供了更精细的粒度描述。

ATT&CK框架 (ACK模型)

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

MITRE提出的ATT&CK框架，是将入侵期间可能发生的情况，做出更细的画分，区隔出12个策略阶段。包括：入侵初期、执行、潜伏、权限提升、防御逃避、凭证访问、发现、横向移动、采集数据、指挥与控制、透出、冲击。截止2019年4月，ATT&CK 矩阵收集了244多种攻击者战术和技术。

入侵初期	执行				潜伏				权限提升				躲避防御				凭证访问		发现		横向移动		采集数据		命令控制		渗透		冲击		
Drive-by Compromise	AppleScript	LSASS驱动程序	签名二进制代理执行	.bash_profile/.bashrc	组件固件	内核模块及扩展	新服务	计划任务	有效账户	访问令牌操控	钩子	Setuid/Setgid	访问令牌操作	控制面板项目	文件系统逻辑编辑	间接命令执行	Plist修改	签名二进制文件代理执行	账户操控	Kerberoasting	账户发现	进程发现	AppleScript	SSH劫持	音频捕获	屏幕截图	常用端口	多跳代理	自动渗透	数据销毁	服务停止
利用面向公众的应用程序	CMSTP利用	Launchctl	签名脚本代理执行	辅助功能	组件对象模型劫持	LC_LOAD_DYLIB 插入命令	Office应用程序启动	屏幕保护	Web Shell	辅助功能	图像文件执行选项注	启动项	BITS Jobs	DCShadow	gatekeeper 防御绕过	安装根证书	端口探测	脚本签名代理执行	Bash历史	keychain	应用窗口发现	查询注册表	应用部署软件	共享 Webroot	自动收集	视频截取	通过可移动媒体进行	多跳通信	数据压缩	针对破坏的数据加密	存储数据操作
外部远程服务	命令行界面	本地任务调度	源文件	账户操控	创建账号	LSASS驱动程序	路径拦截	安全支持提供商	WMI事件订阅	AppCert DLL	启动守护进程	sudo 缓冲	添加二进制数据	DLL搜索顺序劫持	修改组策略	InstallUtil	Process Doppelganging	软件打包	暴力破解	LLMNR/NBT-NS拦截及中间攻击	浏览器书签发现	远程系统发现	分布式组件对象模型	污染共享内容	剪贴板数据	连接代理	多层加密	数据加密	数据损坏	传输数据操作	
增加硬件	编译的HTML文件	MSHTA	文件名后面的空格	AppCert DLL	DLL搜索顺序劫持	Plist修改	服务注册表权限弱点	Winlogon Helper DLL	Applnit DLL	新服务	sudo	绕过用户账户控制	DLL文件侧载漏洞	HISTCONTROL	LC_MAIN劫持	进程挖空	文件名后面的空格	凭证转储	网络嗅探	可信域发现	安全软件发现	远程服务的利用	第三方软件	数据分段	自定义命令及控制协	端口开启	数据传输大小限制	磁盘内容擦除			
通过可移动媒体进行钓鱼附件	控制面板项目	powershell	第三方软件	Applnit DLL	Dylib劫持	启动守护进程	端口探测	Setuid/Setgid	Application	路径拦截	有效账户	CMSTP	反混淆/解密文件或禁用安全工具	隐藏文件和目录	Launchctl	进程注入	模板注入	文件中的凭证注册表中的凭证	密码过滤DLL	文件和目录发现	系统信息发现	登录脚本	Windows管理	信息库中的数	自定义加密协	远程访问工具	对替代协议渗透	磁盘结构擦除			
通过API执行命令	动态数据交换	Regsvcs/Regasm	陷阱	Application Shimming	外部远程服务	Launchctl	端口监测	快速方式修改	绕过用户账户控制	Plist修改	WebShell	清除命令历史	隐藏窗口	修改注册表	Regsvcs/Regasm	值得信赖的开发者工具	对证书访问的强制认证	安全存储	网络共享发现	系统网络配置发现	Pass the Ticket	网络共享中的数	数据混淆	标准应用层协议	渗透到物理介质的渗透	阻止系统恢复					
通过服务进行鱼叉式网络钓鱼	通过模块加载执行命令	Rundll32	用户执行	BITS Jobs	隐藏文件和目录	登录项目	重新打开应用程序	系统固件	Dylib劫持	进程注入	传输后编译	额外的窗口内存注入	指示器阻塞	NTFS文件属性	Rootkit	虚拟化/沙箱逃避	钩子	密码策略发现	系统服务发现	远程桌面协议	网络嗅探	系统所有者/用户发现	远程文件复制	电子邮件收集	域前捕获	标准非应用层协议	计划传输	网络拒绝服务			
供应链妥协	利用客户端执行命令	计划任务	Windows Management Instrumentation	bootkit	钩子	登录脚本	冗余访问	系统服务	开发权限提升	SID-历史注入	编译HTML文件	额外的窗口内存注入	指示器阻塞	NTFS文件属性	Rootkit	虚拟化/沙箱逃避	钩子	密码策略发现	系统服务发现	远程文件复制	电子邮件收集	域生成算法	标准非应用层协议	计划传输	网络拒绝服务						
可信关系	图形用户界面	脚本	Windows远程管理	浏览器扩展	管理程序	修改现有服务	注册表运行键/启动项	时间提供者	额外的窗口内存注入	计划任务	修改系统固件	文件删除	移除工具中的指示器	删除网络共享连接	SIP和信任提供商劫持	网络服务	输入捕获	外围设备发现	系统时间发现	远程服务	输入捕获	备用信道	不常用的端口	资源劫持							
有效账户	安装实用工具	服务执行	XSL脚本处理	更改默认文件关联	图像文件执行选项注入	Netsh Helper DLL	SIP和信任供应商劫持	陷阱	文件系统权限弱点	服务注册表权限弱点	组件对象模型 (COM)	文件权限修改	移除主机上的指标器	混淆的文件或信息	脚本	输入提示	权限组发现	虚拟化/沙箱逃避	通过可移动媒体进行复制	Man in the Browser	多个通信通道	网络服务	实时数据操作								

86种APT示例: [HTTPS://ATTACK.MITRE.ORG/GROUPS/](https://attack.mitre.org/groups/)

入侵初期	执行	持久性	权限提升	防御逃避	凭证访问	发现	横向移动	收集	渗透	指挥与控	冲击
10项	33项	58项	28项	63项	19项	20项	17项	13项	9项	21项	数据销毁
驾车妥协	AppleScript的	_bash_profile 和 bashrc	访问令牌操作	访问令牌操作	账户操纵	账户发现	AppleScript的	音频捕获	自动渗透	常用端口	针对破坏的数据加密
利用面向公众的应用程序	命令行界面	辅助功能	辅助功能	二进制填充	Bash历史	应用窗口发现	分布式组件对象模型	自动收集	数据压缩	通过可移动媒体进行通信	数据污损
硬件增加	编译的HTML文件	账户操纵	AppCert DLL	BITS乔布斯	蛮力	浏览器书签发现	登陆脚本	剪贴板数据	数据加密	连接代理	磁盘内容擦除
通过可移动媒体进行复制	控制面板项目	AppCert DLL	Applnit DLL	绕过用户账户控制	凭证倾销	文件和目录发现	传递哈希	来自本地系统的数据	数据传输大小限制	自定义命令和控制	磁盘结构擦除
Spearphishing 附件	动态数据交换	Applnit DLL	应用匀场	清除命令历史	文件中的凭证	网络服务扫描	通过机票	网络共享驱动器中的数据	对替代议定书的渗透	数据编码	端点拒绝服务
通过服务进行鱼叉式网络钓鱼	通过API执行	应用匀场	绕过用户账户控制	CMSTP	挂钩	网络共享发现	远程桌面协议	来自可移动媒体的数据	通过命令和控制通道进行渗透	数据混淆	固件损毁
供应链妥协	图形用户界面	认证包	DLL搜索顺序劫持	代码签名	输入捕获	网络嗅探	远程文件复制	数据分阶段	渗透到其他网络介	域前端	阻止系统恢复

APT33是一个可疑的伊朗威胁组织，自2013年以来一直在开展攻击。该组织针对美国，沙特阿拉伯和韩国多个行业的组织，特别关注航空和能源领域。

入侵初期	执行	潜伏	权限提升	躲避防御		凭证访问		发现	横向移动	采集数据	命令控制		渗透	冲击
Drive-by Compromise	AppleScript	新服务	访问令牌操控	控制面板项目	间接命令执行	账户操控	Kerberoasting	账户发现	AppleScript	音频捕获	常用端口	多跳代理	自动渗透	数据销毁
利用面向公众的应用程序	CMSTP利用	Office应用程序启动	辅助功能	DCShadow	安装根证书	Bash历史	keychain	应用窗口发现	应用部署软件	自动收集	通过可移动媒体进行通信	多频带通信	数据压缩	针对破坏的数据加密
外部远程服务	利用客户端执行命令	注册表运行键/启动文件夹	AppCert DLL	DLL搜索顺序劫持	InstallUtil	暴力破解	LLMNR/NBT-NS拦截及中间攻击	浏览器书签发现	分布式组件对象模型	剪贴板数据	连接代理	多层加密	数据加密	数据污染
增加硬件	编译的HTML文件	Plist修改	Applnit DLL	DLL文件侧载漏洞	LC_MAIN劫持	凭证转储	网络嗅探	可信域发现	远程服务的利用	数据分段	自定义命令及控制协议	端口开启	数据传输大小限制	磁盘内容擦除
通过可移动媒体进行复制	powershell	端口探测	Application Shimming	反混淆/解码文件或信息	Launchctl	文件中的凭据	密码过滤DLL	文件和目录发现	登录脚本	信息库中的数据	自定义加密协议	远程访问工具	对替代协议渗透	磁盘结构擦除
钓鱼附件	动态数据交换	计划任务	绕过用户账户控制	禁用安全工具	伪装	注册表中的凭据	私匙	网络服务扫描	传递哈希	来自本地系统的数据	数据编码	远程文件复制	通过命令和控制通道进行渗透	端点拒绝服务
鱼叉式钓鱼链接	计划任务	Rc.common	DLL搜索顺序劫持	Execution Guardrails	修改注册表	对证书访问的利用	安全存储	网络共享发现	Pass the Ticket	网络共享中的数据	数据混淆	标准应用层协议	渗透到其他网络	固件损毁
通过服务进行鱼叉式网络钓鱼	通过模块加载执行命令	重新打开应用程序	Dylib劫持	防御软件漏洞	混淆的文件或信息	强制认证	双因素身份验证拦截	网络嗅探	远程桌面协议	来自可移动媒体的数据	域前端	标准密码协议	物理介质的渗透	阻止系统恢复
供应链妥协	用户执行	有效账户	开发权限提升	额外的窗口内存注入	NTFS文件属性	钩子		密码策略发现	远程文件复制	电子邮件收集	域生成算法	标准非应用层协议	计划传输	网络拒绝服务
可信关系	图形用户界面	安全支持提供商	额外的窗口内存注入	文件删除	删除网络共享连接	输入捕获		外围设备发现	远程服务	输入捕获	备用信道	不常用的端口		资源劫持
有效账户	安装实用工具	SIP和信任供应商劫持	有效账户	文件权限修改	有效账户	输入提示		权限组发现	通过可移动媒体进行复制	Man in the Browser	多个通信通道	网络服务		实时数据操作

APT28：在2018年7月美国司法部起诉后归因于俄罗斯总参谋部的俄罗斯主要情报局。据报道，该组织在2016年破坏了希拉里克林顿竞选活动，民主党全国委员会和民主党国会竞选委员会，试图干涉美国总统大选。 APT28自2007年1月以来一直活跃。

入侵初期	执行		潜伏	权限提升			凭证访问	发现	横向移动	采集数据	命令控制	渗透	冲击
Drive-by Compromise	AppleScript	LSASS驱动程序	.bash_profile/.bashrc	访问令牌操控	Setuid/Setgid	文件系统逻辑偏移	账户操控	账户发现	AppleScript	音频捕获	常用端口	自动渗透	数据销毁
利用面向公众的应用程序	CMSTP利用	Launchctl	辅助功能	辅助功能	模板注入	Rootkit	Bash历史	应用窗口发现	应用部署软件	自动收集	通过可移动媒体进行通信	数据压缩	针对破坏的数据加密
外部远程服务	命令行界面	本地任务调度	账户操控	AppCert DLL	sudo缓冲	修改组策略	暴力破解	浏览器书签发现	分布式组件对象模型	剪贴板数据	连接代理	数据加密	数据污损
增加硬件	编译的HTML文件	MSHTA	Office应用程序启动	Applnit DLL	sudo	HISTCONTROL	凭证转储	可信域发现	远程服务的利用	数据分段	自定义命令及控制协议	数据传输大小限制	磁盘内容擦除
通过可移动媒体进行复制	控制面板项目	powershell	Applnit DLL	反混淆/解码文件或信息	有效账户	隐藏文件和目录	文件中的凭据	文件和目录发现	登录脚本	信息库中的数据	自定义加密协议	对替代协议渗透	磁盘结构擦除
钓鱼附件	动态数据交换	Regsvcs/Regasm	Application Shimming	绕过用户账户控制	WebShell	隐藏用户	注册表中的凭据	网络服务扫描	传递哈希	来自本地系统的数据	数据编码	通过命令和控制通道进行渗透	端点拒绝服务
鱼叉式钓鱼链接	通过API执行命令	REGSVR32	认证包	防御软件漏洞	值得信赖的开发者工具	移除主机上的指标器	对证书访问的利用	网络共享发现	Pass the Ticket	网络共享中的数据	数据混淆	渗透到其他网络	固件损毁
通过服务进行鱼叉式网络钓鱼	通过模块加载执行命令	Rundll32	BITS Jobs	Dylib劫持	时间戳修改	图像文件执行选项注入	网络嗅探	网络嗅探	远程桌面协议	来自可移动媒体的数据	域前端	物理介质的渗透	阻止系统恢复
供应链妥协	利用客户端执行命令	计划任务	bootkit	开发权限提升	网络服务	混淆的文件或信息	钩子	密码策略发现	远程文件复制	电子邮件收集	标准应用层协议	计划传输	网络拒绝服务
可信关系	图形用户界面	脚本	浏览器扩展	额外的窗口内存注入	有效账户	移除工具中的指示器	输入捕获	外围设备发现	远程服务	输入捕获	备用信道		资源劫持
有效账户	安装实用工具	用户执行	有效账户	文件删除	虚拟化/沙箱逃避	移除主机上的指标器	输入提示	进程发现	通过可移动媒体进行复制	屏幕截图	多个通信通道		实时数据操作

目录

三大模型：对事前、事中、事后的细化

1

攻击者视角：杀伤链模型KILL CHAIN

2

防护视角：ATT&CK模型（ACK模型）

3

管理视角：NSA/CSS网空威胁框架

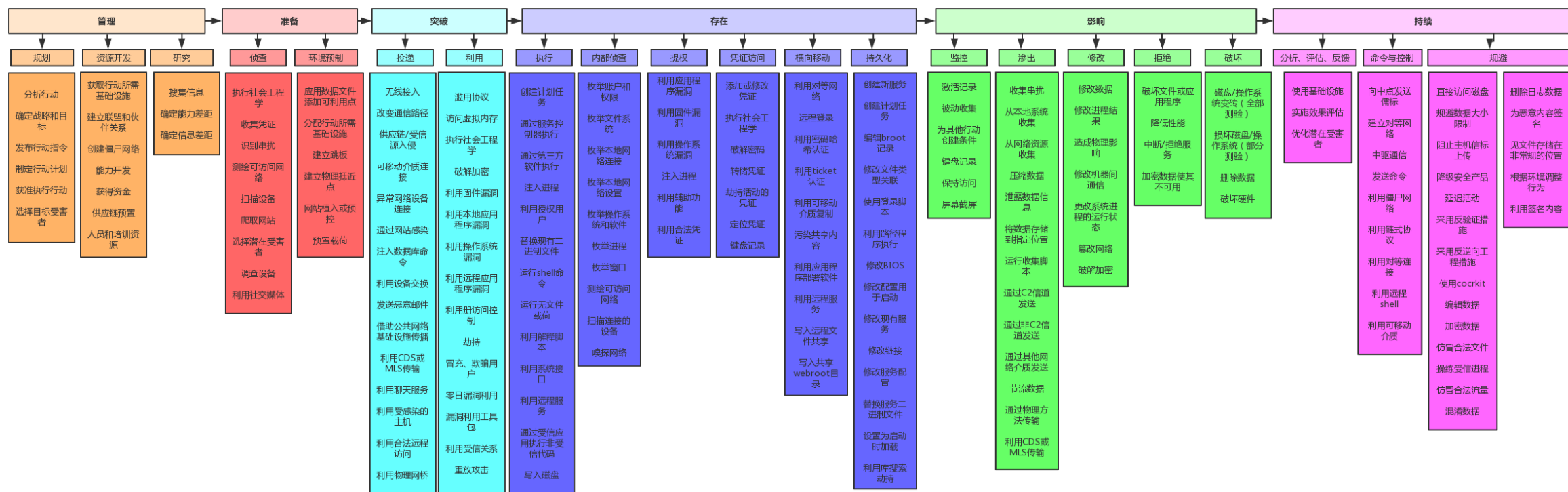
4

系统化的应对方案

ANSA/CSS技术网空威胁框架：2018年发布

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

《NSA/CSS技术网空威胁框架》共包含6个阶段（STAGE）、21个目标（OBJECTIVE）、188种行为（ACTION）和若干个关键词（KEY PHRASES）



目录

三大模型：对事前、事中、事后的细化

1

攻击者视角：杀伤链模型KILL CHAIN

2

防护视角：ATT&CK模型（ACK模型）

3

管理视角：NSA/CSS网空威胁框架

4

系统化的应对方案

- (1) 排查安全隐患
- (2) 被攻击
- (3) 已受控

清除危害、加固



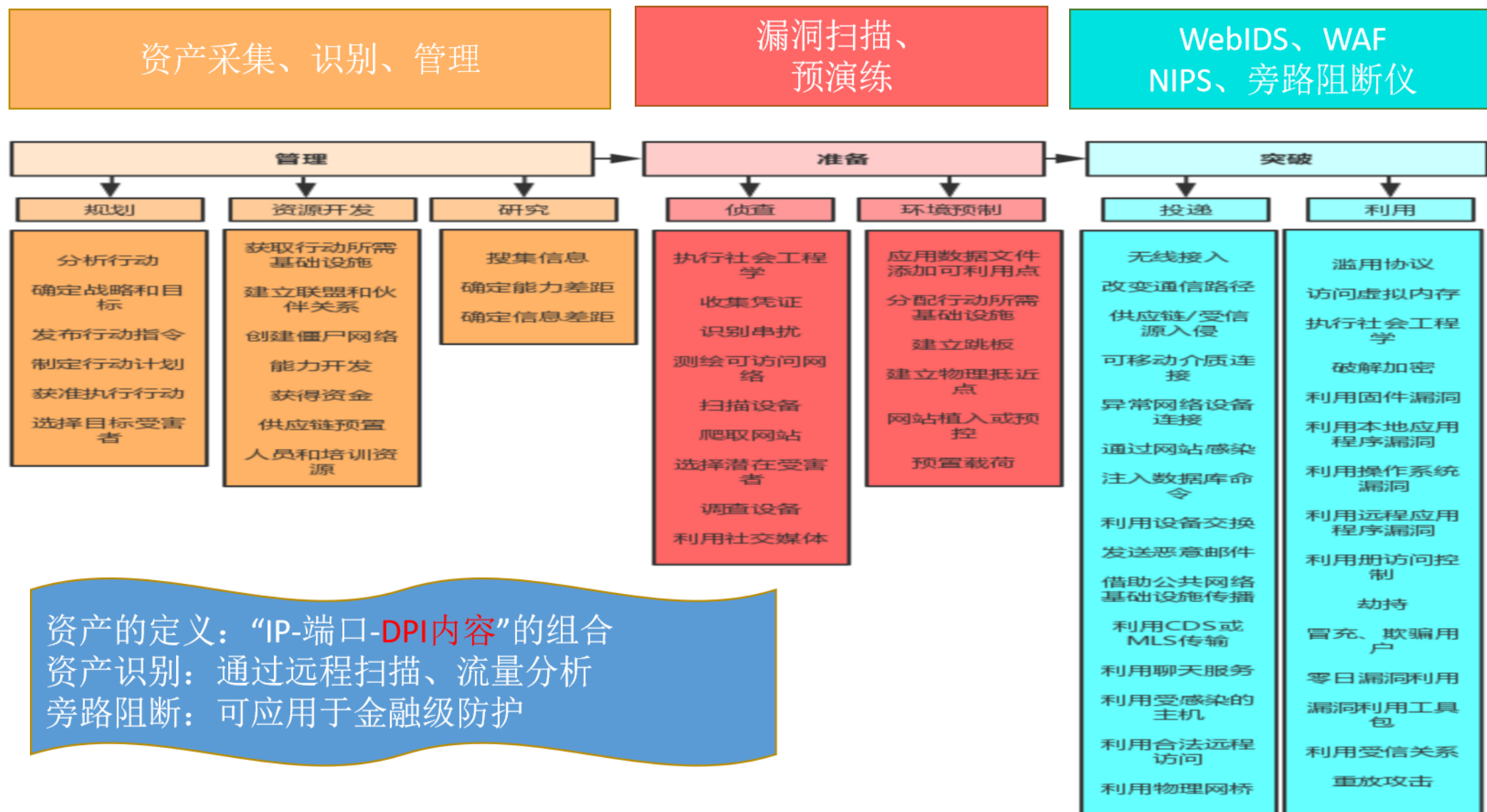
通过数据发掘、防泄漏、应用控制、攻击追踪等技术，防止信息资产被非法访问或外泄

利用线索，回溯分析场景、全局关联分析，评估影响范围

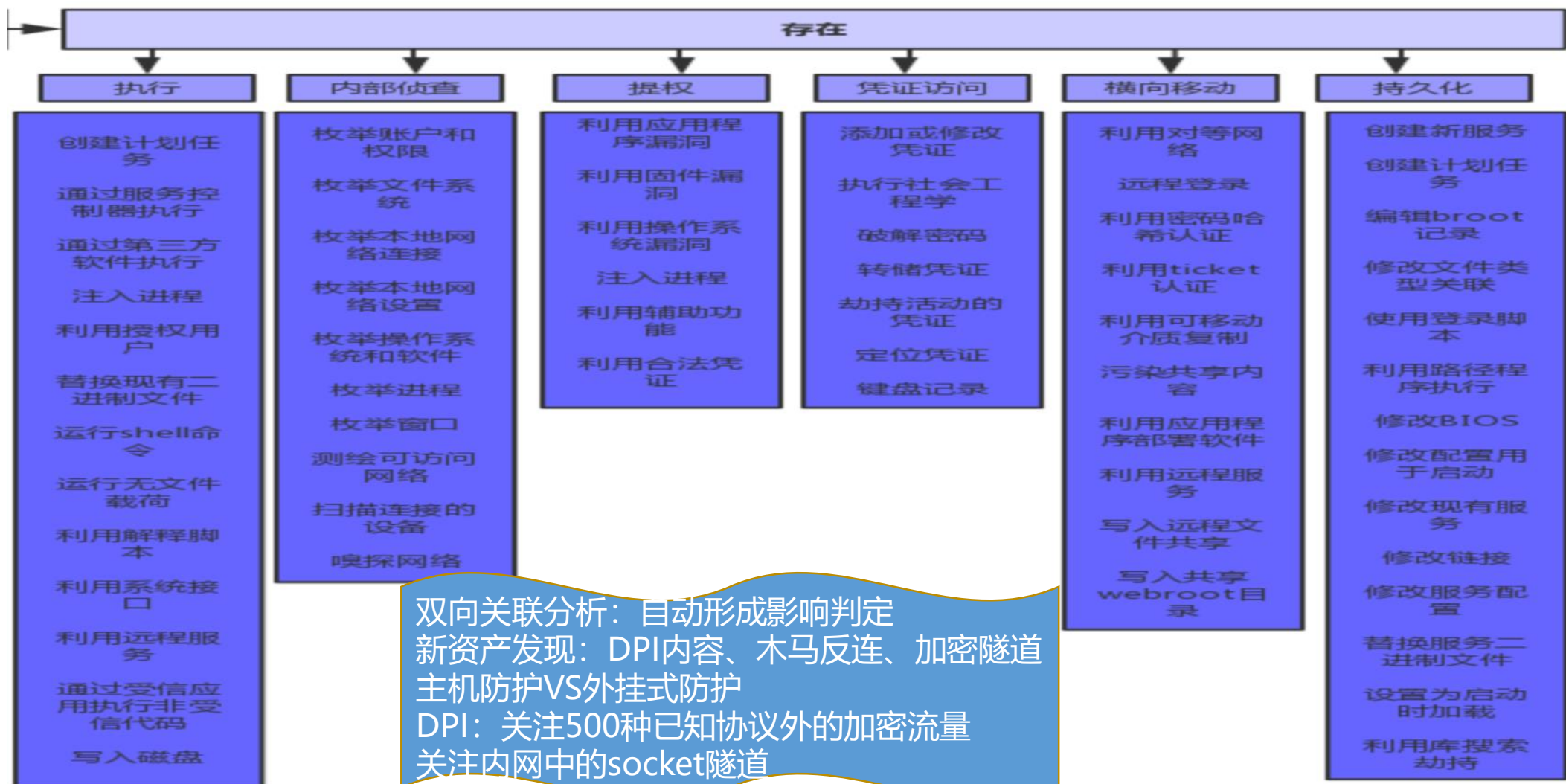
《网空威胁框架》全周期应对

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

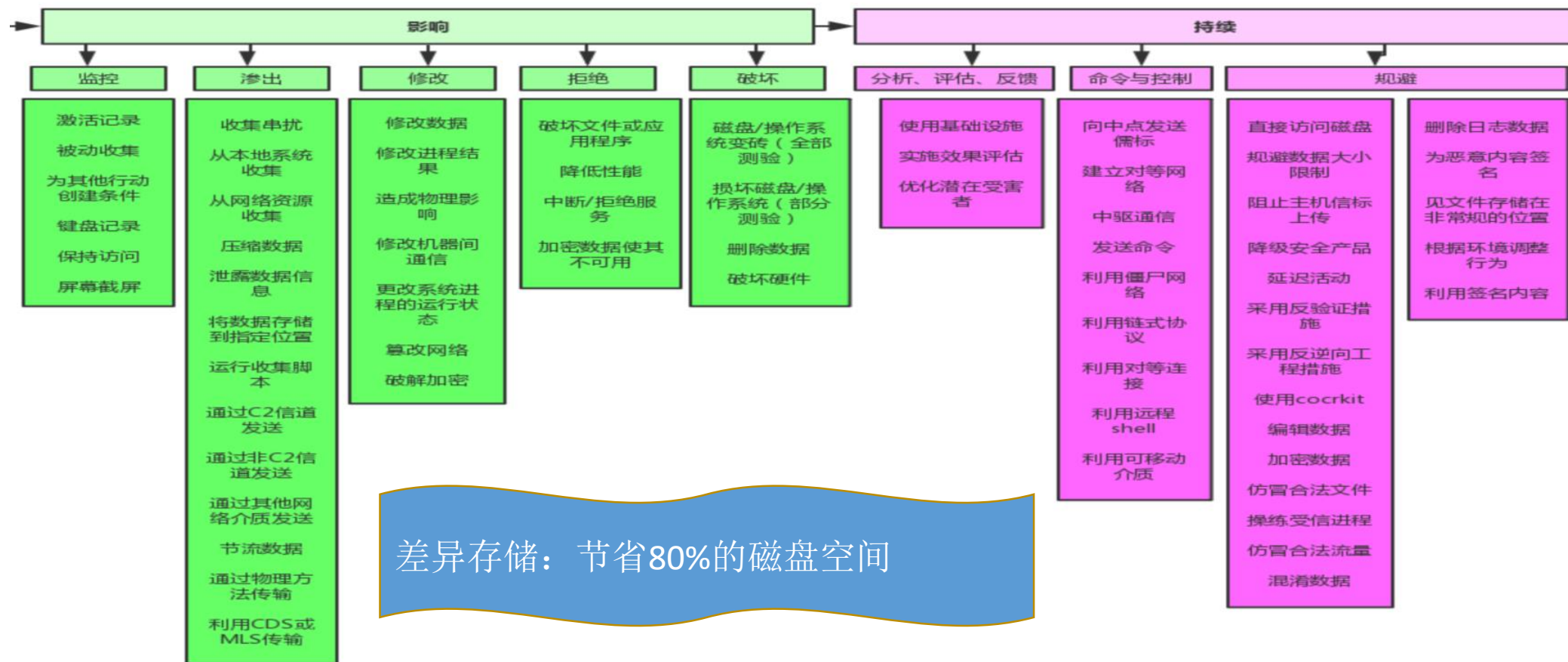


双向数据流关联监测、DNS监测、DPI检测、新资产发现、主机防护



日志审计、SOC关联分析

全流量差异存储、追踪溯源



通用防护手段失效：应用安全时代，企事业的业务千变万化，需要纵深防护

业务越复杂：系统简化

木桶理论的应对：识别攻击链的任何一个链条、快速响应，就能实现发现、瓦解


防火墙&IDS：阻断设备&分析设备；作用于攻击链的不同位置；不同源；暗处

防护永远落后与攻击：0DAY各不一样，却有共性特征、攻击溯源

协议安全&应用安全：HTTPS保证协议安全，应用安全却成了盲点（可视）

成本对抗：封锁IP仍然是有效模式（任务多，挑简单的）

预演练

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE