

# 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

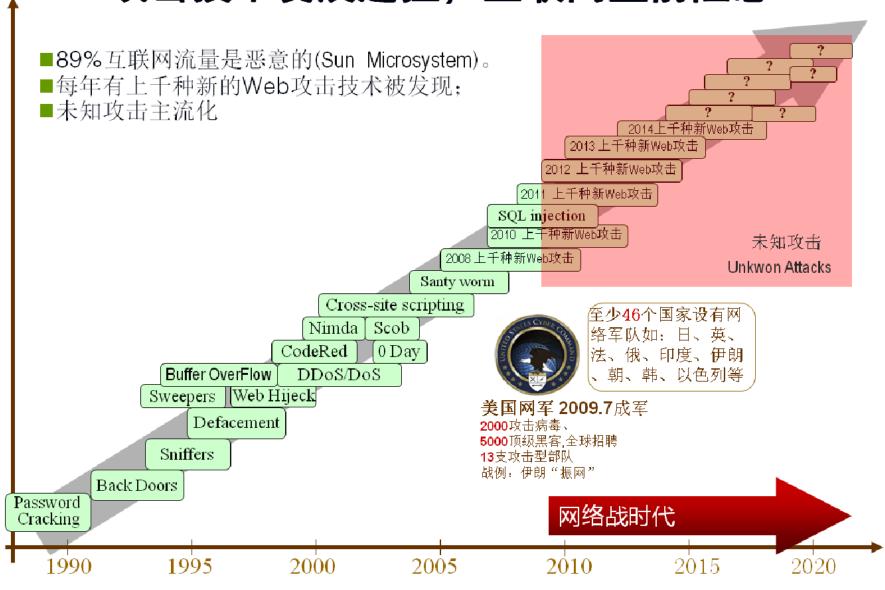
选择系统化模型:用三大模型,细化事前、事中、事后的

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



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)

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 BEIJING CYBER SECURITY CONFERENCE

### 杀伤链模型:7个阶段

### ATT&CK (ACK) 模型:12个阶段, 240多种攻击方式

### 网络杀伤链 Kill Chain



侦查跟踪

武器构建

载荷投递



漏洞利用



安装植入



命令与控制



目标达成

攻击者处在攻击行动的计划阶段,了解被攻击目标,搜寻目标的 弱点。

攻击者使用自动化工具将漏洞利用工具和后门制作成一个可发送 的武器载荷。

(例如Adobe PDF, Microsoft office文件)

攻击者将武器載荷向被攻击系统投递。 (例如直接向web服务器投递和通过电子邮件、USB等间接渠道 投递)

攻击利用系统上的漏洞,以便进一步在目标系统上执行代码。

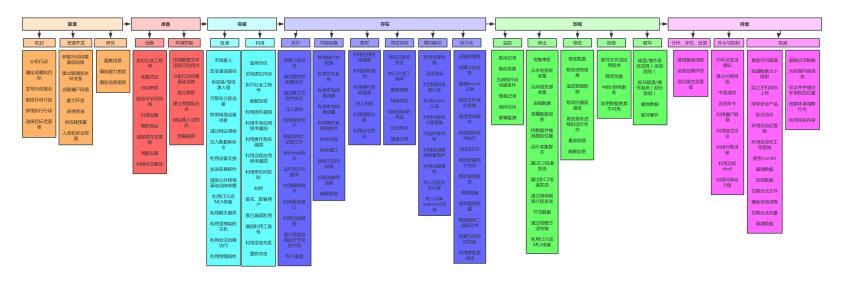
攻击者一般会在目标系统上安装恶意程序、后门 或者其他植入代码,以便获取对目标系统的长期访问途径。

恶意程序开启一个可供攻击者远程操作的命令通道。

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。

	初期		执行				港位					权限提升				解遊					无证访问		现	横向移		采集			控制	渗透	冲	±;
Drive	-by	AppleScript			.bash_profi	组件固件	内核模块及扩	新服务	计划任务	有效账户	访问令牌	钩子	Setuid	访问令牌	控制面板		间接命令	Plist修改		账户操	Kerberoasting	账户发现	进程发	AppleScript	SSH助	音频捕	屏幕截	常用端	多跳代	自动渗	数据销毁	服务停
Comp	promis		程序	制代理执 行	le/.bashrc		展				操控		/Setqi d		项目	損偏移	执行		文件代理执 行	控			现		持	鉄	<b>2</b>		理	透		1E
利用	面向公	CMSTP利用	Launchetl	签名脚本	辅助功能	组件对象	LC_LOAD_D	Office 5	屏幕保护	Web	辅助功能	图像文	启动项	BITS Jobs	DCShado	gatekeeper	安装根证	端口探测	脚本签名代	Bash历	keychain	应用窗口	查询注	应用部署软	共享	自动收	视频截	通过可	多類帯	数据压	针对破坏	存储数
众的	立用程			代理执行		模型动持	YLIB 插入命	用程序		Shell		件执行			w	防御绕过	书		理执行	史		发现	册表	件	Webro	集	取	移动媒	通信	缩	的数据加	据操作
廖							4	启动				选项注													ot			体进行			審	
外部	元程服	命令行界面	本地任务调	源文件	账户操控	创建账号	LSASS驱动箱	路径拦	安全支持	WMI事件	AppCert	启动守	sudo	添加二进	DLL搜索顺	修改组策略	InstallUtil	Process	软件打包	暴力破	LLMNR/NBT-	浏览器书	远程系	分布式组件	污染共	剪贴板		连接代	多层加	数据加	数据污损	传输数
务			度				序	載	提供商	订阅	DLL	护进程	缓冲	制数据	序助持			Doppelg		解	NS拦截及中间	签发现	统发现	对象模型	享内容	数据		理	密	審		据操作
																		änging			攻击				-							
增加研	更件	编译的	MSHTA	文件名后	AppCert	DLL搜索	启动代理	Plist修	服务注册	Winlogo	Applnit	新服务	sudo	绕过用户	DLL文件例	HISTCONT	LC MAIN	进程挖空	文件名后面	凭证转	网络嗅探	可信域发	安全软	远程服务的	第三方	数据分		自定义	端口开	数据传	磁盘内容	
		HTML文件		面的空格	DLL	顺序动持		改	表权限弱	n Helper	DLL			账户控制	載漏洞	ROL	劫持		的空格	借		现	件发现	利用	软件	段		命令及	启	输大小	擦除	
									点	DLL																		控制协		限制		
通过	可移动	控制面板项	powershel	第三方软	Applnit	Dylib劫	启动守护进程	端口探	Setuid/Se		Applicat	路径拦	有效账	CMSTP	反混淆/解	隐藏文件和	Launchct	进程注入	模板注入	文件中	密码过滤DLL	文件和目	系统信	登录脚本	Windo	信息库		自定义			磁盘结构	
媒体	进行复	目	1	件	DLL	持		测	tgid		ion	裁	户		码文件或	目录	1			的凭据		录发现	息发现		ws管理	中的数		加密协	何工具	协议渗	擦除	
钓鱼	付件	动态数据交	Regsvcs/R	陷阱	Applicatio	外部远程	Launchetl	端口监	快捷方式		绕过用户	Plist修	WebS	清除命令	禁用安全	隐藏用户	伪装	冗余访问	时间戳修改	注册表	私點	网络服务	系统网	传递哈希	Windo	来自本		数据编	远程文	通过命	端点拒绝	
		换	egasm		n	服务		<b>(9)</b>	修改		账户控制	改	hell	历史	工具					中的凭		扫描	络配置		wsi元程	地系统		码	件复制	今和拉	服务	
					Shimming															据			发现		管理	的数据				制通道		
鱼叉	(約鱼	通过API执	REGSVR32	值得信赖	认证包	文件系统	本地计划任务	Rc.com	启动项目		DLL搜索	鉄口监		代码签名	Execution	隐藏的窗口	修改注册	Regsvcs	值得信赖的	对证书	安全存储	网络共享	系统网	Pass the		网络共		数据混	标准应	渗透到	固件摄毁	
链接		行命令		的开发者		权限弱点		mom			顺序劫持	測			Guardrails		表	/Regasm	开发者工具	访问的		发现	络连接	Ticket		享中的		滑	用层协	其他网		
通过	服务进	通过模块加	Rundll32	用户执行	BITS Jobs	隐藏文件	登录项目	重新打	系统固件		Dylib劫	进程注		传输后编	防御软件	图像文件执	MSHTA	REGSVR	有效账户	强制认	双因素身份验	网络嗅探	系统所	远程卓面协		来自可		域前筛	标准密	物理介	阻止系统	
行鱼	叉式网	载执行命令				和目录		开应用			持	λ		译	湯河	行选项注入		32		证	证拦截		有者/用	议		移动媒			码协议	质的渗	恢复	
络钓鱼	a l							程序															户发现	1		体的数				透		
供应	连妥协	利用客户講	计划任务	Windows	bootkit	钩子	登录脚本	冗余访	系统服务		开发权限	SID-历		编译	额外的窗	指示器阻塞	NTFS文件	Rootkit	虚拟化/沙箱	钩子		密码策略	系统服	远程文件复		电子部		域生成	标准非	计划传	网络拒绝	
		执行命令		Manage				问			提升	史注入		HTML文	口内存注		属性		逃遊			发现	务发现	制		件收集		算法	应用层	輸	服务	
				ment										件	λ														协议			
				Instrume																												
可信	关系	图形用户界		Windows	浏览器扩展	管理程序	修改现有服务	注册表	时间提供		额外的窗	计划任		修改系统	文件删除	移除工具中	删除网络		网络服务	輸入捕		外围设备	系统时	远程服务		輸入捕		备用信	不常用		资源助持	
		面		远程管理				运行键/	者		口内存注	务		固件		的指示器	共享连接	任提供商		获		发现	间发现			获		道	的錆口			
								启动文			λ							劫持														
有效	版户	安装实用工	服务执行	XSL脚本处	更改默认文	图像文件	Netsh	SIP和信	陷阱		文件系统	服务注		组件对象	文件权限	移除主机上	混淆的文	脚本		輸入提		权限组发	虚拟化/	通过可移动		Man in	•	多个通	网络服		实时数据	
		A		理			Helper DLL	任供应			权限弱点			模型	修改	的指标器	件或信息			示		现	沙箱逃	媒体进行复		the		信通道	务		操作	
			l	1-		5+ X		商助持	1	l	1	限弱点		(COM)	1	7 00		1	I	1	1		180	dol	1	Browser			1			

网空模型: 6个阶段, 21个目标, 188多种攻击方式



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

# 攻击者视角: 网络杀伤链KILL CHAIN

### 网络杀伤链Kill Chain



侦查跟踪



武器构建



载荷投递



漏洞利用



安装植入



命令与控制



目标达成



攻击者处在攻击行动的计划阶段,了解被攻击目标,搜寻目标的弱点。

攻击者使用自动化工具将漏洞利用工具和后门制作成一个可发送的武器载荷。

(例如Adobe PDF, Microsoft office文件)

攻击者将武器载荷向被攻击系统投递。 (例如直接向web服务器投递和通过电子邮件、USB等间接渠道 投递)

攻击利用系统上的漏洞,以便进一步在目标系统上执行代码。

攻击者一般会在目标系统上安装恶意程序、后门 或者其他植入代码,以便获取对目标系统的长期访问途径。

恶意程序开启一个可供攻击者远程操作的命令通道。

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。

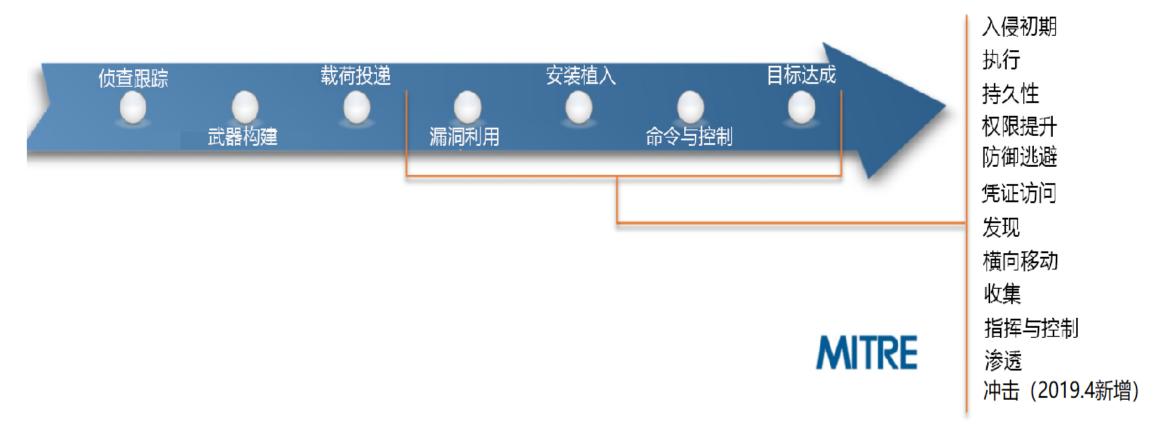
# 攻击者视角:网络杀伤链KILL CHAIN防御应对思路 2019北京网络安全大会 2019 地京网络安全大会 2019 地京 2019 地京网络安全大会 2019 地京 2019 地 2019 地

	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				
V	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			
$\bigvee$	漏洞利用	WebIDS/NIDS	WAF/NIPS/旁 路阻断	DEP			
V	安装植入	WebIDS/NIDS/ HIDS	WAF/NIPS/旁 路阻断/ACL	AV			
V	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	

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

# 防守方视角: ATT&CK模型:



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。

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	ŧ				权限提升				躲遇	防御			!	凭证访问	发	现	横向和	动	采集	数据	命令	控制	渗透	冲	击
Drive-by Compromis	AppleScript	LSASS驱动 程序		.bash_profi le/.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 /Setai		控制面板 项目	文件系统逻 辑偏移	间接命令 执行	Plist修改	签名二进制 文件代理执	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
e			行									d .			1240012			行													
利用面向公众的应用程	CMSTP利用	Launchctl	签名脚本 代理执行	辅助功能		LC_LOAD_D YLIB 插入命	Office <sup>应</sup> 用程序		Web Shell	辅助功能	圏像文 件执行	启动项	BITS Jobs	DCShado `	gatekeeper 防御绕过	安装根证	端口採測	脚本签名代理执行	Bash力	keychain	应用窗口 发现	置词注 册表	应用部署软	共享 Webro	自动收	视频截	通过可 移动媒	多频带通信	数据压	针对破坏 的数据加	
序			10437413		19EE-WIT	\$	启动		Sileii		选项注			, ,	NUMBER 2	To		i-⊞1/N1 J			200	IIII ARE	17	ot	<del>#</del>	1400	体进行	畑田	A#	密	3/A3#1 F
外部远程服	命令行界面	本地任务调	源文件	账户操控	创建账号	LSASS驱动程	路径拦	安全支持	WMI事件						修改组策略	InstallUtil		软件打包	暴力破				分布式组件		剪贴板		连接代	多层加	数据加	数据污损	传输数
务		度				序	截	提供商	订阅	DLL	护进程	缓冲	制数据	序劫持			Doppelg änging		解	NS拦截及中间 攻击	签发现	统发现	对象模型	享内容	数据		理	審	<b>8</b>		据操作
増加硬件	编译的	MSHTA	文件名后	AppCert	DLL搜索	启动代理	Plist修	服务注册	Winlogo	Applnit	新服务	sudo	绕过用户	DLL文件侧	HISTCONT	LC_MAIN		文件名后面	凭证转	网络嗅探	可信域发	安全软	远程服务的	第三方	数据分		自定义	端口开	数据传	磁盘内容	
	HTML文件		面的空格	DLL	顺序劫持		改	表权限弱点	n Helper DLL	DLL			账户控制	载漏洞	ROL	劫持		的空格	储		现	件发现	利用	软件	段		命令及 控制协	启	輸大小 限制	擦除	
通过可移动	控制面板项	powershel	第三方软	Applnit	Dylib劫	启动守护进程	端口探	Setuid/Se		Applicat	路径拦	有效账	CMSTP	反混淆/解	隐藏文件和	Launchct	进程注入	模板注入	文件中	密码过滤DLL	文件和目	系统信	登录脚本	Windo	信息库		自定义	远程访	对替代	磁盘结构	
媒体进行复	目	I	件	DLL	持		测	tgid		ion	截	户		码文件或	目录	I			的凭据		录发现	息发现		ws管理			72 M 172	问工具	协议渗	擦除	
钓鱼附件	动态数据交	Regsvcs/R	陷阱	Applicatio		Launchctl	端口监	快捷方式		绕过用户			清除命令	禁用安全	隐藏用户	伪装	冗余访问	时间戳修改		私匙	网络服务		传递哈希	Windo	1			远程文	通过命	端点拒绝	
	换	egasm		n Shimmina	服务		测	修改		账户控制	改	hell	历史	工具					中的凭		扫描	络配置 发现		ws远程 管理	地系统 的数据		码	件复制	令和控 制通道	服务	
鱼叉式钓鱼	通过API执	REGSVR32			<b>→性系统</b>	本地计划任务	Rc com	启动项目		DLL搜索	端口监		代码签名	Execution	隐藏的窗口	修改注册	Regsycs	值得信赖的	対证书	安全存储	网络共享		Pass the	日理	网络共		数据混	标准应	渗透到	固件损毁	
链接	行命令		的开发者		权限弱点	++0# WILDS	mom	/H-W-XH		顺序劫持			1043111	Guardrails	PENSON JULIE	表		开发者工具	访问的	X 2 13 16	发现	络连接	Ticket		享中的			用层协	其他网		
通过服务进	通过模块加	Rundll32	用户执行	BITS Jobs	隐藏文件	登录项目	重新打	系统固件		Dylib劫	进程注		传输后编	防御软件	图像文件执	MSHTA	REGSVR	有效账户	强制认	双因素身份验	网络嗅探	系统所	远程桌面协		来自可				物理介	阻止系统	
行鱼叉式网 络钓鱼	载执行命令				和目录		开应用 程序			持	λ		译	漏洞	行选项注入		32		证	证拦截		有者/用 户发现	议		移动媒 体的数			码协议	质的渗 透	恢复	
供应链妥协	利用客户端	计划任务	Windows	bootkit	钩子	登录脚本	冗余访	系统服务		开发权限			编译	额外的窗	指示器阻塞	NTFS文件	Rootkit	虚拟化/沙箱	钩子		密码策略		远程文件复		电子邮			标准非	计划传	网络拒绝	
	执行命令		Manage ment				问			提升	史注入		HTML文 件	口内存注 入		属性		逃避			发现	务发现	制		件收集		算法	应用层 协议	輸	服务	
==×=	mr/m÷m	P12-1-	Instrume	Marie Contraction	Advisor de	/ h = / TD - + 10 / h	N-00-	-17718 (11		ATELIAL DE	N I Bullet		the state of the	->- (-)- FD(EA	体験工具士	muno mode	au a da bh	m/h mada	440 \ 140		ti mina	T (street	)=consta		40 \ 100		# m #	T-14 (T)		Mary at the	
可信关系	图形用户界 面		Windows 远程管理	浏克器扩展	管理程序	修改现有服务	运行键/	时间提供 者		额外的窗 口内存注			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	网络服务	輸入捕 获		外围设备 发现	系統时 间发现	远程服务		輸入捕获			不常用 的端口		资源劫持	
±+40/0	rt-Materia EET	마셨나요	VCI BHI-E-N	#-14#21 - <del></del>	Œ1/ <del>45-≥-</del> /+	Nistala	启动文	D/2 DH		人	012/22/5+		40 (+ > + <del>(*)</del>	→/#+F78B	308A→+Π L	:=:XAbababa	劫持 脚本		te ) +8		4D784D44	_E40//k/	海斗可约士		Man in	-	クム海	E242 02		rtnn-t#4tR	
有效账户	安装实用工具	服务执行		更改默认文 件关联		Helper DLL	SIP和信 任供应	PERM		文件系统 权限弱点			组件对象 模型	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		輸入提		权限组发 现	沙箱逃	通过可移动 媒体进行复		Man in the		多个通 信通道	网络服 冬		实时数据 操作	
					注入	S.per DEE	商劫持			o craced/iii	限弱点		(COM)		220 10.00	. 1 501535						避	制		Browser	1				em I F	

### 86种APT示例: 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	AppleScri pt的	_bash_pro file 和 bashrc	访问令牌 操作	访问令牌 操作	账户操纵	账户发现	AppleScri pt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	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	数据传输 大小限制		磁盘结构 擦除
Spearphish ing 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 据	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	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	躲退		ģ.	転送	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	数据污损
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.commo m	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 <del>理</del> 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。

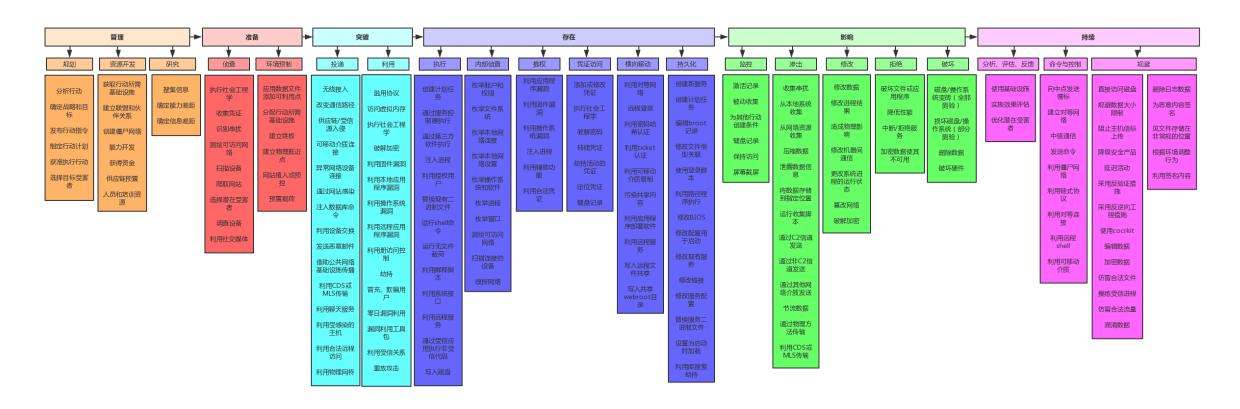
入侵初期	执	 វិភិ	潜伏	权限提升			凭证访问	发现	横向移动	采集数据	命令控制	渗透	冲击
Drive-by Compromise	AppleScript	LSASS驱动 程序	.bash_profile/.b ashrc	访问令牌操控	Setuid/S etgid	文件系统逻辑 偏移	账户操控	账户发现	AppleScript	音频捕获	常用端口	自动渗透	数据销毁
利用面向公众 的应用程序	CMSTP利用	Launchctl	辅助功能	辅助功能	模板注入	Rootkit	Bash历史	应用窗口 发现	应用部署软 件	自动收集	通过可移动 媒体进行通 信	数据压缩	针对破坏 的数据加 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	HISTCONTR OL	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/R egasm	Application Shimming	绕过用户账户控制	WebShe II	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	<del>安装</del> 实用工 具	用户执行	有效账户	文件删除	虚拟化/ 沙箱逃避		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

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

《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)



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

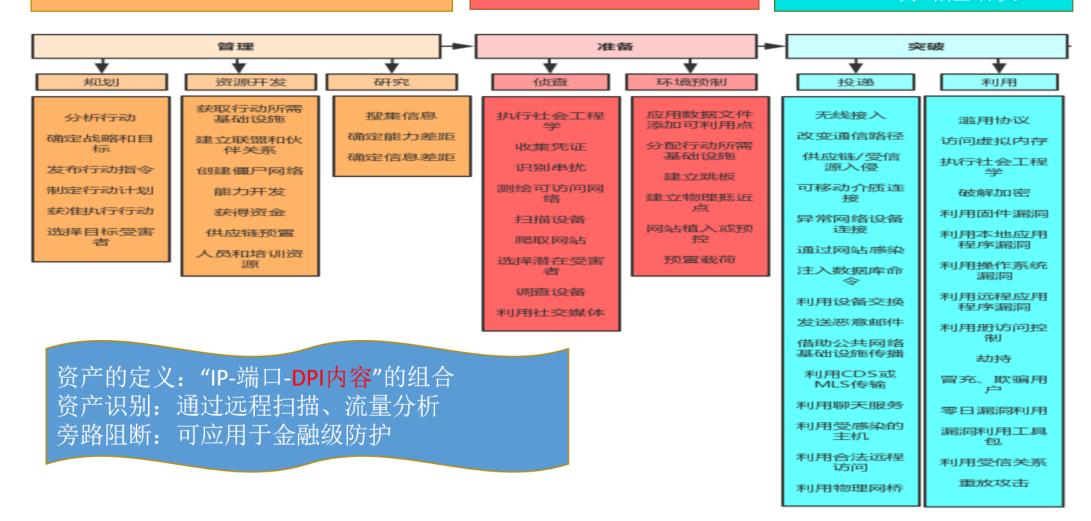
利用线索,回溯分析场景、 全局关联分析,评估影响 范围

# 《网空威胁框架》全周期应对

资产采集、识别、管理

# 漏洞扫描、 预演练

WebIDS、WAF NIPS、旁路阻断仪



# 《网空威胁框架》全周期应对

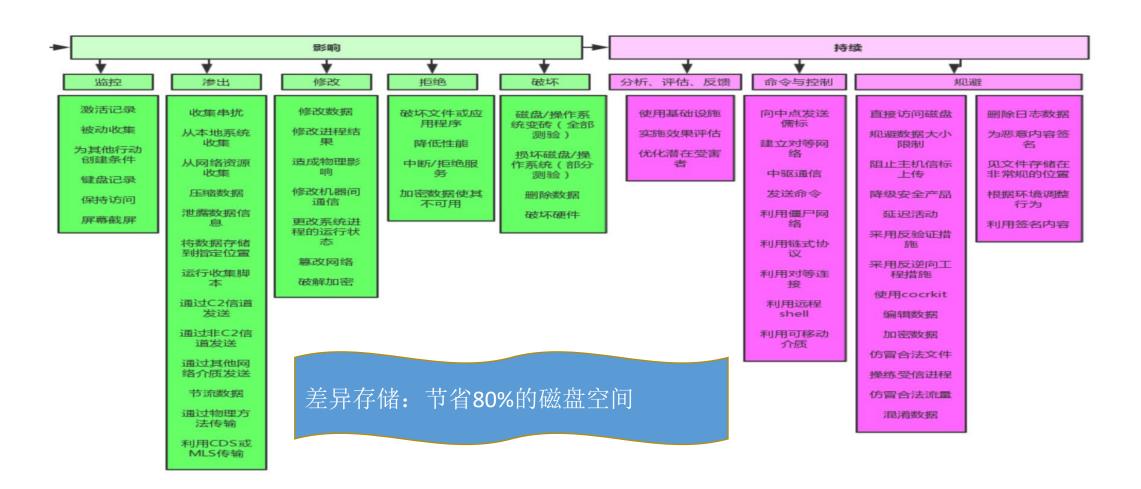
双向数据流关联监测、DNS监测、DPI检测、新资产发现、主机防护



# 《网空威胁框架》全周期应对

### 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: ODAY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

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