网络战争场景下的事前防御思考

张佳发
南方电网数字集团 高级经理

FREEBUF

01 世界战争格局　03 国家企业思考

02 现代战争表现　04 解决方案

01 世界战争格局

- 网络空间战场

随着网络化的迅速发展和全球化进程的加速，各国为维护自身的竞争优势和国家利益，通过互联网收集情报、实施网络攻击等行动，将网络空间与现实地缘政治相互交织，形成新的“战场”，其中高级持续威胁（APT）攻击是最具威胁性的攻击类型。具有专业性、攻击技术手法成熟、攻击方案较为先进等特点，给当前防御手段带来极大的挑战。

因此，亟需防御APT攻击解决方案，提升APT攻击检测和防御能力，应对不断变化的网络威胁。

02 现代战争表现

- 俄乌冲突

自2022年2月24日俄乌冲突正式爆发以来，双方在网络上展开了大规模、高强度的对抗。

俄乌双方在网络对抗中构建了大批前沿阵地，组合运用 DDoS 攻击、数据擦除软件等多种工具及攻击手段，广泛应用于政府单位、关键基础设施等领域，给双方造成巨大损失，凸显网络攻击在现代战争中的巨大威力。

国家	时间	事件
乌克兰	1 月 14 日—15 日	乌克兰当地媒体爆料，乌方外交部、教育部、内政部、能源部等 70 多个政府网站因 DDoS 攻击而关闭，众多重要数据泄露
	2 月 15 日	乌克兰计算机应急响应小组表示，乌克兰国防部、武装部队等多处信息资源遭到强大 DDoS 攻击，导致网站服务中断
	2 月 23 日	监测互联网状态的 NetBlocks 组织证实，乌克兰国防部、安全局、外交部等多个政府、金融机构网站 /App 遭到 DDoS 攻击瘫痪，数百台机器遭到数据擦除攻击
	2 月 24 日—26 日	据美国有线电视新闻网报道，多家乌克兰电信运营商因网络攻击出现严重中断，政府临时切断互联网，境内无线和有线连接受限
	3 月 10 日	思科 Talos 研究人员称，俄罗斯网络黑客使用伪装成安全工具的恶意软件 DDoS，瞄准偷窃乌克兰 IT 军队的关键数据及信息
	3 月 28 日	乌克兰最大电信运营商 Ukrtelecom 于脸书披露，其遭遇自开战以来最严重的网络攻击，导致可正常运行的服务跌至战前水平的 13%
俄罗斯	2 月 24 日—25 日	俄罗斯国家媒体 RT 电视台表示，约 1 亿台设备遭 DDoS 攻击，导致电视台部分时间无法访问
	2 月 26 日	据俄罗斯卫星社报道，“匿名者”黑客组织发动大规模 DDoS 攻击，造成克里姆林宫、国防部、外交部等多个政府网站完全无法访问
	3 月 1 日—3 日	“匿名者”黑客组织发推文宣布，先后攻击俄罗斯多家主流媒体网站、航天局，宣称切断俄方对间谍卫星的控制
	3 月 5 日	“匿名者”黑客组织发起的网络攻击致使俄罗斯联邦银行、国防数据库、政府网站的数据泄露
	3 月 11 日	“匿名者”黑客组织入侵了俄罗斯重要联邦机构、互联网审查部门，窃取了超过 36 万份文件、约 820 GB 数据
	3 月 24 日	“匿名者”黑客组织宣布入侵俄罗斯中央银行，并将发布 3.5 万份以上相关秘密文件

02 现代战争表现

- 俄乌冲突网络战特点

作战力量上，国家力量、黑客组织主导冲突

俄乌冲突的网络作战主力是国家级网络力量、黑客组织及民间力量，多方势力纷纷表态和行动，为此次冲突增加了更多复杂性。

作战目标上，瞄准军事、关键基础设施

双方均将网络攻击目标瞄准对方军事、关键基础设施，旨在造成敌方社会混乱、通信中断，削弱政府军事及民间机构的协同作战能力。

作战方式上，辅以心理战和舆论战作战

俄乌双方在发动网络战的同时，综合运用心理战、舆论战，制造心理威慑、引导舆论走向，以达到全面压制、舆论胜利的效果。

攻击手段上，运用多种手段制造打击

本次冲突中，俄罗斯使用的攻击活动包括DDoS攻击、钓鱼欺诈、漏洞利用、供应链攻击、恶意数据擦除攻击等，扩大网络攻击的杀伤面。

02 现代战争表现

- 巴以冲突

10月7日，伴随着数千枚火箭弹的发射，巴勒斯坦伊斯兰抵抗运动（哈马斯）宣布对以色列发动军事行动。

随着现实世界中的冲突爆发，多方势力的黑客行动主义组织开始在双方网络空间区域内进行持续的博弈，攻击方式主要以DDoS为主，并包括数据窃取、网站污损等其他攻击手段实施网络攻击，宣传对己方有利的言论，引导舆论导向。

02 现代战争表现

- 巴以冲突网络战特点

针对关键基础设施的攻防对抗成为网络战的关键

关键基础设施方面已成为现代战争的首要选项，因其可用性、完整性、保密性对国家安全至关重要。

黑客组织影响网络攻防和认知态势走向

非国家级黑客组织可以在任何时间、任何地点、任何位置自主对目标实施网络攻击。

破坏性DDoS攻击成为国家级网络战重要手段

大量物联设备不断接入互联网，脆弱性广泛存在，成为DDoS攻击的主要目的。

网络战成为现代战争的首要选择

因成本低、隐蔽性强、溢出效应显著等原因，网络攻击行动已成为现代战争的首要选项。

02 现代战争表现

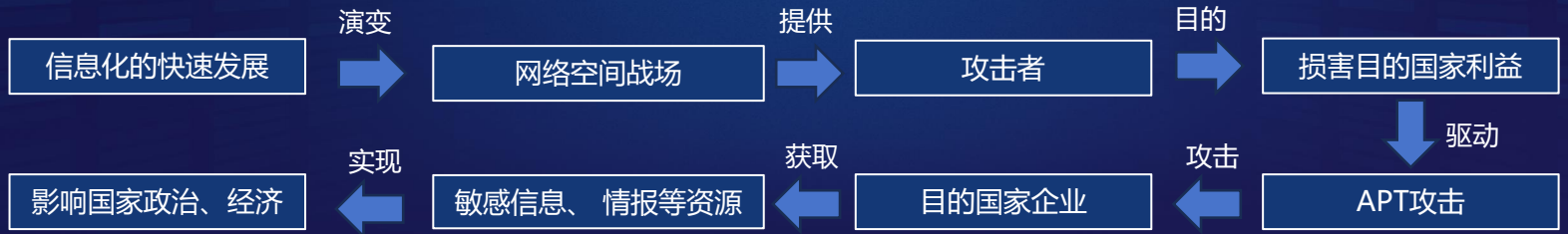
- 关键信息基础设施的攻防战

湖北省武汉市公安局江汉分局发布警情通报称，武汉市应急管理局地震监测中心的部分网络设备被植入木马病毒，初步判定这一事件为境外具有政府背景的黑客组织和不法分子发起的网络攻击行为。国家计算机病毒应急处理中心和360公司对木马病毒进行了溯源分析，获悉该境外黑客组织来自美国，攻击的原因是**地震监测中心的相关数据可推导出某区域的地下结构和岩性**。

03 国家企业思考

- 国家利益驱动

随着信息化的快速发展，国家之间的“战争”已逐渐演变为网络空间的较量。在网络空间新战场上，国家利益是APT攻击的重要驱动原因之一。攻击者针对目标国家企业实施APT攻击，通过获取目标企业的敏感信息、 情报等重要资源，实现对受害国的政治和经济利益产生深远的影响。



03 国家企业思考

遭受APT攻击原因

随着国际局势的紧张变化和网络博弈的加剧，2023 年上半年，趋于政治因素的各类 APT 攻击活动显著增加。国家企业遭受APT攻击的主要原因为以下方面：

政治动机

因地缘政治因素，APT攻击成为国家之间冲突、竞争或敌对关系的表现形式之一。旨在削弱敌对国家或获取战略优势，实现自身利益最大化。

软件漏洞

由于软件行业中的微软产品或服务普遍存在漏洞，已上升为除了政府以外的第二大易受到APT组织攻击的原因。

重要价值

APT攻击其主要目标是政府机构、大型企业、关键基础设施等。通过利用各种技术手段，获取目标的敏感信息、情报等价值。

03 国家企业思考

- 事前防御

为有效应对APT攻击，企业应全面梳理企业数字资产清单，并主动进行漏洞扫描和识别，以发现存在的漏洞和威胁。同时，还应梳理攻击链路，了解攻击者可能利用的路径和手段，以便更好地防范和应对APT攻击。

1、全面梳理企业数字资产清单

通过建立数字资产管理体系，梳理数字资产，完善资产准确性、完整性，为资产漏洞风险排查奠定基础。

2、主动发现资产存在的威胁

对已梳理的资产进行漏洞扫描及威胁识别，识别资产是否存在漏洞，以便后续的修复和应对。

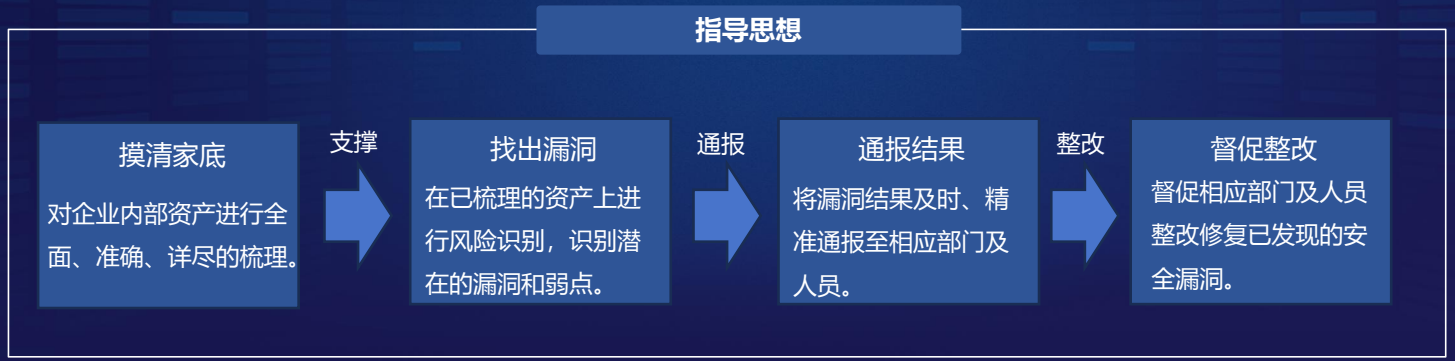
3、梳理明晰攻击链路

通过对传播路径的推导和分析，可了解攻击者的攻击路径、目标等，以便更好防范和应对APT攻击。

04 解决方案

- 指导思想

以“摸清家底、找出漏洞、通报结果、督促整改”为指导思想，全面摸清企业数字资产情况，掌握存在安全风险和漏洞资产，通报漏洞扫描和识别结果，并督促相关部门进行整改，以便更好保护企业数字资产安全，应对APT攻击等网络安全事件。



04 解决方案

- 解决思路

解决思路包括事前、事中、事后三方面，核心为事前检测，全面掌控资产信息、开展安全检测，当发现发现后，事中将快速开展应急工作，定位资产确定威胁范围，事后持续监测存在风险资产，闭环完成整改工作。

1、事前

全面摸查企业全方位资产信息，并主动进行脆弱性分析、弱口令扫描，识别潜在的资产风险漏洞。

2、事中

当发现风险后，快速关联定位风险资产；并提供风险治理规范流程、治理步骤，准确解决问题。

3、事后

实时掌握资产动态、持续监测风险整改状态，全局掌握风险整改进度。

04 解决方案

- 解决技术

以资产测绘技术手段为基础，实现自动化全网资产排查和精准漏洞定位，并关联漏洞资产及风险接口，打破原有资产扫描探测不准确的现状，提升网络资产安全管理效率和质量。

04 解决方案

- 解决技术点

■ 快速定位资产+精准POC扫描验证

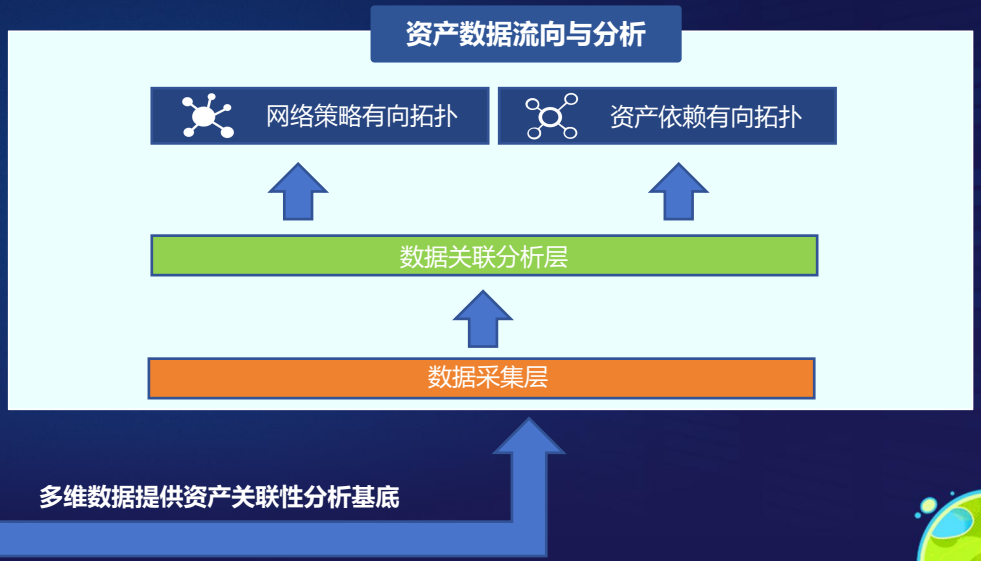
通过主动扫描探测与Agent本机自检两种技术手段，实现快速定位网络资产，精准对指定资产执行POC扫描、弱口令验证等风险检测任务，在威胁来临之前消除资产安全风险。

■ 主机网络拓扑+业务流图形展示结合

通过主机网络拓扑、业务流图形展示结合，并基于资产收集数据和关系模型，关联分析展示主机网络拓扑、业务资产全链路。

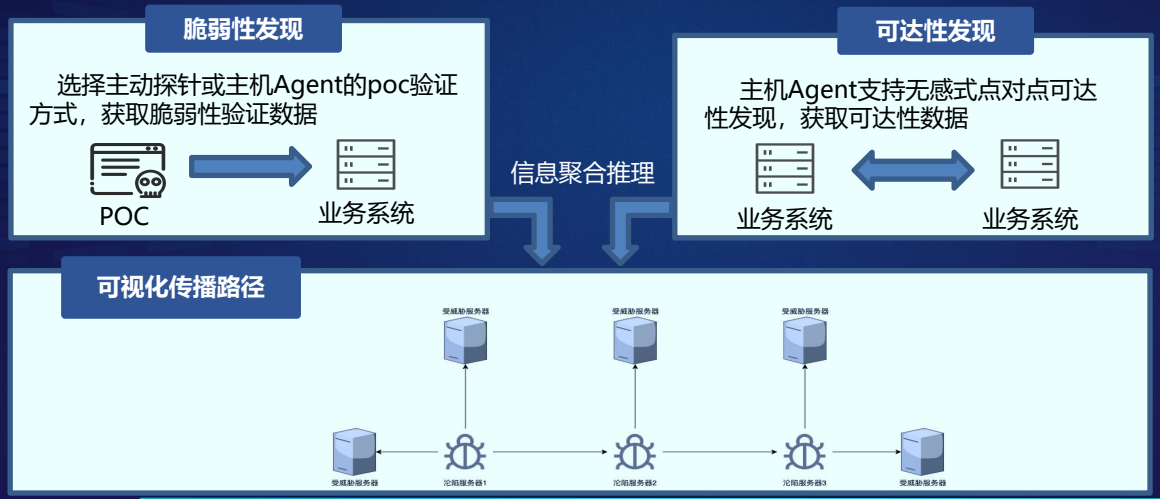
04 解决方案

- 解决流程-资产数据采集与流转分析



04 解决方案

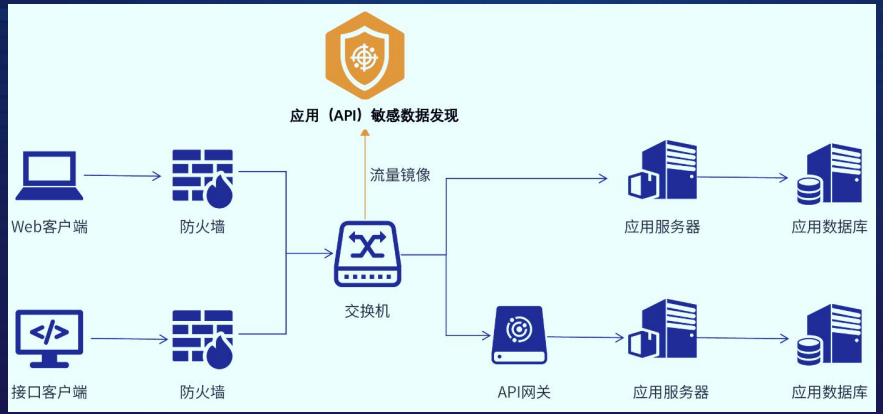
- 解决流程-脆弱性发现与传播路径自主推导



04 解决方案

- 解决流程-敏感数据传输发现

对API访问的数据进行持续监测评估，自动梳理API 接口中的敏感数据流，并生成API接口与敏感数据映射。



04 解决方案

- 解决流程-API威胁检测

在识别API资产的基础之上,综合利用智能规则匹配及行为分析的智能威胁检测，持续监控并分析流量行为。智能威胁检测引擎在用户与应用程序交互的过程中收集数据，并利用统计模型来确定 HTTP 请求的异常。

04 解决方案

- 解决标准和主旨目的

从溯源的角度、攻击者角度开展企业攻击面管理，探测网络资产是否存在潜在漏洞和风险，对突发漏洞进行精准定位。并定位关联漏洞资产，实现以战时可对抗APT攻击为标准，构建事前网络防御工事，打造网络空间民族新长城，提升自身的网络安全防御能力，有效应对APT攻击。

网络安全 FCIS 2023创新大会

THANKS

FREEBUF