安芯网盾

2022 年实网攻防演练
蓝队防守指南

安芯网盾（北京）科技有限公司

目录

Part1.
实网攻防演练概述

网络安全的本质是对抗，对抗的本质是攻防双方能力的角逐。2016 年出台的《网络安全法》中三十四条、三十九条、五十三条多次提出：关键信息基础设施的运营者和网信部门应“制定网络安全事件应急预案，并定期进行演练”。

2016 年，由公安机关组织开展首次全国性的实网攻防演练，主要是公安机关组织红队对目标系统进行集中攻击，检验防守方关键系统的防护能力及指导网络安全建设，此后每年举办一次为期 2~3 周的攻防演练，并以积分的形式确定防守方排名。

2020 年信安标委 WG7 小组发布的《网络安全事件应急演练通用指南》给网络安全演练提供了具体指导，通过演练对参与单位的网络安全事件处置流程进行检验，通过对各单位演练情况进行总结并制定考核奖惩机制，达到改善提升和监督整改应急处置工作的目的。

攻防演练是国家应对网络安全问题所做的重要布局之一，也是对重点的关键基础设施行业单位网络安全能力的一次“大阅兵”，通过暴露隐患、查缺补漏，提升日常的防范意识，增强关键信息基础设施安全防护能力。目前参与的机构众多，包括公安部、政府单位、事业单位、国企单位、名企单位等，攻击手段越来越高级，攻防演练开始以真刀真枪的对抗行为走向实战化。

表 1 2016 年-2021 年实网攻防演练行动介绍

时间	涉及范围	演练要点
2016	公安部、民航局、国家电网 3 家事业单位参与。	参与单位的业务系统有网络应急响应预案，要求定期做演练，对攻击者没有过多的要求，同时演练的基础设施基本上是内网系统，对业务系统对外访问有严格的限制。
2017	国家旅游局、北京市药监局、北京自来水集团、北京教育考试院、中国人寿、中科院、央视网、首汽租车、安贞医院、小米科技等。	政府部门开始参与进来，对外访问的政府网站成为了本阶段攻击的重点，对比 2016 年，这次网站不能关闭，当然也存在被攻击时拔网线的情况，但是攻击方确实能发现很多 web 漏洞拿下网站，这期间也涌现出了一大批专用安全产品和解决方案。
2018	部分国有企事业单位及其他重点单位，约 51 家防守单位。	新增企事业单位参与，这个阶段才出现了真正有价值的攻击团队，防守单位需要防攻击、防破坏、防泄露和防重大网络安全事故，双方采取“背靠背”的方式，即事先不通知，攻击目标和攻击手段也不明确。
2019	工信、安全、武警、交通、铁路、民航、能源、新闻广电、电信运营商等，约 120 家防守单位。	参与单位大大增加，攻击方把精力都放到社会工程学、新型免杀木马、0day 使用等攻击手段。
2020	除了政府部门、国企事业单位、所有商业银行，新增公有云、物联网相关企业加入，约 130 家防守单位。	信息安全基础设施的承载平台出现了一些变化，很多企业的系统已经上公有云、物联网平台，因此云平台的防御能力也受到关注和重视。

2021	规模和范围持续增加，超过 200 余家防守单位。	受到新冠疫情影响，在线办公带来的供应链安全威胁也在增加。2021 年的实战演练规则更为复杂，攻击团队开始利用自动化工具，内存马攻击、邮件钓鱼等攻击手段高频出现。防守侧引入自主防御战略，有部分创新型厂商开始推出 0day 漏洞防御、内存马防护的方案。

安芯网盾从成立的第二年就开始参与实网攻防演习，帮助防守方提供威胁检测能力和防护策略，一是提供内存安全产品，在主机端帮助防守方建设针对 0day/nday 漏洞利用攻击、无文件攻击的防御能力，弥补在未知威胁防护方面的不足；二是提供现场值守，基于安芯网盾安全专家团队在行业十多年的攻防对抗经验，以及应急响应独家工具 PCHunter，帮助防守方对攻击信息进行快速溯源分析和处置。此外，安芯网盾基于对过去演练中出现的防护痛点，在 2020 年、2021 年先后推出了业内首发的域控安全防护解决方案、内存马防护解决方案，帮助防守方抵御演练中出现的高频攻击事件，获得客户感谢信。

图 1 安芯网盾域控安全防护解决方案、内存马防护解决方案手册封面图

Part2.
红队典型攻击手段

孙子兵法中讲“知己知彼，百战不殆”，在信息安全攻防对抗中同样适用。在实战攻防演练中，防守方想要获得好成绩，除了要拥有红队攻击视角，还得熟悉攻击的套路，这样才能有效采取各种预防措施或者应急响应方案，使红队攻击难以奏效甚至实现反制。

红队在实战演练中的技战术首要目标是边界突破和内网渗透。在边界突破阶段，红队通过信息摸查寻找网络边界突破口，实现攻击打点，建立持续、稳定的攻击跳板。一旦跳板建立，红队进而转向第二阶段，即内网渗透阶段。内网渗透阶段利用多项复合的攻击技术，对同网段内的设备不断进行横向渗透，并利用业务连接关系不断向核心网络进行入侵，最终拿下目标系统。

表 2 红队典型攻击手段

攻击阶段	子阶段	攻击方式	典型攻击手段
边界突破	摸查阶段	真实 IP	NSlookup/多地址 Ping DNS 查询 子域名查询 邮件订阅反查 SSL 证书探测 HTTP 标头比对 F5 LTM 解码 第三平台(Fofa/Shodan/Censys)
		服务信息	遍历得到 Web 管理后台地址 Web 服务 banner（Nmap、Fscan） Google Hack
		敏感信息	Google/GitHub/网盘/文库 云主机 AccessKey 目标网站信息泄露/SVN/GitLab 网站备份文件 社工库（组织架构/个人信息）
	准备阶段	业务分析	开发框架分析 上传点分析 业务逻辑分析 Web 请求分析 JS 分析 系统开发商分析 WAF 产品识别（WAFW00F）

		攻击准备	弱口令字典制备 WAF 绕过准备
	攻击打点	业务组件漏洞利用	框架| Struts2/ Shiro Apache| Solr/Tika/Axis/Shiro 中间件|Weblogic/Tomcat/Spring/WAS/Jboss/Jekins/RabbitMQ/Glassfish 数据库|ElasticSearch/Redis/MySql/ MSsql
		第三方软件漏洞	邮件类|Coremail/ Exchange/ PHPMailer 项目管理类|Jira/禅道/ Pingcode 办公类|通达 OA/致远 OA/泛微 OA/金蝶 OA/Zimbra 运维类|Citrix/Jumpserver/Zabbix/Cacti/Nagios/Webmin/Sangfor Vpn
		钓鱼攻击	Office 宏钓鱼/DOCX 文档远程模板注入执行宏 CS 克隆网站钓鱼/假网站钓鱼/CS 鱼叉钓鱼 lnk 快捷方式钓鱼
内网渗透	权限提升	Windows	Wesng/Powerup UAC 绕过 系统漏洞提权 Dll 注入 注册表键提权 AccessToken 窃取 烂土豆 Psexec 提权
		Linux	内核漏洞提权 linux-exploit-suggester Suid 提权 Sudo 提权 DirtyCow/DirtyPipe
	信息收集	本机信息收集	当前权限及内核版本 本机网络配置信息 本机历史信息（历史命令、历史登录） 本机动态信息（应用、网络链接、杀软、外联、计划任务、注册表）
		网内信息收集	机器名及组、域信息 内网端口扫描 内网服务 Banner 内网服务识别（堡垒机、文件共享、数据库、网安设备、打印机）

	凭证窃取	Windows	文本文件（xls,doc,txt 等） 注册表账号信息 密码抓取（Hash、token、MSTSC、VNC 等） SSH 工具密码 Keylogger
		Linux	shadow 暴力破解 LinEnum
		应用与数据库	数据库连接配置 Web 服务配置 Redis 配置 FTP 配置 VPN 配置 SVN 配置
		域控	Lsass 黄金票据 NTLM
	权限维持	内网穿透	内网代理（FRP、CS 等） Socks 转发 DNS 隐蔽隧道 端口复用
		Windows	系统任务/注册表 WMI Dll/COM 劫持 Powershell 后门 克隆账户
		Linux	SSH 后门 Cron 计划 .so 文件劫持 vim 后门 隐藏文件 添加用户 alias 后门 reGeorg
	横向渗透	Windows	WMI RDP PTH Schtasks/at/sc PSexec

			DCOM NTLM Replay SMB
		Linux	增加路由 MSF SSH

Part3.
2022 年攻击手段 TOP5 预测

通过分析过去几年的实网攻防演练，我们发现除了参与演练的单位规模不断增加，每年演练的要点也在跟随关键信息基础设施的建设而变化，随着攻防演练走向实战化，攻防双方的技术水平和对抗能力也在博弈中不断升级。

安芯网盾安全专家通过分析近几年来红队攻击的路径，包括攻击的核心目标、红队攻击手法和实例剖析等，从红队利用频率高低、利用容易程度和危害程度大小出发，预测 2022 年红队将会利用的 TOP5 攻击手段。

TOP1 无文件钓鱼

利用频率高低	利用容易程度	危害程度大小
★★★★★	★★★★☆	★★★★★

入选理由

无文件钓鱼是将社会工程学与无文件攻击相结合的高级网络攻击手段，是近几年真实攻击案例和攻防演练中利用频率最高也是最容易成功的一类攻击手段，比如利用大家对疫情的高度关注、利用大家对八卦信息的猎奇心里等。

攻击者利用无文件钓鱼主要有两大优势：

一是有效降低了攻击门槛，使红队不必强攻用户网络即可有机会获取受信任立足点。它充分利用了人性弱点，通过精心伪造场景，诱使目标下载、执行恶意程序或访问恶意链接，从而达到提权或数据窃取等目的。

二是利用无文件的攻击手法能有效绕过用户网络安全防御体系，提升钓鱼成功概率。无文件攻击通常会利用操作系统的合法程序直接将恶意程序加载至内存运行来攻击计算机，不会有恶意文件在本地磁盘落地，并且不会留下任何足迹，这给检测、溯源带来很大困难。为了逃避检测，攻击者开发的无文件恶意软件变得越来越复杂越来越有针对性。这些软件往往采用最新的技术，并以混淆、加密等方式来伪装自己。

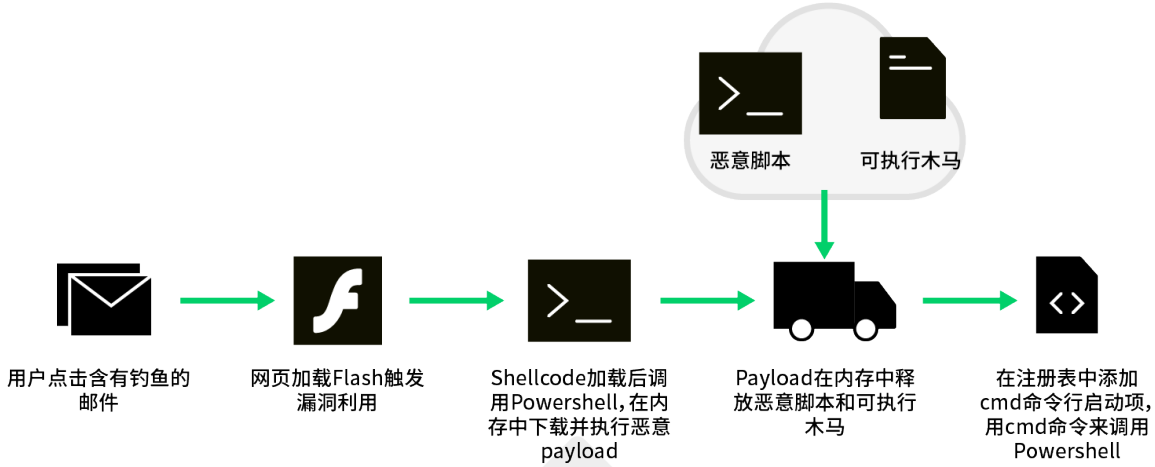

图 2 典型无文件钓鱼攻击场景

策略建议：

目前，关基运营者针对钓鱼攻击的防护主要从“人防”和“技防”两个层面入手。人防主要是通过安全培训、邮件钓鱼演习提高员工的网络安全意识。技防主要是通过部署邮件安全网关、邮件防泄漏等措施应对邮件威胁。要想发现无文件钓鱼这类攻击，需要实现对邮件附件、邮件账号、邮件 URL、邮件来源、邮件异常行为等一体化安全解决方案。

TOP2 弱密码利用

利用频率高低	利用容易程度	危害程度大小
★★★★☆	★★★★☆	★★★★★

入选理由

弱密码利用在真实黑客组织或者攻防演练中是利用频率最高的一类攻击手段，对于攻击方来说弱密码利用的核心吸引力在于具备低成本、高回报。

弱密码利用主要包括两类，一类是应用程序默认的用户密码，另一类是用户自己设置的密码。第一类问题产生于系统管理员未对默认用户进行安全策略加固；第二类问题产生于应用程序未对密码策略做强制要求，导致一些用户使用简单密码来方便自己记忆。符合密码复杂度的也并非绝对安全，也存在被猜测性，一些常见密码如系统默认密码，或者与用户个人姓名、手机号相关的密码，尽管看起来很复杂，但仍然可以被猜到。

使用弱密码是一件很危险的事情，因为大多数红队攻击的初始阶段都会涉及系统信息和用户身份的枚

举。如果用户密码被轻易破解，那么攻击者就可以轻松地进行身份认证。倘若被攻陷的是具有管理权限的默认账户，那么红队将会通过这类账户进行账户创建、权限变更、策略变更等操作，给用户网络带来严重威胁。

基础策略

弱密码利用属于管理漏洞，应从以下几个方面进行加固：

1. 尽可能禁用所有默认账户，并对未禁用账户设置强身份认证策略，如双因素认证方式登录。
2. 管理员为所有用户设置强密码策略，对密码的长度、复杂度、生存周期等做出明确约束，在密码复杂度上推荐使用密码短语方式，并定期检查。
3. 树立单位全体成员密码安全意识，不使用与个人信息有关的易猜测的密码，并正确保管自己的账号和密码信息。

TOP3 内存马攻击

利用频率高低	利用容易程度	危害程度大小
★★★★☆	★★★☆	★★★★★

入选理由：

Webshell 攻击主要分为普通依赖于文件的 Webshell 攻击和更为先进的内存马攻击两种。

普通 Webshell 攻击通常采用 SQL 注入、页面漏洞、跨站脚本（XSS）等方式进行攻击。攻击者通过将 Webshell 恶意文件上传到目标服务器，建立对 Web 应用程序持久化的访问，从而获得远端的代码执行、数据库枚举和文件管理等操作权限。并基于现有权限，利用系统上的本地漏洞来进行权限提升攻击，获取 Web 服务器管理员用户权限，从而进行数据窃取、流量监控、横向渗透等恶意活动。目前主流的 Web 应用防火墙及主机防护系统均能对大部分已知的普通 Webshell 攻击进行有效防护。

内存马攻击，又称无文件马攻击，是 Webshell 的无文件形式，近两年来成为网络安全攻防对抗活动中红队的“王牌武器”。它基于 Web 应用本身存在的漏洞，利用中间件的进程来执行恶意代码来获得 Web 服务权限。以 JAVA 内存马为例，它利用反序化漏洞、代码执行漏洞、文件上传漏洞，来完成 Filter 内存马的注入，在注入完成后，结合其他攻击手法如采用冰蝎的 AES 动态加密 Webshell、使用伪造的 HTTPS 证书进行流量加密或自定义编解码方式，进而达到流量混淆规避监测等效果。

随着攻防演练走向实战化，攻防双方的技术水平和对抗能力也在博弈中不断升级。攻击方通过操纵漏洞利用程序、合法工具、宏和脚本，可以破坏系统、提升特权或在网络上横向传播恶意代码，并在执行后采取尽量隐藏自身或清除的手段，使其难以被检测，以门户网站为例，其服务直接暴露在互联网

环境，十分容易成为红队攻击目标，使用内存 Webshell 的攻击手段可以轻松绕过现有的安全防护体系，达成攻击目标。这在一定程度上导致了普通 Webshell 攻击的“没落”和内存马攻击的“崛起”在 2020 年的攻防演练中，内存马也成为攻击方手里的“王牌手段”。

与普通 Webshell 攻击相比，内存马攻击具有以下特点：

- **易混淆：**支持各类 bytecode 和 payload 的注入，变化多样，便于混淆，容易绕过 WAF 等基于特征的安全检测手段。
- **无文件：**攻击过程对文件落盘依赖程度低，往往在文件落地执行后立即删除自身或是完全不涉及文件落地，给检测带来很大困难。
- **难溯源：**内存 Webshell 在执行后会隐藏在 Web 容器中，普通运维人员很难发现问题，即使察觉到异常也很难去溯源。

防护现状：

对于内存马攻击的防护，单纯依靠基于静态特征的传统检测方式是远远不够的，需要深入 Web 程序内部进行威胁发现。目前对内存马的防护，比较有效的方式是 RASP 技术，它采用进程注入的方式，通过监控 Web 应用程序异常行为来对内存马攻击进行检测。

TOP4 AD 域攻击

利用频率高低	利用容易程度	危害程度大小
★★★★☆	★★★☆	★★★★★

入选理由：

在企业网络信息化建设中，经常会使用 AD 域(Active Directory Domain)来统一管理网络中的 PC 终端。在 AD 域中，DC(域控制器)包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。 在历年来的大型攻防实战演练中，我们发现使用 AD 域进行内部网络管理的单位，攻击方和防守方争夺的核心往往聚焦在 DC 上：对攻击方来说，获得了 DC 的控制权限即可宣告攻击成功；对防守方来讲，只要守护好 DC，则内部网络始终不会遭受到特别严重的损害。

从攻击方的方法论来说，攻击 AD 域常用的方法有 PTH 攻击、黄金票据攻击、白银票据攻击、lsass 进程读取明文密码，以及特权提升漏洞攻击等，攻击者对 AD 域进行攻击时，通常以获取 DC 的控制权限为目标。而大部分安全产品在面对这些攻击时，无法进行有效的防护，难以在第一时间发现并阻断这些攻击。

表 3 AD 域攻击常用攻击方式

攻击方式	攻击描述
Netlogon 漏洞利用	攻击者可以使用 Netlogon 远程协议（MS-NRPC）建立与域控制器的易受攻击的 Netlogon 安全通道连接并进行特权提升。
Lsass dump	攻击者通过读取 lsass.exe 进程的内存就有机会获得域控管理员的密码。
PTH 攻击	攻击者可以通过捕获密码的 hash 值,然后简单地将其传递来进行身份验证，以此来横向访问其他网络系统。
黄金票据攻击	在拿到域管权限后，生成任意权限的票据，从而创建持久化后门。

策略建议：

AD 域服务器攻击防护的重要性不言而喻，要想防御 AD 域攻击就需要具备对 AD 域中认证协议、AD 域中行为和相关流量的采集和解析能力。针对 AD 域控攻击，安芯网盾在 2020 年首发域控服务器攻击防护解决方案，解决用户在使用 AD 域进行内部网络管理过程中所面临的安全风险。

TOP5 0day/nday 漏洞利用攻击

利用频率高低	利用容易程度	危害程度大小
★★★☆	★★☆	★★★★★

入选理由：

在网络攻防博弈过程中，0day 漏洞因具备极强的危害性，以及极高的成功渗透率，而备受攻击者青睐，通过利用 0day 漏洞可成功入侵系统并执行有效载荷，而当载荷为具备感染性和自传播的恶意软件时，其破坏力更是惊人，无论是曾经波及全球且造成严重影响的 Stuxnet、Wannacry，还是 2021 年 4 月影响较广的英国铁路遭受勒索攻击，以及 chrome v8 引擎远程代码执行漏洞，都是值得警醒。

在历年的攻防实战演练中，红队都会将 0day 漏洞作为制胜法宝，甚至会直接利用安全产品自身存在的 0day 漏洞来突破蓝队网络边界防线，进而进行横向渗透。例如，通过攻击安全接入网关、准入控制系统、终端安全系统等，获取网络控制权限，进而攻陷整个网络。

通常红队利用 0day 漏洞攻击目标，会涉及以下步骤：

1. **挖掘漏洞：**寻找程序代码中的漏洞；
2. **识别漏洞：**发现漏洞，并编写恶意代码，与 0day 漏洞整合，验证可行性；
3. **收集信息：**尽可能多的收集目标信息；

4. **执行渗透：**利用攻击武器对目标发起攻击，潜入其内部网络；
5. **远程控制：**获取内部重要主机的控制权限，并在内部横向移动。

表 4 2021 年典型高危漏洞示例

漏洞名称	漏洞编号	影响范围	描述
Apache Log4j2 远程代码执行漏洞	CVE-2021-44228	Apache log4j2 2.0 至 2.14.1 版本。	Log4j2 组件在处理程序日志记录时存在 JNDI 注入缺陷，导致目标服务器任意命令执行。
Chrome 权限提升漏洞	CVE-2021-21224	Google Chrome 87.0.4280.66,87.0.4280.141,88.0.4324.96,88.0.4324.146,88.0.4324.150,88.0.4324.182,89.0.4389.72,89.0.4389.90,89.0.4389.114,89.0.4389.128,90.04430.72	V8 浏览器引擎中的类型混淆错误导致攻击者可以在目标系统上执行任意代码。
Windows Print Spooler 远程代码执行漏洞	CVE-2021-34527	影响包括 WIN7、WIN8、WIN10、Server2008、Server2012、Server2016、Server2019 在内的主流版本系统。	攻击者可利用该漏洞以系统权限运行任意代码，然后可以安装程序，查看、修改或删除数据，或者创建拥有完全用户权限的新账户。
Windows 域服务权限提升漏洞	CVE-2021-42287	影响包括 Server2008、Server2012、Server2016、Server2019、Server2022 在内的主流版本操作系统。	攻击者可利用该漏洞将域内的普通用户权限提升到域管理员权限。
Windows 本地提权漏洞	CVE-2021-1732	影响包括 WIN10、Server2019 在内的主流版本操作系统。	主要用于定向攻击活动，本地攻击者可以利用此漏洞提升到 system 权限。

防护现状

尽管近些年各大安全厂商的产品开始将动态程序分析、静态程序扫描等多种技术应用于 0day 漏洞的检测场景，但却依然收效甚微，其主要原因还是由于 0day 的未知性。当 0day 漏洞被应用于网络杀伤链（Cyber kill chain）时，攻击者通常会先利用 0day 漏洞突破外围防线渗入内网，之后再尝试暴力破解或权限提权等手段，获得系统的绝对控制权，进而实施持久化攻击。

对 0day 漏洞利用的防御，本质上是防御攻击者利用 0day 漏洞投递及执行恶意载荷行为，基于补丁修复、签名检测或流量的方式均难以有效防护。而基于内存保护的解决方案为 0day 漏洞利用的防护提供了全新的思路。

Part4.
蓝队防守能力核心要点

要想做到有效防御，既要对自身安全能力有充分的了解，也要对红队的攻击方式有着充分的认识，在整个实网攻防演习活动过程中，需要充分吸取往年经验，立足“实战化，体系化，常态化”要求，从技术和管理层面构建和完善网络安全防护体系，只有这样才能更有针对性地布防，从而起到事半功倍的效果。

1、准备阶段

准备阶段的主要工作目标是对单位安全现状进行自查评估，发现当前存在的问题，并进行整改和加固。该阶段核心工作内容主要包括信息资产盘点、安全设备优化、漏洞检查与修复、敏感信息处置、供应链风险管理以及安全宣贯培训。在准备工作完成后，需要对工作成果进行确认，确保整改工作的有效性。

信息资产盘点：信息资产盘点是实网攻防演练工作准备阶段的首要任务，是安全设备优化、系统加固等工作得以完整开展的前提。由于红队往往会寻找一些边缘资产或是已经废弃但未下线的设备作为攻击落脚点来隐藏自身，一旦资产清单不完整、不清晰，则有可能被攻击方利用，导致资产被远程控制，乃至整个网络被攻陷。因此，一定要对直接或间接接入单位网络的信息化设备进行完整盘点，明确管理方式和相关责任人，形成信息化资产管理清单，确保信息化资产管理不留死角。

安全设备优化：安全设备优化工作的核心，是最大限度收敛攻击面，减少红队攻击突破口。一方面，通过优化网络拓扑、升级特征库、优化安全设备策略来充分发挥现有网络安全产品的价值和能力；另一方面，通过更新安全设备软件版本、梳理和优化运维管理来消除因安全管理不规范或是安全设备自身存在漏洞而导致的风险隐患。同时，建立和提高安全设备联动能力和安全事件自动化研判和处置能力。

漏洞检查与修复：在红队攻击过程中，会采用 0day 漏洞或 nday 漏洞的方式来进行渗透，这些漏洞可能来自终端、服务器、业务系统、数据库、中间件、网络设备等，甚至是来自安全设备本身。对系统进行安全检查，并对漏洞做修复处置，确保网络环境不存在中、高危漏洞，提高红队攻击门槛。

敏感信息处置：红队在信息收集阶段，会尽可能多地收集信息，以寻求最为简捷的攻击路径。而防守方组织架构信息、成员个人信息、信息化资产信息、开发和运维文档资料乃至业务系统源码都是红队的收集目标，这些资料可能存储在服务器、用户终端、移动存储介质、邮箱、网盘，或是以纸质形式保存。应对这类敏感信息做全面排查，并采取有效措施分级分类管控。

供应链风险管理：受攻击目标局限性影响，供应链攻击在实网攻防演练场景的门槛相对较高，且存在较多的不确定性。通常情况下，红队会将安全建设能力较强的防守方作为攻击目标。但是由于供应链攻击危害较大且隐蔽性很强，因此，对于供应链风险同样不能掉以轻心，需建立科学的流程来管理供

应商及其产品的引入和使用。

安全宣贯培训：网络钓鱼或近源渗透考验着防守方全体职员。一些单位成员因为缺乏安全意识而成为了红队攻击的突破口,一旦该成员掌握着敏感信息，则会给防护工作带来严重的威胁。因此，有必要通过宣贯、培训等方式来增进全员安全意识，强化全员网络安全行为习惯，构筑防守工作牢固基石。

2、攻防预演

网络安全攻防预演是对准备阶段工作的检查和确认，通过模拟真实场景下的网络安全攻防对抗，检验整改和加固工作的有效性，发现安全防护体系存在的不足，同时通过攻防预演，提升单位防守团队分析研判能力和应急响应处置能力。在攻防预演工作结束后，需尽可能完整地对发现的问题进行整改。

3、正式对抗

在正式攻防对抗阶段，需重点加强防守过程中的安全保障工作，各岗位人员各司其职，按照实网攻防演练期间安全事件应急响应流程高质量、高效率完成监测、分析、阻断、修复、溯源、报告等各个环节的任务，必要时引入外部专家团队获取支持。防守过程中，需重视自动化设备和自动化工具，提高安全事件响应处置效率。

此外，单纯防御了来自红队的攻击仅仅是确保自己不会失分，而近些年的计分规则变化导致了守住“自家大门”只是底线。高质量的防守队伍不仅能发现和消除威胁，还能对威胁进行有效溯源，获取攻击者信息，形成画像，并对攻击方进行反制。

4、复盘总结

全面总结本次攻防演练各阶段工作情况，形成总结报告。规划问题整改任务，并按计划逐步逐项落实，不断完善自身网络安全防护体系，推进网络安全运维运营“实战化，体系化，常态化”建设。

Part5.
2022 年蓝队防守能力进阶指南

经过多年的安全能力建设，蓝队的安全防守水平较以前有了显著提升，不断增强网络安全攻防对抗实战能力，并将防守实践转化为常态化的安全运维运营能力，已经能够有效应对大部分常规网络攻击。

然而，近年来更为组织化和团队化的 APT 攻击手法也在红队中广泛应用，这类攻击通常采用内存/漏洞利用、无文件、内存马等新型手段，结合社工钓鱼等方式，具有高迷惑性、高隐蔽性、高成功率等特点。要想有效应对这类威胁，除了需要提升单位全员的网络安全意识外，还需要采用更为先进的安全防护手段。

安芯网盾核心团队深耕未知威胁检测技术领域多年，推出了以内存安全产品和与邮件安全联防预警系统（M01）为基础，以安全服务专家团队为保障，用“技术+服务”模式，构建主机+终端的一体化端点安全解决方案，建立运行时安全防护能力，能有效应对来自红队的高级攻击手段，并能形成常态化的高级威胁检测和防护能力。

1. 无文件攻击防护

无文件攻击常见于 PC 终端，攻击者通常利用钓鱼邮件或是某些软件漏洞发起攻击，并调用 Powershell、WMI、PsExec 等系统自有工具远程下载执行恶意命令，具有隐蔽性强、攻击成功率高、破坏力大、溯源困难等特点。基于特征签名、网络流量、系统日志的传统检测手段很难有效应对无文件攻击，很多勒索病毒、挖矿木马甚至恶意后门程序均是通过无文件攻击实现。

内存保护系统无文件攻击防护模块以行为分析为核心，深入脚本解释器内部，监控脚本执行行为，通过发现脚本敏感动作，结合上下文关联，能有效检测和发现无文件攻击行为，并能对攻击进行阻断。检测过程不依赖特征签名、网络流量、系统日志等静态特征，有效降低了因混淆、变种导致绕过的概率。

◆ 无文件钓鱼专项方案

立足邮件安全综合防护需要，安芯网盾配合公安部第一研究所开发了邮件安全联防预警系统 M01。通过在本地部署邮件网关和威胁样本异常行为分析系统，依托“云端”威胁情报共享平台、威胁样本异常行为分析和专家运营服务团队，有效解决实战攻防对抗过程中人员安全意识参差不齐、难以全面应对邮件钓鱼及恶意程序攻击、预警不及时等痛点问题，大力提升了应对社会工程学攻击的防护水平。

2. 漏洞利用攻击防护

漏洞攻击是近年来安全事件频发的根源，据国家信息安全漏洞共享平台（简称：CNVD）统计查询数据库显示，2021 年共收录漏洞 26562 个，其中高危漏洞达 7284 个。攻击者利用漏洞获取计算机权限、盗取敏感数据、破坏软硬件系统等行为均可称为漏洞攻击，漏洞攻击可导致系统或应用数据遭受泄密、窃取、篡改等威胁，漏洞防护能力直接影响了系统的安全，如何在没有补丁的情况下防止漏洞利用成为信息安全攻防对抗领域的迫切需求。

二进制漏洞攻击技术门槛相对较高，需要攻击者对操作系统底层有深刻的理解。由于内存读、写、执行行为对传统防护手段不可见，因此这类攻击更容易绕过现有安全防护体系。常见的内存/漏洞攻击有缓冲区溢出、ROP 攻击、堆喷射、栈翻转等。

内存保护系统通过对内存的读、写、执行行为进行细粒度的监控，实时检测和发现漏洞利用攻击（尤其是内存破坏型漏洞攻击），并对恶意行为进行阻断，从而有效缓解了漏洞利用攻击。内存保护技术对威胁的识别检测不依赖于文件的静态特征，而是基于程序的动态内存访问行为和程序执行行为，这使得本技术对已知威胁和未知威胁的检测效果是一样的，因此它在应对 0day 漏洞效果相对理想，做到了“未雨绸缪、防患于未然”。

3. 内存马攻击防护

内存马因其隐蔽性强、成功率高而备受攻击者青睐，不仅被网络黑客广泛应用，还成为近两年实网攻防演练中的红方标配手段。在前面提到，目前对内存马的防护比较有效的方式是 RASP 技术，RASP 已演变成一个成熟的应用程序内部安全性概念，它可以根据开发人员希望在应用程序或服务器中实现 RASP 安全层的方式（如 Servlet 过滤器、二进制工具、JVM 的替换、虚拟化）来消除威胁。安芯网盾在 2021 年年初推出的基于内存保护+RASP 的内存马攻击防护解决方案（web 服务器安全解决方案），与传统 RASP 产品相比，内存保护系统具有以下几个优点：

- ✓ **数据分析过程主要在 Web 容器外部进行，最大限度降低对业务内存的占用，降低影响，确保业务系统运行的稳定性；**
- ✓ **采用轻侵入模式，部署或升级过程均不涉及业务系统重启；**
- ✓ **基于行为链结合内存行为进行判断，提升检测精确度，降低误报；**
- ✓ **能通过动态检测发现内存马攻击，防止被绕过；**
- ✓ **能通过静态检测发现内存中已驻留的内存马。**

4. 域控攻击防护

自 2020 年推出 AD 域控攻击防护解决方案以来，安芯网盾已帮助众多政企客户解决在 AD 域中面临的安全及运营问题，通过持续不断的能力迭代，内存保护系统在域控方面具备攻击防护和风险检测两大能力。

其中攻击防护能力包括 PTH 攻击防护、Netlogon 漏洞利用攻击防护、黄金票据攻击防护以及 lsass 进程防护等。

风险检测能力主要是对一些日志关闭、日志删除、用户新增、用户提权、策略修改等方面的敏感操作行为进行监测，具体如下表 5：

表 5 安芯网盾在域控防护方面的功能列表

功能	功能描述
域控探测检测	检测发现使用 SAMR 查询敏感用户。
	检测发现使用 SAMR 查询敏感用户组。
	检测发现 PsLoggedOn 消息收集。
	检测发现 AS-REP Roasting 流量攻击。
	对 Lsass 进程内存异常访问行为的主动防御及告警。
	检测发现显式凭据远程登录行为。
	检测发现 Kerberos 票据加密方式降级攻击。
域控权限提升	检测发现域控 ACL 修改行为。
	检测发现针对域控的 MS17-010 攻击检测。
	检测发现针对域控新增组策略监控。
	检测 MS14-068、CVE2020-1472 等域控漏洞提权利用。
	检测发现域控敏感用户组修改行为。

	检测发现域控新增系统服务行为。
	检测发现域控新增计划任务行为。
	对黄金票据进行实时检测。
域控防御绕过	检测发现域控事件日志清空。
	检测发现域控事件日志服务被关闭。
攻击检测	根据指定的 IP 白名单对域管的登录行为告警。
	PTH 的登录行为和手法进行监控告警。
	支持告警日志 syslog 对接。
	对 Powershell、WMI、VBS 等攻击进行拦截。
	检测内存代码片段攻击，可内存的异常行为进行拦截。
	具备 RCE 远程代码执行漏洞攻击防护能力。
	对二进制 0DAY 漏洞进行防御和攻击拦截。
	检测常用文档编辑器漏洞利用攻击行为并拦截。
	具备可信环境监测能力，可监测 Bootkit 和 Rootkit 行为。
	防御远线程注入、傀儡进程、隐藏进程等进程攻击行为。
资产管理	统一查看域控资产信息。

5. 红队工具防御

针对攻击方常用的 cobalt strike、MSF、Godzilla、Behinder 以及 Mimikatz 等常用工具，安芯网盾能够提供对应的防护能力。

表 6 红队工具防护能力列表

工具名称	识别范围	识别详情
Cobalt Strike	识别 vba、ps1 等格式的恶意载荷，hta 格式的 vba 和 ps1 恶意负载。	• HTML Application（HTA）形式的 VBA 或 Powershell 攻击 • MS Office Macro 形式的 VBA 攻击 • Payload Generator 形式的 Powershell 攻击
Mimikatz	可识别窃取 win 系统密码明文或 Hash、浏览器密码、RDP 密码、防追踪溯源等恶意行为。	• 禁用系统日志记录的行为 • 读取 win 系统密码、浏览器密码、远程连接密码的行为 • 清空日志的行为
Psexec	可识别应用远程的行为	应用执行远程的行为
冰蝎/哥斯拉/蚁剑	可识别利用第三方 webshell 工具进行内存 webshell 注册、webshell 利用等行为	• 注册内存组件 • So 加载 • 敏感文件访问 • 命令执行 • 拖库行为 • 启动虚拟终端 • 内存 Jarload 加载
MSF	可识别 Meterpreter 的攻击行为。	可识别 MeterPreter 组件建立时的内存 DLL 注入行为

Part6.
典型实战演练案例

1. 某大型集团实战案例

1.1 漏洞利用攻击

攻击手法：Purple Fox × 二进制漏洞+无文件攻击

某大型科技企业在终端环境部署了 10 万多点内存保护系统，在企业内部攻防演练期间出现告警信息，提示某台 PC 机上发现脚本执行 HTTP（GET）请求等一系列敏感行为链，并把它定性为含漏洞利用的攻击行为。经安全专家进一步研判，确定该攻击为 Purple Fox 下载型木马的升级版所为，其攻击行为的感染链如下图 3。

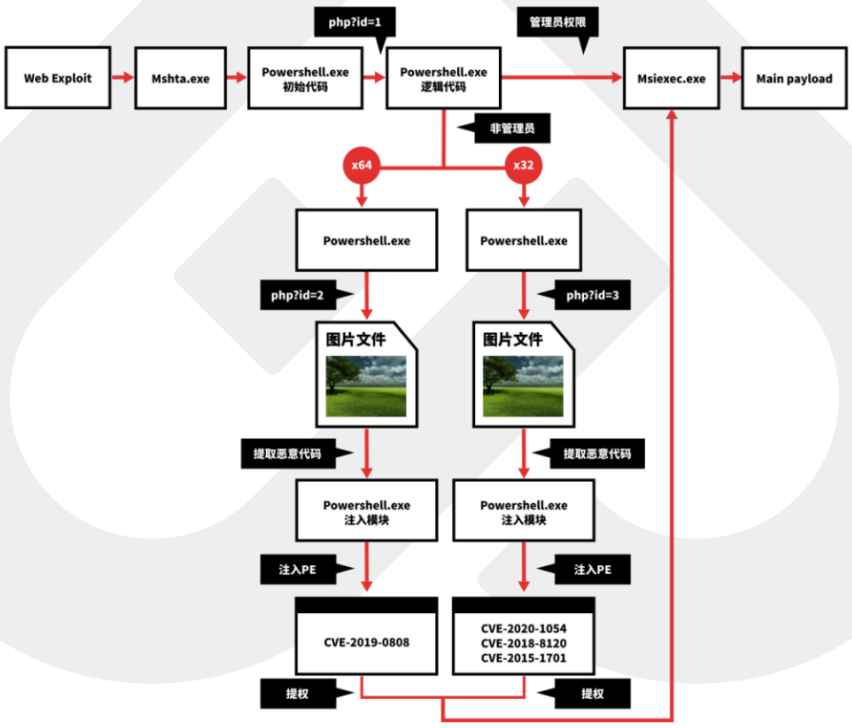

图 3 感染链

整个攻击过程，攻击行为都在内存中进行，通过调用 PowerShell 工具，帮助攻击者实现无文件攻击，利用的漏洞均为危害性极高的二进制漏洞（CVE-2020-1054，CVE-2019-0808，CVE-2018-8120，CVE-2015-1701）。如果此次未拦截成功，客户将可能面临各种恶意入侵的风险，包括信息泄露、挖矿勒索等。同时，该恶意程序安装了 rootkit，使得宿主机上植入的恶意代码更难被发现，以达到长期驻留的目的。

1.2 无文件钓鱼

攻击手法：Emotet × 无文件攻击

北京冬奥会刚刚结束，俄乌冲突第一天。安芯网盾内存保护系统发现客户突遭高频无文件攻击的告警信息，统计数据显示有超过三万余次攻击行为，该攻击通过钓鱼邮件投放 Excel 文档附件，用户打开附件后将在内存中执行恶意行为，攻击手段较为隐蔽，能够绕过大部分安全防护手段，恶意 Excel 文档运行后的进程树如下图 4。

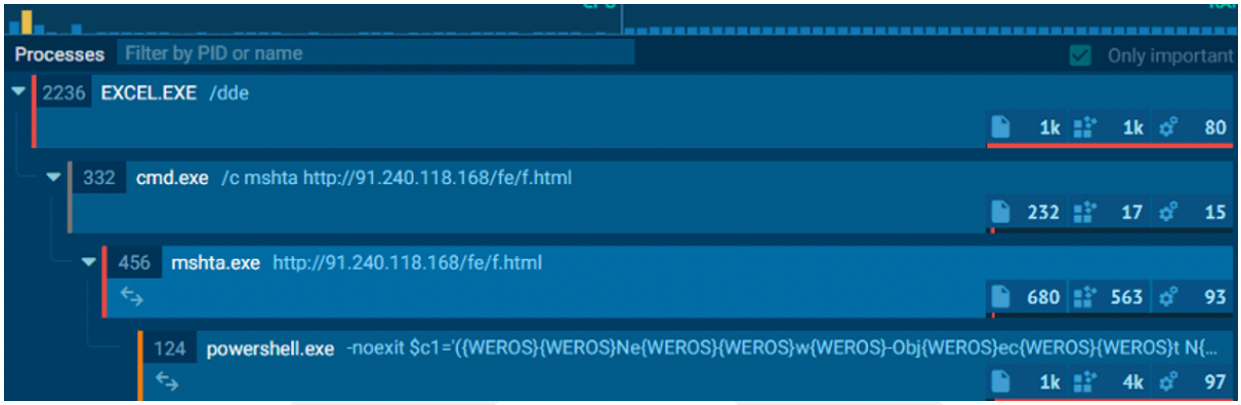

图 4 进程树

在整个攻击事件中，攻击者利用邮件附件传播，用户打开该 Excel 文档并启用宏后，宏代码会启动 cmd.exe。cmd.exe 运行 mshta.exe 解析某 html，下载和执行 PowerShell 恶意代码，该恶意代码会将恶意载荷下载到内存并执行，实现无文件攻击。其最终目的是下载并执行 Emotet 远控木马，控制被攻陷的主机。

2. 某政府机构演练案例

攻击手法：Mimikazt 攻击工具+票据攻击

某政府机构客户内网中存在大量的域控服务器，利用域控服务器管理全国分支机构的十万多台主机终端，便捷了很多。但是，在过去的攻防演练中，红队利用漏洞或者社工等方法获取了外网系统的控制权限，找到了和内网联通的通道，再进一步进行深入渗透，便形成了纵向渗透的通道。然后通过 mimikazt 等工具利用票据传递等攻击手段，实现域控服务器的权限控制，从而访问任意域控下的目标进行数据窃取，最终完成目标突破工作。

在了解到该政企单位的痛点需求之后，安芯网盾为该客户部署了内存保护系统，通过分析内网渗透中常用的技术方法，技术甄别判断黄金票据、PTH、白银票据、暴力破解域用户名密码、内存 dump 等行为，实时检测并拦截了攻击方利用 Mimikazt 攻击工具获取被攻击的域控服务器中的 krbtgt 账户的 hash 值的行为，实时上报异常登录等风险项，同时通过策略调整解决身份认证的黑白名单控制问题，实现用户自定义设置对域控服务器的安全访问机制，帮助客户更清晰、准确、快速地发现、拦截、追

溯攻击者的攻击。

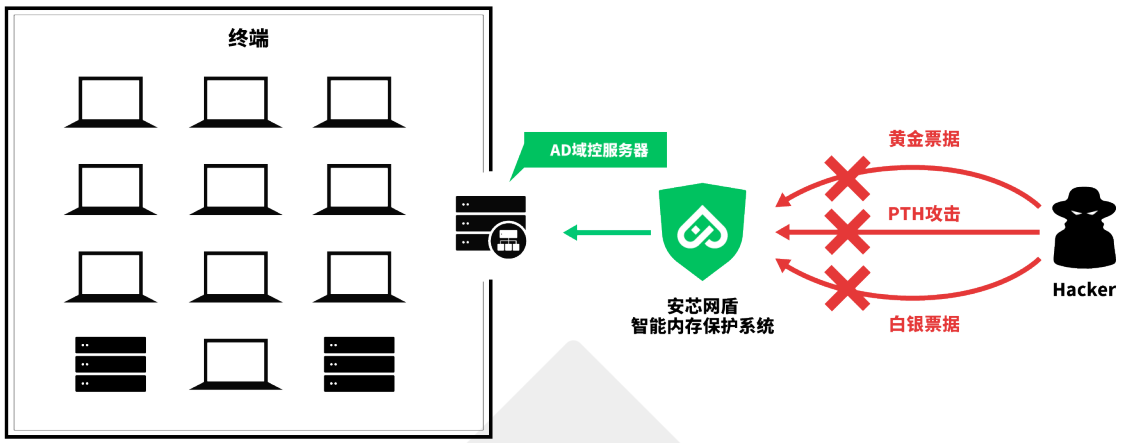

图 5 内存保护系统部署图

3、其它案例

3.1 浏览器 0day 漏洞案例分析

攻击手法：量子攻击× APT-C-40

美国国家安全局（简称 NSA）官方机密文档《Quantum Insert Diagrams》内容显示，Quantum（量子）攻击可以劫持全世界任意地区任意网上用户的正常网页浏览流量，进行 0day 漏洞利用攻击并远程植入后门程序。

通过分析 NSA 官方机密文档《NSA Ant Product Catalog》、《NSA QUANTUM Tasking Techniques for the R&T Analyst》、《QUANTUM Shooter SBZ Notes》，发现 Quantum（量子）攻击系统的核心攻击方式大致如下：

1. **准备阶段：**将攻击平台 FoxAcid（酸狐狸，仿冒网站）服务器部署在互联网骨干网中，在网络传输线路上建立被动监听节点 TurMoil（混乱，后门监听系统）。
2. **劫持阶段：**在受害者访问特定网站(如脸书,推特等)时,TurMoil 会监听该网络流量,通过 Turbine（后门植入工具）发送 Quantum（量子）注入攻击，迫使受害者访问 FoxAcid 服务器。
3. **攻击阶段：**通过 FoxAcid 服务器发起攻击，利用受害者终端使用的浏览器 0day 漏洞，植入 NSA 专属后门程序。
4. **驻留阶段：**通过植入受害者终端的 NSA 专属后门程序如 VALIDATOR (验证器)、UNITEDRAKE(联合耙)等大量窃取受害者个人隐私和上网数据等内容。

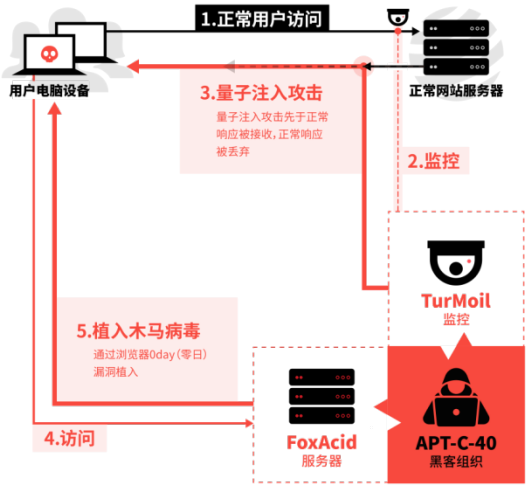

图 6 攻击链条

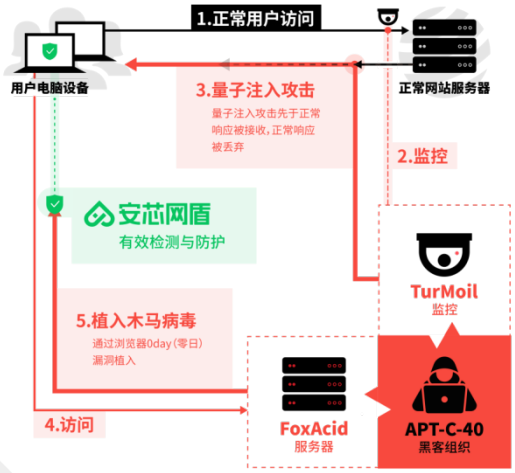

图 7 防御链条

通过上述分析可以发现，Quantum（量子）攻击系统发起最终攻击的主体是 FoxAcid（酸狐狸）服务器，而它的攻击方式是在受害者通过浏览器访问该 FoxAcid 服务器时，FoxAcid 通过浏览器 0day 漏洞向受害者终端中植入后门。

过去两年，安芯网盾发现攻击者利用浏览器 0day 漏洞实施攻击的案例非常多，安芯网盾内存保护系统的核心能力之一即是防止浏览器 0day 漏洞被利用。

3.2 Apache Log4j 漏洞利用

攻击手法：Apache Log4j2× RCE 新漏洞

安芯网盾监测到 Apache Log4j2 官方发布的远程代码执行漏洞 CVE-2021-44832，攻击者通过将恶意的 JNDI URI 数据源写入 JDBC Appender 中，通过该 JNDI URI 可以远程加载代码并执行。

安芯网盾研究人员复现了该漏洞攻击，验证了安芯网盾内存安全产品的内存马防护模块可以在不做任何升级的情况下检测该漏洞攻击。虽然，Apache Log4j2 官方已发布了可更新版本，该漏洞利用的风险一般，但是我们也看到自 Log4j2 漏洞事件（CVE-2021-44228）爆发以来，黑客利用 Log4j 漏洞展开大面积漏洞利用攻击，数以百万的服务器面临巨大安全风险。

图 8 Log4j2 检测图

附 2021 年实网攻防演练战绩

守护客户服务器：100,000+台，成功拦截攻击：1591 次

部分关键攻击拦截：

攻击类型	次数
Java、PHP 内存马攻击	112 次
远程漏洞溢出攻击	78 次
执行 Shellcode 攻击	109 次
Powershell 无文件攻击	98 次
PTH 哈希传递攻击	80+次
恶意登录、密码破解行为	450+次

部分关键漏洞拦截：

漏洞类型
Chrome　0day 漏洞利用
Weblogic　rce 漏洞利用

PS：更多案例详情，可联系安芯网盾商务同事为您介绍。

Part7.
关于安芯网盾

安芯网盾是内存安全领域的开拓者和领军者，致力于为政府、金融、运营商、军工、教育、医疗、互联网及大型企业等行业客户提供新一代高级威胁实时防护端点安全解决方案，帮助企业防御并终止无文件攻击、0da 漏洞攻击、内存马攻击等高级威胁，切实有效保障用户的核心业务不被阻断，保障用户的核心数据不被窃取，已为百度、海关、金山、华为云等众多国际知名企事业单位持续提供服务。

产品+服务双重守护，助力攻防演练+日常防护

即刻咨询: 400-900-6609

www.anxinsec.com

扫描二维码申请试用