OWASP
Open Web Application Security Project

天狗漏洞攻击防护系统

刘　磊

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

安全能力中心
SECURITY CAPACITY OUTPUT CENTRE

OWASP
Open Web Application
Security Project

目录

- 当前的安全形势
- 现在的安全技术
- 全新安全理念
- 新技术的应用
- 产品介绍

OWASP
Open Web Application
Security Project

当前的安全形势

- 我们安全吗?

他们都曾经以为自己很安全：但危害就发生在安全防护之下

2020年Q1

美国国防系统信息局、天然气管道商、钢铁制程商、铁路轨道与运输系统供应商遭受勒索软件攻击；拉斯维加斯市、拉辛市遭受网络攻击……

2020年Q2

日本本田汽车、任天堂、三菱电机等公司被攻击；欧洲能源、以色列水利、伊朗港口、委内瑞电网被攻击；美国系统芯片制造商、移动运营商、佛罗伦萨市被攻击……

2020年Q3

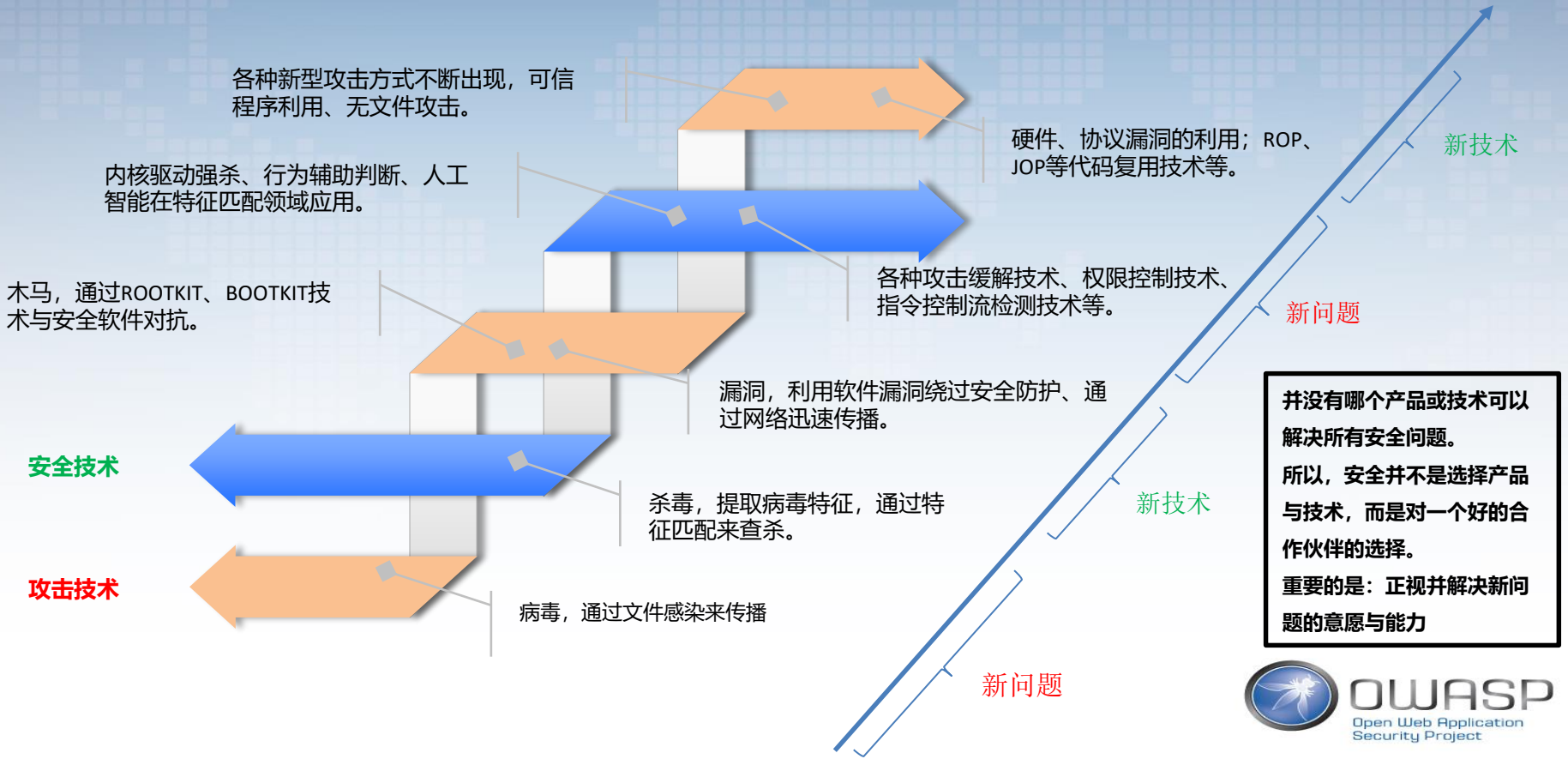
Telegram、美高梅酒店、雅芳、佳能、Intel、LG、Razer、微软被攻击导致数据泄露；全球领先晶圆大厂X-FAB被攻击停产；特斯拉、佳明、CWT等公司被攻击……

2020年Q4

美国网络安全公司FireEye被攻击、瑞典的安全公司GunneboAB遭受攻击；温哥华因网络攻击公交系统瘫痪；APT组织黑进美国政府网络……

安全事件

安全是一个动态攻防过程：没有无坚不催的矛也没有牢不可破的盾



并没有哪个产品或技术可以解决所有安全问题。
所以，安全并不是选择产品与技术，而是对一个好的合作伙伴的选择。
重要的是：正视并解决新问题的意愿与能力

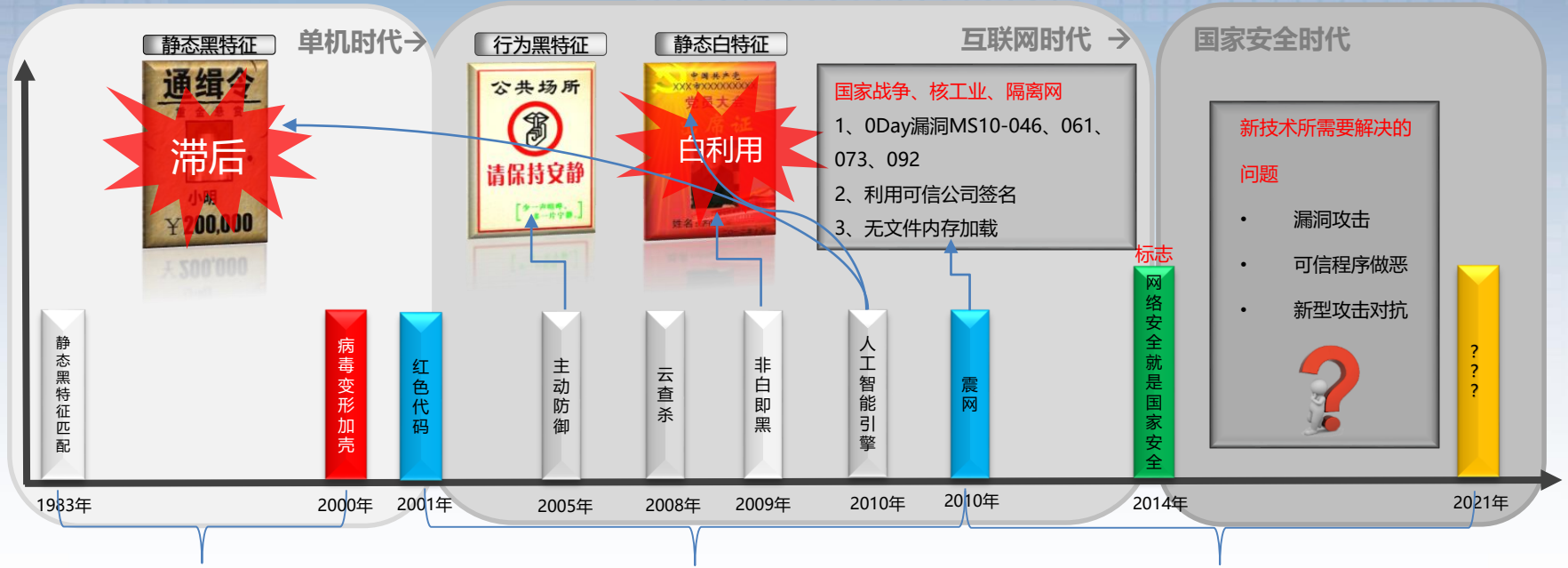
OWASP
Open Web Application Security Project

OWASP
Open Web Application
Security Project

现在的安全技术

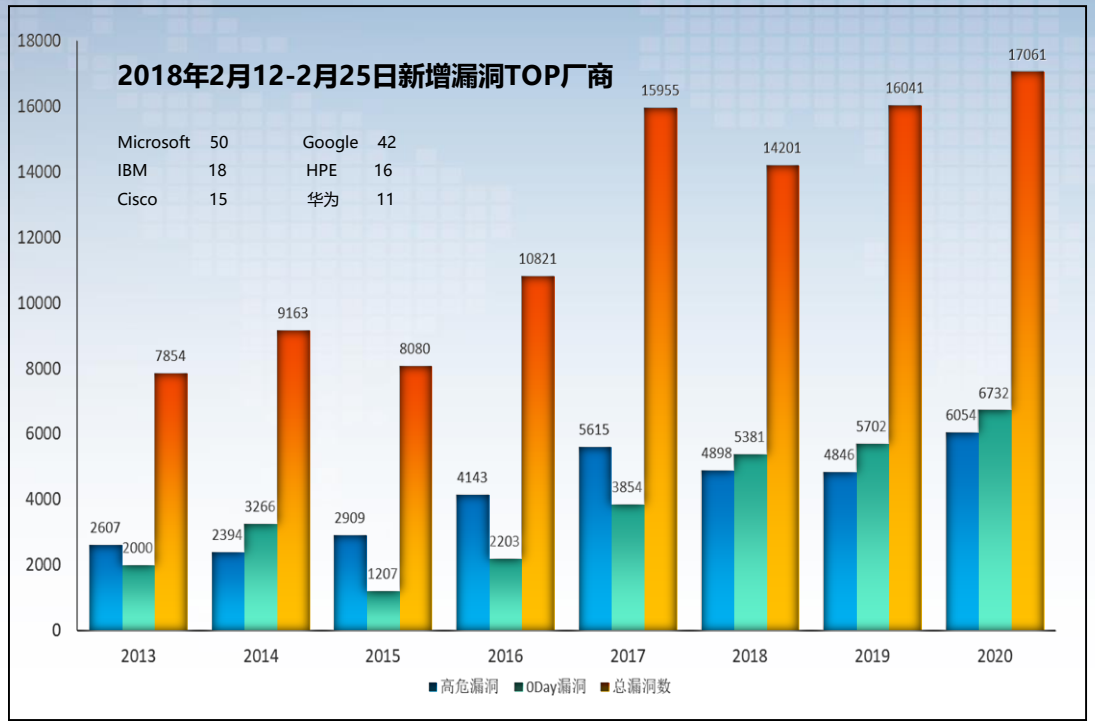
- 当前安全技术是否能解决来自漏洞的威胁?

国家力量的介入与网络战争的开启：网络安全正式进入新时代



一切攻击都是基于漏洞的：漏洞补丁并不能有效的解决漏洞攻击问题

数据来源：CNVD

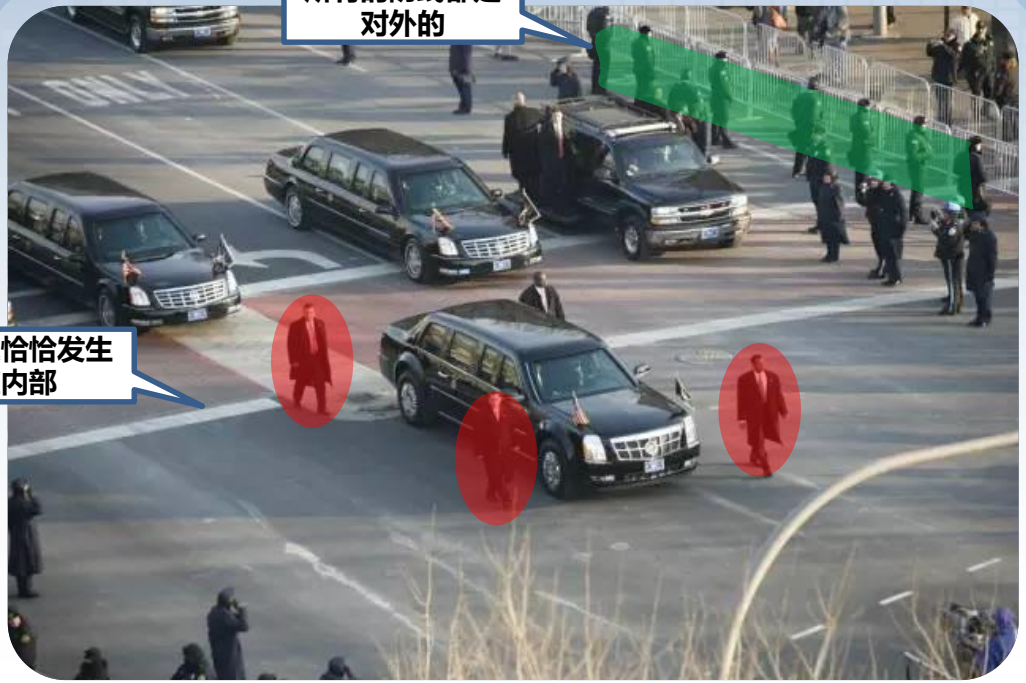


每一个重大安全事件背后，都有着一个高危漏洞的身影：

- 2003年，冲击波病毒利用了MS03 - 026漏洞。
- 2004年，震荡波病毒利用了MS04 - 010漏洞。
- 2008年，Conficker病毒利用了MS08 - 067漏洞。
- 2010年，震网病毒利用了MS10 - 046漏洞。
- 2017年，勒索病毒利用了MS17 - 010漏洞。

OWASP
Open Web Application Security Project

现在的安全技术，为什么解决不了漏洞攻击问题?

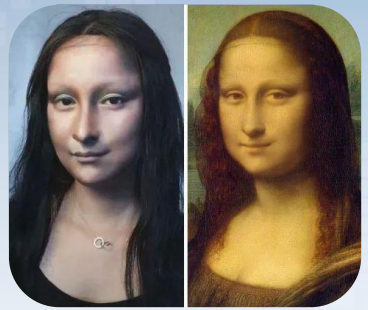


漏洞攻击的实质，其实就是控制“可信程序”来执行恶意指令。

其继承了漏洞所在程序的一切特权。

OWASP
Open Web Application Security Project

攻防技术不匹配是根因：我们需要新一代的安全技术来解决新问题



当用外观已经完全不能区分一个人时，进入微观层次，使用DNA来识别已是必须的选择。

肉眼识别

VS

DNA检测

漏洞利用：

“可被利用的代码缺陷”称之为漏洞，漏洞攻击发生在程序的“内存指令层”，是攻击者利用程序的代码缺陷，让攻击指令执行，并拿到控制权的过程。异常发生在内部，外在并无表现。

安全技术：

当前安全技术的检测，则大多是针对“文件、进程、行为、权限”的表层检测，未能深入到“内存指令层”对攻击代码及指令进行检测。

OWASP
Open Web Application Security Project

OWASP
Open Web Application
Security Project

新技术理论体系的探索

- 如何利用新技术来解决现有技术不能解决的安全问题?

安全技术新方向-基于指令调用序列检测的安全引擎“天狗”

- 炮火在哪里，我们就应该在哪里，即然漏洞攻击都发生在内存指令层，那我们的安全检测与防护，亦应该下沉入内存指令层。

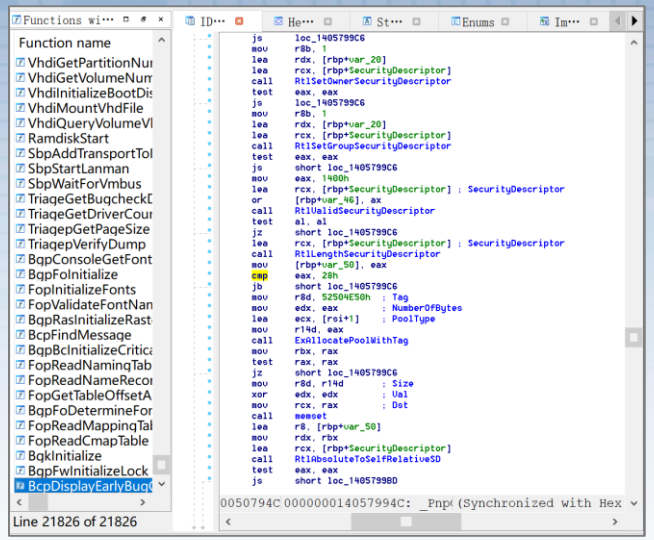
- 基于指令检测的理念，在国际上曾有过相关的研究，2005年加州大学和微软公司提出了控制流完整性（Control Flow Integrity, CFI）的防御机制，用于解决ROP攻击问题。

- 2017年，永恒之蓝事件之后，天狗引擎正式立项，目标是：基于内存指令调用序列检测技术解决0Day漏洞攻击问题

0day漏洞攻击为什么难以发现?

10000+个系统文件

100+个常驻服务

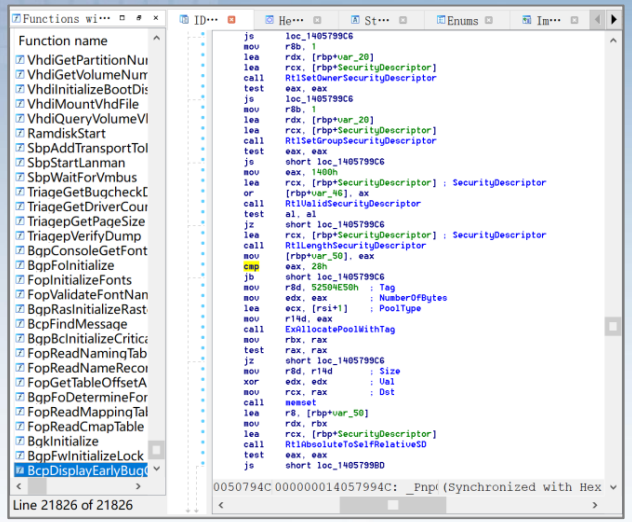


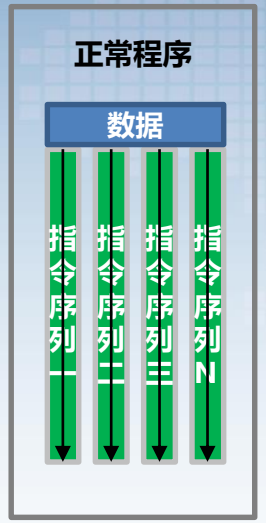
单内核一个文件就有20000+个函数，无数条指令

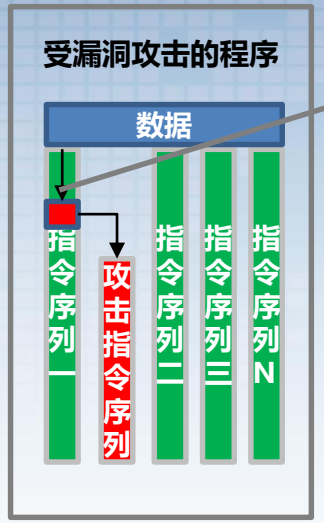
“已知漏洞”的问题容易解决，是因为我们明确的知道漏洞存在于哪一个文件、哪一个函数的哪一条指令中。

而**“未知的0Day漏洞”**难以解决，是因为它有可能存在于任一文件或服务的、任一函数与指令中，已知未知，天差地远。

如何利用指令调用序列检测技术发现0day漏洞攻击?





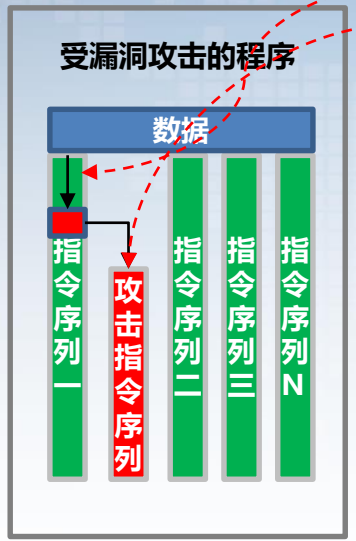


因为“指令序列一”中存在一个漏洞，被攻击者利用后，正常的指令执行序列发生改变，转而去执行攻击者的攻击指令，从而导致危害发生。

由于此漏洞可以发生在任意一个文件的任意一个函数的任意一个指令序列中，所以极其的难以被发现。

利用机器学习与智能采集技术，学习并采集系统中所有可能存在被利用风险的程序的指令序列，并构造成“**指令序列白名单**”，当实际在内存中执行的任意一条指令序列不在白名单中时，即认为是非原生的额外出现的异常攻击指令。如上图所示：当绿色部分都在我们的指令序列白名单中时，红色部分将被充份暴露。0Day漏洞的确是“**未知的**”，但系统及程序却是“**已知的**”，利用已知发现未知，是可行的。

指令调用序列检测技术与传统技术在漏洞防护领域的区别



传统技术的检测逻辑（黑特征或规则匹配：红色部分的特征）：

1、如果代码的执行来源于“指令序列一的xxx位置（漏洞黑特征）”

2、或者“攻击代码符合xxx特征（攻击黑特征）”

那么，这就是一次漏洞攻击。

指令调用序列检测技术的检测逻辑（白特征匹配：绿色部分的特征）：

1、如果所执行的代码并非是已知的可信指令序列“指令序列一 、二、三 直到指令序列N”（指令白特征）

2、或者“虽然是可信的指令，但序列发生变化”（指令白特征）

那么，这就是一次漏洞攻击。

不同的技术，决定了两者存在本质上的区别：

1、无论是漏洞黑特征，还是攻击黑特征，都需要先知道有这个漏洞的存在、先知道有这段攻击代码的存在，才能提取特征。所以，技术原理决定了传统黑特征匹配技术只能解决“已知的漏洞”及“已知的攻击”，且必然存在滞后性，攻击先发生、然后分析、提特征再具备防护能力。

2、指令调用序列检测技术并不需要知道具体的漏洞或攻击代码的特征，只需要学习正常程序的指令序列，技术原理上决定了其可以解决未知漏洞、未知攻击代码发起的攻击。

传统技术可以解决0Day攻击吗？

如果漏洞是未知的，但利用此漏洞的攻击代码却是已经存在，且曾被捕获，并提取了特征的攻击代码，那传统技术也是可以捕获未知漏洞攻击的。

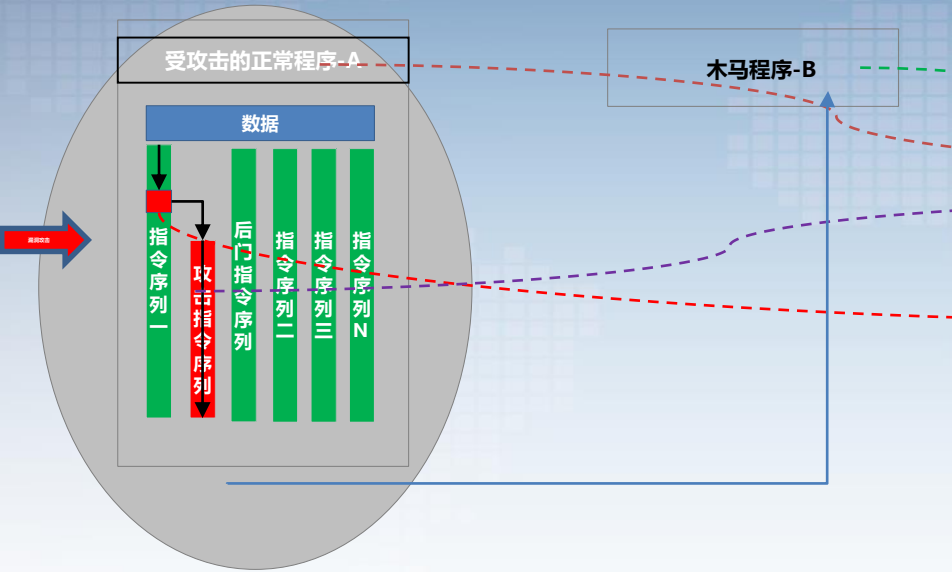
但树桩也曾经撞死过兔子，但捕捉兔子却并不能依赖树桩，那只是运气使然。

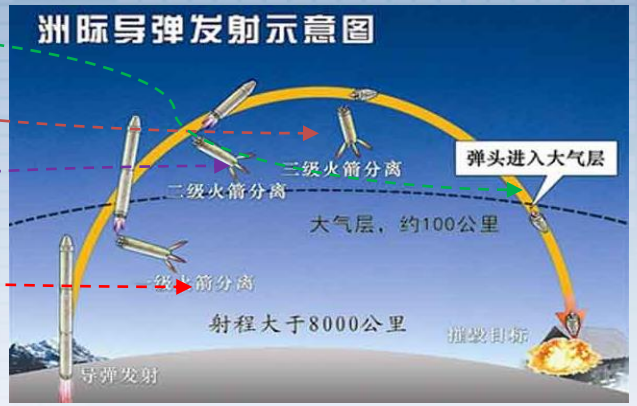
OWASP
Open Web Application
Security Project

新技术的应用

- 新技术可以应用到哪些安全防护领域?

应用场景一：漏洞攻击发现





对发生在更微观层次的，程序内存中的指令调用序列进行安全检测，是漏洞攻击发现新技术的作用领域，也是传统安全防护技术的防护空白领域。

而只有指令级检测才能定位到漏洞所在位置，而只有定位了漏洞，才能真正堵死攻击，否则就是治标不治本，攻击将持续不断的发生。

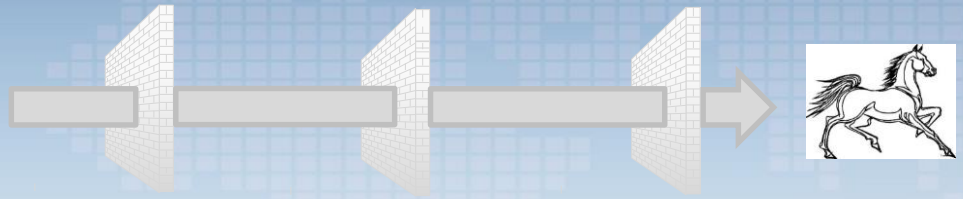
弹头	**木马程序主体** 基于文件检测的杀毒软件可捕获。
三级火箭	**被攻击程序本体** 基于行为检测的EDR/MAC可捕获。
二级火箭	**攻击载荷-ShellCode**：基于指令检测的新技术可捕获。
一级火箭	**漏洞所在位置**：基于指令检测的新技术可捕获。

应用场景二：从实战攻击来看追踪溯源的重要性

理想中的攻击是这样的：

一马当先，冲破层层防护，

悄无声息的，取得最终的胜利。

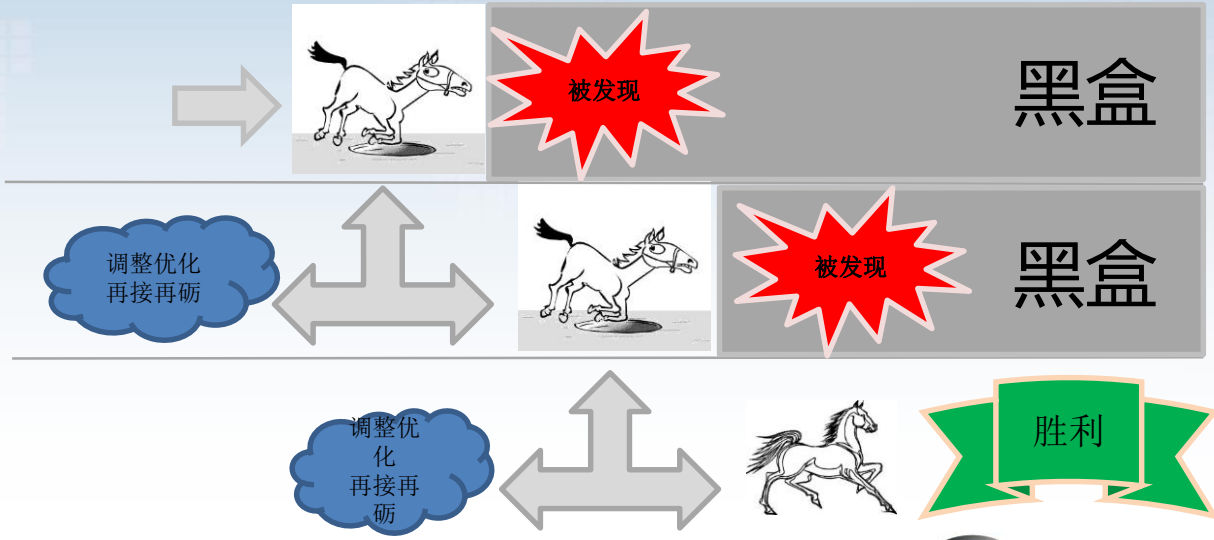


现实中的攻击是这样的：

小心翼翼，层层试探。

不断调整，不断优化。

一马功成，万马枯。



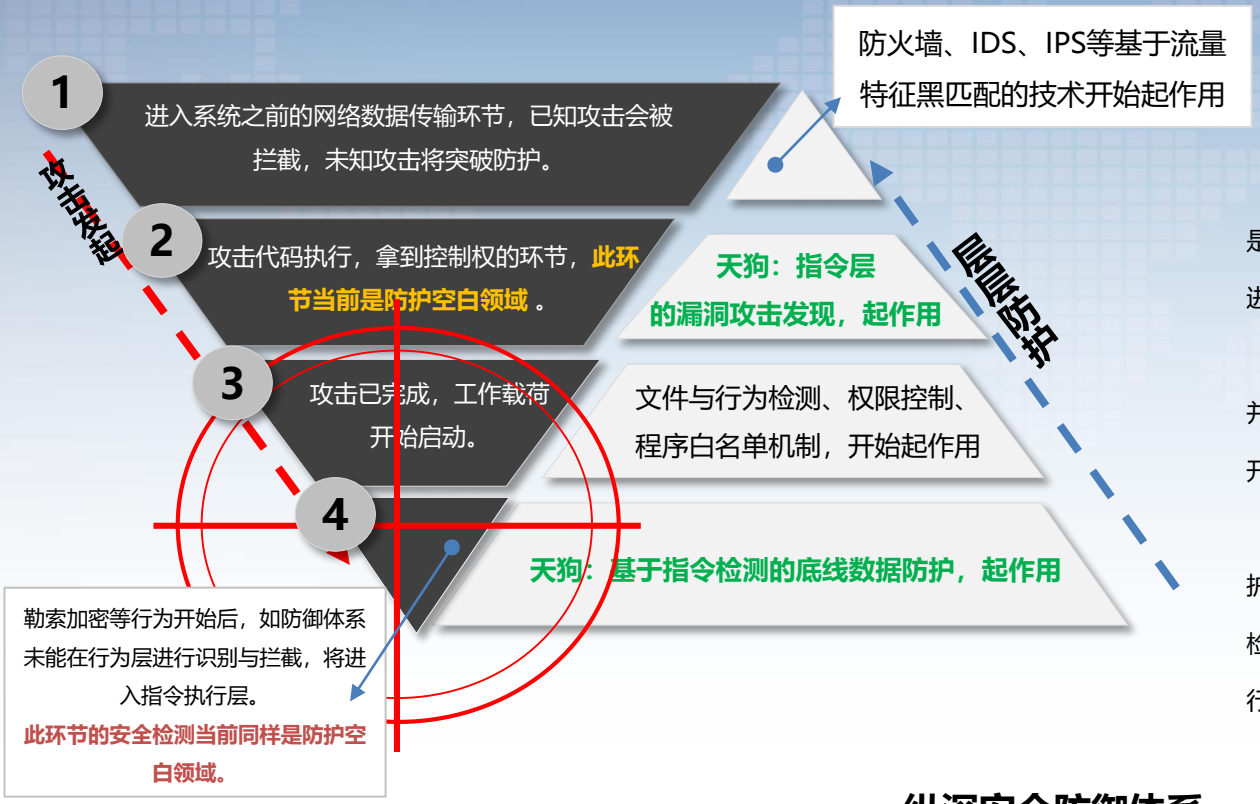
体系化建设：有重叠、但有侧重，没有全能产品，只有针对解决问题的产品

海军编队中，任意一艘舰艇都可以进行攻击，但没有任何一个国家会只造一种舰艇。

在医疗领域，面对细菌感染，也从没有人会质疑，为什么已经有了青霉素，还要研究并生产红霉素、先锋、头孢等同类药品。

在安全领域，仅仅针对终端的攻击方式就有很多种：针对系统漏洞的RCE攻击、针对浏览器漏洞的水坑攻击、针对邮件及文档类程序漏洞的钓鱼攻击等等，但仍然有人会质疑：我已经有了什么了，为什么还要再买什么。

安全是一个体系：安全技术的更新换代，是叠加与补充，而非取代



纵深安全防御体系

当前主流安全技术及产品的作用领域，主要是在“流量层”、“文件、行为、进程权限层”进行安全检测并发挥作用。

但在漏洞攻击发生、攻击指令执行的那一刻，并无有效的防护手段，需要等攻击完成后，才能开始对攻击最后释放的工作载荷进行安全检测。

天狗漏洞攻击防护技术则弥补了这一空白防护领域，在攻击发生时，在内存指令层进行安全检测；在加密文件等最终行为发生后，对指令执行序列的可信度进行检测。

OWASP
Open Web Application
Security Project

天狗漏洞攻击防护系统

- 应用新技术打造全新一代安全产品?

天狗漏洞攻击“系列”防护系统

◆ **产品形态**

管理平台+客户端（支持终端和服务器）

可与天擎一体化安装部署管理，也可单独部署

◆ **天狗系统漏洞攻击防护系统**

RCE攻击防护，防护针对系统的远程代码执行漏洞攻击

◆ **天狗浏览器漏洞攻击防护系统**

浏览器攻击防护，防护针对浏览器漏洞的网页挂马攻击

◆ **天狗文档漏洞攻击防护系统**

本地钓鱼攻击防护，防护针对常用文档编辑程序漏洞的钓鱼攻击

支持适配：平台支持与环境适配

◆ **系统平台支持**

1、Windows全系统

2、Linux、国产化适配支持

◆ **浏览器平台支持**

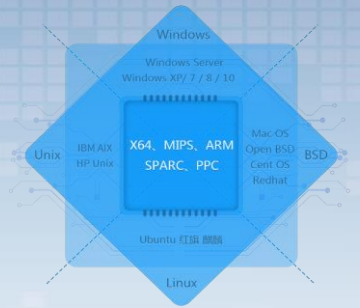
IE、火狐（Firefox）、谷歌（Chrome）、Safari和Opera

◆ **文档处理平台支持**

Microsoft Office WPS PDF

◆ **个性化适配**

根据客户需求进行个性化定制，实现无限可能



OWASP
Open Web Application Security Project


刘磊
北京 朝阳
扫一扫上面的二维码图案，加我微信


BEGIN.

问答时间

Q&A