奇安信

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

BCS2022系列活动-冬奥网络安全“零事故”宣传周

第三代安全防护技术-天狗

李博 奇安信集团安全能力平台部负责人

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

当前安全形式

我们安全吗？

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

这些都只是冰山一角

美情报部门网络攻击证据被发现，外交部：强烈敦促美方解释

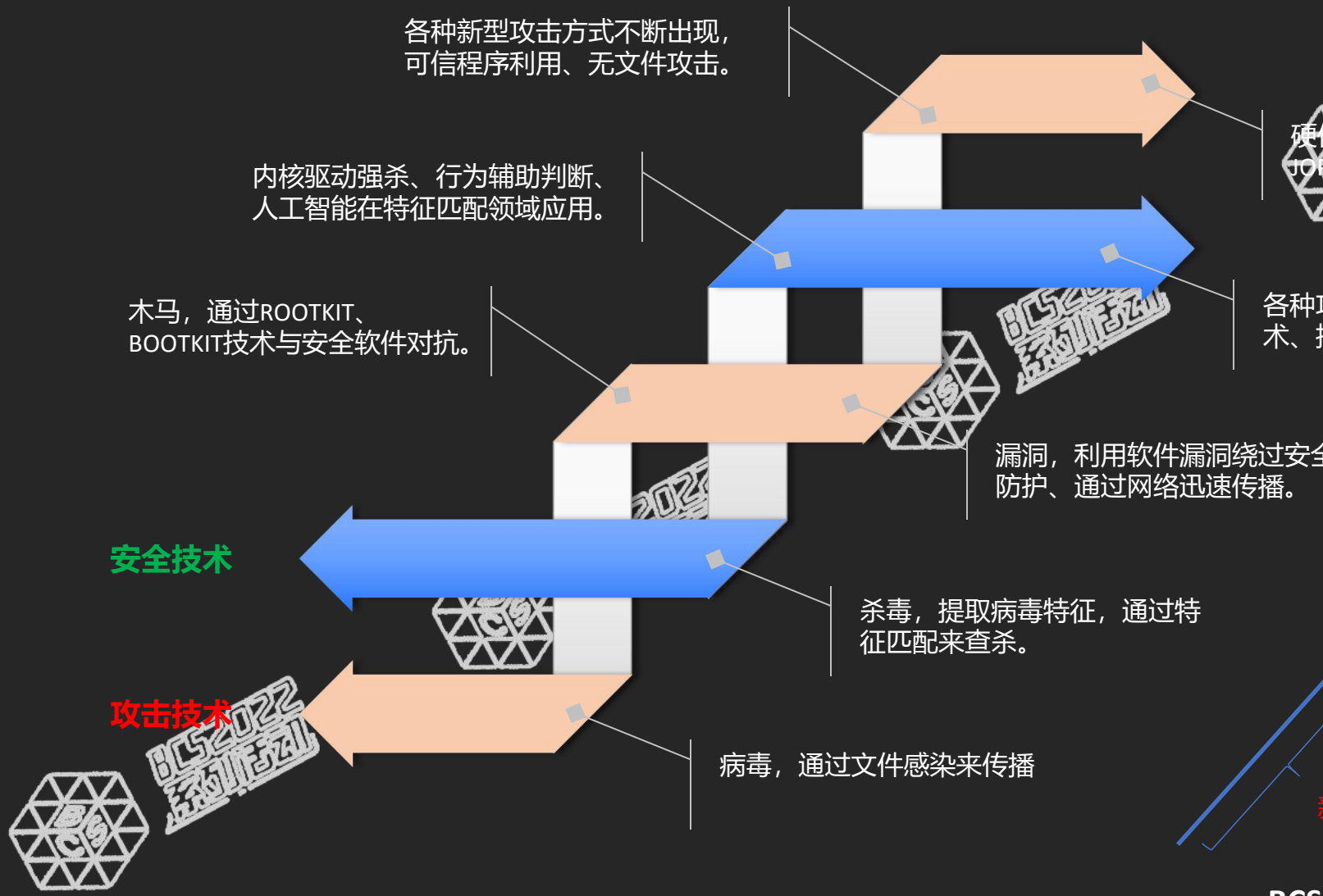
央视新闻 奇安信集团 2022-02-24 19:20

顶级后门再现江湖，随着NSA武器Bvp47后门曝光，再次证实了永恒之蓝、双脉冲星都只是冰山一角。

奇安信

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

安全是一个动态攻防的过程



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。

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

新技术理论体系探索

四大黑科技之首

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

我们需要新技术解决新问题

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。

微观之下、大相径庭

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

用户手动打开Word文档

KERNELBASE! CreateFileW+0x1d1
kernel32! CreateFileW+0x4a
mso! Ordinal1362+0x615
mso! Ordinal1394+0x43f
wwlib! DllGetLCID+0x94ec4
wwlib! DllGetLCID+0xa1de6
wwlib! DllGetLCID+0x94522
wwlib! Osf::OSFCreateOfficeExten.....
wwlib! DllGetLCID+0x326892
wwlib! DllGetLCID+0x17706f
wwlib! DllGetClassObject+0x2e77
wwlib! FMain+0x253
el32! BaseThreadInitThunk...
! RtlInitializeExceptionChain...
ntdll! RtlInitializeExceptionChain...

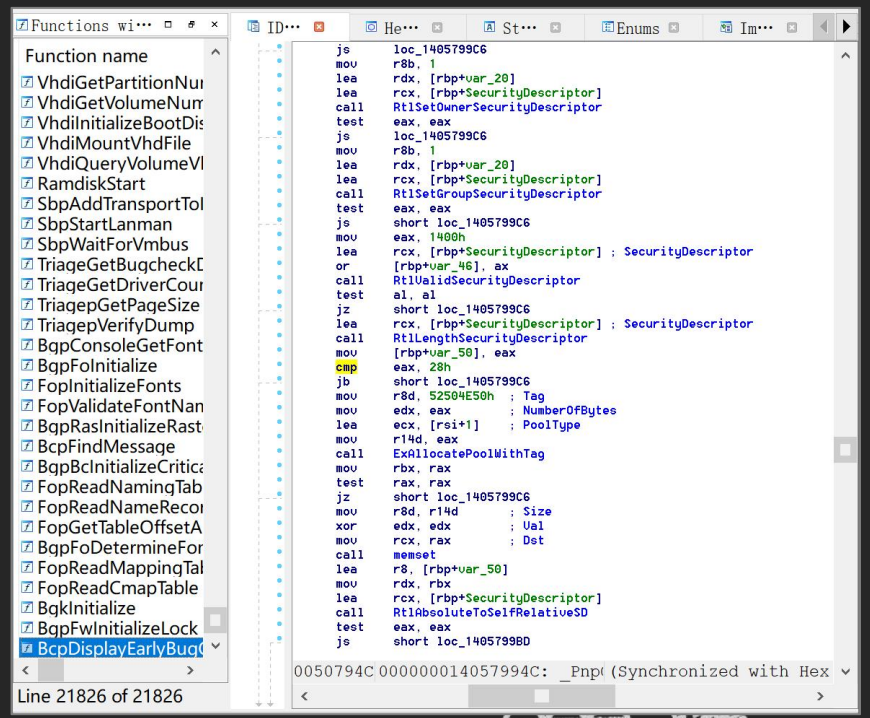
木马控制后打开Word文档

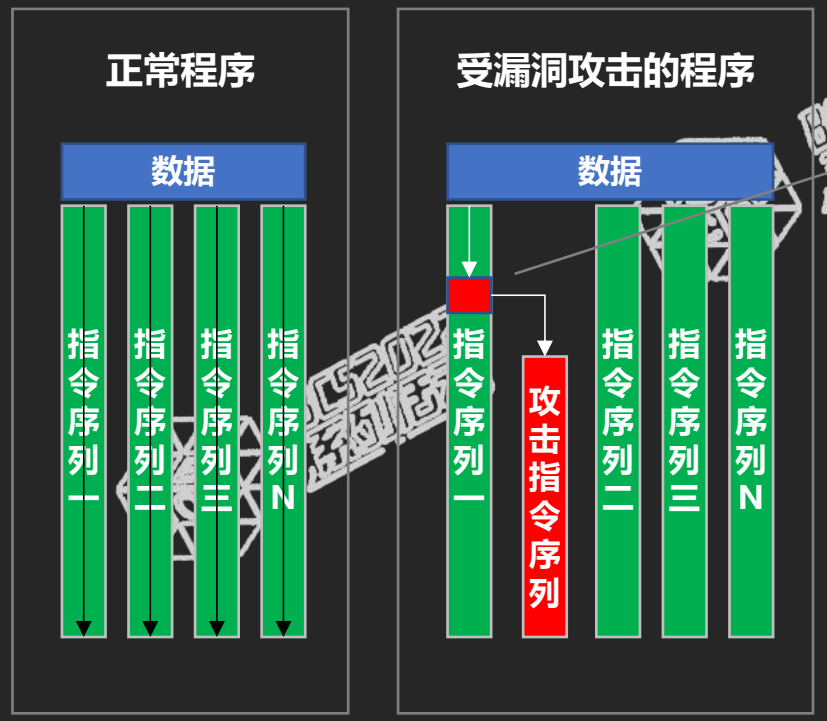
KERNELBASE! CreateFileW+0x1d1
kernel32! CreateFileW+0x4a
ntdll! RtlQueryEnvironmen...
ntdll! LdrResSearchResource...
ntdll! wcspbrk+0x415
ntdll! RtlUlonglongByteSwap...
KERNELBASE! LoadLibraryExW...
KERNELBASE! LoadLibraryExA...
kernel32! LoadLibraryA+0x31
kernel32! BaseThreadInitThunk...
ntdll! RtlInitializeExceptionChain...
ntdll! RtlInitializeExceptionChain...

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

“非白即黑”的指令调用序列检测技术





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。

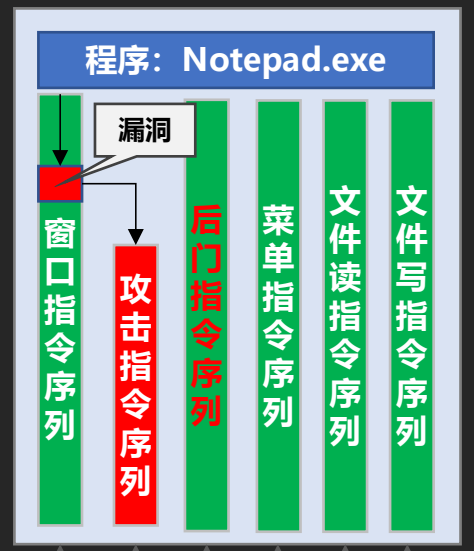
由于此漏洞可以发生在任意一个文件的任意一个函数的任意一个指令序列中，所以极其的难以被发现。

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。

优势一：权限控制精细到了指令层

安全问题-勒索行为发生：Notepad.exe要写“保密文档”是否允许？

传统安全技术以“文件、进程”为单位，进行合法性的判断 **VS** 新技术以“”为单位进行合法性判断，试看两者指令执行序列有何不同？



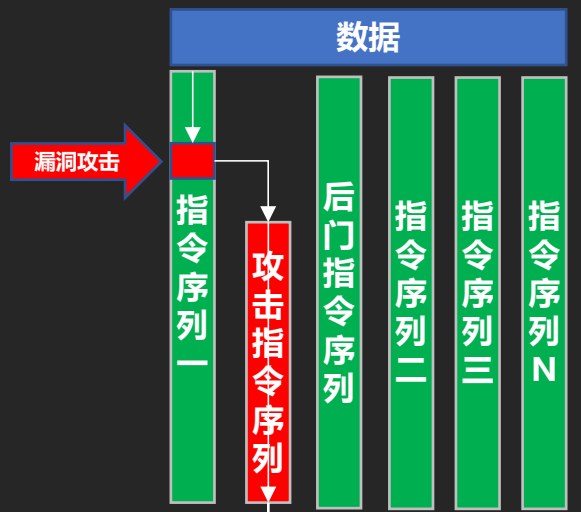
各安全技术对勒索行为的判断逻辑

1. **程序白名单**：**程序主体判断**：Notepad.exe 具备有效的微软数字签名，为可信程序，**允许，勒索成功**。
2. **权限控制**：**程序权限判断**：Notepad.exe 是合法的txt类文件编辑程序，权限具备，**允许，勒索成功**。
3. **指令白名单**：**指令序列判断**：如果是Notepad.exe 中的“**文件写指令序列**”在请求写，则允许，其它的指令序列的请求，则**拒绝，勒索失败**。

优势二：定位漏洞位置，捕获攻击代码

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

受攻击的正常程序-A

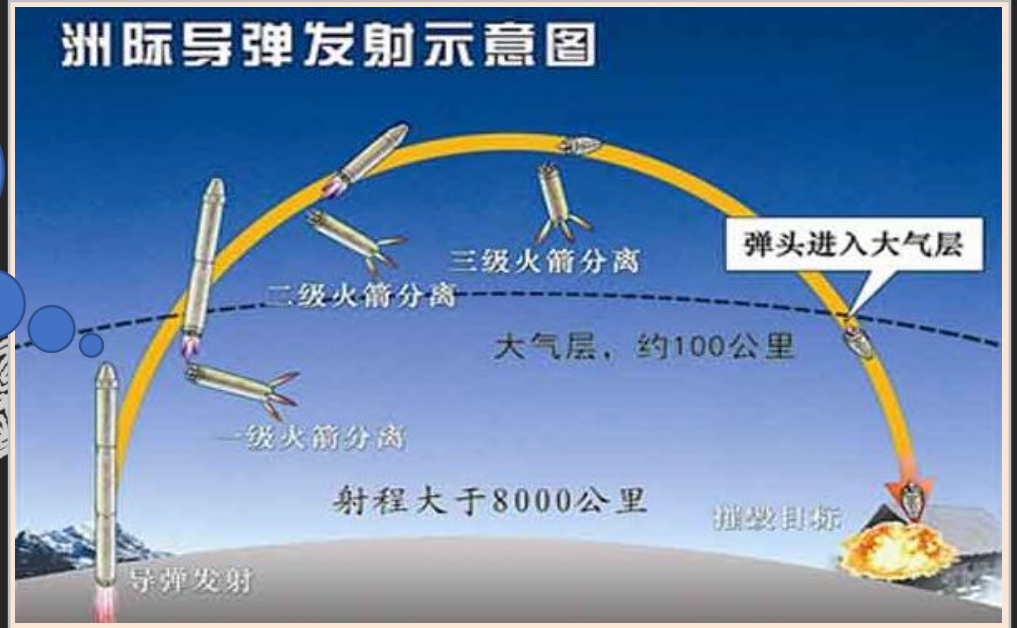


如果只知道自己被攻击了（看到了弹头：木马），却不知道攻击来自哪里（发射方：漏洞），攻击将会持续不断发生。

木马程序-B（弹头）

攻击完成后下载并执行木马程序

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，是传统安全防护技术的防护盲区领域，发生在程序内部的漏洞利用过程一直都是安全的黑盒。但只有作用在程序内部的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。

优势三：利用硬件芯片能力发现高级威胁

缸中之脑：

如何保证，我们看到的、我们读取的、我们写入的都是真实的？

之前的内存指令流劫持检测技术大多是以“内存与文件”中的代码数据作比较来发现内存中指令的异常。

但当系统已经被控制时，安全软件读取到的文件内容就可能已经不再是真实的内容，以虚假来验证虚假，显然结果也一定是虚假的。

而天狗利用CPU硬件的指令分支记录能力来实现可信环境检测，可以有效的杜绝所获取的数据被篡改的问题，从而发现真实的系统异常。

指令控制流劫持案例：

“鬼影变种”，感染磁盘引导扇区（MBR），并备份原始的正常MBR数据。

然后，劫持数据读取指令流，当判断“读”操作的对像是“PHYSICALDRIVE（物理磁盘）”且读取的位置是MBR所在区域时，将备份的原始MBR数据返回给读操作调用者。

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

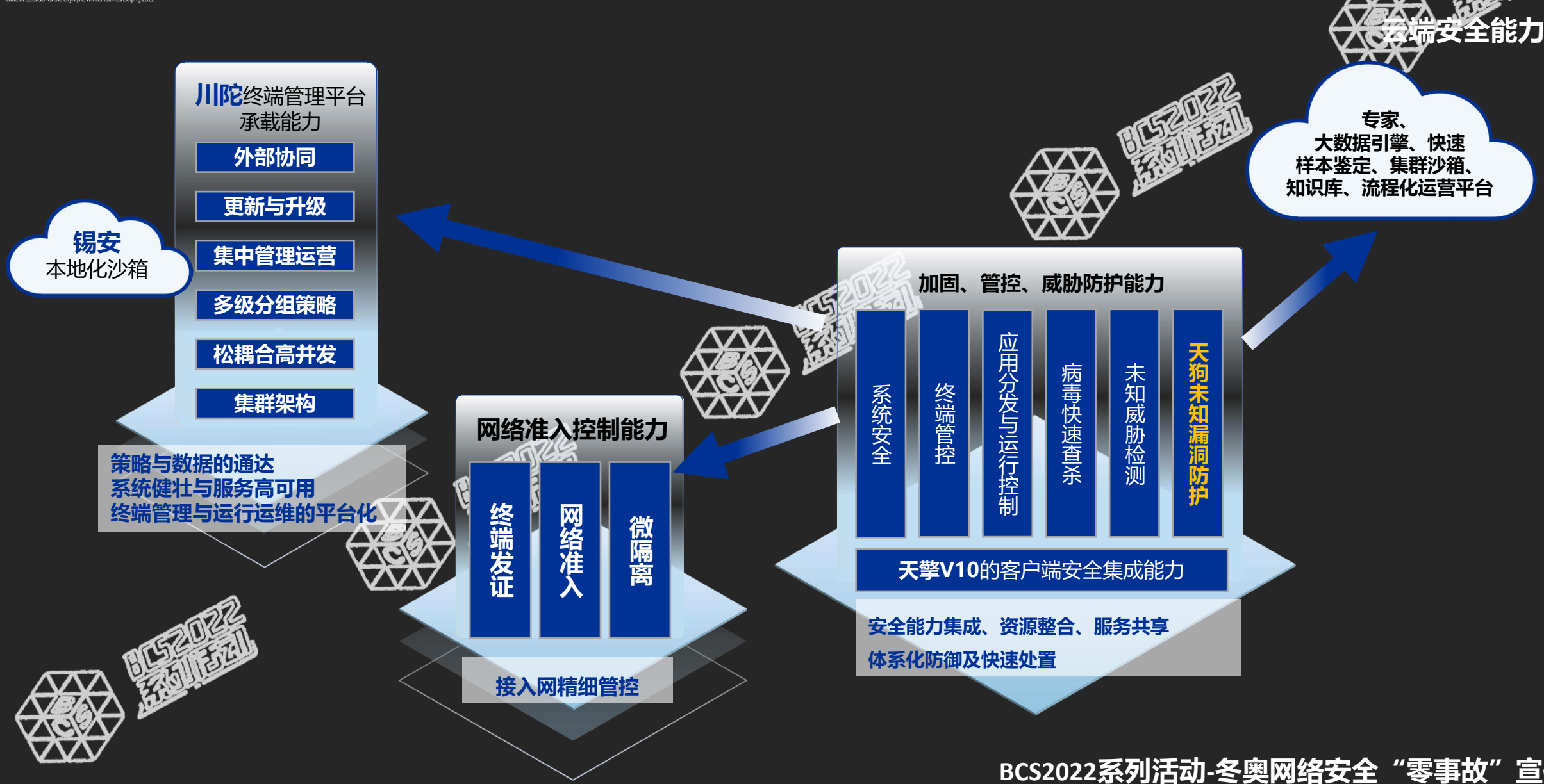
新技术在冬奥的应用

木桶里的最后一块板

奇安信

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

纵深体系防御



奇安信

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

BCS2022系列活动-冬奥网络安全“零事故”宣传周