首都医科大学附属北京友谊医院
Beijing Friendship Hospital,Capital Medical University

仁爱博精

针对VMware vSphere的勒索病毒的预防

首都医科大学附属北京友谊医院
信息中心 任大桅

目录

1 勒索病毒简介

概述

勒索病毒是一类利用各种手段**拒绝用户访问其电脑或者电脑中数据**，并以此**要求用户支付赎金**的一类恶意软件。

随着虚拟货币的发展，以及漏洞利用工具包的工程化利用，勒索病毒已经成为当今网络安全的首要威胁之一，而我国也是受勒索病毒攻击最严重的国家之一。

➢ 医疗行业成为勒索病毒的重灾区

- 医疗数据高价值
- 防护能力差
- 安全意识薄弱

《医疗行业勒索病毒专题报告》

在全国三甲医院中，有 247 家医院检出了勒索病毒。2019年初，某省几十家互联互通医院同时感染 GlobeImposter3.0 变种勒索病毒而被加密，**GlobeImposter 勒索病毒十分偏爱医疗行业**，在众多感染 GlobeImposter 勒索病毒的行业中，医疗行业占比约 50%。

演变历程

1、原始期：

技术能力：技术有限，大多勒索病毒都存在着漏洞，**容易被识别和破解**。

交付方式：交付赎金的方式多数以邮寄现金和转账为主，**很容易暴露黑客的行踪，不划算。**

2、发展期：

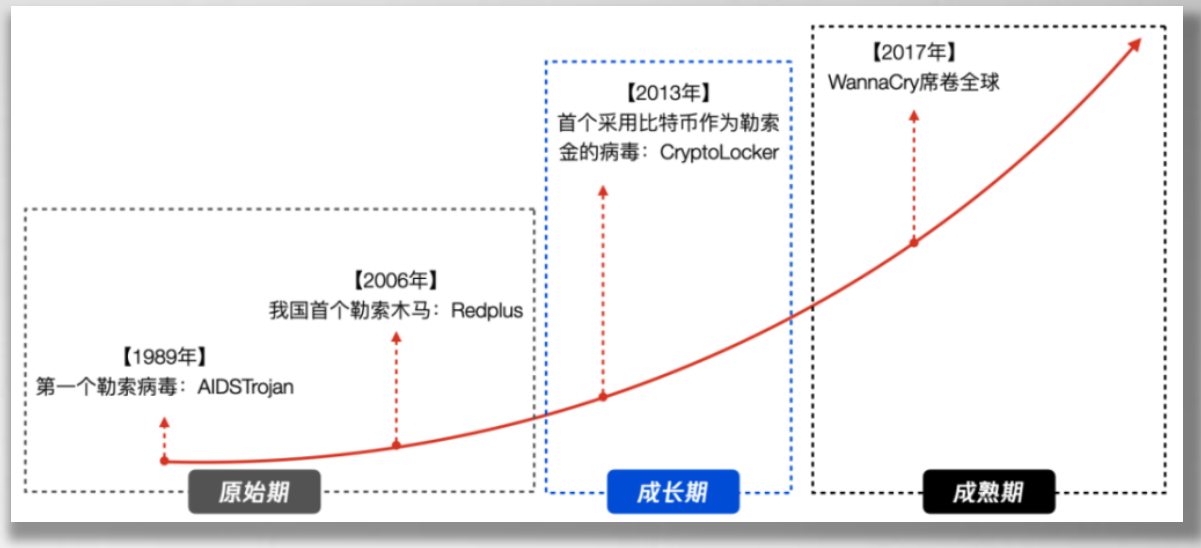
技术能力：使用AES和RSA对特定文件类型进行加密，而这种加密算法就现在的算力来说，**几乎是没办法破解的**。

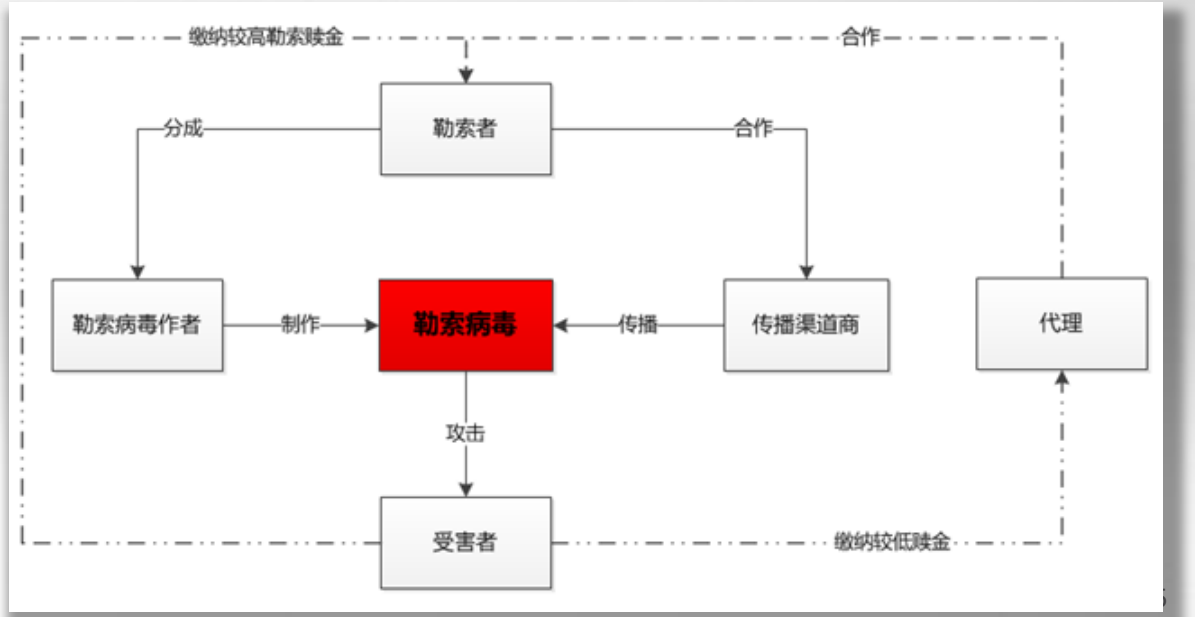
交付方式：以虚拟货币支付，**完美隐藏黑客身份。**

3、成熟期

勒索病毒逐渐演变成了产业化模式，并形成了一条完整的黑产产业链。一次完整的攻击流程可能涉及病毒作者、勒索实施者、传播渠道商、代理等等，各环节分工明细。

攻击的对象从最初的大面积撒网无差别攻击，转向**精准攻击高价值目标。针对企业，尤其是中大型企业**，让企业核心业务陷入瘫痪，而不得不缴纳巨额的赎金。





常用攻击手段

弱口令攻击

口令爆破攻击依然是当前最为流行的攻击手段，使用过于简单的口令或者已经泄露的口令是造成设备被攻陷的最常见原因。

钓鱼和垃圾邮件

“钓鱼邮件”攻击是最常见的一类攻击手段，在勒索病毒传播中也被大量采用。通过具有诱惑力的邮件标题、内容、附件名称等，诱骗用户打开木马站点或者带毒附件，从而攻击用户计算机。

利用系统与软件漏洞攻击

漏洞攻防一直是安全攻防的最前沿阵地，利用漏洞发起攻击也是最常见的安全问题之一。“永恒之蓝”工具就是其中利用漏洞的一个典型代表，其被用来传播 WannaCry勒索病毒。

网站挂马攻击

挂马攻击一直以来是黑客们热衷的一种攻击方式，常见的有通过攻击正常站点，插入恶意代码实施挂马，也有自己搭建恶意站点诱骗用户访问的。

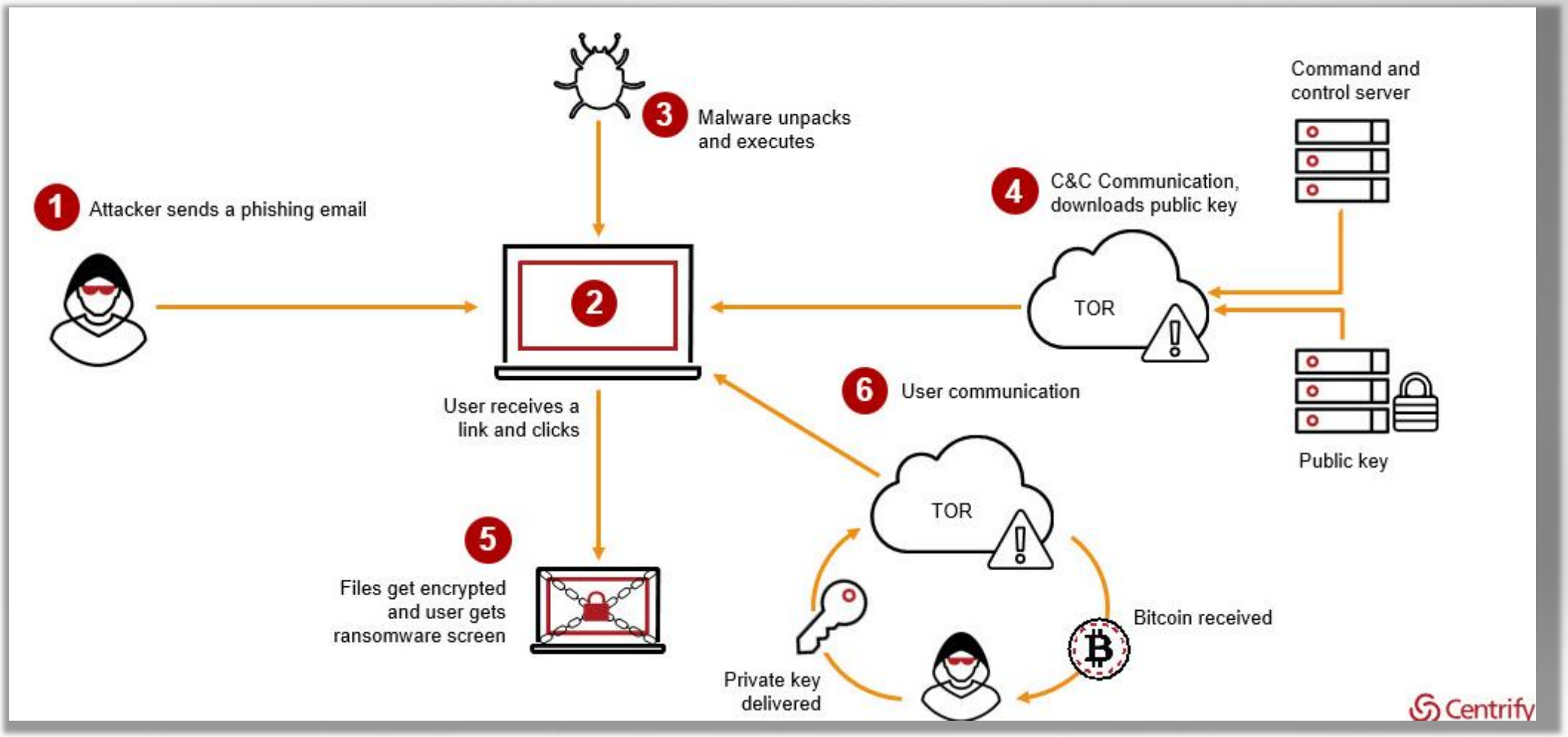
破解软件与激活工具

破解软件与激活工具通常都涉及到知识产权侵权问题，一般是由个人开发者开发与发布，缺少有效的管理，其中鱼龙混杂，也是夹带木马病毒的重灾区。

通过U盘感染

U盘随意使用U盘拷备文件，内外网混用等，易于传播病毒

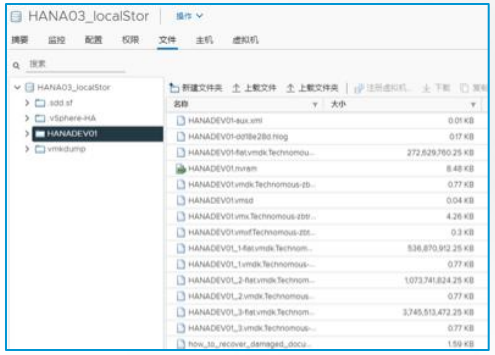
典型的勒索病毒攻击过程

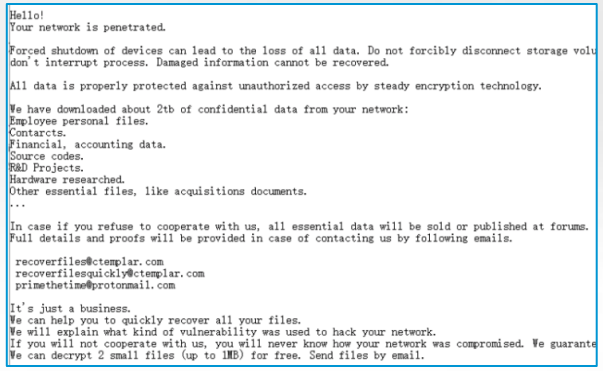


2

针对VMware vSphere的勒索病毒案例分析

针对VMware vSphere的勒索病毒出现





（来源：小岑博客）

中毒现象：VMware+Windows双杀

VMware vSphere部分

- 仅vCenter 处于正常状态，虚机大量被关机并处于无法连接状态。
- 虚拟机磁盘文件.vmdk，虚拟机描述文件.vmx被加密并重命名。
- 在vm-support诊断日志中留下勒索信息

Windows客户端部分

- 客户端出现文件被加密的情况，程度不一
- windows日志被清理，无法溯源
- 安全软件未起作用

处理过程

VMware vSphere部分

- 现有**存储每天执行快照**，VMware vSphere虚拟化主机全部重建后，通过存储LUN快照创建新的LUN挂载给ESXI，进行手动虚拟机注册。
- 部分存储于本地磁盘的虚拟机，无法用存储端快照还原，通过虚拟机整机还原。
- 对于无快照、无备份的虚拟机，只能放弃。后续重构虚拟机。
- 对VMware vSphere进行漏洞修补

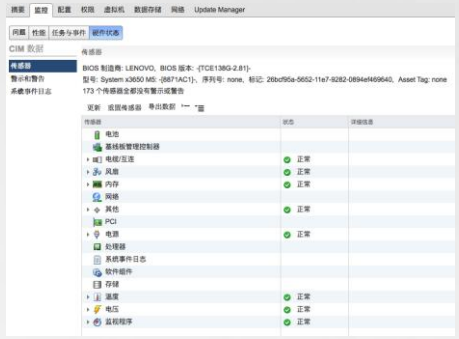
Windows部分

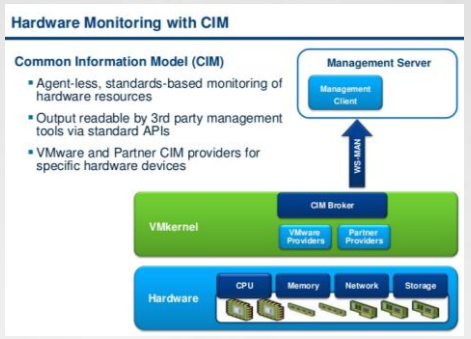
- 断网，抢救式备份数据
- 开启杀毒软件防勒索功能

技术分析

1、ESXi的漏洞

CVE-2019-5544
CVE-2020-3992

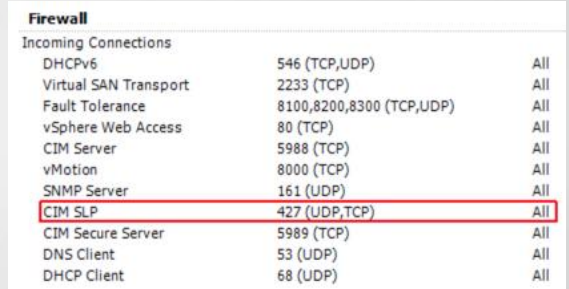




堆溢出 & 内存释放后重用

2、病毒如何利用漏洞

攻击者通过OpenSLP 服务端口 TCP 427 实施攻击，实现远程代码执行效果，从而获得ESXi系统管理权限。

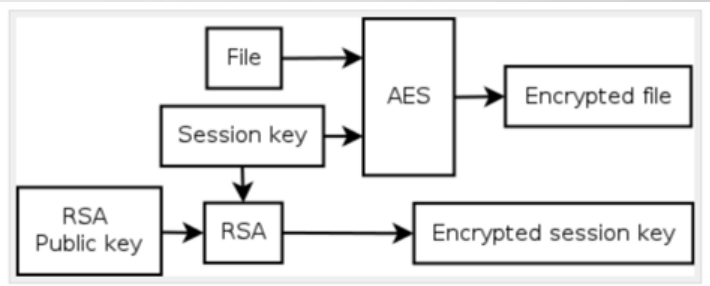


Firewall

Incoming Connections		
DHCPv6	546 (TCP,UDP)	All
Virtual SAN Transport	2233 (TCP)	All
Fault Tolerance	8100,8200,8300 (TCP,UDP)	All
vSphere Web Access	80 (TCP)	All
CIM Server	5988 (TCP)	All
vMotion	8000 (TCP)	All
SNMP Server	161 (UDP)	All
CIM SLP	427 (UDP,TCP)	All
CIM Secure Server	5989 (TCP)	All
DNS Client	53 (UDP)	All
DHCP Client	68 (UDP)	All

3、病毒如何加密数据：

该勒索病毒使用了常见的RSA+AES加密方法，首先生成AES秘钥对文件进行加密，然后使用RSA公钥对AES的秘钥进行加密，只有得到攻击者的私钥才能进行解密。



漏洞如何修补

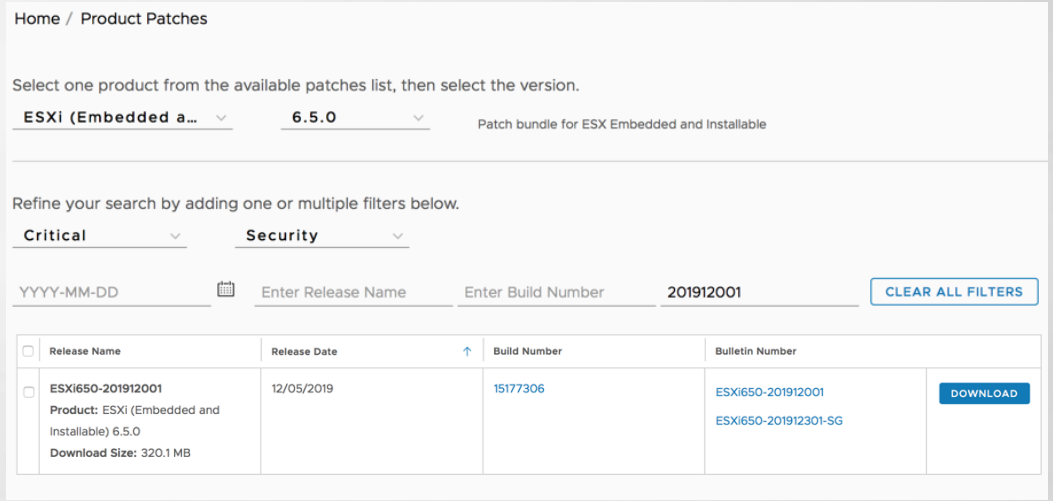
1、及时对ESXi进行升级

- 手动搜索下载补丁并安装
  https://my.vmware.com/group/vmware/patch

- 使用vSphere update Manager 自动升级
  - 升级和修补 ESX/ESXi 主机
  - 安装和更新主机上的第三方软件
  - 升级虚拟机硬件、VMware Tools 和虚拟设备。

2、临时措施，禁用SLP服务，禁用端口427。
（导致硬件状态页不可用）

Product	Version	Running On	CVE Identifier	CVSSV3	Severity	Fixed Version
ESXi	6.7	Any	CVE-2019-5544	9.8	Critical	ESXi670-201912001

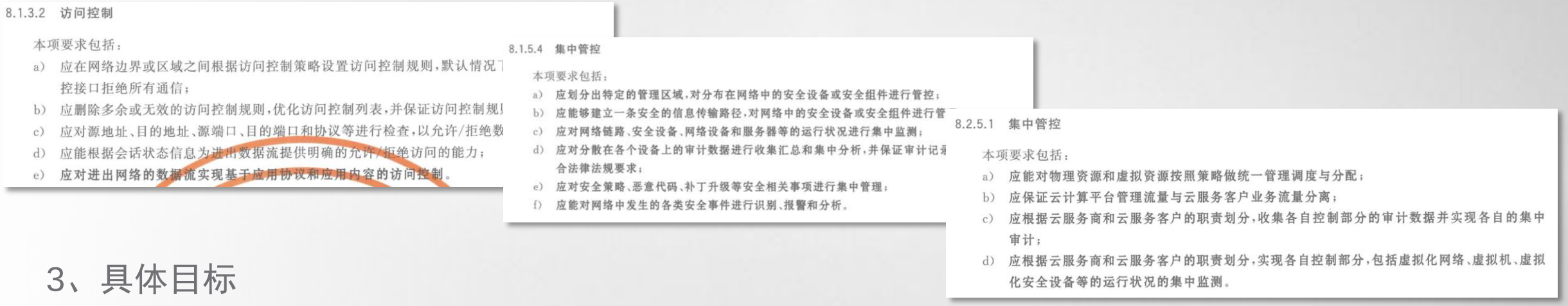


3 虚拟化基础设施的安全防护设计

虚拟化网络安全架构

1、架构设计的必要性： 增加攻击难度和攻击成本，减少防守难度和工作量

2、设计原则　参考等保2.0 8.1.3.2访问控制、8.1.5.4集中管控、云安全扩展8.2.5.1集中管控



8.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下
控接口拒绝所有通信；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数

d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

8.1.5.4 集中管控

本项要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管

c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录
合法律法规要求；

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

f) 应能对网络中发生的各类安全事件进行识别、报警和分析。

8.2.5.1 集中管控

本项要求包括：

a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

b) 应保证云计算平台管理流量与云服务客户业务流量分离；

c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

3、具体目标

- 对于虚拟化基础架构实现管理流量、数据流量、业务流量分离
- 对于业务虚机网段根据位置、服务、应用等因素划分不同的安全区域，在各区域间做访问控制
（内网、办公网、DMZ；数据库、应用；基础服务：WSUS、DNS、NTP；安全管理域：**域控**、杀毒）
- 对虚拟网络的东西向流量进行精细化管理

虚拟化网络安全架构

4、实现方式

- 规划安全区域

			管理流量			数据流量			业务（虚机）流量				
			硬件带外管理（iLO、iDRAC、Console）	VMK_MGMT	VMK_vMotion	VMK_Storage01	VMK_Storage02	VMK_VXLAN	基础服务	安全管理	业务-内网	业务-办公网	业务-DMZ区
分类	分组	设备/服务器	VLAN200	VLAN1	VLAN2	VLAN3	VLAN4	VLAN5	VLAN11	VLAN12	VLAN21	VLAN22	VLAN23
			192.168.200.0/24	192.168.1.0/24	192.168.2.0/24	192.168.3.0/24	192.168.4.0/24	192.168.5.0/24	192.168.11.0/24	192.168.12.0/24	192.168.21.0/24	192.168.22.0/24	192.168.23.0/24
VMware vSphere	ESXi主机	esx-01	192.168.200.1	192.168.1.1	192.168.2.1	192.168.3.1	192.168.4.1	192.168.5.1					
		esx-02	192.168.200.2	192.168.1.2	192.168.2.2	192.168.3.2	192.168.4.2	192.168.5.2					
		esx-03	192.168.200.3	192.168.1.3	192.168.2.3	192.168.3.3	192.168.4.3	192.168.5.3					
		esx-04	192.168.200.4	192.168.1.4	192.168.2.4	192.168.3.4	192.168.4.4	192.168.5.4					
		esx-05	192.168.200.5	192.168.1.5	192.168.2.5	192.168.3.5	192.168.4.5	192.168.5.5					
		esx-06	192.168.200.6	192.168.1.6	192.168.2.6	192.168.3.6	192.168.4.6	192.168.5.6					
	VMware vSphere管理服务器	vCenter		192.168.1.201									
		NSX Manager		192.168.1.202									
		NSX Controller-01		192.168.1.203									
		NSX Controller-02		192.168.1.204									
		NSX Controller-03		192.168.1.205									
		vRealize Operations Manager		192.168.1.206									
		vRealize Network Insight		192.168.1.207									
	虚拟化备份管理服务器	BackupMGMT-01		192.168.1.208									
硬件	SAN存储	存储控制器01	192.168.200.51										
		存储控制器02	192.168.200.52										
	NAS存储	NAS-node-01	192.168.200.101			192.168.3.101	192.168.4.101						
		NAS-node-02	192.168.200.102										
	光纤交换机	光纤交换机01	192.168.200.151										
		光纤交换机02	192.168.200.151										
服务器-基础设施	NTP	NTP-01							192.168.11.1				
	WSUS	WSUS-01							192.168.11.2				
	DNS	DNS-01							192.168.11.3				
		DNS-02							192.168.11.4				
服务器-安全与管理	域控制器	DomainCtr-01								192.168.12.1			
		DomainCtr-02								192.168.12.2			
	杀毒软件管理	Anti-virus								192.168.12.3			
服务器-内网	HIS应用服务器	HISAPP01									192.168.21.1		
		HISAPP02									192.168.21.2		
		HISAPP03									192.168.21.3		
		HISAPP04									192.168.21.4		
		HISAPP05									192.168.21.5		
服务器-办公网	OA应用服务器	OA-APP-01										192.168.22.1	
		OA-APP-02										192.168.22.2	
服务器-DMZ区	医院主页	WEB-01											192.168.23.1

虚拟化网络安全架构

- 部署安全设备

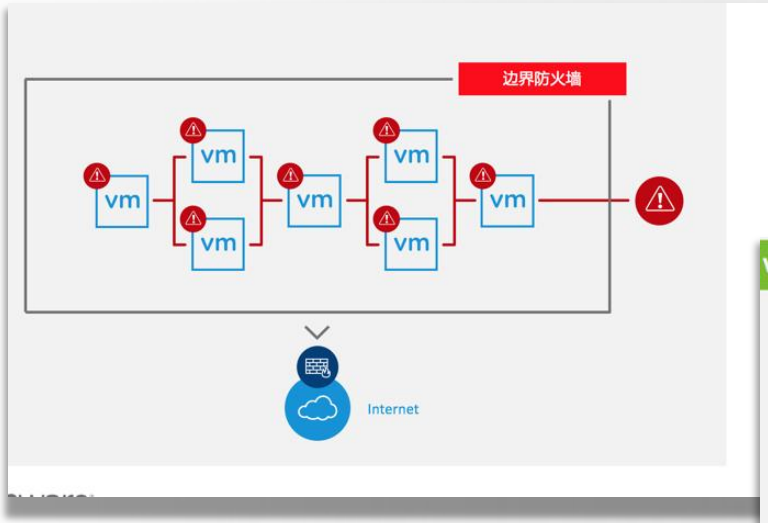
① 防火墙、IPS和防病毒网关。（网络防护）

② 防病毒软件、漏洞扫描、主机安全防护、堡垒机。（主机防护）

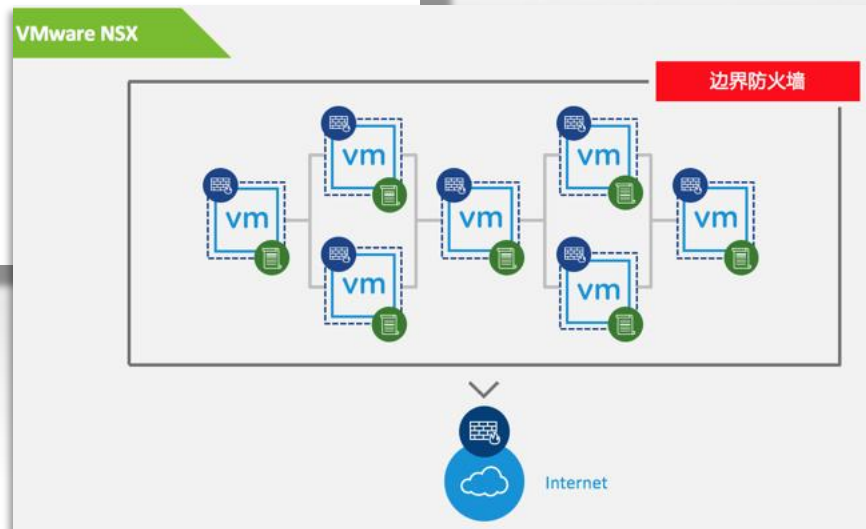
③ 流量分析、态势感知（安全审计）

虚拟化网络安全架构

- 利用**分布式防火墙**，加强虚拟网段管控



- 虚拟化区域往往是个安全盲区
- 一旦某一台VM被攻击（比如蠕虫病毒），会迅速传染给同VLAN中其他VM



- 在每个虚拟机，容器颗粒度的防火墙
- 基于虚拟机特征值的应用安全策略
- 自动化的部署

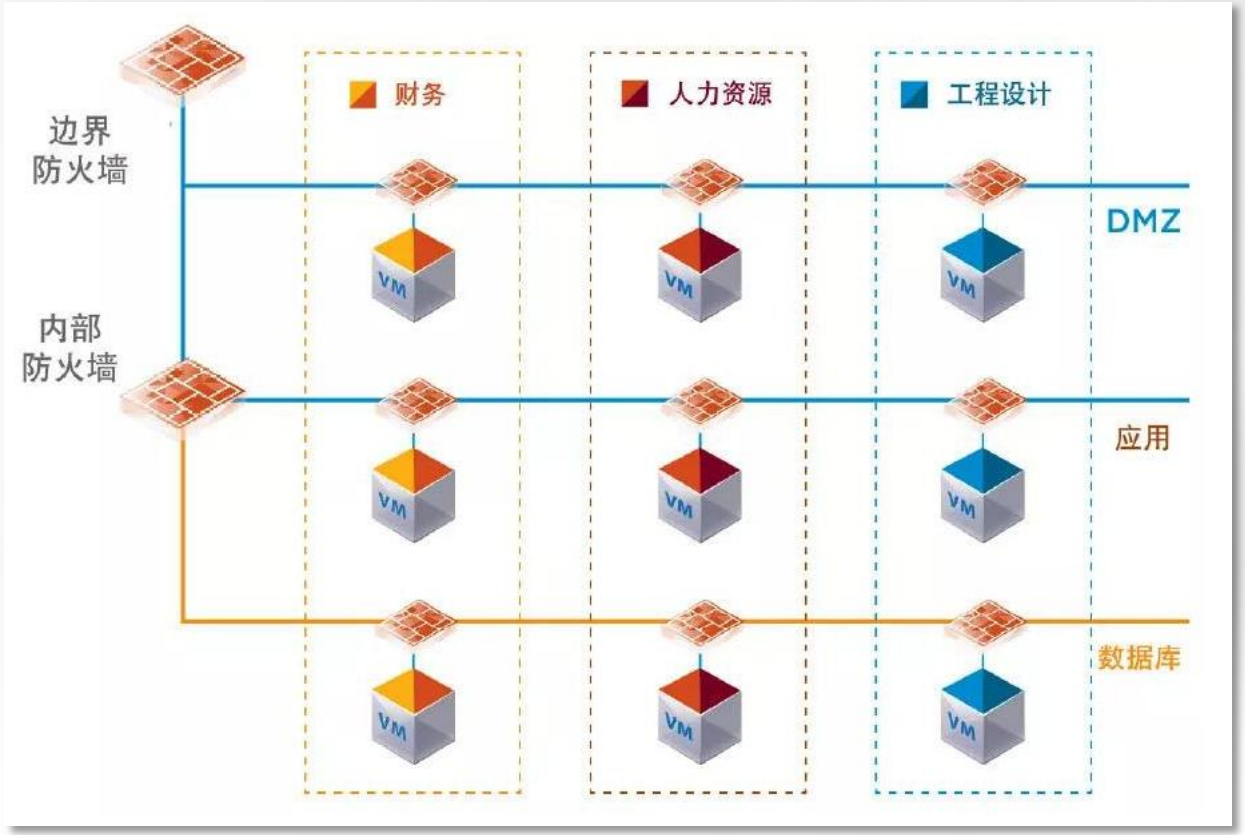
启用NSX防火墙之后，无法对相邻机器进行扫描

```
~ $ sudo nmap -Pn -sSVC -n 10.10.50.101

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-16 19:57 CST
Nmap done: 1 IP address (0 hosts up) scanned in 1.00 seconds
~ $
```

虚拟化网络安全架构

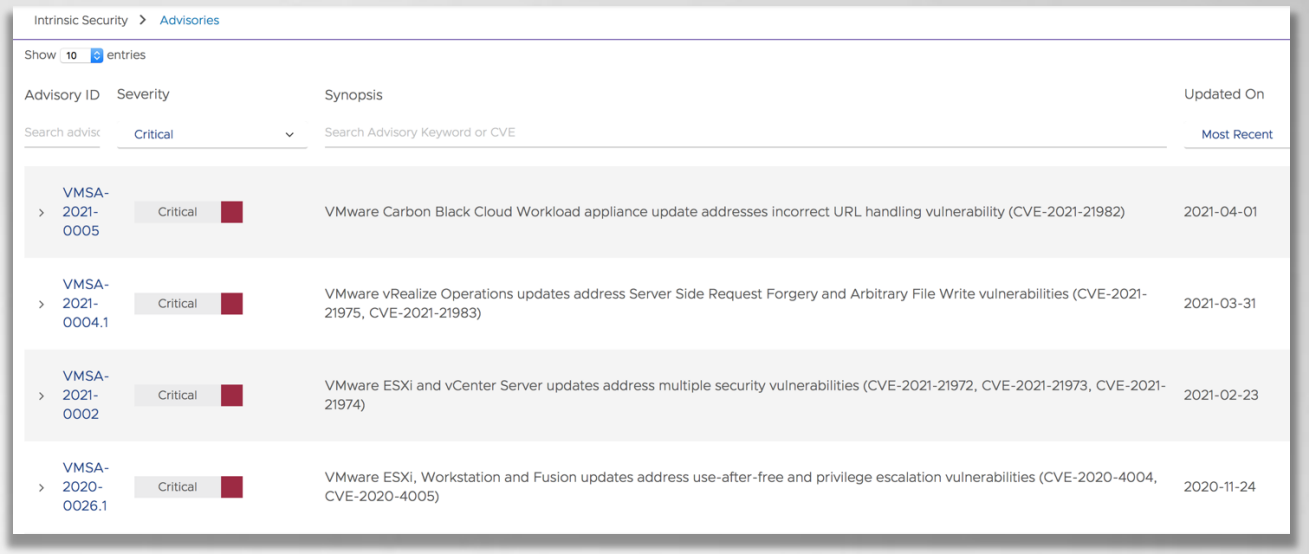
- 利用**网络微分段**技术，将内部网络划分为可以单独保护的逻辑区域。



虚拟化主机安全防护

虚拟平台的安全防护

关注厂商的安全公告，及时升级虚拟平台组件。



虚拟机的安全防护

补丁更新、部署具有反勒索功能的杀毒软件、避免弱密码、更改RDP端口、限制出访互联网

虚拟化备份系统

备份的必要性：备份是数据安全的最后一道防线

设计目标：

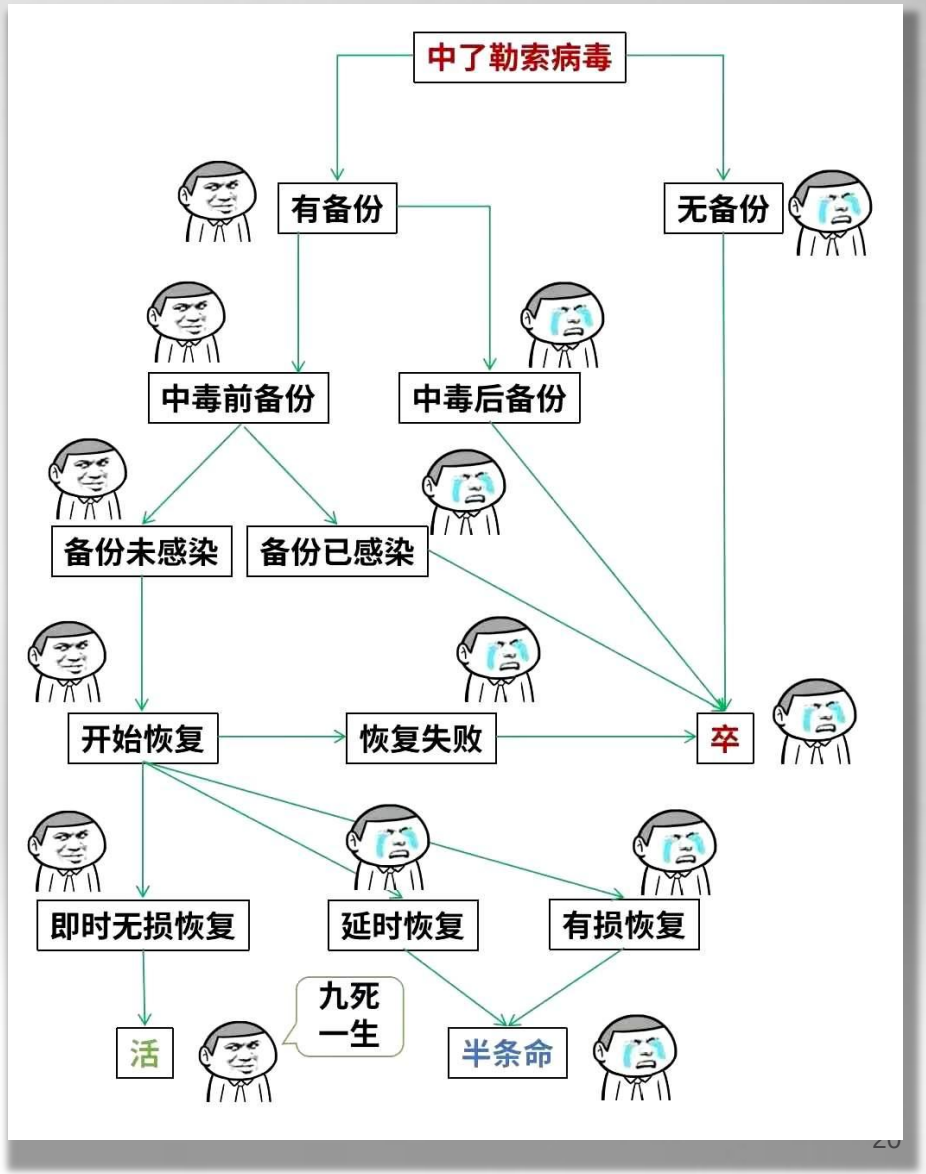
1、备份系统应具有足够大的存储空间，备份数据至少保留三个月。

2、备份系统应具有强安全防护能力，或具有离线备份能力，以保障备份数据安全。

3、备份系统应具有进行恢复演练，验证备份数据可用性的能力。

4、选用具有高速数据还原能力的备份系统，减小RTO。

5、选用具有高速备份能力的备份系统，缩小备份窗口，增加备份频率，减小RPO。



虚拟化备份系统

三种备份方式对比：

	数据备份	虚机整备	存储端备份
原理	在服务器上安装备份代理，备份业务数据	利用vCenter接口进行无代理备份	利用存储的快照备份能力进行整卷备份
对业务的影响	中	大	小
备份速度	慢	快	最快
还原速度	慢	快	最快
成本	中	中	高

4

总　结

总结

- 重视基础架构、基础协议的漏洞修补和攻击防范

  基础架构、基础协议的漏洞虽然数量少，但波及范围广、破坏性强。

- 重视安全架构的设计

  做好安全架构设计，改变攻防态势，以逸待劳

- 针对虚拟平台的勒索病毒防御

  限制管理网络的访问：让敌人打不到
  及时更新补丁：让敌人打不透
  做好备份：随时复活，让敌人打不赢

感谢聆听