常见病毒攻击摘要

一、扫描事件

利用TCP协议原理，对网络中存在主机IP和端口进行扫描，根据是否影响，查找互联网中存在的存活主机或开放的端口；而根据开放端口可以判断出该主机对外提供的协议；扫描事件相当于攻击事件前期的踩点活动，为攻击者下一步攻击做准备。

主机感染类病毒，病毒欲想感染更多主机，先会对内网其他主机进行扫描，获取内网更多主机相关信息，为下一步攻击做准备；主机感染病毒后，可能导致该主机信息被攻击者窃取，如机密文件、关键资产的用户名和密码等。对互联网其他主机发起扫描，违反网络安全法，遭至网信办、网安等监管单位的通报处罚。

以下仅列出有专杀工具的流行病毒列表（**建议依次使用以下杀软进行查杀**）：  
EDR通用扫描工具<http://edr.sangfor.com.cn/tool/SfabAntiBot.zip>  
飞客蠕虫<http://edr.sangfor.com.cn/tool/Kidokiller.zip>  
Ramnit <http://sec.sangfor.com.cn/download/index?file=FxRamnit.exe>  
Sality <http://sec.sangfor.com.cn/download/index?file=SalityKiller.exe>  
Virut <http://sec.sangfor.com.cn/download/index?file=VirutKiller.exe>  
Zeus <http://sec.sangfor.com.cn/download/index?file=ZbotKiller.exe>  
Parite <http://sec.sangfor.com.cn/download/index?file=avast.bat>  
Spybo <http://sec.sangfor.com.cn/download/index?file=FixSpybot.exe>  
EmsisoftEmergencyKit:第三方公司Emsisoft提供的本地查杀工具  
<http://sec.sangfor.com.cn/download/index?file=EmsisoftEmergencyKit.exe>

二、永恒之蓝和Struts2漏洞攻击

永恒之蓝和Struts2漏洞攻击，经过安全专家排查发现服务器存在较大的安全隐患，攻击者利用Web漏洞作为入口深入内网进行探测，试图窃取敏感数据。

主要攻击过程如下：

1. 通过Struts2漏洞，执行系统命令写入webshell、并上传proxy工具
2. 通过proxy工具对内网发起扫描
3. 利用frp暴露内网端口
4. 对其他内网主机发起永恒之蓝和Struts2漏洞攻击

主要推荐以下几种方式进行预防与查杀：

1.在此强烈建议广大互联网用户及时进行下载并更新最新的Struts2包：<https://struts.apache.org/>，同时还可以参考官方提出的意见处置方法：[https://cwiki.apache.org/confluence/display/WW/Security Bulletins](https://cwiki.apache.org/confluence/display/WW/Security%20Bulletins)  
2.删除主机Web目录下的Webshell文件，并停止Webshell起的子进程，关闭frp反向代理，停止暴露内网端口；  
3.根据安全平台的分析中心的安全检测日志，筛选被攻击成功的主机日志，参照建议1、2再次进行Struts2版本升级、对应的Webshell和黑客工具删除以及关闭恶意进程。  
4.平时多注意平台的安全警报，关注内网安全动态，及时升级安全平台和威胁感知探针。推荐使用深信服安全感知+防火墙+EDR，对内网进行感知、查杀和防护。

三、DNS隧道

DNS隧道是一种隐秘隧道，通过将其他协议封装到DNS协议中传输建立通信的方式。因为DNS协议在网络中一种基础必不可少的服务，所以大部分防火墙和入侵检测设备是不会对对DNS流量进行拦截过滤，这就给DNS作为隐蔽通信提供了有力条件，从而可以利用它实现诸如僵尸网络或木马的远程控制通道和对外传输数据等。

主要具有以下危害：

1、主机可能已中毒，攻击者利用DNS隧道控制主机对外发起DoS攻击，可能存在被网安、网信办通报的风险。  
2、主机可能已中毒，攻击者利用DNS隧道对外传输敏感数据，导致客户信息被泄露。

主要推荐以下几种方式进行预防与查杀：

深信服EDR分析并查杀：<http://edr.sangfor.com.cn/tool/SfabAntiBot.zip>