# 1.目前的存在的线索

1.直播时间30分钟

2.传输的文件大小 1080P\*60\*30； 1080P 视频 1分钟 100M

3.传输文件的速度 1080p 速率大约 100M\*30/s 3G/S

4.在30分钟的末尾出现骇客开始渗透的提示

5.媒体的连接数达到200家。

6.眼镜片上出现了 绿色的规则形状的屏幕反光

7.以色列最大的软件公司

8.不用翻墙，国内直接观看

9.使用裂变的传播方式进行传播

10.主要的视频服务商采用软件的措施进行视频控制。

11.存在多个地区 伦敦眼，美国黄石国家公园，美国纽约。

12.上亿条评论被删除，数百万个微信群被解散。

13.不定时直播，游击战术。直播时间美国时间上午8点，下午15-18点。

# 2.所采用的技术手段分析

1.直播时间30分钟

直播时间30分钟画质十分清晰，没有杂音干扰。没有断网。

2.传输的文件大小 1080P\*60\*30； 1080P 视频 1分钟 100M

视频文件的大小 3G左右

3.传输文件的速度 1080p 速率大约 100M\*30/s 3G/S

往国内的传播速率达到3G/S,长春理工大学2017-06-11 0点的时候，出口速率超过3G/s，速率的描述说明，参考韩国国内和北京100M光纤的传播速率，3G/S 在中国互联网进出口速率的比重很小，如果采取分片传送被识别的概率很小，如果使用多态传输的手段，如伪装成网页，伪装成vpn，使用特定的文件解析格式墙内解析，伪装文件特征码。

实际的解决办法是

使用高性能的网络连接设备，性能指标要达到理工大学的水平并不难。

使用伪装软件，编码的时候可以在海外进行，解码的时候需要肉鸡服务器。肉鸡服务器可能采用分布式部署，如果想要长时间使用，那么存在抓鸡程序。

抓鸡程序的特征，

网络的速率快，可以快速的扫描公网服务器，更高级的具有绕过WAF的内网渗透功能。

抓鸡程序掌握大量的0day，1day，nday漏洞

抓鸡程序的可靠性和稳定性高。不会轻易宕机。

抓鸡程序具有隐藏功能类似于病毒和IP池功能，不会被地址屏蔽。

总结

硬件 高性能的网络转发器，多台肉鸡，多台高性能的服务器（抓鸡）

软件 抓鸡程序，伪装程序，控制程序。

4.在30分钟的末尾出现骇客开始渗透的提示

说明直播使用的系统具有欺骗功能，类似于蜜罐技术。

蜜罐技术还不成熟，具有有穷性和绕过性

骇客使用的程序中的Oday没有起作用，但是大量的攻击尝试产生了攻击效果

直播方可以看到受到攻击的状况。

基于linux的定制版系统，deban，和黑客组织有交流，修补了0day漏洞，但是由于各个黑客组织掌握私有的0day，导致了入侵，系统的网络层面上具有入侵检测软件，具有防火墙功能，系统使用容器技术伪造了大量的沙箱系统，每次直播沙箱系统的指纹不同，由于服务器性能和技术的限制导致可以被枚举和突破安全机制。

硬件层面 服务器

软件 定制版linux

5.媒体的连接数达到200家。

采用可靠性传输协议可能是自定义的

视频的压缩技术很成熟，使用高质量传输可以保障。

服务器和网络性能可以支持性能操作。

硬件 摄像头，视频处理硬件，转播服务器

软件 视频压缩器，连接维持工具，成熟的转播软件

6.眼镜片上出现了 绿色的规则形状的屏幕反光

可能是补光灯的反光

可能是实时监控的显示屏幕

可能是摄像头

7.以色列最大的软件公司

- IronSource是以色列最大，也是成长最快的创业公司之一。它5年前 ... IronSource借助大数据分析和精密算法

具有实战经验和网络设备，以及技术支持，与多国的网络公司存在业务来往。

8.不用翻墙，国内直接观看

为了防止视频地址被屏蔽，所以采用动态的视频地址

为了保证观看质量，所以视频的传输速率不能太差

为了防止以后的视频的特征码被识别，所以应该采用伪装技术

9.使用裂变的传播方式进行传播

具有爬虫/蠕虫功能可以主动传播。

具有突破防火墙功能，

具有变形和伪装功能

实际上就是一个蠕虫病毒，这个蠕虫病毒可以抵抗现在的安全机制的检验，如主动防御技术，身份控制技术，防火墙，云检测。

这个病毒采用的机制是 具有常用端口突防，提权，多台的外壳，掌握了安全软件的漏洞。将美国CIA，以及黑客组织的工具集成可以达到这个效果。

10.主要的视频服务商采用软件的措施进行视频控制。

对国内的视频提供商进行了渗透分析，掌握了软件和硬件的架构

掌握了大量的管理员权限账号，掌握了软硬件的漏洞。

使用国内的视频服务商的视频服务器作为主流的传播服务器。

多份的视频备份

在内核级别或者是BIOS级别具有rootkit程序

动态解析地址

特定的视频播放软件。 （可能性极低）

实际上就是使用rootkit技术进行视频传播控制。同时掌握了大量的漏洞，进行攻守方对抗，维持rootkit程序的存在。

11.存在多个地区 伦敦眼，美国黄石国家公园，美国纽约。

具有移动直播的特性，说明硬件的转运不是十分困难

说明硬件的质量很好，可以抗高温

说明掌握了多了直播网络可以保证直播正常进行。

说明对于无线技术的防护达到了一定水平。

12.上亿条评论被删除，数百万个微信群被解散。

13.不定时直播，游击战术。直播时间美国时间上午8点，下午15-18点。