（一， 背景）4月14日，影子经纪人在steemit.com上公开了一大批NSA（美国国家安全局）“方程式组织” (Equation Group)使用的极具破坏力的黑客工具，其中包括可以远程攻破全球约70%Windows机器的漏洞利用工具。一夜之间，全世界70%的windows服务器置于危险之中，国内使用windows服务器的高校、国企甚至政府机构也不能幸免。（背景段，引出下面的方程式组织和影子经济人）

（二， 方程式组织） 在墨西哥坎昆——2009 年，多位知名研究人员通过电子邮件收到一张 CD 光盘，该 CD 光盘含有他们近期在休斯敦参加的一次科技论坛的照片及其他资料。这些科学家们当时并不知道这张光盘还携带有由高级黑客入侵组织开发的一款恶意负载，且该组 织自 2001 年起就处于活跃状态。

这些入侵者被称为“方程式组织”，方程式组织（Equation Group）是一个由卡巴斯基实验室发现的尖端网络犯罪组织，后者将其称为世界上最尖端的网络攻击组织之一，同震网（Stuxnet）和火焰（Flame）病毒的制造者紧密合作且在幕后操作。 方程式组织的名字来源于他们在网络攻击中对使用强大加密方法的偏好。截至2015年，卡巴斯基记录了位于至少42个国家的500个恶意软件感染，同时承认由于其自终止协议的存在，实际数量应有上万例。 该组织被怀疑与美国国家安全局（NSA）有联系。

“方程式”不是一个普通的黑客集团。它的危害，远远超出了我们所熟悉的熊猫烧香、盗号木马等等，它所瞄准的往往是一个国家的关键设施、经济命脉。它所追求的，也不是普通病毒的窃取信息、经济诈骗，而是破坏工业生产，制造社会混乱，乃至直接打击军事设施。

作为史上最强的网络攻击组织，“方程式”拥有一个庞大而强悍的攻击武器库。传统的病毒往往是单兵作战，攻击手段单一，传播途径有限，而“方程式”动用了多种病毒工具协同作战，发动全方位立体进攻，是名副其实的最强网络攻击工具。

六个代码名称：卡巴斯基认定至少共有 6 款不同的恶意软件为方程式组织所为，包括：1，EquationLaser：一款使用于 2001 至 2004 年的早期植入。

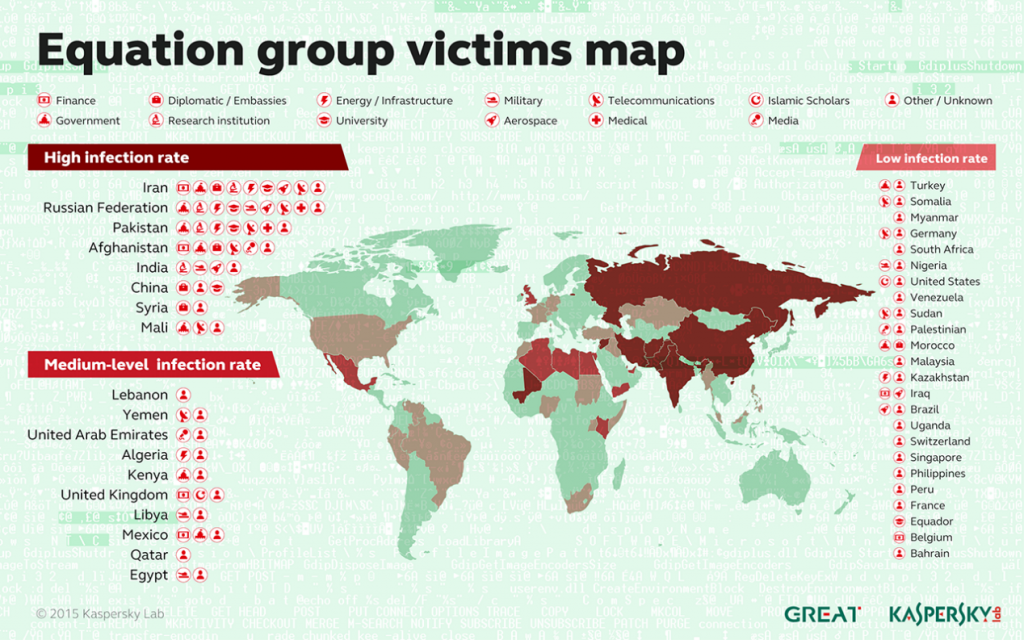
2，DoubleFantasy：一款验证式木马病毒，用来确认受感染人是否为特定目标，经证实后升级至 EquationDrug 或 GrayFish 。

3，EquationDrug：也称 Equestre ，是一款支持 35 种不同模块和 18 种驱动的复杂攻击平台，也是方程式组织重新闪存硬盘固件并用虚拟文件系统隐匿文件和窃得数据的两大恶意软件平台之一。 EquationDrug 仅在目标受 DoubleFantasy 感染且经确认后实现。这款恶意软件于 2002 年开发，2003 年因更先进的 GrayFish 出现而遭到淘汰。

4，GrayFish：EquationDrug 的继承者，也是方程式组织所有攻击平台中最复杂的一个。

5，Fanny： 曾于 2008 年入侵 Windows 两个零日漏洞的计算机蠕虫，每当 USB 闪存盘插入目标计算机就会进行自我复制。Fanny 的主要目的就是在敏感的物理隔绝网络上进行侦查。在感染某台未连至因特网的计算机后，Fanny 搜集网络信息并将其保存至 USB 闪存盘的一个隐蔽区域。如闪存盘随后被插入一台连入因特网的计算机，就会将数据上传至攻击者服务器并下载任何攻击者指令。如闪存盘随后被插入一台物理隔绝 设备，下载指令就会被执行。每当闪存盘在物理隔绝网络中的计算机和连入因特网的计算机间相互切换，进程就会继续。

6，TripleFantasy：全功能的后门程序，有时与 GrayFish  配合使用。



（三，影子经济人）



这不是影子经纪人和NSA（美国国家安全局）方程式组织的第一次厮杀了。

早在2016年8月，影子经纪人就在网上以100万比特币（现价约超过5亿美元）的价格，公开竞拍据称来源于NSA（美国国家安全局）的顶级黑客工具。为了增加可信度，他们还在网上贴出部分文件。但最后的结果不尽如人意，可能是要价过高或是其他原因，黑客工具一直无人问津，拍卖最终只获得了价值25美元的比特币。

2016年10月，该组织取消了销售，开通了类似众筹的活动，当最终收到10,000比特币（630万美元 ）后，他们将提供给每一份参与众筹的人一份黑客工具。

2016年12月份，该组织取消了失败的众筹尝试，并开始在ZeroBin上较小批量销售黑客工具。

2017年1月份，该组织又以750比特币（$ 675,000）的价格出售一批能够绕过杀毒软件的Windows黑客工具。

2017年4月8日，影子经纪人再一次进入安全人的视野中，长文分享了一个能打开世界上所有加密文件的“万能密码”。这批漏洞主要针对linux系统，包含EQGRP这套Linux工具。

2017年4月14日，他们在网上免费公开超大批次的“方程式组织”黑客工具，其中包括强大的0day



（四，应急措施） 这些攻击手段所使用的漏洞，如果针对的是还在服务期的系统，微软大部分已经提供了补丁，但是这些补丁还远远不够，在所有补丁打好之前，所有 Windows 服务器、个人电脑，包括 XP/2003/Win7/Win8，Win 10 最好也不要漏过，即： 所有的windows操作系统！ 重要的事说3遍！ 全部使用防火墙过滤/关闭 137、139、445端口；对于 3389 远程登录，如果不想关闭的话，至少要关闭智能卡登录功能。 此外，确保每台主机上的终端安全软件、策略和防护特征是最新的，检查确认网络中的Windows系统，无论客户端还是服务器系统，安装了最新的安全补丁。