（以下内容来自百度）：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。

（以下内容来自https://www.secpulse.com/archives/5267.html ）：墨西哥坎昆——2009 年，一位或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。这张 CD 光盘似乎在通过电子邮件发送的过程中遭到篡改。

这些入侵者（莫斯科卡巴斯基实验室的研究人员称之为“方程式组织”）在传输过程中秘密拦截数据包、对内容进行篡改后发送至指定目的地的做法绝非偶然。早在 2002 年或 2003 年，方程式组织成员就为了感染另一目标，使用其组织中的海量恶意软件库中的一款恶意软件，对一张 Oracle 数据库安装 CD 光盘做过类似手脚。（卡巴斯基选取方程式组织这个名称的原因在于组织成员在加密算法、高级模糊处理方法及篡改技术方面具有极强的技能。）

卡巴斯基研究人员在至少 42 个国家范围内记录了 500 次感染，其中伊朗、俄罗斯、巴基斯坦、阿富汗、印度、叙利亚，马里名列前茅。由于恶意软件内置自毁机制，研究人员怀疑这仅是冰山一角，受害者实际数量或将达到数以万计。

一长列近乎神级的技能展示阐述了方程式组织的超凡本领、艰苦工作，及无限资源，包括： 虚拟文件系统的使用，这项技能也可以在极度复杂的 Regin 恶意软件中找到。斯诺登近期公布的文件指出 NSA 用 Regin 来感染部分国有的比利时公司 Belgacom 。 某个受感染计算机注册表多个分支的恶意文件藏匿。通过对所有恶意文件加密并将其存储在一个计算机 Windows 注册表的多个分支使反病毒软件无法检测到感染。 将 iPhone 用户发送至独一无二的入侵网页的重新定向。此外，指向方程式组织命令服务器的受感染机器自识别为 Macs ，表示该组织成功入侵了 IOS 和 OS X 设备。 使用 300 多个因特网域名和 100 台服务器托管庞大的命令及控制架构。 使用 USB 闪存盘数据恢复恶意软件映射物理隔绝网络。这些物理隔绝网络极为敏感，以至于未连接至因特网。“震网”和相关的“火焰”恶意软件平台同样拥有缩小物理隔绝的能力。 一 种在 Windows 的现代版本中绕过代码签名限制的特殊方法（或许该方法算不上真正新颖），这要求所有与操作系统内核接口的第三方软件由公认的证书颁发机构签发。为规避这种 限制，方程式组织的恶意软件在一个已经签名的驱动内入侵了一个已知漏洞，供 CloneCD 实现内核级别代码执行。 总而言之，卡巴斯基研究人员通过调查研究得出这样一个结论，即方程式组织可能是世界上最厉害的计算机攻击组织，其技术能力及资源堪比“震网”及“火焰”间谍软件的开发组织。 “在我看来，方程式组织拥有最酷的技能。”卡巴斯基实验室全球研究分析团队负责人 Costin Raiu 对笔者说。他们经常与“震网”及“火焰”组织分享经验，但这些经验最初仅向方程式组织内部人员开放。毋庸置疑，方程式组织扮演着主人的角色，对外分享的内容可能仅是凤毛麟角。他们时不时就会与外界分享一些可以整合到“震网”及“火焰”病毒中的好玩意儿。 在卡巴斯基安全分析峰会周一发布的一份详尽报告中，研究人员对于方程式组织出自 NSA 之手的说法不再缺乏力度，他们提供了详实依据，强有力地暗示其为美国间谍机构。 首先，该组织以其封锁能力著称。例如，在邮件发送过程中，对思科系统路由器安装隐蔽的植入固件。 其次，方程式组织资料库极为先进的键盘记录器在源代码中用“ Grok ”（植物人）表示，与去年三月发表在 Intercept 的一篇题目为《NSA 计划如何用恶意软件感染数百万计算机》文章中的一行惊人相似。这篇文章基于斯诺登泄密文档讨论了一个由 NSA 开发的名为 Grok 的键盘记录器。 再次，方程式组织源码当中其他一些涉及“STRAITCID ”和“ STRAITSHOOTER ”部分的代码语句和 NSA 中一简称为 TAO（TailoredAccess Operations，“入侵特别行动队”）的部门所使用的最先进的恶意软件收录平台——“ STRAITBIZARRE ”中的代码有着惊人的高相似度。此外，两者除了在“strait ”（海峡）一词的拼写上不谋而合地采用了非常规方式，斯诺登此次披露出的文档中还指出，STRAITBIZARRE 在未来可能会进化为可以将被感染电脑变成一次性的，无法追踪的“射手”节点。另，代号名为 FOXACID（酸狐/尖叫的狐狸）的另一黑客工具和此前已经为人所知的 Grok 键盘记录器一样，是同一个NSA 恶意软件框架下的两个分支项目。 除了这些具有共同点的代号，方程式组织还曾于 2008 年利用了 4 个零日漏洞，其中两个后来被用于“震网”病毒。 相似点还不止于此。方程式组织一款名为 GrayFish 的恶意软件利用目标机器独一无二的 NTFS 对象 ID 的 1000 次迭代哈希对其负载进行加密。这项技术导致研究人员在缺少每个感染机器原始磁盘镜像的情况下无法访问最终负载。这与一款用来在 Gauss 中隐匿潜在强有力弹头的高级恶意软件极为相似，该款恶意软件与“震网”和“火焰”病毒在技术层面也具有很大共性。（据《纽约时报》报道，“震网”是 NSA 与以色列的联合作战项目；据《华盛顿邮报》报道，“火焰”由 NSA 、CIA 和以色列军方共同研制）。 方程式组织不仅在技术层面与“震网”和“火焰”开发者具有共性，还鼓吹这类超凡技术人才来自受世界上最富有国家资助的间谍组织。例如，方程式组织的恶意软件 平台之一改写了受感染计算机的硬盘固件，适用于包括西部数码、迈拓、三星、IBM、镁光、东芝，希捷在内的 12 类驱动。 这款恶意固件创建了一个秘密的信息存储库，能有效防止军队级别的磁盘擦除和重新格式化，可使从受害者处窃得的敏感数据即便在重新格式化驱动，重装操作系统后 仍然可用。该固件还提供方程式组织庞大恶意软件库内其他代码可以访问的编程接口。一旦硬盘遭到入侵，感染无法被检测或移除。

关于方程式组织，外界流传其最负盛名的举措就是涉嫌利用封锁的方式感染目标。这种阻断不仅证实了组织的良好架构与先进能力，还表明组织感染利益相关群体的时 间长度。2009 年休斯敦会议上的 CD 光盘试图利用 Windows 系统中的 autorun.inf 机制安装一款名为 DoubleFantasy 的恶意软件。对此，卡巴斯基拒绝予以证实，除非声明此举出于科学研究目的。卡巴斯基知悉会议主办方的确向参会人员发送了一张光盘，而且公司至少了解一位收 到恶意篡改软件的参会者身份，但涉及其他细节。公司研究人员仅提供极少信息，无法解释恶意内容如何会出现在光盘的确切原因。 Raiu 认为，“将攻击溯源至组织方并给出详情非常简单，但是可能造成后果相当严重的外交事件”。“我们能给出的最准确推测是主办方对参会者未有任何恶意举动，但部分 CD-ROMs 在电子邮件发送至参会方的过程中遭到恶意劫持篡改。” 早在六、七年前，关于一张 Windows 版本 Oracle 8i-8.1.7 安装光盘的发送事件也很少有人知晓。人们仅知道这张光盘安装了方程式组织早期开发的一款名为 EquationLaser 的恶意软件。会议及 Oracle CD 光盘是卡巴斯基研究人员迄今为止发现的由方程式组织发起的仅有拦截。从寥寥无几的封锁事件可以看出，他们应该不是经常采取这种做法。 继某字符串出现于一次利用蠕虫进行自我复制的零日入侵后，另外一种感染方式应运而生。这种方式建立在卡巴斯基 2008 年开发的一款名为 Fanny 的蠕虫基础上。那时，这个未知的漏洞存在于处理所谓 .LNK 文件功能中。一旦 USB 闪存盘与计算机相连，Windows 就会用.LNK 文件显示图标。这枚具有诱杀功能的闪存盘就会通过在 .LNK 文件中嵌入的恶意代码自动感染已连接的计算机，且即便关掉计算机的 autorun 功能也能顺利得逞。自我复制和不依赖网络连接这两项特征使该漏洞成为感染物理隔绝设备的绝佳利器。（.LNK 漏洞被划分为 CVE-2010-2568.) 大概在 Fanny 初露头角的两年后，.LNK 入侵被添加到“震网”病毒的某一版本中，这样，蠕虫就可以通过地处伊朗的高度敏感计算机自动繁殖。Fanny 同样依赖于一个在零日产生的权限提升漏洞。2009 年，入侵还曾深入“震网”。但那时，微软已通过发布 MS09-025 修补了潜在故障。

一个更为常见的感染途径是基于 Web 的攻击。此类攻击曾入侵了 Oracle 的 Java 软件框架或 IE 浏览器中的漏洞。范围涉及各类网站，从科技产品测评到伊斯兰圣战组织论坛，无所不包。除了通过这种途径植入漏洞，攻击代码还通过广告网络传播。广泛的漏洞 携带者可以解释卡巴斯基观测到的大量机器的感染源指向域控制器、数据仓库、网站主机及其他类型服务器的原因。由此看来，方程式组织不仅感染终端用户计算 机，其自身也作为被目标终端用户访问的诱杀服务器。 方程式组织的入侵以外科手术般高度的精准性著称，可以保证仅有一个特定目标遭到感染。例如，卡巴斯基公布的一份由方程式组织撰写的 PHP 脚本校验了某网站访客用户名的 MD5 哈希是否为 84b8026b3f5e6dcfb29e82e0b0b0f386 或 e6d290a03b70cfa5d4451da444bdea39 。与首次哈希对应的明文显示“未注册”，表示攻击者没有试图感染未登陆的访客。二次哈希目前已得到破解，参见破解概要。 “经过几周艰苦工作，我们仍然无法破解此 MD5 ，这使我们相信明文用户名相对复杂”， Raiu 表示，“毫无疑问，这意味着使用该用户名的访客不会遭到方程式组织感染，事实上，我们对此次入侵甚至一无所知。我猜想，该访客倘若不是采用虚假身份的组织 成员，就是他们的合伙人或此前遭受感染的已知受害者。” 此 PHP 脚本还特别留意避免感染约旦、土耳其和埃及的 IP 地址。卡巴斯基观测到，访问这些网站的用户中存在不符合上述规则的情况，但这些用户仍未遭到攻击。这表明，还有一层豁免所有人、专门瞄准最抢手访客目标的筛选。

最近，卡巴斯基观测到 standardsandpraiserepurpose.com 上的恶意链接。可以看出，该网站上的 h 值（“ h= ” 后面的文本）似乎为 SHA1 哈希。卡巴斯基仍需破解那些哈希，但公司研究人员怀疑它们专门用来针对特定人群采取定制入侵。公司正在向白帽黑客寻求破解帮助。其他哈希包括： 0044c9bfeaac9a51e77b921e3295dcd91ce3956a 06cf1af1d018cf4b0b3e6cfffca3fbb8c4cd362e 3ef06b6fac44a2a3cbf4b8a557495f36c72c4aa6 5b1efb3dbf50e0460bc3d2ea74ed2bebf768f4f7 930d7ed2bdce9b513ebecd3a38041b709f5c2990 e9537a36a035b08121539fd5d5dcda9fb6336423 PHP 入侵代码还向用 iPhone 访问网站的群体提供独一无二的网页和 HTML 代码。卡巴斯基发现这种做法行之有效。 卡巴斯基周一发布的报告对此给予了相应解释：“这意味着入侵服务器可能已经意识到 iPhone 访客群体的存在，并且也可将其设为攻击目标”。“否则，入侵链接就可以被轻松移除。”这份报告还提出感染服务器受大量中国机器访问，这些机器在浏览器用户 代理字符串中自我标志为 Macs 。虽然卡巴斯基仍需获得方程式组织运行在 OS X 上的恶意软件，他们坚信此类事件确实存在。 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： EquationLaser：一款使用于 2001 至 2004 年的早期植入。 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 。 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。

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。它完全托管于注册表中，凭借 bootkit 在计算机启动时提权。EquationDrug 重新闪存 6 种类型的硬盘，GrayFish 重新闪存 12 种类型的硬盘。GrayFish 入侵了 CloneCD 驱动 ElbyCDIO.sys 中的一个漏洞，从而绕过 Windows 代码签名要求。其他程序的硬盘可能也难幸免。

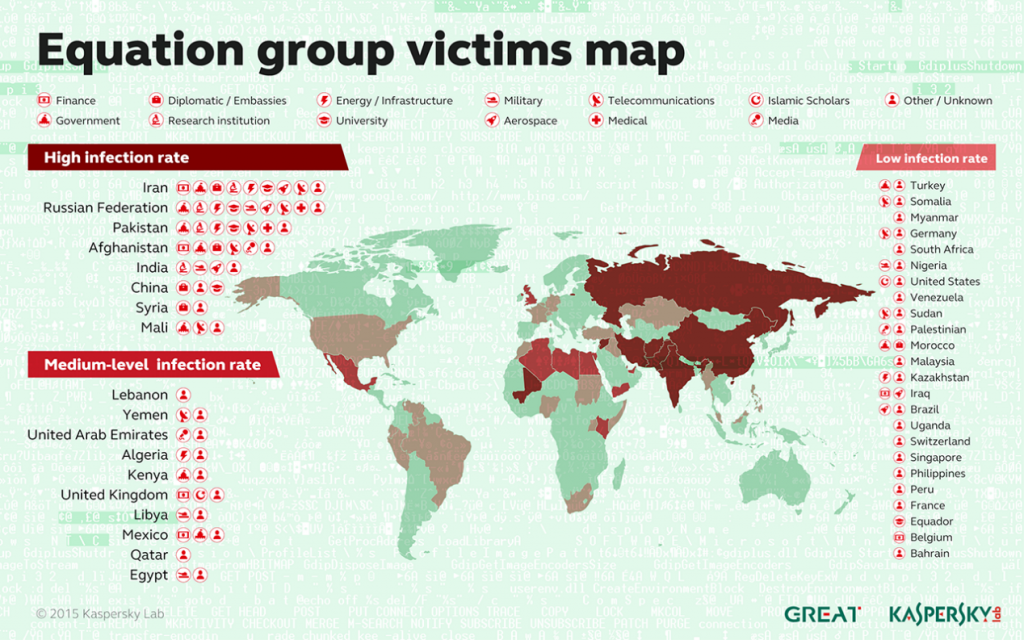
“ VBR ”的全称是“ Virtual Boot Record ”，意为“虚拟引导记录”。这是磁盘负责装载操作系统的一块特殊区域。“ Pill ”（药丸）指一串注入代码（“蓝药丸”、“红药丸”——引用了《黑客帝国》中的典故），负责劫持操作系统加载。工作原理是通过仔细修改加载机制将操作系统 盲目“吞入”的恶意代码包括进来。 BBSVC 服务是另一种 GRAYFISH 机制，用于由某种未知原因导致的“药丸”无法被注入的情况。它在操作系统启动时加载 Grayfish 的后续阶段。实质上，这是一个比药丸更弱的机制，因为它在受害者的硬盘驱动上暴露了一个独立的恶意可执行程序。这很好地解释了为何 BBSVC 是一个多形态可执行程序，程序内部填充的乱码和随机数据使其很难被检测出来。平台内核“ fvexpy.sys ”是 Grayfish 的核心部件之一，在 Windows 内核模式下运行并为平台部件提供相关功能。 GrayFish 是方程式组织取得的至高成就。该恶意软件平台十分复杂，导致卡巴斯基研究人员至今对其能力及内部工作仅有着粗浅了解。 GrayFish 复杂性的关键是 bootkit 使其对感染机器采取非常精细的控制。

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

在 Raiu 看来，无论是多么强大的黑客组织，都难免会犯下错误。方程式组织就曾犯下几次错误，让卡巴斯基研究人员对至少 14 年来从未曾报道过的一次行动获得关键见解。 卡巴斯基对方程式组织的了解始于 2014 年 3 月，当时公司正在调查 Regin 软件感染比利时电信等其他目标事件。在此过程中，公司研究人员分析了一台位于中东地区的计算机并将其命名为“ Magnet of Threats ”（威胁吸附体），因为除 Regin 外，它还被包括 Turla、Careto、Mask、ItaDuke 和 AnimalFarm （动物农场）在内的另外四种高级恶意软件感染。一份前所未见的恶意软件样本引起了研究人员的兴趣，结果证实其为一款 EquationDrug 模块。 此后，卡巴斯基研究人员梳理了他们根据 AV 用户报告的入侵和感染情况搭建起来的卡巴斯基云安全网络，并寻找其中的相似性与关联。在接下来的几个月，研究人员又公布了方程式组织使用的另外几款恶意软件以及用来承载指令信道的域名。 对于攻击者来说，最惨重的代价或许就是未能对这些服务器使用的部分域名进行及时续约。在 300 多个使用的域中，大约有 20 个被允许终止。卡巴斯基快速注册了这些域名，并在过去十个月中用 sinkhole 污染指令信道。在此过程中，研究人员监控了来自方程式受感染计算机的连接。最严重的续约失败涉及一个被 EquationLaser 感染的计算机控制的信道。 EquationLaser 是一个早期的恶意软件平台，大约被丢弃于 2003 年反病毒程序开始对其检测之时。此后，底层域名仍处于活跃状态，直至卡巴斯基将其收购。截至目前，受感染的计算机仍向其报告。 Raiu 表示“看到 12 年来全世界到处充斥着被这款恶意软件感染的受害者着实令人震惊”。他陆续看到大约十几台报告自俄罗斯、伊朗、中国及印度的受感染机器。 据 Raiu 所述，90% 以上的命令和控制服务器于去年关闭，尽管一些在上个月还处于活跃状态。 “我们意识到目前所掌握的情况仅仅是冰山一角，这点值得我们深刻反思。” Sinkhole 让卡巴斯基研究人员有机会搜集此次行动的关键线索，包括报告给已占领指令域的受感染计算机数量、这些遭入侵的计算机可能位于哪些国家，以及这些计算机运行的操作系统类型。 卡巴斯基搜集到的另一条关键信息是：一些被方程式组织感染的机器为“  patient zero ”（首个传染源）。这些机器曾被用于播种“震网”蠕虫，这样蠕虫就可以顺流而下，感染伊朗的纳坦兹设施。 卡巴斯基研究人员在他们的报告中写道：“方程式组织极有可能被用来传递“震网”负载。” 其他关键破绽包括残留在方程式组织各种恶意软件中的变量名称、开发者账户名称等类似的人工痕迹。好比偷东西的猫用带爪套的方式隐藏踪迹，攻击者在发布代码之 前也在试图将此类痕迹消除上下了大工夫。但至少在 13 种情况下均以失败告终。由于附有指向方程式组织的高级键盘记录器，字符串“ -standalonegrok\_2.1.1.1 ”或许称得上是最显著的人工痕迹。 卡巴斯基发现的另一个具有潜在危害的人工痕迹是：属于编译方程式组织恶意软件开发者账户之一的 Windows 的目录路径为：“ c:\users\rmgree5 ”，这里，如果 rmgree 不是随机生成的账户名，而 handle 曾被用于开发者其他账号或其命名与开发者真实姓名相关联（如被命名为“ RichardGree ”或“ Robert Greenberg ”），那么，通过此路径追踪到开发者的真实身份将成为可能。 卡巴斯基研究人员仍不知该如何分析余下的 11 处人工痕迹，但他们希望同事们可以将字符串与其他行动者或事件联系起来。余下的人工痕迹为：

毫无疑问，方程式组织恶意软件的开发、行动技术突破和对目标封锁所花费的时间、金钱，均由国家资助。为此项目提供的资源几乎不受限。在方程式组织键盘记录器 中发现的目标国家与非目标国家、指向“震网”及“火焰”的关联，以及 Grok 中的人工痕迹强有力地支持了 NSA 或美国有关情报部门为事件责任方的理论，但卡巴斯基拒绝将犯罪人员的名单公之于众。 更新：路透社记者 Joseph Menn 认为两位前政府雇员已经证实了硬件驱动固件的能力。他写道： 某位前 NSA 雇员向路透社透露卡巴斯基的分析真实无误，情报部门在职人员将此类情报项目的级别视为等同于“震网”。另外一位前情报人员证实 NSA 开发了在硬盘驱动中隐匿间谍软件的获奖技术，但据说他尚不知哪些间谍技术依赖于此。 更新：这篇文章发布几小时后，NSA 官方通过电子邮件向 Ars 发送了以下声明： 我们看到了这篇刚刚发布不久的报告。对于此篇报告提出的任何敏感问题，我们不做任何公开评论，也不对任何细节予以讨论。2014 年 1 月 7 日，总统为我们的信号情报行动发表了详尽致辞，他还发表了《总统政策指示》 28 ( PPD - 28 )。我们已经公开强调多次，我们将继续坚持发扬总统讲话中的精神及 PPD - 28 。美国政府号召我们情报机构保护美国、美国公民以及美国的同盟国免受包括基地组织、“伊拉克和黎凡特伊斯兰国”（ Islamic State of Iraq and the Levant ，缩写为 ISIL ）等恐怖主义阴谋、大规模杀伤性武器扩散、针对我们及我们同盟国的外族侵略，以及各种国际犯罪组织在内的各种严重威胁。 可以说，方程式组织浮出水面对于计算机及国家安全领域来说都是个新发现，与揭露“震网”相比同等重要甚至有过之而无不及。 Raiu 表示，“方程式组织浮出水面一事非常重要，因为据保守估计，这款无敌的网络间谍组织成功在雷达下隐蔽了大约 15 年。他们掌握了令人难以置信的技术和高科技能力，例如感染十几个不同品牌的硬盘驱动固件等，这在我们看来简直独一无二，无与伦比。随着威胁分子变得越来越 难对付，我们意识到目前所掌握的情况仅仅是冰山一角，这点值得我们深刻反思。”





以下内容来自

（https://baijiahao.baidu.com/po/feed/share?wfr=spider&for=pc&context=%7B%22sourceFrom%22%3A%22bjh%22%2C%22nid%22%3A%22news\_3118532462411263319%22%7D）：

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。

据了解，受影响的Windows 版本包括Windows NT，Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8，Windows 2008、Windows 2008 R2、Windows Server 2012 SP0等。

正在使用这些Windows操作系统的你，有没有在颤抖！！虽然微软宣布已修复大部分的漏洞，但这场由于远程漏洞泄露造成的灾难性网络大地震“余震”仍在。

其实，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。美小创安全后援团搜罗了好多的资料，来给大家说一说，这两个组织的“前世今生”。

黑了人的影子经纪人（ Shadow Brokers）

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。

同年10月份，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。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。

直到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。

时隔一周，耐不住寂寞的Shadow Brokers又有了大动作，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，之后很快有网友解密并长传到github，网络大地震由此开始...

被黑了的方程式组织 (Equation Group)

说来实在嘲讽，方程式组织本身就是一个黑客组织，加密水平以及黑客技术全球领先。根据安全信息领域的媒体报道，“方程式组织”与美国国家安全局关系密切，是一个该局可能“不愿承认”的部门，这在黑客圈几乎是公开的秘密。

“方程式组织”庞大，攻击水平极高，多年来，他们向全世界释放了多种病毒。这些病毒各具特色，分别采用不同的传播手法，设定了不同的攻击目标，给全世界的网络安全造成了极大破坏。例如，有多条证据表明，曾经破坏伊朗核工厂的“震网病毒”，就是“方程式组织”的一大“杰作”。

因此，“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。

“方程式”病毒另一个可怕之处，在于其特别擅长攻击隔离网络，并在隔离网络和互联网之间传送信息。所谓隔离网络，是指那些隔离开来、与互联网并不直接连通的网络，广泛应用于工业控制之中，用以隔绝在互联网上泛滥成灾的病毒。

但在“方程式”面前，隔绝网络也并不安全。据大名鼎鼎的泄密者爱德华·斯诺登所言，即使是美国国家安全局（NSA）也难免百密一疏。NSA人员也会偷懒，有时会将文件留在自己所黑的服务器中。

这样，影子经纪人成功获取疑为NSA的攻击工具也就不足为奇了。

攻击工具

说回事件本身，本次攻击影响的微软产品的漏洞攻击工具一共12个：



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。