WannaCry只是前戏 黑客组织还要再放一个大招

2017-05-17 Coremail论客

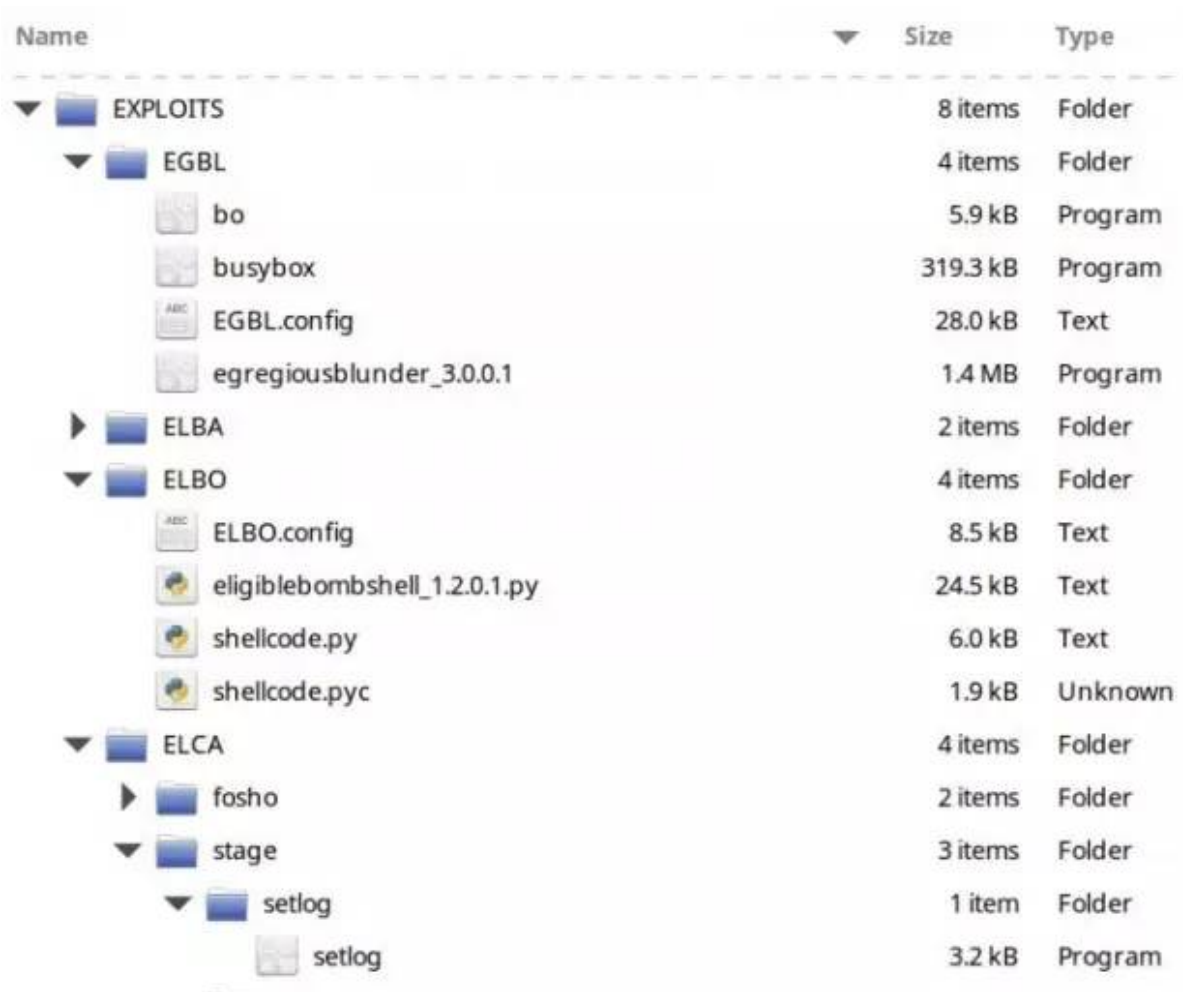
最近，一场惊天勒索大案在全世界明目张胆的上演，犯罪分子在众目睽睽之下向全世界网民索要赎金，而且七天之内不给，就会撕票。如今的科技大片果然骨骼清奇，一不小心我等吃瓜群众都可能成为其中的小虾米被吃掉。

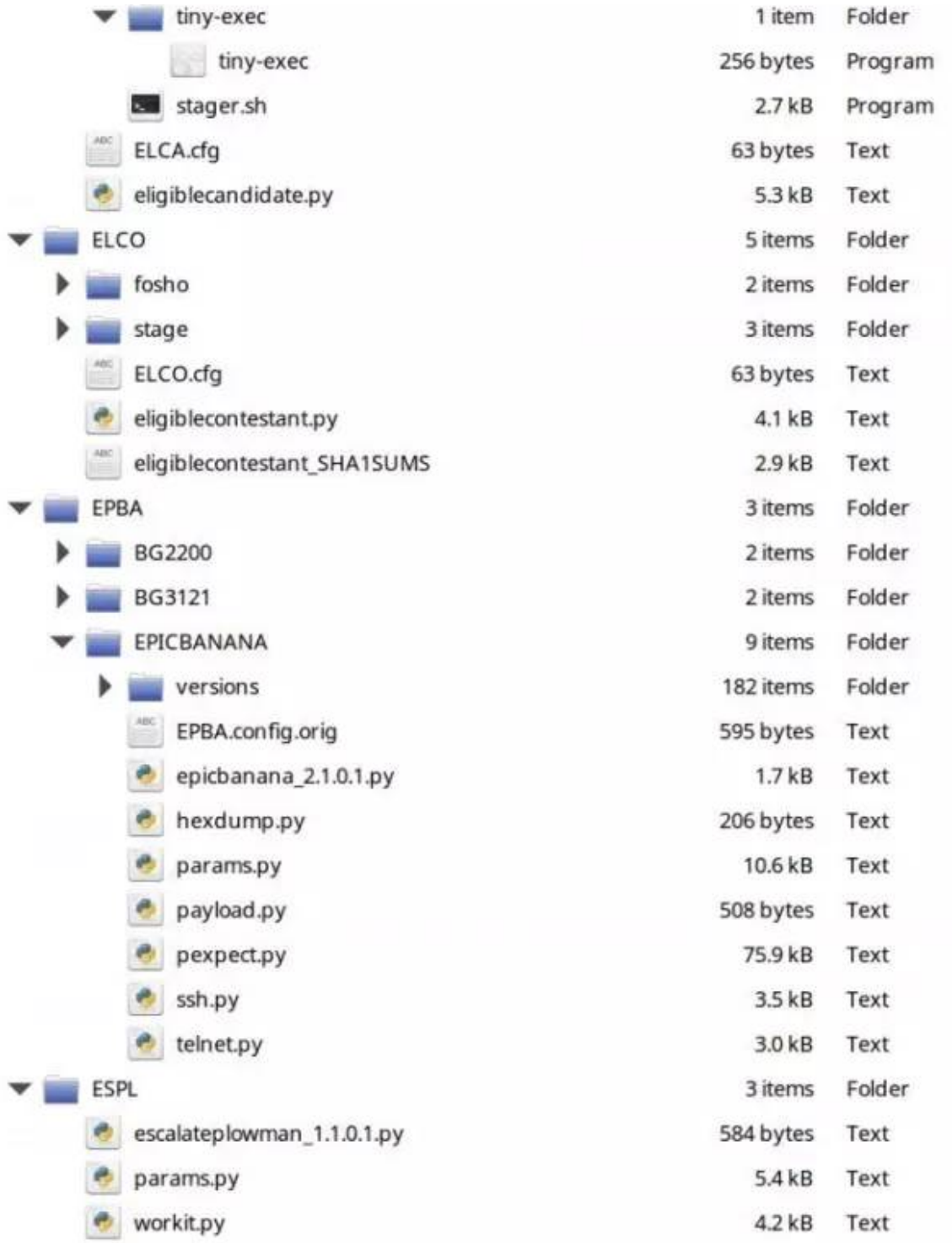
案情说起来也并非那么扑朔迷离：黑客组织“影子经纪人”和美国NSA黑吃黑，互相掐架不成，前者恼羞成怒，决定给点颜色看看，于是发起举世闻名的“WannaCry”勒索病毒，最终导致全球150多个国家跟着遭殃。

首选，我们将目光锁定一个机构——NSA（National Security Agency），美国国家安全局。这一机构又称国家保密局，隶属于美国国防部，是美国政府机构中最大的情报部门，专门负责收集和分析外国及本国通讯资料。黑客所使用的“永恒之蓝”，就是NSA针对微软MS17-010漏洞所开发的网络武器。

事情是这样的：NSA本身手里握有大量开发好的网络武器，但在2016年6月，“永恒之蓝”等十几个武器被黑客组织“影子经纪人”（ShadowBreakers）窃取。

8月份，影子经纪人将部分被盗的黑客工具在网上售卖，还将其中一部分供人民免费下载。当时影子经纪人当时的心里价值是100万比特币（折合 5.68亿美元）。





这些工具来自和美国 NSA有着说不清道不明关系的黑客团队——方程式组织（Equation Group）。而很多证据都表明，方程式组织就是 NSA 旗下用来进攻全世界重要目标的“黑客特种兵”。

影子经纪人本意是想让 NSA 的方程式小组自己把工具赎回去，结果后者完全没有搭理他们。更加不幸的是，其他人也对这些工具没有表现出太大的兴趣。

结果影子经纪人收到的竞拍款只有25美元左右。

于是，影子经纪人再也坐不住了，开始放大招了。

今年1月，影子经纪人在网上发布了多个NSA 网络武器库中的程序截图，其中包括微软Windows 系统的重大漏洞。

到了2月份，微软公司果然打破了原本雷打不动的在周二发布系统补丁的习惯，这说明他们遇到了重大的漏洞需要修补和发布。

3月，微软方面针对多个 SMB远程通讯漏洞发布了修复补丁。其中影响此次全球勒索病毒传播的“永恒之蓝”漏洞补丁就包括在内。同期，甲骨文公司也修复了“大量安全漏洞”。

到了4月，影子经纪人在网上公开当时截图中的多个黑客武器和漏洞。

时至5月，影子经纪人发起了施虐全球的WannaCry 勒索事件。这次事件让全球150多个国家的超过10万家组织和机构被攻陷，其中包括1600家美国组织，11200家俄罗斯组织，中国则有29000多个IP被感染。在西班牙，电信巨头Telefonica，电力公司Iberdrola，能源供应商Gas Natural在内的众多公司网络系统瘫痪；葡萄牙电信、美国运输巨头FedEx、瑞典某地方政府、俄罗斯第二大移动通信运营商Megafon都已曝出遭受攻击。随着病毒版本的更新迭代，具体数字可能还会增加。

截至5月16日 ，勒索病毒总计约讹到35万人民币。

显然，黑客分子对这一数字很不满意。当晚，黑客组织“影子经纪人”在外国社交媒体 Steemit 网站上宣称接下来还会有一个大招：

6月，影子经纪人将公布“影子经纪人数据曝光月（The Shadow Brokers Data Dump of the Month）”服务。

计划推出一项新的月度订阅模式，类似于俱乐部每月向会员提供酒水的形式。会员按月支付费用，而我们则向每位会员提供曝光数据。会员可根据自身意愿对这些数据加以使用。

影子经纪人月度数据曝光服务可能包括：

网络浏览器、路由器与手机漏洞及相关工具；

来自更新Ops Disks中的选定条目，包括适用于Windows10的其它新型漏洞；

来自更多SWIFT供应商及中央银行机构的内部网络数据；

来自俄罗斯、中国、伊朗以及朝鲜的核武器与导弹项目的内部网络数据。

更多细节信息将于今年6月正式披露。

如果责任方在全面出售前买下所有丢失数据，则影子经纪人将不再拥有持续出售此类敏感信息的经济动力，并承诺将相关内容永久移除。相信有关方面知道我们的比特币地址。

细思极恐，想想当年金融危机，在一片歌舞升平之下，危机突然而来，然后经济进入大规模萧条，多少人破产、跳楼。在如今这个地球村，除了人为的金融危机，网络安全危机，再没有一种自然灾害是具有世界影响性的了。

而这次“WannaCry”勒索病毒感染，踏踏实实给我们上了一堂非常生动、非常深刻的网络安全教育课。科技最发达的美国已经拥有了自己的网络军队，随时利用信息发起政治、经济大战，更有不少心怀不轨的黑客分子利用网络黑洞攫取利益。网络安全防不胜防，无论是普罗大众，还是政府、企业、机构再也不能对此视若无睹、置若罔闻。

好在我们国家早已经意识到网络安全的重要性。《网络安全法》将在今年6月会全面实施，网络安全已经成为上升到国家发展层面上的战略方向，维护网络净土，保护用户隐

私安全，也是企业不可推卸的社会责任。Coremail也多次代表中国电子邮件行业出席国际网络安全大会，为世界网络安全建言献策。

网络安全已经成为一个新常识。作为普通网民，企业CIO，更应该意识到网络安全的重要性，及时更新系统，选择安全可靠的软件产品。

更多精彩文章，请点击标题

Coremail&网易：我们的目标是搞个大事情！
Coremail吴秀诚受聘为华南理工大学MBA校外导师
网易市值逼近400亿美金，丁磊对发家产品邮箱业务放松了吗？
Coremail校园邮论客v1.0正式上线
春成集团升级Coremail XT5邮件系统
取代IBM，本土邮件品牌扛起软件国产化大旗