研究人员发现更多 WannaCry 与朝鲜黑客组织关联的证据

pigsrollaroundinthem (39396)发表于 2017年05月23日 16时58分 星期二

来自私下黑钱部门

Google、赛门铁克和卡巴斯基的安全研究人员上周报告了勒索软件 WannaCry 可能与朝鲜黑客组织 Lazarus Group 有关联的证据。现在，赛门铁克通过最新的官方博客报告了更多的证据。在 5 月 12 日WannaCry 全球性爆发前，其早期版本曾在二月、三月和四月份用以执行少量目标性攻击。早期版本的 WannaCry 和 2017 年 5 月的版本基本相同，只是传播方式有所差别，区别是后者整合了 NSA 的代码。攻击者所使用的工具、技术和基础设施与之前 Lazarus 攻击事件有大量共同点：

> 在 WannaCry 于二月份的首次攻击之后，受害者网络上发现了与 Lazarus 有关恶意软件的三个组成部分—— Trojan.Volgmer 和 Backdoor.Destover 的两个变体，后者是索尼影业公司攻击事件中所使用的磁盘数据清除工具；Trojan.Alphanc 用以在三月和四月份中传播 WannaCry，该病毒是 Backdoor.Duuzer 的修正版，而 Backdoor.Duuzer 之前与 Lazarus 有所关联；Trojan.Bravonc 与 Backdoor.Duuzer 和 Backdoor.Destover 使用相同的 IP 地址以进行命令和控制，而后两者均与 Lazarus 有所关联；Backdoor.Bravonc 的代码混淆方法和 WannaCry 与 Infostealer.Fakepude（与 Lazarus 有所关联）相似。

回复

« 储存在空间站的小鼠精子繁育了健康的后代 | 诺基亚与苹果达成专利授权协议，和解诉讼 »

研究人员发现更多 WannaCry 与朝鲜黑客组织关联的证据 | **8**条评论

显示选项

样式: 嵌套平铺

声明: 下面的评论属于其发表者所有，不代表本站的观点和立场，我们不负责他们说什么。

“让你吹嘘的专家先表演着，后面更精彩。” 匿名用户 (得分:0) 2017年05月23日 17时05分 星期二

“写程序的跟幕后金主是一回事么？” 匿名用户 (得分:0) 2017年05月23日 17时05分 星期二

“再仔细找找，过两天说不定还能发现朝文注释呢” 匿名用户 (得分:0) 2017年05月23日 17时09分 星期二

“我们找到了朝鲜文的注释！一定是朝鲜干的！” 匿名用户 (得分:0) 2017年05月23日 18时57分 星期二

“写程序的跟幕后金主是一回事么？” 匿名用户 (得分:0) 2017年05月23日 20时13分 星期二

原文：“但WannaCry攻击事件并不具有民族或国家所资助活动的特点，更像是典型的网络犯罪活动” 匿名用户 (得分:0) 2017年05月23日 17时07分 星期二

wannacry是使用tor跟C&C服务器通信的，怎么确定的C&C的IP地址？ 匿名用户 (得分:0) 2017年05月23日 17时09分 星期二

估计再过两天就能找到朝鲜文注释了 匿名用户 (得分:0) 2017年05月23日 20时27分 星期二

程序员的问题是你无法预料他在做什么，直到为时已晚--Seymour Cray

消息

本文已被查看 1580 次

科技行者

您可能关注的文章

朝鲜的网络战能力引起关注

几乎所有的 WannaCry 受害者运行的是 Winc

新 SMB 僵尸网络利用了 7 个 NSA 工具

HandBrake 黑客窃取了 Panic 的源代码，勒

Shadow Brokers 威胁出售新的黑客工具

研究人员向 XP 用户提供 WannaCry 免费解

官媒认为美国应该对勒索软件攻击承担部分

挖矿僵尸网络在 WannaCry 前利用相同的 N

FileZilla 用户创建分支 FileZilla Secure

研究人员发现第一种利用Telegram的勒索软