披露美国中央情报局CIA攻击组织对中国关键领域长达十一年的网络渗透攻击

国际安全智库 2020-03-04 共100878人围观，发现 14 个不明物体 网络安全

记载历史时刻，全球首家实锤！涉美CIA攻击组织对我国发起网络攻击。

全球首家实锤

360安全大脑捕获了美国中央情报局CIA攻击组织（APT-C-39）对我国进行的长达十一年的网络攻击渗透。在此期间，我国航空航天科研机构、石油行业、大型互联网公司以及政府机构等多个单位均遭到不同程度的攻击。

不但如此，360安全大脑通过关联相关情报，还定位到负责从事研发和制作相关网络武器的CIA前雇员：约书亚·亚当·舒尔特(Joshua Adam Schulte)。在该组织攻击我国目标期间，他在CIA的秘密行动处(NCS)担任科技情报主管职位，直接参与研发了针对我国攻击的络武器：Vault7（穹窿7）。这部分相关线索，更进一步地将360安全大脑发现的这一APT组织的攻击来源，锁定为美国中央情报局。

美国中央情报局（Central Intelligence Agency，简称CIA），一个可以比美国国家安全局（NSA）更为世人熟知的名字，它是美国联邦政府主要情报搜集机构之一，下设情报处(DI)、秘密行动处 (NCS) 、科技处(DS&T)、支援处(DS)四大部门，总部位于美国弗吉尼亚的兰利。

其主要业务包括：

收集外国政府、公司和个人的信息；

分析其他美国情报机构收集的信息以及情报；

提供国家安全情报评估给美国高级决策者；

在美国总统要求下执行或监督秘密活动等。

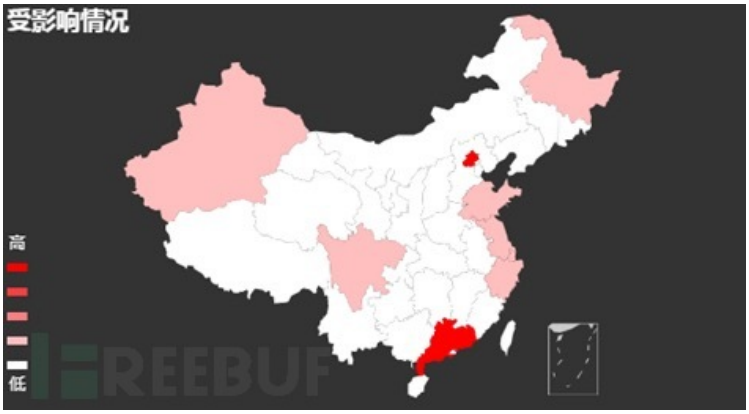
CIA核心网络武器“Vault7”成重要突破口，360安全大脑全球首家捕获涉美攻击组织 APT-C-39

时间追溯到2017年，维基解密接受了来自约书亚的“拷贝情报”，向全球披露了8716份来自美国中央情报局CIA网络情报中心的文件其中包含涉密文件156份，涵盖了CIA黑客部队的攻击手法、目标、工具的技术规范和要求。而这次的公布中，其中包含了核心武器文——“Vault7（穹窿7）”。

360安全大脑通过对泄漏的“Vault7（穹窿7）”网络武器资料的研究，并对其深入分析和溯源，于全球首次发现与其关联的一系列针我国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等长达十一年的定向攻击活动。

而这些攻击活动最早可以追溯到2008年（从2008年9月一直持续到2019年6月左右），并主要集中在北京、广东、浙江等省份。

而上述这些定向攻击活动都归结于一个鲜少被外界曝光的涉美APT组织——APT-C-39（360安全大脑将其单独编号）。



关于APT-C-39组织其攻击实力如何，有多大的安全隐患？这里以航空航天机构为例说明。

因涉及国家安全领域，所以我们只披露360安全大脑所掌握情报数据的部分细节：其中CIA在针对我国航空航天与科研机构的攻击中，们发现：主要是围绕这些机构的系统开发人员来进行定向打击。

而这些开发人员主要从事的是：航空信息技术有关服务，如航班控制系统服务、货运信息服务、结算分销服务、乘客信息服务等。

(航空信息技术有关服务：指为国内与国际商营航空公司提供航班控制系统服务，乘客信息服务，机场旅客处理系统服务及相关数据、伸信息技术服务。)

值得注意的是，CIA所攻击的航空信息技术服务，不仅仅是针对国内航空航天领域，同时还覆盖百家海外及地区的商营航空公司，CIA举的目的到底为何?

其实，对于CIA来说，为获取类似的情报而进行长期、精心布局和大量投入是很常见的操作。

就在今年2月初，《华盛顿邮报》等媒体的联合调查报道指出，CIA从上世纪五十年代开始就布局收购并完全控制了瑞士加密设备厂商Crypto AG，在长达七十年的历史中，该公司售往全球一百多个国家的加密设备都被CIA植入了后门程序，使得这期间CIA都可以解密些国家的相关加密通讯和情报。

至此，我们可以推测：CIA在过去长达十一年的渗透攻击里，通过攻破或许早已掌握到了我乃至国际航空的精密信息，甚至不排除CIA实时追踪定位全球的航班实时动态、飞机飞行轨迹、乘客信息、贸易货运等相关情报。

如猜测属实，那CIA掌控到如此机密的重要情报，将会做出哪些意想不到的事情呢？获取关键人物的行程信息，进而政治威胁，或军事压……

这并不是危言耸听，2020年1月初，伊朗一代“军神”卡西姆·苏莱曼尼被美国总统特朗普轻易“猎杀”，其中掌握到苏莱曼尼航班和程的精确信息就是暗杀成功的最关键核心，而这些信息正是以CIA为代表的美国情报机构通过包括网络攻击在内的种种手段获取的。这事件，是美国情报机构在现实世界作用的一个典型案例。

CIA”武器”研发关键人物：约书亚•亚当•舒尔特(Joshua Adam Schulte)

提到CIA关键网络武器——Vault7（穹窿7），就不得不介绍一下这位CIA前雇员：约书亚·亚当·舒尔特(Joshua Adam Schulte)。

约书亚·亚当·舒尔特(Joshua Adam Schulte，以下简称约书亚)，1988年9月出生于美国德克萨斯州拉伯克，现年31岁，毕业于德萨斯学斯汀分校，曾作为实习生在美国国家安全局（NSA）工作过一段时间，于2010年加入美国中央情报局CIA，在其秘密行动处（NCS担任科技情报主管。

国家秘密行动处(NCS)充当中央情报局秘密部门，是协调、去除冲突以及评估美国情报界秘密行动的国家主管部门。

精通网络武器设计研发专业技术，又懂情报运作，约书亚成为CIA诸多重要黑客工具和网络空间武器主要参与设计研发者核心骨干之一这其中就包含“Vault7（穹窿7）” CIA这一关键网络武器。

2016年，约书亚利用其在核心机房的管理员权限和设置的后门，拷走了“Vault7（穹窿7）” 并“给到”维基解密组织，该组织于20年将资料公布在

2018年，约书亚因泄露行为被美国司法部逮捕并起诉，2020年2月4日，在联邦法庭的公开听证会上，**检方公诉人认定，约书亚作为网络武器的核心研发人员和拥有其内部武器库最高管理员权限的负责人，将网络武器交由维基解密公开，犯有“在中央情报局历史上大的一次机密国防情报泄露事件”。**

以上约书亚的个人经历和泄露的信息，为我们提供了重要线索，而其研发并由美国检方公诉人证实的核心网络武器“Vault7（穹窿7）”，成为实锤APT-C-39隶属于美国中央情报局CIA的重要突破口。

五大关联证据实锤：APT-C-39组织隶属于美国中央情报局

以“Vault7（穹窿7）” 为核心关联点，再透过约书亚以上一系列经历与行为，为我们定位APT-C-39组织的归属提供了重要线索信息。此外，再综合考虑该APT-C-39网络武器使用的独特性和时间周期，360安全大脑最终判定：该组织的攻击行为，正是由约书亚所在的CIA主导的国家级黑客组织发起。具体关联证据如下：

证据一

APT-C-39组织使用了大量CIA”Vault7(穹窿7)”项目中的专属网络武器。

研究发现，APT-C-39组织多次使用了Fluxwire，Grasshopper等CIA专属网络武器针对我国目标实施网络攻击。

通过对比相关的样本代码、行为指纹等信息，可以确定该组织使用的网络武器即为“Vault7（穹窿7）” 项目中所描述的网络攻击武器。

证据二

APT-C-39组织大部分样本的技术细节与“Vault7（穹窿7）”文档中描叙的技术细节一致。

360安全大脑分析发现，大部分样本的技术细节与“Vault7（穹窿7）” 文档中描叙的技术细节一致，如控制命令、编译pdb路径、加方案等。

这些是规范化的攻击组织常会出现的规律性特征，也是分类它们的方法之一。所以，确定该组织隶属于CIA主导的国家级黑客组织。

证据三

早在“Vault7（穹窿7）”网络武器被维基解密公开曝光前，APT-C-39组织就已经针对中国目标使用了相关网络武器。

2010年初，APT-C-39组织已对我国境内的网路攻击活动中，使用了“Vault7（穹窿7）”网络武器中的Fluxwire系列后门。这远远早2017年维基百科对“Vault7（穹窿7）”网络武器的曝光。这也进一步印证了其网络武器的来源。

在通过深入分析解密了“Vault7（穹窿7）” 网络武器中Fluxwire后门中的版本信息后，360安全大脑将APT-C-39组织历年对我国境目标攻击使用的版本、攻击时间和其本身捕获的样本数量进行统计归类，如下表：

从表中可以看出，从2010年开始，APT-C-39组织就一直在不断升级最新的网络武器，对我国境内目标频繁发起网络攻击。

证据四

APT-C-39组织使用的部分攻击武器同NSA存在关联。

WISTFULTOLL是2014年 NSA泄露文档中的一款攻击插件。

在2011年针对我国某大型互联网公司的一次攻击中，APT-C-39组织使用了WISTFULTOOL插件对目标进行攻击。

与此同时，在维基解密泄露的CIA机密文档中，证实了NSA会协助CIA研发网络武器，这也从侧面证实了APT-C-39组织同美国情报机的关联。

证据五

APT-C-39组织的武器研发时间规律定位在美国时区。

根据该组织的攻

恶意软件的编译时间是对其进行规律研究、统计的一个常用方法，通过恶意程序的编译时间的研究，我们可以探知其作者的工作与作规律，从而获知其大概所在的时区位置。

下表就是APT-C-39组织的编译活动时间表（时间我们以东8时区为基准），可以看出该组织活动接近于美国东部时区的作息时间，符CIA的定位。（位于美国弗吉尼亚州，使用美国东部时间。）

综合上述技术分析和数字证据，我们完全有理由相信：APT-C-39组织隶属于美国，是由美国情报机构参与发起的攻击行为。

尤其是在调查分析过程中，360安全大脑资料已显示，该组织所使用的网络武器和CIA “Vault7（穹窿7）” 项目中所描述网络武器/完全吻合。而CIA “Vault7（穹窿7）” 武器从侧面显示美国打造了全球最大网络武器库，而这不仅给全球网络安全带来了严重威胁更是展示出该APT组织高超的技术能力和专业化水准。

战争的形式不止于兵戎相见这一种。网络空间早已成为大国较量的另一重要战场。而若与美国中央情报局CIA博弈，道阻且长！

***本文作者：国际安全智库，转载请注明来自FreeBuf.COM**

更多精彩 # apt # APT-C-39 # CIA # 中情局 # 网络渗透

相关推荐

全球高级持续性威胁（APT）2019年中报告

CIA泄露文档最新曝光：针对Windows系统的网络武器Grassho...

年终盘点：南亚APT组织“群魔乱舞”，链条化攻击“环环相...

全球高级持续性威胁（APT）2019年中报告

这些评论亮了

嗷嗷嗷 (1级)
这是人家泄漏导致暴漏的资料分析出来，没泄漏的呢？？？

回复

亮了(18

已有 14 条评论

斯坦尼斯拉夫斯基的拖拉机 2020-03-03 1楼 回

被钉在墙上狠狠的锤了

亮了 (

嗷嗷嗷 (1级) 2020-03-03 2楼 回

这是人家泄漏导致暴漏的资料分析出来，没泄漏的呢？？？

亮了 (1

CIA 2020-03-03 3楼 回

气死我了！！！

咱们搞了那么多次入侵，哪次是别人披露出来的？？？

耻辱啊耻辱!

哼哼哼啊啊啊啊啊啊啊啊啊啊啊

亮了

老司机 2020-03-03 4楼 回

照这种理论其他国家使用美国CIA Vault7武器那就是美国干的?

亮了

嘟嘟读 2020-03-04

@ 老司机 17年泄漏出来，17年之前的肯定是美帝干的啊，长点脑子啊

亮了

lovebear (1级) 2020-03-05

@ 老司机 看文章都不仔细看就发评论吗

亮了

咿呀 2020-03-03 5楼 回

美帝亡我之心不死

亮了

CDra90n (1级)... 2020-03-04 6楼 回

666

亮了

j4543519 (1级) 2020-03-04 7楼 回

同意老司机的说法 下次发这种文章的时候最好把样本发出来

亮了

样本 2020-03-04

@ j4543519 360能发现不就是因为它样本多吗？不如叫老周把股权交出来算了

亮了

test 2020-03-04 8楼 回

讲道理

就这些"证据"来看,不是很充分.

如果能反向渗透,在"有限控制"的条件下,获得该组织成员的信息.

以及该组织和CIA的内部关联证据，对"技术派"会比较有说服力

应该要这么干才对

不过,这么干了,获得的证据是否能公布,要怎么公布,又是一个问题

360太着急了

亮了

WWW 2020-03-04 9楼 回

啧啧啧，终于有证据了

嘎嘎嘎 2020-03-04 10楼 回

淡定 我国机密电脑不允许连公网 都是私网 而且严禁u盘拷贝文件 都是用光碟储存重要文件的

亮了 (

dj0733 (1级) 2020-03-05 11楼 回

我还以为是什么大咖，原来是个新兵蛋子，2019 年 9 月份注册的 ID 上来就对美国一顿黑。

亮了 (

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。登录? 注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

国际安全智库

这家伙太懒，还未填写个人描述!

1 文章数

0 评论数

6 关注者

关注

最近文章

披露美国中央情报局CIA攻击组织对中国关键领域长达十一年的网络渗透攻击 2020.03.04

如此高调的网络部队被“轻易秒杀”，奥地利这波网络战运作堪称完美 2020.03.02

再揭秘一场阴谋！半岛APT“趁势之危”对我国商贸相关政府机构发动攻击！阴险狡诈！ 2020.02.13

浏览更多

文章目录

相关阅读

APT组织“拍拍熊”对巴勒斯坦政府攻...
新冠危机未除，印度又对我国卫生部门...
海莲花组织针对中国APT攻击的最新样...
维基解密又更新：BothanSpy和Gyrfal...
BUF大事件丨实锤！涉美CIA攻击组织...

推荐关注

活动预告

3月

漏洞挖掘组合拳，各大SRC打通关

未开始

3月

如何在Windows系统下进行二进制安全学习

已结束

2月

漏洞挖掘神器训练营

已结束