选自Wired

作者：Andy Greenberg

机器之心编译

参与：Panda

> 22 岁那年，马库斯·哈钦斯（Marcus Hutchins）凭一己之力阻止了有史以来最严重的网络攻击 WannaCry。不久后他因为开发恶意软件 Kronos 被 FBI 逮捕。本文将讲述他不为人知的故事。

窥探暗面的青少年黑客

许多母亲对互联网恶魔的恐惧被夸大了，但 Janet 的恐惧并没有。

哈钦斯得到自己的计算机后不到一年，就开始探索初级黑客网络论坛——一个致力于在当时流行的即时通信平台 MSN 上搞破坏的论坛。他在这里发现了一个社区，里面都是和他想法一样的年轻黑客在炫耀自己的成果。有一个黑客吹嘘自己创造了

一种可以伪装成 JPEG 的 MSN 蠕虫病毒。当有人打开这个文件时，这个恶意软件会立即以隐藏方式将自己发送给该用户的所有 MSN
联系人；其中一些人会打开这张图片，进而导致下一轮的传播。

哈钦斯当时并不知道这样的蠕虫有什么实际用处，但这却给他留下了非常深刻的印象。「我当时想，太酷了，编程居然能做这种事。」他说，「我也想做这种事。」

14 岁那年，他为该论坛做出了自己的贡献——一个简单的密码窃取软件。只要将其安装在某人的电脑上，它就能直接拉取受害者存储在 IE
浏览器中的网络账户的密码。这些密码是经过加密的，但哈钦斯找到了 IE
浏览器隐藏解密密钥的位置。

哈钦斯的第一款恶意软件得到了该论坛的认可。但他想用这款恶意软件盗取谁的密码呢？「我不知道，真的。」哈钦斯说
，「我当时只是想：我做了个很酷的东西。」

随着哈钦斯的黑客事业开始成型，他的学业受到了影响。他傍晚从海滩回家后会径直回自己的卧室，在电脑面前吃饭，然后假装睡觉。在他的父母看他熄灯之后回自己房间睡觉时，他又会回到电脑前。「他瞒着我们一直编程到凌晨。」Janet 说，当她第二天早上叫醒他时，「他看起来很憔悴，因为他只睡了半小时。」不明就里的母亲非常担心，于是带他去看了医生，结果被诊断为睡眠不足。

大约 15 岁那年的一天，哈钦斯在学校发现自己的网络账户被锁定了。几小时后，他被叫到了学校的行政办公室，并被指控攻击学校的网络，导致学校不得不换掉一台遭到严重破坏的服务器。哈钦斯坚决否认参与此事，并要求查看证据。但他说学校管理员拒绝分享证据。不过那时候他在学校 IT 人员那里已经臭名昭著了。即使今天他还认为自己是最方便的替罪羊。「马库斯不擅长说谎。」他的母亲同意这一点，「他很喜欢自吹自擂。如果是他干的，他肯定会说是他干的。」

哈钦斯的账号被停用了两周，然后学校永久性地禁止他在学校使用计算机。他的回应很简单：尽可能少地待在学校。他完全变成了夜猫子，白天在课堂上睡大觉，甚至常常不去上课。他的父母很生气，但他要么乘车去学校，要么就去冲浪，大部分时候都能躲开父母的责骂和惩罚。「他们总不能强行拖我去学校，」哈钦斯说，「我是个大个子。」

2009 年，哈钦斯一家从原来那座农场搬到了前邮局房子里，新住所坐落在仅有一个酒吧的小村子中。马库斯占了顶楼的一个房间。除了获取食物和咖啡，他很少离开自己的房间，而且他大部分时间都把自己的门锁着。

差不多同时，哈钦斯经常访问的那个 MSN 论坛关闭了，因此他转到了另一个名为 HackForums 的社区。这个论坛的人技术略先进一点，而道德观也更晦暗一些：一群年轻黑客构成的「蝇王」想要通过虚无的黑客行动来折服另一群年轻黑客。要赢得 HackForums 的尊重，最小的筹码是拥有一个僵尸网络，即成百上千台会遵照该黑客的指令办事的被恶意软件感染的计算机。黑客可以使用僵尸网络向目标灌入大量垃圾流量，迫使其网络服务器离线——这种攻击方式被称为分布式拒绝服务攻击（DDoS 攻击）。

这时候，哈钦斯的英国乡村田园生活与秘密的网络朋克生活并无重叠，没有任何现实的约束能防止他进入那充斥着不道德的网络地下世界。于是年仅 15 岁的哈钦斯很快就在那个论坛上吹嘘自己运行着一个包含 8000 台计算机的僵尸网络，其中大多数都是他通过 BitTorrent 上传的虚假文件劫持的。

不仅如此，哈钦斯还开始了自己的事业。他开始租用服务器，然后以按月收费的方式向 HackForums 的成员出售网络托管服务。哈钦斯称自己的公司为 Gh0sthosting，并在 HackForums 上宣传说这是一个允许「所有非法网站」的地方。有一次一位客户问能否托管黑市软件 warez，哈钦斯立即回复说：「除了儿童色情，任何网站都可以。」

哈钦斯说，在自己当时那青少年的思想里，这些东西都算不上是「真正的」犯罪，不会让他受到执法部门注意。

但是，不到一年时间，哈钦斯就对他的僵尸网络和托管服务感到厌倦了，因为他发现这需要应付很多「喜欢抱怨的客户」。于是他不再做这两件事，而是专心于他更喜欢的事情：完善自己的恶意软件。很快他就拆分了其他黑客的 rootkit，即用于修改计算机操作系统的程序，使得恶意软件可以隐藏起来。他研究了它们的功能，学会了将自己的代码隐藏到其它计算机进程中，使得他的文件在计算机的文件目录中不可见。

当哈钦斯在 HackForums 发布了一些示例代码炫耀自己的技术时，另一位会员注意到了他，并让他写一段检查特定杀毒软件能否检测某个恶意软件的代码。从这个任务中，哈钦斯获得了价值 200 美元的 Liberty Reserve，这是一种早期的数字货币。之后，这位客户又用 800 美元购买了哈钦斯写的 formgrabber，这是一个可以秘密窃取人们输入网络表单的密码和其它数据的 rootkit。

哈钦斯在当恶意软件枪手方面开始有了些名气。然后 16 岁那年，一位更加严肃的客户接洽了他。这个人的化名是

Vinny，他为哈钦斯提供的工作任务是：一个多功能且易于维护的 rootkit，以便他能在 Exploit.in 和 Dark0de 等比 HackForums 更加专业的黑客市场上进行销售。而且回报不是预付款，而是一半的销售利润。他们将这款产品称为 UPAS Kit，得名于爪哇的 upas 毒树，其毒汁曾在东南亚地区用于制作毒镖和毒箭。

Vinny 不同于哈钦斯曾遇到过的那些喜欢自吹自擂的黑客；他更专业，口风更紧，从不谈论有关自己个人生活的任何细节。而且哈钦斯和 Vinny 都非常注意，从不保存他们的对话日志。

但哈钦斯却并未对自己的个人生活那么守口如瓶。哈钦斯曾有一次提到过自己生活在英格兰的农村地区。然后他们谈到了当时的一个新黑市网站「丝绸之路（Silk Road）」。

那时还是 2011 年，这个网站尚不为大众所知。哈钦斯当时也觉得这是个骗局。「屁话，」哈钦斯这样对 Vinny 说，「证明一下！」

于是 Vinny 要了哈钦斯的地址和出生日期。他说要给哈钦斯送一个生日礼物。哈钦斯提供了这两个信息，但很快他就后悔了。

哈钦斯 17 岁生日那天，一个包裹被邮寄到了他父母家。里面是一包毒品。

黑客明星

几个小时之后，哈钦斯及其 Kryptos Logic 的同事才意识到 WannaCry 的威胁仍

然存在。哈钦斯注册的域名仍然继续收到大量连接，说明这个蠕虫仍在继续传播。接下来的两天时间里，其收到了近 100 万个连接。如果他们的网站域名离线，那么这么多计算机中的内容都会被加密，WannaCry 的破坏还会继续。「如果这个网站下线，那么 WannaCry 就会重新开始。」哈钦斯的老板 Salim Neino 回忆说，「它会在 24 小时内感染全世界每一台易受攻击的计算机。」

问题很快就出现了。他们设置的网站遭受了 DDoS 攻击。这场攻击来自一个他们所监控的 Mirai 僵尸网络。「我们感觉自己像是阿特拉斯，全世界都在我们肩上。」Neino 说，「但现在还有人在背后踢阿特拉斯的背。」

此后的几天时间里，攻击规模逐渐升级，几乎使这个沉洞域名瘫痪。Kryptos Logic 紧张地应对，一边过滤流量，一边使用亚马逊数据中心和法国托管公司 OVH 的服务器分流。在接下来的一周里，为了保证 WannaCry 死亡开关能有效工作，哈钦斯的连续睡眠时间不超过 3 小时。

与此同时，新闻媒体也在不断刺探匿名的哈钦斯的真实身份。WannaCry 爆发两天后的星期天上午，当地一位记者出现在哈钦斯家的前门。这位记者的女儿曾与哈钦斯一起上学，并在一张写了 MalwareTech 的 Facebook 照片中看见过他。

不久之后，更多记者来按他家的门铃，他家对街的停车场停满了车，而且电话太多让他父母都不再接听了。英国小报还用夸张的标题报道他，称他是在卧室中「意外」拯救世界的英雄。为了满足这些媒体的胃口，哈钦斯接受了一次采访，但他太紧张，连自己的名字都写错了。

那些天，哈钦斯担心 WannaCry 的作者还会修改代码再次发动攻击，毕竟做起来不难。但还好并没出现这个问题。此后，在英国国家网络安全中心的协调下，亚马逊数据中心和 Cloudflare 为 Kryptos Logic 提供了流量保证，让他们能稳定地运行这个死亡开关域名。

WannaCry 爆发一周之后，最危险的时间过去了，Neino 很担心哈钦斯的健康，于是提供奖金让他休息：在床上每睡觉一小时就有 1000 美元奖金。

聚光灯虽然让哈钦斯不适，但并非全无好处。一夜之间，他的 Twitter 关注者就超过了 10 万。有在当地酒吧里认出他的人请他喝饮料，感谢他拯救了互联网。当地一家餐厅赠送了他一年的免费披萨。他的父母才终于知道儿子做了什么

，并深深地为他感到骄傲。

但直到 WannaCry 爆发三个月后的 Defcon 大会，哈钦斯才开始真正接受自己「网络安全领域巨星」的身份。为了避免总有粉丝找他合影，他和一些朋友用 AirBnb 租了一套带有巨大私人游泳池的豪宅。他们基本没有参会听演讲，而是到处参加派对聚会——充斥着各种豪华露天活动和荒唐的娱乐活动。

他玩得很嗨很开心。

此时已是离开 Kronos 三年后，哈钦斯感觉自己已经是完全不同的人了。这个冉冉升起的明星也终于开始放下自己的心结，不再担忧过去的网络犯罪经历。

然后，在拉斯维加斯最后一天的上午，他看见了一辆黑色 SUV 停在租来的豪宅门前的街道上。