

区块链基础设施被用于托管和隐藏恶意活动

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Threat Actors Turn to Blockchain Infrastructure to Host & Hide Malicious Activity		
原文作者	Jai Vijayan	原文发布日期	2018 年 4 月 23 日
作者简介	<p>Jai Vijayan 是一位经验丰富的技术记者，在 IT 行业新闻方面拥有超过 20 年的经验。</p> <p>https://www.darkreading.com/author-bio.asp?author_id=1912</p>		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/vulnerabilities---threats/threat-actors-turn-to-blockchain-infrastructure-to-host-and-hide-malicious-activity/d/d-id/1331622		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

区块链基础设施被用于托管和隐藏恶意活动

Jai Vijayan

2018 年 4 月 23 日

火眼公司指出，越来越多的威胁源使用 .bit 域名来隐藏载荷、窃取的数据和 C&C 服务器。

一个让企业和执法部门头疼的趋势是，威胁源正在加大对区块链域名的使用，以隐藏其恶意活动并提高其对抗清除的能力。

火眼公司发现，最近网络黑市中对加密货币基础设施的兴趣正在增加。在过去的一年中，开始在恶意软件工具中整合对区块链域名支持的威胁源数量出现了大幅增长。

据火眼公司称，许多不同的恶意软件家族——包括一些知名家族，如 Necurs、GandCrab、Emotet、SmokLoader 和 Corebot——已经被重新配置，以使用区块链域名作为 C&C 基础设施。

自 2016 年起，使用 “Namecoin”（域名币）、“blockchain”（区块链）和 “.bit” 等关键字的搜索频率大幅增加，这表明犯罪分子对于使用区块链基础设施隐藏载荷、窃取数据以及 C&C 服务器的兴趣增长。

火眼公司高级分析师兰迪·艾兹曼（Randi Eitzman）表示，威胁源使用区块链域名的主要优势在于，他们注册的域名没有集中监管机构——例如互联网名称与数字地址分配机构（ICANN）或其他第三方注册商。

“在传统的由 ICANN 控制的域中，如果一个域名被认为托管了恶意内容，那么执法机构可以联系域名监管机构，要求其撤销该域名。” 艾兹曼说。

由于区块链顶级域名（如 .bit）并未集中管理，并且在 P2P 网络中共享 DNS 查询表，因此清除工作变得更加困难。“要注册一个 .bit 域名或其他基于区块链的域名，只需几个步骤，这个过程只需花费几块钱。”

域名注册与个人姓名或地址无关，而是与每个用户的唯一加密散列相关。“这基本上就是为互联网基础设施创建与比特币相同的匿名系统，只能通过加密身份识别用户。”

犯罪分子对加密货币相关主题感兴趣并不是什么新鲜事。正如火眼公司所指出的，威胁源至少自 2009 年以来一直在探索利用区块链技术的独特属性来支持恶意活动的可能性。

以威胁源对域名币的兴趣为例。域名币是一种基于比特币代码的加密货币，允许几乎任何人注册和管理.bit 域名。任何人都可以使用域名币注册.bit 域名，而不必将身份或地址与它关联起来。

域名币自我描述为支持域名所有权完全匿名的分散域名系统，因此很难在不造成附带损害的情况下关闭这些域名。

通过标准域名系统（DNS）无法直接访问利用域名币注册的域名。因此，越来越多的犯罪分子开始配置他们的恶意软件，以查询他们自己管理的、与域名币兼容的域名服务器，以便访问.bit 域名。或者，他们配置恶意软件来查询黑市中与域名币兼容的服务器。在很多情况下，恶意软件作者在样本中硬编码了与区块链兼容的 DNS 服务器。

“由于 DNS 查询表是分散在区块链中的，因此常用和默认的 DNS 服务器（如谷歌和各个互联网服务提供商[ISP]运行的服务器）无法解析域名。”艾兹曼解释说。

所谓的防弹（bulletproof）托管服务的提供商也开始加入战场。据火眼公司称，其中一个例子是 Group 4，该公司最近增加了允许威胁源查询.bit 兼容服务器的服务。

火眼公司预测威胁源将会继续使用洋葱头（Tor）、域名生成算法（DGA）和快速通量（Fast-flux）技术来隐藏恶意活动。但是，他们也会越来越多地使用区块链基础设施。

火眼公司高级分析师金伯利·古迪（Kimberly Goody）表示：“吸引网络犯罪分子使用加密货币作为支付方法的优势也存在于此。”

区块链域名是分散的，对清除更具抵抗性，并能够提供更好的匿名性。“由于这些因素以及越来越多支持.bit 的恶意软件开发人员，我们预计这些域名将会继续受到威胁源的青睐。”古迪说。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队,为用户提供端点防护、流量监测、快速处置、深度分析等产品,以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门,提供高级威胁和新兴威胁解决方案和能力体系,产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点,全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴,安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可,安天已连续五届蝉联国家级安全应急支撑单位资质,亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点,在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面,提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动,进行了深度的解析,对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上,安天创始人、首席技术架构师作为网络安全领域的发言代表,向习总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了位于哈尔滨科技创新城的安天公司,对安天负责人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问: <http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问: <http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>