# 区块链基础设施被用于托管和隐藏恶意活动

哈尔滨安天科技集团股份有限公司

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。