

简译版

DARPA 资助的一项新研究寻求缩短攻击驻留时间

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	New Research Seeks to Shorten Attack Dwell Time		
原文作者	Curtis Franklin Jr.	原文发布日期	2018 年 5 月 18 日
作者简介	Curtis Franklin Jr. 是 Dark Reading 的高级编辑。 https://www.darkreading.com/author-bio.asp?author_id=512		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/threat-intelligence/new-research-seeks-to-shorten-attack-dwell-time/d/d-id/1331837		
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。 		

DARPA 资助的一项新研究寻求缩短攻击驻留时间

Curtis Franklin Jr.

2018 年 5 月 18 日

企业可能需要几个月的时间才能发现他们已被黑客入侵。美国国防部高级研究计划局（DARPA）资助的一个新项目试图将这一时间缩短到几个小时。

IT 安全的一个主要问题，不是攻击和漏洞利用是否成功，而是它们成功后在很长时间内不被发现。一项由 DARPA 资助，乔治亚理工学院进行的新研究项目正在应用各种技术，将攻击的“驻留时间”从当前的平均 6 个月以上缩短至 24 小时。

该项目称为“Gnomon”，预计历时 4 年，获得了 DARPA 1280 万美元的投资。该项目承认网络被攻陷不可避免，其目标是检查连接到网络的设备和系统的行为，以识别可疑行为，帮助专家或自动化系统及时进行修复。

Gnomon 的操作不依赖于识别恶意文件。“我们不是在查找恶意软件，因为攻击者可能不使用实体恶意软件，而是使用像 Powershell 这样的工具。”乔治亚理工学院电气与计算机工程学院副教授马诺斯·安东卡基斯（Manos Antonakakis）说。该项目采用基于动态行为的监测模式，能够有效缓解攻击者多变的操作手法，其多变的操作手法是防御者疲于应付的原因之一。

“我们去年的一项研究表明，在我们获得样本之前，威胁早已肆虐了数月。”安东卡基斯说。该研究发现：“.....在我们开始动态分析相应的样本之前，与 PUP（潜在有害程序）相关的域名平均活跃了 192 天。”

分析延迟导致大量的域名（以及恶意软件家族）横行无阻。该研究还发现：“.....在对相应的恶意软件样本进行分析之前，302,953 个恶意软件域名至少已经活跃了两周，有的甚至是数月。”

实时分析大型网络的行为需要强大的计算能力。在 Gnomon 项目中，这种计算能力用于“动态智能”服务。当被问及动态智能的定义，以及它与机器智能或人工智能（AI）的区别时，安东卡基斯说：“动态智能基于动态建模概念，可以构建能够表征短期和长期行为的模型。”这种动态模型能够随着时间的推移查看对象行为，对分析至关重要。

一旦发现恶意行为，网络安全专家需要知道如何处理，例如是否需要引入黑洞、启用蜜罐、重建系统、修复文件或采取其他措施。安东卡基斯说，项目成员研究了如何更好地清除僵尸网络，并获得了一些见解。目标初一看似乎违反常识：迫使恶意软件越来越复杂。

“该项目将持续 3 - 4 年，目的是增加攻击者的攻击难度和成本，使他们黔驴技穷。”安东卡基斯说，“这样一来，他们不得不执行更复杂的攻击，这会增加他们犯错误的机会，有助于我们更早地发现他们。”

另外，复杂的恶意软件和恶意活动往往比简单的软件更加明显。如今，Gnomon 正在与两家不具名的美国电信公司合作分析网络并分享信息。“你需要在一天内，就所保护的网路，多次研究威胁的域名信息，”安东卡基斯说，“我们的目标是能够在 24 小时内发现恶意网络行为。”

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>