精译版

高级低成本勒索软件不断增加

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	Advanced, Low-Cost Ransomware Tools on the Rise		
原文作者	Ericka Chickowski	**原文发布日期**	2017 年 4 月 18 日
作者简介	Ericka Chickowski 进入信息安全领域已将近 10 年，专注于研究信息技术和业务创新。http://www.darkreading.com/author-bio.asp?author_id=962		
原文发布单位	Darkreading		
原文出处	http://www.darkreading.com/attacks-breaches/advanced-low-cost-ransomware-tools-on-the-rise/d/d-id/1328675?		
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	• 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。		

高级低成本勒索软件不断增加

Ericka Chickowski

2017 年 4 月 18 日

新的勒索软件成本低至 175 美元，并具有大量的反检测功能。

恶意软件开发人员致力于开发廉价和用户友好的勒索软件工具，帮助攻击者（甚至技术最低端的攻击者）进入勒索行业，这种趋势将会导致 2017 年出现更多的勒索攻击。今天，Recorded Future 研究人员发布了一份报告，称俄罗斯网络犯罪分子通过软件即服务（SaaS）交付机制提供的一个新变种成本低至 175 美元。

Recorded Future 研究人员指出，Karmen Cryptolocker 恶意软件是在开源 Hidden Tear 项目的基础上创建的勒索软件即服务（RaaS）。它遵循标准的勒索软件手法，采用 AES-256 算法加密数据，要求受害者以比特币的形式支付赎金，并在受害者支付赎金后自动解密数据。除了成本低廉，该勒索软件还能够记录获取的赎金总额，并在出现更新时及时更新。

RaaS 并不是什么新鲜事了。两年前，McAfee Labs 的研究人员发现了 Tox 恶意软件工具包，自此一直在研究类似的例子。但是，Karmen 的专业性说明勒索软件工具不断地发展，因为各种类型的犯罪分子都想在勒索市场中分一杯羹。

目前，开源项目（如 Hidden Tear）的代码广泛可用，因此许多技术高明的犯罪分子能够为低端犯罪分子开发诸如 Karmen 的变种。例如，就在今天，Cylance 研究人员报告了 CrypVault 勒索软件的另一个新变种，它使用 GnuPG 开源加密工具来加密文件。

Cylance 公司的隆美尔·拉莫斯（Rommel Ramos）写道："与普通的勒索软件不同，CrypVault 使用 Windows 脚本语言编写，如 DOS 批处理命令，JavaScript 和 VBScrip。因此，攻击者很容易修改其代码来创建新变种。任何具有一般脚本语言知识的网络犯罪分子都能够创建自己的版本来赚钱。"

举例来说，Hidden Tear 原本是作为"教育性勒索软件"开发的。但是几年前，坏家伙们开始将其代码用于自己的目的。安全专家的一线希望是：其基本代码中嵌入了漏洞，这使得勒索软件研究人员，如麦克尔·吉尔斯比（Michael Gillespie），能够创建解密器。现在，麦

克尔正在通过 Twitter 为任何受到 Karmen 感染的人提供帮助。

尽管如此，Karmen 仍然具有一些能够阻止沙箱分析的功能，这意味着它会用来开发危险的勒索软件。

“Karmen 的一个显著特征是 ,如果它在受害者的计算机上检测到沙箱环境或分析软件，它就会自动删除自己的解密器。” Recorded Future 的戴安娜·格兰杰（Diana Granger）写到。她的同事告诉 Dark Reading，这是为了阻止安全工具和研究人员了解其代码。

很多种类的恶意软件都会使用规避技术。上个月，趋势科技报道称 Cerber 的新变种具有反沙箱功能，能够规避机器学习安全技术。

Tripwire 的高级安全研究工程师特拉维斯·史密斯（Travis Smith）表示：“这是一种典型的猫鼠游戏，犯罪分子在技术上进行了创新，防御者也是如此。一旦犯罪分子的活动受到防御措施的阻挠，他们就会继续改变战术。就这些规避技术的严重性而言，最终用户不会面临额外的风险。”

不幸的是，SecureWorks 最近的一项研究指出，尽管有 76%的组织认为勒索软件是一种严重的威胁，但是只有 56%的组织具有勒索软件响应计划。SecureWorks 高级安全研究员基思·贾维斯（Keith Jarvis）指出，担心勒索软件的组织不仅需要确保到位的备份和端点保护协议，还需要关注电子邮件过滤和补丁管理。

他说：“我们发现，大部分勒索软件都是通过电子邮件和浏览器漏洞利用包传播的，这些工具包依赖于未修复的环境。”他指出 Adobe Flash 漏洞很常见，“电子邮件防御的第一步是阻止可执行文件和脚本最常滥用的文件扩展名，接下来是阻止包含宏的 Word 文档。如果您采取了这些措施，就能够阻止绝大多数的勒索软件了。”