精译版

NukeBot 银行木马的源代码被公布

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	NukeBot Banking Trojan Source Code Leaked Online by Author		
原文作者	Chris Brook	原文发布日期	2017 年 3 月 30 日
作者简介	Chris Brook 是 Threatpost 的副编辑。 http://www.linkedin.com/in/chris-brook-91223712/		
原文发布单位	Threatpost		
原文出处	https://threatpost.com/nukebot-banking-trojan-source-code-leaked-online-by-author/124653/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
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。		

NukeBot 银行木马的源代码被公布

Chris Brook

2017 年 3 月 30 日

本月中，模块化银行木马 NukeBot 的作者发布了其源代码，以期重获网络犯罪社区的信任。

两个星期前，NuosBot 的作者 Gosya 在几个地下论坛上发布了指向该恶意软件的 GitHub 链接，称之为“zeus 式银行木马”。本周，IBM X-Force 研究团队的人员表示，这一举动可能是反向报复。

IBM 研究员里默尔·凯瑟姆(Limor Kessem)和伊利亚·科尔曼诺维奇(Ilya Kolmanovich ）在周二表示，Gosya 在销售该木马时出现了一些失误，这可能导致他除了公布其代码之外别无选择了。

黑客的恶意软件通常由论坛管理员验证，但是 Gosya 在加入一个论坛后立即开始兜售该木马。当他回答有关 NukeBot 的问题时，他也显得“紧张和警惕，这引起了其他论坛成员的怀疑”。也许 Gosya 是在不同的论坛上以不同的名义出售同一个恶意软件。

凯瑟姆和伊利亚科尔曼诺维奇写道：“当欺诈者意识到同一个人正试图以不同的名义出

售恶意软件时，他们更加怀疑他是一个破解者，试图歪曲或出售并非他所有的产品。”

Gosya 甚至将 NukeBot 的名称更改为 Micro Banking Trojan，但这也没什么用，他被各个地下论坛禁止了。

NukeBot，也称为 Nuclear Bot，在 2016 年 12 月首次出现在地下市场。Arbor Networks 是最先分析该木马的团队之一，其研究人员声称它包含大量的命令，具有浏览器功能以及从 C&C 服务器下载 webinject 的功能。

X-Force 的研究人员也在 12 月份分析了该木马，他们表示，该恶意软件可能是能够动态窃取数据的“HTTP bot”。

Arbor 认为当时无法确定它的活跃性和传播程度，但是承认它的售价已经接近 2500 美元，是同一时间流行的木马 Flokibot 的两倍多，这会吓退潜在买家。

尽管如此，研究人员仍然认为 NukeBot 是合法的。IBM 的研究人员没有提供消除该恶意软件的方法(凯瑟姆表示它没有用于攻击),但在周二承认它有一个基于 web 的管理面板，用来控制受感染的终端和 web 注入。

Gosya 在论坛上发布了几篇帖子，声称该恶意软件（现名为 TinyNuke）还具有其他功能：

- 能够对 Firefox，IE 和 Chrome 浏览器进行格式化和 web 注入。
- 感染 x86 和 x64 浏览器
- 逆向工程 SOCKS 4
- 具有 HNVC 式的隐藏桌面
- 具有包含模糊字符串的 32kb 二进制文件

Gosya 试图出售该恶意软件却屡屡碰壁，这很可能导致他公布了代码。

凯瑟姆说：“一个靠谱的猜测是，Gosya 对他在地下市场的不受信感到很失望，因此决定发布该恶意软件的主要模块供他人测试和证明。”

现在，该恶意软件的代码已经广为人知。凯瑟姆指出，它的修改和进一步传播只是时间问题。她说最可能的情况是：代码被重新编译，被僵尸网络运营者使用，并嵌入到其他恶意

软件代码中。虽然目前还没有出现任何攻击事件，但这一情况很快就会改变了。

周四，凯瑟姆对《安全周报》（Threatpost）说："我们认为每次代码泄漏都会导致攻击者的利用和微调。这个案例也是非常相似的。"

也就是说，该木马的代码泄露会导致什么样的后果，我们仍需拭目以待。2013 年夏，Carberp 木马的源代码在网上公布；早在此前（2011 年 5 月），Zeus 犯罪软件套件的代码就已经被泄露了。

攻击者设法修改 Zeus 的代码，添加了新的 web 注入技术、定制模块和新的 C&C 服务器通信介质：Tor。

去年，Gozi 木马和 Nymaim 木马的代码在网上泄露。犯罪分子立马将这两个木马整合到了一起，创造了 GozNym。去年春天，GozNym 木马一经部署，就为攻击者创收了 400 万美元，主要的受害者是商业银行机构、信用社和零售银行。