

基于 Njw0rm 源代码的新型 RAT

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 RATs Emerge from Leaked Njw0rm Source Code		
原文作者	Michael Marcos	原文发布日期	2015 年 1 月 22 日
作者简介	Michael Marcos 是趋势科技的威胁响应工程师。		
原文发布单位	趋势科技		
原文出处	http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/		
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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>		

基于 Njw0rm 源代码的新型 RAT

Michael Marcos

2015 年 1 月 22 日

在研究称为“njrat”或“Njw0rm”的 RAT(远程访问木马)时,我无意中发现了 dev-point.com 网站,该网站伪装为“IT 爱好者”网站,但事实上却托管了各种各样的下载器、间谍软件和远程访问木马。我探索了以下该网站,发现该网站在“Protection Devices”板块托管恶意软件。在该板块下有一个用阿拉伯语编写的论坛,预示着有个以阿拉伯语为母语的国家隐藏其后。

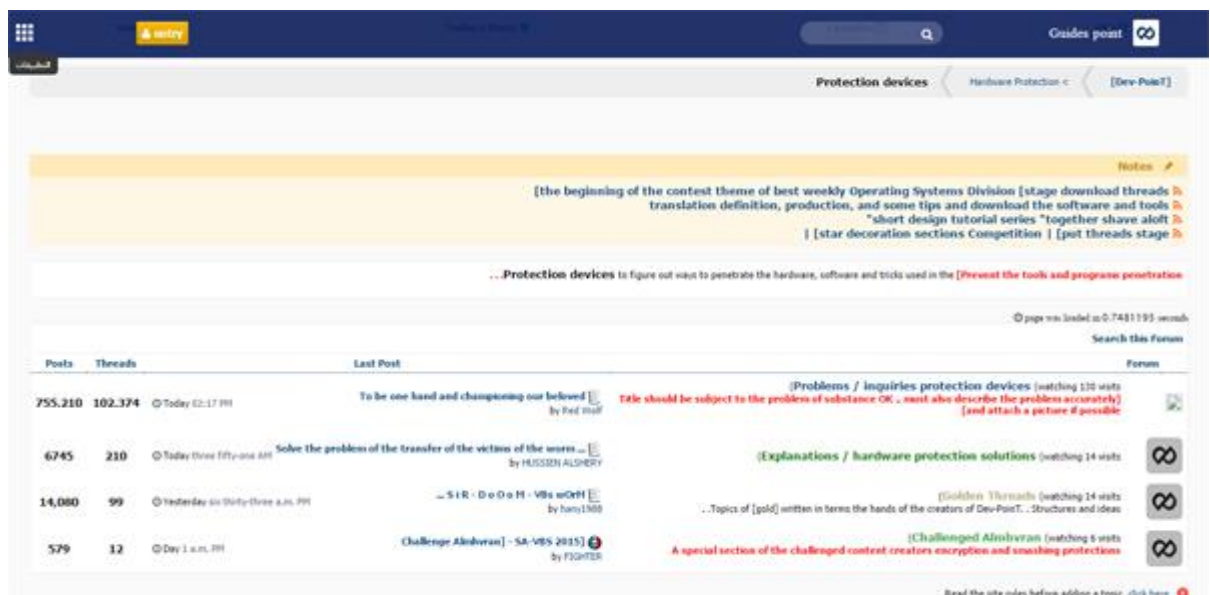


图 1 : dev-point.com 网站的“Protection Devices” 板块的截图 (点击以上图片放大)

基于 Njw0rm 源代码的恶意软件

该论坛最引人注意的话题就是新型恶意软件“kjwt0rm”(或 [HKTL_KJWORM](#)) 及蠕虫“Sir DoOom,”(或 [HKTL_DOOMWORM](#)), 两者都是该论坛发布恶意软件 Njw0rm 源代码之后出现的。2013 年 5 月, Njw0rm 的源代码的在知名黑客网站(如 [hackforums.net](#) 及 [dev-point.com](#)) 发布,我据此推断,网络罪犯发现了利用 Njw0rm 的蠕虫及后门功能来创建有更多功能的恶意软件的办法。

我们发现, dev-point.com 网站在 2014 年 1 月和 12 月分别共享了 Kjwt0rm 的两个版本 V2.0 和 0.5X。2014 年 12 月, 蠕虫 Sir DoOoM 也在该网站被发现。

与之前的 Njw0rm 版本不同, 新型恶意软件不用 Autott 编写, 而是用 Visual Basic Script

编码。

检查恶意软件生成器

与 Njw0rm 相似，我们发现的新型恶意软件要求攻击者为即将到来的数据流分配一个端口，kjlw0rm 用默认值 Port 1991, Port 1010，蠕虫 Sir DoOom 的默认值则是 Port 4000。蠕虫 Sir DoOom 先生要求生成器用“管理员身份操作”方可运作。

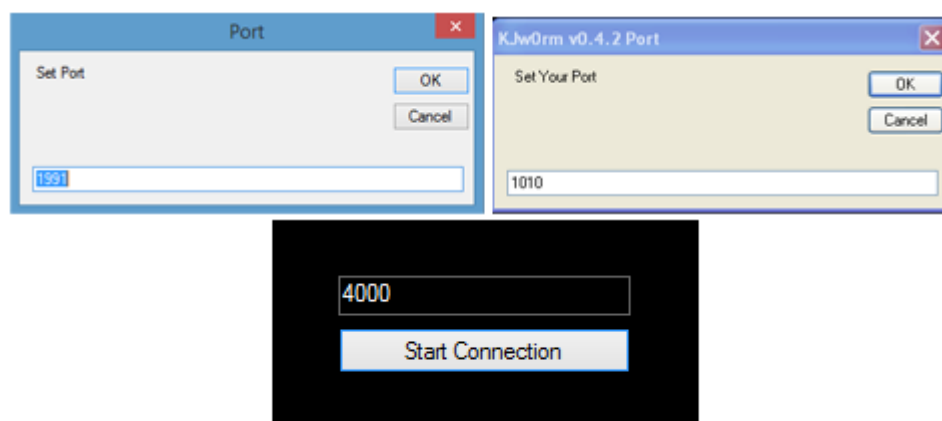


图 2: 上方：分别为 kjw0rm V2.0 和 Kjlw0rm 0.5x 的端口；下方：Sir DoOom 的端口

查看控制面板

与 2013 年 5 月的 Njw0rm 版本相比较，生成器在新型恶意软件的控制面板中添加了更多信息。

Njw0rm (May 2013)	Kjlw0rm V2.0 (January 2014)	Kjlw0rm 0.5x (December 2014)	Sir DoOom worm (December 2014)
Bot ID			
IP address			
Country			
OS Info			
Malware Version			
USB (Y/N)			
Active Window	Installed antivirus	Installed .NET (Y/N)	Size of RAM
		.NET Version	Firewall Information
			Installed Antivirus
			Install Date
			CPU Information
			GPU Information
			Product Name
			Product ID
			Product Key
			Processor ID

图 3: Kjw0rm 与 蠕虫 Sir DoOom 的新字段

我们同样看到了 Kjw0rm 各版本与蠕虫 Sir DoOom 的新功能。

Njw0rm (May 2013)	Kjw0rm V2.0 (January 2014)	Kjw0rm 0.5x (December 2014)	Sir DoOom worm (December 2014)
Execute File	WOrm (Close malware, Uninstall malware, Restart malware)	Download Execute File	Execute (Download and Execute File, Execute File)
Run remote shell	Computer Control (Shutdown, Log off, Restart)	Download and Execute .VBS code	Computer Control (Shutdown, Logoff, Restart)
Update malware	Run (Download and Execute File, Download and execute script file)	Uninstall malware	Computer Control with Timer (Shutdown, Logoff, Restart)
Uninstall	Options (Run remote shell, DoS attack, Open Web Page)		Bitcoin Miner (Download Bitcoin Miner, Start Bitcoin, Add Bitcoin Program to Startup)
Get Passwords (Filezilla, Google Chrome etc.)			DDOS Attack
			Start Live Quran Site
			Display Message Box
			Uninstall Malware
Execute File	WOrm (Close malware, Uninstall malware, Restart malware)	Download Execute File	Execute (Download and Execute File, Execute File)
Run remote shell	Computer Control (Shutdown, Logoff, Restart)	Download and Execute .VBS code	Computer Control (Shutdown, Logoff, Restart)

图 4: Kjw0rm 各版本与蠕虫 Sir DoOom 的新功能

传播例程

新型恶意软件基于 njw0rm 传播。njw0rm 通过可移动设备从根目录中获取一个包含十个文件夹的列表，将它们设置为‘Hidden’（隐藏），并用指向恶意软件可执行文件的文件夹名来生成快捷链接。

一段时间后，恶意软件调整传播方法，以实现成功的攻击，使用社会工程学战术，如创建看起来合法的文件夹来欺骗用户。

Kjw0rm V2.0

该蠕虫通过可移动设备传播。该蠕虫首先在可移动设备的根目录自我复制(Hidden, System File Attribute)。隐藏所有文件夹，创建用相同文件夹名命名的“文件夹”属性快捷方式-皆旨在执行恶意软件。

Kjw0rm V0.5X

该恶意软件与 Kjw0rm V2.0 有相同路径。然而，此软件从可移动设备上获取有 20 个文件夹的列表，隐藏这 20 个文件夹并创建用相同文件夹名命名的“文件夹”属性快捷方式-

皆旨在执行恶意软件。接着，该软件创建一个名为 *Videos* 的文件夹。创建此文件夹后，该软件用同样的传播路径又获取了一个有 20 个文件夹的列表，但这次包含了恶意软件创建的子文件夹。

Sir DoOom 蠕虫

Sir DoOom 蠕虫与 Kjw0rm V0.5x 的传播方式相同。唯一的差异是 Sir DoOom 蠕虫会在可移动设备的根目录创建五个文件夹，命名为：*Videos*、*Pictures*、*Movies*、*Games*、和 *DCIM*。

有效载荷/独一无二的特征

Kjw0rm V2.0

该恶意软件的传播方式将可移动设备的根目录内所有文件夹都定为目标。

Kjw0rm V0.5X

该蠕虫会将部分恶意软件代码变模糊。恶意软件作者利用混淆器将字符转变为十六进制、增加填充功能，并执行使分析更艰和耗时的计算。

```
Set szxquzftjy = GetObject( "w" & chrw(cint(33+72)) & "n" & "m" & "g" & "m" & "t" &
chrw(cint(124-9)) & ":" & chrw(cint(2.86046511627907 * 43)) & chrw(cint(105)) &
chrw(cint(63+46)) & "p" & "e" & chrw(3534 / 31) & chrw(115) & chrw(2775 / 25) & "n" &
chrw(87+10) & "t" & "i" & chrw(13+98) & "n" & chrw(76) & "e" & chrw(cint(93+25)) & "e"
& chrw(3888 / 36) & "=" & "i" & "m" & "p" & chrw(101) & chrw(3876 / 34) & chrw(115) &
"o" & "n" & "a" & chrw(cint(116)) & chrw(cint(101)) & chrw(32 * 3.90625) & chrw(cint(51-
18)) & "\" & chrw(6+86) & "." & chrw(cint(71+21)) & chrw(72+42) & "o" & chrw(111)
& chrw(116) & chrw(cint(92)) & chrw(17+82) & "i" & chrw(218 / 2) & chrw(139-21) &
chrw(300 / 6) )
```

图 5：样本代码片段

该恶意软件还拥有反虚拟机例程。此例程先在被感染的计算机内搜索安装程序列表，如果此变种发现计算机已安装了虚拟机程序，它就会终止运行并自我卸载。这样就会阻止分析员通过测试来确定恶意软件行为。

Sir DoOom 蠕虫

该恶意软件有独一无二的新功能。

- 操作系统产品密钥的解析
- 终止反病毒相关进程（终止 *Tiger-Firewall.exe* 和 *bavtray.exe*）
- 反虚拟机例程（在已安装程序列表内寻找字符串‘虚拟’；如果找到，终止运行并卸载）
- 比特币开采
- 发动 DDoS（分布式拒绝服务）攻击

Kjw0rm 从 njRAT 进化

Kjw0rm 第一版 (V2.0X) 于 2014 年 1 月发布，紧接着第二版 (V0.5X) 于同年底发布。Sir DoOom 蠕虫与 2014 年 12 月 21 日发布。这样的进展说明恶意软件研发者用 njw0rm 做模板，在研发新型恶意软件上变得越来越积极了。鉴于这样的形式，我们可以预测在将来会看到更多该恶意软件的变种。



图 6: 恶意软件 njRAT 的进化

解决方法及最佳实践

为了免受这些新型威胁，我们建议用户禁止连接来自不明计算机或没有安全保护的计算机可移动设备。避免打开及安装来自不明网络资源的程序。

注意小细节也会有所帮助。比如：发现用你的文件夹名编写的“文件夹”属性快捷方式，就是可移动设备已被感染的强烈信标。

通过了解最新的网络罪犯把戏和技术来保持警惕。最后，为了检测及移除相似威胁，要确保安全软件持续更新。

相关哈希值：

- 5408477d7491d883251fa0fcbe7f6b4e6a9d4493 – HKTL_DOOMWORM
- b579ac4af93cc0212ed00c6468e948810bce0d27 – HKTL_KJWORM
- 4fd150b489673ea089320811a533944416a4fd66 – HKTL_KJWORM