# New RATs Emerge from Leaked Njw0rm Source Code

blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/

January 23, 2015

In the middle of my research on the remote access Trojan (RAT) known as “njrat” or “Njw0rm”, I stumbled upon *dev-point.com*, a site that disguises itself as a site for “IT enthusiasts” but actually hosts various downloaders, different types of spyware, and RATs. I explored the site and found that they host malware under the “Protection Devices” section in their website. Under this section was a forum written in Arabic, which may suggest that an Arabic-speaking country is behind it.

*Figure 1. Screenshot of the “Protection Devices” section under* dev-point.com. *(Click the image above to enlarge)*

***Malware from Njw0rm Source Code*** One of the notable topics in the forum talked about new malware “kjw0rm” (or HKTL_KJWORM) and a worm named “Sir DoOom,” (or HKTL_DOOMWORM) which both came about after the release of the Njw0rm malware source code in the same forum. The leaking of Njw0rm’s source code last May 2013 in known hacking websites like *hackforums.ne*t and *dev-point.com* led me to the conclusion that cybercriminals found a way to leverage the worm and backdoor capabilities in Njw0rm to create new malware with added functionalities. We discovered two versions of Kjw0rm (V2.0 and 0.5X) being shared in *dev-point.com* in January 2014 and December 2014 respectively. The Sir DoOoM worm was also discovered in the same site last December 2014. The new malware are coded in Visual Basic Script, unlike its earlier version, Njw0rm, which was compiled with AutoIt. ***Checking the Malware Builder*** Similar to Njw0rm, the new malware we found asks the attacker to assign a port to open for incoming traffic, with the default values being Port 1991, Port 1010 for kjw0rm, and Port 4000 for the Sir DoOom w0rm. The Sir DoOom worm requires the builder to ‘Run as Administrator’ for it to work.

*Figure 2. Top: Ports for kjw0rm V2.0 and Kjw0rm 0.5x, respectively, Bottom: port for Sir DoOom w0rm*

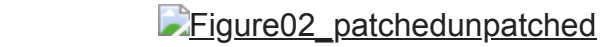
***Looking at Control Panels*** The new malware added a lot more information in the Control Panel view of the malware builder, compared to that of the Njw0rm version in May 2013.



*Figure 3. New fields for Kjw0rm and the Sir DoOom worm*

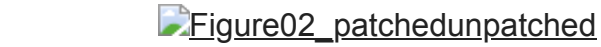
We're also seeing new functions for both Kjw0rm versions and the Sir DoOom worm.



*Figure 4. New functions for Kjw0rm and the Sir DoOom worm*

***Propagation Routines*** The new malware based their propagation routines on njw0rm. Njw0rm propagates via removable devices by getting a list of ten folders in the root directory, setting them to 'Hidden' and making shortcut links using the folder names pointing to the malware executable. Over a period a time, the malware tweak their propagation methods to make the attack successful and employ social engineering tactics such as creating legitimate looking folder to deceive the user.

> **Kjw0rm V2.0** This worm propagates in removable devices. The worm first drops a copy of itself (Hidden, System File Attribute) in the root directory of the removable drive. It hides all folders**,** and creates shortcut files with folder icons with the same folder names – all pointing to the malware executable. **Kjw0rm V0.5X** This malware has the same routines as Kjw0rm V2.0. However, it gets a list of 20 folders on the removable drive, hides the 20 folders, and creates shortcut files with folder icons with the same folder names—all pointing to the malware executable. The malware then creates a folder named *Videos*. After creating the folder, the malware redoes the propagation routine to get a list of 20 folders, but now includes the subfolders. **Sir DoOom worm** The Sir DoOom worm has the same propagation method as Kjw0rm V0.5x. The only difference is that the malware creates five folders namely: *Videos, Pictures, Movies, Games*, and *DCIM* in the removable drive's root directory.

***Payload/Unique Features***

> **Kjw0rm V2.0** The propagation method of this malware targets **all folders** in the root directory of the removable drive. **Kjw0rm V0.5X** This worm obfuscated some portions of the malware code. The malware author utilizes an obfuscator tool that converts characters to hex values, adds filler functions, and performs computations that make analysis more difficult and time-consuming.
> *Figure 5. Sample code snippet*
>
> This malware also has an anti-VM (virtual machine) routine. It first searches for a list of the installed programs in the affected computer. If this variant found itself to be in a computer where a VM program is installed, it will uninstall and terminate itself from the affected system. This prevents analyst to do testing to determine malware behavior.
> **Sir DoOom worm** This malware incorporates new functionalities that are unique to this malware.
>
> - Parsing of OS product key
> - Termination of antivirus-related processes (terminates *Tiger-Firewall.exe* and *bavtray.exe*)
> - Anti-VM routines (looks for the string 'Virtual' in the list of installed programs; if found, it uninstalls and terminates itself)
> - Bitcoin mining
> - Launching of DDOS attacks

***Kjw0rm evolution from njRAT*** The first version of Kjw0rm was released on January 2014 (V2.0X) followed by the second version (v0.5x) by the end of the year. The Sir DoOom worm was released in December 21, 2014. This evolution shows that the malware authors are becoming more active in developing new malware and using njw0rm as a template. Because of this pattern, we can expect to see more variants of this malware in the future.



*Figure 6. Malware evolution of njRAT*

***Solutions and best practices*** To stay protected against these new threats, we advise users to refrain from plugging removable drives that came from unknown computers or computers that aren't protected by security solutions. Avoid opening and installing programs from unknown web sources. Paying attention to small details also helps. For example, finding shortcut files in "folder" icons with your folder names is a strong indicator that the removable drive is infected. Stay vigilant by keeping abreast of the latest cybercriminals tricks and techniques. Finally, make sure your security software is always updated in order to detect and remove similar threats. Related hashes:

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

Content added to Folio

Malware

By: Trend Micro January 23, 2015 Read time:  ( words)