

from trying to find or disable the malware. Strings such as `\\xneo\\lock\\Release\\lock.pdb` and "Conteneur ActiveX" were found in memory.

At this time, the piece of malware analyzed is unable to communicate back to attacker. The malware is supposed to make an HTTP request for `hxxp://<random>.my-files-download.ru/status.php`, but instead requests the invalid URL `hxxp://<random>.my-files-download.ru/.ru'utr/qiq`. This causes further issues because the callback thread determines if the victim has paid the ransom. If the malware is unable to communicate back, the attacker does not know if the ransom has been paid or not.

Keep in mind that this represents the analysis of one specific malware sample and other malware developed exploiting this vulnerability will probably utilize different tactics and techniques.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the Java application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

This vulnerability is being exploited in the wild by multiple exploit kits, such as BlackHole, Redkit, Nuclear Exploit Kit and CoolExploit Kit. Exploit code for this vulnerability is also publicly available.

RECOMMENDATIONS

We recommend the following actions be taken:

- ▶ Consider disabling or uninstalling Java browser plugin on all systems until a patch is available.
- ▶ Consider following the Oracle guidelines provided for Java 7 update 10 to disable Java in web browsers (http://www.java.com/en/download/help/disable_browser.xml).
- ▶ Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- ▶ Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- ▶ Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

Comment: Note that as the MS-ISAC has more time to analyze the threat, the intelligence product (shown above) becomes more sophisticated in describing and assessing

(Continued)