Towards Korean (shell)code*

Ji-Hyeon Yoon and Hae Young Lee

Department of Information Security
Seoul Women's University
Seoul 139-774 Republic of Korea
haelee@swu.ac.kr

Extended Abstract

In this talk, we present approaches to hiding shellcode in Korean text. To this end, shellcode is first converted into Chinese characters. These Chinese characters are inserted into Korean text, or placed with some Sino-Korean words, which originate from or were influenced by Chinese words. Such use of Korean characters with Chinese ones is often used in South Korea; Sino-Korean words often share the same sounds, so that Chinese characters are put within Korean text, in order to clarity the meanings of the words. Many Korean people in their 20s and 30s, however, are not much familiar with Chinese characters, so that they may not find mismatches between Sino-Korean words and pseudo Chinese ones. We can also place some corresponding Chinese words, which may make the text look 'real.' Thus, such 'Korean shellcode' may be effective against inline payload based inspection. Shellcode can be easily reconstructed from Korean shellcode, with simple decoders attached to the payloads. They can use parts of Korean characters around pseudo-Chinese words as 'hints' on choosing instructions. In our proof-of-concept attacks, shellcode could be reconstructed with about 30 instructions, regardless of its complexity. We can also conduct code-reuse attacks, such as return-oriented programming, to reconstruct Korean shellcode, which may prevent the shellcode from being detected due to the signature of the decoders. Although our approaches address 'Korean' shellcode, issues posed by them may not be confined to Korea; Korean text may be considered to be a part of multilingual support. Moreover, the approaches may be applied to East Asian text. Furthermore, we may apply them to the Web. For instance, an application of the approaches for the obfuscation of JavaScript code may be more effective, in terms of network monitoring, since the use of Korean with Chinese is more frequently found in the Web traffic (e.g., online newspapers).

* This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2013R1A1A1006542).