JPCERT CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-PR-2016-03
Issued: 2016-10-12

JPCERT/CC Activities Overview [July 1, 2016 - September 30, 2016

Activity Overview Topics

－Topic 1－ JPCERT/CC verifies the effectiveness of the new Windows security functions and discusses its findings in Analysis Center News

JPCERT/CC verified some of the new security functions offered by the latest Windows operating system (OS), using a malware sample used in actual attacks. Specifically, JPCERT/CC focused on the following functions: AppContainer, which runs applications in an isolated environment (a sandbox), and the LSA protected mode and Credential Guard, which protect account information. The findings are discussed in Analysis Center News articles titled "Effectiveness of AppContainer in defending a web browser against attacks targeting its vulnerability" and "Verifying new Windows security functions: LSA protected mode and Credential Guard", which are translated and published on JPCERT/CC English blog website.

Microsoft has implemented various new additional security functions in its Windows OS to defend against cyber attacks that recently have become increasingly sophisticated. Among these security functions, JPCERT/CC studied AppContainer, which restricts access to files and other processes by sandboxing applications, and the LSA protected mode and Credential Guard, which protect the account information of devices within a domain. The tests were conducted in a realistic setting using attack tools and specimens used in actual cases of targeted attack that JPCERT/CC investigated. The articles also offer tips on how to ensure that the effectiveness of the security functions is not lost. The verification findings should provide valuable reference material for considering steps to be taken in countering cyber attacks that grow increasingly sophisticated.

AppContainer’s Protecting Effects on Vulnerability-Exploited Web Browsers
http://blog.jpcert.or.jp/2016/08/appcontainers-p-d296.html

Verification of Windows New Security Features – LSA Protection Mode and Credential Guard
http://blog.jpcert.or.jp/2016/10/verification-of-ad9d.html

Analysis Center News is issued from time to time by analysts at JPCERT/CC's Analysis Center to share with malware analysts and information security experts information and insight gleaned from daily activities, as well as investigation findings directly linked to individual cases, compiled from the perspective of each analyst. The contents are translated into English and published on JPCERT/CC English Blog website (http://blog.jpcert.or.jp/).