NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | *September 23, 2015*

Recent Threat Analysis

September 23, 2015

[Higher Education: An Attractive Target for Range of Malicious Actors](#)

The NJCCIC assesses New Jersey's higher education institutions are increasingly attractive targets for a range of cyber threat actors due to breadth and value of data available on their largely accessible and often vulnerable networks. One of the key cybersecurity challenges facing universities stems from their reliance on federated information technology systems, which allow for interoperability and information sharing between many decentralized components. Institutions involved with research and development in collaboration with the private sector, Federal government, or Department of Defense are at a high risk of network exploitation and intellectual property theft on behalf of sophisticated state-sponsored espionage groups, often referred to as advanced persistent threats (APTs). Furthermore, universities are soft targets for cybercriminals seeking to steal sensitive personal and financial data, and frequently victims of website defacements and

Latest Cyber Alerts

[Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution](#)

[Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR](#)

[Updated Multiple Vulnerabilities in Apple Product](#)

[Multiple Vulnerabilities in Mozilla Firefox](#)

NJ CyberLog

[Malvertising: More Than a Nuisance](#)

Malicious advertising, more commonly known as malvertising, has quickly ascended on the list of everyday Internet threats due to the prevalence of online advertising in today's digital media environment, where consumers expect free content in exchange for exposure to various forms of ads. Malvertising simply involves hackers injecting malicious code into digital advertisements that, in turn, infect computers and mobile devices of unsuspecting victims visiting legitimate, often reputable websites. Malvertising is not only increasingly

distributed denial of service (DDoS) attacks conducted by hacktivists and other malicious hacking groups.

effective at infecting users, but easy for cybercriminals to execute and difficult for investigators to determine who is responsible.

Tip of the Week

"Know Your Peer-to-Peer Partner"

Peer-to-peer (P2P) networking is a popular method for sharing files, music, photographs and other information. Remember that this method can come with its share of major risks. It is best to know with whom you are sharing data and files versus browsing for a site that you believe meets your criteria. The data may be corrupted with malware or expose you to legal ramifications (e.g., copyrights, pirated software or music).

NJCCIC Announcements

Fairleigh Dickinson University's Center for Cybersecurity and Information Assurance (CCIA) announces its third annual Cybersecurity Symposium on Law Enforcement and Cyber Defense will be held on Wednesday, September 30, 2015 in Lenfell Hall at FDU's Florham Campus. This free event is scheduled from 8 a.m. - 3:45 p.m. Registration - See more at: http://view2.fdu.edu/fdu-whats-new/press-releases/2015-2016/09/fdu-presents-third-annual-cybersecurity-symposium/#sthash.4XpyLKB3.dpuf

Connect with us!

TLP: White

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

Traffic Light Protocol (TLP). For more information about TLP, see <u>https://www.us-cert.gov/tlp/</u>.