NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | January 14, 2016

Alert: Microsoft Ends Support for Windows 8 and Internet Explorer 8, 9, and 10

As of Tuesday, January 12, Windows will no longer publish bug fixes and security patches for Windows 8 and Internet Explorer versions 8, 9, and 10. Microsoft is encouraging customers to upgrade to the latest version of their operating system, Windows 10, which includes a new built-in browser called Microsoft Edge. Users of Windows 8 should immediately update to version 8.1, which will continue to receive Extended Support through January 10, 2023. Users who do not choose to upgrade to Windows 10, and Microsoft Edge, should immediately update their browser to Internet Explorer 11, which will continue to receive security updates, compatibility fixes, and technical support on Windows 7, Windows 8.1, and Windows 10.

Alert: RIG and Neutrino Exploit Kits Surge in 2016

As highlighted in our threat analysis from August 2015, exploit kits (EKs) became increasingly effective infection vectors throughout 2015 – specifically the Angler EK. Though Angler holds reign as one of the most sophisticated EKs, Neutrino and RIG EK activity has reportedly increased substantially in the first two weeks of 2016, each with new tactics and functionality. Read more.

Breach Notification

Tax software maker TaxAct

On January 11, TaxAct informed an unknown number of customers that an unauthorized third party accessed their TaxAct account between November 10 and December 4, 2015. In a letter to victims,

Latest Cyber Alerts

Vulnerability in Fortinet FortiOS

Multiple Vulnerabilities in PHP

Multiple Vulnerabilities in Apple QuickTime

Cumulative Security Update for Microsoft Edge

TaxAct stated that certain accounts were accessed and the attacker viewed and possibly copied or printed stored tax returns, including customers' SSNs and other sensitive information. TaxAct is offering one year of free credit monitoring and $1 million identity-theft insurance.

JB Autosports, Inc

JB Autosports notified an unknown number of customers who shopped on their subispeed.com and ft86speedfactory.com sites between August 1 and November 9, 2015, that their payment card data was intercepted during transmission and acquired by an unknown party at a Russian IP address. Customers with questions can contact JB Autosports customer service at (888) 885-2002.

Tip of the Week

"Preventing and Responding to Identity Theft"

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to

Cumulative Security Update for Internet Explorer

Vulnerability in VBScript Scripting Engine

Multiple Vulnerabilities in Microsoft Office

Vulnerabilities in Windows Kernel-Mode Drivers

Vulnerability in Microsoft Silverlight

Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader

Vulnerabilities in Microsoft Windows

Cyber News

How websites help criminals phish customers' passwords

via Graham Cluley

Why thinking like a criminal is good for security

via CSO Online

IoT Devices Easily Hacked to be Backdoors: Experiment

via Security Week

Android Trojan Intercepts Voice Call-Based 2FA

via Symantec

Global Operation Against DD4BC Results in Arrests

via WeLiveSecurity

Report: 90% of Mobile Health & Finance Apps Vulnerable to Critical Security Risks

impersonate you to purchase items, open new accounts, or apply for loans.

[Read more about this cyber tip and others from US-CERT]

via TechRepublic

Update: Ukraine Power Outage

On Tuesday, the US Department of Homeland Security announced that its Industrial Control Systems Computer Emergency Response Team (ICS-CERT) is assisting Ukraine in investigating the cyber attack that occurred on December 23, 2015, disrupting electricity distribution at three substations in Western Ukraine. ICS-CERT has confirmed that BlackEnergy malware was involved in the incident, however, the direct cause of the power outages remains unclear. While previous open source reporting indicated a malicious Microsoft Excel attachment was involved, ICS-CERT reported the infection vector appears to have been a Microsoft Word document spread via a spear-phishing email. The ICS Director of the SANS Institute confirmed in a blog post that this was a coordinated incident, involving multiple components, including telephony denial-of-service targeting the utility's call-center in order to prevent customers from reporting outages. We will provide more updates as additional details are confirmed.

ICS Resource: Critical infrastructure asset owners and operators are encouraged to review and implement the strategies identified in ICS-CERT's Seven Steps to Effectively Defend Industrial Control Systems. This paper, published in December 2015, details mitigation measures organizations can take to counter common exploitable weaknesses in control systems.

Questions?

Email a Cyber Liaison Officer at njccic@cyber.nj.gov.

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

DISCLAIMER: This bulletin is provided as is for informational purposes only. The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and the Regional Operations Intelligence Center (ROIC) do not provide any warranties of any kind regarding any information contained within. The NJCCIC and ROIC do not endorse any commercial product or service, referenced in this bulletin or otherwise. Further dissemination of this bulletin is governed by the Traffic Light Protocol (TLP). For more information about TLP, see https://www.us-cert.gov/tlp/.